

Oorlog voeren zonder geweld

*onderzoek naar de regels binnen het humanitair
oorlogsrecht voor militaire cyberoperaties die de
drempel van aanval niet halen*

G.L.C. van den Bosch

© 2019 G.L.C. van den Bosch

Vormgeving: Merel de Hart, Multimedia NLDA

ISBN: 9789493124059

Oorlog voeren zonder geweld

Onderzoek naar de regels binnen het humanitair oorlogsrecht voor militaire cyberoperaties
die de drempel van aanval niet halen

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van Rector Manificus

Prof. dr. ir. K.I.J. Maex

ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Agnietenkapel
op donderdag 24 oktober 2019, te 12.00 uur

door Gijsbertus Lambertus Cornelis **van den Bosch**

geboren te Vlijmen

Promotiecommissie:

Promotores:	Prof. dr. T.D. Gill	Universiteit van Amsterdam
	Prof. dr. P.A.L. Ducheine	Universiteit van Amsterdam

Overige Leden:	Prof. dr. D. Abels	Universiteit van Amsterdam
	Prof dr. T.M. van Engers	Universiteit van Amsterdam
	mr. dr. M. den Heijer	Universiteit van Amsterdam
	Prof. dr. J.K. Kleffner	Swedish National Defence University
	mr. dr. M. Zwanenburg	Ministerie van Buitenlandse Zaken

Faculteit der Rechtsgeleerdheid

voor Astrid

Inhoudsopgave

Inhoudsopgave

Hoofdstuk 1	17
1.1 Inleiding.....	17
1.1.1 Achtergrond.....	18
1.1.2 Het cyberdomein.....	20
1.1.3 Het cyberdomein en militaire operaties	22
1.1.4 Het humanitair oorlogsrecht is van toepassing op militaire operaties in het cyberdomein.....	25
1.2 Centrale vraagstelling en opbouw	27
1.2.1 Centrale vraagstelling	27
1.2.2 Opbouw	28
1.3 Beperkingen.....	28
1.3.1 Alleen tijdens een gewapend conflict	28
1.3.2 Alleen humanitair oorlogsrecht.....	28
1.3.3 De grondbeginselen en de regels	30
1.4 Relevantie van het onderzoek	3
1.4.1 Wetenschappelijk belang	31
1.4.2 Maatschappelijk belang	31
1.4.3 Strategisch belang.....	32
1.4.4 Operationeel en tactisch militair belang.....	33
1.4.5 Onderscheid tussen rechtsregimes	33
Hoofdstuk 2 .De ondergrens van ‘aanval’ in traditionele zin	35
2.1 Inleiding.....	35
2.2 Het doel van het humanitair oorlogsrecht.....	36
2.2.1 Inleiding, een dubbele doelstelling.....	36
2.2.2 De achtergrond van de dubbele doelstelling	38

2.3 De balans tussen militaire noodzaak en humaniteit.....	41
2.3.1 De uitersten	41
2.3.2 Het evenwicht bepalen.....	43
2.3.3 Het evenwicht uitgewerkt in een concrete regel	44
2.4 Toepassingsgebied humanitair oorlogsrecht.....	46
2.4.1 Wat is een gewapend conflict?	47
2.4.1.1 Internationaal gewapend conflict.....	48
2.4.1.2 Niet-internationaal gewapend conflict	50
2.4.2 Conclusie toepassingsgebied humanitair oorlogsrecht	53
2.5 Aanval in de context van het humanitair oorlogsrecht	54
2.5.1 Schematisch overzicht	55
2.5.2 Oorlogvoering	55
2.5.3 Militaire operaties.....	57
2.5.4 Vijandelijkheden	60
2.5.5 Militaire operaties versus vijandelijkheden.....	60
2.6 Aanvallen.....	64
2.6.1 Gericht tegen de tegenstander.....	65
2.6.2 Hetzij defensieve hetzij offensieve	65
2.6.3 Waarom is militaire operatie een breder begrip dan aanval?	66
2.6.4 De ondergrens van aanval	69

Hoofdstuk 3 .Regels uit het humanitair oorlogsrecht van toepassing op militaire operaties die de drempel van aanval niet halen.....73

3.1 Inleiding.....	73
3.2 Gewoonterecht als bron van humanitair oorlogsrecht	74
3.3 Grondbeginselen van het humanitair oorlogsrecht.....	76
3.3.1 Militaire noodzaak	77
3.3.2 Humaniteit	80
3.3.2.1. De keuze van middelen en methoden van oorlogvoering is niet onbegrensd.....	81
3.3.2.2 Veroorzaken van overbodig letsel of onnodig leed is verboden.....	83
3.3.3 Onderscheid	85
3.3.3.1 Het grondbeginsel van onderscheid	86
3.3.3.2 'Ontzien en beschermd'	87
3.3.3.3 Personen	89
3.3.3.3.1 Burgerbevolking en afzonderlijke burgers, algemene bescherming	89
3.3.3.3.2 Bescherming tegen militaire operaties beneden de drempel van aanval..	91

3.3.3.3 Personen zonder bescherming tegen operaties beneden de drempel van aanval	92
3.3.3.4 Personen met gelijke bescherming als burgers tegen operaties beneden de drempel van aanval	92
3.3.3.5 Personen met extra bescherming tegen militaire operaties beneden de drempel van aanval.	93
3.3.3.4 Objecten.....	93
3.3.3.4.1 Burgerobjecten; algemene bescherming	93
3.3.3.4.2 Burgerobjecten; bijzondere bescherming tegen militaire operaties beneden de drempel van aanval	94
3.3.3.5 Voorzorgsmaatregelen.....	96
3.3.3.6 Objecten en onbruikbaarmaking	97
3.3.4 Proportionaliteit	99
3.3.5 Eervol gedrag als grondbeginsel	101
3.3.5.1 Perfidie	104
3.3.5.2 Erkende kentekenen	106
3.3.5.3 Nationaliteitstekenen	107
3.4 Regels uit het humanitair oorlogsrecht van toepassing op militaire operaties die de drempel van aanval niet halen	109
3.4.1 Militaire noodzaak	109
3.4.2 Humaniteit	109
3.4.3 Onderscheid	110
3.4.4 Proportionaliteit	110
3.4.5 Eervol gedrag	110
Hoofdstuk 4 .De ondergrens van aanval in het cyberdomein	113
4.1 Inleiding.....	113
4.2 Het cyberdomein	113
4.2.1 Wat is het cyberdomein?	113
4.2.1.1 Verdragen en internationaal gewoonterecht	113
4.2.1.2 Algemene erkende rechtsbeginselen.....	115
4.2.1.3 Rechterlijke uitspraken en opvattingen van de meest bevoegde schrijvers	116
4.2.1.4 Andere mogelijke bronnen.....	118
4.2.1.5 Het cyberdomein in dit onderzoek.....	119
4.2.2 De componenten van het cyberdomein	120
4.2.2.1 Hebben niet-fysieke componenten een geografische locatie?	120
4.2.2.2 De niet-fysieke componenten van het cyberdomein.	122
4.2.2.3 De componenten van het cyberdomein in dit onderzoek	123

4.3 Het cyberdomein en het internationaal recht	128
4.3.1 Inleiding.....	128
4.3.2 Het cyberdomein en het internationaal recht.....	129
4.4 Militaire cyberoperaties	132
4.4.1 Inleiding	132
4.4.2 Militaire cyberoperaties	134
4.5 De ondergrens van aanval in het cyberdomein	135
4.5.1 Inleiding.....	135
4.5.2 Wat is een cyberaanval?.....	135
4.5.3 Twee verschillende denkrichtingen	137
4.5.4 De status van virtuele componenten in het humanitair oorlogsrecht	140
4.5.4.1 Inleiding.....	140
4.5.4.2 Is de indeling personen-objecten voldoende?.....	140
4.5.4.3 De status van virtuele componenten in het strafrecht	147
4.5.4.3.1 Nationaal strafrecht	147
4.5.4.3.2 Extraterritoriale toepassing van het nationaal strafrecht	149
4.5.4.4 Intellectueel eigendom.....	151
4.5.4.5 Conclusie status virtuele componenten in het humanitair oorlogsrecht. ...	152
4.5.5 Schade aan virtuele componenten	154
4.5.5.1 Drempel voor schade aan virtuele componenten	154
4.5.5.2 Schade aan virtuele componenten in andere rechtsgebieden	157
4.5.5.3 Wanneer zijn fysieke gevolgen mogelijk?.....	158
4.5.5.3.1 Vertrouwelijkheid	159
4.5.5.3.2 Integriteit	160
4.5.5.3.3 Beschikbaarheid	166
4.5.5.3.4 Overlappende beginselen.....	168
4.5.5.3.5 Samenvatting Confidentiality-Integrity-Availability	169
4.5.5.4 Conclusie schade aan virtuele componenten binnen het humanitair oorlogsrecht	169
4.5.6 De ondergrens van cyberaanval	170
4.5.6.1 Terug naar het doel van het humanitair oorlogsrecht	170
4.5.6.2 Humanitair oorlogsrecht wordt gemaakt door staten	172
4.5.6.3 Doorwerking verschuiving jus in bello naar jus ad bellum	173
4.5.6.4 Conclusie.....	174

**Hoofdstuk 5 .Regels uit het humanitair oorlogsrecht voor militaire cyberoperaties
onder de drempel van artikel 49 lid 1 Aanvullend Protocol I en hoe deze
regels worden toegepast177**

5.1 Inleiding.....	177
--------------------	-----

5.2 Militaire noodzaak	177
5.3 Humaniteit.....	179
5.3.1 De keuze van methoden en middelen van oorlogvoering is niet onbegrensd ..	179
5.3.2 Veroorzaken van overbodig letsel of onnodig leed is verboden	183
5.4 Onderscheid.....	183
5.4.1 Het grondbeginsel van onderscheid	183
5.4.2 'Ontzien en beschermd'	184
5.4.3 Personen	185
5.4.3.1 Burgerbevolking en afzonderlijke burgers, algemene bescherming	185
5.4.3.2 Personen met bijzonder bescherming	185
5.4.4 Objecten.....	186
5.4.4.1 Burgerobjecten; algemene bescherming	186
5.4.4.2 Burgerobjecten; bijzondere bescherming	187
5.4.5 Voorbereiding	191
5.5 Proportionaliteit	193
5.6 Eervol gedrag als grondbeginsel.....	194
5.6.1 Perfidie	194
5.6.2 Erkende kentekenen	195
5.6.3 Nationaliteitskentekenen	197
5.7 Regels van humanitair oorlogsrecht van toepassing op militaire cyber operaties beneden de grens van aanval.	199
5.7.1 Militaire noodzaak	199
5.7.2 Humaniteit	199
5.7.3 Onderscheid	200
5.7.3.1 Personen	200
5.7.3.2 Objecten.....	200
5.7.3.3 Voorbereiding.....	201
5.7.4 Proportionaliteit	201
5.7.5 Eervol gedrag	201
5.8 Conclusies en synthese.....	202
Samenvatting.....	211
Summary	221
Verdragen	229

Uitspraken	233
Geraadpleegde literatuur	235
Overige publicaties	253

1

Hoofdstuk 1

1.1 Inleiding

Mag je een vijandelijk radarstation uitschakelen, door met een cyberoperatie de stroomvoorziening van het gebied waar het radarstation zich bevindt plat te leggen? Mag je een vijandelijke commandant 'uitschakelen', door heimelijk kinderporno op zijn computer te zetten en dit vervolgens te laten lekken, waardoor hij publiekelijk aan de schandpaal wordt genageld en daardoor het gezag en vertrouwen van zijn soldaten verliest? Mag je de bankrekening van vijandelijke soldaten wissen met als waarschijnlijk gevolg dat zij gedemotiveerd raken en minder bereid zullen zijn te vechten? Mag je jezelf voordoen als iemand anders en vervolgens berichten versturen aan de familieleden van militairen met dreigende en intimiderende boodschappen?¹ Zomaar vier vragen uit een ontelbare reeks van mogelijke vragen die je kunt stellen naar aanleiding van nieuwe mogelijkheden voor oorlogvoering, die zijn ontstaan door de opkomst van het cyberdomein en met name internet. Deze vragen zijn interessant, omdat bovenstaande acties de uitkomst van een gewapend conflict kunnen beïnvloeden, zonder dat daarbij geweld gebruikt hoeft te worden. De antwoorden op de vragen zijn in een aantal gevallen echter juridisch uitdagend.

Kijkend naar het humanitair oorlogsrecht, het rechtsgebied binnen het internationaal publiekrecht dat gewapende conflicten reguleert en soms beperkt door bepaalde categorieën personen en objecten te beschermen,² valt op dat de aandacht grotendeels is gericht op het gebruik en de regulatie van militair geweld en veel minder op militaire operaties waarbij geen geweld wordt gebruikt. Dit betekent niet dat deze laatste operaties niet bestonden ten tijde van de ontwikkeling van het huidige humanitair oorlogsrecht, denk bijvoorbeeld aan inlichtingenoperaties, of psychologische operaties. Deze operaties hadden echter minder schadelijke gevolgen en waren vooral van ondersteunende aard voor operaties met militair geweld, die uiteindelijk de beslissing binnen een gewapend conflict moesten brengen. De mogelijkheid dat dit laatste gewijzigd is met de komst van de nieuwe mogelijkheden in het cyberdomein, waarin volgens sommigen alle militaire doelstellingen binnen een gewapend conflict te behalen zouden zijn zonder de toepassing van geweld,³ lijkt niet erg realistisch. Toch is het van belang, daar waar nieuwe mogelijkheden ontstaan om in een gewapend conflict op te treden, te weten hoe hiermee om te gaan binnen de grenzen van het humanitair oorlogsrecht.⁴ Omdat, zoals hiervoor opgemerkt, veel van de

1 <https://www.military.com/daily-news/2018/05/08/russians-posed-isis-hackers-threatened-us-military-wives.html> laatst geraadpleegd 28 nov. 2018. Dit is een voorbeeld uit de praktijk waarbij Russische hackers zich voordeden als IS-strijders en familieleden van Amerikaanse militairen bedreigden.

2 Op de rol die het humanitair oorlogsrecht speelt binnen een gewapend conflict kom ik in het volgende hoofdstuk uitgebreid terug.

3 Smith 2008, p. 272.

4 Dit is een verplichting die gecodificeerd is in bijvoorbeeld art. 36 Aanvullend Protocol I: "Op een Hoge Verdragsluitende Partij rust bij de bestudering, ontwikkeling, aanschaf of invoering van een nieuw wapen, een nieuw middel of een nieuwe methode van oorlogvoering de verplichting, vast te stellen of het gebruik daarvan, in bepaalde of in alle omstandigheden,

regels uit het humanitair oorlogsrecht gericht zijn op geweldgebruik, is relatief minder aandacht geweest voor militaire operaties zonder geweldgebruik. Hierdoor zijn vragen over dit soort militaire operaties binnen het humanitair oorlogsrecht soms lastig te beantwoorden, als al een antwoord gevonden kan worden. Soms zullen de bestaande regels zo uitgelegd moeten worden dat ze toepasselijk en toepasbaar zijn voor de nieuwe mogelijkheden voor militair optreden in het cyberdomein⁵ en daar waar dit onmogelijk blijkt, zijn misschien nieuwe regels noodzakelijk.

1.1.1 Achtergrond

Nederland is een democratische rechtsstaat. Dit houdt onder meer in dat het geweldsmonopolie bij de staat ligt en dat in Nederland het mogelijke gebruik van dat geweldsmonopolie, de zogenaamde zwaarmacht, is vastgelegd in democratisch tot stand gekomen wetten. Voor de krijgsmacht is dit geregeld in artikel 97 van de Grondwet waarin, naast het bestaan van de krijgsmacht, ook de doelomschrijving is weergegeven.⁶ Defensie heeft de doelomschrijving uit de Grondwet in de Defensienota 2000 uitgewerkt in een drietal hoofdtaken⁷ namelijk:

1. De bescherming van de integriteit van het eigen en het bondgenootschappelijke grondgebied, inclusief de Nederlandse Antillen en Aruba;
2. De bevordering van de internationale rechtsorde en stabiliteit;
3. De ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal.⁸

In hetzelfde grondwetsartikel staat dat het de regering is die bepaalt waarvoor en wanneer de krijgsmacht wordt ingezet.⁹ Het is evident dat de regering zich daarbij dient te houden aan de geldende rechtsregels, zowel nationaal¹⁰ als internationaal.¹¹ Dit geldt niet alleen voor de regering maar voor alle overheidsorganen. Dit is voor de krijgsmacht niet anders, temeer indien men beschouwt dat de taken mogelijkserwijs uitgevoerd moeten worden met

door dit Protocol of door enige andere regel van het ten aanzien van de Hoge Verdragsluitende Partij toepasselijke volkenrecht is verboden.”

5 De Nederlandse overheid erkent het cyberdomein als vijfde domein voor militair optreden, naast land, zee, lucht en ruimte, zie bijvoorbeeld de Defensie Cyber Strategie, Kamerstukken II 2011-2012 33.321 nr. 1.

6 Art. 97 lid 1 Grondwet luidt: “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.”

7 Ducheine & Arnold 2015, p. 59.

8 Defensienota 2000, Kamerstukken II 1999-2000, 26900 nr. 1-2, p. 41. Later diverse malen herhaald laatstelijk in de Defensienota 2018: Investeren in onze mensen, slagkracht en zichtbaarheid Kamerstukken II 2017-2018, 34919 nr. 2.

9 Art. 97 lid 2 Grondwet luidt: “De regering heeft het oppergezag over de krijgsmacht”

10 Ducheine 2008, p. 3. “De overheid dient zich bij de bescherming van de rechtsstaat en haar onderdanen te houden aan de grenzen die de rechtsstaat zelf stelt.”

11 De verplichting van een staat zich te houden aan het internationaal recht in het algemeen en het humanitair oorlogsrecht in het bijzonder wordt gerekend tot het gewoonterecht. Heckaerts & Doswald-Beck 2005, p. 495 Rule 139, “The obligation of States to respect international law is part of their general obligation to respect international law”.

gebruikmaking van militair geweld. Het kan daarbij gaan om kleinschalige, lichte vormen van geweld tot en met het uitvechten van een *full scale war* met diverse schakeringen binnen het geweldsspectrum daartussenin.

De rechtsregels voor het optreden van de krijgsmacht in het hoogste deel van het geweldsspectrum, het deelnemen aan gewapende conflicten, worden grotendeels bepaald door het internationaal recht en meer in het bijzonder het *ius ad bellum* en het *ius in bello* waarbij het eerste de rechtsbases bestrijkt en het tweede het toepasselijke rechtsregime. Anders gezegd, het *ius ad bellum* bepaalt wanneer een staat rechtmatig gebruik mag maken van militair geweld en het *ius in bello* geeft de regels hoe dat militair geweld toegepast moet worden in een gewapend conflict.¹² Omdat ik mij in dit onderzoek zal richten op de regels die van kracht zijn tijdens een gewapend conflict zal ik vanaf hier primair aandacht besteden aan het *ius in bello*.¹³

De focus op het *ius in bello* is ook de reden dat ik geen aandacht besteed aan mensenrechten. Hoewel “*International Human Rights Law and Law of Armed Conflict are generally considered to be complementary*”,¹⁴ biedt het rechtsbeginsel *lex specialis derogat lex generalis* de oplossing om de toepasselijke rechtsregels te vinden.¹⁵ “*Where both regimes [International Human Rights Law and the Law of Armed Conflict] cover a particular aspect, there can be no doubt that the norm that regulates that aspect in most detailed fashion prevails over the other norm by application of the maxim of lex specialis*”¹⁶ In het geval van een gewapend conflict zal voor militaire operaties gericht tegen de vijand het humanitair oorlogsrecht de *lex specialis* zijn, waardoor het mensenrechtenregime geen nadere aandacht behoeft in dit onderzoek.

Het huidige *ius in bello* is een weerslag van een ontwikkeling van vele decennia gebaseerd op grondbeginselen die soms nog (veel) verder terug gaan in de tijd. Van belang hier is te beseffen dat het stelsel ontwikkeld is met het oog op het reguleren van klassiek militair optreden met de nadruk op het zogenaamde kinetisch optreden.¹⁷ Met dit laatste bedoel ik het fysiek schade of letsel toebrengen aan een tegenstander of het fysiek bezetten dan wel beheersen van bepaalde gebieden. Dit vindt zijn weerslag in veel van de regels. Zo mogen binnen het humanitair oorlogsrecht bijvoorbeeld alleen militaire doelen worden aangevallen, waarbij militaire doelen zijn gedefinieerd als “objecten die naar hun aard, ligging of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarbij de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden

12 Zie bijv. Ducheine 2008, p. 6.

13 Andere vaak gebezigde termen voor het *ius in bello* zijn humanitair oorlogsrecht (HOR), *Law of Armed Conflict* (LOAC), law of war, internationaal humanitair recht en *international humanitarian law* (IHL). In het vervolg van dit onderzoek zal ik zoveel mogelijk de term humanitair oorlogsrecht gebruiken.

14 Pouw 2013, p. 440.

15 Turns in Evans 2010, p. 816.

16 Pouw 2013, p. 457. Voor verdere behandeling en nuances van dit onderwerp, zie Pouw 2013.

17 De term ‘kinetisch’ verwijst hier naar het militaire optreden gebaseerd op het vrijlaten van kinetische energie in hoofdzak veroorzaakt door explosies.

van dat moment een duidelijk militair voordeel oplevert.”¹⁸ Andere regels beschermen specifieke objecten of personen juist tegen een aanval, waarbij onder aanvallen in deze context moet worden verstaan, “*dadens van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve.*”¹⁹ Deze laatste definitie van aanval is van een niet te overschatten betekenis binnen het humanitair oorlogsrecht omdat het voldoen aan deze definitie een aantal, veelal beperkende, bepalingen met zich meebrengt.²⁰

Relatief minder aandacht is er binnen het humanitair oorlogsrecht geweest voor militaire operaties die niet voldoen aan de criteria van aanvallen zoals gedefinieerd in artikel 49 Aanvullend Protocol I.²¹ Zoals eerder vermeld zijn ook andere militaire operaties mogelijk, denk bijvoorbeeld aan psychologische oorlogvoering²² of elektromagnetische oorlogvoering,²³ maar deze werden toch vooral gezien als ondersteunende operaties. De ‘echte’ militaire doelen werden behaald met klassiek (kinetisch) militair optreden. De vraag is hoe zich dit verhoudt met de komst van het nieuwe cyber, of digitale, domein, waarin ook militaire operaties plaats kunnen vinden.

1.1.2 Het cyberdomein

Het cyberdomein²⁴ onderscheidt zich doordat het maar deels een fysiek domein is.²⁵ Het domein heeft weliswaar fysieke componenten, zenders, satellieten, computers etc.,²⁶ maar het belang ligt vooral in de niet-fysieke, ook wel aangeduid als virtuele, componenten. Het ontstaan van dit domein, en het gebruik ervan voor militaire operaties, maakt deel uit van een veel bredere ontwikkeling, door sommigen aangeduid als de derde transformatiegolf van onze geschiedenis.²⁷ Deze ontwikkeling wordt gekenmerkt door een verschuiving in de relatie tussen tastbare en niet-tastbare methoden van productie en destructie. “*Knowledge, in its broadest sense, [...] has moved from a peripheral to a central position, where ideas, innovation, values, imagination, symbols, and imagery, not just computer data, play more and more important roles.*”²⁸

18 Art. 52 lid 2 Aanvullend Protocol I, mijn accentuering.

19 Art. 49 lid 1 Aanvullend Protocol I, mijn accentuering.

20 Zo mogen in een internationaal gewapend conflict burgers niet het doelwit van een aanval zijn, art. 51 lid 2 Aanvullend Protocol I, mogen burgerobjecten niet het doelwit zijn van een aanval, art. 52 lid 1 Aanvullend Protocol I, maar moeten ook voorzorgsmaatregelen getroffen worden bij een aanval, art. 57 lid 2 Aanvullend Protocol I. Bij een niet-internationaal gewapend conflict is een soortgelijke bepaling voor burgers en burgerobjecten opgenomen onder art. 13 lid 2 Aanvullend Protocol II.

21 Voluit: Aanvullend Protocol I bij de Verdragen van Genève van 12 augustus 1949, betreffende de bescherming van slachtoffers van internationale gewapende conflicten. In het vervolg van dit onderzoek zal ik de verkorte aanduiding Aanvullend Protocol I en Aanvullend Protocol II gebruiken.

22 *Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*, AAP-6 (2014)

23 *Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects*, AAP-6 (2014)

24 Op wat precies verstaan wordt onder het cyberdomein kom ik later uitgebreid terug.

25 Zie bijv. Tradoc 525-7-8 2018, p. 8-9.

26 Vaak aangeduid onder de verzamelnaam ‘hardware’, zie bijv. Schmitt 2013, p. 259.

27 Toffler & Toffler in Arquilla & Ronfeldt 1997, *The new Intangibles* p. xiv. De eerste respectievelijk tweede transformatiegolf waren de neolithische en industriële revolutie. Zie ook van Haaster 2018, p. 71-72.

28 Toffler & Toffler in Arquilla & Ronfeldt 1997, *The new Intangibles* p. xiv.

Of het cyberdomein wel of niet een zelfstandig vijfde operatiegebied voor militair optreden²⁹ vormt, is voor dit onderzoek van ondergeschikt belang.³⁰ Het gaat om de militaire operaties die mogelijk zijn in of via het cyberdomein. Duidelijk is dat ook Nederland zijn krijgsmacht in wil kunnen zetten in dit cyberdomein, wat onder andere blijkt uit de aankondiging in 2012 door de minister van Defensie: “De Nederlandse krijgsmacht [...] wil in het digitale domein de vooraanstaande rol spelen die bij ons land past. Om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt zij het vermogen om *cyber operations* uit te voeren.”³¹

De ontwikkeling van het cyberdomein voltrekt zich in een min of meer voorspelbare trend van exponentieel versnellende groei op het gebied van de rekenkracht en opslagcapaciteit van computers en de overdrachtssnelheid van gegevens.³² Hiermee is een zichzelf versterkend proces op gang gekomen. De mogelijkheden van meer en snellere verbindingen, rekenkracht en opslagcapaciteit leidt tot meer cybertoeepassingen. Er ontstaat een trend van *dematerialization* waarmee wordt bedoeld op “*the elimination of materials altogether for certain functions*.”³³ Een sprekend voorbeeld is de mobiele telefoon. Hierin zijn functies als “*(alarm) clocks, calendars, calculators, cameras, flashlights, mail correspondence, phones, phonebooks, voice recorders, notepads, maps, compasses, books, music players, remote controls, newspapers, navigational systems, keys, wallets and a suitcase worth of other items*” beschikbaar.³⁴ Daarbovenop heeft een mobiele telefoon toegang tot “*libraries worth of content, such as news, books, music, photos, videos, and other kinds of content, on a virtually limitless cloud, on top of which sits God-like computation power*.”³⁵ Deze *dematerialization* leidt weer tot toename van meer en snellere verbindingen, rekenkracht en opslagcapaciteit. Alhoewel de mobiele telefoon, of welke andere computer dan ook, geen volledige vervanging van de fysieke goederen zal zijn, is het belang van fysieke goederen ten opzichte van virtuele zaken³⁶ wel afgenomen. Met andere woorden, “*bits are replacing atoms and they are doing so at an exponential pace*,”³⁷ of om een praktisch voorbeeld te geven, wie gebruikt er nog papieren telefoonboeken, als deze überhaupt nog verkrijgbaar zouden zijn?

29 Voor erkenning als domein voor militaire operaties zie bijvoorbeeld Law of War Manual 2015, p. 995, NATO Warsaw Communiqué 9 July 2016 par 70-71 http://www.nato.int/cps/en/natohq/official_texts_133169.htm. Voor Nederland zie bijv. Defensie Cyber Strategie, Kamerstukken II 2011-2012 33.321 nr. 1.

30 In par. 1.1.3 kom ik hier op terug.

31 Kamerstukken II 2011-2012, 33 321, nr. 1, p. 1.

32 Kurzweil 2008, hoofdstuk 2, p 35-72.

33 Keulen 2018, p. 24.

34 Keulen 2018, p. 24.

35 Keulen 2018, p. 24.

36 De vraag of virtuele zaken kunnen kwalificeren als goederen, en meer speciaal als objecten in het humanitair oorlogsrecht, komt uitgebreid aan de orde in Hoofdstuk 4.

37 Keulen 2018, p. 25. In dezelfde zin spreekt McCormack 2018, p. 239 van “*a growing ‘objectification’ of data.*”

Naarmate bovenstaande trend verder doorzet wordt de samenleving meer en meer afhankelijk van niet-tastbare of virtuele zaken, waardoor het niet beschikbaar zijn van deze virtuele zaken³⁸ steeds grotere, beoogde en onvoorziene, consequenties kan hebben.

1.1.3 Het cyberdomein en militaire operaties

Wat betekent de ontwikkeling van het cyberdomein voor de uitvoering van militaire operaties? Als eerste is bovengenoemde trend van *dematerialization* van invloed op militaire operaties. Indien militaire operaties vooral gericht zijn op of tegen fysieke personen en objecten is kinetisch optreden vaak de eerste optie, en soms de enige manier om een operatie te laten slagen. Bij militaire operaties tegen virtuele zaken hoeft kinetisch optreden niet de enige optie te zijn. Alhoewel kinetische cyberoperaties zeker tot de mogelijkheden behoren³⁹ bieden *non-violent* of *non-kinetic* militaire operaties gericht op of tegen virtuele zaken juist nieuwe mogelijkheden. Naarmate het belang van de *bits* ten opzichte van de *atoms* toeneemt zullen ook de mogelijkheden voor niet-kinetische militaire operaties op twee manieren groeien. Ten eerste zal een tegenstander, als gevolg van de toegenomen reken- en opslagcapaciteit van computers, de betere en snellere verbindingsmogelijkheden voor uitwisseling van gegevens en de hierboven beschreven *dematerialization*, steeds afhankelijker worden van virtuele zaken en dus steeds meer virtuele zaken hebben waarop militaire operaties gericht kunnen worden. Ten tweede zullen de mogelijkheden om zelf gebruik te maken van niet-fysieke middelen, bijvoorbeeld computerprogramma's toenemen.

Het beschikbaar komen van nieuwe mogelijkheden dwingt bepaalde concepten opnieuw te bezien in het licht van deze veranderingen, ook het concept van militaire operaties. Volgens sommigen verandert zelfs het concept van oorlogvoering⁴⁰ van “*war is contention between two or more states through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases*”⁴¹ naar “*to establish a condition or conceptual space in which the political objective can be obtained by other means and in other ways. We seek to create a conceptual space for diplomacy, economic incentives, political pressure and other measures to create a desired political outcome of stability, and if possible democracy.*”⁴²

Deze laatste ontwikkeling, dat het concept van oorlogvoering verandert door de ontwikkeling van het informatiedomein, onderschrijf ik niet. Ten eerste omdat, indien al sprake is van een ontwikkeling en niet van een tijdelijke verschuiving, deze ontwikkeling met name plaatsvindt in de westerse denkwijze over oorlogvoering die niet geldt voor oorlogvoering in het algemeen.

38 Dit kan tijdelijk of permanent zijn, bijvoorbeeld doordat ze onbruikbaar of onvindbaar gemaakt zijn. Ook kan verstoring optreden omdat deze virtuele zaken, bijv. door manipulatie, andere uitkomsten genereren dan zonder manipulatie het geval zou zijn.

39 Zie bijv Applegate, 2013 *The Dawn of Kinetic Cyber*.

40 Dinniss 2012, p. 23.

41 Lauterpacht 1953, p. 202 geciteerd in Harrison-Dinniss 2012, p. 23.

42 Smith 2005, p. 270 geciteerd in Harrison-Dinniss 2012, p. 23.

De tweede, en voor mij belangrijkste, reden is dat een staat naast het militaire machtsmiddel andere machtsmiddelen ter beschikking heeft om zijn doelen te bereiken, maar dat het militaire machtsmiddel als zodanig door de opkomst van het cyberdomein niet is veranderd. Naast militaire middelen noemt de Nederlandse Defensie Doctrine diplomatie, economie en informatie als machtsmiddel.⁴³ Dit onderzoek richt zich op de regels die gelden binnen het humanitair oorlogsrecht, maar opgemerkt moet worden dat het militair optreden in een gewapend conflict onderdeel kan, en meestal zal, zijn van een *Grand Strategy*⁴⁴ waarbij de scheidslijn tussen de uitwerking van de machtsmiddelen waarover een staat beschikt soms minder makkelijk aan te brengen is dan op het eerste gezicht lijkt. Zeker als men beziet dat “een trend waarneembaar [is] van een verschuiving van militaire inzet die niet per definitie zelfstandig gebeurt” naar “militaire inzet die per definitie niet zelfstandig gebeurt.”⁴⁵ Een staat kan derhalve een mix van machtsmiddelen inzetten voor oorlogvoering, waarbij overigens alleen het gebruik van het militaire machtsmiddel, dat wil zeggen de inzet van militaire middelen,⁴⁶ zal vallen onder het regime van het humanitair oorlogsrecht.

Dat het militaire machtsmiddel ‘slechts’ een onderdeel is van het totale pakket aan mogelijkheden waarover een staat beschikt komt ook duidelijk naar voren binnen het concept van hybride oorlogvoering. Deze vorm van oorlogvoering, vaak toegeschreven aan Rusland naar aanleiding van de gebeurtenissen op de Krim in 2014 is wel omschreven als de “georkestreerde inzet van conventionele militaire middelen, irreguliere strijdmethoden, subversieve activiteiten, inzet van paramilitaire eenheden, opruiing, psychologische oorlogvoering, propaganda, media manipulatie, misleidingsactiviteiten, inzet van speciale eenheden zonder herkenningstekens op het uniform, cyberaanvallen en controle over media met op de achtergrond dreiging met escalatie van het conflict en tegelijkertijd ontkenning van betrokkenheid bij wat er op het strijdtoneel plaatsvindt.”⁴⁷ Alhoewel niet altijd duidelijk is wat precies bedoeld wordt met de term ‘hybride oorlogvoering’,⁴⁸ is een aantal generieke kenmerken te onderkennen.⁴⁹ Een van die generieke kenmerken is het gebruik van een combinatie van middelen en instrumenten waarbij een actor gebruik maakt van “een mix van traditionele en moderne middelen, letaal en niet-letaal. Oorlogvoering

43 Nationale Defensie Doctrine 2013, p. 21. Andere landen volgen eenzelfde indeling, zie bijvoorbeeld de Amerikaanse JP-1, *Doctrine for the Armed Forces of the United States*, die DIME (afkorting voor Diplomatic, Informational, Military, Economic) zien als de theoretische Instruments of National Power.

44 *Grand Strategy* is de gecoördineerde, systematische ontwikkeling en aanwending van alle machtsmiddelen van een staat, een bondgenootschap of coalitie, om nationale, bondgenootschappelijke of coalitiebelangen te behartigen, Nationale Defensie Doctrine 2013, p. 105. Opgemerkt kan worden dat Nederland geen formeel uitgebrachte *Grand Strategy* kent.

45 Nationale Defensie Doctrine 2013, p. 24.

46 Personeel, materieel of een combinatie daarvan.

47 Osinga 2016, p. 17.

48 MCDC 2017, p. 3. “The international consensus on ‘hybrid warfare’ is clear: no one understands it but everyone, including NATO and the European Union, agrees it is a problem.” De NAVO heeft geen definitie maar omschrijft *hybrid warfare* als “a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives.” Warsaw Summit Communiqué 2016, par. 72.

49 Saathof 2018, p. 251.

beperkt zich niet alleen meer tot het inzetten van het militaire machtsinstrument.⁵⁰ Een hybride tegenstander maakt gebruik van alle machtsinstrumenten: “*diplomatic, information, military, economic, financial, intel, legal/law enforcement (DIMEFIL)*.”⁵¹

De constatering dat het militaire machtsmiddel onderdeel is van een groter pakket aan machtsmiddelen is met de opkomst van het cyberdomein niet veranderd. Wat mogelijk wel verandert met de komst van nieuwe mogelijkheden in het cyberdomein is een verschuiving in de onderlinge verhoudingen tussen de machtsmiddelen. Het toenemen van mogelijkheden binnen een van de machtsmiddelen kan leiden tot een relatieve toename van het belang binnen een *Grand Strategy*. Een voorbeeld van deze verschuiving noemt Ducheine: “*Whereas western armed forces tend to focus on kinetic action (and thus kinetic targeting) and support that action with other lines of action (e.g., information activities), irregular armed forces have reversed this practice. Groups like Al Qaeda, Hamas and to some extent Anonymous place more emphasis on information activities and use physical action to supplement them.*”⁵²

Het zijn overigens niet alleen niet-statelijke actoren die aandacht hebben voor niet-kinetische oorlogvoering. Zo beschrijft Halper dat China het belang van niet-kinetische oorlogvoering in het informatietijdperk erkent.⁵³ Public opinion warfare, bestaande uit *psychological warfare, legal warfare en media warfare*, is oorlogvoering met andere middelen.⁵⁴ De visie dat China ‘*all means whatsoever*’, dus inclusief niet-kinetische middelen en methoden, in zal zetten om zijn strategische doelstellingen te verwezenlijken komt ook terug in het concept van *unrestricted warfare*.⁵⁵ Volgens deze theorie is het voor China steeds moeilijker de doelstellingen voor een toekomstige oorlog vast te stellen omdat “*the goals of warfare have become blurred due to the pursuit of a variety of agendas. Thus, it is more and more difficult for people to say clearly just why they are fighting*”⁵⁶ waarbij “het conventionele en technologische gevechtsveld in elkaar overlopen.”⁵⁷ Om succesvol te kunnen zijn in een dergelijke omgeving is het noodzakelijk “de verschillende methodes, niveaus, middelen, actoren en domeinen van oorlogvoering met elkaar te combineren.”⁵⁸ Het militaire machtsinstrument heeft in deze theorie niet langer het monopolie op oorlogvoering, wat terugkomt in de omschrijving van deze theorie: ‘*unrestricted warfare*’.

De exponentiële groei van het cyberdomein, de trend van *dematerialization* met de daarmee samenhangende afhankelijkheid van niet-fysieke zaken, de toenemende mogelijkheden voor niet-fysieke militaire operaties gecombineerd met de eerdergenoemde ambitie een

50 Saathof 2018, p. 251.

51 Saathof 2018, p. 251.

52 Ducheine in Ducheine, Schmitt & Osinga 2015 p. 202.

53 Halper 2013, p. 12.

54 Halper 2013, p. 222.

55 Xiangsui & Liang 1999.

56 Xiangsui & Liang 1999, p. 38.

57 Saathof 2018, p. 257.

58 Saathof 2018, p. 258.

operationele cybercapaciteit te ontwikkelen, maken dat (hernieuwde) aandacht voor militaire operaties die niet vallen onder de definitie van aanval binnen het humanitair oorlogsrecht zoals gedefinieerd in artikel 49 Aanvullend Protocol I, opportuun is. Bij deze hernieuwde belangstelling rees de vraag of het humanitair oorlogsrecht als geheel en de individuele regels die gelden voor reguliere militaire operaties ook (onverkort) gelden voor militaire operaties in het cyberdomein of dat een aanpassing of aanvulling noodzakelijk is. Dit laatste zou dan mogelijk een gevolg kunnen zijn van de eerdergenoemde focus op het kinetisch optreden bij de ontwikkeling van het humanitair oorlogsrecht. Inmiddels lijkt de vraag over de geldigheid van het humanitair oorlogsrecht in zijn algemeen positief beantwoord te kunnen worden.⁵⁹

1.1.4 Het humanitair oorlogsrecht is van toepassing op militaire operaties in het cyberdomein

Een uitgangspunt van dit onderzoek is dat het humanitair oorlogsrecht van toepassing is op militaire operaties in het cyberdomein voor zover deze zich afspelen in een gewapend conflict.⁶⁰ Dit volgt uit de volgende logische redenering. Oorlogvoering is de meest omvattende term waarop het humanitair oorlogsrecht van kracht is.⁶¹ Het maakt daarbij niet uit binnen welk domein, of combinatie van domeinen, die oorlogvoering plaatsvindt. Het humanitair oorlogsrecht geldt voor oorlogvoering in het kader van een gewapend conflict in zijn geheel en is daarmee onafhankelijk van het middel en de methode waarmee, of het domein waarin, de oorlogvoering plaatsvindt. Laat ik dit verduidelijken met een voorbeeld.

Neem de uitschakeling van een vijandelijk radarstation.⁶² Indien dit geschiedt door middel van een bombardement vanuit de lucht, een artilleriebeschieting vanaf zee of een specifieke operatie met behulp van *special forces*, in al deze gevallen zijn de regels van het humanitair oorlogsrecht van kracht. Het zou onlogisch zijn als, indien hetzelfde effect bereikt kan worden met een cyberoperatie,⁶³ voor deze laatste operatie de regels van het humanitair oorlogsrecht niet zouden gelden.⁶⁴ De redenering dat deze cyberoperatie niet onder het humanitair oorlogsrecht valt, zou leiden tot de situatie van een methode van oorlogvoering niet vallend onder het humanitair oorlogsrecht,⁶⁵ met andere woorden, “dit zou met recht een juridisch zwart gat opleveren.”⁶⁶

59 Zie ook par. 1.1.4 hierna.

60 Dit uitgangspunt wordt breed geaccepteerd. Zie bijv. Schmitt 2013, p. 5, Henckarts & Doswald-Beck, 2005 p. xxxvi, ILA 2016b, p. 3.

61 Ik kom hier in Hoofdstuk 2 op terug.

62 Uiteraard binnen de context van een gewapend conflict, anders is het humanitair oorlogsrecht niet van toepassing.

63 Wat ik versta onder een cyberoperatie behandel ik in Hoofdstuk 4.

64 In dezelfde zin Schmitt en Watts 2015, p. 221: “*Assertions of non-applicability, however, fly in the face of the object and purpose of IHL.*”

65 Dit nog los van het feit dat voor de uitvoering van een cyberoperatie ook fysieke componenten nodig zullen zijn (denk daarbij aan operators maar ook computers en cyberinfrastructuur) welke componenten worden gedeeld met andere domeinen (zie hiervoor par. 2.2.2). Via deze fysieke componenten is daarmee het humanitair oorlogsrecht ook van toepassing op de cyberoperatie.

66 Ducheine 2008, p. 539.

Het humanitair oorlogsrecht is van toepassing op alle middelen en methoden van oorlogvoering. Het geldt voor bestaande en toekomstige middelen en methoden van oorlogvoering of, zoals verwoord door het *International Court of Justice*: “the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and all kinds of weapons, those of the past, those of the present and those of the future.”⁶⁷ Humanitair oorlogsrecht is daarmee middel en methode onafhankelijk. Dit kan “omdat het internationaal recht adaptief is, en het oorlogsrecht steeds in staat is geweest nieuwe technologie te omarmen.”⁶⁸ Elke keer als een nieuwe ontwikkeling vraagtekens oproept over de toepasbaarheid van het humanitair oorlogsrecht en de daaruit voortkomende roep om “adopting a new treaty coming to grips with this controversial innovation”⁶⁹ resulteerde dit in de conclusie dat de nieuwe ontwikkeling moet voldoen aan de “general rules of LOAC.”⁷⁰

Het feit dat het humanitair oorlogsrecht van toepassing is, betekent nog niet dat daarmee alle vragen opgelost zijn. Zoals altijd bij nieuwe ontwikkelingen zullen zich problemen voordoen bij de interpretatie en toepassing van de bestaande regels van het humanitair oorlogsrecht op de nieuwe middelen of methoden van oorlogvoering. Dit doet dan de vraag rijzen “whether existing law is sufficiently clear or whether there is a need to clarify IHL or develop new rules to deal with these challenges?”⁷¹

Onduidelijkheid over de toepasselijkheid en toepassing van bestaande regels uit het humanitair oorlogsrecht kan op een tweetal manieren tot ongewenste resultaten binnen een gewapend conflict leiden.

Als eerste kan bij onduidelijkheid een regel verkeerd worden toegepast met als gevolg dat een humanitair oorlogsrechtelijke regel wordt geschonden. Een dergelijke schending kan leiden tot strafrechtelijke gevolgen voor de persoon die de regel heeft overtreden, of daar strafrechtelijk voor verantwoordelijk gehouden kan worden. Daarnaast zal een staat, onder wiens verantwoordelijkheid de militaire operaties worden uitgevoerd, de verplichting “[to] respect and ensure respect for international humanitarian law by its armed forces and other persons or groups acting in fact on its instructions, or under its direction or control”, een verplichting die gerekend wordt tot het gewoonterecht,⁷² schenden.

Als tweede kunnen, bij onduidelijkheid, militaire cyberoperaties niet serieus genomen worden als alternatief voor kinetische operaties, of zelfs helemaal niet als alternatief in beeld komen.⁷³ Hierdoor blijft mogelijk een scala aan alternatieve militaire operaties onbedoeld onbenut.

67 *International Court of Justice* 1996, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion par. 86.

68 Ducheine 2016, p. 17.

69 Dinstein 2013, p. 286. Verwijzend naar de inzet van het nieuwe middel onderzeeër in de Eerste Wereldoorlog.

70 Dinstein 2013, p. 286.

71 ICRC 2015, p. 39.

72 Henckaerts & Doswald-Beck 2005, p. 495.

73 Van Haaster 2018, p. 16 noemt dit “the negligence towards ‘the cyber option’”.

1.2 Centrale vraagstelling en opbouw

1.2.1 Centrale vraagstelling

Als de regels voor militair optreden in een gewapend conflict ook gelden voor militaire operaties in het cyberdomein mag dan geconcludeerd worden dat er weinig problemen op zullen treden bij de implementatie van deze regels? Kunnen alle regels zonder meer worden toegepast of is nadere uitleg en definiëring van begrippen, en mogelijk regels, voor toepassing in het cyberdomein noodzakelijk?

Hierboven is al opgemerkt dat de aandacht in het humanitair oorlogsrecht, weliswaar niet exclusief maar toch wel grotendeels, gericht is op het traditioneel kinetisch militair optreden, dat wil zeggen gericht op het fysiek schade of letsel toebrengen. Hierbij neemt het begrip ‘aanval’, zoals gedefinieerd in Aanvullend Protocol I artikel 49, een centrale plaats in. Een van de uitdagingen is de interpretatie van het begrip ‘aanval’ wanneer deze plaatsvindt in of via het cyberdomein. Wat moet hieronder binnen het humanitair oorlogsrecht worden verstaan?

De groep experts die de in 2013 gepubliceerde *Tallinn Manual on the International Law applicable to Cyber Warfare*⁷⁴ samenstelde, lijkt de traditionele focus op fysieke schade of letsel te volgen. Zij definiëren een cyberaanval als “a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects”,⁷⁵ daarbij duidelijk aansluitend bij de eerdergenoemde definitie van aanval uit artikel 49 lid 1 Aanvullend Protocol I. Het zijn hierbij de voorzienbare fysieke gevolgen van een cyberoperatie die bepalen of sprake is van ‘dadens van geweld’, en daarmee van een aanval in oorlogsrechtelijke zin, of niet.

Nu is het zeer wel mogelijk dat juist bij een pure cyberoperatie, hiermee doel ik op een cyberoperatie die niet gecombineerd wordt met, of onderdeel is van, een kinetische operatie, de gevolgen de drempel van verwonding of dood van personen of beschadiging of vernietiging van objecten niet zullen halen. Het is met cyberoperaties voorstelbaar dat doelstellingen gehaald worden zonder de fysieke gevolgen van traditioneel militair geweldgebruik. Ingevolge de beschrijving van cyberaanval uit de *Tallinn Manual* is een dergelijke operatie niet aan te merken als een aanval in oorlogsrechtelijke zin.⁷⁶ Wat betekent dit? Houdt dit dan in dat de bepalingen uit het humanitair oorlogsrecht die gelden voor een aanval niet gelden voor cyberoperaties zolang deze beneden de ondergrens van aanval blijven? En als dat het geval is, welke regels gelden er dan? Met het ontstaan van de nieuwe mogelijkheden voor niet-kinetische militaire cyberoperaties is er daarom alle reden om met hernieuwde belangstelling te kijken naar militaire operaties die onder de

⁷⁴ Schmitt 2013, hierna te noemen de *Tallinn Manual*. De tweede (uitgebreidere) editie van de *Tallinn Manual*, bekend onder de naam *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations* (2017) zal ik aanduiden als *Tallinn Manual 2.0*.

⁷⁵ *Tallinn Manual*, rule 30, p. 106.

⁷⁶ Schmitt 2013, p. 109.

drempelwaarde van een aanval blijven en te zien hoe deze vertaald kunnen worden naar militaire operaties in het cyberdomein. Vandaar de centrale vraag van dit onderzoek;

Welke regels gelden in het humanitair oorlogsrecht voor militaire cyberoperaties die beneden de drempel van aanval, zoals gedefinieerd in artikel 49 lid 1 Aanvullend Protocol I, blijven?

1.2.2 Opbouw

Om deze centrale vraag te kunnen beantwoorden zal ik in Hoofdstuk 2 allereerst antwoord geven op de deelvraag: Waar ligt de ondergrens van ‘aanval’ voor militaire operaties in traditionele zin? In het daaropvolgende Hoofdstuk 3 behandel ik de vervolgvraag: Welke regels gelden in het humanitair oorlogsrecht voor militaire operaties die de drempel uit de eerste deelvraag niet halen?

Na deze twee deelvragen te hebben beantwoord kan ik de overstap maken naar militaire operaties in het cyberdomein. In Hoofdstuk 4 zal ik de derde deelvraag beantwoorden: Hoe moet de drempelwaarde van ‘aanval’ geïnterpreteerd worden voor militaire operaties in het cyberdomein? De laatste (deel)vraag, en tevens hoofdvraag van dit onderzoek, die aan bod komt in Hoofdstuk 5 luidt vervolgens: Welke regels gelden in het humanitair oorlogsrecht voor militaire cyberoperaties onder de drempel van artikel 49 lid 1 Aanvullend Protocol I en hoe kunnen deze regels worden toegepast? Hoofdstuk 5 eindigt met conclusies en een synthese van het onderzoek.

1.3 Beperkingen

1.3.1 Alleen tijdens een gewapend conflict

Omdat ik op zoek ben naar de regels uit het humanitair oorlogsrecht die beneden de drempel van aanval gelden, zal ik mij focussen op de inhoud van het humanitair oorlogsrecht. Dit heeft twee belangrijke beperkingen tot gevolg. Allereerst beperk ik mij tot militaire operaties die plaatsvinden in een situatie van gewapend conflict. Het bestaan van een gewapend conflict is namelijk een *sine qua non* voor het van kracht zijn van het humanitair oorlogsrecht als geldend rechtsregime. Ik zal in Hoofdstuk 2 aandacht besteden aan de vraag wanneer sprake is van een gewapend conflict om het doel en de plaats van het humanitair oorlogsrecht te kunnen duiden, maar ik ga *niet* op zoek naar het exacte begin en einde van het humanitair oorlogsrecht als toepasselijk rechtsregime. Een direct gevolg daarvan is dat ik ook de vraag of een, of meerdere, militaire cyberoperatie(s) de toestand van een gewapend conflict op kunnen leveren, niet zal beantwoorden. Ik beperk me tot de situaties waarin het humanitair oorlogsrecht van kracht is.

1.3.2 Alleen humanitair oorlogsrecht

Ten tweede betekent de focus op de inhoud van het humanitair oorlogsrecht dat ik me niet bezig zal houden met vragen over overlappende rechtsregimes. Situaties waarin rechtsregimes elkaar (kunnen) overlappen zijn niet nieuw of ongewoon binnen het internationaal recht. Zo bestaat er bijvoorbeeld een samenspel tussen het humanitair

oorlogsrecht en mensenrechten waarbij *“the boundaries between these two bodies of law [International Humanitarian Law and Human Rights Law] has become increasingly blurred in recent years.”*⁷⁷ Overtredingen van het humanitair oorlogsrecht, inbreuken en ernstige inbreuken⁷⁸ hebben een overlap met internationaal strafrecht⁷⁹ en daarnaast ook met nationaal strafrecht.⁸⁰

Onderscheid aanbrengen tussen de verschillende rechtsregimes, zeker als het gaat om nieuwe ontwikkelingen zoals militaire operaties in het cyberdomein, is niet altijd eenvoudig. Een belangrijk kenmerk van het cyberdomein is namelijk dat het klassieke onderscheid tussen militaire en civiele, publieke en private en nationale en internationale dimensies minder scherp is.⁸¹ De verbondenheid van allerlei netwerken maakt dat het cyberdomein zich weinig aan zal trekken van de grenzen die in de andere domeinen gelden,⁸² of zoals verwoord in de Nationale Cyber Security Strategie I, “Cyberaanvallen en -verstoringen overschrijden in een oogwenk landsgrenzen, culturele en juridische stelsels.”⁸³ Toch is en blijft het scheiden van de rechtsregimes noodzakelijk. Laat ik dit illustreren met een voorbeeld.

Stel dat Nederland betrokken is bij een gewapend conflict waarop het humanitair oorlogsrecht van toepassing is. Om een goed beeld van de tegenstander te krijgen wordt een militaire cyberoperatie op touw gezet waarmee heimelijk ingebroken wordt in systemen van de tegenstander om daaruit gegevens te kunnen downloaden en zo waardevolle informatie te verkrijgen. Deze operatie zal moeten voldoen aan de regels van het humanitair oorlogsrecht. Op hetzelfde moment is de Militaire Inlichtingen en Veiligheidsdienst ook bezig met het vergaren van digitale inlichtingen om bij te dragen aan de informatiepositie over de aard en herkomst van (potentiële) digitale dreigingen. Deze laatste bezigheid valt onder het regime van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017. Hoe houd je beide operaties gescheiden en, als dat al mogelijk is gelet op het gegeven dat gebruik gemaakt wordt van dezelfde technieken met alleen een andere doelstelling,⁸⁴ hoe ga je om met gegevens die je onder het humanitair oorlogsrecht op juridisch verantwoorde wijze hebt verkregen maar die je op basis van de Wet Inlichtingen en Veiligheid 2002 niet had kunnen verkrijgen?⁸⁵ De positie van Nederland

77 Turns in Evans 2010, p. 816.

78 Zie bijvoorbeeld Aanvullend Protocol I, deel V, sectie II, artt. 85–91.

79 Zie bijvoorbeeld Statuut van Rome inzake het Internationaal Strafhof van 17 juli 1998 met name art. 8 *war crimes*.

80 Denk voor Nederland aan het Wetboek van Militair Strafrecht en de Wet Internationale Misdrijven. Voor een praktisch voorbeeld zie BBC 12 april 2018 (<http://www.bbc.com/news/technology-43738953>) Als commentaar op de NonPetya ransomware gericht op Oekraïne bericht het Government Communications HQ UK over Rusland “*They’re blurring the boundaries between criminal and state activity.*”

81 Actualisering Defensie Cyber Strategie, Kamerstukken II 2014–2015 33.321 nr. 5, p. 7.

82 Nederlandse Defensie Doctrine 2013, p. 98.

83 Kamerstukken II 2010–2011 26643 nr. 174, p. 4.

84 AIV/CAVV Advies Digitale Oorlogvoering, p. 15. Gelet op de beperkte operationele capaciteit worden de operaties waarschijnlijk ook nog uitgevoerd met dezelfde middelen en misschien wel door dezelfde personen.

85 Zie bijvoorbeeld Ducheine & Voetelink 2011, en Ducheine, Voetelink, Stinissen & Gill in Ducheine, Osinga & Soeters 2012. Zie ook AIV/CAVV Advies Digitale Oorlogvoering, p. 37 conclusies en aanbevelingen 10 waarin de omgekeerde situatie is

is duidelijk in het feit dat de rechtsregimes gescheiden zijn. “Digitale daden van geweld vallen alleen onder het humanitair oorlogsrecht wanneer ze worden gepleegd in de context van een gewapend conflict, door de partijen bij dat conflict. Dit vormt een belangrijke afbakening ten opzichte van andere daden van digitaal geweld.”⁸⁶ Het onderscheid moet vorm krijgen door een “functiescheiding tussen de CDS en de directeur van de MIVD”,⁸⁷ maar de regering constateert tevens dat “voor offensief optreden vaak dezelfde technieken worden gebruikt als voor inlichtingendoeleinden. Voor de realisatie van een offensieve capaciteit is een efficiënte inzet van alle schaarse cybercapaciteiten (waaronder inlichtingencapaciteiten) binnen Defensie dan ook noodzakelijk.”⁸⁸

Bovenstaand voorbeeld maakt duidelijk hoe lastig onderscheid aanbrengen, en vervolgens borgen en handhaven, tussen verschillende rechtsregimes in de praktijk kan zijn. Dat is echter geen onderwerp van dit onderzoek. Ik beperk mij tot het humanitair oorlogsrecht. Om dit te kunnen doen zal ik wel vast moeten stellen wanneer militaire operaties onder het regime van het humanitair oorlogsrecht vallen. Dit doe ik in Hoofdstuk 2.

1.3.3 De grondbeginselen en de regels

Zoals hiervoor al aangegeven was elke keer als een nieuwe ontwikkeling vraagtekens opriep over de toepasbaarheid van het humanitair oorlogsrecht de conclusie dat de nieuwe ontwikkeling moet voldoen aan de “*general rules of LOAC*.”⁸⁹ Daar waar een regel toegepast moet worden op een nieuwe situatie of wanneer een nieuwe ontwikkeling lijkt te vragen om nieuwe regels, kan altijd teruggevallen worden op de grondbeginselen van het humanitair oorlogsrecht. Deze grondbeginselen vormen daarmee het normatieve framework waarop het gehele systeem van regels is gebaseerd⁹⁰ zodat “*general law-of-war principles are often well-suited to emerging military technology and tactics not anticipated or addressed by specific law-of-war prohibitions*.”⁹¹ Deze grondbeginselen van het humanitair oorlogsrecht⁹² leveren weliswaar geen zelfstandige juridische verplichting op, maar door te kijken op het abstractieniveau van de grondbeginselen is het niet alleen mogelijk een aangepaste invulling van bestaande regels te geven, het heeft als bijkomend voordeel dat “*in contrast to many specific prohibitions, law-of-war principles operate nearly universally, paying less regard to technical legal elements, peculiarities of conflict classification, or the legal status of affected persons*”,⁹³ waardoor

beschreven. Hierin concludeert het AIV/CAVV ook dat problemen op kunnen treden. “Het is om goede redenen op basis van de WIV niet toegestaan dat een inlichtingendienst een geplaatst exploit gebruikt voor een netwerkaanval met een militair oogmerk, die het wijzigen of beschadigen van een systeem tot doel heeft” en merkt hierover op dat duidelijke procedurele afspraken gemaakt moeten worden om de functiescheiding te garanderen.

86 Kamerstukken II 2011-2012 33000 X nr. 79, p. 4.

87 Kamerstukken II 2011-2012 33000 X nr. 79, p. 4.

88 Kamerstukken II 2011-2012 33000 X nr. 79, p. 4.

89 Dinstein 2013, p. 286.

90 Gill in Matthee, Toebees & Brus 2013, p. 40.

91 Watts 2014, p. 122.

92 Welke die grondbeginselen zijn komt in Hoofdstuk 3 aan bod.

93 Watts 2014, p. 122.

minder aandacht besteed hoeft te worden aan de verschillen in regels die gelden voor een internationaal en een niet-internationaal gewapend conflict.

Bij de beantwoording van de tweede en de vierde deelvraag zal ik daarom primair gebruikmaken van de grondbeginselen en alleen indien daar aanleiding toe is ook aandacht besteden aan individuele regels uit het humanitair oorlogsrecht. Deze benaderingswijze is methodologisch verdedigbaar omdat de grondbeginselen van het humanitair oorlogsrecht gezien kunnen worden als “door beschaafde naties erkende algemene rechtsbeginselen”⁹⁴ die een rechtsbron voor internationaal recht vormen.⁹⁵

1.4 Relevantie van het onderzoek

1.4.1 Wetenschappelijk belang

Dit onderzoek draagt bij aan de theorievorming over de toepasselijkheid en toepassing van het humanitair oorlogsrecht op militaire operaties die niet gericht zijn op het toebrengen van fysieke schade en/of letsel, zowel in het algemeen als ook binnen het relatief nieuwe cyberdomein. Dit deelgebied van het humanitair oorlogsrecht heeft tot op heden relatief minder aandacht gekregen dan traditioneel kinetische operaties. De uitkomsten van dit onderzoek geven aan welke regels uit het humanitair oorlogsrecht gelden voor militaire operaties die de drempel van aanval, zoals gecodificeerd in artikel 49 Aanvullend Protocol I, niet halen. Daarmee draagt dit onderzoek bij aan een manier om de restrictieve en permissie benadering van cyberaanvallen binnen de academische discussie nader tot elkaar te brengen.⁹⁶

1.4.2 Maatschappelijk belang

Met de opkomst en ontwikkeling van het cyberdomein is de gehele maatschappij, maar ook groepen en individuele burgers, afhankelijker geworden van virtuele zaken.⁹⁷ Belangrijke vraag is dan of militaire operaties beneden de drempel van aanval, bijvoorbeeld beïnvloedingsoperaties, gericht mogen zijn op deze niet-fysieke zaken van de burgerbevolking, specifieke groepen of individuele burgers. Indien dit zou mogen, gelden daar dan specifieke regels voor of zijn dergelijke operaties altijd geoorloofd zolang ze maar

■
94 Statuut van het Internationaal Gerechtshof art. 38 lid 1c.

95 Bothe, Partch & Solf 2013, p. 43 “*They are general principles in the sense of Art. 38 of the Statute of the ICJ.*”

96 Deze twee benaderingen worden in Hoofdstuk 4, par. 4.5.3 behandeld. In gesimplificeerde vorm komt de restrictieve benadering erop neer dat binnen het humanitair oorlogsrecht alle militaire cyberoperaties cyberaanvallen zijn en daarmee aan de regels die gelden voor aanvallen, waaronder het aanvalsverbod op burgers en burgerobjecten, moeten voldoen. Het belangrijkste gevolg is dat cyberoperaties alleen gericht mogen zijn op of tegen militaire doelen. De permissieve benadering stelt dat militaire cyberoperaties die geen fysieke schade veroorzaken geen aanvallen in de zin van het humanitair oorlogsrecht zijn en dus niet onder het aanvalsverbod vallen. Militaire cyberoperaties mogen in deze visie gericht zijn op of tegen burgers of burgerobjecten zolang deze operaties maar beneden de drempel van aanval blijven.

97 Zie par. 1.1.2.

beneden de drempel van aanval blijven?⁹⁸ Gelet op de mogelijk verstrekkende gevolgen is duidelijkheid hierover van belang.

1.4.3 Strategisch belang

Zoals hiervoor aangegeven kan en zal een staat gebruik maken van een mix aan machtsmiddelen om zijn belangen zo optimaal mogelijk na te streven. Het kan daarbij voorkomen dat een staat betrokken raakt bij een gewapend conflict en het militaire machtsmiddel, met andere woorden de krijgsmacht, inzet. Dit zal hoogstwaarschijnlijk in samenwerking met de andere machtsmiddelen gebeuren zodat de uitkomsten van dit onderzoek zowel politiek als militair op het strategisch niveau⁹⁹ van belang zijn. In de mix van middelen is het belangrijk te weten welke andere capaciteiten, naast de traditioneel kinetische capaciteiten, de krijgsmacht bezit en hoe deze in een gewapend conflict ingezet kunnen worden binnen de grenzen van het humanitair oorlogsrecht. Duidelijkheid over de toepasselijke regels uit het humanitaire oorlogsrecht beneden de drempel van aanval kan onterechte inzet, of misschien nog belangrijker, onterechte terughoudendheid bij de inzet van dergelijke militaire (cyber)operaties voorkomen of in elk geval beperken.

Hiervoor is al aangegeven dat de Nederlandse regering benadrukt dat daden van digitaal geweld alleen onder het humanitair oorlogsrecht vallen als ze worden uitgevoerd in de context van een gewapend conflict.¹⁰⁰ Door helderheid te krijgen over de regels die gelden onder het humanitair oorlogsrecht voor deze vorm van cyberoperaties wordt tevens de mogelijkheid gecreëerd hier rekening mee te houden in de gevallen dat (nog) geen algemene overeenstemming bestaat over het bestaan van een gewapend conflict in een bepaalde situatie.¹⁰¹ Dit is van belang omdat in deze laatste situaties “binnen de NAVO, maar ook nationaal in Nederland, als vaststaand beleid [geldt] dat ook in operaties waarop het humanitair oorlogsrecht formeel niet van toepassing is, de restricties uit dat recht (zoals het verbod op aanvallen op de burgerbevolking als zodanig) zullen worden nageleefd.”¹⁰²

98 Denk daarbij aan vragen als; is het toegestaan om social media accounts van familieleden van militairen te gebruiken om zo militairen te beïnvloeden? Mogen met hetzelfde doel bankrekeningen van familieleden of kennissen van militairen (tijdelijk) geblokkeerd worden?

99 Strategisch, en in de volgende paragraaf operationeel en tactisch, verwijst naar de drie niveaus van operaties conform NATO AJP-01, 2017. Strategisch: “the level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them.” NATO AJP-01, 2017, p. 1-8. Operationeel: “the level at which campaigns and major operations are planned, conducted and sustained to achieve strategic objectives within theatres or areas of operations.” NATO AJP-01, 2017, p. 1-10. Tactisch: “the level at which activities, battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units.” NATO AJP-01, 2017, p. 1-11.

100 Kamerstukken II 2011-2012 33000 X nr. 79, bijlage p. 5.

101 Zie bijv. Ducheine & Pouw 2010.

102 Kamerstukken I 2003-2004, 29200 X, C, p. 3. Zie bijv. ook Nationale Defensie Doctrine 2013, p. 55. Ducheine 2009, p. 492. Ook andere landen hebben een vergelijkbare visie, zie bijv. USA Law of War program DoDD 5100.77 par. 5.3.1. “Ensure that the members of their DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and with the principles and spirit of the law of war during all other operations,” mijn accentuerend.

1.4.4 Operationeel en tactisch militair belang

Het onderzoek heeft ook direct praktisch militair nut. Zodra een land een operationele cybercapaciteit heeft ontwikkeld en er doet zich een situatie van gewapend conflict voor zal bij de keuze voor militaire operaties zeker ook gekeken worden naar de effecten en de schade die militaire cyberoperaties tot gevolg hebben. Het is daarbij niet onrealistisch te veronderstellen dat de keuze voor militaire cyberoperaties die geen fysieke schade of letsel veroorzaken vanuit die optiek relatief laagdrempelig zal zijn en daarmee een reële optie voor inzet zal worden.¹⁰³ Een voorwaarde hiervoor is dan wel dat deze operatie niet in strijd is met het humanitair oorlogsrecht. Om dit te kunnen beoordelen is het noodzakelijk te weten welke regels uit het humanitair oorlogsrecht van toepassing zijn op dergelijke operaties. Ook op operationeel en tactisch niveau kan duidelijkheid over de toepasselijke regels uit het humanitaire oorlogsrecht beneden de drempel van aanval onterechte inzet, of onterechte terughoudendheid, bij inzet van dergelijke militaire (cyber)capaciteiten voorkomen of in elk geval beperken.

1.4.5 Onderscheid tussen rechtsregimes

Als laatste kan inzicht in de toepasselijkheid van regels onder het rechtsregime van het humanitair oorlogsrecht behulpzaam zijn bij het maken van onderscheid in de gevallen dat verschillende rechtsregimes elkaar (mogelijk) overlappen.¹⁰⁴ Zeker in een tijd waar gewapende conflicten niet meer alleen op het traditionele gevechtsveld zullen worden uitgevochten,¹⁰⁵ kan het lastig zijn het toepasselijke rechtsregime te duiden.¹⁰⁶ Helderheid over de regels die gelden binnen het regime van het humanitair oorlogsrecht is weliswaar geen garantie voor een goede scheiding van overlappende rechtsregimes; onduidelijkheid over de toepasselijke regels leidt vrijwel zeker tot verkeerde uitkomsten.

Na dit inleidende hoofdstuk is het nu de plek over te gaan naar de eerste inhoudelijke deelvraag van dit onderzoek, de vraag naar de ondergrens van 'aanval' in traditionele zin.

103 Het is niet onvoorstelbaar dat een dergelijke optie zelfs de voorkeur moet krijgen gelet op de tekst van API art. 57(3) dat luidt: "Wanneer een keuze mogelijk is tussen verschillende militaire doelen om een gelijkwaardig militair voordeel te behalen, dient dat doel te worden uitgekozen, waarop de aanval naar kan worden verwacht het minste gevaar voor de levens van de burgerbevolking en voor de burgerobjecten oplevert."

104 Zie par. 1.3.2 hiervoor.

105 Zie par. 1.1.3 met als voorbeelden hybride oorlogvoering en 'unrestricted warfare'.

106 Dit zal zeker lastig zijn als een tegenstander bewust gebruikt maakt van "hybrid activities that aim to create ambiguity and blur the lines between peace, crisis, and conflict." NATO: Brussels Summit Declaration 2018, par. 21.

2

Hoofdstuk 2 De ondergrens van ‘aanval’ in traditionele zin

2.1 Inleiding

Gelden voor een bombardement met bommen dezelfde regels als voor het uit een vliegtuig werpen van pamfletten om de burgerbevolking te waarschuwen? Gevoelsmatig zal het antwoord waarschijnlijk ontkennend zijn. Maar waarin, en waarom, verschillen, in oorlogsrechtelijke zin, bovenstaande militaire operaties? Het antwoord hierop volgt uit de deelvraag die in dit hoofdstuk centraal staat: Wat is de ondergrens van ‘aanval’ in traditionele zin? Artikel 49 lid 1 Aanvullend Protocol I definieert aanvallen als “daden van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve.”¹ Zoals de hiervoor gegeven voorbeelden aangeven, bestaan ook militaire operaties die in het kader van een gewapend conflict uitgevoerd kunnen worden zonder dat daarbij geweldgebruik benodigd is, zodat artikel 49 lid 1 impliciet een ondergrens aangeeft voor het begrip ‘aanval’ binnen het humanitair oorlogsrecht. Het onderscheid is van belang omdat een aantal regels uit het humanitair oorlogsrecht specifiek gericht is op aanvallen,² terwijl andere regels een bredere toepassing hebben.³ Daarom zal ik in dit hoofdstuk onderzoeken wat onder de definitie van aanval valt en daarmee ook impliciet wat niet, om daarmee vast te stellen wat de ondergrens van aanval, zoals gedefinieerd in artikel 49 lid 1, is.

Om dit te kunnen doen zal ik allereerst dieper ingaan op een aantal zaken waarbij ik gebruik maak van de algemene regel van verdragsuitleg zoals geformuleerd in artikel 31 van het Verdrag van Wenen inzake het verdragenrecht.⁴ In paragraaf 2.2 ga ik in op het doel van het humanitair oorlogsrecht met een verbijzondering in paragraaf 2.3 naar de balans tussen militaire noodzaak en humaniteit.⁵ In paragraaf 2.4 ga ik vervolgens in op de vraag wanneer het humanitair oorlogsrecht van toepassing is om daarmee de context te verduidelijken.⁶ Overigens zal ik deze bevindingen over het humanitair oorlogsrecht niet alleen gebruiken in dit hoofdstuk maar ook bij de beantwoording van de volgende deelvragen van mijn onderzoek. In paragraaf 2.5 zal ik het begrip ‘aanval’ in relatie tot de begrippen ‘militaire operaties’, ‘vijandelijkheden’ en ‘oorlogvoering’ plaatsen om daarmee de onderlinge verhouding tussen deze begrippen te duiden. Ik gebruik daarbij de gewone

1 Aanvullend Protocol I art. 49 lid 1. De authentieke Engelse versie luidt: “*attacks’ means acts of violence against the adversary, whether in offence or in defence.*”

2 Voorbeelden hiervan zijn het verbod om de burgerbevolking of burgerobjecten doelwit van een aanval te maken en de verplichting om voorzorgen te nemen bij aanvallen en voorzorgen te nemen tegen de gevolgen van aanvallen, respectievelijk art. 51 lid 2, art. 52 lid 1, art. 57 en art. 58 Aanvullend Protocol I.

3 Voorbeelden hiervan zijn de regels voor methoden en middelen van oorlogvoering zoals gecodificeerd in deel III, sectie I van Aanvullend Protocol I.

4 Verdrag van Wenen, art. 31. Een Verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het verdrag in hun context en in het licht van het voorwerp en doel van het Verdrag.

5 Verdrag van Wenen, art. 31. Een Verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het verdrag in hun context en in het licht van het voorwerp en doel van het Verdrag. Accentuering mijnerzijds.

6 Verdrag van Wenen, art. 31. Een Verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het verdrag in hun context en in het licht van het voorwerp en doel van het Verdrag. Accentuering mijnerzijds.

betekenis van termen zoals die gebruikt worden in verdragen.⁷ Een helder begrip van deze termen en hun onderlinge verhoudingen is essentieel om spraakverwarring te voorkomen, zeker omdat de begrippen niet altijd eenduidig gebruikt worden. Tot slot zal ik, in paragraaf 2.6, nader ingaan op het begrip ‘aanval’ en een antwoord formuleren op de deelvraag uit dit hoofdstuk, “wat is de ondergrens van ‘aanval’ in traditionele zin?”

2.2 Het doel van het humanitair oorlogsrecht

2.2.1 Inleiding, een dubbele doelstelling

Humanitair oorlogsrecht reguleert het gewapend conflict.⁸ Dit geschiedt aan de hand van een dubbele doelstelling met enerzijds het reguleren, waaronder beperken, van de toegestane middelen en methoden van oorlogvoering en anderzijds het beschermen van verschillende groepen en objecten die niet, of niet langer, direct betrokken zijn bij het gewapend conflict.

De eerste doelstelling van het humanitair oorlogsrecht is onder andere terug te vinden in de preambule van de Haagse Conventie IV waarin is opgenomen dat “Oordelende, dat het te dien einde noodig is de algemeene wetten en gebruiken van den oorlog te herzien, hetzij met het doel deze nauwkeuriger te omschrijven, hetzij om daarin zekere grenzen te stellen, bestemd om de hardheid er van zooveel mogelijk te beperken.”⁹ Deze doelstelling komt nadrukkelijk naar voren in het zogenaamde Haags oorlogsrecht. Het International Court of Justice verwoordt dit als “*the Hague Law fixed the rights and duties of belligerents in their conduct of operations and limited the choice of methods and means of injuring the enemy in an international armed conflict.*”¹⁰

De tweede doelstelling, de bescherming van de slachtoffers van gewapende conflicten, is onder andere terug te vinden in de vier Geneefse Conventies,¹¹ maar ook in de Aanvullende Protocolen I¹² en II,¹³ al moet worden opgemerkt dat met name in Aanvullend Protocol I ook de eerste doelstelling van het humanitair oorlogsrecht aan bod komt. Deze tweede

7 Verdrag van Wenen, art. 31, Een Verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het verdrag in hun context en in het licht van het voorwerp en doel van het Verdrag. Accentuering mijnerzijds.

8 Kleffner (in Fleck) 2013a, p. 43, *Black Letter Rule no. 201: International humanitarian law regulates, and as a rule applies in times of, armed conflict.*

9 Hague Convention IV 1907, Preamble.

10 ICJ, *legality of the threat or use of nuclear weapons*, 8 July 1996 par. 75.

11 Verdrag van Genève I t/m IV, 1949.

12 Aanvullend Protocol I, Preamble: Van oordeel, dat het niettemin noodzakelijk is, de bepalingen ter bescherming van de slachtoffers van gewapende conflicten opnieuw te bevestigen en uit te breiden, en maatregelen toe te voegen met het oog op een strengere toepassing daarvan.

13 Aanvullend Protocol II, Preamble: De nadruk leggende op de noodzaak tot het verzekeren van een betere bescherming aan de slachtoffers van die gewapende conflicten.

doelstelling, ook wel aangeduid als het Geneefs oorlogsrecht,¹⁴ is het beschermen van diegenen die niet (meer) deelnemen aan vijandelijkheden.

Beide doelstellingen dienen binnen de juiste context gezien te worden, namelijk het gewapend conflict dat gewonnen dient te worden. Of zoals gesteld door Green: *“The purpose of what is known as the law of war – jus in bello – is to reduce the horrors inherent therein to the greatest extent possible in view of the political purpose for which war is fought, namely to achieve one’s policies by victory over one’s enemy.”*¹⁵ Twee zaken komen in deze beschrijving naar boven. Aan de ene kant wordt bij een gewapend conflict geaccepteerd dat, bij het verslaan van de vijand of tegenstander inherent leed en schade veroorzaakt zal worden. Aan de andere kant moet dit leed en deze schade zoveel als mogelijk, binnen de doelstelling van het gewapend conflict, beperkt worden. Met andere woorden, het humanitair oorlogsrecht probeert “de rampen van den oorlog te verminderen, voor zoover de militaire noodzakelijkheid zulks toelaat”.¹⁶ Of in modernere termen *“to achieve a balance between military necessity and the requirements of humanity.”*¹⁷

Een algemene opmerking is hier op zijn plaats. De aard of oorzaak van het gewapend conflict doet er, vanuit het perspectief van het humanitair oorlogsrecht, niet toe.¹⁸ Dit principe, ook wel aangeduid als de *“neutrality”* van het humanitair oorlogsrecht¹⁹ of *“principle of equal application”*²⁰ is onder meer gecodificeerd in de Preamble van Aanvullend Protocol I.²¹ Het maakt voor de toepassing van het humanitair oorlogsrecht niet uit of een gewapend conflict wel of niet is ontstaan binnen de regels van het jus ad bellum, *“international humanitarian law applies equally to all the parties to an armed conflict irrespective of the legality or illegality of their resort to force.”*²²

Veel regels²³ van het humanitair oorlogsrecht zijn terug te voeren op de balans tussen de twee hierboven genoemde grondbeginselen van militaire noodzaak en humaniteit.²⁴

14 ICJ, *legality of the threat or use of nuclear weapons*, 8 July 1996 par. 75, “Geneva Law protects the victims of war and aims to provide safeguard for disabled armed forces and persons not taking part in the hostilities.”

15 Green 2000, p. 15.

16 Hague Convention IV 1907, Preamble.

17 O’Connell (in Fleck) 2013a, p. 37.

18 Sandoz, Swinarski & Zimmermann 1987, p. 23. In dezelfde zin Fleck 2013a, p. 48 *Black letter rule* 206

19 Bothe, Partsch & Solf 1982 p. 33.

20 Roberts 2008, p. 932.

21 Aanvullend Protocol I Preamble: Voorts opnieuw bevestigende, dat de bepalingen van de Verdragen van Geneve van 12 augustus 1949 en van dit Protocol ten volle dienen te worden toegepast in alle omstandigheden op alle personen die door deze akten worden beschermd, zonder enig nadelig onderscheid gebaseerd op de aard of de oorsprong van het gewapende conflict of op de motieven van of toegeschreven aan de partijen bij het conflict. Accentuering mijnerzijds.

22 Kleffner (in Fleck) 2013a, p. 48, *Black letter rule* 206.

23 Maar niet alle. Een voorbeeld van een regel waar humaniteit geen invloed heeft uitgeoefend is het verbod op het gebruik van vijandelijke kentekens, onderscheidingstekens en uniformen, API art. 39(2). Een voorbeeld van een regel waar militaire noodzaak geen invloed heeft gespeeld is het verbod op *“medical interference with POWs not justified by the medical, dental or hospital treatment of the prisoner concerned and carried out in his interest.”* Geneva Convention II, art. 13.

24 Kolb & Hyde 2008, p. 44.

Ook andere beginselen van het humanitair oorlogsrecht die vaak genoemd worden, zoals onderscheid, proportionaliteit en soms ook wel eerlijkheid en goede trouw,²⁵ kunnen in principe teruggevoerd worden op deze balans. Het is hier van belang te constateren dat de twee grondbeginselen, militaire noodzaak en humaniteit vaak tot verschillende uitkomsten leiden zodat de balans alleen in de vorm van een compromis gevonden kan worden.²⁶ Op de situaties waarin beide grondbeginselen niet tot verschillende uitkomsten leiden kom ik later nog terug.

2.2.2 De achtergrond van de dubbele doelstelling

Voordat ik dieper inga op de balans tussen militaire noodzaak en humaniteit is het goed terug te komen op de dubbele doelstelling van het humanitair oorlogsrecht aan de hand van het Haags en het Geneefs oorlogsrecht. Deze achtergrond is namelijk mede bepalend geweest voor de manier waarop naar de balans, het evenwicht, gekeken is en wordt. Hoewel beide onderdelen inmiddels zo met elkaar verweven zijn dat gesproken kan worden van één complex systeem,²⁷ is het goed stil te staan bij hun oorsprong.

Eenzijds ziet het Haags oorlogsrecht met name op de middelen en methoden van oorlogvoering. Het reguleert het optreden van strijdende partijen door middel van verboden.²⁸ Haags oorlogsrecht gaat niet in op zaken die zijn toegestaan omdat het uitgaat van soevereine staten die vrij zijn alle middelen en manieren van oorlogvoering te gebruiken zonder dat ze daarvoor specifieke toestemming behoeven.²⁹ In termen van de balans tussen militaire noodzaak en humaniteit kan sterk gesimplificeerd gesteld worden dat, mits een militaire noodzaak aanwezig is, geweld is toegestaan tenzij het in een specifieke regel uit het humanitair oorlogsrecht is verboden. Op deze sterk gesimplificeerde stelling dient echter direct een nuancering te worden aangebracht. Daar waar een handeling niet expliciet in een verdrag verboden wordt, betekent dit niet altijd dat deze handeling geoorloofd is omdat ook uit het gewoonterecht een beperking kan volgen. Dit principe wordt vaak aangeduid als de zogenaamde Martens Clausule,³⁰ en is onder andere opgenomen in de Preamble van het Haags Verdrag (IV) uit 1907. Deze Clausule komt erop neer dat in de gevallen waarin niet in een verdrag is voorzien, de burgerbevolking

25 Op de grondbeginselen van humanitair oorlogsrecht kom ik het volgende Hoofdstuk uitgebreid terug.

26 O'Connell (in Fleck) 2013a, p. 36. Black Letter Rule 133 "International humanitarian law in armed conflict is a compromise between military and humanitarian requirements. Its rules comply with both military necessity and the dictates of humanity. Considerations of military necessity cannot, therefore, justify departing from the rules of humanitarian law in armed conflicts to seek a military advantage using forbidden means."

27 ICJ, *Legality of the threat or use of nuclear weapons*, 8 July 1996 par. 75. "These two branches of the law applicable in armed conflict have become so closely interrelated that they are considered to have gradually formed one single complex system, known today as international humanitarian law." Overigens is het onderscheid Haags – Geneefs oorlogsrecht nooit absoluut geweest. Een aantal normen is in beide regimes tot ontwikkeling gekomen. Dinstein 2004, p. 13, noemt oorlogvoering op zee en de regels met betrekking tot krijgsgevangenen als voorbeelden.

28 Watts 2014, p. 117 noemt dit "the rules applicable to targeting."

29 Kolb & Hyde 2008, p. 17.

30 Genoemd naar de uit Estland afkomstige jurist Friedrich Martens die als adviseur van de Russische minister van Buitenlandse Zaken deelnam aan de Haagse Vredesconferenties van 1899 en 1907.

en de oorlogvoerenden in elk geval beschermd blijven door, en onderworpen zijn aan, de beginselen van het volkenrecht.³¹

Anderzijds is er het Geneefs oorlogsrecht, met name de Geneefse Verdragen I tot en met IV en de Aanvullende Protocolen daarop, dat de bescherming van potentiële en daadwerkelijke slachtoffers van oorlogsgeweld tracht te reguleren door middel van normen die deze bescherming moeten garanderen.³² Je zou kunnen stellen dat het begrip humaniteit dient als uitgangspunt, waarbij inbreuken op de beschermingsnormen alleen mogelijk zijn indien daar voldoende militaire noodzaak voor is. In dezelfde gesimplificeerde vorm als bij militaire noodzaak: militair geweld mag niet (op grond van humaniteit) tenzij het is toegestaan (op grond van militaire noodzaak).

In theorie komen beide benaderingen op dezelfde uitkomst uit, namelijk het punt waar militaire noodzaak en humaniteit met elkaar in balans zijn. In de praktijk, waar het gaat om de vergelijking tussen twee niet of nauwelijks vergelijkbare grootheden, zou het uit kunnen maken welk aanvangspunt genomen wordt. Hier zien we een bepaalde mate van beoordelingsruimte voor hen die de regels toe moeten passen waarbij de effectiviteit van de regels *“will depend to a large extent on the good faith of the belligerents and on their wish to conform to the requirements of humanity.”*³³

Overigens is niet iedereen het eens met de vaak gebruikte metafoor van de balans. Volgens Hayashi berust de metafoor van de balans op een *“inevitable conflict thesis”*.³⁴ Hierbij vallen de grondbeginselen militaire noodzaak en humaniteit nooit samen en leiden normatief gezien tot verschillende noodzakelijkheden die altijd met elkaar in conflict zijn.³⁵ In deze benadering kan *“no act [...] be both humane and materially necessary, or both inhumane and materially unnecessary”*³⁶ en als deze redenering logisch wordt voortgezet leidt dit tot de conclusie dat *“materially necessary acts always [...] be inhumane, and humane acts always [...] be materially unnecessary.”*³⁷ Om te verklaren dat het humanitair oorlogsrecht ook ziet op militaire operaties die *“inhumane and unnecessary”*³⁸ of *“humane and necessary”*³⁹ zijn, introduceert hij de

31 De letterlijke tekst luidt: “In afwachting dat een meer volledig wetboek voor de oorlog kan worden uitgevaardigd, achten de Hoge Verdragsluitende Partijen het gepast te verklaren, dat in de gevallen, welke niet begrepen zijn in de door haar aangenomen reglements-bepalingen, de bevolkingen en oorlogvoerenden verblijven onder de bescherming en de heerschappij van de beginselen van het Volkenrecht, zoals deze voortvloeien uit de tussen beschaafde volkeren gevestigde gebruiken, de wetten van de menselijkheid en de eisen van openbaar rechtsbewustzijn.”

32 Kolb & Hyde 2008, p. 17. Watts 2014, p. 117, noemt dit *“rules for treatment of persons under control of an enemy belligerent”*.

33 Sandoz, Swinarski & Zimmermann 1987, p. 589.

34 Hayashi 2017, p. 78.

35 Hayashi 2017, p. 78.

36 Hayashi 2017, p. 82.

37 Hayashi 2017, p. 91.

38 Hayashi 2017, p. 94. Als voorbeeld noemt hij het martelen van een gevangen genomen strijder om zo informatie te verkrijgen.

39 Hayashi 2017, p. 98. Als voorbeelden noemt hij *ethical fighting in counterinsurgency* waarbij militairen *“Rather than bursting in, for instance, [...] soldiers would surround the house and then go to the door and knock”*

“joint satisfaction thesis”.⁴⁰ Deze *joint satisfaction thesis* gaat uit van de stelling dat het humanitair oorlogsrecht geen verplichting oplegt om een militaire operatie uit te voeren, ook niet als deze *“materially necessary”* is.⁴¹ Tevens staat het humanitair oorlogsrecht militaire operaties toe die niet militair noodzakelijk zijn. Met deze theorie kan een strijder altijd voldoen aan beide grondbeginselen, ook in het geval van *inhumane and unnecessary* of *humane and necessary*.⁴²

Zeker niet iedereen gaat zover als Hayashi maar ook een aanhanger van de metafoor van de balans als Dinstein erkent dat afwegingen op basis van militaire noodzaak en humaniteit niet per definitie tot een andere uitkomst leiden. Hij noemt als voorbeeld het verbod op het aanvallen van onverdedigde plaatsen waar een aanval niet nodig is omdat de plaats zonder tegenstand ingenomen kan worden of worden omtrokken.⁴³ De beginselen van militaire noodzaak en humaniteit liggen hier in elkaars verlengde. Hij geeft hierbij wel aan dat dit uitzonderlijk is omdat humaniteit en militaire noodzaak meestal een andere richting in zullen wijzen.⁴⁴

In dit onderzoek zal ik de metafoor van de balans wel blijven gebruiken waarbij ik opmerk dat ik deze gebruik voor de situaties waar een afweging op basis van militaire noodzaak of humaniteit tot verschillende uitkomsten zou leiden. Hierbij erken ik wel dat er ook situaties bestaan waarin beide grondbeginselen elkaar versterken, waarbij acties zowel *“inhumane and unnecessary”*⁴⁵ als *“humane and necessary”*⁴⁶ kunnen zijn en de metafoor van een balans onbruikbaar is. Deze situaties zullen echter zelden tot juridische complicaties leiden omdat de eerste categorie meestal absoluut verboden is,⁴⁷ terwijl acties van de tweede categorie juist aangemoedigd zullen worden.

Tot zover de achtergrond van de doelstelling van het humanitair oorlogsrecht. Hoe pakt deze achtergrond uit in de praktijk, met andere woorden hoe is en wordt de balans gevonden tussen militaire noodzaak en humaniteit? Dat is het onderwerp van de volgende paragraaf.

■
40 Hayashi 2017, p. 93.

41 Hayashi 2017, p. 93.

42 Hayashi 2017, p. 112 *“Wherever military necessity permits what humanity demands, or wherever the former merely tolerates what the latter condemns, it always remains open to the belligerent to act in a manner that satisfies both simultaneously.”*

43 Dinstein 2009b, A3.

44 Dinstein 2009b, A4.

45 Hayashi 2017, p. 94.

46 Hayashi 2017, p. 98.

47 Absoluut in de zin van dat er geen uitzonderingen mogelijk zijn. Denk aan het verbod op doden van personen *‘hors de combat’* API art 41 lid 1 of het verbod op doden van krijgsgevangenen GC III, art 13.

2.3 De balans tussen militaire noodzaak en humaniteit

Hoe is de balans tussen militaire noodzaak en humaniteit gevonden bij het vastleggen van de regels van het humanitair oorlogsrecht en hoe moet deze balans gevonden worden bij toepassing van de regels in de praktijk? Zijn beide grondbeginselen even belangrijk of legt één van beide toch meer gewicht in de schaal, zodat het ene beginsel voorrang zou kunnen hebben over het andere?

Voor de beantwoording van deze vragen kan de balans gezien worden op twee niveaus. Op de eerste plaats kan de balans worden gezien als onderliggend fundamenteel evenwicht waarop het totale stelsel van regels berust. Het resultaat hiervan is op veel plaatsen terug te vinden in gecodificeerde regels, bijvoorbeeld in de *Saint Petersburg Declaration* waar de partijen “fixed the technical limits at which the necessities of war ought to yield to the requirements of humanity”,⁴⁸ of het eerder aangehaalde citaat uit de preambule van de Haagse Conventie IV om “de rampen van den oorlog te verminderen, voor zoover de militaire noodzakelijkheid zulks toelaat.”⁴⁹ Op dit niveau kan de balans gebruikt worden om een uitspraak te doen over de manier waarop, en de snelheid waarmee, het humanitair oorlogsrecht zich ontwikkelt.⁵⁰

Als tweede kan gekeken worden naar het niveau waarbij de balans gebruikt dient te worden bij de toepassing van een bepaalde regel. Een voorbeeld hiervan is de proportionaliteitstest voor een militaire aanval, zoals gecodificeerd in onder andere artikel 51 van Aanvullend Protocol I, waarbij een aanval verboden is indien verwacht kan worden dat bijkomende schade aan de burgerbevolking of burgerobjecten ontstaat die buitensporig is in verhouding tot het verwachte militaire voordeel.⁵¹ Hoewel de niveaus waarop naar de balans gekeken wordt, kunnen verschillen, zijn de redeneringen die de uitkomst bepalen hetzelfde. De navolgende bespreking van de twee zijden van de balans geldt derhalve voor beide niveaus.

2.3.1 De uitersten

In absolute zin zijn geen van de beginselen zo zwaarwegend dat daarmee het andere volledig opzij gezet kan worden. In het verleden is door een aantal, met name Duitse, auteurs de theorie aangehangen dat in geval van absolute militaire noodzaak andere rechtsregels moesten wijken, en daarmee ook het beginsel humaniteit. De redenering loopt dan als volgt: omdat rechtsregels een weerslag vormen van de balans tussen militaire noodzaak en humaniteit kan dat, als de militaire noodzaak maar zwaar genoeg is, andere overwegingen volledig tenietdoen.⁵² Deze theorie wordt vaak aangeduid met de Duitse uitdrukking *Kriegsraison geht vor Kriegsmanier* of ook wel *Not kennt kein Gebot*. Alhoewel deze

48 St. Petersburg Declaration 1868.

49 Hague Convention IV 1907, Preamble.

50 Schmitt 2012, p. 90. Gill in Matthee, Toebes & Bus 2013, p. 40 spreekt van “the two keystone principles which lie at the heart of the balance between military requirements and the need and objective to limit the suffering and devastation caused by war.”

51 Aanvullend protocol I 1977, artikel 51 lid 5 (b). Later in deze paragraaf kom ik in meer detail terug op deze regel.

52 Voor een overzicht van (Duitse) auteurs die dit standpunt huldigden, zie Lauterpacht 1952, p. 231.

theorie tot en met de Tweede Wereldoorlog werd gebruikt als argument om (oorlogs)regels te overtreden kan en moet deze als achterhaald worden beschouwd.⁵³ Deze theorie als rechtvaardigingsgrond voor oorlogsmisdaden is afgewezen in vonnissen van na-oorlogse Tribunalen als Neurenberg⁵⁴ en is nadien door vele schrijvers verworpen.⁵⁵

Aan de andere kant van de balans staat humaniteit. In de ultieme vorm zou humaniteit leiden tot het geweldloos oplossen van conflicten. Op die manier bestaan geen slachtoffers oftewel iedereen wordt maximaal beschermd tegen de verschrikkingen van een gewapend conflict. Dit zou echter betekenen dat gewapende conflicten uitgebannen zijn en hoewel het streven al lang bestaat⁵⁶ en zelfs als verbod is gecodificeerd in het Handvest van de Verenigde Naties⁵⁷ is de realiteit anders. Humanitair oorlogsrecht gaat uit van het bestaan van een gewapend conflict,⁵⁸ wat bijna per definitie betekent dat sprake is van gewapend geweld.⁵⁹ Dinstein verwoordt de onmogelijkheid om humaniteit absolute voorrang te geven als volgt, *“if benevolent humanitarianism were the only beacon to guide the path of armed forces, war would have entailed no bloodshed, no destruction and no human suffering; in short, war would not have been war. In actuality, LOIAC takes a middle road.”*⁶⁰ In een gewapend conflict is het toegestaan de tegenstander aan te vallen en ook te doden als daar een militaire noodzaak voor is. Zolang gewapende conflicten bestaan, kan en mag militair geweld gebruikt worden mits dit binnen de regels van het humanitair oorlogsrecht geschiedt. Humaniteit heeft een belangrijke rol gespeeld bij de totstandkoming van de regels van het humanitair oorlogsrecht, en continueert die invloed bij zowel het ontstaan van nieuwe regels als bij de toepassing van bestaande regels. Dit is echter niet onbeperkt, of om met Dinstein te spreken: *“The humanitarian desire to attenuate human anguish in any armed conflict is natural. However, the thrust of the concept is not absolute mitigation of the calamities of war (which would be utterly impractical), but relief from the tribulations of war as much as possible.”*⁶¹

53 Sandoz, Swinarski & Zimmermann 1987, p. 391.

54 Zie bijv. *The Hostage Case, United States v. Wilhelm List et al. Par. 1272-1273*. “Here again the German Theory of expediency and military necessity (*Kriegsraison geht vor Kriegsmanier*) superseded established rules of International Law. As we have previously stated in this opinion, the rules of International Law must be followed even if it results in the loss of a battle or even a war.”

55 Sandoz, Swinarski & Zimmermann 1987, p. 391. Zie ook Dinstein, 2009b, B8.

56 Zie bijv. Hague Convention IV 1907 Preamble: “Overwegende dat, hoezeer ook naar de middelen gezocht wordt om den vrede te waarborgen en de strijd met de wapenen tusschen de volken te voorkomen.”

57 VN Handvest art. 2(4), “In hun internationale betrekkingen onthouden alle Leden zich van bedreiging met of het gebruik van geweld tegen de territoriale integriteit of de politieke onafhankelijkheid van een staat, en van elke andere handelswijze die onverenigbaar is met de doelstellingen van de Verenigde Naties.” Hierbij zij wel opgemerkt dat dit geen absoluut geweldverbod is maar dat uitzonderingen mogelijk zijn. Zo worden in het VN Handvest als uitzonderingen genoemd optreden met autorisatie van de VN Veiligheidsraad (art. 42) en optreden in het kader van zelfverdediging (art. 51).

58 Het bestaan van een gewapend conflict is zelfs een voorwaarde voor het van toepassing zijn van het humanitair oorlogsrecht, zie hierna par. 2.4.

59 Bijna per definitie omdat ook sprake kan zijn van een gewapend conflict zonder dat er sprake is van gewapend geweld. Dit kan zijn doordat een oorlog is verklaard (gemeenschappelijk art. 2 Verdragen van Genève 1949) waarbij (nog) geen gewapend geweld heeft plaatsgevonden of ingeval van een gehele of gedeeltelijke bezetting waarbij geen gewapende tegenstand is geboden (gemeenschappelijk art. 2 Verdragen van Genève). In beide gevallen gaat het om uiterst uitzonderlijke situaties, als ze al voorkomen.

60 Dinstein 2004, p. 16-17.

61 Dinstein 2004, p. 17.

2.3.2 Het evenwicht bepalen

Als geen van beide grondbeginselen zo zwaar kan wegen dat het daarmee het andere grondbeginsel volledig opzij kan zetten, hoe moeten ze dan, in relatieve zin, tegen elkaar afgewogen worden om tot een juiste balans te komen? Een eenduidig antwoord over het relatieve gewicht is niet te geven.⁶² Op het niveau van de concrete toepassing van een regel zal de balans gevonden moeten worden in de context waarop de regel van toepassing is. Hierbij dient ook de ontwikkeling van het onderliggende fundamentele evenwicht van het hele stelsel van individuele regels gezien te worden. Over dit onderliggende evenwicht constateren Kolb en Hyde dat *“As to a relative pre-eminence, all times have found a new equilibrium between the two principles in which one has prevailed somewhat over the other in a concrete context. Thus, for example, before World War II, the principle of military necessity seemed to have some pre-eminence; today, the principle of humanity has gained a significant amount of ground and obtained an equilibrium which is more favourable to it.”*⁶³ Ook Schmitt constateert een soortgelijke evolutie die zelfs terug te vinden zou zijn in de veranderende naamgeving van *law of war*, via *law of armed conflict*, naar *international humanitarian law*⁶⁴ terwijl Kolb spreekt van *“the progressive ‘humanisation’ of IHL.”*⁶⁵

In veel gevallen bestaat een zekere ruimte bij het bepalen van het evenwicht. Daar waar echter een evenwicht tussen militaire noodzaak en humaniteit tot stand gekomen is,⁶⁶ dat vervolgens is verworden tot een gewoonterechtelijke regel of is vastgelegd in een verdrag, is het niet zo dat het strijdende partijen vrij staat om, met een beroep op militaire noodzaak, de implementatie van de regel in een concreet geval te omzeilen,⁶⁷ zelfs niet als de toepassing van de regel op het eerste gezicht onlogisch lijkt. Een klassiek voorbeeld hiervan is een groep *special forces*,⁶⁸ die in het geheim achter de vijandelijke linies een actie uitvoert en hierbij een vijandelijke soldaat gevangen neemt. De gevangene meenemen kan het verloop van de missie in gevaar brengen. Onder deze omstandigheden zou de vijandelijke soldaat in vrijheid moeten worden gesteld,⁶⁹ maar deze zou dan direct alarm kunnen slaan en de positie van de *special forces* verraden. De gevangene doden mag niet omdat de vijandelijke soldaat *hors de combat* is als gevolg van zijn gevangenneming.⁷⁰ Deze regels zijn de vastlegging van een norm waarbij de militaire noodzaak al is meegewogen en zij laten daarbij geen ruimte tot herinterpretatie met een beroep op militaire noodzaak. De *special*

62 Voor de individuele zijden van de balans kan nog wel een relatieve uitspraak gedaan worden in de zin dat een operatie ‘humaner’ is dan een andere of een groter militair voordeel oplevert. Een bepaalde waarde aan een grondbeginsel toekennen waardoor het vergelijkbaar wordt met een ander grondbeginsel is echter niet mogelijk.

63 Kolb & Hyde 2008, p. 50.

64 Schmitt 2012, p. 98.

65 Kolb in Larsen, Cooper & Nystuen 2013, p. 52.

66 Het evenwicht geldt dan voor die specifieke regel. Per regel kan het gewicht van militaire noodzaak en humaniteit verschillen tot zelfs helemaal ontbreken. Voor voorbeelden van deze laatste situatie zie par. 2.2.1. voetnoot 129.

67 Dinstein 2009b, A7.

68 Voorbeeld ontleend aan Schmitt 2012, p. 98.

69 Ingevolge Aanvullend Protocol I 1979, art 41 lid 3 dat luidt: Wanneer personen die aanspraak kunnen maken op bescherming als krijgsgevangene, in handen van een tegenpartij zijn gevallen onder ongebruikelijke gevechtssomstandigheden die evacuatie verhinderen,[...], dienen zij te worden vrijgelaten.

70 Aanvullend Protocol I 1979, art 41 lid 2 (a): een persoon verkeert buiten gevecht indien hij zich in de macht van de tegenpartij bevindt.

forces in dit voorbeeld zullen moeten kiezen. De gevangen genomen vijandelijke soldaat in vrijheid stellen (met alle risico's van dien), de missie afbreken om de gevangengenomen soldaat over te brengen naar een gebied onder eigen controle, de gevangene toch meenemen en het risico voor de missie aanvaarden of een andere oplossing bedenken. Wat echter niet mag, is, met een beroep op de militaire noodzaak, de gevangene doden.

Om een beter inzicht te verkrijgen in de manier waarop de hierboven beschreven balans is gevonden in het stelsel van regels en hoe de balans gevonden dient te worden bij de toepassing in de praktijk zal ik hieronder een concreet voorbeeld van een regel bespreken.

2.3.3 Het evenwicht uitgewerkt in een concrete regel

Houdt de analogie van een balans, het vinden van een evenwicht tussen twee vaak tegenstrijdige grondbeginselen,⁷¹ ook in dat naarmate de militaire noodzaak groter is, meer concessies aan de humaniteit gedaan mogen worden? Het antwoord hierop is ja. Een goed voorbeeld hiervan is terug te vinden in de uitwerking van het proportionaliteitsbeginsel bij aanvallen.⁷² Deze regel verbiedt een aanval indien de verwachte bijkomende schade aan burgers of burgerobjecten buitensporig is in verhouding met het verwachte tastbare en rechtstreekse militaire voordeel. Het gebruik van het woord buitensporig is hier relevant. Omdat militaire noodzaak en humaniteit nauwelijks zijn te kwantificeren, kan alleen een evidente onbalans gezien worden als buitensporig.⁷³ Hiermee wordt aangegeven dat deze proportionaliteitstest niet wordt bepaald door “abstracte wetmatigheden”,⁷⁴ maar beoordeeld moet worden “in het licht van ieder afzonderlijk concreet geval.”⁷⁵ Deze constatering houdt tevens in dat ook andere factoren, zoals bijvoorbeeld politiek-opportunistische of militair-strategische overwegingen een grote invloed kunnen hebben op de uitkomst van de proportionaliteitstest.⁷⁶ Zo kan in het een gewapende conflict meer bijkomende schade aanvaard worden dan in een andere situaties die niet als gewapend conflict gekenmerkt kunnen worden maar waar het humanitair oorlogsrecht om beleidsmatige redenen wordt nageleefd,⁷⁷ ook als het te behalen militaire voordeel van vergelijkbare (orde)grootte is.

71 Voor de mogelijkheid dat deze grondbeginselen niet tegenstrijdig zijn, zie par 2.2.1.

72 Het proportionaliteitsbeginsel is op diverse plaatsen binnen zowel het internationaal als het nationaal recht te vinden. Het beginsel heeft echter niet overal dezelfde betekenis. Ik gebruik het beginsel hier alleen in de betekenis van het humanitair oorlogsrecht zoals bijv. opgenomen in Aanvullend Protocol I, art 51 lid 4: “Niet onderscheidende aanvallen zijn verboden”, gevolgd door lid 5b waarin is omschrijven wat als niet-onderscheidend dient te worden beschouwd: “aanvallen die, naar kan worden verwacht bijkomend verlies van mensenlevens onder de burgerbevolking, verwonding van burgers, schade aan burgerobjecten of een combinatie daarvan ten gevolge zullen hebben, in een mate die buitensporig zou zijn in verhouding tot het verwachte tastbare en rechtstreekse militaire voordeel.” In diezelfde betekenis ook Aanvullend Protocol I art. 57 lid 2(a): “af te zien van enige aanval die naar kan worden verwacht mede bijkomend verlies van mensenlevens onder de burgerbevolking, verwonding van burgers, schade aan burgerobjecten of een combinatie daarvan zal veroorzaken, in een mate welke buitensporig zou zijn in verhouding tot het te verwachten tastbare en rechtstreekse militair voordeel.”

73 Bothe, Partch & Solf 1982 p. 310.

74 Ducheine & Pouw 2010, p. 115.

75 Ducheine & Pouw 2010, p. 115.

76 Ducheine & Pouw 2010, p. 118.

77 Zie par. 1.4.2.

Overigens werkt deze balans tussen militaire noodzaak en humaniteit naar beide zijden. Zo zal de aanwezigheid van één militair de verwoesting van een dorp niet kunnen rechtvaardigen. Indien, aan de andere kant, de vernietiging van een brug van het opperste belang is voor de bezetting van een strategische zone, of juist ter voorkoming daarvan, zal deze vernietiging gerechtvaardigd zijn ondanks het feit dat een aantal huizen geraakt kan worden.⁷⁸

Wat betekent de constatering dat de balans tussen militaire noodzaak en humaniteit naar beide kanten werkt? Als geen of nauwelijks inbreuk op het beginsel van humaniteit wordt gepleegd, hoeft er dan ook maar weinig, of, *in extremis*, helemaal geen militaire noodzaak te bestaan om een militaire actie legitiem te laten zijn? De laatste situatie, helemaal geen militaire noodzaak, is in elk geval voor aanvallen makkelijk en eenduidig te beantwoorden.⁷⁹ Er dient altijd een militaire noodzaak te zijn, hoe klein dan ook. Het beginsel van militaire noodzaak is al oud en reeds gecodificeerd in de Lieber Code.⁸⁰ Tegenwoordig is het beginsel onder andere terug te vinden in artikel 52 Aanvullend Protocol I waarin aanvallen alleen zijn toegestaan op militaire doelen, waarbij militaire doelen, voor zover het objecten betreft,⁸¹ gelimiteerd zijn tot die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel oplevert.⁸² Indien geen *duidelijk militair voordeel* te behalen is, bestaat geen militaire noodzaak en is een aanval op deze objecten niet toegestaan. Dit principe behoort tot het gewoonterecht.⁸³ Het humanitair oorlogsrecht vereist derhalve altijd een militaire noodzaak in de vorm van een te behalen militair voordeel⁸⁴ om een aanval te kunnen legitimeren.

Er dient dus altijd sprake te zijn van een militaire noodzaak, maar hoe wordt dit bepaald? Het zal niet mogelijk zijn een maatstaf te vinden waarin dit militaire voordeel in absolute termen is uit te drukken. Door de toevoeging van het bijvoeglijk naamwoord 'duidelijk' aan militair voordeel in de definitie van militaire doelen wordt wel enige duidelijkheid gegeven.

78 Sandoz, Swinarski & Zimmermann 1987, p. 684.

79 In het volgende hoofdstuk kom ik terug op militaire operaties beneden de drempel van aanval.

80 Lieber Code in Schindler en Toman 2004, artt. 14-16 van de Lieber Code waarin achtereenvolgens worden genoemd; een definitie van militaire noodzaak (art. 14), een opsomming van handelingen welke op grond van militaire noodzaak zijn toegestaan (art. 15) en een opsomming van handelingen welke niet zijn toegestaan met een beroep op militaire noodzaak (art. 16).

81 Artikel 52 spreekt slechts van objecten als mogelijk militaire doelen. Het mag echter duidelijk zijn dat ook het personeel van vijandelijke strijdkrachten een legitiem militair doel vormt. Zie hiervoor bijvoorbeeld de preambule van de St. Petersburg Declaration 1868, die spreekt van "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy; [...] for this purpose it is sufficient to disable the greatest possible number of men."

82 Aanvullend protocol I 1979, art 52 lid 2, accentuering mijnerzijds.

83 Heckaerts & Doswald-Beck 2005, p. 29. Rule 8. "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage."

84 Voor de relatie tussen militaire noodzaak en militair voordeel zie Watkin 2014, p. 344.

Hiermee komt tot uitdrukking dat “*it is not legitimate to launch an attack which only offers potential or indeterminate advantages.*”⁸⁵

Hoe de balans in praktijk, bijvoorbeeld in de hiervoor genoemde proportionaliteitsregel uit artikel 51 Aanvullend Protocol I, uit zal vallen hangt af van de beoordeling door de verantwoordelijk commandant, waarbij deze een behoorlijke beoordelingsvrijheid heeft.⁸⁶ Juist door het gebrek aan kwantificeerbaarheid van zowel bijkomende schade als militair voordeel,⁸⁷ wordt van de commandant gezond verstand en goeder trouw verwacht,⁸⁸ door het Joegoslavië Tribunaal ook wel aangeduid als de standaard van een “*reasonable military commander.*”⁸⁹

De dubbele doelstelling van het humanitair oorlogsrecht, te weten het reguleren van de middelen en methoden van oorlogvoering en het beschermen van (potentiële) slachtoffers van een gewapend conflict, is terug te vinden in zowel het onderliggende fundamentele evenwicht waarop het totale stelsel van regels rust, als ook in de toepassing van concrete regels.

Na de behandeling van de doelstelling kan ik nu overgaan naar de context van het humanitair oorlogsrecht.

2.4 Toepassingsgebied humanitair oorlogsrecht

De vraag naar het toepassingsgebied van het humanitair oorlogsrecht is relevant om het humanitair oorlogsrecht in de juiste context te plaatsen, namelijk oorlogvoering. Oorlogvoering impliceert het met geweld opleggen van de eigen doelstellingen aan een tegenstander,⁹⁰ waarbij het doden van personen en het vernietigen van objecten vaak tot de harde realiteit behoren. Het is belangrijk dit nadrukkelijk hier te vermelden omdat dit besef (mede) bepalend is voor de manier waarop naar het humanitair oorlogsrecht gekeken moet worden. Humanitair oorlogsrecht geeft geen normatief oordeel over het verschijnsel oorlog, het gaat uit van het bestaan van oorlog en tracht dit vervolgens te reguleren, onder andere door eisen te stellen aan de status van personen die gedood en objecten die vernietigd mogen worden. Dit uitgangspunt dient in het vervolg van dit hoofdstuk en van dit onderzoek steeds in ogenschouw genomen te worden.

85 Sandoz, Swinarski & Zimmermann 1987, p. 636.

86 Sandoz, Swinarski & Zimmermann 1987, p. 684. Dinstein 2009b, E28: “*a great deal of latitude.*”

87 Zie bijv. Oeter (in Fleck) 2013a, p. 197. “*Objective standards for the appraisal and balancing of expected collateral damage and intended military advantage are virtually non-existent.*”

88 Sandoz, Swinarski & Zimmermann 1987, p. 683.

89 ICTY, Final Report to the Prosecutor 2000, par. 50. Voor een nadere beschouwing over “*reasonable military commander*”, zie Rogers 2004, p. 110-11.

90 Vergelijk de klassieke definitie van Lauterpacht 1952, p. 202; “*War is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.*”

Het humanitair oorlogsrecht zoals we dat tegenwoordig kennen komt voort uit en bouwt verder op traditioneel oorlogsrecht. Dit traditioneel oorlogsrecht, behorend tot het volkenrecht,⁹¹ valt uiteen in twee delen, het *jus ad bellum* en het *jus in bello*. Onder het eerste valt dat deel van het volkenrecht dat ziet op het recht tot gebruik van statelijk geweld in internationale relaties oftewel het aanwenden van geweld als zodanig. Zoals eerder aangegeven laat ik in dit onderzoek het *jus ad bellum* verder buiten beschouwing.⁹² Het andere deel, het recht dat betrekking heeft op de wijze van oorlogvoering, ook wel bekend als humanitair oorlogsrecht, is wel omschreven als: “*International humanitarian law constitutes a reaffirmation and development of the traditional international laws of war (jus in bello)*.”⁹³

Bovenstaande beschrijving geeft, naast de bevestiging dat humanitair oorlogsrecht gebaseerd is op, en een doorontwikkeling is van, het oorlogsrecht, ook weer dat het tegenwoordig gebruikelijker is te spreken over een gewapend conflict dan over een oorlog,⁹⁴ of zoals de International Law Committee concludeerde: “*the Committee found that the term ‘war’, while still used, has, in general, been replaced in international law by the broader concept of ‘armed conflict’*.”⁹⁵

Het humanitair oorlogsrecht is van toepassing zodra sprake is van een gewapend conflict. Hiermee dient zich automatisch de volgende vraag aan: wat is een gewapend conflict?

2.4.1 Wat is een gewapend conflict?

De term gewapend conflict is niet gedefinieerd in een van de humanitair oorlogsrechtelijke verdragen. Ik zal daarom hier kort ingaan op het begrip gewapend conflict. De nadruk leg ik hierbij op het begin van een gewapend conflict.⁹⁶ Het punt waarop aan de voorwaarden van een gewapend conflict wordt voldaan is namelijk ook het punt waarop het overgrote deel van het humanitair oorlogsrecht van kracht wordt.⁹⁷ Het humanitair oorlogsrecht maakt onderscheid tussen twee typen gewapende conflicten, internationale en niet-internationale gewapende conflicten.⁹⁸ In het vervolg van deze paragraaf zal ik deze indeling volgen.

91 Voor de plaats van het oorlogsrecht binnen het volkenrecht, zie bijvoorbeeld Lauterpacht 1953, p. 201-287.

92 Zie Hoofdstuk 1, par. 1.1.1.

93 O’Connell (in Fleck) 2013a p. 11, *Black letter rule* 102.

94 O’Connell (in Fleck) 2013a p. 11. “*Most rules of the law of war now extend even to those armed conflicts that the parties do not regard as wars.*”

95 International Law Committee 2010, p. 1.

96 Dit is een combinatie van het materiële en het temporele bereik van het humanitair oorlogsrecht. Voor een uitgebreide beschrijving van deze aspecten, alsmede die van het personele en het geografische bereik van het humanitair oorlogsrecht zie Kleffner (in Fleck) 2013a p. 43 – 68.

97 Zie bijv. ICTY, *The Prosecutor v. Dusko Tadic*, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 oktober 1995, par. 70. “*International law applies from the initiation of such armed conflicts.*” De opmerking ‘het overgrote deel’ slaat op het feit dat enkele bepalingen uit het humanitair oorlogsrecht ook al van kracht zijn voordat sprake is van een gewapend conflict of juist gelden na het beëindigen van het gewapend conflict. Een voorbeeld van het eerste is de verspreiding van -en onderwijs in- het humanitair oorlogsrecht. Een voorbeeld van het tweede is de verplichting krijgsgevangenen na afloop van het gewapend conflict in vrijheid te stellen en te repatriëren.

98 Voor een uitgebreide beschrijving van de historie van de classificatie van gewapende conflicten en de relevante juridische implicaties daarvan, zie Akande (in Wilmshurst) 2012, p. 32-70.

2.4.1.1 Internationaal gewapend conflict

Wanneer sprake is van een internationaal gewapend conflict is vastgelegd in gemeenschappelijk artikel 2 van de Verdragen van Genève, namelijk “ingeval een oorlog is verklaard of bij ieder ander gewapend conflict dat ontstaat tussen twee of meer der Hoge Verdragsluitende Partijen, zelfs indien de oorlogstoestand door één der Partijen niet wordt erkend.”⁹⁹ Het gaat daarbij om een geschil tussen twee of meer staten waarbij “*any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2.*”¹⁰⁰ Deze vaak geciteerde zinsnede van Pictet is een nadere aanduiding van de term gewapend conflict waarbij “*neither the duration of the conflict, nor its intensity, play a role.*”¹⁰¹ Een situatie van gewapend conflict bestaat vanaf de feitelijke opening van de vijandelijkheden.¹⁰²

Deze visie op een internationaal gewapend conflict waarbij de intensiteit of de duur van de vijandelijkheden geen rol speelt voor het bestaan van het gewapend conflict wordt ook wel aangeduid als de *first-shot* theorie die echter niet unaniem wordt aangehangen.¹⁰³ Een andere visie is dat pas gesproken kan worden van een gewapend conflict als de vijandelijkheden een minimumdrempel overschrijden, zodat ten minste sprake dient te zijn van vijandelijkheden met “*fighting of some intensity.*”¹⁰⁴ De redenen die voor deze laatste visie worden aangedragen zijn enerzijds het onderscheid dat “*States, international organizations, courts, and other legitimate actors in the international legal system distinguish lower level or chaotic violence from armed conflict,*”¹⁰⁵ anderzijds het gebrek aan “*evidence to support the view that the Conventions apply in the absence of fighting of some intensity.*”¹⁰⁶

De visie dat sprake moet zijn van een zekere intensiteit van de gevechten voordat een internationaal gewapend conflict bestaat heeft echter het gevaar in zich dat een internationaal juridisch vacuüm kan ontstaan tussen het eerste schot en het moment dat de vijandelijkheden voldoende intensiteit bereiken. Men kan zich namelijk afvragen welk internationaal rechtsregime van kracht is op vijandelijkheden tussen twee staten tijdens een grensconflict dat nog niet voldoet aan een intensiteit die nodig is om als gewapend

■
99 Gemeenschappelijk art. 2 Verdragen van Genève 1949. Hetzelfde gemeenschappelijke art. 2 bepaalt ook dat de Verdragen van toepassing zijn in alle gevallen van gehele of gedeeltelijke bezetting van het Grondgebied van een Hoge Verdragsluitende Partij, zelfs indien deze bezetting geen gewapende tegenstand ontmoet. Gelet op het onderwerp van mijn onderzoek laat ik bezetting verder buiten beschouwing.

100 Pictet 1952, p. 32. Artikel 2 waaraan gerefereerd wordt is het gemeenschappelijke artikel 2 van de vier Verdragen van Genève uit 1949.

101 Sandoz, Swinarski & Zimmerman 1987, p. 40.

102 Pictet 1952, p. 32.

103 Aanhangers van de *first-shot* theorie zijn bijvoorbeeld Pictet 1952, p. 32, Sandoz, Swinarski & Zimmerman 1987 p. 40, Kleffner (in Fleck) 2013a, p. 45 maar bijvoorbeeld ook het ICTY, *The prosecutor v. Dusko Tadic, Decision on the Motion for Interlocutory Appeal on Jurisdiction*, IT-94-1-A, 2 oktober 1995, par. 70.

104 ILA Final report on the meaning of Armed Conflict in International Law 2010, p. 2. Zie ook IIHL & ICRC 2003, p. 3, Ducheine 2008, p. 506.

105 ILA Final report on the meaning of Armed Conflict in International Law 2010, p. 2.

106 ILA Final report on the meaning of Armed Conflict in International Law 2010, p. 2.

conflict te gelden.¹⁰⁷ Het humanitair oorlogsrecht is nog niet van kracht want er is nog geen sprake van een gewapend conflict. Een neergeschoten vlieger van een straaljager die terechtkomt op het grondgebied van de andere staat en gevangengenomen wordt, kan dan geen beroep doen op een krijgsgevangenenstatus, waardoor hem mogelijk een aantal rechten onthouden worden.

Naar mijn mening hoeft de *first-shot* theorie, waarbij het humanitair oorlogsrecht in een internationaal gewapend conflict *de jure* van toepassing is vanaf het 'eerste schot', staten niet te belemmeren om incidenten niet te behandelen als gewapend conflict zolang daartoe geen aanleiding is.¹⁰⁸ De feitelijke praktijkomstandigheden kunnen namelijk bepalen welk deel van het humanitair oorlogsrecht toegepast dient te worden.¹⁰⁹ Ik zal dit aan de hand van een voorbeeld verduidelijken.

Neem het geïsoleerde grensincident waarbij een straaljager wordt neergeschoten en de piloot zich weet te redden met zijn schietstoel. Volgens de *first-shot* theorie is vanaf het eerste schot sprake van een internationaal gewapend conflict waarop het humanitair oorlogsrecht van toepassing is. Indien de piloot weet te landen op eigen grondgebied, bestaat geen behoefte om het krijgsgevangenenregime daadwerkelijk toe te passen. Indien hij landt op het grondgebied van de vijandige staat en hij wordt gevangengenomen is het krijgsgevangenenregime automatisch van toepassing.

In de andere mogelijke benadering is in het geval van bovenstaand grensincident mogelijk nog geen sprake van een gewapend conflict, omdat de drempel daarvoor nog niet is overschreden. Mogelijk kunnen de beginselen van het oorlogsrecht dan wel houvast bieden en de reactie beheersen.¹¹⁰ Deze benadering leidt de facto waarschijnlijk tot een vergelijkbare uitkomst als hierboven aangegeven bij de *first-shot* theorie, namelijk dat indien de piloot op eigen grondgebied landt er niets gebeurt en, indien de piloot in de andere staat landt en gevangen genomen wordt de regels met betrekking tot krijgsgevangenen worden toegepast. De bescherming die de gevangene volgens de *first-shot* theorie heeft is in mijn optiek echter beter gegarandeerd omdat het krijgsgevangenenregime ook *de jure* van kracht is. De mogelijkheid om situaties waarop het humanitair oorlogsrecht *de jure* van toepassing is (beleidsmatig) niet te beschouwen als gewapend conflict, omdat men bijvoorbeeld naar een de-escalatie streeft, bestaat nog steeds. Zodra zich echter feiten voordoen waarin het humanitair oorlogsrecht extra bescherming verleent, is een staat juridisch verplicht die bescherming ook daadwerkelijk te bieden.

■
107 Kleffner (in Fleck) 2013a, p. 45.

108 Dit feitelijk niet behandelen als gewapend conflict in diverse gevallen werd door de ILA gezien als argument voor een minimale intensiteit van gevechten. ILA Final report on the meaning of Armed Conflict in International Law 2010, p. 18.

109 Kleffner (in Gill & Fleck 2015), p. 38.

110 Ducheine 2008, p. 507, voetnoot 951. Dit kan bijvoorbeeld omdat een staat de restricties uit het humanitair oorlogsrecht al wel beleidsmatig naleeft ook al is dit humanitair oorlogsrecht nog niet formeel van toepassing. Voor Nederland zie Kamerstukken I 2003-2004, 29200 X, C, p. 3, Nationale Defensie Doctrine 2013, p. 55. Ducheine 2009, p. 492. Ook andere landen hebben een vergelijkbare visie, zie bijv. USA Law of War program DoDD 5100.77 par. 5.3.1. "Ensure that the members of their DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, and with the principles and spirit of the law of war during all other operations," mijn accentuering.

Bij de bovenstaande redenering ga ik wel uit van de veronderstelling dat een (gewapend) incident door een (lid van) de krijgsmacht plaatsvindt door sturing van de desbetreffende staat en dat het niet gaat om een 'privédaad'. Een dronken soldaat die, volstrekt tegen alle instructies in, een schot over de grens afvuurt, en daarbij eventueel letsel of schade veroorzaakt, zal daarmee nog geen internationaal gewapend conflict ontketenen. Van leden van een krijgsmacht kan worden verondersteld dat zij handelen naar opdracht, en met goedkeuring, van hun staat. Het zal daarom, ingeval van twijfel, aan de staat die het incident veroorzaakt zijn om, voor de andere staat bevredigend, aan te tonen dat het ging om een onbedoeld incident.

2.4.1.2 *Niet-internationaal gewapend conflict*

In tegenstelling tot de relatief eenvoudige constatering van een internationaal gewapend conflict is de vaststelling van een niet-internationaal gewapend conflict een stuk lastiger. In het internationaal recht zijn staten soeverein¹¹¹ en bij aangelegenheden die wezenlijk vallen onder de nationale rechtsmacht van een staat is het aan de betreffende staat om deze aangelegenheden te behandelen zonder inmenging van buitenaf.¹¹² Interne veiligheid binnen een staat is een aangelegenheid die binnen de nationale rechtsmacht valt en waarvoor de staat eigen regels kan en mag stellen, ook met betrekking tot geoorloofd geweldgebruik. Een karakteristiek voorbeeld is het optreden van de politie ter handhaving van de orde en veiligheid. Ook beteugeling van interne ongeregeldheden en opstanden behoort tot de nationale rechtsmacht van een staat waarbij, zoals gezegd, de betreffende staat zelf regels stelt voor welke (gewelds)bevoegdheden door welke overheidsorganisatie(s) uitgeoefend mogen worden. Hierbij is ook de legitieme inzet van de krijgsmacht mogelijk.

De situatie dat interne veiligheid geheel binnen de nationale rechtsmacht valt, verandert zodra sprake is van een (niet-internationaal) gewapend conflict, omdat een staat dan ook gehouden is het toepasselijk gedeelte van het humanitair oorlogsrecht toe te passen. Met andere woorden, er bestaat een kantelpunt waarop, juridisch gezien, een situatie verandert van puur onder de nationale rechtsmacht van een staat vallend naar een situatie die mede geregeerd wordt door regels van het humanitair oorlogsrecht.¹¹³ De logische vraag is dan, wanneer spreekt men nu van een niet-internationaal gewapend conflict?

111 Dit principe is vastgelegd in art 2 lid 1 van het Handvest van de Verenigde Naties: De Organisatie is gegrond op het beginsel van soevereine gelijkheid van al haar leden.

112 Zie bijvoorbeeld art 1 lid 7 van het Handvest van de Verenigde Naties: Geen enkele bepaling van dit Handvest geeft de Verenigde Naties de bevoegdheid tussenbeide te komen in aangelegenheden die wezenlijk onder de nationale rechtsmacht van een staat vallen, noch wordt op grond van enige bepaling daarin van de Leden verlangd dat zij zodanige aangelegenheden krachtens dit Handvest tot een oplossing brengen. Dit beginsel staat de toepassing van dwangmaatregelen ingevolge Hoofdstuk VII evenwel niet in de weg.

113 Dit is overigens niet de enige mogelijkheid waarbij de interne veiligheid niet langer beperkt wordt tot de exclusieve rechtmacht van die staat. Indien de interne veiligheidssituatie van een staat zich zo ontwikkelt dat er volgens de Veiligheidsraad van de Verenigde Naties sprake is van "bedreiging van de vrede, verbreking van de vrede of daad van agressie" (art. 39 VN Handvest) kan diezelfde Veiligheidsraad maatregelen nemen tot handhaving of herstel van de internationale vrede en veiligheid, waardoor de betreffende staat zich ook aan deze internationale maatregelen zal moeten houden. Voor dit onderzoek is een dergelijke situatie niet van belang en ik laat deze dan verder ook buiten beschouwing.

Gemeenschappelijk artikel 3 van de Verdragen van Genève geeft aan dat sprake is van een niet-internationaal gewapend conflict “in geval van een gewapend conflict op het grondgebied van één der Hoge Verdragsluitende Partijen, hetwelk geen internationaal karakter draagt.”¹¹⁴ Wat verstaan moest worden onder een niet-internationaal gewapend conflict was tijdens de totstandkoming van de verdragen “*the burning question which arose again and again at the Diplomatic Conference.*”¹¹⁵ Gevreesd werd dat “*all forms of insurrection, rebellion, anarchy, and the break-up of States, and even plain brigandage*” onder de term konden worden gebracht¹¹⁶ en diverse pogingen werden gedaan om voorwaarden op te stellen waaraan voldaan zou moeten zijn voordat sprake zou zijn van een gewapend conflict in de zin van gemeenschappelijk artikel 3. Dit heeft in 1949 weliswaar niet geleid tot nadere definiëring van de term niet-internationaal gewapend conflict, maar de discussies leverden wel “*different conditions, although in no way obligatory [that] constitute convenient criteria.*”¹¹⁷ Als criteria werden onder andere genoemd dat de opstandelingen moeten beschikken over een georganiseerde militaire strijdmacht, een autoriteit moeten hebben die verantwoordelijk is voor hun daden, moeten optreden in een aan te duiden grondgebied en moeten beschikken over de middelen om de verdragen van Genève en andere wetten van de oorlog te respecteren en te garanderen.¹¹⁸ Deze criteria zijn met name bedoeld als “*means of distinguishing a genuine armed conflict from a mere act of banditry or an unorganized and short-lived insurrection.*”¹¹⁹

Bij de totstandkoming van Aanvullend Protocol II is voortgeborduurd op bovenstaande criteria. Dit resulteerde in artikel 1, genaamd het materieel toepassingsgebied met als tekst: “Dit Protocol, dat de gemeenschappelijke artikelen 3 van de Verdragen van Genève van 12 augustus 1949 uitbreidt en aanvult, zonder wijziging aan te brengen in de omstandigheden waaronder deze artikelen thans worden toegepast, is van toepassing op alle gewapende conflicten waarop artikel 1 van het Aanvullende Protocol bij de Verdragen van Genève van 12 augustus 1949 betreffende de bescherming van slachtoffers van internationale gewapende conflicten (Protocol I) niet van toepassing is, en die plaatsvinden op het grondgebied van een Hoge Verdragsluitende Partij tussen de strijdkrachten van die Partij en dissidente strijdkrachten of andere gewapende groepen die, staande onder een verantwoordelijk bevel, het grondgebied van die partij gedeeltelijk beheersen op een zodanige wijze dat zij in staat zijn aanhoudende en samenhangende militaire operaties uit te voeren en de bepalingen van dit Protocol toe te passen.”¹²⁰ De bedoeling van dit artikel was drieledig, namelijk om de boven- en ondergrens van een niet-internationaal gewapend conflict vast te stellen, te voorzien in de elementen van een definitie en zeker te stellen dat de werking van gemeenschappelijk artikel 3 van de Verdragen van Genève intact zou blijven.¹²¹

114 Gemeenschappelijk art. 3 Verdragen van Genève 1949.

115 Pictet 1952, p. 49.

116 Pictet 1952, p. 43.

117 Pictet 1952, p. 49.

118 Pictet 1952, p. 50.

119 Pictet 1952, p. 50.

120 Aanvullend Protocol II art. 1 lid 1.

121 Sandoz, Swinarski & Zimmerman 1987, p. 1349.

Artikel 1 van Aanvullend Protocol II geeft aan dat dit Protocol van toepassing is op alle gewapende conflicten die niet vallen onder het toepassingsgebied van artikel 1 van Aanvullend Protocol I. Dit vormt de bovengrens van een niet-internationaal gewapend conflict.¹²² De ondergrens wordt gegeven door lid 2 van artikel 1 Aanvullend Protocol II, dat aangeeft dat interne ongeregelde heden en spanningen, zoals rellen, op zichzelf staande en sporadisch voorkomende daden van geweld en andere handelingen van soortgelijke aard niet tot het toepassingsgebied van Aanvullend Protocol II behoren.¹²³ Bij de totstandkoming van de bepaling over de ondergrens was het de bedoeling “*to specify the characteristics of a non-international armed conflict by means of objective criteria so that the Protocol could be applied when those criteria were met and not be made subject to other considerations.*”¹²⁴ Het bleek echter moeilijk om consensus te bereiken over de criteria van een niet-internationaal gewapend conflict en de drie eisen voor de opstandelingen die uiteindelijk terechtgekomen zijn in artikel 1, onder verantwoordelijk bevel, een grondgebied gedeeltelijk beheersen zodat aanhoudende en samenhangende militaire operaties uit te voeren zijn en de mogelijkheid om Aanvullend Protocol II te implementeren, maken dat niet alle gevallen van niet-internationaal gewapend conflict erdoor afgedekt zijn, wat wel het geval is voor gemeenschappelijk artikel 3 van de Verdragen van Genève.¹²⁵

De verdragsteksten, noch de officiële *Commentaries*, geven uitputtende criteria om te beoordelen wanneer een situatie een niet-internationaal gewapend conflict is. Daarom wordt voor het onderscheid tussen de situaties van interne ongeregelde heden en een niet-internationaal gewapend conflict tegenwoordig vrij algemeen gebruik gemaakt van twee criteria, te weten de intensiteit van het gebruikte geweld en de organisatiegraad van de gewapende groepering(en). Hiermee wordt aangesloten bij de vaak geciteerde uitspraak van het *International Criminal Tribunal for the Former Yugoslavia* (hierna het Joegoslavië Tribunaal) waarin werd geconcludeerd dat “*an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.*”¹²⁶ Het tweede gedeelte van deze ‘beschrijving’ van een gewapend conflict, handelend over een niet-internationaal gewapend conflict, is in vergelijkbare bewoordingen opgenomen in het Statuut van Rome.¹²⁷

In 1997 heeft het Joegoslavië Tribunaal de voorwaarden van intensiteit van de vijandelikheden en organisatiegraad van de gewapende groepering(en) expliciet genoemd

122 Aanvullend Protocol II art. 1 lid 1 via Aanvullend Protocol I art. 1.

123 Aanvullend Protocol II art. 1 lid 2.

124 Sandoz, Swinarski & Zimmerman 1987, p. 1349.

125 Sandoz, Swinarski & Zimmerman 1987, p. 1349.

126 ICTY, *The Prosecutor v. Dusko Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, IT-94-1-A, 2 oktober 1995, par. 70.

127 Statuut van Rome 1998, art. 8 lid 2 sub f spreekt van: “gewapende conflicten die plaatsvinden op het grondgebied van een Staat in het geval van een langdurig gewapend conflict tussen overheidsautoriteiten en georganiseerde gewapende groepen of tussen deze groepen onderling.”

als ondergrens van een niet-internationaal gewapend conflict¹²⁸ om vervolgens in 2008 te concluderen dat *“the criterion of protracted armed violence has therefore been interpreted in practice, including by the Tadić Trial Chamber itself, as referring more to the intensity of the armed violence than to its duration”*.¹²⁹ Om te kunnen concluderen of voldaan is aan het intensiteitscriterium, gebruikte het Joegoslavië Tribunaal de volgende indicatieve factoren: aantal, duur en intensiteit van de individuele confrontaties; het type wapens en andere militaire uitrusting die werd gebruikt; het aantal en het kaliber munitie dat werd afgeschoten; het aantal personeel en het type eenheden dat deelnam aan de strijd; het aantal slachtoffers; de materiële schade en het aantal burgers dat gevlucht is vanuit de gebieden waar gevochten werd. Ook de betrokkenheid van de Veiligheidsraad van de Verenigde Naties kan een indicatie geven over de intensiteit van de strijd.¹³⁰

Net als bij het intensiteitscriterium heeft het Joegoslavië Tribunaal voor het organisatiecriterium van gewapende groeperingen een aantal indicatoren gebruikt¹³¹ te weten: het bestaan van een commandostructuur en een disciplinair systeem met regels en mechanismen binnen de groep; het bestaan van een hoofdkwartier; het feit dat de groep een gedeelte van het grondgebied controleert; de mogelijkheid van de groep om zich toegang tot wapens en andere militaire uitrusting te verschaffen; de mogelijkheid tot rekrutering en militaire training; de capaciteit om militaire operaties te plannen, coördineren en uit te voeren inclusief verplaatsing en logistiek; de capaciteit om een eendrachtige militaire strategie te definiëren en militaire tactieken uit te kunnen voeren en de capaciteit om met één mond te spreken en overeenkomsten zoals staakt-het-vuren en vredesakkoorden uit te kunnen onderhandelen en af te kunnen sluiten.¹³²

Voor zowel het intensiteits- als het organisatiecriterium geldt dat de genoemde indicatieve factoren niet gezien moeten worden als een checklist die afgewerkt kan worden en die vervolgens leidt tot een onomstreden uitkomst. De lijst moet meer gezien worden als een richtlijn om, aan de hand van de concrete omstandigheden, te komen tot een oordeel of wel of niet sprake is van een gewapend conflict, om daarmee tegelijkertijd te oordelen of het humanitair oorlogsrecht wel of niet van toepassing is.¹³³

2.4.2 Conclusie toepassingsgebied humanitair oorlogsrecht

Samengevat is het humanitair oorlogsrecht van toepassing op situaties van gewapend conflict oftewel *“International humanitarian law regulates, and as a rule applies in times of, armed*

128 ICTY, *Prosecutor v. Tadić (judgement)*, IT-94-1-T, par. 562. *“In an armed conflict of an internal or mixed character, these closely related criteria are used solely for the purpose, as a minimum, of distinguishing an armed conflict from banditry, unorganized and short-lived insurrections, or terrorist activities, which are not subject to international humanitarian law.”*

129 ICTY, *Prosecutor v. Ramush Haradinaj et al*, IT-04-84-T, 3 april 2008, par. 49. Dinstein is echter van mening dat duur en intensiteit gescheiden criteria zijn die ook gescheiden beoordeeld moeten worden, Dinstein 2014, p.35.

130 ICTY, *Prosecutor v. Ramush Haradinaj et al*, IT-04-84-T, 3 april 2008, par. 49.

131 Deze criteria zijn uitsluitend nodig voor het bepalen van de organisatiegraad van gewapende groeperingen omdat van de strijdkrachten van een staat wordt verondersteld dat ze voldoen aan het organisatiecriterium.

132 ICTY, *Prosecutor v. Ramush Haradinaj et al*, IT-04-84-T, 3 april 2008, par. 60.

133 Voor een voorbeeld van de toepassing van deze criteria zie Ducheine & Pouw 2010, Hoofdstuk 5.

conflict.¹³⁴ Dit geldt voor een gewapend conflict in zijn algemeenheid, dus zowel voor een internationaal, als voor een niet-internationaal gewapend conflict. Dat het humanitair oorlogsrecht van kracht is tijdens een gewapend conflict betekent overigens niet dat het daarbuiten geen enkele rol speelt. Zo geeft het humanitair oorlogsrecht ook bepalingen die al van kracht zijn voor het uitbreken van een gewapend conflict¹³⁵ of nog door kunnen werken nadat het gewapend conflict is geëindigd.¹³⁶

Om de context van het humanitair oorlogsrecht te voltooien geef ik hier nog een aanvulling ter voorkoming van verwarring, omdat deze situatie *niet* valt onder het regime van het humanitair oorlogsrecht. Het humanitair oorlogsrecht reguleert de operaties van de strijdende partijen met betrekking tot het gewapend conflict.¹³⁷ Andere militaire activiteiten die plaatsvinden tijdens een gewapend conflict, maar hier geen relatie mee hebben, bijvoorbeeld humanitaire hulpverlening na een natuurramp of hulpverlening aan de civiele autoriteiten ter handhaving van de openbare orde,¹³⁸ vallen niet onder het regime van het humanitair oorlogsrecht.¹³⁹

Met het gewapend conflict als context voor, en de dubbele doelstelling van, het humanitair oorlogsrecht in het achterhoofd kan ik nu overgaan tot bespreking van het begrip ‘aanval’ en dit plaatsen in relatie tot de begrippen militaire operaties, vijandelijkheden en oorlogvoering.

2.5 Aanval in de context van het humanitair oorlogsrecht

Zoals ik in de inleiding van dit hoofdstuk al constateerde, bestaat binnen het humanitair oorlogsrecht een relatie tussen de begrippen ‘militaire operaties’ en ‘aanvallen’, maar zijn het geen synoniemen. Omdat ik op zoek ben naar de regels binnen het humanitair oorlogsrecht die van kracht zijn beneden de drempel van aanval is het noodzakelijk de relatie tussen ‘militaire operatie’ (*military operation*) en ‘aanval’ (*attack*) zo nauwkeurig mogelijk te omschrijven. In deze paragraaf zal ik dit doen, waarbij ik ook aangeef wat de plaats van deze twee is ten opzichte van de begrippen ‘vijandelijkheden’ (*hostilities*) en ‘oorlogvoering’ (*warfare*). Ik doe dit door eerst een schematisch overzicht te geven en vervolgens, in een top-down benadering, steeds verder in te zoomen om uit te komen op de kleinste deelverzameling, namelijk ‘aanval’.

¹³⁴ Kleffner (in Fleck) 2013a, p. 43, *Black letter rule* 201.

¹³⁵ Denk hierbij bijvoorbeeld aan verspreiding van en onderwijs in het humanitair oorlogsrecht (o.a. vastgelegd in Aanvullend Protocol I art. 83).

¹³⁶ Denk hierbij bijvoorbeeld aan bepalingen over vermisten en stoffelijke overschotten (o.a. vastgelegd in Aanvullend Protocol I art. 33 en 34).

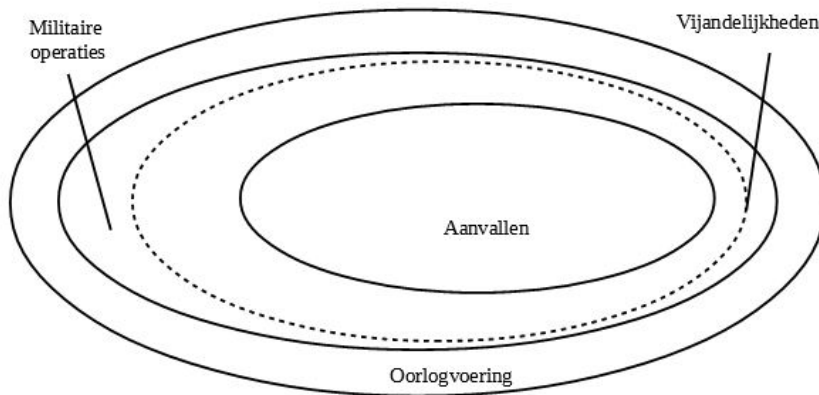
¹³⁷ In par. 5 van dit hoofdstuk besteed ik aandacht aan het onderscheid tussen militaire operaties, vijandelijkheden en aanvallen.

¹³⁸ Zo zal in de Nederlandse situatie bijstand door defensie aan civiele autoriteiten op basis van de Wet Veiligheidsregio's of Politiewet 2012, indien geen directe relatie bestaat met een gewapend conflict, niet onder het regime van het humanitair oorlogsrecht vallen, ook niet als Nederland op dat moment betrokken is bij een gewapend conflict.

¹³⁹ Zie ook Hoofdstuk 1 par. 1.3.2.

2.5.1 Schematisch overzicht

Voordat ik overga tot het geven van het overzicht een opmerking vooraf. Met uitzondering van de term ‘aanval’ is geen van de andere begrippen gezaghebbend gedefinieerd binnen het humanitair oorlogsrecht. Toch bestaat wel enige consensus over de onderlinge relaties tussen de begrippen,¹⁴⁰ zoals hieronder weergegeven in figuur 1, al dient daarbij opgemerkt te worden dat met name de grens tussen militaire operaties en vijandelijkheden niet altijd hetzelfde wordt uitgelegd, waardoor discussie blijft bestaan. Vanwege het gebrek aan gezaghebbende definities en om spraakverwarring te voorkomen, zal ik in het vervolg van deze paragraaf ingaan op de verschillende begrippen en de onderlinge grenzen zoals ik ze hanteer, en als laatste, uitgebreider, stilstaan bij het onderscheid tussen militaire operaties en aanvallen.



Figuur 1 Relatie tussen de begrippen binnen het humanitair oorlogsrecht.¹⁴¹

2.5.2 Oorlogvoering

Eerder in dit hoofdstuk, in paragraaf 2.4.1, heb ik aangegeven wat wordt verstaan onder een gewapend conflict. Dit wordt gezien als de meest omvattende term¹⁴² waarop het humanitair oorlogsrecht van kracht is. Omdat een gewapend conflict een toestand is terwijl de begrippen die ik hier beschrijf activiteiten betreffen, heb ik gekozen voor oorlogvoering als meest omvattend begrip van activiteiten die plaatsvinden in het kader van een gewapend conflict,¹⁴³ daarbij gebruik makend van de officiële vertaling van *warfare*, zoals gebruikt in bijvoorbeeld artikel 35 Aanvullend Protocol I.¹⁴⁴

¹⁴⁰ DPH 2005, p.18-19, *Basic Hierarchy of Notions*.

¹⁴¹ Grotendeels gebaseerd op Ducheine 2008, p. 486.

¹⁴² DPH 2005, p.18.

¹⁴³ Ducheine 2008, p. 486 gebruikt hiervoor de term algemene oorlogsinspanning.

¹⁴⁴ Aanvullend Protocol I art. 35 geeft de grondregels voor de methoden en middelen van oorlogvoering.

Artikel 35 Aanvullend Protocol I geeft ook een indicatie dat oorlogvoering meer in kan houden dan vijandelijkheden of militaire operaties. Bij de totstandkoming van Aanvullend Protocol I is gediscussieerd over de terminologie, waarna methoden van oorlogvoering de voorkeur kreeg boven methoden van gevechtshandelingen (*methods of combat*), omdat “*combat can be construed more narrowly than warfare*.”¹⁴⁵ Zo vallen militaire activiteiten die niet specifiek gevechtshandelingen zijn, bijvoorbeeld psychologische of informatie operaties, wel onder methoden en middelen van oorlogvoering, maar niet onder gevechtshandelingen.¹⁴⁶

Een andere indicatie dat oorlogvoering het meest omvattende begrip is levert de *Commentary* bij artikel 51 Aanvullend Protocol I. Hier worden vijandelijkheden omschreven als “*acts which by their nature and purpose are intended to cause actual harm to the personnel and equipment of the armed forces*”.¹⁴⁷ Bij de beoordeling van wat onder vijandelijkheden valt, bestaat ongetwijfeld enige beoordelingsruimte. Vijandelijkheden beperken tot daadwerkelijke gevechtshandelingen is te beperkt, maar het begrip uitbreiden tot de algehele oorlogsinspanning is te breed omdat in moderne oorlogvoering de gehele bevolking op de een of andere manier deelneemt aan oorlogvoering, zij het vaak indirect.¹⁴⁸

De laatste indicatie dat oorlogvoering het meest omvattende begrip is, is te vinden in de *Interpretive Guidance van het International committee of the Red Cross*. Deze gaat uit van de situatie dat naast directe deelname aan vijandelijkheden ook indirecte deelname aan vijandelijkheden bestaat, die niet leidt tot het verlies van oorlogsrechtelijke bescherming.¹⁴⁹ Zaken als ontwerp, productie en verplaatsing van wapens en militaire uitrusting, constructie en reparatie van wegen, havens, vliegvelden, bruggen en andere infrastructurele werken behoren tot de algehele oorlogsinspanning en zolang dit buiten de context van een concrete militaire operatie geschiedt, behoren deze activiteiten niet tot vijandelijkheden. In tegenstelling tot vijandelijkheden zijn deze activiteiten niet bedoeld om schade te veroorzaken, maar slechts om de capaciteit om schade te veroorzaken te handhaven of op te bouwen.¹⁵⁰

In dit verband verwijs ik ook terug naar het gegeven dat een staat meerdere mogelijkheden heeft om zijn doelstellingen te bereiken.¹⁵¹ Zo kunnen ook economie, diplomatie en informatie ingezet worden voor oorlogvoering zonder dat dit militaire operaties hoeven

145 Sandoz, Swinarski & Zimmermann 1987, p. 397.

146 Dörmann 2004, p. 4 “the concept of ‘attacks’ excludes dissemination of propaganda, embargoes and other non-physical means of psychological, political or economic warfare”

147 Sandoz, Swinarski & Zimmermann 1987, p. 618.

148 Sandoz, Swinarski & Zimmermann 1987, p. 516.

149 De *Interpretive Guidance on the notion of Direct Participation in Hostilities* is een uitgave van het International Committee of the Red Cross (ICRC).

150 *Interpretive guidance* 2009, p. 1020. Naast de algehele oorlogsinspanning identificeert het ICRC ook nog activiteiten die ondersteunend zijn aan de oorlogsinspanning (*war-sustaining activities*) zoals politieke, economische en media activiteiten die de oorlogsinspanning ondersteunen. Deze laatste categorie heeft weliswaar te maken met het gewapend conflict, maar maakt volgens het ICRC geen deel uit van de gehele oorlogsinspanning.

151 Zie Hoofdstuk 1 par. 1.1.2.

te zijn of deze direct tot de vijandelijkheden gerekend moeten worden.¹⁵² Deze activiteiten worden ook wel samengevat onder de noemer *war-sustaining activities*.¹⁵³ Voorbeelden hiervan zijn politiek propaganda, financiële transacties, productie van agrarische of niet-militaire producten¹⁵⁴ maar ook een diplomatiek offensief om de tegenstander te isoleren.

Na oorlogvoering als meest omvattend begrip ben ik aangekomen bij de volgende twee begrippen, namelijk 'militaire operaties' en 'vijandelijkheden'. Beide begrippen zijn deels overlappend en aan elkaar gerelateerd¹⁵⁵ en worden ook niet altijd onderscheidend gebruikt. Het onderscheid is mede afhankelijk van de manier waarop het begrip 'vijandelijkheden' wordt uitgelegd, in brede of in enge zin.¹⁵⁶ Omdat over het algemeen 'militaire operaties' als het meeromvattende begrip wordt gezien, begin ik in de volgende paragraaf met militaire operaties, gevolgd door vijandelijkheden in paragraaf 2.5.4.¹⁵⁷

2.5.3 Militaire operaties

Hiervoor is al aangegeven dat de term militaire operaties in het humanitair oorlogsrecht nergens gedefinieerd is en ook niet altijd eenduidig wordt gebruikt. Zo luidt de titel van deel IV, sectie I van Aanvullend Protocol I "Algemene bescherming tegen de gevolgen van de vijandelijkheden"¹⁵⁸ terwijl het eerste artikel van deze sectie, artikel 48 getiteld grondregel, de term 'operaties' gebruikt. Deze laatste term moet worden begrepen als militaire operaties omdat "*for reasons which have nothing to do with the discussions in the Diplomatic Conference, the adjective "military" was not used with the term "operations"*".¹⁵⁹ De term refereert aan "*military operations during which violence is used, and not to ideological, political or religious campaigns*".¹⁶⁰ Uit deze omschrijving blijkt dat er, naast vijandelijkheden, ook bewegingen en daden gerelateerd aan vijandelijkheden bestaan. Als deze worden ondernomen door strijdkrachten is in alle gevallen, dus zowel bij vijandelijkheden als bij alle bewegingen en daden gerelateerd aan vijandelijkheden, sprake van militaire operaties.

Uit bovenstaande blijkt dat militaire operaties in het humanitair oorlogsrecht een vrij breed begrip is en dat zowel de gevechtsacties als de voorbereidingen daarop, zoals planning, bevoorrading, verplaatsing naar en terugkeer van de gevechtsacties (etc.) onder het begrip vallen. De term 'militaire operaties' moet echter wel gelezen worden in de context waarin

152 Zie bijv. Ducheine & Osinga 2017, NLARMS 2017.

153 *Interpretive guidance* 2009, p. 1020.

154 *Interpretive guidance* 2009, p. 1020. Deze voorbeelden hebben weliswaar te maken met het gewapend conflict, maar maken volgens het ICRC geen deel uit van de gehele oorlogsinspanning.

155 Zo geeft de *Commentary* op Aanvullend Protocol I de volgende beschrijving van militaire operaties: "*all the movements and activities carried out by armed forces related to hostilities*." Sandoz, Swinarski & Zimmerman 1987, p. 617.

156 DPH 2005 p. 19. *narrow or wide interpretation of hostilities*.

157 Zoals aangegeven in par. 2.4.1 werk ik van het meest omvattende begrip 'oorlogvoering' naar de kleinste deelverzameling 'aanvallen'.

158 Aanvullend Protocol I, deel IV, sectie I, mijn accentuering.

159 Sandoz, Swinarski & Zimmerman 1987, p. 600.

160 Sandoz, Swinarski & Zimmerman 1987, p. 600.

hij wordt gebruikt.¹⁶¹ In de context van het humanitair oorlogsrecht betekent ‘militaire operaties’ dat de operatie uitgevoerd moet worden in het kader van een gewapend conflict oftewel *“any military action or the carrying out of a strategic, tactical, service, training or administrative military mission, the process of carrying on combat, including movement, supply, attack, defense and maneuver needed to gain the objective of any battle or campaign.”*¹⁶² Het laatste gedeelte van deze beschrijving lijkt daarmee in de buurt te komen van het grotere begrip oorlogvoering. Ik breng hier echter in herinnering de opmerking uit Hoofdstuk 1¹⁶³ dat een staat meerdere mogelijkheden heeft om zijn doelstellingen te bereiken. Zo kunnen diplomatieke druk of economische maatregelen zeker een uitwerking hebben in het kader van de oorlogvoering, maar het zijn daarmee nog geen militaire operaties.¹⁶⁴

Om te kwalificeren als militaire operatie in het kader van een gewapend conflict moet de operatie gerelateerd zijn aan de vijandelijkheden,¹⁶⁵ waarbij ‘gerelateerd aan de vijandelijkheden’ betekent dat de doelstelling moet zijn een voordeel ten opzichte van de tegenstander te behalen. Dit onderscheidt deze operaties van andere militaire operaties die ook buiten een situatie van gewapend conflict kunnen plaatsvinden, zoals bijvoorbeeld steunverlening aan civiele autoriteiten of humanitaire hulpverlening.¹⁶⁶ Voor dit onderzoek beperk ik mij dan ook tot militaire operaties die gerelateerd zijn aan de vijandelijkheden, wat verklaart waarom militaire operaties in figuur 1 een deelverzameling is van oorlogvoering.¹⁶⁷

Bij gebrek aan een eenduidige definitie in verdragen kan, voor een goed begrip van een bepaalde term, gebruik gemaakt worden van de gewone betekenis van de term.¹⁶⁸ Van Dale omschrijft een (militaire) operatie als het “grootschalig geheel van krijgsverrichtingen van leger, vloot en/of luchtmacht.”¹⁶⁹ Het ‘woordenboek’ van de Noord-Atlantische Verdragsorganisatie (NAVO) geeft een militaire operatie weer als: *“A military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defense and maneuvers needed to gain*

161 Verdrag van Wenen, artikel 31.

162 Bothe, Partch & Solf 1982, p. 286.

163 Zie Hoofdstuk 1, par. 1.1.2.

164 Indien dergelijke acties worden uitgevoerd of ondersteund met militaire middelen ontstaat een minder helder onderscheid. Het zal dan van de mate van ondersteuning afhangen of gesproken kan worden van een militaire operatie of niet. Als een diplomaat een militair communicatiemiddel gebruikt om een boodschap over te brengen zal dit waarschijnlijk onvoldoende zijn om te spreken over een militaire operatie. Als het militaire inlichtingenapparaat wordt ingezet om zwakheden van de tegenstander op te sporen en de daaruit voortkomende informatie wordt door een diplomaat gebruikt als diplomatiek drukmiddel kan wel sprake zijn van een militaire operatie.

165 Sandoz, Swinarski & Zimmerman 1987, p. 600.

166 Op deze laatste operaties is het humanitair oorlogsrecht niet van toepassing. Zie ook hiervoor in par. 2.4.2.

167 Deelverzameling gebruik ik hier in de wiskundige zin van het woord namelijk dat alle militaire operaties ook tot oorlogvoering behoren.

168 Verdrag van Wenen 1969, art. 31 lid 1.

169 Groot Woordenboek der Nederlandse Taal, vijftiende herziene druk 2015.

*the objectives of any battle or campaign.*¹⁷⁰ De Nederlandse Defensiedoctrine omschrijft een militaire operatie als het “feitelijk militair optreden dat voor een specifiek doel (inzet) wordt uitgevoerd, in tegenstelling tot trainingsactiviteiten.”¹⁷¹ Het gaat daarbij om het aanwenden van het militaire machtsmiddel,¹⁷² ook wel aangeduid als militair vermogen¹⁷³ voor daadwerkelijke activiteiten.¹⁷⁴ Door in de bovenstaande omschrijvingen van de NAVO en de Nederlandse Defensiedoctrine het (succesvol) beëindigen van een gewapend conflict als specifiek doel in te vullen,¹⁷⁵ worden ze bruikbaar voor toepassing binnen een gewapend conflict.

De omschrijvingen van de NAVO en de Nederlandse Defensiedoctrine hebben gemeen dat ze spreken van de daadwerkelijke inzet van militaire middelen om een bepaald doel (objective) te bereiken.¹⁷⁶ Tevens blijkt uit deze omschrijvingen dat militaire operaties meer omvatten dan alleen gevechtshandelingen (*combat*), wat ook, meer impliciet, blijkt uit de taalkundige beschrijving van Van Dale. Zo zijn een inlichtingen-operatie of een luchtverkenning, maar ook een evacuatie-operatie van burgers uit een risicovol operatiegebied, te kwalificeren als militaire operaties in de context van het humanitair oorlogsrecht terwijl deze operaties niet kwalificeren als de hierna te bespreken vijandelijkheden.

Uit het bovenstaande kom ik voor de toepassing van het humanitair oorlogsrecht tot de volgende beschrijving van militaire operaties. Militaire operaties in de context van het humanitair oorlogsrecht zijn acties uitgevoerd door militairen en/of met militaire middelen om een specifieke militaire doelstelling te verwezenlijken. In het paradigma van ‘oorlogvoering’ is de militaire doelstelling gericht op het behalen van een militair voordeel ten opzichte van de tegenstander.

Hierboven is aangegeven wat onder militaire operaties in de context van het humanitair oorlogsrecht verstaan moet worden. Maar waarin verschillen deze operaties, als ze al verschillen, van dat andere begrip, ‘vijandelijkheden’? Dat is onderwerp van paragraaf 2.5.5. Voordat ik dit kan doen bespreek ik eerst het begrip ‘vijandelijkheden’.

170 NATO GLOSSARY ON TERMS AND DEFINITIONS, Allied Administrative Publication AAP-o6(2013) te raadplegen op nsa.nato.int/nsa/nsdd/listpromulg.html. Dezelfde definitie wordt ook gegeven in de *United States of America Department of Defense. Military terms* te raadplegen op www.military_terms.net.

171 LDP-1 2009, p. 29.

172 Nationale Defensie Doctrine 2013, p. 21. De M uit DIME.

173 Nationale Defensie Doctrine 2013, p. 71.

174 Ducheine & van Haaster 2013, p. 370.

175 Dit valt daarmee binnen de noemers van strategische functies van het militaire machtsmiddel: “Beschermen: Het beschermen en zo nodig verdedigen van het eigen en het bondgenootschappelijke grondgebied, alsmede het waarborgen van de veiligheid van de Nederlandse staatsburgers in binnen- en buitenland en van de in het koninkrijk geregistreerde eigendommen. Intervenieren: Het afdwingen van een gedragsverandering bij actoren die de veiligheidsbelangen van het koninkrijk of de internationale rechtsorde bedreigen. Stabiliseren: Het assisteren bij de beëindiging van een conflict en het bevorderen van een stabiele politieke, economische en sociale ontwikkeling in een (voormalig) conflictgebied in dienst van de belangen van het koninkrijk en de internationale rechtsorde. Nederlandse Defensiedoctrine 2013, p. 42.

176 In dezelfde zin ook Gill & Fleck 2015, p. 682: “*Military operation(s)* – i.e. sequence(s) of coordinated actions with a defined purpose – conducted by armed forces.”

2.5.4 Vijandelijkheden

Hague Convention IV, Afdeling II ‘Van de vijandelijkheden’ begint met Hoofdstuk I over middelen om de vijand te benadelen (*means of injuring the enemy*), belegeringen (*sieges*) en bombardementen (*bombardments*).¹⁷⁷ Dit is een voorbeeld van een brede uitleg van vijandelijkheden waarbij het in essentie gaat om alle activiteiten van een oorlogvoerende partij gericht op het winnen van het gewapend conflict.¹⁷⁸ In de meest brede uitleg wordt de term ‘vijandelijkheden’ als equivalent van oorlogvoering gezien.¹⁷⁹

Naast deze brede uitleg van vijandelijkheden is ook een andere, engere uitleg van vijandelijkheden mogelijk die kan worden omschreven als “daden van oorlog die naar aard en doelstelling bedoeld zijn om feitelijk schade aan personeel of materieel van de vijandelijke strijdkrachten te veroorzaken.”¹⁸⁰ Deze enge uitleg wordt soms ook aangeduid als *active hostilities*,¹⁸¹ en is dan synoniem aan *fighting*.¹⁸² Bij deze beperkte uitleg van vijandelijkheden behoren militaire operaties die niet gericht zijn op directe fysieke gevolgen bij de vijandelijke strijdkrachten of deze gevolgen hebben, niet tot de vijandelijkheden of zoals Droege het verwoordt: “Operations such as propaganda, espionage, or psychological operations will not fall under the concept of hostilities or military operations and are therefore not governed by the principles of distinction, proportionality, and precaution, even if they are carried out by the armed forces.”¹⁸³

In de brede interpretatie van vijandelijkheden komt het begrip redelijk in de buurt van het begrip militaire operaties, of misschien zelfs oorlogvoering, binnen het humanitair oorlogsrecht. In een enge interpretatie, waarbij het begrip synoniem staat aan gevechtsacties, zou het een deelverzameling van militaire operaties zijn. In de volgende paragraaf zal ik aangeven waarom ik voor de laatste interpretatie kies.

2.5.5 Militaire operaties versus vijandelijkheden

Zijn vijandelijkheden niet eenduidig te zien als deelverzameling van militaire operaties?¹⁸⁴ Bij een internationaal gewapend conflict worden militaire operaties uitgevoerd door strijdkrachten.¹⁸⁵ Strijdkrachten vechten met elkaar en voeren daarnaast andere militaire operaties uit die gerelateerd zijn aan die gevechten, zoals verplaatsingen, logistieke

177 *Hague Convention IV*, section II Hostilities.

178 DPH 2005, p.19. In dezelfde zin Dinstein 2015, p.1.

179 DPH 2005, p.18, “actual prosecution of the armed conflict on behalf of the parties to the conflict,” *Interpretive Guidance* 2009, p. 43 voetnoot 80.

180 Sandoz, Swinarski & Zimmermann 1987, p. 619. Voor de ruimte die bestaat tussen de ruime en enge uitleg van vijandelijkheden zie hiervoor Hoofdstuk 2 par. 2.5.2 over oorlogvoering.

181 Verdrag III van Geneve 1949, art. 108. *Prisoners of war shall be released and repatriated without delay after the cessation of active hostilities*. De Nederlandse vertaling spreekt hier slechts over ‘vijandelijkheden’.

182 Pictet 1960b, p. 547.

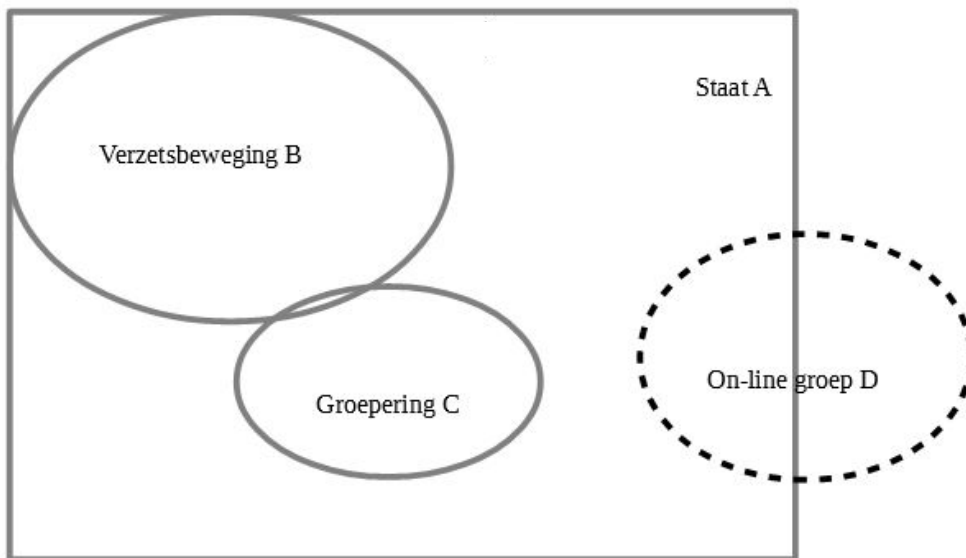
183 Droege 2012, p. 556. Deze opmerking is opmerkelijk omdat Droege activiteiten als spionage, propaganda en psychologische operaties niet ziet als een militaire operaties in elk geval niet als militaire operaties vallend onder het humanitair oorlogsrecht.

184 Deelverzameling ook hier in de wiskundige zin dat alle vijandelijkheden ook militaire operaties zijn.

185 Sandoz, Swinarski & Zimmerman 1987, p. 600.

operaties, maar ook psychologische operaties die geen gevechten zijn. Dit zal over het algemeen weinig kwalificatieproblemen opleveren en dus kunnen ‘vijandelijkheden’ gezien worden als een deelverzameling van ‘militaire operaties’.

Hoe is dit bij een niet-internationaal gewapend conflict? In een niet-internationaal gewapend conflict treden één of meerdere, georganiseerde gewapende groeperingen op als partij in het conflict.¹⁸⁶ Een van de elementen die in de beoordeling of een gewapende groepering georganiseerd is, wordt meegenomen, is de capaciteit om militaire operaties te plannen, te coördineren en uit te voeren.¹⁸⁷ Er zal, met andere woorden, een zekere mate van organisatie aanwezig moeten zijn voordat meer of minder complexe operaties, waarbij planning en coördinatie nodig is, tot uitvoering kunnen worden gebracht. Georganiseerde gewapende groeperingen kunnen dus zowel militaire operaties als vijandelijkheden¹⁸⁸ uitvoeren. Een spontane actie door één persoon of groepering, ook als de actie wordt uitgevoerd met geweld in het kader van het gewapend conflict is echter nog niet per definitie een militaire operatie of een vijandelijkheid. Een dergelijke operatie zal er zeker niet toe leiden dat gesproken kan worden van de start van een niet-internationaal gewapend conflict,¹⁸⁹ maar wat als er al een niet-internationaal gewapend conflict gaande is? Neem nu de volgende situatie:



Figuur 2 Overzicht situatie Staat A

■
¹⁸⁶ Zie par. 2.4.1.2.

¹⁸⁷ ICTY, *Prosecutor v. Ramush Haradinaj et al*, IT-04-84-T, 3 april 2008, par. 60.

¹⁸⁸ In de zin van daden van oorlog die naar aard en doelstelling bedoeld zijn om feitelijk schade aan personeel of materieel van de vijandelijke strijdkrachten te veroorzaken.

¹⁸⁹ Zie par. 2.4.1.2.

In Staat A bestaat een niet-internationaal gewapend conflict tussen de krijgsmacht van Staat A en verzetsbeweging B. B voldoet ruimschoots aan de organisatiegraad en ook aan het intensiteitscriterium wordt voldaan: over en weer vinden al langere tijd vijandelijkheden plaats.

Groepering C is een groepering die niet voldoet aan de organisatiegraad om te worden gezien als een gewapende groepering in het niet-internationaal gewapend conflict. Zij onderhouden echter banden met verzetsbeweging B en hebben belang bij het verzwakken van de autoriteit van A. Sommige leden van C doen, als het hun uitkomt, mee met acties van verzetsbeweging B.

D is een spontaan ontstane *on-line* actiegroep na een oproep via *social media*. Zowel mensen uit A, als uit het buitenland (veelal personen met een binding met Staat A) hebben zich *on-line* aangesloten. Zij hebben genoeg van alle onrust in A en onder de naam *patriotic hackers of A* roepen zij op tot het ondernemen van acties tegen verzetsbeweging B en groepering C waarbij de stelling is, 'als het met geweld moet, dan moet het maar.' Zij worden weliswaar niet actief gesteund door de autoriteiten van A maar zeker ook niet tegengewerkt. Via diverse *on-line* fora wisselen ze ideeën voor acties uit en geven elkaar tips voor uitvoeringsmogelijkheden zonder dat hierbij sprake is van centrale sturing.

Situatie 1: Een fanatiek lid van groepering C, die eerder deelgenomen heeft aan acties van verzetsbeweging B, pleegt een aanslag gericht tegen een militair complex van A waarbij hijzelf en enkele militairen omkomen. In een afscheidsbrief, die later gevonden wordt, staat dat hij de aanslag namens groepering C pleegt. Dit heeft behoorlijke impact op het vertrouwen in de autoriteit van A, wat hierdoor afneemt.

Situatie 2: Aangemoedigd door het succes uit situatie 1 nemen andere leden van groepering C zich voor iets soortgelijks te ondernemen, maar omdat de militaire complexen inmiddels veel beter beveiligd worden, nemen ze hun toevlucht tot aanslagen op civiele objecten en personen.

Situatie 3: Door de toegenomen onrust groeit de actiebereidheid binnen de *on-line* groep D. Met malware die gedeeld is via een van de fora, lukt het een groepje hackers om een wapensysteem van verzetsbeweging B zo te beïnvloeden dat bij het eerstvolgende gebruik niet de geplande militaire doelen van A worden geraakt, maar onschuldige burgers.

Situatie 4: Via allerlei kanalen wordt de mislukte operatie van B uit situatie 3 door leden van D uitgebreid in de publiciteit gebracht, wat resulteert in een afname aan steun voor verzetsbeweging B.

Behoren bovenstaande situatiebeschrijvingen tot vijandelijkheden en zo ja, zijn het dan ook militaire operaties? In hedendaagse complexe gewapende conflicten, waarbij strijders soms in wisselende groeperingen allianties aangaan maar elkaar elders bestrijden, worden soms gewelddadige aanslagen gepleegd of acties ondernomen die feitelijk schade veroorzaken

aan personeel of materieel van een van de strijdende partijen. Daarbij kan onduidelijkheid ontstaan aan welke partij of coalitie de actie toegerekend moet worden, maar ook over de intentie van de aanslag of actie. Met dit laatste vervaagt de scheidslijn tussen vijandelijkheden en gewone misdaden. Bij de juridische kwalificatie is één ding echter duidelijk. Bij zowel ‘militaire operaties’ als bij ‘vijandelijkheden’ moet een nexus met het gewapende conflict bestaan. Bij ontbreken van (voldoende) nexus valt een actie niet onder het regime van het internationaal humanitair oorlogsrecht, waarbij opgemerkt moet worden dat *“it may task the skills of lawyers and judges to neatly compartmentalize crimes into discrete categories of those that are, and those that are not, linked to the NIAC [Non International Armed Conflict].”*¹⁹⁰

Om duidelijkheid te kunnen scheppen in de onderlinge relatie tussen de begrippen,¹⁹¹ zal ik een keuze moeten maken tussen de brede en de enge interpretatie van ‘vijandelijkheden’. Voor mij is doorslaggevend de manier waarop de term ‘vijandelijkheden’ in zowel gemeenschappelijk artikel 3 van de Verdragen van Genève als in Aanvullend Protocol I en II gebruikt wordt en dat is in de combinatie van ‘deelname aan vijandelijkheden’. Combattanten hebben het recht “rechtstreeks deel te nemen aan de vijandelijkheden”,¹⁹² terwijl burgers humanitair oorlogsrechtelijke bescherming genieten zolang zij niet “rechtstreeks aan de vijandelijkheden deelnemen.”¹⁹³ In beide gevallen is het duidelijk dat ‘vijandelijkheden’ hier op de beperkte manier uitgelegd moet worden. Het recht van combattanten om rechtstreeks deel te nemen aan vijandelijkheden verleent hen de bevoegdheid om iets te doen wat buiten het regime van het humanitair oorlogsrecht niet is toegestaan, namelijk het feitelijk schade toebrengen aan personeel of materieel van de vijandelijke strijdkrachten. Het zou onlogisch en overbodig zijn combattanten een recht te verlenen op iets wat niet verboden is, zoals bijvoorbeeld een eenheid verplaatsen of logistiek bevoorraden.

Bij burgers kan ik een gelijksoortige redenering opzetten. Burgers mogen niet rechtstreeks deelnemen aan de vijandelijkheden en zolang ze dit niet ook doen, genieten zij bescherming tegen aanvallen. Dit uitgangspunt is een van de kenmerkende doelstellingen van het humanitair oorlogsrecht, namelijk het beschermen van hen die niet (langer) rechtstreeks betrokken zijn bij een gewapend conflict.¹⁹⁴ Wanneer burgers wel direct deelnemen aan de vijandelijkheden,¹⁹⁵ verliezen ze hun bescherming. Dit is echter

190 Dinstein 2014, p. 15.

191 Zie par. 2.4.1.

192 Aanvullend Protocol I art. 43 (2).

193 Gemeenschappelijk art. 3 Verdragen van Genève, Aanvullend Protocol I artikel 51, lid 3, Aanvullend Protocol II art. 4.

194 Zie par. 2.2.1.

195 Met vijandelijkheden wordt bedoeld op “not only the time that the civilian actually makes use of a weapon, but also, for example the time that he is carrying it, as well as situations in which he undertakes hostile acts without using a weapon” Sandoz, Swinarski & Zimmermann 1987, p. 619. Zie ook de drie voorwaarden voor directe deelname aan vijandelijkheden geformuleerd in de *Interpretive guidance* 2009 die cumulatief vervuld moeten worden. Schadedrempel,: de daad van deelname beoogt een militair nadeel voor de tegenpartij of veroorzaakt dood, verwonding of vernietiging van personen en goederen beschermd door het internationaal humanitair oorlogsrecht; direct causaal verband, er moet een direct causaal verband zijn tussen de daad van deelname en de schade die hierdoor wordt veroorzaakt; doel, de daad van deelname moet erop gericht zijn om op directe wijze een militair nadeel voor de tegenpartij te berokkenen.

een uitzondering op de hoofdregel. Zeker gelet op de gevolgen van de uitzondering is het logisch deze uitzondering beperkt te houden en te kiezen voor de enge uitleg van ‘vijandelijkheden’. Een brede uitleg van de uitzondering betekent namelijk automatisch een zwakkere positie voor de hoofdregel.

Met bovenstaande algemene redenering wil ik geenszins aangeven dat daarmee ook de exacte betekenis van de term ‘directe deelname aan vijandelijkheden’ eenduidig vastligt. De discussies die hierover plaatsvinden¹⁹⁶ gaan echter niet over vijandelijkheden *sec* maar over ‘directe deelname aan vijandelijkheden’ dat bestaat uit twee componenten te weten ‘directe deelname’ en ‘vijandelijkheden’, die elkaar onderling beïnvloeden of anders gezegd *“on the one hand, one could combine a narrower definition of “hostilities” with a broader interpretation of “direct participation”. On the other hand, if the term “hostilities” was defined more broadly, then “direct participation” would have to be interpreted more narrowly.”*¹⁹⁷ Verschillende interpretaties van het begrip ‘vijandelijkheden’ blijven dus mogelijk. Voor dit onderzoek hoeft dit geen probleem te zijn omdat ik op zoek ben naar de regels uit het humanitair oorlogsrecht die gelden beneden de drempel van aanval. Aanval is in elk geval een deelverzameling van zowel ‘militaire operaties’ als van ‘vijandelijkheden’ ongeacht de brede of enge interpretatie van ‘vijandelijkheden’.

Mijn conclusie over de relatie tussen ‘militaire operaties’ en ‘vijandelijkheden’ is weergegeven in figuur 1. Militaire operaties, in de context van een gewapend conflict, en vijandelijkheden overlappen elkaar voor een aanzienlijk deel. Omdat ik kies voor de enge interpretatie van ‘vijandelijkheden’ is ‘militaire operaties’ het bredere begrip. Hiermee ben ik aangekomen bij de laatste en tevens kleinste deelverzameling binnen de onderlinge relaties van Figuur 1, namelijk ‘aanval’.

2.6 Aanvallen

Zoals eerder aangehaald in dit hoofdstuk luidt de letterlijke tekst van Aanvullend Protocol I artikel 49 lid 1, “ ‘aanvallen’ betekent daden van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve.”¹⁹⁸ Gelet op de hiervoor beschreven dubbele doelstelling van het humanitair oorlogsrecht en de manier waarop die bereikt wordt, namelijk door het vinden van een evenwicht tussen militaire noodzaak en humaniteit, is het logisch dat het humanitair oorlogsrecht in veel gevallen gericht is op (de gevolgen van) het daadwerkelijk uitvoeren van aanvallen. Dit zijn de situaties waarbij de aard van een gewapend conflict nadrukkelijk zichtbaar is: het met militair geweld opleggen van de eigen doelstellingen aan een tegenstander, waarbij het doden van mensen en het vernietigen van objecten vaak tot de harde realiteit behoren. Sterker nog, het humanitair oorlogsrecht verleent legitimiteit

¹⁹⁶ Bijvoorbeeld in het kader van de totstandkoming van de *Interpretive Guidance on the notion of Direct Participation in Hostilities*, zie oa DPH 2004, DPH 2005 en DPH 2006.

¹⁹⁷ DPH 2005, p. 20.

¹⁹⁸ Art. 49 lid 1 Aanvullend Protocol I.

aan deze realiteit, als het bij personen combattanten of strijders, of bij objecten militaire doelen betreft. Om te voorkomen dat deze legitimering misbruikt kan worden, waardoor het grondbeginsel van humaniteit onder druk zou komen te staan, is het begrip ‘aanval’, in tegenstelling tot de andere begrippen uit voorgaande paragrafen, in het humanitair oorlogsrecht *wel* gedefinieerd.

Alvorens in te gaan op de relatie van ‘aanval’ in de zin van artikel 49 lid 1 Aanvullend Protocol I en ‘militaire operaties’, zal ik eerst aandacht besteden aan twee elementen uit de definitie die in het verleden aanleiding zijn geweest voor discussie, namelijk ‘gericht tegen de tegenstander’ en ‘hetzij offensieve hetzij defensieve’. Vervolgens zal ik bespreken waarom militaire operaties een breder begrip is dan aanvallen en wat aanvallen onderscheidt van militaire operaties die geen aanvallen zijn. Als laatste formuleer ik het antwoord op de deelvraag van dit Hoofdstuk, waar ligt de ondergrens van ‘aanval’ uit artikel 49 lid 1 aanvullend protocol I in traditionele zin?

2.6.1 Gericht tegen de tegenstander

Dat een aanval gericht is tegen de tegenstander, is een bevestiging van de grondregel van onderscheid zoals geformuleerd in artikel 48 Aanvullend Protocol I, voorafgaand aan de definitie van aanval. Hierin staat omschreven dat de partijen bij het conflict te allen tijde onderscheid moeten maken tussen de burgerbevolking en combattanten en tussen burgerobjecten en militaire doelen. Zij dienen derhalve hun militaire operaties uitsluitend tegen militaire doelen te richten.¹⁹⁹ Oeter noemt het een poging het gewoonterechtelijke vereiste van onderscheid om te vormen tot een specifieke regel voor gevechtshandelingen, waarbij militair geweld alleen geoorloofd kan zijn tegen een militair doel en iets²⁰⁰ alleen een militair doel kan vormen als het daadwerkelijk bijdraagt aan de vijandelijke inspanningen.²⁰¹ De keerzijde van ditzelfde principe is namelijk dat als iets geen legitiem militair doel vormt, militair geweld niet toegepast mag worden en deze persoon of dit object daarmee dus bescherming geniet. Aanvallen en militair doelen, zowel personeel als materieel, worden hier nadrukkelijk aan elkaar gekoppeld.²⁰²

Bovenstaande betekent overigens niet dat daden van geweld die niet zijn gericht tegen een militair doel geen aanvallen zouden zijn. Ook daden van geweld tegen burgers of burgerobjecten vormen een aanval, maar ze zijn verboden en in strijd met het humanitair oorlogsrecht.

2.6.2 Hetzij defensieve hetzij offensieve

Het begrip aanval zoals gedefinieerd in artikel 49 lid 1 Aanvullend Protocol I heeft volgens sommige schrijvers een verkeerde betekenis gekregen. Zo geeft Hays Parks aan dat de “use

■
199 Aanvullend Protocol I art. 48.

200 lets verwijst hier naar objecten. Voor personen bepaalt de status of iemand wel of niet een legitiem doelwit van een aanval vormt.

201 Oeter (in Fleck) 2013a, p. 166.

202 Op de definitie van militair doel en de relatie met aanval kom ik in het volgende hoofdstuk terug.

of “attacks” to refer to acts of defense is etymologically inconsistent with its customary use in any of the six languages of Protocol I.”²⁰³ Hij doelt daarmee op het feit dat het begrip aanval, in militaire zin, normaal gesproken gebruikt wordt voor offensieve militaire operaties, waarbij de nadruk ligt op het element van initiatief, het initiëren van een actie.²⁰⁴ Zuiver defensieve operaties of reacties op aanvallen ook als aanval kwalificeren is in zijn optiek dan ook onjuist.

Voorgaande kritiek op de uitleg van het begrip ‘aanval’ wordt niet algemeen onderschreven,²⁰⁵ al wordt wel erkend dat “it is quite clear that the meaning given here [Additional Protocol I article 49] is not exactly the same as the usual meaning of the word.”²⁰⁶ Ik zal in dit onderzoek de bredere definitie van aanval volgen waarbij aanval gelijk staat aan combat action.²⁰⁷ Deze keuze is vanuit de doelstelling van het humanitair oorlogsrecht verdedigbaar, omdat zowel offensieve als defensieve acties implicaties voor de burgerbevolking én strijdende partijen (kunnen) hebben. Bijkomend voordeel is dat het “unmistakably brings home to commanders and soldiers in combat that the ‘defensive character’ of a specific act of violence does not exempt it from the provisions for the protection of the civilian population.”²⁰⁸

2.6.3 Waarom is militaire operatie een breder begrip dan aanval?

De definitie van aanval zoals gegeven in artikel 49 lid 1 Aanvullend Protocol I valt geheel binnen de beschrijving die ik hiervoor gaf van militaire operaties,²⁰⁹ zodat aanvallen in elk geval militaire operaties zijn. Maar waaruit volgt dat aanvallen en militaire operaties niet als synoniemen gebruikt kunnen worden binnen het humanitair oorlogsrecht?

Een eerste indicatie volgt impliciet uit het woordgebruik en de systematiek in deel IV, sectie 1 van Aanvullend Protocol I. De grondregel, als algeheel principe weergegeven in artikel 48, spreekt van operaties waarna vervolgens het begrip aanval wordt gedefinieerd in artikel 49. Ook op andere plaatsen in Aanvullend Protocol I wordt gesproken van bescherming tegen aanvallen of militaire operaties,²¹⁰ een woordgebruik dat niet verklaarbaar is als geen verschil tussen beide termen zou bestaan.

De constatering dat naast aanvallen ook andere vormen van militaire operaties mogelijk zijn, is ook terug te vinden in de ontstaansgeschiedenis van artikel 49 Aanvullend Protocol I, waarin de definitie van aanvallen uiteindelijk is vastgelegd. De discussie die plaatsvond

■
²⁰³Hays Parks 1990, p.114.

²⁰⁴Zo geeft bijvoorbeeld de Collins English Dictionary 2007 een aanval weer als “to launch a physical assault (against) with or without weapons: begin hostilities (with).”

²⁰⁵Zie bijvoorbeeld Oeter (in Fleck) 2013a, p. 166, “the critique is certainly exaggerated”, in dezelfde zin Rogers 2004, p. 28 “fails to follow Parks’s contention.”

²⁰⁶Sandoz, Swinarski & Zimmermann 1987, p. 603.

²⁰⁷Sandoz, Swinarski & Zimmermann 1987, p. 603. In gelijke bewoordingen Oeter (in Fleck) 2013a p.167.

²⁰⁸Oeter (in Fleck) 2013a, p. 167.

²⁰⁹Zie par. 2.5.3. Militaire operaties in de context van het humanitair oorlogsrecht zijn acties uitgevoerd door militairen en/of met militaire middelen om een specifieke militaire doelstelling te verwezenlijken. In het paradigma van ‘oorlogvoering’ is de militaire doelstelling gericht op het behalen van een militair voordeel ten opzichte van de tegenstander.

²¹⁰Zie bijvoorbeeld art. 43 lid 3, 51 lid 7 en art. 57 lid 1 en 2.

bij de totstandkoming van dit artikel ging over de vraag of gesproken moest worden van militaire operaties of aanvallen waarbij *“the former [is] being considered a more general term than the latter.”*²¹¹

Een ander voorbeeld van de bredere betekenis van militaire operatie is te vinden in artikel 51 lid 1 Aanvullend Protocol I waarin de burgerbevolking en de afzonderlijke burgers worden beschermd tegen uit militaire operaties voortvloeiende gevaren. De *Commentary* geeft aan dat militaire operaties slaan op “alle verplaatsingen en activiteiten van de krijgsmachten *gerelateerd* aan de vijandelijkheden.”²¹²

Als praktisch voorbeeld van een militaire operatie die geen aanval is noem ik hier het bezetten van een onverdedigde plaats. Volgens artikel 59 Aanvullend Protocol I is een onverdedigde plaats “een bewoonde plaats gelegen in de nabijheid van of in een zone, waar de strijdkrachten contact gemaakt hebben en welke gemakkelijk door een tegenpartij kan worden bezet.”²¹³ Een onverdedigde plaats mag niet aangevallen worden.²¹⁴ Indien de plaats echter door bijvoorbeeld de ligging of de aard een daadwerkelijke bijdrage tot de krijgsvrchtelingen levert en de verovering een duidelijk militair voordeel oplevert voldoet de plaats aan de definitie van militair doel.²¹⁵ Indien controle over de plaats het militaire doel van een eenheid is en bezetting mogelijk blijkt zonder gebruikmaking van vuurkracht of andere daden van geweld, dan kan de militaire operatie worden uitgevoerd zonder ‘aan te vallen’.²¹⁶

Nu ik hierboven geconcludeerd heb dat alle aanvallen militaire operaties, maar niet alle militaire operaties aanvallen zijn, rijst de vraag, wat onderscheidt een aanval van andere militaire operaties die geen aanval zijn? Het verschil zit in de zinsnede ‘daden van geweld’,²¹⁷ meer specifiek daden van geweld gericht tegen de tegenstander uit de definitie van Aanvullend Protocol I artikel 49 lid 1. Wat dient hieronder te worden verstaan?

Ik roep in herinnering dat de context van het humanitair oorlogsrecht het gewapend conflict is en dat ‘daden van geweld’ gelezen moet worden in deze context,²¹⁸ namelijk daden van militair geweldgebruik tijdens een gewapend conflict. Maar wat is dan militair geweldgebruik?

■
²¹¹ Levie 1980 volume 3, p.85. In dezelfde zin Oeter (in Fleck) 2013a, p. 166.

²¹² Sandoz, Swinarski & Zimmerman 1987, p. 617, mijn accentuering. Dezelfde bewoording wordt gebruikt bij de toelichting op art. 48, p. 600.

²¹³ Aanvullend Protocol I art. 52 lid 2.

²¹⁴ Aanvullend Protocol I art. 59 lid 1.

²¹⁵ Aanvullend Protocol I art. 52 lid 2.

²¹⁶ Het hier gegeven voorbeeld is beschreven in Bothe, Partch & Solf 1982 p. 285. Hier wordt ook nog gewezen op de vergelijking met art. 60 Aanvullend Protocol I handelend over gedemilitariseerde zones, waarin het partijen verboden wordt militaire operaties uit te voeren. Accentuering mijnerzijds.

²¹⁷ Zie bijvoorbeeld Dinstein 2016, p. 3. “Violence is a *condicio sine qua non* of attack.”

²¹⁸ Ingevolge artikel 31 van het Verdrag van Wenen dient als algemene regel van uitlegging van een verdrag gekeken te worden naar de gewone betekenis van de termen van het verdrag in hun context en in het licht van voorwerp en doel van het verdrag.

De term ‘daden van geweld’ duidt primair op fysiek geweld.²¹⁹ Door aanvallen gelijk te stellen met “*any combat action*”,²²⁰ wordt een verbinding gelegd met de fysieke component van geweld. Dit is ook af te leiden uit het taalgebruik elders in Aanvullend Protocol I, dat duidt op de fysieke gevolgen van de daden van geweld. Zo wordt in de zogenaamde (dis)proportionaliteitstest²²¹ gesproken van verlies van mensenlevens onder de burgerbevolking, verwonding van burgers of schade aan burgerobjecten. Dit betreft allemaal fysieke gevolgen. Artikel 57 Aanvullend Protocol I, handelend over voorzorgsmaatregelen bij aanvallen, gebruikt dezelfde taal.

De opvatting dat gekeken moet worden naar de fysieke uitwerking van daden van geweld wordt breder aangehangen. Dit blijkt bijvoorbeeld uit de discussie of het plaatsnemen van een (land)mijn een aanval in de zin van artikel 49 Aanvullend Protocol I is: “*The general feeling was that there is an attack whenever a person is directly endangered by a mine laid*”,²²² waarmee werd aangegeven dat pas sprake is van een aanval vanaf het moment dat gevaar voor de gevolgen van het plaatsnemen van de mijn ontstaat.²²³

Militaire acties zonder directe fysieke gevechtscomponent vallen buiten de definitie van aanval. Denk hierbij bijvoorbeeld aan het eerder aangehaalde innemen van een onverdedigde plaats zonder tegenstand wat geen schending van het aanvalsverbod oplevert,²²⁴ maar ook een verplaatsing van een militaire eenheid *sec* zal niet onder de definitie van aanval vallen.²²⁵ Andere voorbeelden zijn “*non-violent resource to psychological warfare; disruption of enemy communications, issuing false orders or using other ruses; sleep-depriving sonic booms; airdropping leaflets calling for surrender etc.*”²²⁶

Drie aanvullende opmerkingen over de fysieke gevolgen van geweld wil ik nog maken. Als eerste moet bij het optreden van fysiek letsel of schade de nuance worden aangebracht dat dit gevolg redelijkerwijs voorzienbaar moet zijn geweest. Ik bedoel hiermee dat indien schade ontstaat door een militaire operatie die weliswaar de schade niet als primaire doelstelling heeft, maar die wel redelijkerwijs is te voorzien, deze schade meegenomen moet worden bij de beoordeling of het wel of geen aanval is. Dit in tegenstelling tot het geval dat de schade ontstaan is door een ongeluk of een andere oorzaak van buitenaf die

219 Bothe, Partch & Solf 1982, p. 289.

220 Sandoz, Swinarski & Zimmermann 1987, p. 603, in gelijke bewoordingen Oeter (in Fleck) 2013a, p.167.

221 Zoals verwoord in bijvoorbeeld artikel 51 lid 5 (b) van aanvullend protocol I.

222 Sandoz, Swinarski & Zimmermann 1987, p. 603

223 In het kader van dit hoofdstuk over de ondergrens van artikel 49 in traditionele zin is deze conclusie niet omstreden. In het kader van *Computer Network Attacks* is er wel een debat ontstaan of ook zonder fysieke schade sprake kan zijn van een aanval. In het tweede deel van dit onderzoek zal ik op deze discussie (door sommigen aangemerkt als het Dörmann-Schmitt debat) terugkomen.

224 Zie par. 2.2.2.

225 Al is discussie mogelijk welke handelingen wel en welke niet bij een aanval horen. Zo worden in discussie over directe deelname aan vijandelijkheden de voorbereidingen op, evenals de terugkeer na afloop van een aanval gezien als directe deelname aan de vijandelijkheden. Of deze activiteiten daarmee ook onder de definitie van aanval vallen blijft onduidelijk.

226 Dinstein 2016, p. 3.

niet beïnvloedbaar of redelijkerwijs voorzienbaar was. Een voorbeeld hiervan zou kunnen zijn een militair vliegtuig dat wordt ingezet om pamfletten uit te gooien met als doel mensen te beïnvloeden (informatieoperatie) maar vervolgens neerstort door een niet voorziene motorstoring met slachtoffers en schade op de grond als gevolg.

Een tweede opmerking over de fysieke gevolgen van geweld is dat niet alle vormen van fysiek geweld onder de definitie van aanval gebracht kunnen worden. Dit heeft te maken met de beperking die ik in paragraaf 2.5.3 over militaire operaties in de context van het humanitair oorlogsrecht heb gemaakt. Het moet gaan om geweld gerelateerd aan het gewapend conflict, oftewel het moet gaan om *“acts of warfare involving the use of violent means: the term covers the rifle shot and the exploding bomb, not the act of taking someone prisoner (even though the latter may also involve the use of force).”*²²⁷ Alleen bij voldoende nexus met het gewapend conflict²²⁸ valt het geweldgebruik onder het humanitair oorlogsrecht en is sprake van een aanval in de zin van artikel 49 Aanvullend Protocol I.

De laatste opmerking betreft operaties die gericht zijn op fysieke effecten, maar vervolgens, om wat voor reden dan ook, niet daadwerkelijk tot de fysieke schade leiden. Deze kwalificeren ook als aanval. Een voorbeeld kan dit verduidelijken. Een combattant die zijn wapen afvuurt op een tegenstander pleegt een ‘aanval’, ook als hij het doel mist en verder geen schade veroorzaakt.

2.6.4 De ondergrens van aanval

De ondergrens van het begrip ‘aanval’ is de voorwaarde die een aanval onderscheidt van andere militaire operaties die geen aanval vormen. Als niet wordt voldaan aan deze voorwaarde is geen sprake van ‘aanval’, militaire operaties die wel aan deze voorwaarde voldoen zijn ‘aanvallen’ in traditionele zin.

Nu ik militaire operaties gedefinieerd heb als acties uitgevoerd door militairen en/of met militaire middelen om een specifieke militaire doelstelling te behalen en vastgesteld heb dat binnen het paradigma van ‘oorlogvoering’ de militaire doelstelling gericht is op het behalen van een militair voordeel ten opzichte van de tegenstander,²²⁹ kan aan de hand van de hierboven beschreven analyse de ondergrens van een aanval in traditionele zin worden gedefinieerd als: acties uitgevoerd met militairen en/of militaire middelen, die gericht zijn op fysiek letsel of schade of deze fysieke gevolgen hebben, welke in het kader van een gewapend conflict worden uitgevoerd met als doel een militair voordeel op de tegenstander te behalen.

■
227 Kalshoven & Zegveld 2011, p.100. Als het echter zou gaan om krijgsgevangen bestaat de nexus met het gewapend conflict weer wel.

228 Zie bijvoorbeeld Dinstein 2016, p. 3. *“Certain acts of violence, performed by organs of a Belligerent Party in the course of an IAC, are excluded from the range of hostilities. These acts, not related to military operations against the enemy, are especially apposite to law enforcement measures taken against common felons transgressing the domestic penal code.”*

229 Zie Hoofdstuk 2 par. 2.5.3.

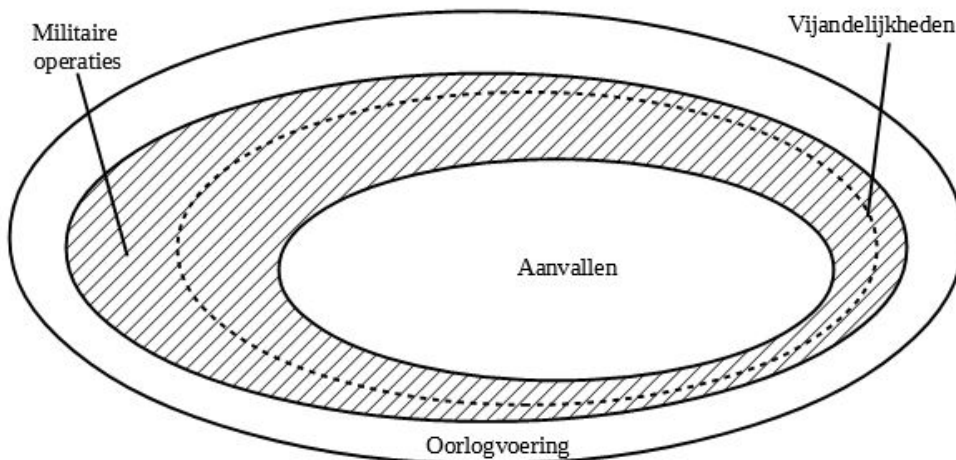
Na deze vaststelling van de ondergrens van een aanval kan ik nu overgaan naar de tweede deelvraag, welke regels gelden in het humanitair oorlogsrecht voor militaire operaties die de drempel van aanval niet halen?

3

Hoofdstuk 3 Regels uit het humanitair oorlogsrecht van toepassing op militaire operaties die de drempel van aanval niet halen

3.1 Inleiding

Het humanitair oorlogsrecht reguleert gewapende conflicten en is daarmee van toepassing op de hele situatie van gewapend conflict, waarbinnen een diversiteit aan militaire activiteiten plaatsvindt. Een deel van deze activiteiten is specifiek gedefinieerd als aanvallen. Dat is niet zo vreemd omdat een gewapend conflict naar zijn aard gaat om het met militair geweld opleggen van de eigen doelstellingen aan een tegenstander waarbij het doden van strijders en het vernietigen van militaire objecten vaak tot de harde realiteit behoren. Het gaat daarbij per definitie om aanvallen.¹ Toch reikt het humanitair oorlogsrecht verder en reguleert het ook andere activiteiten die plaatsvinden in het kader van een gewapend conflict. De deelvraag die centraal staat in dit hoofdstuk luidt: Welke regels zijn van toepassing op de militaire operaties binnen een gewapend conflict die niet vallen onder de definitie van aanval? Schematisch is dit aan te duiden als het gearceerde gebied in figuur 3.²



Figuur 3 Toepassingsgebied van humanitair oorlogsrecht beneden de drempel van aanval.

Omdat de centrale vraag van dit onderzoek gaat over de regels van het humanitair oorlogsrecht beneden de grens van aanval in het cyberdomein is het antwoord op de deelvraag uit dit hoofdstuk vooral van belang om te dienen als referentiepunt voor de beantwoording van de onderzoeksvragen in het tweede deel van dit onderzoek. Het is

-
- 1 Per definitie gebruik ik hier in de letterlijke zin van art 49 lid 1 Aanvullend Protocol I "aanvallen betekent: daden van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve".
- 2 Voor het verschil tussen militaire operaties en vijandelijkheden verwijs ik naar het vorige hoofdstuk. De nadruk zal liggen op militaire operaties en alleen indien dit noodzakelijk is, zal ik aandacht besteden aan vijandelijkheden.

daarom niet nodig om tot een uitputtende, opsommende lijst van toepasselijke regels te komen. Net als bij het bepalen van de balans tussen militaire noodzaak en humaniteit³ kan op verschillende niveaus naar de centrale vraag van dit hoofdstuk gekeken worden. Dit kan op het niveau van de individuele regels, maar ook op een hoger abstractieniveau. Zoals al aangegeven in Hoofdstuk 1, neem ik als uitgangspunt een hoger abstractieniveau, namelijk de grondbeginselen van het humanitair oorlogsrecht. Deze benaderingswijze is verdedigbaar omdat de grondbeginselen van het humanitair oorlogsrecht gezien worden als “door beschaafde naties erkende algemene rechtsbeginselen”⁴ die een rechtsbron voor internationaal recht vormen.⁵ Deze grondbeginselen vormen het normatieve kader waarop het gehele systeem van regels is gebaseerd.⁶ Veel regels, zowel de regels uit het internationaal gewoonterecht, als die vastgelegd in verdragen, vinden hun basis in deze grondbeginselen.⁷ Daarmee is de rol van de grondbeginselen nog niet uitgespeeld. Ook nu nog, *“after more than a century of international codification of specific prohibitions, law-of-war principles still perform critical regulatory functions in combat.”*⁸

Omdat het internationaal gewoonterecht naast het verdragenrecht, als belangrijke bron voor het internationaal recht geldt, zal ik in paragraaf 3.2 eerst enkele woorden aan het internationaal gewoonterecht wijden. Vervolgens zal ik in paragraaf 3.3 de grondbeginselen van het humanitair oorlogsrecht bespreken en daarbij beoordelen of, en zo ja, in welke mate, ze ook van toepassing zijn op militaire operaties beneden de drempel van aanval. Tot slot kan ik dan, in paragraaf 3.4, een antwoord formuleren op de deelvraag uit dit hoofdstuk. Dit zal zijn aan de hand van de grondbeginselen die van toepassing zijn op militaire operaties binnen het humanitair oorlogsrecht die de drempel van aanval niet halen.

3.2 Gewoonterecht als bron van humanitair oorlogsrecht

In de vorige paragraaf heb ik aangegeven dat vrijwel alle regels van het humanitair oorlogsrecht hun basis hebben in de grondbeginselen.⁹ Die grondbeginselen vormen als het ware het fundament waarop het *corpus* van het humanitair oorlogsrecht rust. Dit *corpus* wordt gevormd door de regels van internationaal gewoonterecht en verdragenrecht. Hierin verschilt humanitair oorlogsrecht niet van andere takken van internationaal recht. Zo worden verdragen en gewoonterecht als eerste genoemd worden in artikel 38 van het

3 Zie Hoofdstuk 2 par. 2.3.2.

4 Statuut van het Internationaal Gerechtshof art 38 lid 1c.

5 Bothe, Partch & Solf 2013, p. 43 “*They are general principles of in the sense of Art. 38 of the Statute of the ICJ*”

6 Gill (in Matthee, Toebes & Brus) 2013, p. 40.

7 ICRC 2013, p. 54.

8 Watts 2014, p. 121.

9 De verplichting om zorg te dragen voor juridische adviseurs in de strijdkrachten en de verplichting tot het verspreiden van kennis over het humanitair oorlogsrecht (respectievelijk art. 82 en 83 Aanvullend Protocol I) zijn mogelijk voorbeelden van regels die niet berusten op de grondbeginselen.

Statuut van het Internationaal Gerechtshof.¹⁰ Dit artikel wordt bij het ontbreken van een document dat gezaghebbend de internationale rechtsbronnen benoemt¹¹ in het algemeen wel als zodanig gezien, zij het dat de daar genoemde opsomming niet uitputtend is.¹²

Internationaal gewoonterecht bestaat zodra sprake is van een “internationale gewoonte, als blijk van een als recht aanvaarde algemene praktijk.”¹³ Deze omschrijving bevat twee elementen. Ten eerste het objectieve element van (algemene) statenpraktijk en ten tweede het subjectieve element van “als recht aanvaard”,¹⁴ veelal weergegeven met de Latijnse term *opinio juris sive necessitatis* of kortweg *opinio juris*.

De exacte betekenis en inhoud van deze twee elementen is al geruime tijd onderwerp van veel academische verhandelingen,¹⁵ terwijl ook over de verhouding en wisselwerking tussen internationaal gewoonterecht en verdragenrecht het nodige is geschreven.¹⁶ Zo zijn de meeste regels over de uitvoering van vijandelijkheden over een periode van decennia verworpen tot internationaal gewoonterecht,¹⁷ terwijl veel van deze regels inmiddels ook zijn opgenomen in verdragen. Soms wordt een verdrag in zijn geheel gezien als internationaal gewoonterecht¹⁸ maar het is niet zo dat de ene bron ter vervanging van de andere kan dienen. Verdragenrecht en gewoonterecht bestaan naast elkaar en vullen elkaar aan, zoals bijvoorbeeld blijkt uit de Martens clause, zoals die onder andere is opgenomen in Aanvullend Protocol I. Hierin is aangegeven dat bij gebrek aan internationale overeenkomsten burgers en combattanten beschermd worden door en onderworpen zijn aan de beginselen van het volkenrecht die voortvloeien uit het gewoonterecht, de beginselen van menselijkheid en de eisen van het openbaar rechtsbewustzijn.¹⁹

Voor dit onderzoek is het van belang dat met betrekking tot het humanitair oorlogsrecht internationaal gewoonterecht en verdragenrecht naast elkaar bestaan, maar gestoeld zijn op dezelfde grondbeginselen. Wat deze grondbeginselen zijn is onderwerp van de volgende paragraaf.

10 Statuut van het Internationaal Gerechtshof art 38 lid 1 sub a tot en met d noemt naast verdragen en internationale gewoonte, algemene rechtsbeginselen en, onder voorwaarden, rechterlijke beslissingen en opvattingen van de meest bevoegde schrijvers als rechtsbronnen voor internationaal recht.

11 Wolfrum 2011, p. 3. Thirlway (in Evans) 2010, p. 97.

12 Gill & Fleck 2012, p. 8.

13 Statuut van het Internationaal Gerechtshof art. 38 lid 1b.

14 ILC 2016 p 76, *Conclusion 2: Two constituent elements*.

15 Een samenvatting voor het humanitair oorlogsrecht is te vinden in Henckarts & Doswald-Beck, 2005 p. xxv-xlv.

16 Zie bijvoorbeeld ILA 2000, pp 754-765 of CAVV 2017, p. 11 “De verhouding tussen verdragen en internationaal gewoonterecht blijft evenwel zeer gecompliceerd”, welk standpunt werd gedeeld door de Nederlandse regering, Kamerstukken II 2017-2018, 34775-V nr. 51.

17 Dinstein 2004, p. 5

18 Zo werd bijv. de *Hague Convention of 1907* tijdens de 1946 *Nuremberg judgement* gezien als internationaal gewoonterecht, “these rules laid down in the convention were recognized by all civilized nations, and were regarded as being declaratory of the laws and customs of war.”

19 Aanvullend Protocol I art 1 lid 2.

3.3 Grondbeginselen van het humanitair oorlogsrecht

In het vorige hoofdstuk schreef ik dat veel regels uit het humanitair oorlogsrecht gebaseerd zijn op een balans tussen de twee grondbeginselen militaire noodzaak en humaniteit.²⁰ Deze worden ook wel aangeduid als de grondbeginselen op het hoogste, algemene niveau.²¹ Op een lager niveau bestaan nog meer grondbeginselen, waarbij de aanduiding van een lager niveau niet slaat op het belang van het betreffende grondbeginsel maar een aanduiding is voor het feit dat het een beginsel is dat medebepalend is voor de uitwerking van het grondbeginsel militaire noodzaak of humaniteit op het meest algemene niveau.²²

In Aanvullend Protocol I staat een aantal 'grondregels' (*basic rules*) genoemd.²³ Deze hebben weliswaar een overlap met de grondbeginselen, maar zijn feitelijk een uitwerking van die beginselen. In andere verdragen wordt nergens een opsomming gegeven van de grondbeginselen, zodat ik ervoor kies om uit te wijken naar militaire handleidingen en operationele handboeken. Deze laatste bekleden binnen het humanitair oorlogsrecht een bijzondere positie.²⁴ Militaire handleidingen kunnen gezien worden als een indicatie voor 'statenpraktijk' en *opinio juris* van de staat die de handleiding uitgeeft,²⁵ terwijl operationele handboeken vaak bedoeld zijn ter bevordering en ontwikkeling van internationaal recht,²⁶ zodat ze bij gebrek aan vermelding in verdragen als alternatief kunnen dienen voor het vinden van de grondbeginselen van het humanitair oorlogsrecht.

■
20 Zie Hoofdstuk 2, par. 2.3.

21 Kolb & Hyde, p. 43.

22 Een voorbeeld van een schematische weergave van grondbeginselen op het hoogste algemene niveau met daaronder een 'lager' grondbeginsel is te vinden in Ducheine & Pouw 2010, p. 99.

23 Aanvullend Protocol I art 35 over methoden en middelen van oorlogvoering en art. 48 over de bescherming van de burgerbevolking.

24 Dinstein 2004, p. 6.

25 Voor kritiek op de zienswijze dat militaire handboeken bewijs van statenpraktijk opleveren, zie bijv. Arajärvi 2014, p. 20.

26 Garraway (in Hayashi) 2010, p. 46.

Kijkend naar handboeken en handleidingen kies ik als grondbeginselen:

- militaire noodzaak (military necessity);²⁷
- humaniteit (humanity);²⁸
- onderscheid (distinction);²⁹
- proportionaliteit (proportionality);³⁰
- eervol gedrag (chivalry).³¹

Andere indelingen of uitbreidingen zijn mogelijk.³² Het verschil in indeling wordt ingegeven door het standpunt dat wordt ingenomen bij de vraag of een bepaald beginsel een zelfstandig grondbeginsel is (bijvoorbeeld eervol gedrag) of dat het onderdeel uitmaakt van een ander grondbeginsel (bijvoorbeeld ‘overbodig letsel en onnodig leed’ als onderdeel van humaniteit en militaire noodzaak, of voorzorgsmaatregelen als onderdeel van onderscheid en proportionaliteit). In de bespreking van de grondbeginselen zoals ik ze hier heb weergegeven zal ik ook, daar waar nodig, andere beginselen terug laten komen.

3.3.1 Militaire noodzaak

In het vorige hoofdstuk heb ik aangegeven dat bij elke aanval sprake moet zijn van militaire noodzaak om een aanval te kunnen legitimeren.³³ Dat staten beperkt zijn in hun keuze van methoden en middelen van oorlogvoering is bijvoorbeeld mede gebaseerd op het gewoonterechtelijke principe dat elke vorm en elke daad van oorlogvoering geleid moet worden door de vereisten van militaire noodzaak.³⁴ Maar hoe zit het met militaire operaties

27 O.a. UK *Manual JSP 383* ed. 2004, p. 21 en 23, DoD *Law of War Manual* 2016, p. 50, Canadian *LOAC Manual* 2001, p. 2-1, Handleiding militair oorlogsrecht 2005, p. 163, ICRC *Handbook on International rules governing military operations* 2013, p. 53, Rogers 2004, p. 3, Watts 2014, p. 121.

28 O.a. UK *Manual JSP 383* ed. 2004, p. 21 resp 23, DoD *Law of War Manual* 2016, p. 50, Canadian *LOAC Manual* 2001, p. 2-1, Handleiding militair oorlogsrecht 2005, p. 163, ICRC *Handbook on International rules governing military operations* 2013, p. 53, Rogers 2004, p. 3, Watts 2014, p. 121.

29 O.a. UK *Manual JSP 383* ed. 2004 p. 24, DoD *Law of War Manual* 2016, p. 50, Canadian *LOAC Manual* 2001, p. 2-2, Handleiding militair oorlogsrecht 2005, p. 163, ICRC *Handbook on International rules governing military operations* 2013, p. 53, Rogers 2004, p. 3, Watts 2014, p. 121.

30 O.a. UK *Manual JSP 383* ed. 2004 p. 24, DoD *Law of War Manual* 2016, p. 50, Canadian *LOAC Manual* 2001, p. 2-2, Handleiding militair oorlogsrecht 2005, p. 163, ICRC *Handbook on International rules governing military operations* 2013, p. 53, Rogers 2004, p. 3, Watts 2014, p. 121.

31 *US-Operational law Handbook* ed. 2014 p.14. In de DoD *Law of War Manual* 2016, p. 50 benoemd als “Honor”, Canadian *LOAC Manual* 2001, p. 2-1, Handleiding militair oorlogsrecht 2005, p. 163.

32 Naast de hierboven vermelde grondbeginselen vermeldt het *US-Operational law Handbook* ed 2014, p.14 nog onnodig leed (*unnecessary suffering*) en het ICRC *Handbook on International rules governing military operations* (2013) voorzorgen (*precautions*) en beperking (*limitation*) als grondbeginselen. Het ICJ noemt onderscheid en het verbod op onnodig leed bij combattanten als essentiële principes (*cardinal principles*), *advisory opinion on the threat or use of nuclear weapons* (1996), par. 78.

33 Zie Hoofdstuk 2 par. 2.3.3.

34 Fleck 2013b, p. 122

beneden de drempel van aanval? Al in de *St Petersburg Declaration* is opgenomen dat het enige legitieme doel van een gewapend conflict “het verzwakken van de tegenstander is”,³⁵ waarmee wordt aangegeven dat alle militaire operaties in een gewapend conflict een militaire noodzaak moeten hebben om legitiem te kunnen zijn.

Een moderne versie is terug te vinden in artikel 48 Aanvullend Protocol I dat luidt: “Ten einde te verzekeren, dat de burgerbevolking en de burgerobjecten worden ontzien en beschermd, dienen de partijen bij het conflict te allen tijde onderscheid te maken tussen de burgerbevolking en combattanten en tussen burgerobjecten en militaire doelen en dienen derhalve *hun operaties uitsluitend tegen militaire doelen te richten*.”³⁶ Militaire doelen, zowel ‘strijders’ als militaire objecten, kwamen in het vorige hoofdstuk al kort aan de orde, wat leidde tot de conclusie dat militaire noodzaak aanwezig moet zijn om een aanval te kunnen legitimeren.³⁷ Artikel 48, dat de grondregel van de algemene bescherming tegen de gevolgen van vijandelijkheden vastlegt, gaat echter verder door te spreken van ‘operaties’ en zoals ik in het vorige hoofdstuk heb aangegeven, dient dit gelezen te worden als militaire operaties. De *Commentary* geeft aan dat met operaties bedoeld wordt op “*military operations during which violence is used, and not to ideological, political or religious campaigns*”³⁸ waarbij operaties “*refers to all movements and acts related to hostilities that are undertaken by armed forces*”,³⁹ wat duidelijk verder gaat dan alleen ‘aanvallen’.

Aanvullend Protocol I definieert in artikel 52 lid 2 militaire doelen⁴⁰: “voor zover het objecten betreft, zijn militaire doelen uitsluitend die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment *een duidelijk militair voordeel oplevert*.”⁴¹ Zoals ik in Hoofdstuk 2 al concludeerde, bestaat er geen militaire noodzaak als geen duidelijk militair voordeel is te behalen.⁴² Artikel 52 Aanvullend Protocol I is geschreven in de vorm van een verbod op aanvallen op burgerobjecten. Burgerobjecten zijn alle objecten die niet aan de hiervoor gegeven definitie van artikel 52 lid 2 voldoen. De definitie van militair doelen geldt echter breder. Volgens de *Commentary* moet de definitie worden gebruikt “*to apply the basic rule in Article 48*”.⁴³ Omdat artikel 48 gaat over het bredere begrip ‘operaties’ zal dus bij alle

35 St Petersburg Declaration, 1868, Preamble; *That the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy*

36 Aanvullend Protocol I art. 48, mijn accentuering.

37 Zie Hoofdstuk 2 par. 2.3.3.

38 Sandoz, Swinarski & Zimmerman 1987, p. 600.

39 Sandoz, Swinarski & Zimmerman 1987, p. 600, mijn accentuering.

40 Militaire doelen kunnen zowel personen als objecten behelzen. Art 52 Aanvullend Protocol I definieert alleen objecten. Voor personen bepaalt de status of zij een legitiem militair doel vormen.

41 Aanvullend Protocol I art. 52 (2), mijn accentuering.

42 Zie Hoofdstuk 2 par. 2.3.3 voor de uitwerking van de proportionaliteitsregel.

43 Sandoz, Swinarski & Zimmerman 1987, p. 630.

militaire operaties sprake moeten zijn van een te behalen militair voordeel oftewel een militaire noodzaak.⁴⁴

In het vorige hoofdstuk heb ik al een aantal militaire operaties genoemd die zeker als ‘acties gerelateerd aan de vijandelijkheden’ gelden.⁴⁵ Ook voor deze acties geldt dat ze legitiem zijn, zolang ze gericht zijn op ‘het verzwakken van de tegenstander’,⁴⁶ met andere woorden er is een militair voordeel te behalen op de tegenstander. Ik kan daarmee concluderen dat militaire noodzaak een vereiste is voor alle militaire operaties, ook die beneden de drempel van aanval.

Overigens is niet iedereen ervan overtuigd dat binnen het humanitair oorlogsrecht militaire noodzaak aanwezig moet zijn om een militaire operatie te rechtvaardigen. Hayashi beargumenteert dat militaire noodzaak “*normative[ly] indifferent*” is.⁴⁷ Hij doelt hiermee op het feit dat het humanitair oorlogsrecht geen verplichting oplegt om militair noodzakelijke acties uit te voeren, maar ervoor zorgt dat ze toegestaan zijn. Een voorbeeld kan dit verduidelijken. Stel dat een vijandelijke colonne oprukt in de richting van eigen troepen, waarbij ze een brug naderen. Om de opmars te stuiten kan de brug vernietigd worden waarmee de colonne tot staan gebracht wordt. Het te behalen militaire voordeel is hier overduidelijk aanwezig. Toch bestaat op basis van het humanitair oorlogsrecht geen verplichting om de brug ook daadwerkelijk te vernietigen, het staat ‘slechts’ toe. Tegelijkertijd geeft het humanitair oorlogsrecht geen verbod op militair onnodige acties, het staat het niet uitvoeren ervan toe, maar tolereert ook het uitvoeren van acties die onnodig zijn.⁴⁸ Anders gezegd, “*military necessity can be seen essentially as an amoral notion that merely separates competent fighting from incompetent fighting.*”⁴⁹ Tegelijkertijd stelt hij ook vast dat “*it is in one’s strictly strategic self-interest to perform an act to the extent that it is materially conducive to success. Second, it is similarly in one’s strictly strategic self-interest to refrain from an act to the extent that it is not so conducive.*” In zijn visie zal een partij bij een gewapend conflict zich focussen op het uitvoeren van militair noodzakelijke operaties en onnodige operaties vermijden. Dit is echter niet op basis van het humanitair oorlogsrecht, maar uit eigenbelang. Militair noodzakelijk of onnodig wordt daarbij bepaald door de (non)bijdrage die een operatie levert aan het gewenste einddoel.⁵⁰

Bovenstaande redenering van Hayashi over militaire noodzaak gaat mijns inziens niet op voor aanvallen. In de definitie van objecten als militair doel, zoals gegeven in artikel 52 Aanvullend Protocol I zit militaire noodzaak opgesloten. Militaire doelen, voor

44 Op de vraag of het te behalen militaire voordeel bij militaire operaties beneden de drempel van aanval hetzelfde moet zijn als bij aanval, kom ik in Hoofdstuk 5 terug.

45 Zie Hoofdstuk 2 par. 2.6.3.

46 St Petersburg Declaration, 1868, Preamble; “*That the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy.*”

47 Hayashi 2017, p. 103.

48 Hayashi 2017, p. 103.

49 Hayashi 2017, p. 27.

50 Hayashi 2017, p. 27.

zover het objecten betreft, mogen namelijk alleen aangevallen worden indien onder de omstandigheden van dat moment een duidelijk militair voordeel te behalen is door vernietiging, verovering of onbruikbaarmaking van dat object. Is dat voordeel niet te behalen is er geen militaire noodzaak en mag het object niet aangevallen worden.

Dit ligt anders bij een militaire operatie beneden de drempel van aanval. Als deze militaire operatie geen effecten heeft op de burgerbevolking of burgerobjecten stelt het humanitair oorlogsrecht inderdaad geen eisen aan militaire noodzaak en zou een operatie ook onnodig kunnen zijn zonder in conflict te komen met het humanitair oorlogsrecht. Indien een militaire commandant besluit om zijn eenheid van A naar B te verplaatsen zonder dat dit militair noodzakelijk is, is dit niet verboden. Zodra echter burgers of burgerobjecten negatief beïnvloed worden, bijvoorbeeld omdat voor de verplaatsing van de eenheid van A naar B een gebied tijdelijk voor alle andere civiele verkeer wordt afgesloten, gaat het gewoonterechtelijke principe van onderscheid⁵¹ meewegen. Militaire noodzaak moet dan wel aanwezig zijn in de zin dat het te behalen militaire voordeel op moet wegen tegen de negatieve invloed van de operatie op burgers of burgerobjecten.⁵² Hoe dit in de praktijk vorm kan krijgen komt in Hoofdstuk 5 aan de orde.

Als gevolg van bovenstaande redenering moet ik de nuance aanbrengen dat militaire noodzaak alleen aanwezig moet zijn in de situaties waarin militaire noodzaak en humaniteit als grondbeginselen met elkaar in balans gebracht moeten worden, met andere woorden, alleen bij situaties waar een afweging op basis van militaire noodzaak of humaniteit alléén tot verschillende uitkomsten zou leiden⁵³ en, op basis van het grondbeginsel van onderscheid, negatieve gevolgen voor burgers of burgerobjecten voorzienbaar zijn. Indien niet aan deze voorwaarden is voldaan laat het humanitair oorlogsrecht een militaire operatie die geen militaire noodzaak heeft toe.⁵⁴

3.3.2 Humaniteit

Zoals eerder aangegeven zijn veel regels uit het humanitair oorlogsrecht terug te voeren op een balans tussen militaire noodzaak en humaniteit.⁵⁵ Daarom is het grondbeginsel van humaniteit terug te vinden in vrijwel alle delen van het humanitair oorlogsrecht en ook in beide delen van de dubbele doelstelling zoals beschreven in het vorige hoofdstuk.

Bij het reguleren, en soms beperken, van de vijandelijkheden is humaniteit bijvoorbeeld terug te vinden in de regel dat de keuzemogelijkheid voor methoden en middelen

■
51 Henckaerts & Doswald-Beck, 2005 *Black letter rule* 1 tot en met 13.

52 In dezelfde zin DoD Law of War Manual 2016 p. 59 2.3.1.1 "Humanity is related to military necessity, and these principles logically complement one another. Humanity may be viewed as the logical inverse of the principle of military necessity. If certain necessary actions are justified, then certain unnecessary actions are prohibited."

53 Zie Hoofdstuk 2 par. 2.2.2.

54 Vanuit militair oogpunt beschouwd is het overigens onlogisch en oneconomisch om militair onnodige operaties uit te voeren, maar het is niet verboden op basis van het humanitair oorlogsrecht.

55 Hoofdstuk 2 par. 2.3.1.

van oorlogvoering die partijen bij een conflict hebben, niet onbeperkt is.⁵⁶ Ook in de andere doelstelling, de bescherming van slachtoffers van gewapende conflicten, is het grondbeginsel van humaniteit alom vertegenwoordigd. Het ligt ten grondslag aan het beginsel van onderscheid waarbij burgers en burgerobjecten gevrijwaard dienen te blijven van aanvallen. Ook de bescherming van gewonden en gevangengenomen combattanten is gebaseerd op het beginsel van humaniteit.

Kortom, humaniteit als grondbeginsel is terug te vinden in vrijwel het gehele humanitair oorlogsrecht en is daarmee van toepassing op het hele spectrum van militaire operaties, ook die beneden de drempel van aanval. Hoe dit uitpakt wordt ingevuld door de toepassing van de andere grondbeginselen zodat bij de bespreking van die andere grondbeginselen humaniteit als vanzelf wordt meegenomen. Eén beginsel direct voortvloeiend uit het grondbeginsel van humaniteit wil ik hier echter nog onder de loep nemen, namelijk het beginsel van beperking⁵⁷ dat concretisering krijgt in twee regels, de regel dat de keuze van middelen en methoden van oorlogvoering niet onbegrensd is en de regel dat het veroorzaken van overbodig letsel en onnodig leed verboden is.

3.3.2.1 De keuze van middelen en methoden van oorlogvoering is niet onbegrensd

Het grondbeginsel van humaniteit in het oorlogsrecht ligt ten grondslag aan de overtuiging dat, in weerwil van het gezegde,⁵⁸ in oorlog niet alles geoorloofd is. Een principe dat teruggaat tot Grotius in zijn werk uit 1625, *'De iure belli ac pacis'*.⁵⁹ Dat het humanitair oorlogsrecht legitieme oorlogvoering begrenst, is onder andere vastgelegd in Aanvullend Protocol I: "In geen enkel gewapend conflict is het recht van de partijen bij het conflict ten aanzien van de keuze der methoden of middelen van oorlogvoering onbegrensd."⁶⁰

Eerder gaf ik al aan dat (extreme) nood geen reden kan zijn om een oorlogsrechtelijke regel te breken.⁶¹ Het principe van beperking was al gecodificeerd in het Haags Verdrag IV, zij het dat hier alleen gesproken werd over 'middelen'.⁶² Het is voor dit onderzoek niet noodzakelijk de hele ontwikkeling die heeft geleid tot de bovenstaande tekst van artikel 35 Aanvullend Protocol I te beschrijven,⁶³ echter drie zaken zijn relevant om te noemen.

Als eerste is het relevant te kijken naar de positie van deze regel in Aanvullend Protocol I, namelijk direct aan het begin van deel III handelend over methoden en middelen van

56 Deze regel is (onder andere) gecodificeerd in artikel 35 lid 1 van Aanvullend Protocol I en eerder ook al in artikel 22 van het *Hague convention IV* 1907.

57 Door het ICRC eveneens aangemerkt als een grondbeginsel, *ICRC Handbook on International rules governing military operations* 2013, p. 53.

58 Het aan Cicero toegeschreven klassieke *Inter arma silent leges* moet daarmee als cynisch worden verworpen.

59 Sandoz, Swinarski & Zimmermann 1987, p. 390.

60 Aanvullend Protocol I, art 35 lid 1.

61 Sandoz, Swinarski & Zimmermann 1987, p. 391.

62 Hague Convention IV 1907, artikel 22: "De oorlogvoerenden hebben geen onbegrensd recht ten aanzien van de keuze der middelen om de vijand te benadelen."

63 Voor een uitgebreide beschrijving van deze ontwikkeling zie Levie 1980, p. 252-280.

oorlogvoering. Een drietal zaken onderstreept het belang dat werd gehecht aan deze regel. Beginnen met deze regel is een eerste indicatie. Een tweede indicatie is dat de regel is weergegeven als een ‘grondregel’ (*basic rule*) refererend aan het niet te overschatten belang van dit principe.⁶⁴ Als laatste vormt ook het feit dat de regel is vastgelegd in een separaat artikel een weerspiegeling van het belang dat eraan werd gehecht.⁶⁵

Een tweede opmerking over methoden en middelen betreft het gebruik van het woord ‘oorlogvoering’ (*warfare*) in plaats van ‘gevechtshandelingen’ (*combat*) dat gebruikt werd in een eerdere, door het *International Committee of the Red Cross* voorgestelde, conceptversie van Aanvullend Protocol I in zowel de titel van sectie 1 als in artikel 35. Uit de discussies gevoerd tijdens de totstandkoming van Aanvullend Protocol I blijkt dat bewust is gekozen voor de term ‘oorlogvoering’ omdat “*combat might be construed more narrowly than warfare*.”⁶⁶ De beperkingen vervat in dit artikel zijn “*obviously intended to have wider application [than methods and means of combat]*.”⁶⁷ Zoals ik hiervoor al heb aangegeven is oorlogvoering de meest omvattende term waarop het humanitair oorlogsrecht van kracht is,⁶⁸ zodat ik kan concluderen dat de beperking, zoals weergegeven in deze ‘grondregel’, geldt voor alle methoden en middelen van oorlogvoering en daarmee ook voor niet-gevechtshandelingen zoals bijvoorbeeld psychologische of informatie operaties.

Als derde is het relevant dat het principe niet beperkt is tot middelen, lees met name wapens, maar ook van toepassing is op methoden van oorlogvoering.⁶⁹ Dit houdt onder meer in dat niet alleen naar een wapen sec gekeken moet worden, maar ook naar de manier van inzet en wijze van opereren. Beide kunnen onrechtmatig zijn⁷⁰ en daarmee in strijd zijn met deze ‘grondregel’. Een voorbeeld van het eerste is het gebruik van vergif of vergiftigde wapens.⁷¹ Een voorbeeld van het tweede zijn landmijnen. Deze zijn niet per definitie in strijd met het humanitair oorlogsrecht. Als landmijnen gebruikt worden als middel om een vijandelijke opmars te vertragen, te verhinderen of te vernietigen is dit niet in strijd met het humanitair oorlogsrecht. Als daarentegen een mijnenveld wordt aangelegd op een plaats waar mogelijk ook burgers komen terwijl het mijnenveld ook nog verborgen wordt, dan zal de manier van inzet in strijd kunnen zijn met het principe van onderscheid (waarover later meer⁷²).

Uit de plaats van en het woordgebruik in deze regel kan ik concluderen dat het beginsel van beperking in de middelen en methoden van oorlogvoering algemene gelding binnen het

64 Sandoz, Swinarski & Zimmermann 1987, p. 390. “*The necessity of reaching complete agreement on this essential basic principle before any attempt could be made at formulating specific regulations was obvious.*”

65 Sandoz, Swinarski & Zimmermann 1987, p. 390.

66 Sandoz, Swinarski & Zimmermann 1987, p. 398.

67 Bothe, Partsch & Solf p. 193.

68 Zie Hoofdstuk 2 par. 2.4.2.

69 Sandoz, Swinarski & Zimmermann 1987, p. 621 “*The term “means of warfare” generally refers to the weapons being used, while the expression “methods of warfare” generally refers to the way in which such weapons are used.*”

70 Sandoz, Swinarski & Zimmermann 1987, p. 398.

71 Hague Convention IV 1907, article 23 (a).

72 Hoofdstuk 3 par 3.3.3.

humanitair oorlogsrecht heeft en derhalve ook van kracht is op militaire operaties beneden de drempel van aanval.⁷³

3.3.2.2 Veroorzaken van overbodig letsel of onnodig leed is verboden

Zoals gesteld is de keuze in middelen en methoden van oorlogvoering niet onbeperkt. Soms wordt de keuze beperkt in de vorm van een verbod op een concreet soort wapens, gecodificeerd in een verdrag zoals het Conventionele Wapens Verdrag.⁷⁴ Vaker echter zal de keuze beperkt worden door een algemene beperking, namelijk dat geen overbodig letsel of onnodig leed veroorzaakt mag worden.⁷⁵

Voor dit onderzoek is het van belang te constateren dat deze beperking betrekking heeft op middelen en methoden van oorlogvoering en dus primair van toepassing is ten opzichte van vijandelijke combattanten. Het verbod op overbodig letsel (*superfluous injury*) en onnodig leed (*unnecessary suffering*) impliceert namelijk ook dat letsel en leed bestaat dat wel geoorloofd is, namelijk noodzakelijk om, met inachtneming van de regels van het humanitair oorlogsrecht, het gewapend conflict te winnen. Hiermee wordt voortgeborduurd op de St Petersburg Declaratie⁷⁶ en de *Hague Convention IV*.⁷⁷ De regel geeft een mooi voorbeeld van de balans tussen militaire noodzaak, de tegenstander buiten gevecht stellen, en humaniteit, geen onnodig lijden veroorzaken. Het verbod ziet zowel op de fysieke als op de geestelijke component van lijden bij de tegenstander.⁷⁸ Zo geeft Dinstein een voorbeeld van psychologisch letsel: “*As far as harm to human beings, severe mental trauma (such as shell shock) may count as much as serious physical injury (e.g., shrapnel wounds).*”⁷⁹ Met name deze geestelijke component zou wel eens van belang kunnen zijn bij militaire operaties beneden de drempel van aanval, waarbij ik wel opmerk dat het geestelijk leed, en zeker ernstig geestelijk leed als de hierboven genoemde ‘shell shock’, veelal het resultaat is van fysiek geweld dat binnen een gewapend conflict plaatsvindt. Met andere woorden, in die gevallen is het geestelijk leed ook een gevolg van ‘aanvallen’. Omdat geestelijk leed als gevolg van ‘aanvallen’ buiten het bereik van dit onderzoek valt, zal ik mij hier concentreren op het verbod op onnodig leed veroorzaakt door militaire operaties beneden de drempel van aanval. Te denken valt daarbij aan beïnvloedingsoperaties via *social media* of een campagne om iemands geloofwaardigheid te ondermijnen.⁸⁰

73 Dat deze regel van beperking ook geldt beneden de drempel van aanval blijkt bijv. ook uit DoD Law of War Manual 2016, p. 331. “In general, propaganda, information gathering and bribery are permissible means and methods of warfare.”

74 Conventionele Wapens Verdrag (CCW1980) met aanvullende Protocollen.

75 Zoals gecodificeerd in Aanvullend Protocol I, art 35 lid 2: “Het is verboden wapens, projectielen en stoffen alsmede methoden van oorlogvoering te gebruiken, die naar hun aard overbodig letsel of onnodig leed veroorzaken.”

76 St. Petersburg Declaration 1868: “That this object [to disable the greatest possible number of men] would be exceeded by the employment of arms which uselessly aggravate the suffering of disabled men, or render their death inevitable.”

77 Hague Convention IV 1907, article 23 (e) To employ arms, projectiles, or material calculated to cause unnecessary suffering.

78 Sandoz, Swinarski & Zimmermann 1987, p. 407. Tijdens de conferentie bleek dat de Engelse vertaling (*unnecessary suffering*) niet de volledige lading van de originele Franse tekst (*maux superflus*) dekte. De oplossing werd gevonden in de zinsnede overbodig letsel of onnodig leed omdat “the phrase ‘superfluous injury or unnecessary suffering’, as the French expression covers ‘simultaneously the sense of moral and physical suffering.’”

79 Dinstein 2016, p. 2.

80 Een dergelijke campagne kan gevoerd worden met feitelijke waarheden maar ook met leugens en valse beschuldigingen.

Vervolgens dient de vraag zich aan, hoe onderscheid tussen noodzakelijk en onnodig leed gemaakt kan worden. Op zoek naar een standaard wordt hiervoor wel teruggegrepen op de Sint Petersburg Declaratie: *“the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy.”*⁸¹ Het is daarvoor voldoende *“to disable the greatest possible number of men”*,⁸² of anders gezegd, *“to render the greatest number of enemy combatants hors de combat.”*⁸³ De test voor overbodig letsel en onnodig leed is echter bedoeld om de uitwerking van wapens en wapensystemen te beoordelen om zo bepaalde wapens of methoden van oorlogvoering te verbieden. Deze test is uitvoerbaar indien wapens en methoden van oorlogvoering specifiek bedoeld zijn voor gebruik tegen personeel. Sommige wapens zijn echter ontworpen voor de vernietiging van militair materieel of om militaire bewegingen te vertragen of te verhinderen waardoor *“an artillery projectile or missile designed to destroy field fortifications or heavy material may be expected to cause injuries to personnel in the vicinity of the target which would be more severe than necessary to render these combatants hors de combat, but no authority has questioned the lawfulness of such projectiles despite the gravity of their incidental effect on personnel.”*⁸⁴ Het verbod op overbodig letsel of onnodig leed ligt dus op het niveau van wapens, wapensystemen en methoden van oorlogvoering waarbij ook de doelstelling van het gebruik van deze middelen meegewogen moet worden. De test is dus niet bedoeld om in individuele gevallen nog een afweging te maken tussen militair voordeel en leed of letsel analoog aan de proportionaliteitstest.⁸⁵

Is bij fysiek letsel al lastig aan te geven waar de grens tussen noodzakelijk en overbodig letsel ligt, helemaal problematisch wordt het als deze problematiek geprojecteerd wordt op de geestelijke component. Analoog aan de afweging hierboven omschreven zou het moeten gaan om wapens, wapensystemen of methoden van oorlogvoering met een doelstelling om onnodig leed te veroorzaken. Wapens en wapensystemen zullen ontworpen zijn om fysieke gevolgen te veroorzaken en daarmee buiten het bereik van dit onderzoek vallen. Misschien is een methode van oorlogvoering een mogelijkheid maar hoe bepaal je of het doel van een bepaalde methode van oorlogvoering is om onnodig leed te veroorzaken? Hoe maak je onderscheid tussen het leed van een operatie ten opzichte van het algemene geestelijke leed dat een gewapend conflict sowieso kan veroorzaken? Welk psychologisch leed moet meegenomen worden in de afweging, alleen het directe psychologische leed of ook leed als Posttraumatische Stressstoornis dat zich pas later openbaart en niet of nauwelijks voorspelbaar is, omdat het ontstaan mede afhankelijk is van persoonlijkheidskenmerken en omgevingsfactoren?⁸⁶

81 St. Petersburg Declaration 1868, preamble.

82 St. Petersburg Declaration 1868, preamble.

83 Bothe, Partch & Solf 1982 p. 196.

84 Bothe, Partch & Solf 1982 p. 197.

85 Hoofdstuk 2 par. 2.3.3.

86 Veteraneninstituut, Factsheet Posttraumatische Stress Stoornis na uitzendingen. Beschikbaar op <https://www.veteraneninstituut.nl/wp-content/uploads/2015/02/FS6-Posttraumatische-stressstoornis-na-uitzending1.pdf> laatst geraadpleegd 28 nov. 2018

Uit bovenstaande beschouwing kan ik concluderen dat het principe dat onnodig leed verboden is ook geldt voor militaire operaties beneden de drempel van aanval, maar ik maak daarbij direct de opmerking dat de praktische implementatie hiervan in de praktijk lastig tot vrijwel onmogelijk zal zijn, gelet op de moeilijkheid om de grens tussen toelaatbaar en overbodig geestelijk leed als gevolg van een militaire operatie vast te stellen.

3.3.3 Onderscheid

Het grondbeginsel 'onderscheid' is al oud en heeft zijn wortels in zowel humaniteit, het beschermen van burgers tegen de verschrikkingen van militair geweld, als in militaire noodzaak. Er is geen militair voordeel bij het aanvallen van burgers of burgerobjecten, het is een verspilling van militaire middelen en zal in zijn algemeenheid het verzet versterken.⁸⁷ Het *International Court of Justice* noemt het principe van onderscheid zelfs een van de "cardinal principles" van het humanitair oorlogsrecht.⁸⁸

De opvatting dat burgers niet aangevallen mogen worden is niet van alle tijden (*"for centuries it was considered that war was not only waged against States and their armies, but also against their people"*)⁸⁹, maar wordt nu gerekend tot het gewoonterecht, zowel in een internationaal als in een niet-internationaal gewapend conflict.⁹⁰ Daar waar geen onduidelijkheid lijkt te bestaan over het verbod op directe aanvallen op de burgerbevolking of individuele burgers,⁹¹ bestaat daarentegen wel onduidelijkheid of militaire operaties beneden de drempel van aanval op burgers gericht mogen zijn. De discussie draait daarbij vooral om welke militaire operaties onder de noemer van aanval vallen.⁹² Los van deze discussie worden operaties als het verspreiden van propaganda⁹³ of *non-violent psychological warfare*⁹⁴ gezien als operaties die gericht mogen worden op de burgerbevolking, met andere woorden *"operations not amounting to an attack [...] are generally accepted as lawful."*⁹⁵ Ook bij deze laatste operaties wordt het grondbeginsel van onderscheid toegepast en gerespecteerd door te eisen dat deze operaties niet mogen kwalificeren als 'aanval'.

Het zal dan ook niet verbazen dat de uitvloeisels van het grondbeginsel van onderscheid ruimschoots voorkomen in verdragen⁹⁶ en, zoals hierboven vermeld, erkend worden als

87 Bothe, Partch & Solf 1982, p. 279.

88 *International Court of Justice* 1996, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion par. 434.

89 Sandoz, Swinarski & Zimmerman 1987, p. 585.

90 Henckaerts & Doswald-Beck, 2005 *Black letter rule* 1.

91 Er bestaan nog wel andere meningen. Zo benoemt Warden (1995) in zijn vijf-ringen model de burgerbevolking als vierde, van vijf, 'centers of gravity' in het systeem van de vijand dat daarmee ook een aangrijpingspunt vormt om het gewapend conflict te beslechten. Hij plaatst hierbij wel de kanttekening dat *"let us reiterate that we hold direct attacks on civilians to be morally reprehensible and militarily difficult (too many targets and willingness to suffer grievously before it will turn on its own government)"* en hij bepleit dan ook een "indirect attack", in tegenstelling tot een directe fysieke aanval, op de bevolking.

92 Op deze discussie, ook wel aangeduid als het Schmitt-Dörmann debat, kom ik in Hoofdstuk 4 uitgebreid terug.

93 Bothe, Partch & Solf 1982, p. 329.

94 Dinstein 2016, p. 143.

95 Schmitt 2013a, p. 92.

96 Zie bijv. Aanvullend Protocol I, deel IV (burgerbevolking) en Aanvullend Protocol II, deel IV (burgerbevolking).

gewoonterecht.⁹⁷ Dit grondbeginsel ligt ten grondslag aan de tweedeling combattant – burger en militair object – burgerobject maar kan ook gebruikt worden om het verschil te duiden tussen personen en objecten met algemene bescherming en bijzondere bescherming.

Als ik specifiek kijk naar de invloed van dit grondbeginsel op militaire operaties beneden de drempel van aanval, zal ik als eerste het algemene beginsel van onderscheid bespreken (3.3.3.1). Hierna zal ik in paragraaf 3.3.3.2 aandacht besteden aan de term ‘ontzien en beschermd’ zoals deze gebruikt wordt in bijvoorbeeld Aanvullend Protocol I, artikel 10: “Alle gewonden, zieken en schipbreukelingen, tot welke partij zij ook behoren, dienen te worden *ontzien en beschermd*.”⁹⁸ Deze term komt namelijk op diverse plaatsen in het humanitair oorlogsrecht terug en heeft een specifieke betekenis in de bescherming tegen militaire operaties beneden de drempel van aanval voor zowel personen als objecten. Vervolgens zal ik een splitsing aanbrengen in bescherming voor personen (3.3.3.3) en objecten (3.3.3.4) waarbij ik een groepering aan zal brengen aan de hand van de bescherming tegen militaire operaties beneden de drempel van aanval. Hierna zal ik het onderwerp ‘voorzorgsmaatregelen’ (*precautionary measures*) bespreken (3.3.3.5), omdat ik deze zie als voortvloeiend uit het grondbeginsel onderscheid,⁹⁹ gevolgd door een schematisch overzicht waarin ik de verschillende vormen van bescherming op basis van onderscheid zal weergeven.

De definitie van burgerobjecten is in artikel 52 Aanvullend Protocol I gekoppeld aan de definitie van militair doel. Dit artikel definieert burgerobjecten als alle objecten die geen militair doel vormen. Militaire doelen zijn: “die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel opleveren.”¹⁰⁰ Twee onderwerpen uit de definitie van militair doel zal ik in de laatste paragraaf (3.3.3.6) aanstippen, namelijk de betekenis van de woorden ‘objecten’ en ‘onbruikbaarmaking’. Ik doe dit zodat ik deze in het tweede deel van mijn onderzoek nader kan uitwerken, omdat ze in de cybercontext een aangepaste uitleg behoeven.

3.3.3.1 Het grondbeginsel van onderscheid

Het grondbeginsel ‘onderscheid’ is zowel internationaal gewoonterecht¹⁰¹ als gecodificeerd in bijvoorbeeld artikel 48 van Aanvullend Protocol I en houdt in dat partijen bij het conflict te allen tijde onderscheid moeten maken tussen de burgerbevolking en combattanten en

97 Henckaerts & Doswald-Beck, 2005 begint er zelfs mee. *Black letter rule* 1 tot en met 13.

98 Aanvullend Protocol I, art. 10 lid 1, mijn accentuering.

99 Al heeft het onderwerp ‘voorzorgsmaatregelen’ ook connecties met de grondbeginselen proportionaliteit, humaniteit en militaire noodzaak.

100 Aanvullend Protocol I, art. 52 lid 2. Opgemerkt dient te worden dat deze definitie alleen geldt voor objecten. Daarnaast kunnen ook personen een militair doel vormen, wat bepaald wordt door de status van die personen.

101 Henckaerts & Doswald-Beck, 2005 *Black letter rule* 1 en 7.

tussen burgerobjecten en militaire doelen. Hiertoe dienen zij “hun operaties uitsluitend tegen militaire doelen te richten.”¹⁰²

In het vorige hoofdstuk heb ik al aandacht besteed aan de betekenis van de term operaties uit artikel 48,¹⁰³ zodat ik hier kan volstaan met de conclusie dat militaire operaties een ruimer begrip is dan aanvallen. Omdat alle militaire operaties gericht moeten zijn tegen militaire doelen,¹⁰⁴ kan ik hieruit concluderen dat deze grondregel van onderscheid ook van kracht is beneden de drempel van aanval. Hoe dit uitwerkt voor de categorieën personen en objecten volgt in de volgende subparagrafen.

3.3.3.2 ‘Ontzien en beschermd’

De term ‘ontzien en beschermd’ komt op diverse plaatsen terug in het humanitair oorlogsrecht. Voorbeelden hiervan zijn de bepalingen over zieken, gewonden en schipbreukelingen,¹⁰⁵ medische formaties,¹⁰⁶ medisch personeel en medische vervoermiddelen¹⁰⁷ en religieus personeel,¹⁰⁸ maar ook burgerinstellingen voor civiele bescherming en haar personeel¹⁰⁹ en personeel dat deelneemt aan hulpverleningsacties.¹¹⁰ Wat deze formaties, personen en objecten gemeen hebben is dat ze bedoeld zijn in een gewapend conflict humanitaire hulp te verlenen.¹¹¹ Omdat de term ‘ontzien en beschermd’ oorspronkelijk afkomstig is uit de behandeling van gewonden, zal ik deze term vanuit die achtergrond nader behandelen.

In de periode vanaf de oudheid, door de Middeleeuwen tot ver in de 19e eeuw waren gewonden op het slagveld overgeleverd aan de genade van de overwinnaar.¹¹² De slag bij Solferino en het boek dat Henry Dunant hierover schreef,¹¹³ met als reactie daarop de oprichting van het *International Committee of the Red Cross*, leidde in 1864 tot de eerste *Geneva Convention*. Hierin werd het belangrijke principe beschreven dat leden van de krijgsmacht die gewond of ziek waren, en daarom ongevaarlijk en niet in staat zichzelf te verdedigen, gerespecteerd en verzorgd moesten worden zonder onderscheid op basis van nationaliteit.

■
102 Aanvullend Protocol I art. 48.

103 Hoofdstuk 2 par. 2.4.4.

104 Dit is, voor objecten, vastgelegd in art. 52 lid 2 Aanvullend Protocol I. Zoals eerder opgemerkt in Hoofdstuk 2 par. 2.3.3 is het duidelijk dat ook vijandelijke strijdkrachten een legitiem doel van een aanval vormen. Welke militaire operaties beneden de grens van aanval, gericht op personen die geen combattant zijn, legitiem zijn, bespreek ik in par. 3.3.3 van dit hoofdstuk.

105 Aanvullend Protocol I art. 10.

106 Geneefse Conventie I art. 19, Aanvullend Protocol I art. 12.

107 Geneefse Conventie I art. 24-26, Geneefse Conventie II, art. 36, Geneefse Conventie IV art. 20, Aanvullend Protocol I art. 15, Aanvullend Protocol II art. 9.

108 Geneefse Conventie I art. 24, Geneefse Conventie II, art. 36, Aanvullend Protocol I art. 15, Aanvullend Protocol II art. 9.

109 Aanvullend Protocol I art. 62.

110 Aanvullend Protocol I art. 71 lid 2.

111 Of ingeval van schipbreukelingen, zieken en gewonden humanitaire hulp te ontvangen.

112 Pictet 1952, p. 10.

113 Henry Dunant 1862, *A memory of Solferino*.

Als gevolg hiervan, in het exclusieve belang van de gewonden, moesten ambulances en militaire hospitalen, inclusief het medisch personeel, worden beschermd tegen vijandelijke daden.¹¹⁴

Deze bescherming van zieken en gewonden op het slagveld is in de daaropvolgende jaren verder uitgebreid tot uiteindelijk het Eerste Verdrag van Genève (1949) om met de totstandkoming van Aanvullend Protocol I de bescherming van burgergewonden op hetzelfde peil te brengen als die voor militairen.¹¹⁵

De term 'ontzien' (*respected*) werd voor het eerst gebruikt in de eerste revisie van 1906 van de *Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field* van 1864. Tot dan was 'ontzien' van gewonden slechts impliciet opgenomen. Bij de tweede revisie van 1929 werd de term uitgebreid met 'beschermd' (*protected*).¹¹⁶

Ontzien betekent in deze zin "*to spare, not to attack*"¹¹⁷ en heeft daarmee een passieve strekking in tegenstelling tot de term 'beschermen' die duidt op een actief element namelijk "*to come to someone's defence, to lend help and support*"¹¹⁸ of "*to shield, to keep safe, to take care of*".¹¹⁹

Hoe deze termen uitgelegd moeten worden kan het best besproken worden aan de hand van de bescherming van medische formaties¹²⁰ omdat diverse auteurs hier voorbeelden bij hebben gegeven die verhelderd werken. Zo merkt Pictet met betrekking tot 'ontzien' van medische formaties op dat "*to respect such units means, first of all, not to attack them or harm them in any way*"¹²¹ om daar vervolgens aan toe te voegen "*to respect such units means, secondly, not to interfere with their work. It is not enough for the enemy to simply refrain from taking action against them; he must allow them to continue to give treatment to the wounded in their care, as long as this is necessary.*"¹²² Anderen merken hierover op dat "*this [respect] also means that there should be no interference with their work (for example, by preventing supplies from getting through)*"¹²³ en "*they must not knowingly be attacked, fired upon, or unnecessarily prevented from discharging their proper function.*"¹²⁴

114 Pictet 1952, p. 11.

115 Bothe, Partch & Solf 1982 p. 89. "A major deficiency of the four Geneva Conventions is that, in the medical field, the protection is much better developed for the military than for civilians. It is the purpose of this Part [Part II of Additional Protocol I] to plug in a number of loopholes in, and to remedy certain deficiencies of, provisions of the Geneva Conventions."

116 Pictet 1953, p. 134.

117 Pictet 1953, p. 134, in dezelfde zin Sandoz, Swinarski & Zimmerman 1987, p. 146 en Bothe, Partch & Solf 1982, p. 108

118 Pictet 1953, p. 135, in dezelfde zin Sandoz, Swinarski & Zimmerman 1987, p. 146

119 Bothe, Partch & Solf 1982, p. 108.

120 Zoals vastgelegd in Verdrag I van Genève art. 19 en Aanvullend Protocol I art. 12.

121 Pictet 1953, p. 196.

122 Pictet 1953, p. 196.

123 Sandoz, Swinarski & Zimmerman 1987, p. 166.

124 Bothe, Partch & Solf 1982, p. 118.

Met betrekking tot de term ‘beschermd’ merkt Pictet op dat “to protect the units is to ensure that they are respected, that is to say to oblige third parties to respect them. It also means coming to their help in case of need.”¹²⁵ ‘Beschermd’ heeft daarmee een actief element oftewel “it is no longer only a matter of not preventing supplies from reaching their units, [...] but, if necessary, to help to ensure the delivery of these supplies (for example, by providing a vehicle) or even to make sure that they are not jeopardized by third parties (looting etc.).”¹²⁶

Deze analyse van de term ‘ontzien en beschermd’ (*respected and protected*), die zoals eerder opgemerkt, op een aantal andere plaatsen wordt gebruikt, betekent niet dat deze woorden in alle gevallen exact dezelfde betekenis hebben.¹²⁷ “While the duty to spare the persons or objects in question from attack is of general validity, the duty to give assistance and to shield can, or even must, mean different things in different contexts.”¹²⁸ Aan het gedeelte ‘ontzien’ lijkt overal dezelfde betekenis toegekend te worden. Maar met name de vraag hoever ‘beschermen’ in concreto dient te gaan zal afhangen van de omstandigheden van het moment, maar gaat in elk geval verder dan alleen ‘niet-aanvallen’.

Van belang voor dit onderzoek is dat telkens als de term ‘ontzien en beschermd’ wordt gebruikt, dit betekent dat de bescherming verder gaat dan alleen bescherming tegen een aanval in de zin van artikel 49 Aanvullend Protocol I, die zoals eerder is aangegeven gericht is op fysiek letsel of schade. Door de term ‘ontzien en beschermd’ zijn niet alleen aanvallen op formaties, personen en objecten bedoeld voor humanitaire hulpverlening verboden, maar moet ook bij militaire operaties beneden de drempel van aanval worden voorkomen dat deze interfereren met het humanitaire werk van deze formaties, personen en objecten of anderszins de humanitaire werkzaamheden of behoorlijke taakuitoefening belemmeren. Met andere woorden, de bescherming van deze formaties, personen en objecten gaat verder dan alleen bescherming tegen aanvallen en geldt tegen alle militaire operaties, ook die beneden de drempel van aanval, indien deze operaties gericht zijn tegen het humanitair optreden of functioneren of die dit optreden of functioneren negatief beïnvloeden.

3.3.3.3 Personen

3.3.3.3.1 Burgerbevolking en afzonderlijke burgers, algemene bescherming

“De burgerbevolking en de afzonderlijke burgers genieten algemene bescherming tegen uit militaire operaties voortvloeiende gevaren.”¹²⁹ Deze algemene regel bevestigt expliciet de gewoonterechtelijke regel dat “onschuldige burgers buiten de vijandelikheden gehouden moeten worden en zoveel als mogelijk beschermd zijn tegen de gevaren

■ 125 Pictet 1953, p. 196.

126 Sandoz, Swinarski & Zimmerman 1987, p. 166.

127 Bothe, Partch & Solf 1982, p. 118.

128 Bothe, Partch & Solf 1982, p. 118.

129 Aanvullend Protocol I art. 51 lid 1. Omdat de bescherming van de burgerbevolking tot het internationaal gewoonterecht wordt gerekend voor zowel een internationaal als een niet-internationaal gewapend conflict (Henckarts & Doswald-Beck, 2005 *Black letter rule* 1) bespreek ik hier alleen de bepaling uit Aanvullend Protocol I maar dit geldt in dezelfde mate voor de burgerbevolking in een niet-internationaal gewapend conflict.

voortvloeiend uit vijandelijkheden.”¹³⁰ Deze algemene regel vormt de opmaat naar een verdere concretisering, verduidelijking en aanvulling in het vervolg van Aanvullend Protocol I artikel 51,¹³¹ waarvan de eerste wordt genoemd in lid 2, namelijk het verbod om de burgerbevolking noch de afzonderlijke burgers het doelwit van een aanval te laten vormen.¹³²

De algemene regel van bescherming van de burgerbevolking spreekt, net als de grondregel van onderscheid, expliciet van de meeromvattende term militaire operaties. Daarna volgt een verbod op aanvallen. Een taalkundige analyse van artikel 51 gecombineerd met artikel 48 van Aanvullend Protocol I levert de volgende conclusie; militaire operaties beneden de drempel van aanval gericht op burgers zijn niet verboden mits de burgerbevolking beschermd wordt tegen de gevaren die voortvloeien uit die militaire operaties en waarbij, als uitvloeisel van het grondbeginsel van militaire noodzaak, tevens sprake is van een te behalen militair voordeel.¹³³

Wat dient verstaan te worden onder ‘gevaren die voortvloeien uit militaire operaties’? Indicaties zijn te vinden in de *Commentary* bij artikel 58 van Aanvullend Protocol I, dat handelt over voorzorgen tegen de gevolgen van aanvallen. Lid 3 van dit artikel draagt partijen op om “alle andere noodzakelijke voorzorgen te nemen om de burgerbevolking, de individuele burgers en de burgerobjecten onder hun gezag tegen de uit militaire operaties voortvloeiende gevaren te beschermen.”¹³⁴

Voordat ik de term ‘uit operaties voortvloeiende gevaren’ bespreek eerst een opmerking over ‘onder hun gezag’. Artikel 58 Aanvullend Protocol I is bedoeld voor toepassing “*in its own territory in favour of its nationals, or in territory under its control.*”¹³⁵ Het artikel geldt echter in gelijke mate voor de tegenstander zodat “*they [the adversaries] themselves must also cooperate by taking all possible precautions for the benefit of their own population.*”¹³⁶ Met andere woorden er is altijd een partij die de voorzorgen tegen de gevolgen van aanvallen moet nemen. Wat verstaan moet worden onder ‘uit militaire operaties voortvloeiende operaties’ is dus voor alle burgers gelijk. Het verschil bestaat uit de partij die de voorzorgen moet nemen. De term ‘uit militaire operaties voortvloeiende gevaren’ is daarmee op dezelfde manier gebruikt als in artikel 51 Aanvullend Protocol I.

De *Commentary* geeft bij artikel 58 Aanvullend Protocol I enkele voorbeelden van de te nemen voorzorgen. Ten aanzien van personen geeft de *Commentary* het bouwen van bunkers of beschermde onderkomens die voldoende bescherming bieden tegen de effecten van

■
130 Sandoz, Swinarski & Zimmermann 1987, p. 615.

131 Bothe, Partch & Solf 1982, p. 299.

132 Aanvullend Protocol I art. 51, lid 2.

133 Zie hiervoor par 3.3.1 militaire noodzaak.

134 Aanvullend Protocol I art. 58 lid 3.

135 Sandoz, Swinarski & Zimmermann 1987, p. 692.

136 Sandoz, Swinarski & Zimmermann 1987, p. 692.

wapens.¹³⁷ Voor objecten worden maatregelen genoemd ‘om schade te limiteren’, zoals effectieve brandweerbewaking.¹³⁸ In beide gevallen wijzen de voorbeelden op fysiek letsel of fysieke schade waartegen voorzorgen genomen moeten worden, met andere woorden de uit militaire operaties voortvloeiende gevaren zijn van fysieke aard.

Een militaire operatie beneden de grens van aanval, gericht op de burgerbevolking of individuele burgers, is niet verboden indien de burgerbevolking beschermd wordt tegen de gevaren van fysieke aard die voortvloeien uit die militaire operatie en sprake is van een te behalen militair voordeel. De enige uitzondering hierop is het verbod op het dreigen met geweld met als doel het zaaien van angst zoals verwoord in artikel 51 lid 2 van Aanvullend Protocol I.¹³⁹ Een voorbeeld van een toegestane militaire operatie beneden de drempel van aanval kan bovenstaande redenering verduidelijken. Een psychologische operatie gericht op de burgerbevolking van een bepaald gebied om de daar aanwezige militairen niet, bij vijandelijke militairen, of juist wel, bij eigen troepen, te steunen is niet verboden binnen het humanitair oorlogsrecht¹⁴⁰ op basis van het grondbeginsel onderscheid.¹⁴¹ Het stelt de burgerbevolking immers niet bloot aan fysieke gevaren.

Bovenstaande redenering leidt tot de conclusie dat het grondbeginsel van onderscheid van de burgerbevolking en afzonderlijke burgers van toepassing is voor militaire operaties beneden de drempel van aanval. In tegenstelling tot aanvallen leidt het grondbeginsel echter niet tot een verbod op operaties beneden de grens van aanval gericht op burgers, zolang deze burgers maar niet worden blootgesteld aan uit die operaties voortvloeiende fysieke gevaren of aan de dreiging van geweld waarvan het oogmerk is om de burgerbevolking angst aan te jagen.

3.3.3.2 Bescherming tegen militaire operaties beneden de drempel van aanval

Naast de algemene bescherming voor burgers bestaan categorieën personen die een bijzondere aanvullende bescherming genieten. Het kunnen echter ook personen zijn die op basis van hun beroep, bijvoorbeeld geneeskundig personeel, of omstandigheden, bijvoorbeeld schipbreukelingen, een bijzondere bescherming genieten. Er zijn diverse categorieën, zo komt Dinstein tot elf.¹⁴² Voor de bescherming tegen militaire operaties beneden de drempel van aanval onderken ik een driedeling in oplopende graden van

¹³⁷ Sandoz, Swinarski & Zimmermann 1987, p. 694.

¹³⁸ Sandoz, Swinarski & Zimmermann 1987, p. 695.

¹³⁹ Art. 51, lid 2 luidt: “daden van geweld of bedreiging met geweld, waarvan het belangrijkste oogmerk is de burgerbevolking angst aan te jagen, zijn verboden.”

¹⁴⁰ Oeter (in Fleck) 2013a, p. 227, *Black letter rule* 483: “classic forms of propaganda...the incitement of the entire population the revolt against its government.” In dezelfde zin Chainoglou 2011, p. 14, “Psychological warfare activities which are directed against military objectives are legal; psychological warfare activities directed against the civilian population should be also accepted as legal.” Schmitt 2012, p. 187 “for it is well accepted that propaganda and other psychological operations directed at the enemy population are lawful methods of warfare.” Dinstein 2016, p. 143. “After all, it is incontrovertible that non-violent psychological warfare[...] may be lawfully directed against civilians.”

¹⁴¹ Waarbij uiteraard geen andere regels van het humanitair oorlogsrecht overtreden mogen worden, bijvoorbeeld door dreiging met geweld met als doel angst te zaaien. Dit verbod is gecodificeerd in Aanvullend Protocol I art 51 lid 2.

¹⁴² Dinstein 2004, p. 141 – 149.

bijzondere bescherming. De laagste graad van bijzondere bescherming biedt alleen bescherming tegen aanvallen. Dit houdt in dat geen bescherming bestaat tegen militaire operaties beneden de drempel van aanval, met andere woorden, deze mogen gericht zijn op deze personen. De tweede graad van bescherming is gelijk aan de algemene bescherming van burgers namelijk bescherming tegen aanvallen plus bescherming tegen de fysieke gevaren van andere militaire operaties. De derde en hoogste graad van bescherming is de bescherming zoals hiervoor besproken bij de term 'ontzien en beschermd'. Deze bescherming houdt een bescherming in tegen aanvallen plus een bescherming tegen alle andere militaire operaties gericht op het verstoren van het humanitair optreden of functioneren van deze personen of die dit optreden of functioneren negatief beïnvloeden.

3.3.3.3.3 *Personen zonder bescherming tegen operaties beneden de drempel van aanval*

Deze groep van personen genieten, als gevolg van specifieke omstandigheden bescherming tegen een aanval. Dit zijn parachutisten uit een vliegtuig in nood (met uitzondering van luchtlandingseenheden),¹⁴³ personen *hors de combat*¹⁴⁴ (tenzij de buitengevechtstelling het gevolg is van verwonding of ziekte waardoor deze personen 'ontzien en beschermd' moeten worden) en parlementairen.¹⁴⁵

Deze categorieën van personen genieten alleen bescherming tegen aanvallen en niet tegen militaire operaties beneden de drempel van aanval. Zij vallen daarmee buiten het bereik van dit onderzoek.

3.3.3.3.4 *Personen met gelijke bescherming als burgers tegen operaties beneden de drempel van aanval*

De categorieën personen met bijzondere bescherming die, voor wat betreft hun bescherming tegen militaire operaties beneden de drempel van aanval, gelijkgesteld kunnen worden met de algemene bescherming van de burgerbevolking zijn vrouwen,¹⁴⁶ kinderen¹⁴⁷ en journalisten.¹⁴⁸ Deze drie categorieën staan vermeld onder sectie III van deel IV van Aanvullend Protocol I. Deel IV handelt in zijn geheel over de burgerbevolking, maar waar sectie I de algemene bescherming tegen de gevolgen van de vijandelijkheden aangaat (met daarin het hiervoor behandelde artikel 52 Aanvullend Protocol I over de algemene bescherming van de burgerbevolking), gaat sectie III specifiek over de behandeling van personen in de macht van de tegenpartij. Sectie I (en II) handelen over de burgerbevolking als een collectief concept terwijl sectie III een aantal regels formuleert ter bevoordeling van burgers als individuen.¹⁴⁹ Deze bepalingen zijn bedoeld om een minimum aan bescherming

■
¹⁴³ Aanvullend Protocol I art. 42.

¹⁴⁴ Aanvullend Protocol I art. 41.

¹⁴⁵ Haags Verdrag IV 1907 art. 32.

¹⁴⁶ Aanvullend Protocol I art. 76.

¹⁴⁷ Aanvullend Protocol I art. 77.

¹⁴⁸ Aanvullend Protocol I art. 79.

¹⁴⁹ Sandoz, Swinarski & Zimmermann 1987, p. 837.

tijdens een gewapend conflict te bieden aan personen die om welke reden dan ook geen aanspraak kunnen maken op een andere beschermende status.¹⁵⁰

Het zal dan ook geen verbazing wekken dat de categorieën die hier genoemd zijn voor wat betreft hun bescherming tegen militaire operaties beneden de drempel van aanval uitkomen op dezelfde bescherming als de burgerbevolking in zijn geheel, namelijk bescherming tegen aanvallen plus bescherming tegen fysieke gevaren voortvloeiend uit overige militaire operaties.

3.3.3.3.5 *Personen met extra bescherming tegen militaire operaties beneden de drempel van aanval.*

De laatste groep van personen met bijzondere bescherming is de groep met de meest vergaande bescherming tegen militaire operaties beneden de drempel van aanval. De personen in deze groep zijn allen gerelateerd aan humanitaire hulpverlening waarbij in alle gevallen de bescherming geldt die hiervoor is besproken bij de term ‘ontzien en beschermd’. Het betreft gewonden, zieken en schipbreukelingen,¹⁵¹ medisch personeel,¹⁵² geestelijk verzorgers,¹⁵³ personeel van de civiele bescherming¹⁵⁴ en personeel deelnemende aan hulpverleningsacties.¹⁵⁵ Zoals opgemerkt bij de uitleg van ‘ontzien en beschermd’ worden al deze categorieën personen niet alleen beschermd tegen aanvallen maar ook tegen alle andere militaire operaties gericht op het verstoren van het humanitair optreden of functioneren of die dit optreden of functioneren negatief beïnvloeden.

3.3.3.4 *Objecten*

3.3.3.4.1 *Burgerobjecten; algemene bescherming*

Net als de algemene bescherming van de burgerbevolking wordt de bescherming van burgerobjecten tegen aanvallen gerekend tot het gewoonterecht.¹⁵⁶ In tegenstelling tot de bepaling met betrekking tot de bescherming van de burgerbevolking begint artikel 52 Aanvullend Protocol I niet met een regel van algemene bescherming, maar direct met een verbod op aanvallen op burgerobjecten waarbij burgerobjecten negatief gedefinieerd worden als alle objecten die geen militair doel zijn.¹⁵⁷ Lid 2 van hetzelfde artikel bepaalt dat aanvallen gericht moeten zijn op militaire doelen en definieert vervolgens, voor zover het objecten betreft, militaire doelen.¹⁵⁸

■
150 Sandoz, Swinarski & Zimmermann 1987, p. 664.

151 Geneefse Conventie I art 12 en II art. 12, Aanvullend Protocol I art.10.

152 Geneefse Conventie I art 24 en 25 en II art. 36 en 37, Aanvullend Protocol I art.15.

153 Geneefse Conventie I art 24 en II art. 36 en 37, Aanvullend Protocol I art.15.

154 Geneefse Conventie IV art 63 lid 2, Aanvullend Protocol I art. 62.

155 Aanvullend Protocol I art 71 lid 2.

156 Henckarts & Doswald-Beck 2005 *Black letter rule* 7. Omdat de bescherming van de burgerobjecten tot het internationaal gewoonterecht wordt gerekend voor zowel een internationaal als een niet-internationaal gewapend conflict bespreek ik hier alleen de bepaling uit Aanvullend Protocol I, maar dit geldt in dezelfde mate voor de burgerobjecten in een niet-internationaal gewapend conflict.

157 Aanvullend Protocol I art. 52 lid 1.

158 Ook personen kunnen een legitiem militair doel vormen maar dat is afhankelijk van de status van deze personen.

De vraag die zich aandient is of, en zo ja, hoe algemene bescherming bestaat van burgerobjecten tegen militaire operaties beneden de drempel van aanval. Een voorbeeld kan hier weer helderheid scheppen. Stel dat een eenheid wil verplaatsen om een gunstige positie in te nemen. Dit is een militaire operatie beneden de drempel van aanval met een militair voordeel, dus aan het grondbeginsel van militaire noodzaak is voldaan. De eenheid maakt hierbij gebruik van een bestaande brug (die normaal alleen civiel gebruikt wordt) zonder deze te beschadigen. De brug loopt hierdoor weliswaar gevaar, omdat tijdens het gebruik voor het militair transport de brug een militair doel vormt voor een tegenstander, maar een algemeen verbod op het gebruik van dergelijke objecten bestaat niet, ook niet als deze objecten daardoor gevaar lopen.

Deze conclusie dat objecten die normaal alleen civiel gebruik kennen, gebruikt mogen worden voor militaire operaties beneden de drempel van aanval volgt impliciet ook uit Aanvullend Protocol I artikel 53(b) handelend over de bescherming van culturele goederen. Uit het feit dat culturele goederen niet gebruikt mogen worden ter ondersteuning van de militaire inspanning houdt via een *a contrario* redenering in dat andere civiele goederen hiervoor wel gebruikt mogen worden.¹⁵⁹ Een verbod op gebruik voor militaire operaties komt dus mogelijk wel aan de orde indien sprake is van een bijzondere bescherming.

Hieruit concludeer ik dat het grondbeginsel van onderscheid bij burgerobjecten geen algemene bescherming biedt tegen militaire operaties beneden de drempel van aanval. Overigens is het wel mogelijk dat burgerobjecten, net als burgers, bescherming genieten tegen meer dan alleen aanvallen, maar die vloeit dan voort uit een bijzondere status van het object en niet uit de status van burgerobject.

Het hierboven geconstateerde verschil in bescherming tussen personen en objecten is mogelijk te verklaren vanuit de doelstelling van het humanitair oorlogsrecht. Zoals in het vorige hoofdstuk beschreven, bestaat die doelstelling uit het vinden van een balans tussen militaire noodzaak en humaniteit. Het lijkt daarbij logisch dat humaniteit bij personen meer gewicht in de schaal legt dan bij objecten.¹⁶⁰

3.3.3.4.2 Burgerobjecten; bijzondere bescherming tegen militaire operaties beneden de drempel van aanval

Daar waar bij burgerobjecten geen algemene bescherming tegen militaire operaties beneden de drempel van aanval bestaat, is het nodig om te bezien hoe dit is bij

159 Zie ook de *Commentary* op Aanvullend Protocol I art. 58 lid 2 handelend over voorzorgen tegen de gevolgen van aanvallen. Hierin staat: "If military objectives located in an urban area are camouflaged, for example, so as to appear to be inoffensive buildings, ...the danger for the population is increased, particularly because of the incidental damage caused by bombing or artillery fire." Sandoz, Swinarski & Zimmermann 1987, p. 694. *A contrario* geredeneerd: als bij het gebruik van civiele gebouwen als camouflage rekening gehouden moet worden met het bijkomende gevaar voor personen is het dus niet verboden.

160 Een andere indicatie dat de bescherming van objecten binnen het humanitair oorlogsrecht kleiner is dan die van personen is te vinden in Aanvullend Protocol I art. 85 lid 3 (b). "It should be noted that damage to objects, [...], is only mentioned in relation to the state of mind of the person committing the breach. The actual consequences defined by the opening sentence of the paragraph as constitutive elements of a breach, are death or serious injury to body or health in excess of what would be justified under the principle of proportionality" Sandoz, Swinarski & Zimmermann 1987, p. 996. Schade aan objecten is geen constitutief element bij de bepaling of een niet-onderscheidende aanval een ernstige inbreuk binnen het humanitair oorlogsrecht is.

burgerobjecten met bijzondere bescherming. Net als bij personen kom ik bij objecten tot drie categorieën.

De eerste categorie beschrijf ik als de categorie met een verhoogde bescherming tegen aanvallen. Deze verhoogde bescherming is op een drietal manieren vormgegeven. Er worden bijzondere eisen aan het object gesteld voordat het aangevallen mag worden,¹⁶¹ er worden hogere eisen gesteld aan de voorwaarden voor verlies van bescherming¹⁶² of de objecten worden ook beschermd tegen andere militaire operaties die hetzelfde fysieke effect hebben als aanvallen.¹⁶³ Al deze vormen van speciale bescherming blijven echter bescherming tegen aanvallen waarop uitzonderingen mogelijk zijn. De voorwaarden voor deze uitzonderingen liggen hoger dan bij gewone burgerobjecten. Tot deze categorie behoren plaatsen van godsdienstige verering,¹⁶⁴ voor het overleven van de burgerbevolking onmisbare objecten,¹⁶⁵ werken en installaties die gevaarlijke krachten bevatten¹⁶⁶ en het natuurlijk milieu.¹⁶⁷ Ondanks het aanvullende karakter blijft in al deze gevallen de bescherming beperkt tot bescherming tegen aanvallen en niet tegen operaties beneden de drempel van aanval.

De tweede categorie omvat culturele goederen. Voor culturele goederen geldt een relatieve bescherming tegen het gebruik van deze goederen voor militaire operaties beneden de drempel van aanval. Daar waar civiele objecten gebruikt mogen worden voor militaire doeleinden, mits voldaan wordt aan de voorwaarde van militaire noodzaak, mogen culturele objecten en hun directe omgeving niet gebruikt worden voor doeleinden welke deze goederen aan vernietiging of beschadiging zouden kunnen blootstellen in geval van een gewapend conflict.¹⁶⁸ Indien de brug uit het voorbeeld van paragraaf 3.3.5.1 ook een cultureel object zou zijn, zou de eenheid deze brug niet mogen gebruiken voor de verplaatsing. Dit verbod op het gebruik van een object met de bescherming van een cultureel goed is echter niet absoluut. Uitzondering is namelijk mogelijk indien “de militaire noodzaak een dergelijk gebruik gebiedend vereist”,¹⁶⁹ of, als het gaat om culturele objecten met speciale bescherming, “in uitzonderlijke gevallen van onvermijdelijke

161 Bijvoorbeeld werken en installaties die gevaarlijke stoffen bevatten. Deze mogen niet het doelwit van een aanval worden, zelfs niet wanneer zij een militair doel zijn, indien die aanval het vrijkomen van gevaarlijke krachten zou veroorzaken en daardoor zware verliezen aan mensenlevens onder de burgerbevolking teweeg zou brengen. Aanvullend Protocol I art. 56 lid 1.

162 Bothe, Partch & Solf 1982, p. 355. Zo vereist art 56 lid 2 Aanvullend Protocol I “aanzienlijke en rechtstreekse ondersteuning van de militaire operaties” als voorwaarde voor verlies van bescherming tegen aanvallen terwijl artikel 52 slechts spreekt over “daadwerkelijke bijdrage”.

163 Weghalen en onbruikbaar maken van voor het overleven van de burgerbevolking onmisbare objecten. Aanvullend Protocol I art 54 lid 2.

164 Onder andere Aanvullend Protocol I art. 53, Aanvullend Protocol II art. 16 en Verdrag inzake de bescherming van culturele goederen 1954 art. 1.

165 Aanvullend Protocol I art. 54.

166 Aanvullend Protocol I art. 56.

167 Aanvullend Protocol I art. 55.

168 Verdrag inzake de bescherming van culturele goederen 1954, art. 4 lid 1.

169 Verdrag inzake de bescherming van culturele goederen 1954, art. 4 lid 2. Het 1999 *Second Hague Protocol* geeft in art. 6 nadere aanwijzingen wanneer en door wie “gebiedend vereist” mag worden vastgesteld.

militaire noodzaak en slechts zolang deze noodzaak voortduurt.¹⁷⁰ De bescherming komt dan alsnog te vervallen.¹⁷¹ Deze bescherming zal ik aanduiden als relatieve bescherming tegen operaties beneden de drempel van aanval indien het object door deze operatie aan gevaar van vernietiging of beschadiging wordt blootgesteld.

De derde categorie objecten bestaat uit de objecten die de bescherming genieten die ik heb besproken onder 'ontzien en beschermd'. Deze bescherming tegen aanvallen en tegen alle andere militaire operaties gericht op het verstoren van het humanitair optreden of functioneren of die dit optreden of functioneren negatief beïnvloeden geldt voor objecten die nodig zijn voor humanitaire hulpverlening. Hieronder vallen medische formaties,¹⁷² medisch vervoer¹⁷³ en instellingen voor civiele bescherming.¹⁷⁴

3.3.3.5 Voorzorgsmaatregelen

Voorzorgsmaatregelen, zoals gecodificeerd in Aanvullend Protocol I, artikel 57 en 58, worden gerekend tot het gewoonterecht.¹⁷⁵ Hoewel het beginsel van voorzorgen (*precautions*) soms wel aangemerkt wordt als zelfstandig beginsel binnen het humanitair oorlogsrecht,¹⁷⁶ deel ik de mening van de *Commentary* dat de voorzorgen zoals vermeld in Aanvullend Protocol I “reaffirms rules which are already contained explicitly or implicitly in other articles, in particular: Article 48 (Basic rule), which lays down the “basic rule” of distinction, Article 51 (Protection of the civilian population), which reiterates the general immunity enjoyed by the civilian population and prohibits indiscriminate attacks, Article 52 (General protection of civilian objects), which restricts attacks to military objectives and defines these, and Article 54 (Protection of objects indispensable to the survival of the civilian population), which protects indispensable objects.”¹⁷⁷ Al deze artikelen zijn gebaseerd op het algemene beginsel van onderscheid dat ik hiervoor al heb besproken.

Wat opvalt is dat vrijwel alle voorzorgsmaatregelen zijn gedefinieerd in termen van aanvallen. De enige uitzondering is de verwijzing naar militaire operaties in het eerste lid van artikel 57. Hoewel dit artikel de titel ‘Voorzorgen bij aanvallen’¹⁷⁸ draagt, spreekt het eerste lid over militaire operaties. Het betreft hier echter ‘slechts’ een verplichting ervoor te waken dat de burgerbevolking, de burgers en de burgerobjecten worden ontzien. Ontzien moet hier gelezen worden in de zin van “to spare, not to attack”,¹⁷⁹ zodat ook het eerste lid van artikel 57 gerelateerd lijkt aan aanvallen.

170 Verdrag inzake de bescherming van culturele goederen 1954, art 11 (2). Het 1999 *Second Hague Protocol* geeft in art. 13 (2) nadere aanwijzingen wanneer en door wie ‘onvermijdelijke militaire noodzaak’ mag worden vastgesteld.

171 Dinstein 2004 p. 160. *But the stark fact is that the status of special protection does not guarantee to any cultural object – not even of the greatest importance – genuine immunity from attack and destruction.*

172 Aanvullend Protocol I art. 12.

173 Aanvullend Protocol I sectie II, art. 21 t/m 31.

174 Aanvullend Protocol I art. 62.

175 Henckaerts & Doswald-Beck 2005, *Black letter rule* 15-24.

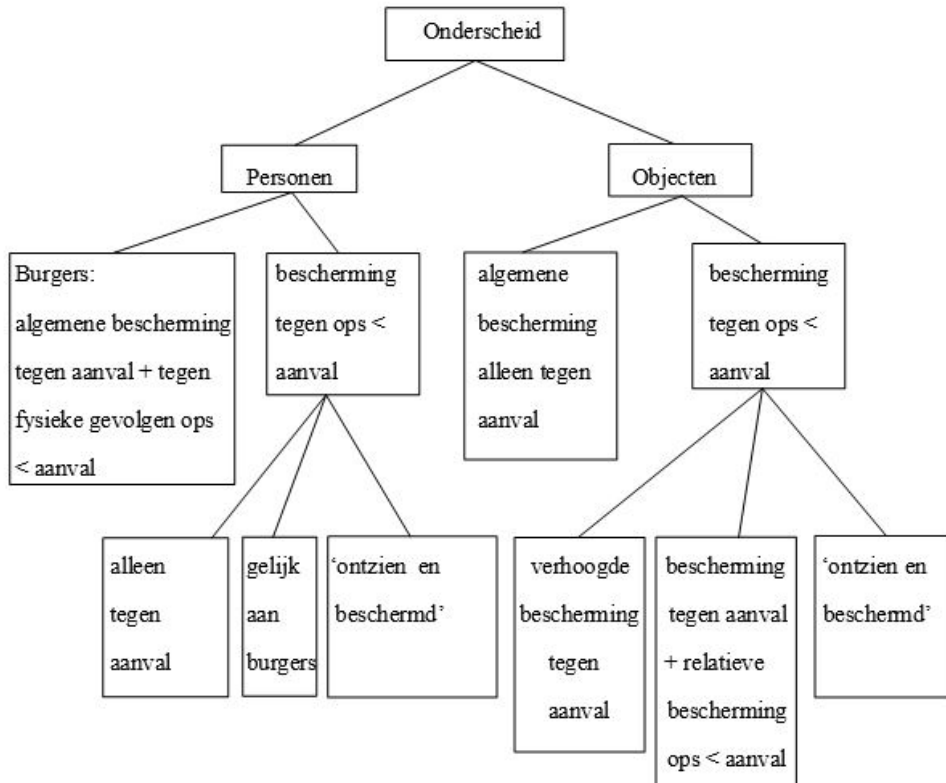
176 ICRC *Handbook on International rules governing military operations* 2013, p. 53.

177 Sandoz, Swinarski & Zimmerman 1987, p. 679.

178 Aanvullend Protocol I art. 57 lid 1, mijn accentuering.

179 Pictet 1953, p. 134, in dezelfde zin Sandoz, Swinarski & Zimmerman 1987, p. 146 en Bothe, Partch & Solf 1982, p. 108.

Mijn conclusie is daarmee dat de regels uit het humanitair oorlogsrecht die handelen over voorzorgsmaatregelen gelden voor aanvallen, beneden de drempel van aanval gelden ze niet.



Figuur 4 Samenvattend schema bescherming op basis van onderscheid.

3.3.3.6 Objecten en onbruikbaarmaking

Voordat ik doorga met het volgende grondbeginsel zal ik hier nog twee onderwerpen aanstippen die ik in het tweede deel van mijn onderzoek nader zal bezien, namelijk de betekenis van ‘object’ en van ‘onbruikbaarmaking’. Beide hebben te maken met de definitie van militair doel en zijn mogelijk aanleiding voor een aangepaste interpretatie in het cyberdomein. Omdat beide onderwerpen samenhangen met de definitie van militair doel dat weer in nauwe relatie staat tot het grondbeginsel onderscheid, heb ik besloten deze twee onderwerpen hier te bespreken. In dit hoofdstuk zal ik mijzelf beperken tot een uitleg in traditionele zin en antwoord geven op de vragen wat is een ‘object’ en wat moet worden verstaan onder ‘onbruikbaarmaking’? De volledige tekst van Aanvullend Protocol I artikel 52 lid 2 luidt: “Aanvallen dienen strikt tot militaire doelen te worden beperkt. Voor zover het

objecten betreft, zijn militaire doelen uitsluitend die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel oplevert.”¹⁸⁰

Allereerst het woordgebruik objecten (*objects*). Zowel het Engelse *objects* als het Franse *biens* verwijst naar zichtbare en tastbare objecten.¹⁸¹ Deze verwijzing naar zichtbare en tastbare objecten wordt bevestigd door de uitleg over het bredere begrip ‘militaire doelen’ (*military objectives*).¹⁸² De *Commentary* merkt hierover op: “*There is no doubt that in this article both the English and French texts intended tangible and visible things by the word ‘objective’*”¹⁸³ In beide gevallen, bij zowel ‘objecten’ als bij ‘militaire doelen’, gaat het dus om fysieke objecten. In traditionele zin levert dit weinig tot geen problemen op.

Een tweede onderwerp is de term ‘onbruikbaarmaking’ (*neutralization*). Hiermee wordt bedoeld het (tijdelijk) ontzeggen van gebruik van een object door de vijand zonder dat het daarvoor noodzakelijkerwijs geheel of gedeeltelijk vernietigd wordt.¹⁸⁴ Dit kan bijvoorbeeld door middel van het leggen van een mijnenveld of het beschieten van een artillerie-eenheid met anti-personeel munitie. De bedoeling van deze laatste actie is dat het personeel in dekking gaat, zodat de artillerie-eenheid tijdelijk niet operationeel is, zonder dat het militaire doel, de artillerie-eenheid, geheel of gedeeltelijk vernietigd wordt.¹⁸⁵ Beide voorbeelden zijn aanvallen in traditionele zin, daden van geweld, zodat dit niet tot interpretatieproblemen zal leiden. Dit wordt waarschijnlijk anders zodra andere methodes, zoals bijvoorbeeld ‘*jamming*’,¹⁸⁶ worden gebruikt voor tijdelijke onbruikbaarmaking.¹⁸⁷ Neem een radarvolgsysteem voor vliegtuigen dat wordt gebruikt voor het begeleiden van civiele vluchten, maar ook militaire vliegtuigen kan detecteren. Indien dat radarsysteem door middel van *jamming* tijdelijk niet meer kan functioneren, zodat een militair vliegtuig onopgemerkt een inlichtingenvlucht kan maken (de operatie is dus niet gericht op het fysiek beschadigen van het radarsysteem en heeft dit ook niet tot gevolg), is er dan sprake van een aanval?

■
180 Aanvullend Protocol I art. 52, lid 2. Voor wat betreft personen als militair doel verwijs ik naar de opmerking bij de bespreking van militair doel in Hoofdstuk 3 par. 3.3.3.

181 Sandoz, Swinarski & Zimmerman 1987, p. 634.

182 Naast objecten kunnen ook personen legitieme militaire doelen vormen. Zie Hoofdstuk 3 par. 3.3.3.

183 Sandoz, Swinarski & Zimmerman 1987, p. 634.

184 Bothe, Partch & Solf 1982, p. 325.

185 Voorbeelden ontleend aan Bothe, Partch & Solf 1982, p. 325.

186 *Jamming is the deliberate interference, caused by emissions intended to render unintelligible or falsify the whole or part of a wanted signal.* NATO GLOSSARY ON TERMS AND DEFINITIONS, Allied Administrative Publication AAP-06(2013) te raadplegen op <https://nso.nato.int/nso/zPublic/ap/aap6/AAP-6.pdf>.

187 *Jamming* komt ook meer overeen met de manier waarop onbruikbaarmaking in het cyberdomein toegepast kan worden. Ik kom daar in Hoofdstuk 4 op terug.

De laatst beschreven situatie heeft geleid tot twee denkrichtingen.¹⁸⁸ De eerste denkrichting gaat uit van de gedachte dat een aanval fysieke gevolgen moet hebben. Indien een militaire operatie dit niet heeft, is het geen aanval en komt het vraagstuk van militair doel niet aan de orde.¹⁸⁹ De andere denkrichting gaat uit van het standpunt dat militaire operaties alleen gericht mogen zijn tegen militaire doelen en omdat in de definitie van militaire doelen ook ‘onbruikbaarmaking’ is opgenomen, is de redentie dat het niet relevant is of een object onbruikbaar is gemaakt door vernieling of op een andere wijze.¹⁹⁰ In deze redentie is een militaire operatie die een systeem onbruikbaar maakt, zoals in het hierboven vermelde voorbeeld van het *jammen* van een radarsysteem, óók een aanval. De afwezigheid van fysieke schade is in deze redentie niet relevant.

Een aspect aan de tweede denkwijze maakt dat ik de eerste denkwijze als de betere beschouw. De tweede methode maakt mijns inziens een fout in de gevolgtrekking uit de volgorde en het taalgebruik van de bepalingen in Aanvullend Protocol I. Het klopt dat de algemene regel, gecodificeerd in artikel 48, bepaalt dat alle militaire operaties gericht moeten zijn tegen militaire doelen. Echter, in de daarop volgende uitwerking van militair doel in artikel 52 wordt een militair doel negatief gedefinieerd ten opzichte van een burgerobject¹⁹¹ dat niet mag worden aangevallen. Omdat ‘militaire operatie’ een breder begrip is dan ‘aanval’, is het onjuist conclusies over alle militaire operaties te trekken uit de definitie van militair doel gegeven in de context van aanval. Hierdoor worden militaire operaties die geen aanval zijn, mijns inziens, onterecht onder de noemer aanval geschaard. Zo zou het voorbeeld van het bezetten van een onverdedigde plaats zonder gebruikmaking van vuurkracht of andere daden van geweld volgens de tweede denkwijze ook als aanval gelden, terwijl dit niet zo is.¹⁹²

Mijn conclusie is dan ook dat onbruikbaarmaking ook kan zonder fysieke gevolgen. Deze definitie is echter alleen bruikbaar bij het bepalen of iets een militair doel is of niet. De definitie van militair doel mag niet gebruikt worden om een nadere interpretatie van het begrip ‘aanval’ te geven.¹⁹³ ‘Onbruikbaarmaking’ zonder fysieke gevolgen blijft in mijn conclusie dan ook beneden de drempel van aanval.

3.3.4 Proportionaliteit

De rol van het grondbeginsel proportionaliteit wordt vaak beperkt tot de proportionaliteitstest, zoals onder andere weergegeven in artikel 57 van aanvullend Protocol I.¹⁹⁴ Ik zal de gelijkschakeling van het grondbeginsel van proportionaliteit

■ 188 Schmitt (in Gill & Fleck) 2012, p. 246. Zie ook van Haaster 2018, p. 203.

189 Schmitt 2002, p. 381.

190 Dörmann 2004, p. 6. Ook ICRC 2015, p. 41. Opmerkelijk is dat in hetzelfde stuk op p. 42 gemeld wordt dat “*jamming of radio communications or television broadcasts has not traditionally been considered an attack in the sense of IHL.*”

191 Sandoz, Swinarski & Zimmerman 1987, p. 634.

192 Bothe, Partch & Solf 1982, p. 285.

193 Voor eenzelfde conclusie zie bijv.. Harrison-Dinniss 2012, p. 198. Schmitt 2013a, p. 95.

194 Sandoz, Swinarski & Zimmerman 1987, p. 683.

en de proportionaliteitsregel¹⁹⁵ hier vooralsnog volgen.¹⁹⁶ In dat geval kan ik voor dit onderzoek kort zijn; op militaire operaties beneden de drempel van aanval is de proportionaliteitsregel per definitie niet van toepassing.

Als eerste wordt de proportionaliteitsregel zowel binnen het internationaal gewoonterecht¹⁹⁷ als in Aanvullend Protocol I¹⁹⁸ gekoppeld aan de verplichting van een aanval af te zien, of een aanval af te breken, zodra kan worden verwacht dat deze bijkomende schade veroorzaakt die buitensporig is in verhouding tot het te verwachten militaire voordeel. Hier wordt telkenmale gesproken van *aanval* en niet van het bredere begrip (militaire) operaties. Als een militaire operatie niet kwalificeert als aanval, is deze regel daarom niet van toepassing.

Als tweede, en daarmee niet minder belangrijk, heb ik de ondergrens van aanval gedefinieerd als acties uitgevoerd met militairen en/of militaire middelen, die gericht zijn op fysiek letsel of schade of deze fysieke gevolgen hebben, welke in het kader van een gewapend conflict worden uitgevoerd met als doel een militair voordeel op de tegenstander te behalen. Omdat door deze definiëring van militaire operaties beneden de drempel van aanval geen fysieke schade kan ontstaan komt de proportionaliteitsregel, waarbij afgewogen moet worden of de bijkomende schade of letsel buitensporig is, juist vanwege het ontbreken van fysieke schade, niet aan de orde.

Eén zaak verdient hier nog bespreking, namelijk hoe zit het met geestelijk leed? Voor de bescherming van de burgerbevolking en individuele burgers bestaat één regel die verwijst naar de geestelijke component, namelijk het verbod op daden van geweld of bedreiging met geweld met als hoofddoel de burgerbevolking angst aan te jagen.¹⁹⁹ Deze regel is echter gerelateerd aan aanvallen.²⁰⁰ Een nadere beschouwing leert dat een analoge toepassing op operaties beneden de drempel van aanval niet voor de hand ligt.

Daden van geweld gerelateerd aan oorlogvoering zullen zonder twijfel aanleiding geven tot enige vorm van angst onder de bevolking of soms ook onder de leden van de krijgsmacht.²⁰¹ Tegen deze vorm van angst is het verbod echter niet gericht. Het verbod is gericht op daden van geweld met als hoofddoel (*primary purpose*) verspreiding van angst onder de burgerbevolking (zonder dat daar een substantieel militair voordeel tegenover

195 Zoals besproken in Hoofdstuk 2 par. 3.3.3.

196 In Hoofdstuk 5 zal ik nader terugkomen op het verschil tussen het grondbeginsel van proportionaliteit en de proportionaliteitsregel.

197 Henckarts & Doswald-Beck 2005, *Black letter rule* 14.

198 Aanvullend Protocol I art. 51 lid 5(b), art. 57 lid 2(a)(iii) en 57 lid 2(b)

199 Deze regel wordt gerekend tot het internationaal gewoonterecht, Henckarts & Doswald-Beck 2005, *Black letter rule* 2 en is gecodificeerd in Aanvullend Protocol I art. 51 lid 2.

200 Bothe, Partch & Solf 1982, p. 300, Aanvullend Protocol I art. 51 lid 2 spreekt van daden van geweld of dreiging met geweld hiermee refererend aan het woordgebruik in de definitie van aanval uit art. 49 Aanvullend Protocol I.

201 Sandoz, Swinarski & Zimmerman 1987, p. 618.

staat).²⁰² Angst als bijverschijnsel ten gevolge van aanvallen is niet onrechtmatig, ook niet als die angst, als gevolg van bijvoorbeeld grootschalige luchtbombardementen die leiden tot omvangrijke vernietiging van militaire eenheden en doelen, de burgerbevolking doodsbang maakt.²⁰³ Met andere woorden, niet de mate van angst maar de *doelstelling* van de aanval is bepalend. Analoge toepassing van deze regel op operaties beneden de drempel van aanval betekent dat de doelstelling van een operatie die geen fysieke gevolgen mag hebben,²⁰⁴ het zaaien van angst zou moeten zijn. Juist vanwege het ontbreken van fysieke gevolgen acht ik dit niet realistisch. Datzelfde geldt voor het dreigen met een operatie die niet zal leiden tot fysieke gevolgen.²⁰⁵

3.3.5 Eervol gedrag als grondbeginsel

Hoewel eervol gedrag niet altijd meer gezien wordt als een grondbeginsel, is het beginsel al heel lang onderdeel van het humanitair oorlogsrecht.²⁰⁶ In de benaming eervol gedrag (*chivalry*) is een verwijzing te zien naar de in de Middeleeuwen geldende riddercode met een aantal strikte principes. Zo moesten vrouwen, kinderen en ouderen beschermd worden tegen de vijandelijkheden en moest een vijandelijke ridder als gelijke worden beschouwd die alleen in een eervol gevecht mocht worden verslagen.²⁰⁷

In het hedendaagse humanitair oorlogsrecht zijn veel regels die volgen uit dit beginsel terug te vinden in verdragsrechtelijke regels,²⁰⁸ waaronder een verbod op perfidie,²⁰⁹ het ongepast gebruik maken van erkende kentekenen²¹⁰ en het verbod op nationaliteitsteken van bepaalde staten.²¹¹ Deze regels appelleren namelijk aan het vertrouwen van de combattant, wat een fundamentele voorwaarde is voor het bestaan van recht.²¹² Toch kan het grondbeginsel ook buiten de gecodificeerde regels nog invloed hebben, namelijk als hulpmiddel bij de uitleg van gecodificeerde regels of om hiaten te vullen mochten deze bestaan.²¹³ Twee voorbeelden kunnen dit verduidelijken.

202 Sandoz, Swinarski & Zimmerman 1987, p. 618.

203 Dinstein 2004, p. 216.

204 Dan zou de operatie namelijk niet meer voldoen aan de definitie van militaire operatie beneden de drempel van aanval.

205 Dit in tegenstelling tot het dreigen met een operatie die wel fysieke gevolgen hebben. Zo kan het dreigen met vergiftiging van het drinkwater of een gerucht verspreiden dat het drinkwater besmet is, best de *bedoeling* hebben om angst te zaaien.

206 *US-Operational law Handbook* (ed 2014) p. 14. Gill (in Mathee, Toebe & Brus) 2013 p. 34.

207 O'Connell (in Fleck) 2013a, p. 112.

208 Al heeft deze codificatie wel een prijs: zie Watts 2014, p. 108: "The price of doctrinal clarity has been reduced attention and fidelity to good faith conduct of hostilities critical to humane combat and to sustaining the law-of-war as a trusted means of communication and interaction between belligerents."

209 Aanvullend Protocol I art. 37.

210 Aanvullend Protocol I art. 38.

211 Aanvullend Protocol I art. 39.

212 Sandoz, Swinarski & Zimmerman 1987, p. 473.

213 Gill (in Mathee, Toebe & Brus) 2013, p. 44.

Neem het verbod op het niet-verlenen van kwartier.²¹⁴ Stel dat in een gevecht de tegenstander zich in een hopeloze positie bevindt. Moet het verbod op niet-verlenen van kwartier zo geïnterpreteerd worden dat in een dergelijke situatie de verplichting bestaat om de tegenstander aan te bieden zich over te geven?²¹⁵ Een ander voorbeeld is de zogenaamde *kill-wound* discussie naar aanleiding van de vraag of het humanitair oorlogsrecht een regel kent die voorschrijft dat, indien een keuze bestaat tussen middelen om een vijandelijke combattant uit te schakelen, het voor die combattant minst nadelige middel moet worden gekozen.²¹⁶

Bij beide voorbeelden is de vraag of een juridische verplichting binnen het humanitair oorlogsrecht bestaat. De meningen hierover zijn verdeeld.²¹⁷ Bij de aanhangers van afwezigheid van een juridische verplichting kan het beginsel van eervol gedrag een betekenis hebben bij de uitleg van het humanitair oorlogsrecht. De effectiviteit van de regels van het humanitair oorlogsrecht hangt namelijk in sterke mate af van de goeder trouw van de strijdkrachten en van hun wil de vereisten van humaniteit toe te passen.²¹⁸ Anders verwoord, vanuit het humanitair oorlogsrecht gezien bestaat de verplichting niet als juridisch principe of regel, als moreel principe is een dergelijke verplichting wel aanwezig.²¹⁹ Tot een soortgelijke conclusie komt Gill, maar dan met eervol gedrag als grondbeginsel, niet in de zin van een juridisch principe maar in de zin van een niet-juridische overweging.²²⁰

Terug naar de voorbeelden. Houdt het verbod op het niet-verlenen van kwartier tevens een verplichting in tot het aanbieden van overgave aan een tegenstander die zich in een hopeloze positie bevindt? Moet, in geval van keuze, het voor de tegenstander minst nadelige middel gekozen worden? Al zijn deze handelingen mogelijk in strijd met het grondbeginsel van eervol gedrag, het niet aanbieden van overgave, of doden in plaats van verwonden, zal in elk geval niet kunnen leiden tot vervolging en berechting voor een oorlogsmisdrijf door een gerecht of tribunaal. Dit vanwege het ontbreken van de codificatie als “ernstige inbreuk” op het humanitair oorlogsrecht. Oneervol gedrag dat niet tevens een andere regel uit het humanitair oorlogsrecht overtreedt, kan een inbreuk op het humanitair oorlogsrecht zijn indien dat gedrag “*can and should lead to administrative, disciplinary or even*

214 Aanvullend Protocol I art. 40: “Het is verboden het bevel te geven dat niemand mag overleven, een tegenstander daarmee te dreigen of op die grondslag de vijandelikheden te bedrijven.”

215 Zie bijv. Interpretive Guidance 2009, p. 82: “In sum, while operating forces can hardly be required to take additional risks for themselves or the civilian population in order to capture an armed adversary alive, it would defy basic notions of humanity to kill an adversary or to refrain from giving him or her an opportunity to surrender where there manifestly is no necessity for the use of lethal force.”

216 Ook wel aangeduid als de Pictet-theorie verwijzend naar de beroemde uitspraak van Pictet: “if we can put a soldier out of action by capturing him, we should not wound him; if we can obtain the same result by wounding him, we must not kill him. If there are two means to achieve the same military advantage, we must choose the one which causes the lesser evil”. Pictet 1985, p. 75.

217 Voorbeelden van schrijvers die een juridische verplichting in het humanitair oorlogsrecht aanwezig achten zijn Pictet 1985 en Goodman 2013, schrijvers die de aanwezigheid van een dergelijke verplichting ontkennen zijn bijvoorbeeld Henderson 2009 en Schmitt 2013.

218 Sandoz, Swinarski & Zimmerman 1987, p. 589.

219 Henderson 2009, p. 87.

220 Gill (in Matthee, Toebes & Brus) 2013, p. 45.

*penal sanctions in accordance with the general principle that every punishment should be proportional to the severity of the breach.*²²¹ Juist omdat “significant elements [of chivalry and honorable conduct] have found their way into treaty and customary law”,²²² acht ik een dergelijke inbreuk op het humanitair oorlogsrecht op basis van het grondbeginsel ‘eervol gedrag’ niet mogelijk. In die zin zie ik geen juridische verplichting.

Dit neemt niet weg dat mogelijk een morele verplichting niet is nagekomen. Degene die hiertoe besloot zal dit enerzijds richting zichzelf moeten verantwoorden, terwijl het besluit anderzijds ook kan leiden tot verontwaardiging, of zelfs afkeur, door mede-combattanten of de publieke opinie. Ook deze vooruitzichten, anders dan juridische gevolgen, zullen de besluiten van een combattant beïnvloeden, of zoals Gill het verwoordt “non-binding moral obligations and traditions can also act as a powerful incentive for particular conduct.”²²³

Wat betekent bovenstaande voor het grondbeginsel ‘eervol gedrag’ in het humanitair oorlogsrecht en dan met name, in hoeverre is het ook van toepassing beneden de drempel van aanval?

Allereerst is de toepassing van ‘eervol gedrag’ niet beperkt tot het gebruik van geweld. Het grondbeginsel leidt in een aantal gevallen juist tot matiging of geheel achterwege laten van geweld, zodat dit grondbeginsel ook van toepassing is beneden de drempel van aanval. Het aanbieden van een mogelijkheid tot overgave in plaats van een aanval is hier een sprekend voorbeeld van. Het grondbeginsel is van invloed geweest op de codificatie van regels, waarvan ik een aantal hieronder in meer detail zal bespreken. Bij de interpretatie van die regels kan ik terugvallen op dit grondbeginsel, zoals hiervoor opgemerkt, ook beneden de drempel van aanval.

Naast deze juridische betekenis kan het grondbeginsel ‘eervol gedrag’ tevens een bijdrage leveren aan andere vraagstukken, bijvoorbeeld morele of operationele, en het is in die hoedanigheid ook van toepassing beneden de drempel van aanval. Hiermee doel ik op het feit dat het merendeel van de regels van het humanitair oorlogsrecht focust op de fysieke gevolgen van militaire operaties (dood, verwonding en vernieling, met andere woorden de gevolgen van aanvallen) en veel minder op de gevolgen van militaire operaties beneden de drempel van aanval. Bij gebrek aan regels, of onduidelijkheid over de toepasselijkheid van deze regels op militaire operaties die geen aanval zijn, kan het grondbeginsel van ‘eervol gedrag’ helpen bij het vinden van een oplossing. In deze laatste betekenis levert het echter geen juridische bindende verplichtingen op.²²⁴

■
221 Sandoz, Swinarski & Zimmerman 1987, p. 975.

222 Gill (in Matthee, Toebe & Brus) 2013, p. 41.

223 Gill (in Matthee, Toebe & Brus) 2013, p. 46.

224 Men kan erover discussiëren of in dergelijke gevallen wel sprake is van een ‘regel’. Van Dale geeft als beschrijving voor ‘regel’ onder andere: “Bepaling waarnaar met zich richten moet, vastgestelde of aanvaarde norm” (Groot Woordenboek der Nederlandse Taal, vijftiende herziene druk 2015). Dit gaat breder dan alleen het hebben van (juridische) consequenties bij niet-nakomen van de regel.

Overigens kan het voorkomen dat de juridische, morele en operationele invloed van ‘eervol gedrag’ tegelijkertijd spelen. Neem het eerder aangehaalde voorbeeld van de proportionaliteitsregel uit artikel 51 Aanvullend Protocol I.²²⁵ Eerder werd al aangegeven dat de verantwoordelijke commandant een behoorlijke beoordelingsvrijheid heeft.²²⁶ In zijn juridische beoordeling moet de commandant bepalen of een aanval niet-onderscheidend is. Dit laatste is het geval als het te verwachten bijkomend verlies onder de burgerbevolking of schade aan burgerobjecten buitensporig is in verhouding tot het verwachte tastbare en rechtstreekse militaire voordeel.²²⁷ Bij de bepaling van wat de commandant als buitensporig beschouwt, zal hij zeker operationele, maar ook morele argumenten, meenemen.²²⁸ ‘Eervol gedrag’ komt hier via meerdere invalshoeken, gelijktijdig, terug.

Met deze conclusie over ‘eervol gedrag’ als grondbeginsel zal ik nu een drietal regels die gebaseerd zijn op dit grondbeginsel nader bezien met het oog op hun toepasselijkheid op militaire operaties beneden de drempel van aanval. Het betreft de regels over perfidie, erkende kentekenen en nationaliteitstekenen, die zijn gecodificeerd in de artikelen 37, 38 en 39 van Aanvullend Protocol I.²²⁹

3.3.5.1 Perfidie

Het verbod op perfidie zoals verwoord in artikel 37 Aanvullend Protocol I is ook van toepassing op militaire operaties beneden de drempel van aanval, zij het dat het daarbij gaat om hele specifieke, en daarmee waarschijnlijk weinig voorkomende, operaties. Ik kom tot deze conclusie op basis van de volgende redenering. Artikel 37 verbiedt een tegenstander te doden, te verwonden of gevangen te nemen door middel van perfidie, om vervolgens perfidie te definiëren als “gedragingen die het vertrouwen wekken bij een tegenstander ten einde deze te doen geloven dat hij gerechtigd is tot bescherming krachtens de regels van het volkenrecht toepasselijk in geval van gewapende conflicten of dat hij verplicht is zodanige bescherming te verlenen, met de bedoeling dat vertrouwen te misbruiken.”²³⁰ De definitie van perfidie is daarmee ruim omschreven, echter artikel 37 verbiedt alleen het doden, verwonden of gevangen nemen van een tegenstander door middel van perfidie, daarmee voortbordurend op artikel 23(b) van Haagse Conventie IV.²³¹ Hiermee is het verbod op perfidie in essentie beperkt tot aanvallen, wat evident is uit de context en de lijst van

■
225 Zie Hoofdstuk 2 par. 2.3.3.

226 Sandoz, Swinarski & Zimmermann 1987, p. 684. Dinstein 2009b, Ez8 “a great deal of latitude.”

227 Aanvullend Protocol I art. 51 lid 5b.

228 Van een commandant wordt hierbij verwacht te besluiten met “common sense and good faith.” Sandoz, Swinarski & Zimmermann 1987, p. 683.

229 Alhoewel ook andere regels gerelateerd zijn aan het grondbeginsel van eervol gedrag (Sandoz, Swinarski & Zimmermann 1987, p. 430) beperk ik mij hier tot de regels die gebaseerd zijn op dit grondbeginsel. Veel regels zijn namelijk gerelateerd aan meer dan één grondbeginsel.

230 Aanvullend Protocol I art. 37.

231 Art. 23(b) luidt; “Behalve de verbodsbepalingen door bijzondere verdragen vastgesteld, is met name ontzegd: personen behorende tot het vijandelijk volk of leger, verraderlijk te doden of te verwonden.”

voorbeelden.²³² Het is geen verbod van perfidie *per se*, zoals de titel van dit artikel zou kunnen suggereren, maar slechts het verbod op een “*particular category of acts of perfidy*.”²³³

Of andere vormen van perfidie, die niet vallen onder het verbod artikel 37,²³⁴ wel geoorloofd zijn, is onderwerp van een langlopende discussie tussen wetenschappers²³⁵ en wordt veroorzaakt doordat “*two modes of law-of-war regulation, specific provision and general principle, have not been distinct in terms of coverage*.”²³⁶ Aan de ene kant kan als uiterste opvatting genoemd worden dat perfidie alleen verboden is als het daadwerkelijk leidt tot dood, verwonding of gevangenneming van een tegenstander. Zo is sabotage of vernietiging van vijandig materieel door middel van perfidie in deze zienswijze niet verboden.²³⁷ Aan de andere uiterste zijde staat de opvatting dat perfidie *per se* verboden is.²³⁸ Uit de wetenschappelijke discussie mag men de conclusie trekken dat een grijs gebied is blijven bestaan tussen verboden perfidie en toegestane krijgslisten²³⁹ ondanks het feit dat de doelstelling van Aanvullend Protocol I juist was “*to reaffirm the prohibitions of Hague Regulations, Art. 23(b), as unambiguously as possible, and to illustrate examples of prohibited perfidy in order to further clarify the definition and to distinguish perfidy from permissible ruses*.”²⁴⁰

Al bij de totstandkoming van artikel 37 was duidelijk dat het onderscheid tussen verboden perfidie en toegestane krijgslisten lastig zou zijn omdat de experts het eens waren over het feit dat het verbod op perfidie uit de Haagse Conventie IV een bevestiging nodig had in Aanvullend Protocol I. Of dit kwam door een afname in respect voor het internationaal recht of door afname in het moreel besef, bleef daarbij onduidelijk.²⁴¹ De discussie vertoont daarmee gelijkenis met de discussie over de hiervoor genoemde voorbeelden van de verplichting tot aanbieden van overgave of het aanwenden van het voor de tegenstander minst nadelige middel.²⁴²

Deze constatering is van belang voor een antwoord op de vraag of het verbod op perfidie ook geldt voor militaire operaties beneden de drempel van aanval. Als de perfidie tot doel

■
232 Sandoz, Swinarski & Zimmerman 1987, p. 433.

233 Sandoz, Swinarski & Zimmerman 1987, p. 432.

234 Deze andere vormen van perfidie voldoen wel aan de definitie van perfidie zoals genoemd in Aanvullend Protocol I, art. 37 maar leiden niet tot dood, verwonding of gevangenneming van een tegenstander.

235 Rusinova 2011, p. 3-11.

236 Watts 2014, p. 123.

237 Aan deze zijde van de discussie bevinden zich bijvoorbeeld Bothe (in Bothe Parch & Solf) 1982, p. 204, en Oeter (in Fleck) 2013a, p. 225.

238 Tot deze zijde behoren bijvoorbeeld Sandoz, Swinarski & Zimmerman 1987, p. 433, Rusinova 2011, F-21 al geeft deze laatste toe dat in de praktijk ook steun is voor een strikte uitleg van de bewoordingen van art 37 lid 1 en Doswald-Beck 2015, *San Remo Manual on International Law Applicable to Armed Conflict at Sea*, p. 29, par. 11.

239 Sandoz, Swinarski & Zimmerman 1987, p. 433

240 Bothe, Parch & Solf 1982, p. 203. Zie ook Watts 2014, p. 124: *While splitting the jus in bello between specific prohibitions and broad principles has offered States regulatory diversity and flexibility, the arrangement has rendered many of the precise contours of the law illusive.*

241 Sandoz, Swinarski & Zimmerman 1987, p. 431.

242 Zie par. 3.3.5.

heeft een tegenstander te doden of te verwonden, of dit tot gevolg heeft, zal sprake zijn van een aanval in de zin van artikel 49 Aanvullend Protocol I zodat ik deze situatie hier verder niet hoeft te bespreken. Ook indien alleen materiële schade wordt toegebracht door middel van perfidie, een onderdeel van de discussie binnen het grijze gebied, zal dit onder de definitie van aanval, en daarmee buiten het bereik van dit onderzoek vallen.²⁴³

Als daarentegen het resultaat van de op perfidie gebaseerde militaire operatie ‘slechts’ gevangenneming van een tegenstander tot gevolg heeft, bijvoorbeeld een militaire operatie waarbij militairen zich voordoen als een medisch team dat vervolgens onder het voorwendsel van overplaatsing een patiënt meeneemt en vervolgens gevangen neemt, is het verbod op perfidie geschonden terwijl de militaire operatie beneden de drempel van aanval blijft.²⁴⁴ Hierbij merk ik op dat het verbod op perfidie resulterend in gevangenneming niet algemeen erkend is als gewoonterecht²⁴⁵ en daarmee alleen geldt voor staten die Aanvullend Protocol I hebben geratificeerd.

3.3.5.2 Erkende kentekenen

Artikel 38 Aanvullend Protocol I verbiedt het ongepast gebruik van een aantal erkende kentekenen zoals het kenteken van het Rode Kruis, de Rode Halve Maan, de Rode Leeuw en Zon, alsmede andere kentekenen, tekens of seinen als voorzien in de Verdragen van Genève of in de aanvullende Protocollen.²⁴⁶ Het is in een gewapend conflict eveneens verboden opzettelijk misbruik te maken van internationaal erkende beschermende kentekenen, tekens of seinen daaronder begrepen de parlementaire vlag en het beschermende kenteken van culturele goederen. Lid 2 van dit artikel verbiedt vervolgens het gebruik van het kenteken van de Verenigde Naties zonder toestemming van die organisatie.

²⁴³ Dit laatste geval, toebrengen van materiële schade door gebruik van perfidie, zou ik in navolging van mijn ingenomen positie over ‘eervol gedrag’ willen kwalificeren als een daad die weliswaar geen juridische gevolgen heeft, maar wel in strijd is met het grondbeginsel van eervol gedrag.

²⁴⁴ Zij het dat het erop lijkt dat dit minder ernstig wordt aangerekend dan andere vormen van perfidie. Zo wordt op basis van Aanvullend Protocol I art 85, lid 3 (f) het perfide gebruik, in strijd met artikel 37, van het kenteken van het Rode Kruis, de Rode Halve Maan of de Rode Leeuw en Zon of van andere door de Verdragen en Aanvullend Protocol I erkende beschermde tekens gezien als een ernstige inbreuk op het Protocol, en daarmee beschouwd als oorlogsmisdrijf (art 85 lid 5), echter alleen indien het perfide gebruik de dood of ernstig lichamelijk letsel met zich mee heeft gebracht dan wel de gezondheid in ernstige mate benadeeld heeft (artikel 85 lid 3 aanhef). Perfidie gebruik van beschermde tekens om een tegenstander gevangen te nemen zonder dat daarbij doden of gewonden vallen wordt derhalve niet aangemerkt als een ernstige inbreuk. Ook Internationaal Strafhof, Statuut van Rome 1998, art 8 (2)(b)(xi) spreekt alleen over het “op verraderlijke wijze doden of verwonden van personen” als oorlogsmisdrijf.

²⁴⁵ In de ICRC studie wordt deze regel wel gerekend tot het gewoonterecht, zie Henckaerts & Doswald-Beck 2005, *Black letter rule* 65, p. 221. Het verbod op gevangenneming door middel van perfidie wordt door het ICRC wel gezien als gewoonterecht maar overtreding levert geen oorlogsmisdaad op in tegenstelling tot dood of verwonding door perfidie, Henckaerts & Doswald-Beck 2005, p. 225. Voor een afwijkende mening, zie bijvoorbeeld Schmitt 2013, p. 181, waarin een meerderheid van de experts van mening was dat het internationaal gewoonterecht alleen daden van perfidie verbiedt die resulteren in, of gericht zijn op, dood of verwonding. Zie bijv. ook DoD war Manual 2016, p. 320 “It may not be prohibited to invite the confidence of the adversary that he or she is obligated to accord protection under the law of war, for certain purposes (e.g., to facilitate spying, sabotage, capturing enemy personnel, or evading enemy forces).” Mijn accentuering.

²⁴⁶ Met de totstandkoming van het Aanvullend Protocol III is het Rode Kristal toegevoegd als aanvullend onderscheidend embleem.

Anders dan het verbod op perfidie is het verbod op ongepast gebruik van erkende kentekenen een absoluut verbod.²⁴⁷ Zo is het ongepast gebruik van bijvoorbeeld het Rode Kruis verboden en een overtreding van dit verbod is een inbreuk op het humanitair oorlogsrecht. Geschiedt het misbruik om een tegenstander te doden, te verwonden of gevangen te nemen dan is bovendien sprake van perfidie zoals besproken in de vorige paragraaf, zodat misbruik in dat geval een ernstige inbreuk op het humanitair oorlogsrecht oplevert,²⁴⁸ oftewel een oorlogsmisdrijf.²⁴⁹

Vanwege het absolute karakter van het verbod als verwoord in artikel 38 geldt dit verbod, dat gerekend wordt tot het gewoonterecht,²⁵⁰ voor alle militaire operaties, dus ook voor operaties beneden de drempel van aanval.

3.3.5.3 Nationaliteitstekenen

Artikel 39 Aanvullend Protocol I, handelend over nationaliteitskentekenen, maakt onderscheid tussen nationaliteitskentekenen van neutrale staten en staten die geen partij zijn bij het conflict (lid 1) en nationaliteitskentekenen van de tegenpartijen (lid 2). Onder nationaliteitstekenen worden in beide gevallen genoemd vlaggen of militaire kentekenen, onderscheidingstekens en uniformen. Lid 3 bepaalt dat de bestaande en algemeen erkende regels van het volkenrecht met betrekking tot spionage of het gebruik van vlaggen tijdens een gewapend conflict op zee van kracht blijven en niet gewijzigd worden door dit artikel.

Lid 1 van artikel 39 bepaalt dat het verboden is in een gewapend conflict gebruik te maken van de genoemde kentekenen van neutrale staten of andere staten die geen partij zijn bij het conflict. Dit is een codificatie van internationaal gewoonterecht en verbiedt *“any use by a Party to the conflict of neutral symbols or uniforms during the armed conflict, whether in an attack or any other military operation to promote the interest of a Party to the conflict.”*²⁵¹ Dit verbod is absoluut in een gewapend conflict, maar betekent ook dat *“they may be used as long as they are not used for the promotion of the interests of a Party to the conflict,”*²⁵² dus bijvoorbeeld wel voor diplomatieke missies, humanitaire hulpverlening door een neutrale staat etc.²⁵³ Bij militaire operaties, uitgevoerd in het kader van een gewapend conflict, zal het echter voor de strijdende partijen verboden zijn gebruik te maken van neutrale nationaliteitstekenen, ook waar het operaties beneden de drempel van aanval betreft. Het is hierbij van belang op te merken dat dit niet geldt voor een gewapend conflict op zee. Op zee geldt dat *“according to custom, it is permissible for a warship to fly false colours in order to deceive an enemy, provided that prior to going into*

247 Sandoz, Swinarski & Zimmerman 1987, p. 448.

248 Aanvullend Protocol I art. 85 lid 3 (f).

249 Aanvullend Protocol I art. 85, lid 5.

250 Henckaerts & Doswald-Beck 2005, p. 203-212, *Black letter rule* 58, 59, 60 and 61, handelend over respectievelijk de witte vlag, onderscheidende kentekenen van de Verdragen van Genève, het ongeautoriseerde gebruik van het embleem en uniform van de Verenigde Naties en het ongepast gebruik van internationaal erkende kentekenen.

251 Bothe, Partch & Solf 1982, p. 213.

252 Sandoz, Swinarski & Zimmerman 1987, p. 463.

253 Sandoz, Swinarski & Zimmerman 1987, p. 471.

action such a warship shows her true colours."²⁵⁴ In het tweede deel van mijn onderzoek zal ik nog terugkomen over een mogelijke analoge toepassing van dit principe op militaire operaties in het cyberdomein.

Lid 2 van artikel 39 bepaalt dat het verboden is de nationaliteitskentekenen van de tegenpartijen te gebruiken tijdens aanvallen of met het oogmerk militaire operaties te dekken, te begunstigen, te beschermen of te belemmeren. Deze constructie is een compromis tussen twee stromingen die waren ontstaan bij de uitleg van artikel 23(f) van Hague Convention IV 1907 dat het onrechtmatig gebruik (*improper use*) van de nationale vlag, militaire onderscheidingstekenen of uniform van de vijand verbood. Aan de ene kant bestond de stroming die vond dat het gebruik van vijandelijke kentekenen slechts tijdens de daadwerkelijke gevechten verboden was maar daarbuiten een legitieme krijgslist vormde, in analogie met het gewapend conflict op zee. Aan de andere kant bevond zich de stroming die vond dat elk gebruik dat leidt tot een voordeel over de tegenstander verboden was.²⁵⁵ Artikel 39 lid 2 had de bedoeling een einde te maken aan deze discussie. Over het succes daarvan blijven de meningen echter verdeeld.²⁵⁶

Door de toevoeging van de bepaling dat het gebruik van nationaliteitskentekenen van de tegenpartijen niet alleen verboden is tijdens aanvallen, maar ook indien dit geschiedt "met het oogmerk militaire operaties te dekken, te begunstigen, te beschermen of te belemmeren"²⁵⁷ is duidelijk dat het verbod, in elk geval voor partijen bij Aanvullend Protocol I,²⁵⁸ verder gaat dan het gebruik tijdens aanvallen. Ik heb militaire operaties gedefinieerd als acties uitgevoerd door militairen en/of met militaire middelen gericht op het behalen van een militair voordeel op de tegenstander.²⁵⁹ Vanwege de grote overlap die ik zie tussen 'militaire operaties dekken, begunstigen, beschermen of belemmeren' en 'militair voordeel behalen op de tegenstander' kan ik concluderen dat het gebruik van nationaliteitskentekenen van de tegenpartij of tegenpartijen ook verboden is bij militaire operaties beneden de drempel van aanval.

Nog wel interessant voor dit onderzoek is de opmerking dat de term "vlaggen, militaire kentekenen, onderscheidingstekens of uniformen" alleen van toepassing is op concreet zichtbare objecten.²⁶⁰ Het verbod geldt niet voor de krijgslist van het gebruik van codes,

254 Bothe, Partch & Solf 1982, p. 212. Zie ook Doswald-Beck 2015, p. 184.

255 Bothe, Partch & Solf 1982, p. 213.

256 Zie bijv.. Sandoz, Swinarski & Zimmerman 1987, p. 466, "this text, ..., put an end to the longstanding uncertainty arising from both the imprecise text of the Hague, and from unclear customary law." Een andere mening is te vinden in Bothe, Partch & Solf 1982, p. 214, "the boundary between forbidden and permissible uses is not very distinct" gevolgd door een aantal voorbeelden van "probably prohibited" en "probably unprohibited uses."

257 Aanvullend Protocol I art. 39 lid 2.

258 Het verbod vloeit niet voort uit het gewoonterecht. Henckaerts & Doswald-Beck, 2005, p. 216. "It cannot be concluded that the wearing of enemy uniforms outside combat would be improper."

259 Zie Hoofdstuk 2, par. 2.6.5.

260 Bothe, Partch & Solf 1982, p. 214.

wachtwoorden of bevestigingstekens van de tegenstander ter ondersteuning van een militaire operatie.²⁶¹ Ik zal hier in het tweede deel van mijn onderzoek dieper op ingaan.

Over nationaliteitskentekenen kan ik de conclusie trekken dat het verbod op gebruik van nationaliteitskentekenen van neutrale staten of staten die geen partij zijn bij het conflict ook van toepassing is op militaire operaties beneden de drempel van aanval. Deze regel wordt gerekend tot het gewoonterecht.²⁶² Het gebruik van nationaliteitskentekenen van de tegenpartij tijdens aanvallen is verboden. Deze regel wordt ook gerekend tot het gewoonterecht.²⁶³ Het verbod geldt ook voor militaire operaties beneden de drempel van aanval, al wordt deze conclusie niet door iedereen gedeeld.²⁶⁴

3.4 Regels uit het humanitair oorlogsrecht van toepassing op militaire operaties die de drempel van aanval niet halen

Aan het eind van dit hoofdstuk is het tijd de deelvraag, welke regels uit het humanitair oorlogsrecht van toepassing zijn op militaire operaties die de drempel van aanval niet halen, te beantwoorden. Ik doe dit aan de hand van de grondbeginselen van het humanitair oorlogsrecht waarbij de door mij gegeven regels, gebaseerd op een grondbeginsel, bedoeld zijn ter verduidelijking.

3.4.1 Militaire noodzaak

Militaire noodzaak als grondbeginsel van het humanitair oorlogsrecht is van toepassing op alle militaire operaties en daarmee ook op militaire operaties beneden de drempel van aanval, met de nuance dat dit alleen voor de laatstgenoemde geldt indien negatieve gevolgen voor de burgerbevolking, individuele burgers of burgerobjecten zijn te voorzien.

3.4.2 Humaniteit

Humaniteit als grondbeginsel is terug te vinden in vrijwel het gehele humanitair oorlogsrecht en is van toepassing op het hele spectrum van militaire operaties, ook die beneden de drempel van aanval. Als voorbeeld noem ik het beginsel van beperking, dat rechtstreeks is gebaseerd op het grondbeginsel van humaniteit. Twee regels die daaruit voortvloeien, de regel dat de keuze van middelen en methoden van oorlogvoering niet onbegrensd is en de regel die het veroorzaken van overbodig letsel en onnodig leed verbiedt, zijn onverkort van kracht op operaties beneden de drempel van aanval. Voor de

261 Bothe, Partch & Solf 1982, p. 214.

262 Henckaerts & Doswald-Beck 2005, p. 218, *Black letter rule* 63. "Use of the flags or military emblems, insignia or uniforms of neutral or other States not party to the conflict is prohibited."

263 Henckaerts & Doswald-Beck 2005, p. 213, *Black letter rule* 62. "Improper use of the flags or military emblems, insignia or uniforms of the adversary is prohibited."

264 Zo stelt de USA (geen partij bij Aanvullend Protocol I), "It is a legitimate ruse to use enemy flags, insignia, and military uniforms outside of combat." DoD Law of War Manual 2016, p. 323.

laatste geldt wel de opmerking dat, vanwege de definitie van aanval, alleen het gedeelte over onnodig leed van belang is. Omdat de beperking van deze regel geldt ten aanzien van vijandelijke combattanten, waarbij onnodig leed nog onderscheiden moet worden van noodzakelijk leed, schat ik in dat de bruikbaarheid van deze regel beneden de drempel van aanval alleen theoretisch is.

3.4.3 Onderscheid

De grondregel van onderscheid, waarbij partijen bij een gewapend conflict onderscheid moeten maken tussen de burgerbevolking en combattanten en tussen burger- en militaire objecten is ook van kracht beneden de drempel van aanval. Hierbij bestaat wel verschil tussen de toepassing van deze regel bij personen en objecten.

Het grondbeginsel van onderscheid van de burgerbevolking en afzonderlijke burgers is van toepassing voor militaire operaties beneden de drempel van aanval. Dit grondbeginsel leidt daarbij, in tegenstelling tot aanvallen, niet tot een algemeen verbod. Zolang burgers niet worden blootgesteld aan fysieke gevaren voortvloeiend uit die operaties mogen militaire operaties beneden de drempel van aanval gericht zijn op burgers.

Als algemene regel geldt dat burgerobjecten beschermd zijn tegen aanvallen, maar dat ze wel gebruikt mogen worden voor militaire operaties beneden de drempel van aanval.

Voor culturele objecten geldt dat ze niet gebruikt mogen worden voor militaire operaties beneden de drempel van aanval indien het object door deze operaties aan gevaar voor vernietiging of beschadiging wordt blootgesteld.

Een bijzondere regel van bescherming, mede gebaseerd op onderscheid, geldt voor zieken, gewonden en schipbreukelingen en personeel en materieel met een humanitaire functie. Zij worden beschermd tegen zowel aanvallen als alle andere militaire operaties gericht op het verstoren van het humanitair optreden of functioneren, of die dit optreden of functioneren negatief beïnvloeden.

3.4.4 Proportionaliteit

De proportionaliteitsregel uit het humanitair oorlogsrecht geldt niet voor militaire operaties beneden de drempel van aanval.

3.4.5 Eervol gedrag

Eervol gedrag als grondbeginsel is niet beperkt tot daden van geweld en is daarom ook van toepassing beneden de drempel van aanval. Het grondbeginsel kan in juridische zin een rol spelen bij de interpretatie van bestaande regels. Daarnaast kan het grondbeginsel een bijdrage leveren bij morele of operationele vraagstukken en is in die hoedanigheid ook van toepassing beneden de drempel van aanval. In deze laatste betekenis levert het echter geen juridische bindende verplichtingen op.

‘Eervol gedrag’ ligt ook aan de basis van een drietal regels uit het humanitair oorlogsrecht. Het verbod op perfidie, onder specifieke omstandigheden, het verbod op het ongepast gebruik van erkende kentekenen en het verbod op het gebruik van nationaliteitskentekenen van neutrale staten of staten die geen partij zijn bij het conflict, zijn ook van toepassing op militaire operaties beneden de drempel van aanval. Het verbod op gebruik van nationaliteitskentekenen van een tegenstander geldt ook beneden de drempel van aanval, al wordt deze laatste conclusie niet door iedereen gedeeld.

4

Hoofdstuk 4 De ondergrens van aanval in het cyberdomein

4.1 Inleiding

Kan de ondergrens van aanval uit artikel 49 lid 1 van Aanvullend Protocol I in traditionele zin op gelijke wijze worden toegepast op militaire operaties in het cyberdomein? Dat is de vraag die ik in dit hoofdstuk ga beantwoorden. Om dit op een gestructureerde manier te kunnen doen zal ik in paragraaf 4.2 allereerst aangeven wat ik versta onder het cyberdomein en aandacht besteden aan de verschillende componenten waaruit dit domein is opgebouwd.¹ In Hoofdstuk 1 heb ik als uitgangspunt geformuleerd dat het humanitair oorlogsrecht van toepassing is op militair operaties in het cyberdomein. Toch zal ik in paragraaf 4.3 nog bezien hoe het internationaal recht omgaat met het cyberdomein, voordat ik in paragraaf 4.4 nader inga op militaire cyberoperaties binnen het humanitair oorlogsrecht, waarbij ik deze enerzijds beschrijf en anderzijds afbaken wanneer deze operaties vallen onder het regime van het humanitair oorlogsrecht. Als laatste zal ik kijken naar de ondergrens van aanval in het cyberdomein waarbij ik de ondergrens in traditionele zin als uitgangspunt neem.² Ik zal daarbij bezien of, en zo ja, waar behoefte of noodzaak bestaat deze ondergrens anders te definiëren. Hierbij zal ik met name aandacht besteden aan de rol die de niet-fysieke, of virtuele, componenten van het cyberdomein hierin spelen.

4.2 Het cyberdomein

4.2.1 Wat is het cyberdomein?

Wat versta ik onder het cyberdomein? Bij ontbreken van een eenduidige gezaghebbende definitie zal ik die vraag beantwoorden door de traditioneel positiefrechtelijke methode te volgen, namelijk te rade gaan bij de rechtsbronnen voor internationaal recht, gebruikmakend van de opsomming en volgorde genoemd in het gezaghebbende artikel 38 lid 1 van het Statuut van het Internationaal Gerechtshof, aangevuld met andere mogelijke bronnen, om te eindigen met de door mij te hanteren omschrijving van het cyberdomein.

4.2.1.1 Verdragen en internationaal gewoonterecht

Gelet op de relatief jonge geschiedenis van het cyberdomein, wanneer deze wordt afgezet tegen de belangrijkste verdragen van het humanitair oorlogsrecht, wekt het geen verbazing dat in de bestaande verdragen binnen het humanitair oorlogsrecht, (nog) geen verwijzingen te vinden zijn naar het cyberdomein. Elders in het internationaal recht zijn zulke verwijzingen al wel te vinden. Het is dan ook zinvol om, op zoek naar mogelijke

1 Cyberdomein wordt in dezelfde betekenis ook wel aangeduid als 'digitaal domein' of met de Engelse term *cyberspace*. Ik zal zoveel als mogelijk de term cyberdomein gebruiken, behalve bij verwijzingen naar bronnen die andere termen gebruiken.

2 Zie Hoofdstuk 2. Aanvallen zijn acties uitgevoerd met militairen en/of militaire middelen, die gericht zijn op fysiek letsel of schade of deze fysieke gevolgen hebben, welke in het kader van een gewapend conflict worden uitgevoerd met als doel een militair voordeel op de tegenstander te behalen.

analogieën, te zien hoe men daar met het begrip cyberdomein omgaat. Om die reden zal ik een kort uitstapje naar het strafrecht maken als voorbeeld van een internationaal rechtsgebied dat ontwikkelingen in het cyberdomein tot onderwerp van een verdrag heeft gemaakt en waarin ook enige begrippen zijn gedefinieerd.

In 2001 kwam de Raad van Europa tot het zogenaamde *Cybercrime*-verdrag,³ ook wel bekend als de *Budapest Convention*, waar in artikel 1 begrippen als ‘computersysteem’ (*computer system*)⁴ en ‘computergegevens’ (*computer data*)⁵ gedefinieerd zijn, maar waarin, anders dan de titel van het verdrag kan doen vermoeden, het begrip cybercrime of cyberdomein niet wordt gedefinieerd. Als mogelijke reden hiervoor kan genoemd worden dat het verdrag tot doel heeft “to improve the means to prevent and suppress computer- or computer-related crime”⁶ en omvat daarmee zowel cybercrime in enge zin als in ruime zin.⁷ Het verschil zit in het onderscheid tussen strafbare handelingen “gericht tegen (het resultaat) van een geautomatiseerde gegevensverwerking”⁸ en strafbare handelingen die ook anderszins strafbaar zijn maar nu “het resultaat zijn van al dan niet bevoegd gebruik van een geautomatiseerde gegevensverwerking” ook wel aangeduid als computer-gerelateerde delicten.⁹ De Commissie van de Europese Gemeenschappen bevestigt deze uitleg in een mededeling aan het Europees Parlement, de Raad en het Europees Comité van de Regio’s, door onder cybercriminaliteit te verstaan “misdrijven gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen.”¹⁰

Uit bovenstaande blijkt dat een begrip als *cybercrime* zowel in enge zin als ook in ruime zin uitgelegd kan worden. De toevoeging van cyber aan een bekend begrip als *crime* kan zowel slaan op strafbare handelingen die worden gepleegd binnen een computersysteem als ook op strafbare handelingen die worden gepleegd door gebruik te maken van een computersysteem.¹¹

3 *Convention on Cybercrime*, European Treaty Series No 185, Trb. 2002, 18. Voor Nederlandse vertaling, Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (het Cybercrime-verdrag) Trb. 2004, 290. In februari 2017 was dit verdrag geratificeerd door 44 landen uit de *Council of Europe* en door 10 landen die niet behoren tot de *Council of Europe*.

4 Cybercrime-verdrag art. 1: “computersysteem: ieder apparaat of geheel van onderling verbonden en samenhangende apparaten, waarvan een of meer overeenkomstig een programma geautomatiseerde gegevensverwerking uitvoert.”

5 Cybercrime-verdrag art. 1: “computergegevens: iedere weergave van feiten, informatie of begrippen in een vorm die geschikt is voor verwerking in een computersysteem, met inbegrip van een programma dat geschikt is om een computersysteem een functie te laten verrichten.”

6 Explanatory Report ETS 185 Cybercrime Convention, p. 7.

7 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 8.

8 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 9. Dit zijn de delicten genoemd in titel 1 van het verdrag, delicten tegen de vertrouwelijkheid, integriteit en beschikbaarheid van computergegevens en -systemen.

9 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 9. Dit zijn de delicten opgenomen in de titels 2 t/m 4 van het verdrag, computer-gerelateerde valsheid, computer-gerelateerde fraude, delicten in verband met kinderpornografie en delicten met betrekking tot inbreuken op auteursrecht en naburige rechten.

10 Mededeling van de Commissie aan het Europees Parlement, de Raad en het Europees Comité van de Regio’s, ‘Naar een algemeen beleid voor de bestrijding van cybercriminaliteit’ COM(2007)267 definitief 22 mei 2007.

11 Explanatory Report ETS 185 Cybercrime Convention, p. 7, pt 35.

Hier is mogelijk een analoge redenering toe te passen op het begrip cyberoperaties binnen het humanitair oorlogsrecht. Afhankelijk van de doelstelling kan volgens die redenering het begrip cyberoperatie zowel eng, in de zin van alleen betrekking hebbend op het computersysteem, of de -systemen sec, als ruim, betrekking hebbend op het computersysteem of de -systemen met daarbij de omgeving die gebruik maakt van die computersystemen, worden uitgelegd. Net als bij het *Cybercrime*-verdrag is dan geen specifieke definiëring van het cyberdomein nodig. Ik kom daar later in dit hoofdstuk nog uitgebreider op terug.

Terug naar het humanitair oorlogsrecht. Zoals eerder opgemerkt is binnen de verdragen van het humanitair oorlogsrecht (nog) geen verwijzing naar het cyberdomein te vinden. De relatief jonge geschiedenis van het cyberdomein, in combinatie met de beperkte ervaringen van cyberoperaties in een gewapend conflict,¹² maakt ook dat nog niet gesproken kan worden van specifiek gewoonterecht gericht op het cyberdomein.¹³ Ik zal daarom verder gaan met de andere bronnen van internationaal recht, zoals algemeen erkende rechtsbeginselen, rechterlijke uitspraken, gezaghebbende publicaties¹⁴ en andere mogelijke bronnen.

4.2.1.2 Algemene erkende rechtsbeginselen

De algemeen erkende rechtsbeginselen¹⁵ als bron voor internationaal recht komen na de “primary sources”,¹⁶ maar “escapes classification as a ‘subsidiary means’ in paragraph (d).”¹⁷ Deze rechtsbeginselen zijn bedoeld voor situaties waarin een rechter een oordeel moet vormen en zich realiseert, “there is no law covering exactly that point, neither parliamentary statute nor judicial precedent. In such instances the judge will proceed to deduce a rule that will be relevant by analogy from already existing rules or directly from the general principles that guide the legal system.[...]Such a situation is perhaps even more likely to arise in international law because of the relative underdevelopment of the system in relation to the needs with which it is faced.”¹⁸

12 En indien er al ervaringen zijn, zijn deze vaak geclassificeerd en niet of nauwelijks toegankelijk, bijvoorbeeld operaties tegen Georgië tijdens de oorlog met Rusland in 2008. Of het is de vraag of het inderdaad cyberoperaties binnen een gewapend conflict betrof, bijvoorbeeld de cyberoperaties tegen Estland in 2007 maar ook het cyberincident uitgevoerd met Stuxnet, zoals dat werd ontdekt in 2010, gericht tegen Iraanse nucleaire faciliteiten. Soms geven nieuwsberichten wel een indicatie van cyberoperaties in het kader van een gewapend conflict zoals BBC 2018, <http://www.bbc.com/news/technology-43738953>, laatst geraadpleegd 28 nov 2018, waar de directeur van het Government Communications HQ UK opmerkte over een UK actie tegen IS: “It is the first time the UK has systematically degraded an adversary’s online efforts in a military campaign.”

13 De regels van gewoonterecht in het algemeen met betrekking tot het humanitair oorlogsrecht zijn wel van toepassing op het cyberdomein, zij het dat de wijze waarop ze van toepassing zijn nog niet altijd volledig duidelijk is.

14 Statuut van het Internationaal Gerechtshof art. 38 lid 1. Dit artikel benoemt achtereenvolgens; a. internationale verdragen, b. internationale gewoonte, c. de door beschaafde naties erkende algemene rechtsbeginselen, d. rechterlijke beslissingen, alsmede de opvattingen van de meest bevoegde schrijvers der verschillende naties.

15 Statuut van het Internationaal Gerechtshof art. 38 lid 1c.

16 Brownlie 2003, p. 5. Gill & Fleck 2012, p. 8. Hiermee doelend op de eerste twee in art 38 van het Statuut van het Internationaal Gerechtshof genoemde bronnen.

17 Brownlie 2003, p. 15.

18 Shaw 2014, p. 69.

Uit bovenstaande doelstelling blijkt al dat, los van welke rechtsbeginselen behoren tot de categorie van algemeen erkende rechtsbeginselen,¹⁹ deze beginselen niet de rechtsbron zijn waar een beschrijving of aanduiding van het begrip cyberdomein te vinden zal zijn. Toch zijn de algemeen erkende rechtsbeginselen zeker van belang voor dit onderzoek. Ik verwijs hiervoor naar het gebruik van de grondbeginselen van het humanitair oorlogsrecht die, zoals eerder vermeld, gezien kunnen worden als “door beschaafde naties erkende algemene rechtsbeginselen.”²⁰

4.2.1.3 Rechterlijke uitspraken en opvattingen van de meest bevoegde schrijvers

De volgende rechtsbron uit artikel 38 van het Internationaal Gerechtshof luidt: “rechterlijke beslissingen alsmede de opvattingen van de meest bevoegde schrijvers der verschillende naties.”²¹ Strikt genomen zijn dit slechts hulpmiddelen (*subsidiary means*) voor het bepalen van rechtsregels²² en daarmee geen “*formal source*”²³, maar zeker uitspraken van het Internationaal Gerechtshof worden gezien als gezaghebbend.²⁴ Vooralsnog zijn er echter nog geen rechterlijke uitspraken gedaan die het begrip cyberdomein binnen het humanitair oorlogsrecht verder verduidelijken.

Van groter belang is het andere hulpmiddel voor het vinden van rechtsregels, “*the teachings of the most highly qualified publicists of the various nations.*”²⁵ Inmiddels zijn voldoende publicaties met verwijzingen naar en definities van het cyberdomein in relatie tot het humanitair oorlogsrecht voorhanden, maar welke zijn aan te merken als opvattingen van de meest bevoegde schrijvers zoals bedoeld in artikel 38 van het Statuut? Vooropgesteld dat schrijvers weliswaar geen rechtsregels maken maar “*merely reflect and reinforce national prejudices*”,²⁶ zij worden wel regelmatig geraadpleegd en geciteerd door bijvoorbeeld “*states in their presentation of claims, national law officials in their opinions to their governments and various international judicial and arbitral bodies in considering their decisions.*”²⁷

Indien ik raadpleging en citering als criterium neem, kan ik in elk geval niet om de *Tallinn Manual on the international law applicable to cyber warfare*,²⁸ hierna te noemen *Tallinn Manual*,²⁹

19 Thirlway (in Evans) 2010, p. 109. “There is however no unanimity among scholars as to the nature of the principles which may be invoked under this head” Brownlie 2003, p. 18 noemt als voorbeelden, “consent, reciprocity, equality of states, finality of awards and settlements, the legal validity of agreements, good faith, domestic jurisdiction and the freedom of the seas.”

20 Bothe, Partch & Solf 2013, p. 43. Zie Hoofdstuk 3 par. 1. Deze grondbeginselen waren uitgangspunt in Hoofdstuk 3 en zullen dat ook zijn in Hoofdstuk 5.

21 Statuut van Internationaal Gerechtshof art. 38 lid 1 d.

22 Statuut van Internationaal Gerechtshof art. 38 lid 1 d.

23 Brownlie 2003, p. 19.

24 Shaw 2014, p. 78. Brownlie 2003, p. 20.

25 Statuut van Internationaal Gerechtshof art. 38 lid 1 d.

26 Shaw 2014, p. 80.

27 Shaw 2014, p. 80.

28 Schmitt 2013.

29 De tweede (uitgebreidere) editie van de *Tallinn Manual*, bekend onder de naam *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations* (2017) zal ik aanduiden als *Tallinn Manual 2.0*.

heen. Een drietal redenen ligt hieraan ten grondslag. Ten eerste bestond de internationale groep van experts die de *Tallinn Manual* heeft samengesteld uit ‘*distinguished international law practitioners and scholars*’.³⁰ Ten tweede heeft deze groep van experts, bij de totstandkoming van de *Tallinn Manual*, naast de gebruikelijke bronnen genoemd in artikel 38 van het Statuut van het Internationaal Gerechtshof, gebruik gemaakt van de militaire handboeken van Canada, Duitsland, Verenigd Koninkrijk en de Verenigde Staten.³¹ Het gebruik van militaire handboeken verdient hier speciale vermelding. De status van militaire handboeken als bron van internationaal recht is weliswaar onduidelijk,³² waarbij de meningen uiteen lopen tussen de uitersten van “*evidence of international custom*”³³ tot “*Manuals do not constitute international law*”³⁴, toch vormen zij in de ogen van het *International Criminal Court for the former Yugoslavia* zeker een element in de “*formation of customary rules or general principles*.”³⁵ Als derde en laatste argument noem ik hier dat de *Tallinn Manual*, sinds het verschijnen ervan “*served as an invaluable resource for government legal advisors and scholars*.”³⁶

De toekomst zal leren hoe gezaghebbend de *Tallinn Manual* en zijn opvolger, de *Tallinn Manual 2.0*,³⁷ zal worden voor de uitleg van het humanitair oorlogsrecht in het cyberdomein. Op dit moment vormen deze *Manuals* zeker een belangrijke bron waarvan de invloed nog is toegenomen doordat bij de samenstelling van de *Tallinn Manual 2.0* gebruik is gemaakt van het zogenaamde ‘*Hague Process*’. Hierbij zijn staten door de Nederlandse regering uitgenodigd “*to unofficially comment on the working drafts of the Manual in a Chatham House environment*”.³⁸

Het cyberdomein wordt in de *Tallinn Manual 2.0* omschreven als “*The environment formed by the physical and non-physical components to store, modify, and exchange data using computer networks*”.³⁹ Wat opvalt aan deze definitie is dat hij breed is, in de zin dat zowel de componenten (fysiek en niet-fysiek) als ook het gebruik van die componenten voor processen als opslaan, modifieren en uitwisselen behoren tot het cyberdomein. Uit de *Commentary* bij de *Tallinn Manual 2.0* blijkt dat “*for the purpose of this Manual, [...] The physical layer comprises the physical network components (i.e. hardware and other infrastructure, such as cables, routers, servers, and*

30 Schmitt 2013, p. 1.

31 Schmitt 2013, p. 8.

32 Turns (in Hayashi) 2010, p. 65.

33 Brownlie 2003, p. 6. Zie ook Garraway (in Hayashi) 2010, p. 46 “*national Manuals provide evidence of state practice and opinio juris in relation to the states by whom they are issued.*”

34 Lord Wright of Durley, “foreword”. *United Nations war crimes commission, law reports of trials of war criminals Vol VIII* p. x, geciteerd in Turns (in Hayashi) 2010, p. 66

35 ICTY, *The Prosecutor v. Dusko Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction*, IT-94-1-A, 2 oktober 1995, par. 99.

36 Schmitt 2017, p. 1. Met de opmerking dat deze uitspraak komt van een van de prominente samenstellers van de *Tallinn Manual*.

37 Schmitt 2017. Voluit *Tallinn Manual 2.0 on the International Law applicable to cyberoperations*.

38 Schmitt 2017, p. 6. *Three two-day sessions in The Hague were attended by delegations from over 50 States and international organisations*.

39 Schmitt 2017, p. 564. In de *Tallinn Manual* is een uitgebreidere omschrijving opgenomen met daarin de toevoeging *characterized by the use of computers and the electro-magnetic spectrum*. Schmitt 2013, p. 258.

computers). The logical layer consists of the connections that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities".⁴⁰ Hieruit is af te leiden dat ook gebruikers zijn inbegrepen in bovenstaande definitie van het cyberdomein.

4.2.1.4 Andere mogelijke bronnen

Op zoek naar mogelijke definities van het cyberdomein, en de veelheid aan verschillende variaties daarin, verwijs ik naar het werk van het NATO Cooperative Cyber Defence Centre of Excellence. Deze organisatie heeft een verklarende woordenlijst samengesteld met daarin een overzicht van hoe staten en instituties aankijken tegen diverse cyber-gerelateerde onderwerpen.⁴¹ Met betrekking tot *cyberspace* geeft deze verklarende woordenlijst 23 verschillende versies⁴² aangevuld met nog een omschrijving van het *cyberdomain*.⁴³ Een aantal elementen komt veelvuldig in de verschillende omschrijvingen terug namelijk 'computersystemen', 'informatiesystemen', 'verbonden', 'internet', 'wereldwijd' en 'vervagende en niet bestaande grenzen' waarbij sommige omschrijvingen ook specifiek de gebruikers van het cyberdomein noemen als onderdeel van dat cyberdomein.⁴⁴

Ook voor Nederland lijkt te gelden dat de gebruikers van het cyberdomein gerekend worden tot het cyberdomein, getuige bijvoorbeeld de beschrijving van het cyberdomein als "het geheel van digitale informatie, informatie-infrastructuren, computers, systemen, toepassingen en de interactie tussen informatietechnologie en de fysieke wereld waarover communicatie en informatie-uitwisseling plaatsvindt."⁴⁵ Ik gebruik de term 'lijkt te gelden' met opzet, omdat de Nederlandse regering de term niet altijd op dezelfde manier gebruikt. Zo merkt de Minister van Defensie in de Defensie Cyber Strategie over het cyberdomein op dat: "er bestaat op dit ogenblik geen internationaal geaccepteerde definitie van het begrip digitaal domein (*cyber space*). In deze strategie wordt het digitale domein beschouwd als alle entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente verbindingen als tijdelijke of plaatselijke verbindingen en betreft altijd op enigerlei wijze de gegevens (data, programmacode, informatie, etcetera) die zich in dit domein bevinden."⁴⁶ Deze laatste omschrijving benoemt de informatie-uitwisseling met de fysieke wereld, bijvoorbeeld de gebruikers, niet specifiek.

40 Schmitt 2017, p. 12. Op de verschillende layers van het cyberdomein kom ik later nog terug.

41 CCDOE *Cyber definitions* beschikbaar op <https://ccdcoe.org/cyber-definitions.html>, laatst geraadpleegd 28 nov 2018. Hierbij maakt het CCDOE gebruik van strategische en beleidsdocumenten zoals veiligheidsstrategieën.

42 <https://ccdcoe.org/cyber-definitions.html> geraadpleegd op 17 apr 2018.

43 <https://ccdcoe.org/cyber-definitions.html> geraadpleegd op 17 apr 2018.

44 Als voorbeelden, *users* (Spanje), *and any form of human activity on them* (Rusland), *interaction between people* (India). <https://ccdcoe.org/cyber-definitions.html> geraadpleegd op 03 feb 2018.

45 Defensie Cyber Strategie, brief van de regering: informatie over de ontwikkeling van offensieve cybercapaciteiten bij Defensie. Kamerstukken II 2013-2014, 33 321, nr.3.

46 Kamerstukken II 2011-2012, 33 321, nr.1 voetnoot 1.

4.2.1.5 Het cyberdomein in dit onderzoek

Uit de hierboven gegeven voorbeelden moge duidelijk zijn dat (nog) geen eenduidige gezaghebbende definitie van het cyberdomein voor toepassing binnen het humanitair oorlogsrecht bestaat en dat vele varianten mogelijk zijn. Sommige daarvan neigen naar een enge beschrijving in de zin dat het cyberdomein zich beperkt tot de onderling verbonden computer- en informatiesystemen en hetgeen zich daarbinnen afspeelt.⁴⁷ Andere neigen naar een bredere interpretatie en beschouwen ook de interactie met de fysieke buitenwereld, bijvoorbeeld gebruikers die informatie verstrekken of onttrekken aan die systemen, tot het cyberdomein.⁴⁸

De onderzoeksvraag “welke regels gelden binnen het *ius in bello* voor militaire cyberoperaties die beneden de drempel van aanval uit artikel 49 lid 1 Aanvullend Protocol I blijven” is impliciet een vraag naar regels die gelden voor menselijk handelen, dat is namelijk hetgeen het humanitair oorlogsrecht reguleert, los van het gegeven waar of in welk domein dat handelen plaatsvindt.

Hier is het verstandig terug te kijken naar de analogie die ik hiervoor maakte met *cybercrime*.⁴⁹ Om ook het menselijk handelen te omvatten moet het begrip cyberdomein ruim, namelijk betrekking hebbend op het computersysteem of de -systemen met daarbij de omgeving die gebruik maakt van die computersystemen, worden uitgelegd. Door te kiezen voor een brede definitie van het cyberdomein, dus inclusief de interactie met de fysieke wereld waaronder de personen die informatie verstrekken of onttrekken aan het cyberdomein stel ik zeker dat het menselijk handelen binnen de definitie valt.

Gelet op het niet geringe aanzien dat de *Tallinn Manual* heeft weten te verwerven en het feit dat de daarin gehanteerde omschrijving van het cyberdomein een brede uitleg hanteert, zal ik in dit onderzoek, dus binnen het paradigma van het humanitair oorlogsrecht, de omschrijving uit de *Tallinn Manual 2.0* gebruiken, namelijk de omgeving gevormd door de fysieke en niet-fysieke componenten om gegevens op te slaan, te modificeren en uit te wisselen door middel van het gebruik van computernetwerken.⁵⁰

Dit onderzoek richt zich op militaire cyberoperaties. Om een goed begrip van deze cyberoperaties te kunnen vormen is het noodzakelijk nader in te gaan op de opbouw van het cyberdomein. Waaruit bestaat dit domein en dan met name waaruit bestaan de niet-fysieke, of virtuele, componenten? Dit is de vraag die ik in de volgende paragraaf ga beantwoorden.

47 Zie bijv. USA JP 1-02. UK Cyber Security Strategy, available on https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, laatst geraadpleegd 28 nov 2018. Op basis van de CCDCOE (zie voetnoot 640) Japan, Italië, België.

48 *Tallinn Manual 2.0*, p. 564. Defensie Cyber Strategie, Kamerstukken II 2013-2014, 33 321, nr. 3. Op basis van de CCDCOE (zie voetnoot 640), Spanje, Rusland, Polen, India, Zuid-Afrika.

49 Zie par. 4.2.1.1.

50 Schmitt 2017, p. 564, mijn vertaling. De originele Engelse tekst luidt: “The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks.”

4.2.2 De componenten van het cyberdomein

Het cyberdomein is de omgeving gevormd door de fysieke en niet-fysieke componenten om gegevens op te slaan, te modificeren en uit te wisselen door middel van het gebruik van computernetwerken.⁵¹ Als domein is dit weer te geven als een gelaagd model, bijvoorbeeld als model met drie,⁵² met vier,⁵³ met vijf⁵⁴ of zelfs met zeven lagen.⁵⁵ Wat opvalt aan de beschrijvingen is dat ze uiteenlopen in de beschrijving van de niet-fysieke componenten van het cyberdomein. Over de fysieke componenten, die bestaan uit de personen die gebruik maken van het cyberdomein en de fysieke objecten zoals de fysieke netwerk infrastructuur (bedraad, draadloos en optisch) en fysieke hardware zoals computers, servers, routers, kabels en bedrading,⁵⁶ bestaat nauwelijks onderscheid tussen de modellen.⁵⁷ Deze fysieke componenten hebben een, eenvoudig vast te stellen, geografische locatie⁵⁸ waarmee het cyberdomein deze fysieke componenten deelt met de conventionele domeinen lucht, land, zee en ruimte.⁵⁹ Maar hoe zit dit met de niet-fysieke componenten? Voordat ik verderga met de indeling van de verschillende componenten van het cyberdomein zal ik kort ingaan op de geografische locatie van de niet-fysieke componenten omdat dit bijvoorbeeld van belang is bij “sovereignty issues tied to the physical domains.”⁶⁰

4.2.2.1 Hebben niet-fysieke componenten een geografische locatie?

Dit betreft een lastig éénduidig te beantwoorden vraag waarover ook verschillend wordt gedacht. Een voorbeeld: in het hierboven aangeduide drielagenmodel behoorde *systems software* tot de *Physical Network Layer*.⁶¹ Omdat deze *systems software* direct na de hardware genoemd wordt vermoed ik dat hier specifieke software bedoeld wordt, namelijk de software die aanwezig is op de *hardware* om deze te laten functioneren. Om dit te verduidelijken is het goed om een schematische indeling te maken voor de verschillende soorten software die hiervoor nodig zijn.

51 Schmitt 2017, p. 564.

52 Zoals bijvoorbeeld in JP 3-1 (R), *Cyberspace operations*, p. 1-2. De drie lagen zijn de *Physical Network layer*, de *Logical Network Layer* en de *Cyber-persona Layer*.

53 Ducheine & van Haaster 2014, p. 309. “The Transmission Control Protocol/Internet Protocol (TCP/IP) recognises four layers: the link, internet, transport and application layers.”

54 TRADOC Pam 525-7-8 p. 8. “Physical Layer, Logical Layer and Social layer with five sub-layers, geographic, physical, logical, persona and cyber persona components.”

55 International Organization for Standardization. Available on: <https://www.iso.org/standard/16011.html>. The Open Systems Interconnection (OSI) model describes seven layers: “the physical, data link, network, transport, session, presentation, and application layers.”

56 TRADOC Pam 525-7-8 p. 9. De Tallinn Manual verstaat onder hardware: de fysieke componenten waaruit een computernetwerk en de cyberinfrastructuur bestaat, Schmitt 2013, p. 259.

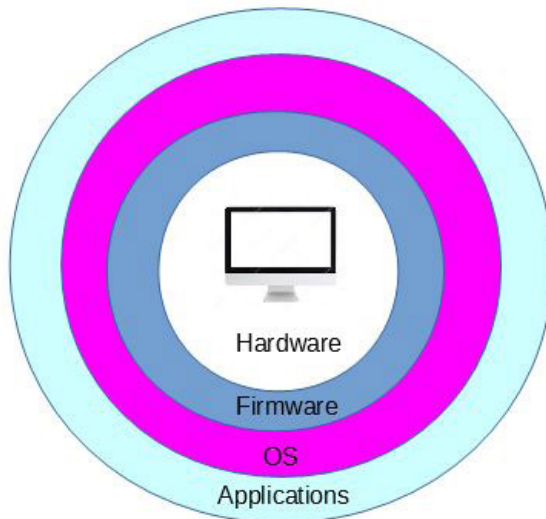
57 Hardware (computers en servers) en network infrastructure (wires, cables, routers, switches) worden vaak genoemd (JP 3-12 (R), *Cyberspace operations*, p. 1-3). Soms is daar ‘associated geography’ aan toegevoegd, van Haaster 2018, p. 122.

58 US JP 3-1 (R) *Cyberspace operations*, p. 1-2.

59 Ducheine & van Haaster 2014, p. 309

60 JP 3-12 (R), *Cyberspace operations*, p. 1-3.

61 US JP 3-12 (R) editie 2013, *Cyberspace operations*, p. 1-3. In de editie uit 2018 wordt *systems software* niet langer benoemd als onderdeel van de *Physical Network Layer*.



Firmware: The read-only software installed on a hardware component enabling the functioning and interoperability of that specific piece of hardware

OS: Operating System: Software that administers hardware, software and common services for applications. An OS consists of a kernel that processes the input and output of applications and translates it into instructions for the central processing unit (CPU, memory and devices)

Applications: Installed software with which users interact when using their device.

Figuur 5 Schematische weergave verschillende soorten software.⁶²

De combinatie van firmware en *operating system* maakt dat de hardware kan functioneren. Om daadwerkelijk gebruik te maken van de hardware zullen, afhankelijk van het doel, een of meerdere applicaties gebruikt worden.⁶³ Het is mogelijk dat alle drie de soorten software op de hardware staan en daarmee de geografische locatie van de hardware delen.

De gelaagdheid van de verschillende soorten software heeft echter als consequentie dat niet alle drie de soorten software volledig op de hardware aanwezig hoeven te zijn. De firmware zal zich op de hardware bevinden, maar het besturingssysteem (*Operating system*) kan al gedeeltelijk op andere hardware of in de 'cloud'⁶⁴ zijn ondergebracht. Dit geldt in nog grotere mate voor de applicaties. Zo merkt de Commissie Dessens bijvoorbeeld op dat een

62 Schema en legenda afkomstig uit van Haaster 2018, p. 131.

63 Hierbij ontstaat een onderlinge relatie. Om de applicaties te kunnen gebruiken is hardware met bijbehorende firmware en *operating system* noodzakelijk maar anderzijds zijn applicaties nodig om gebruik te kunnen maken van de hardware. De hardware met bijbehorende firmware en *operating system* kan weliswaar zelfstandig functioneren maar kan nog geen taken uitvoeren zoals bijv berekeningen maken, teksten opmaken en opslaan of gegevens verzenden. Om dergelijke taken uit te kunnen voeren met behulp van de hardware zullen veelal applicaties gebruikt worden (het is mogelijk zelf een applicatie te bouwen maar ook daarvoor zal veelal gebruik gemaakt worden van een programma gemaakt voor het ontwikkelen van applicaties).

64 The term "cloud" comes from early network diagrams, in which the image of a cloud was used to indicate a large network, such as a WAN. The cloud eventually became associated with the entire internet, and the two terms are now used synonymously. The cloud may also be used to describe specific online services, which are collectively labeled "cloud computing", <http://techterms/definition/cloud> laatst geraadpleegd 30 jan 2019.

‘programmacode’ behoort tot de gegevens die zich in het cyberdomein bevinden waarbij geen geografische beperkingen zijn gesteld.⁶⁵ Dit betekent dat deze ‘programmacode’ niet alleen op de hardware zelf, maar ook elders, waar ook ter wereld, opgeslagen kan zijn, waarbij het mogelijk is dat dit niet op één locatie maar op vele plaatsen tegelijkertijd is. Zeker als gebruik gemaakt wordt van zogenaamde *cloud computing techniques*,⁶⁶ als *data storage technology*, *data management technology*,⁶⁷ of een combinatie daarvan⁶⁸ zal het niet eenvoudig zijn, en in sommige gevallen zelfs onmogelijk, om één of meerdere geografische locaties toe te bedelen aan niet-fysieke componenten.

Als conclusie kan ik zeggen dat niet altijd eenduidig vast te stellen is of niet-fysieke componenten één of meerdere geografische locatie hebben. Het zal van de situatie afhangen. In mijn eigen indeling van niet-fysieke componenten kom ik hier nog op terug.

4.2.2.2 De niet-fysieke componenten van het cyberdomein.

Na de fysieke componenten ben ik nu aangekomen bij de niet-fysieke componenten. Deze zijn minder eenduidig ingedeeld dan de fysieke componenten van het cyberdomein. In het eerder genoemde drielagenmodel⁶⁹ behoort de *Logical Network Layer* (in zijn geheel) en de *Cyber-persona Layer* (gedeeltelijk) tot het niet-fysieke gedeelte. De *Logical Network Layer* bestaat in dit model uit “those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node.”⁷⁰ Een voorbeeld hiervan is een website die is ondergebracht op verschillende servers op verschillende fysieke locaties maar benaderd kan worden via één *Uniform Resource Locator* (URL).⁷¹ De *Cyber-persona Layer*, in andere publicaties aangeduid als de *social layer*,⁷² bestaat in dit model uit de “digital representation[s] of an individual or entity identity in cyberspace”⁷³ (niet-fysiek) en “the people actually on the network”⁷⁴ (fysiek). Voorbeelden van niet-fysieke elementen uit de *Cyber-persona Layer* zijn e-mailadressen, IPadressen, webpagina’s en telefoonnummers.

65 Evaluatie Wet op de inlichtingen en veiligheidsdiensten. Kamerstukken II 2013-14, 33 820, nr. 1 bijlage, p. 85.

66 Schmitt 2017, p. 563: “A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing allows for efficient pooling of computer resources and the ability to scale resource to demand.”

67 Wang, Wang & Huang 2011, p. 406.

68 Een voorbeeld daarvan is het *Dynamic Distributed Dimensional Data Model (D4M) Database and Computation System*. http://www.mit.edu/~kepner/pubs/Kepner_2012_D4M_Paper.pdf, laatst geraadpleegd 28 nov 2018.

69 US JP 3-12 (R), *Cyberspace operations*, p. 1-2.

70 US JP 3-12 (R), *Cyberspace operations*, p. 1-3.

71 US JP 3-12 (R), *Cyberspace operations*, p. 1-3.

72 TRADOC Pam 525-7-8, p. 8. De *social layer* omvat in dit model zowel de *cyber-persona components* (niet fysiek) als de *persona components* (fysiek). Let op de mogelijke spraakverwarring omdat de *Tallin Manual 2.0* iets anders verstaat onder de *social layer*, namelijk de individuen en groepen die zich inlaten met cyberactiviteiten. Schmitt 2017, p. 12.

73 US JP 3-12 (R), *Cyberspace operations*, p. 1-3.

74 US JP 3-12 (R), *Cyberspace operations*, p. 1-3.

Duchaine en van Haaster maken een iets andere indeling binnen de niet-fysieke dimensie van het cyberdomein, namelijk cyberobjecten en cyberidentiteiten,⁷⁵ waarbij cyberobjecten de virtuele reflectie van tastbare objecten zijn en cyberidentiteiten van personen.⁷⁶ Voor de verzameling van cyberobjecten reserveren zij de aanduiding *Logical Network Layer*⁷⁷ terwijl zij het geheel aan cyberidentiteiten kwalificeren als de *Cyber persona Layer*.⁷⁸ In een latere publicatie heeft Duchaine nog een verdere verdeling aangegeven van cyberobjecten met enerzijds gegevens en anderzijds een verzameling die is samen te vatten onder de noemer software, bestaande uit protocollen, firmware, *operating systems* en applicaties.⁷⁹

Andere onderverdelingen van de niet-fysieke componenten zijn mogelijk. Zo maakt Harrison Dinniss onderscheid tussen 'inhoudelijk niveau gegevens' (*content-level data*) en 'operationeel niveau gegevens' (*operation-level data*).⁸⁰ 'Inhoudelijk niveau gegevens' lijken op de *Cyber-persona layer* zoals hierboven omschreven, maar omvatten daarnaast ook de inhoud van andere databases zoals tekstbestanden, bibliotheekbestanden en medische databases.⁸¹ 'Operationeel niveau gegevens', vaak aangeduid als *logical level* of programmatuurdata, maken dat de hardware zijn functionaliteit krijgt en de taken kan uitvoeren die wij van die hardware verlangen.⁸² Deze laatste categorie lijkt daarmee op de *Logical Network Layer* uit het hierboven beschreven drielagenmodel.

4.2.2.3 De componenten van het cyberdomein in dit onderzoek

Uit bovenstaande beschrijving van de componenten komt naar voren dat het cyberdomein een aantal fysieke componenten kent die niet specifiek zijn voor dit domein, omdat deze ook voorkomen in de natuurlijke domeinen land, zee, lucht en ruimte. Wat het cyberdomein onderscheidt van deze andere natuurlijke domeinen zijn de niet-fysieke componenten. Deze kunnen op verschillende manieren aangeduid en gegroepeerd worden. Ik kies voor een combinatie van bovenstaande onderverdelingen, waarbij ik onderscheid maak tussen firmware, besturingsprogramma's, cyberidentiteiten, computerprogramma's (waaronder applicaties) en computergegevens. In onderstaande figuur is deze onderverdeling gevisualiseerd. Hierbij heb ik bewust gekozen om niet de verschillende lagen maar de groeperingen centraal te zetten, omdat hiermee de relaties tussen de verschillende fysieke en niet-fysieke componenten van het cyberdomein, als ook de relaties tussen de niet-fysieke componenten onderling, beter naar voren komen. Na een

75 Duchaine & van Haaster 2014, p. 310.

76 Duchaine & van Haaster 2014, p. 310. *Operating systems* software, wordt hier specifiek genoemd als een voorbeeld van een (niet-fysiek) cyberobject.

77 Duchaine & van Haaster 2014, p. 310.

78 Duchaine & van Haaster 2014, p. 310.

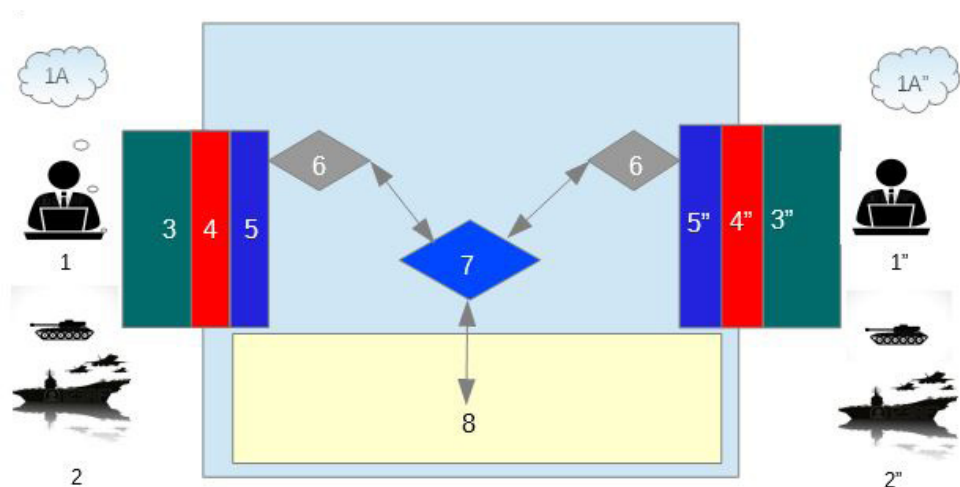
79 Duchaine 2016, p. 10. Vergelijk Schmitt 2017, p. 567 waar software is omschreven als: "The non-physical components of a computer system and cyber infrastructure. These components encompass programs, including operating systems, applications and related configuration and run-time data."

80 Harrison-Dinniss 2015, p. 41.

81 Harrison-Dinniss 2015, p. 41.

82 Harrison-Dinniss 2015, p. 41.

korte beschrijving van de figuur en de daarin aangebrachte groeperingen, zal ik aangeven waarom ik specifiek voor deze groeperingen kies.



Fysieke componenten

- 1: fysieke personen/instaties die gebruiken van het cyberdomein.
- 1A: denkbeelden, ideeën en manieren van handelen.
- 2: militair materieel.
- 3: fysieke hardware (computers, modems etc.)

Niet-fysieke componenten

- 4: firmware.
- 5: besturingsprogramma's.
- 6: cyberidentiteiten.
- 7: applicaties, programma's etc.
- 8: computergegevens (bestanden, foto's, adressen etc.).

Figuur 6: Onderverdeling elementen cyberdomein

Fysieke componenten:

Categorie 1 (en 1") staat voor de menselijke gebruikers van het cyberdomein. Om gegevens op te slaan, te modifieren of uit te wisselen maken deze gebruikers gebruik van hardware zoals bijvoorbeeld computers weergegeven als 3. Bijzonder aan de menselijke gebruikers is dat zij ideeën, denkbeelden en dergelijke, weergegeven als 1A (en 1A"), hebben die beïnvloed (kunnen) worden door het gebruik van het cyberdomein. Op deze beïnvloeding kom ik later terug.

Categorie 2 (en 2") zijn de militaire wapensystemen als vliegtuigen, schepen tanks etc. voor zover ze voor hun functioneren gebruikmaken van het cyberdomein. Dit zal veelal gebeuren middels eenzelfde soort hardware (3) als menselijke gebruikers.

Categorie 3 (en 3") is de hardware die deel uitmaakt van het cyberdomein. Te denken valt aan computers, telefoons, laptops, modems maar ook routers, kabels en bedrading.⁸³

Categorie 4 (en 4") is de interface-categorie. Deze categorie vormt de schakel tussen de fysieke en de niet-fysieke componenten van het cyberdomein. Het is apparatuur, voorzien van de bijbehorende programmatuur (de firmware, zie hierna), die de fysieke input kan omzetten in een digitale output of vice versa. Deze interface-categorie is visueel weergegeven door blok 4 (en 4") gedeeltelijk in de fysieke omgeving en gedeeltelijk in de virtuele omgeving te plaatsen. Bij interactie tussen mensen (1) of militaire wapensystemen (2) en het virtuele deel van het cyberdomein (5 tot en met 8) wordt deze categorie vaak samengevat onder de noemer gebruikersinterface of *human-machine* interface. Soms werken deze alleen van mens naar het virtuele deel van het cyberdomein,⁸⁴ of andersom,⁸⁵ maar steeds vaker is tweerichtingsverkeer met dezelfde apparatuur mogelijk.⁸⁶ Bij interactie tussen fysieke apparaten of systemen (3) met het virtuele gedeelte van het cyberdomein wordt veelal gebruik gemaakt van zogenaamde *Programmable Logic Controllers*. Dit zijn apparaten die, volgens een ingesteld programma (de firmware, zie hierna), informatie van inputs verwerken en outputs aansturen.⁸⁷

Niet-fysieke componenten:

De eerste groep is de firmware, weergegeven in figuur 6 als deel van 4 (en 4"). Dit is het virtuele gedeelte van de interface-categorie en betreft de specifiek voor bepaalde hardware (zoals de gebruikersinterface of de *Programmable Logic Controllers*) gemaakte programma's die maken dat de hardware van de interface-categorie 'weet' hoe te reageren op input vanuit de virtuele elementen en *vice versa*.⁸⁸ In het kader van dit onderzoek is deze firmware op twee manieren specifiek van belang. Allereerst bevindt deze firmware zich vast 'op' de hardware zodat het als het ware de geografische locatie met de hardware waar het 'op' zit, deelt. Dit in tegenstelling tot de andere virtuele elementen die op verschillende geografische locaties opgeslagen kunnen zijn of zich in transitie kunnen bevinden, waardoor überhaupt geen geografische locatie aan te duiden is. Ten tweede fungeert firmware als een soort van schakelaar tussen de fysieke en niet-fysieke componenten. Om door middel van niet-fysieke

83 Oxford Dictionary: *The machines, wiring, and other physical components of a computer or other electronic system.*

84 Voorbeelden hiervan zijn een microfoon, een toetsenbord of een computermuis.

85 Voorbeelden zijn een monitor of een speaker.

86 Voorbeelden hiervan zijn een interactief scherm (*touchscreen*) of actieve speakers.

87 http://www.plcdev.com/definition_of_a_plc, laatst geraadpleegd 28 nov 2018. Een eenvoudig voorbeeld ter verduidelijking. Neem een lichtschakelaar. Een druk op de knop laat het licht aan of uit gaan. Andere mogelijkheden zijn er niet. Indien aanpassingen, bijvoorbeeld een tijdsvertraging of gedimd licht gewenst is, moet hiervoor nieuwe apparatuur en bedrading geïnstalleerd worden, wat tijd, geld en arbeid vergt voor een relatief eenvoudige aanpassing. Indien tussen de lichtschakelaar en de lamp een *Programmable Logical Controller* (PLC) geïnstalleerd is, vormt het omzetten van de schakelaar de *input* en het aangaan van de lamp de *output*. Indien een vertraging of gedimd licht gewenst wordt, is het enige dat gewijzigd moet worden het programma van de PLC, de firmware.

88 Een voorbeeld is een toetsaanslag "x" op een toetsenbord. De fysieke handeling geeft de input die door de firmware wordt omgezet in een digitaal signaal, waardoor een tekstverwerkingsprogramma 'weet' dat een "x" is bedoeld. Verandering in de firmware maakt het mogelijk dat dezelfde fysieke aanslag door het tekstverwerkingsprogramma wordt gezien als een "y".

componenten fysieke gevolgen te kunnen veroorzaken moet op enig moment gebruik gemaakt worden van een onderdeel uit de interface-categorie.⁸⁹

De tweede groep niet-fysieke componenten bestaat uit besturingsprogramma's (in Figuur 6 aangegeven met 5), ook bekend onder de Engelse benaming 'Operating Systems'.⁹⁰ Dit betreft "*Software that administers hardware, software and common services for applications. An OS consists of a kernel that processes the input and output of applications and translates it into instructions for the central processing unit (CPU), memory and devices*".⁹¹ Tezamen met de firmware, specifiek voor elk onderdeel van de hardware, zorgt het besturingsprogramma ervoor dat de verschillende hardwarecomponenten, bijvoorbeeld harde schijf, processor en intern geheugen, of randapparatuur, bijvoorbeeld een muis, een beeldscherm of een toetsenbord, met elkaar één werkend geheel vormen. In Figuur 6 is het besturingsprogramma voorgesteld alsof het in zijn geheel op de computer is geïnstalleerd. Dit betekent dat de computer in zijn geheel op kan starten zonder gebruik te maken van een verbinding met andere virtuele componenten uit het cyberdomein. Hiervoor heb ik aangegeven dat een gedeelte van de besturingssoftware niet op de hardware zelf hoeft te staan, maar ook elders in het virtuele gedeelte van het cyberdomein opgeslagen kan zijn.⁹² In die gevallen zal eerst, via een cyberidentiteit (in Figuur 6 weergegeven als 6, zie hierna) contact gelegd moeten worden met andere componenten uit het cyberdomein. Het besturingsprogramma (in Figuur 6 weergegeven als 5) is dan opgesplitst in een gedeelte voor en een gedeelte na de cyberidentiteit.

De volgende groep niet-fysieke componenten zijn de cyberidentiteiten, waaronder ik allereerst de digitale "*reflections of persons*" versta.⁹³ Deze zijn niet-fysiek en niet tastbaar maar wel intrinsiek verbonden met hun fysieke tegenhanger, al hoeft die verbondenheid niet noodzakelijk een directe verbinding te zijn.⁹⁴ Deze cyberidentiteiten, die "bestaan uit profielgegevens op de social media, mailadressen, blogs en alle andere data die online staan en gelieerd zijn aan een bepaald persoon"⁹⁵, zijn in Figuur 6 weergegeven als 6. Daarnaast kunnen cyberidentiteiten ook de digitale reflecties van fysieke objecten betreffen zoals een

89 Een voorbeeld hiervan beschreven in Rid & Mc Burney 2012, p. 10. In 2006 voerde het Idaho National Laboratory een test uit naar de zogenaamde 'Aurora' zwakheid van het Noord-Amerikaans energie-netwerk en werd een 27-ton industriële dieselgenerator op de proef gesteld. "The lab allegedly came up with twenty-one lines of code that caused the generator to blow up. The malicious code caused the machine's circuit breakers to cycle on-and-off in rapid succession, causing permanent damage through vibration." Een ander, vaak genoemd voorbeeld is Stuxnet. Symantec noemt het "one of the most complex threats .. a large, complex piece of malware with many different components and functionalities." Symantec 2011, p. 1. Ondanks deze gecompliceerdheid kon het uiteindelijke doel, fysieke sabotage van het systeem, alleen bewerkstelligd worden door de laatste stap, het functioneren van de PLC door middel van firmware te modificeren. Symantec 2011, p.3.

90 Zie figuur 5 in par. 4.2.2.1.

91 Van Haaster 2018, p. 131.

92 Zie par. 4.2.2.1.

93 Ducheine & van Haaster 2014, p. 311.

94 Ducheine & van Haaster 2014, p. 311. Een voorbeeld kan dit verduidelijken. Iemand kan in de fysieke wereld naar de kapper gaan waardoor hij of zij er anders uit gaat zien. De cyberidentiteit kan gewijzigd worden door bijvoorbeeld een profielfoto te veranderen. Deze twee handelingen kunnen uiteraard overeenkomen, maar dit is geenszins noodzakelijk en de handelingen kunnen ook geheel los van elkaar staan.

95 Ducheine & van Haaster 2013, p. 376.

militair systeem of een computer, bijvoorbeeld via *IP addresses*⁹⁶ of *media access control (MAC) addresses*.⁹⁷ Als laatste kunnen cyberidentiteiten een afspiegeling zijn van een niet-fysiek bestaand iets, bijvoorbeeld een idee of een verzinsel (weergegeven in Figuur 6 als 1A).⁹⁸

Wat alle cyberidentiteiten gemeen hebben is dat ze via een vooraf vastgelegde werkwijze contact maken vanaf de hardware (4) via de firmware (4) en het besturingsprogramma (5) naar de overige niet-fysieke componenten van het cyberdomein (7 en 8). Het meest bekende voorbeeld hiervan is waarschijnlijk het inloggen op een computer met een gebruikersidentificatie, al dan niet in combinatie met een wachtwoord.⁹⁹

In het humanitair oorlogsrecht wordt voor legitieme militaire doelen onderscheid gemaakt tussen de categorieën personen en objecten. Om die reden, en de hierboven vermelde intrinsieke verbondenheid van fysieke personen met hun cyberidentiteiten, zal ik bij cyberidentiteiten terugkomen op de vraag of dit onderscheid personen en objecten doorwerkt in het cyberdomein.

Als 7 is weergegeven de verzameling van virtuele componenten vaak aangeduid als (computer)programma's of software.¹⁰⁰ Hieronder vallen applicaties en protocollen maar ook tekstverwerkingsprogramma's, databases en fotobewerkingsprogramma's. Een specifieke soort software die tot deze verzameling behoort wil ik hier separaat noemen, omdat deze vaak genoemd wordt als mogelijkheid van een digitale aanval met grote fysieke gevolgen.¹⁰¹ Het betreft hier de besturingssoftware voor *Supervisory Control and Data Acquisition (SCADA)*. Dit is software voor "*gathering real-time data, monitoring equipment and controlling processes in industrial facilities and public utilities*."¹⁰² Met behulp van deze software wordt in industriële processen vaak (grote) aantallen *Programmable Logic Controllers* gemonitord en aangestuurd. Bij de analyse van schade aan niet-fysieke componenten kom ik nog terug op deze specifieke besturingssoftware.

De laatste groep van virtuele componenten is 8, de computergegevens. Dit is de groep die Harrison-Dinniss aanduidt met *content-level data*.¹⁰³ Het gaat hier om bijvoorbeeld de gegevens opgeslagen in een database, de tekstbestanden gemaakt met een tekstverwerkingsprogramma of foto's opgeslagen en eventueel bewerkt met een fotobewerkingsprogramma.

96 Ducheine & van Haaster 2014, p. 310. "*IP address: the digital postal code of hardware*."

97 Ducheine & van Haaster 2014, p. 310. "*MAC address: The identification number/code of a particular device*."

98 Zo kan een fysieke persoon een cyberidentiteit aanmaken voor een verzonnen persoon of organisatie. Ook een computer kan geprogrammeerd worden om cyberidentiteiten aan te maken van niet bestaande mensen of objecten.

99 Een gebruikersidentificatie kan bestaan uit een numerieke reeks getallen en letters, maar kan bijvoorbeeld ook in de vorm van een magneetpas of biometrische eigenschappen als een vingerafdruk of irisscan.

100 Schmitt 2017, p. 567.

101 Zie bijv. Gill (in Tsagourias & Buchan) 2015, p. 376, Droegge 2012, p. 538, Harrison-Dinniss 2012, p. 5.

102 Slay & Miller 2008, p. 73.

103 Harrison Dinniss 2015, p. 41.

Twee eenvoudige voorbeelden kunnen de onderlinge relaties en verschillen in virtuele elementen verduidelijken. Een fysiek persoon (1) heeft een gedachte (1A). Hij start een laptop (hardware 3) via het toetsenbord (de interface 4), voorzien van firmware. De laptop start op door middel van een besturingsprogramma (5) en de persoon logt in met zijn cyberidentiteit (6), om vervolgens zijn gedachte te verwoorden in een tekstbestand (8). Om dit te kunnen doen maakt hij gebruik van een tekstverwerkingsprogramma (7). Hij kan dit bestand via een ander programma (6), bijvoorbeeld een e-mail programma, delen met een andere fysieke persoon (1"). Omdat het tekstbestand als computergegevens voor die andere fysieke persoon niet tastbaar of zichtbaar is, gebruikt deze ook weer een programma (6) en hardware (3") voorzien van een besturingsprogramma (5) en een interface (4) voorzien van firmware om het tekstbestand om te zetten in voor hem waarneembare, leesbare tekst op een beeldscherm of misschien wel in een tastbare variant in de vorm van een afdruk.

Een tweede voorbeeld is een tank (2) die, mits voorzien van de juiste computerhardware (3) met daarop firmware en een besturingsprogramma via een cyberidentiteit (6) inlogt op een programma (7) als het *Global Positioning System* (GPS) om daarmee exact te bepalen waar hij zich bevindt. Om dit mogelijk te maken gebruikt het *Global Positioning System* een enorme hoeveelheid opgeslagen gegevens (8). Samen met computergegevens (8) uit gegevensbestanden over bijvoorbeeld het weer berekent een computerprogramma (7) dat zich bevindt op de hardware van de tank (3), een mogelijke projectielbaan. Een schutter gebruikt vervolgens een afvuurknop (gebruikersinterface 4) waardoor een granaat wordt afgevuurd om (hopelijk) het gewenste fysieke effect te hebben op een vijandelijke tank (2").

Bovenstaande groepering van de niet-fysieke componenten heb ik aangebracht met het oog op de door mij verwachte verschillende gevolgen van militaire operaties gericht op deze niet-fysieke componenten. Deze operaties kunnen op verschillende wijzen worden uitgevoerd bijvoorbeeld door de niet-fysieke componenten te wissen, te veranderen, onbereikbaar te maken of alleen maar te kopiëren of bestuderen om erachter te komen hoe ze werken. Bij de analyse van schade aan virtuele componenten, later in dit hoofdstuk, kom ik hierop terug.

4.3 Het cyberdomein en het internationaal recht

4.3.1 Inleiding

In Hoofdstuk 1 heb ik als uitgangspunt voor dit onderzoek geformuleerd dat het humanitair oorlogsrecht van toepassing is op militaire operaties in het cyberdomein.¹⁰⁴ Omdat het humanitair oorlogsrecht deel uitmaakt van het internationaal recht, is het goed te bezien of, en zo, ja hoe het internationaal recht in het algemeen binnen het cyberdomein van kracht is, om daarmee het uitgangspunt voor wat betreft de toepasselijkheid van het humanitair oorlogsrecht te verifiëren.

■
104 Hoofdstuk 1 par 1.1.3.

Zoals met veel nieuwe ontwikkelingen is ook met het ontstaan van het cyberdomein de vraag opgekomen over de toepasselijkheid van bestaande rechtsregimes en de daaruit voortvloeiende regels.¹⁰⁵ Vraagt deze ontwikkeling om nieuwe regels, moeten de bestaande regels worden aangepast, of kunnen de bestaande regels zo worden uitgelegd dat ze ook toepasbaar zijn op de nieuw ontstane werkelijkheid? In concreto, hoe gaat het internationaal recht om met het cyberdomein?

4.3.2 Het cyberdomein en het internationaal recht

Het cyberdomein is in het verleden wel voorgesteld als een “*purely non-legal domain*”¹⁰⁶ waar “*legal concepts of property, expression, identity, movement, and context do not apply*.”¹⁰⁷ Toch is heden ten dage de visie dat het cyberdomein onderhevig is aan recht, en ook aan internationaal recht, niet langer omstreden,¹⁰⁸ een standpunt dat ik inneem op basis van argumenten die ik baseer op een korte bespreking van een aantal bronnen van het internationaal recht.¹⁰⁹

De eerste bron die zich aandient zijn verdragen. Een algemeen verdrag voor het gebruik van het cyberdomein bestaat nog niet en op dit moment lijkt de kans daarop ook niet erg groot. Dit betekent echter niet dat zonder een dergelijk algemeen verdrag het internationaal recht niet van toepassing zou zijn. Zo zijn op deelgebieden al wel verdragen tot stand gekomen die betrekking hebben op activiteiten binnen het cyberdomein, bijvoorbeeld op het gebied van strafrecht in het hiervoor genoemde *Cybercrime*-verdrag.¹¹⁰

Of al gesproken kan worden van specifiek gewoonterecht in de gebruikelijke betekenis van het woord,¹¹¹ dat is “internationale gewoonte, als blijk van een als recht aanvaarde algemene praktijk”,¹¹² valt te betwijfelen. Toch kan de manier waarop het internationaal recht in het verleden is omgegaan met grote (technologische) ontwikkelingen een indicatie opleveren voor de manier waarop het internationaal recht toepasselijk is op activiteiten in het cyberdomein. In de geschiedenis zijn vele (technische) ontdekkingen gedaan die hebben geleid tot veelomvattende ontwikkelingen, denk hierbij bijvoorbeeld aan de ontdekking en ontwikkeling van radiotelegrafie, de luchtvaart of de ruimtevaart. Geen van deze ontwikkelingen heeft geleid tot een vorm van *non-applicability* van het internationaal recht. Deze lijn doortrekkend bestaat geen reden om aan te nemen dat dit met het ontstaan van het cyberdomein anders zou zijn.

■
¹⁰⁵ Zie bijvoorbeeld Lodder 2012.

¹⁰⁶ Tsagourias in Tsagourias & Buchan 2015, p. 13.

¹⁰⁷ Barlow 1996, p. 1.

¹⁰⁸ Tsagourias in Tsagourias & Buchan 2015, p. 13.

¹⁰⁹ Zoals weergegeven in art 38 van het Statuut van het Internationaal Gerechtshof, zie ook par. 4.2.1.

¹¹⁰ Zie par. 4.2.1.1.

¹¹¹ De regels van gewoonterecht in het algemeen met betrekking tot het humanitair oorlogsrecht zijn wel van toepassing op het cyberdomein, zij het dat de wijze waarop ze van toepassing zijn nog niet volledig duidelijk is.

¹¹² Statuut van het Internationaal Gerechtshof art. 38 lid 1b.

Verschillende vooraanstaande experts op het gebied van internationaal recht hebben geconcludeerd dat erkende rechtsbeginselen uit het internationaal recht ook van toepassing zijn op activiteiten in het cyberdomein. Zo concludeert de *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* dat “State Sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT related activities, and to their jurisdiction over ICT infrastructure within their territory.”¹¹³

De conclusie dat internationaal recht van toepassing is op activiteiten in het cyberdomein is overigens niet voor iedereen vanzelfsprekend, of zoals verwoord door Koh: “this view [international law principles do apply in cyberspace] has not necessarily been universal in the international community. At least one country has questioned whether existing bodies of international law apply to the cutting edge issues presented by the internet. Some have also said that existing international law is not up to the task, and that we need entirely new treaties to impose a unique set of rules on cyberspace.”¹¹⁴ Volgens Segal¹¹⁵ verwees Koh met ‘at least one country’ naar China en met ‘some’ naar de initiatiefnemers van de zogenaamde *International Code of Conduct for Information Security*.¹¹⁶

Deze *Code of Conduct*, in 2011 opgesteld door een groep van vier landen,¹¹⁷ was een gezamenlijke gedragscode, open voor alle landen op vrijwillige basis, met als doel “to identify the rights and responsibilities of States in information space.”¹¹⁸ De aanbiedingsbrief maakt duidelijk dat de initiatiefnemers van deze *Code of Conduct* tot doel hadden consensus te bereiken over internationale normen en regels voor het gedrag van staten binnen het cyberdomein.¹¹⁹ De steun voor dit initiatief bleef beperkt, onder meer omdat “the Code was seen as a step towards formalising new rules governing cyberspace and the use of information technology, a notion generally opposed by the US and other liberal democracies which have mostly adopted the stance that existing international law is sufficient.”¹²⁰ Toch kreeg deze *Code of Conduct* nog een vervolg in 2015,¹²¹ dus nadat de hierboven besproken *United Nations Group of Governmental Experts* concludeerde dat internationaal recht van toepassing is op het cyberdomein.¹²² De aanbiedingsbrief van de herhaalde poging om te komen tot een *Code of Conduct* vermeldde onder meer dat “An international consensus is now emerging on the need to strengthen international

113 UN general Assembly A/68/98 par. 20. Deze conclusie is vervolgens verwelkomd in een resolutie van de Algemene Vergadering van de Verenigde Naties. UN GA RES A/RES/70/327, preambule.

114 Koh 2012, p. 3.

115 Segal 2012.

116 UN General Assembly A/66/359.

117 China, de Russische Federatie, Tadzjikistan en Oezbekistan

118 UN General Assembly A/66/359, p. 4.

119 UN General Assembly A/66/359, p. 1.

120 Rõigas 2015.

121 UN General Assembly A/69/723. Nu gesteund door China, Kazachstan, Kirgizstan, de Russische Federatie, Tadzjikistan en Oezbekistan.

122 In de *UN Group of Governmental Experts* waren zowel China als Rusland vertegenwoordigd. In het rapport wordt expliciet gemeld dat kennis is genomen van de voorgestelde *Code of Conduct*, UN General Assembly A/68/98, par. 18.

*cooperation and formulate relevant norms.*¹²³ Het blijft daarmee onduidelijk of de oproep tot formulering van relevante normen gedaan is omdat, volgens de initiatiefnemers, dergelijke normen ontbreken in het internationaal recht, of dat de ondertekenaars andere motieven nastreefden.¹²⁴ De hernieuwde poging om te komen tot een *International Code of Conduct for Information Security* is echter niet in stemming gebracht binnen de Algemene Vergadering van de Verenigde Naties, zodat onduidelijk is gebleven hoe groot de steun voor deze opvatting was.

Bovenstaande argumenten, ondanks het tegengeluid van de *Code of Conduct*, zijn voor mij voldoende overtuigend om het eens te zijn met de conclusie van de eerder genoemde *United Nations Group of Governmental Experts* dat “international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”¹²⁵

Het uitgangspunt dat het internationaal recht van toepassing is op activiteiten in het cyberdomein betekent echter niet dat daarmee duidelijk is hoe het internationaal recht moet worden toegepast op of binnen het cyberdomein. De conclusie gaat namelijk vaak gepaard met een kwalificatie als “international law should adapt its rules in order to grapple with the particularities of cyberspace”.¹²⁶ Met andere woorden, het internationaal recht kan niet altijd direct worden toegepast op het cyberdomein. Hiervoor is nadere studie, uitleg en misschien in sommige situaties zelfs aanpassing noodzakelijk.

Het is derhalve niet meer de vraag of het internationaal recht toepasselijk is, maar hoe dit moet worden toegepast.¹²⁷ Deze laatste vraag is ook verwoord in het verzoek van de Algemene Vergadering van de Verenigde Naties aan de Secretaris Generaal om gezamenlijk met een *United Nations Group of Governmental Experts* “continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States.”¹²⁸ Bij de verdere studie naar de wijze waarop het internationaal recht toegepast moet worden kan de *Talinn Manual 2.0* zeker van betekenis zijn, of zoals de toenmalig Nederlandse Minister van Buitenlandse Zaken Koenders opmerkte: “the Manual will continue to play an important role in the continuing dialogue regarding how international law applies to cyber activities.”¹²⁹

123 UN General Assembly A/69/723, p. 1.

124 Zie bijv. Lewis 2014. Hij noemt de *Code of Conduct* “an ill-disguised effort to dilute the Universal Declaration of Human Rights.” Segal 2012, “China wants new treaties governing cyberattacks. Could there be an ulterior motive?”

125 UN General Assembly A/68/98, par. 19 en later herhaald in UN General Assembly A/70/174, par. 24.

126 Tsagourias in Tsagourias & Buchan 2015, p. 13.

127 Zie bijv. het standpunt van het Verenigd Koninkrijk *Cyber and International Law in the 21st Century*, p.3. Available on <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, laatst geraadpleegd 28 nov 2018. “The UK has always been clear that we consider cyber space to be an integral part of the rules based international order that we are proud to promote. The question is not whether or not international law applies, but rather how it applies and whether our current understanding is sufficient.”

128 UN General Assembly A/RES/237, par. 5.

129 Koenders in Schmitt 2017, p. xxvii.

De conclusie dat internationaal recht van toepassing is op activiteiten in het cyberdomein, maar nog niet eenduidig helder is hoe de specifieke toepassing van het internationaal recht binnen het cyberdomein moet plaatsvinden, versterkt mijn positie (en uitgangspunt) dat het humanitair oorlogsrecht, als onderdeel van het internationaal recht, van toepassing is op militaire operaties in het cyberdomein. Het versterkt ook de stelling dat ‘van toepassing zijn’ niet voldoende is bij het zoeken naar een oplossing voor de interpretatie en toepassing van bestaande regels. Ik zal daarom in de volgende paragraaf nader ingaan op de vraag hoe het humanitair oorlogsrecht toegepast kan worden op militaire operaties in het cyberdomein.

Een van de uitdagingen is de interpretatie van het begrip ‘aanval’, zoals gedefinieerd in artikel 49 Aanvullend Protocol I, wanneer deze plaatsvindt in, of via, het cyberdomein. Hoe moet het begrip cyberaanval binnen het humanitair oorlogsrecht worden verstaan? Dit vormt het onderwerp van de laatste paragraaf van dit hoofdstuk, maar voor ik daaraan kan beginnen zal ik eerst aandacht besteden aan het meeromvattende begrip, militaire cyberoperaties.

4.4 Militaire cyberoperaties

4.4.1 Inleiding

Daar waar binnen het humanitair oorlogsrecht een algemeen gebruikte definitie ontbreekt voor militaire operaties in traditionele zin,¹³⁰ geldt dit in nog sterkere mate voor militaire operaties in het relatief nieuwe cyberdomein. De grote diversiteit aan gebruikers van het cyberdomein, die elk vanuit hun eigen standpunt en daarmee samenhangend met hun eigen idioom over het cyberdomein praten en schrijven,¹³¹ maakt definiëring zeker niet eenvoudiger. Toch is een heldere beschrijving nodig, omdat dit (mede) bepaalt of een operatie wel of niet onder het regime van het humanitair oorlogsrecht valt.¹³²

Als binnen het paradigma van ‘oorlogvoering’, waarop het regime van het humanitair oorlogsrecht van toepassing is, gesproken wordt over operaties,¹³³ heb ik deze gedefinieerd als “acties uitgevoerd door militairen en/of met militaire middelen om een specifieke

130 Zie Hoofdstuk 2, par. 2.5.3.

131 Ducheine in Tsagourias & Buchan 2015, p. 214 schrijft bijvoorbeeld over cyberoperaties: “suitable or not, the term cyber operations seems to become a common denominator for activities in cyberspace, undertaken with the aim of achieving objectives in or through this digital domain. The common denominator however, can be, and indeed is, used in a great variety of situations, by a diversity of actors and, quite obviously, for various reasons,” mijn accentuering.

132 Vergelijk de media-aandacht die de uitspraak van de Nederlandse Minister van Defensie kreeg naar aanleiding van een vrijdelde Russische poging de Organisatie voor het Verbod op Chemische Wapens (OPCW) te hacken. Zij beaamde, reagerend op een vraag, dat Nederland in een “cyberoorlog” met Rusland is verwickeld. In antwoord op vragen vanuit de Tweede kamer nuanceerde zij dit door op te merken: “het karakter van conflicten verandert voortdurend. Dat is wat ik [...] heb gezegd. Oorlogvoering verandert in die zin en wordt meer hybride. Dat is de letterlijke tekst die ik voor mijn rekening heb genomen. Oorlog in de meest traditionele zin is dus achterhaald. Conflicten zijn complexer en meer hybride geworden. Ik heb ook op die diffuse situatie gewezen. Uiteraard is er geen sprake van oorlog in internationaalrechtelijke zin.” Kamerstukken II 2018-2019 29924 nr. 176, p. 21.

133 Zie ook Ducheine & Voetelink 2011, p. 282-283.

doelstelling, namelijk een militair voordeel behalen ten opzichte van de tegenstander, te verwezenlijken.¹³⁴ Binnen het humanitair oorlogsrecht bestaan specifieke regels voor militaire operaties binnen een bepaald domein,¹³⁵ maar deze hangen samen met de kenmerken van dat domein en niet met het concept van militaire operaties. Onafhankelijk van het domein zijn de regels gebaseerd op dezelfde grondbeginselen. Zo maakt het voor het humanitair oorlogsrecht niet uit of een raket, afgevuurd vanaf de grond ter onderschepping van een vliegtuig, gerekend wordt tot een militaire operatie in het land- of in het luchtdomein. Waar het om gaat is of het betreffende vliegtuig een militair doel is. Het humanitair oorlogsrecht is, net als de grondbeginselen waarop het is gebaseerd, onafhankelijk van het domein waarin het gewapend conflict zich afspeelt.¹³⁶

Uit bovenstaande blijkt vooralsnog geen reden om aan te nemen dat dit voor het cyberdomein anders zou zijn. In de praktijk worden militaire cyberoperaties niet anders behandeld dan andere militaire operaties. Zo definieert bijvoorbeeld de *Air and Missile Warfare Manual* een *Computer Network Attack* als “operations to manipulate, disrupt, deny, degrade or destroy information resident in computers and computer networks, or the network itself, or to gain control over the computer or computer network.”¹³⁷ In de *Commentary* van deze *Manual* wordt een *Computer Network Attack* beschreven als een vorm van het bredere begrip ‘informatie operaties’ met als specifieke kenmerk dat de uitvoering van de operatie geschiedt middels een *data stream*.¹³⁸ De *Air and Missile Manual* behandelt deze vorm van militaire operaties, die plaatsvinden in het cyberdomein, op dezelfde manier als militaire operaties in andere domeinen. Overigens betekent de term *Computer Network Attack* niet automatisch dat al deze operaties ook onder ‘aanval’ in de zin van artikel 49 Aanvullend Protocol I vallen.¹³⁹ Wanneer een *Computer Network Attack* resulteert in “death, injury, damage or destruction of persons or objects” is de drempel van aanval gehaald,¹⁴⁰ terwijl dit niet het geval is bij “inconvenience (such as temporary denial of Internet access).”¹⁴¹

Als militaire operaties niet domeinafhankelijk zijn, kan ik de eerder aangehaalde definitie van militaire operaties ook op het cyberdomein toepassen. Vanwege de specifieke eigenschappen van het cyberdomein is het nog wel noodzakelijk de invloed van de toevoeging ‘cyber’ aan militaire operaties te bespreken voordat ik kan onderzoeken welke mogelijke invloed dit heeft op de toepassing van de regels van het humanitair oorlogsrecht.

■
134 Zie Hoofdstuk 2, par. 2.5.3.

135 Zo resulteerden bijvoorbeeld de Haagse Vredesconferenties in *Hague Convention IV Respecting the Laws and Customs of War on Land* en *Hague conventions VII, VIII, IX, XI en XIII* welke laatste conventies verschillende aspecten van oorlog ter zee bevatten.

136 Zie ook Hoofdstuk 1, par. 1.1.3.

137 HPCR 2009, p. 3.

138 HPCR 2010, p. 34.

139 HPCR 2010, p. 34.

140 HPCR 2010, p. 28.

141 HPCR 2010, p. 28.

4.4.2 Militaire cyberoperaties

Net als bij het cyberdomein bestaan voor de beschrijving van militaire cyberoperaties een veelheid van definities en beschrijvingen die, mede gelet op de snelle ontwikkelingen in dit nieuwe domein, vaak nog in ontwikkeling zijn.¹⁴² Voorbeelden zijn de Amerikaanse definitie: “*The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace*”¹⁴³ of “*operations against or via computer or a computer system through a data stream*”¹⁴⁴ waarbij ‘*through a data stream*’ is toegevoegd zodat een kinetische aanval, om een computer of computersysteem uit te schakelen, uitgesloten wordt.¹⁴⁵

De *Tallinn Manual* definieert cyberoperaties als “*the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace.*”¹⁴⁶ Om dezelfde redenen als genoemd bij de definitie van het cyberdomein,¹⁴⁷ zal ik deze laatste definitie als uitgangspunt gebruiken om ‘cyber’ aan mijn definitie van militaire operaties toe te voegen. Door de toevoeging van het element ‘militair’ aan operaties¹⁴⁸ wordt de link met het humanitair oorlogsrecht benadrukt zodat ik voor dit onderzoek, en daarmee voor de toepassing binnen het paradigma van ‘oorlogvoering’, tot de volgende beschrijving van een militaire cyberoperatie kom: militaire cyberoperatie is de toepassing van cybercapaciteiten door militairen en/of met militaire middelen om een specifieke doelstelling, namelijk een militair voordeel ten opzichte van de tegenstander te behalen, in of door het gebruik van het cyberdomein.

Een aanvullende opmerking over deze beschrijving. Het militaire voordeel ten opzichte van de tegenstander is relatief. Hiermee vallen zowel operaties die negatief zijn voor de tegenstander als operaties die positief zijn voor de uitvoerder onder de definitie. Zo valt bijvoorbeeld een operatie om steun te verkrijgen onder de bevolking, waardoor de tegenstander op minder steun kan rekenen, ook onder deze definitie.

142 *Law of War Manual* 2015, p. 996. “DoD doctrine and terminology for cyber operations continue to develop.”

143 JP 1-02, p. 58.

144 Backstrom & Henderson 2012, p. 503. Dezelfde definitie wordt gebruikt in ICRC 2011, p. 36, waarbij deze wordt aangevuld met de tekst “*Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter, or otherwise manipulate processes controlled by the infiltrated computer system.*”

145 Backstrom & Henderson 2012, p. 503 voetnoot 105.

146 Schmitt 2013, p. 258. In de *Tallinn Manual* 2.0 aangevuld met de opmerking “*In this Manual, the term is generally used in an operational context*”, Schmitt 2017, p. 564.

147 Zie hiervoor par. 4.2.1.5.

148 Zie ook Ducheine & van Haaster 2013 die op basis van de eerder aangehaalde definitie van *cyberoperations* uit de *Tallinn Manual* cyberoperaties definiëren als “de inzet van cybercapaciteiten met het primaire (militaire) doel in of via cyberspace te realiseren.”

4.5 De ondergrens van aanval in het cyberdomein

4.5.1 Inleiding

Hoofdstuk 2 eindigde ik met de conclusie dat de ondergrens van het begrip ‘aanval’ de voorwaarde is die een aanval onderscheidt van andere militaire operaties die geen aanval vormen en dat die voorwaarde bestaat uit de bedoeling om fysieke schade of letsel te veroorzaken of die deze fysieke gevolgen daadwerkelijk heeft. Als niet aan deze voorwaarde voldaan is, is geen sprake van ‘aanval’. Militaire operaties die wel aan deze voorwaarde voldoen zijn ‘aanvallen’ in de zin van artikel 49 Aanvullend Protocol I.¹⁴⁹

De vraag die vervolgens rijst, of deze uitleg hetzelfde kan blijven met enkel de toevoeging van het woord cyber? Van belang is dat recht wordt gedaan aan de kenmerken van het cyberdomein, met name de niet-fysieke aard van diverse componenten.¹⁵⁰ Indien dit niet zo is dient mogelijk de ondergrens van aanval principieel anders uitgelegd te worden.

Ik zal deze vraag beantwoorden aan de hand van een nadere definiëring van cyberaanval, waarbij ik inga op het onderscheid met militaire cyberoperaties die geen aanval zijn. Dit onderscheid zal zich met name toespitsen op de vraag of ook niet-fysieke effecten kunnen leiden tot de kwalificatie van een militaire cyberoperatie als ‘aanval’ in de zin van artikel 49 Aanvullend Protocol I.

4.5.2 Wat is een cyberaanval?

Artikel 49 Aanvullend Protocol I definieert ‘aanval’ als “dadens van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve.” Wat betekent de toevoeging van ‘cyber’ aan ‘aanval’ in het begrip ‘cyberaanval’? Nog meer dan bij de definitie van cyberdomein en cyberoperaties bestaat in het gewone spraakgebruik een grote verscheidenheid aan handelingen en gebeurtenissen die worden aangeduid als ‘cyberaanval’.¹⁵¹ Zo wordt de methode om een website plat te leggen door middel van het zenden van teveel berichten, waardoor de site niet meer functioneert, stevast aangeduid met *denial of service attack*¹⁵², terwijl ook bijvoorbeeld over de *Sony-hack* van november 2014 wordt gesproken in termen van een cyberaanval.¹⁵³ Ook een Nederlandse overheidsdienst als de Algemene Inlichtingen en Veiligheidsdienst spreekt in termen van cyberaanvallen als zij de cyberdreiging voor Nederland beschrijft.¹⁵⁴ Een dergelijk brede uitleg past echter niet binnen dit onderzoek.

149 Zie Hoofdstuk 2, par. 2.6.5.

150 Zie par. 4.2.2.2.

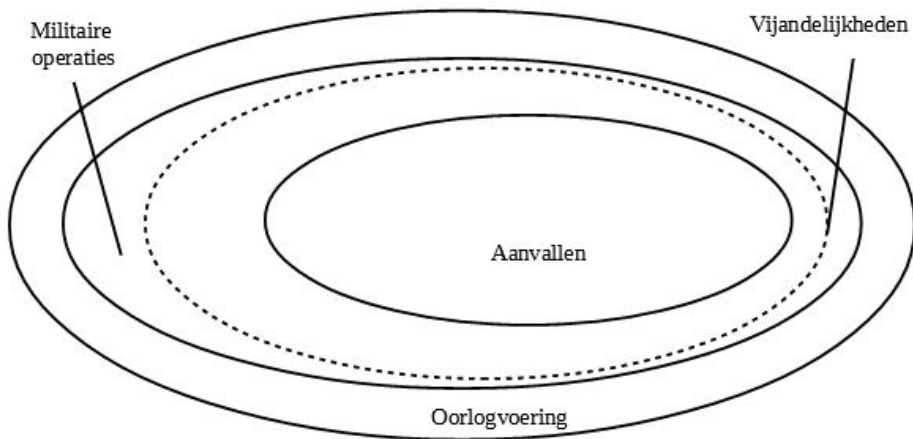
151 Zie bijvoorbeeld Ducheine et al 2012 in Ducheine, Osinga & Soeters 2012, p. 102.

152 Cambridge Business English Dictionary online edition: *definition of denial of service attack: a situation in which people intentionally prevent a website from operating by sending too many requests to use it*. Available at: <http://dictionary.cambridge.org/dictionary/english/denial-of-service>, laatst geraadpleegd 28 nov 2018.

153 Zoals blijkt uit een interne brief van Sony waarin wordt aangegeven dat het bedrijf slachtoffer is geworden van een cyberaanval. http://oag.ca.gov/system/files/12%2008%2014%20letter_o.pdf, laatst geraadpleegd 28 nov 2018. Zie ook Schneier 2014, die de sony hack een ‘*high-skill, high-focus attack*’ noemt.

154 Kamerstukken II 2015-2016, 30977, nr. 145, p. 35-37. Jaarverslag MIVD waar in Hoofdstuk 3, in de drie pagina’s die handelen over ‘cyberdreiging’ maar liefst 26 maal het woord ‘aanval’ of ‘aanvaller’ gebruikt wordt.

Ik concentreer mijzelf op cyberaanvallen als deelverzameling van militaire cyberoperaties binnen het paradigma van oorlogvoering, op dezelfde wijze als ik hiervoor aanvallen heb gezien als deelverzameling van militaire operaties.¹⁵⁵ Ter herinnering hier nogmaals de figuur die de onderlinge relaties tussen de begrippen binnen het humanitair oorlogsrecht weergeeft.



Figuur 7 Relatie tussen de begrippen binnen het humanitair oorlogsrecht.¹⁵⁶

De *Tallinn Manual* definieert een cyberaanval als een cyberoperatie, hetzij offensief, hetzij defensief, waarvan redelijkerwijs kan worden verondersteld dat die verwonding of dood van personen of schade of vernieling van objecten veroorzaakt.¹⁵⁷ Deze definitie is, net als de definitie van aanval uit artikel 49 Aanvullend Protocol, toegespitst op fysieke effecten.

Niet specifiek benoemd bij de commentaren bij de definitie uit de *Tallinn Manual* is of 'fysieke gevolgen' zowel slaat op directe als op indirecte fysieke gevolgen.¹⁵⁸ Toch meen ik uit een analoge toepassing van het standpunt van de expertgroep van de *Tallinn Manual* bij regel 54, over de keuze van middelen en methodes van oorlogvoering,¹⁵⁹ te kunnen concluderen dat 'fysieke gevolgen' zowel slaat op de indirecte als de directe gevolgen. Regel 54 van de *Tallinn Manual* zegt dat bij het plannen van of beslissen over een cyberaanval alle praktisch uitvoerbare voorzorgen genomen moeten worden bij de keuze van middelen en methoden van oorlogvoering, zodat bijkomend verlies van mensenlevens onder de burgerbevolking, verwonding van burgers en schade aan of vernietiging van burgerobjecten wordt

¹⁵⁵ Zie Hoofdstuk 2, par. 2.5.

¹⁵⁶ Grotendeels gebaseerd op Ducheine 2008, p. 486.

¹⁵⁷ Schmitt 2013, p. 106, *Rule 30 definition of cyber attack*. Schmitt 2017, p. 415, *rule 92*.

¹⁵⁸ Het verschil tussen directe en indirecte gevolgen wordt gevormd door het feit of er wel of geen gebeurtenissen of mechanismen plaatsvinden tussen de aanval en de gevolgen. JP 3-60 (2007), p. 1-10.

¹⁵⁹ Schmitt 2013, p. 168.

voorkomen of tenminste wordt geminimaliseerd.¹⁶⁰ De toelichting vermeldt dat de kwestie van indirecte gevolgen met name speelt bij cyberoperaties vanwege de verbondenheid tussen computers, specifiek tussen militaire en civiele systemen, om vervolgens te concluderen dat voor deze regel zowel de directe als de indirecte fysieke gevolgen meegenomen moeten worden.¹⁶¹ Het zou vreemd en zelfs onlogisch zijn, indien de indirecte fysieke gevolgen wel meegenomen moeten worden bij het plannen of beslissen over keuze van een cyberaanval maar niet bij de definitie van cyberaanval zelf. Daarom moet bij het bepalen van de ‘fysieke gevolgen’ van cyberaanval uitgegaan worden van “*any reasonably foreseeable consequential damage*”¹⁶² die kan bestaan uit zowel directe als indirecte schade.

Bij bovenstaande definitie van een cyberaanval uit de *Tallinn Manual* geldt als uitgangspunt dat “*it is the use of violence against a target that distinguishes attacks from other military operations.*”¹⁶³ Ik zal deze definitie met bijbehorend uitgangspunt gebruiken om aan de hand van een aantal discussies die spelen binnen het humanitair oorlogsrecht, uiteindelijk te komen tot de beantwoording van de centrale vraag van dit hoofdstuk, namelijk de vraag naar de ondergrens van ‘aanval’ in de zin van artikel 49 Aanvullend Protocol I voor militaire operaties in het cyberdomein.

4.5.3 Twee verschillende denkrichtingen

Bovenstaande definitie van een cyberaanval uit de *Tallinn Manual*, met de daarbij behorende beperking dat een militaire cyberoperatie fysieke gevolgen moet hebben om te kwalificeren als aanval, is niet onomstreden. De discussie hierover, ook wel aangeduid als het Schmitt-Dörmann debat,¹⁶⁴ woedt al enige jaren en zal nog wel enige tijd aanhouden.¹⁶⁵ Uit bovenstaande definitie van cyberaanval volgt impliciet dat twee soorten doelen onderkend worden, namelijk personen en objecten. Ten aanzien van personen bestaan in het kader van het genoemde Schmitt-Dörmann debat geen meningsverschillen. Naast dood en fysieke verwonding vallen ook “*serious illness and severe mental suffering that are tantamount to injury*”¹⁶⁶ binnen de definitie van cyberaanval. Omdat hierover geen meningsverschillen bestaan zal ik pas in het volgende hoofdstuk terugkomen op de gevolgen voor personen als ik de regels van het humanitair oorlogsrecht bespreek die gelden beneden de grens van aanval. Heel anders verloopt het debat over cyberaanvallen op objecten. Alvorens mijn positie in deze discussie te geven zal ik eerst de verschillende standpunten duiden.

■
160 Schmitt 2013, p. 168.

161 Schmitt 2013, p. 169.

162 Schmitt 2013, p. 107.

163 Schmitt 2013, p. 106.

164 Zie bijv. Harrison-Dinniss 2011, p. 2.

165 Schmitt 2014a, p. 204.

166 Schmitt 2013, p. 108.

In 2002 kwam Schmitt met het artikel “*Wired Warfare: Computer Network Attack and Jus in Bello*”¹⁶⁷ waarin hij een ‘permissieve’ benadering¹⁶⁸ van het begrip ‘aanval’ met betrekking tot cyberoperaties hanteerde. Dit hield in dat hij vasthield aan het criterium dat alleen militaire operaties die “*are intended to, or would foreseeably, cause injury, death, damage or destruction*” gelden als aanval.¹⁶⁹ Indien een militaire cyberoperatie geen van deze fysieke gevolgen heeft, is het, volgens deze ‘permissieve’ benadering, geen aanval en valt het niet onder de regels die in het humanitair oorlogsrecht gelden voor aanvallen, dus ook niet onder het verbod op aanvallen op individuele burgers of de burgerbevolking¹⁷⁰ en burgerobjecten.¹⁷¹ Hierdoor mogen militaire cyberoperaties, zolang deze operaties maar geen fysieke gevolgen hebben, gericht worden op of tegen burgers en burgerobjecten. Deze redenering vergroot de mogelijkheden voor militaire operaties (maar niet voor aanvallen) gericht op burgers of burgerobjecten aanzienlijk.¹⁷² Deze nieuwe mogelijkheden, gecreëerd door technologische ontwikkeling, ziet Schmitt niet als verzwakking van de normatieve architectuur van het humanitair oorlogsrecht, omdat de bestaande normen intact blijven.¹⁷³ Hij maakte hierbij gebruik van de analogie met psychologische operaties gericht tegen of op de civiele bevolking. Zolang deze operaties niet bedoeld zijn om angst aan te jagen en geen fysiek nadeel opleveren zijn ze volledig toegestaan.¹⁷⁴

Een reactie op dit standpunt bleef niet uit. Dörmann reageerde in het artikel “*Applicability of the Additional Protocols to Computer Network Attacks*”¹⁷⁵ met een ‘restrictieve’ benadering,¹⁷⁶ gebaseerd op de stelling dat ook militaire operaties die “*the mere disabling of an object, such as shutting down of the electricity grid, without destroying it*” beogen of veroorzaken, als aanval gekwalificeerd moeten worden.¹⁷⁷ De redenering hierachter is gebaseerd op de definitie van militair doel uit artikel 52 Aanvullend Protocol I, waarin een object een militair doel is, als gehele of gedeeltelijke vernietiging of verovering maar ook ‘onbruikbaarmaking’ (*neutralization*) leidt tot een duidelijk militair voordeel.¹⁷⁸ Deze redenering leidt tot de conclusie dat, op basis van het grondbeginsel van onderscheid, de burgerbevolking of

■
167 Schmitt 2002.

168 Schmitt 2014a, p. 191. In de originele Engelse tekst aangeduid als *permissive*.

169 Schmitt 2002, p. 378.

170 Aanvullend Protocol I, art. 51 lid 2.

171 Aanvullend Protocol I, art. 52 lid 1.

172 Schmitt 2002, p. 378. Schmitt gebruikt de term *dramatically*. In dezelfde zin DoD Law of War Manual 2016, p. 1023, “*Cyber operations that result in non-kinetic or reversible effects can be an important tool in creating options that minimize unnecessary harm to civilians. In this regard, cyber capabilities may in some circumstances be preferable, as a matter of policy, to kinetic weapons because their effects may be reversible, and they may hold the potential to accomplish military goals without any destructive kinetic effects at all.*”

173 Schmitt 2002, p. 378.

174 Schmitt 2002, p. 378.

175 Dörmann 2004.

176 Schmitt 2014a, p. 191. In de originele Engelse tekst aangeduid als *restrictive*.

177 Dörmann 2004, p. 4.

178 Aanvullend Protocol I, art 52 lid 2.

burger objecten nooit het legitieme doelwit van een militaire operatie kunnen zijn, ook niet als de operatie niet resulteert in beschadiging of als de effecten omkeerbaar zijn.¹⁷⁹

De discussie tussen de ‘permissieve’ en de ‘restrictieve’ benadering was relatief statisch totdat de *Tallinn Manual* in 2013 met de zogenaamde ‘functionaliteitstest’ kwam, waarin de functionaliteit van het object, als doelwit van een cyberoperatie, centraal staat.¹⁸⁰ In deze functionaliteitstest is een cyberoperatie die een storing veroorzaakt in de functionaliteit van het doelwit, zodat dit als het ware (tijdelijk) onbruikbaar is, te kwalificeren als ‘schade’ zoals gebruikt in de definitie van cyberaanval.¹⁸¹ Deze functionaliteitstest “*appropriately addresses fair criticism that the permissive approach fails to adequately constrain the effects of cyber operations on the civilian population. At the same time, it adds a degree of clarity as to where the threshold of attack lies that is missing in the restrictive approach.*”¹⁸² Ook bij deze functionaliteitstest blijft echter onduidelijkheid bestaan over wat exact verstaan dient te worden onder ‘schade’.¹⁸³ De meningen van de *International Group of Experts* van de *Tallinn Manual* liepen hierover uiteen. Enkelen vonden dat verstoring van functionaliteit niet kwalificeert als schade.¹⁸⁴ De meerderheid vond dat verstoring van functionaliteit “*qualifies as damage if restoration of functionality requires replacement of physical components.*”¹⁸⁵ Deze meerderheid was vervolgens verdeeld over de kwalificatie ‘schade’ indien de functionaliteit hersteld kan worden door herinstallatie van besturingssoftware. Enkelen gingen nog verder door te stellen dat het verlies van functionaliteit van een doelwit *an sich* voldoende is om te kwalificeren als ‘schade’, en daarmee als cyberaanval, zelfs als alleen het herstel van gegevens nodig is voor herstel van de functionaliteit.¹⁸⁶

Uit bovenstaande discussie blijkt dat verschil van mening bestaat over de gevolgen van verstoring van de functionaliteit van een systeem door bijvoorbeeld beschadiging, verandering, vernietiging, of het ontoegankelijk maken van virtuele componenten van het cyberdomein. De ‘permissieve’ benadering, zoals initieel voorgesteld door Schmitt, biedt volgens sommigen te veel mogelijkheden voor militaire operaties gericht op virtuele componenten met verstreckende gevolgen voor de civiele bevolking. De ‘restrictieve’ benadering gaat uit van de grondgedachte dat op basis van onderscheid, als grondbeginsel van het humanitair oorlogsrecht, civiele objecten nooit een legitiem doel van een militaire operatie kunnen zijn. In deze benadering wordt ‘militaire operatie’ en ‘aanval’ als equivalent gezien. De definitie van militair doel is “*not dependent on the method of warfare used and must be applied both to kinetic and non-kinetic means; the fact that a cyber operation does not lead to the destruction*

179 Dörmann 2004, p. 5.

180 Schmitt 2014a, p. 192.

181 Schmitt 2013, p. 108, *rule* 30 par 10.

182 Schmitt 2014a, p. 192.

183 Schmitt 2013, p. 108.

184 Schmitt 2013, p. 108.

185 Schmitt 2013, p. 108.

186 Schmitt 2013, p. 109.

*of an attacked object is also irrelevant.*¹⁸⁷ Deze laatste benadering naar de letter toegepast, betekent dat alle cyberoperaties gericht op civiele objecten, bijvoorbeeld het tijdelijk onbereikbaar maken van een civiele website (bijvoorbeeld door deze te overladen met verzoeken om informatie),¹⁸⁸ onder de definitie van ‘aanval’ komen, en daardoor verboden zijn. Deze opvatting wordt door diverse schrijvers als te vergaand gezien.¹⁸⁹

In deze discussie speelt de status van virtuele componenten een grote rol waarbij niet alle virtuele componenten, zoals programma’s en computergegevens, dezelfde status lijken te hebben of zoals Boothby met een verwijzing naar George Orwell’s *Animal Farm* het verwoordt, “*some data are more equal than others.*”¹⁹⁰ Daarom zal ik in de volgende paragraaf onderzoeken wat de status van de verschillende virtuele componenten van het cyberdomein binnen het humanitair oorlogsrecht is. In de laatste paragraaf kan ik vervolgens ingaan op de vraag of beschadiging, verandering of vernietiging schade oplevert in de zin van de voornoemde definitie van cyberaanval, en daarmee ook of een cyberoperatie wel of niet kwalificeert als ‘aanval’ in de zin van artikel 49 Aanvullend Protocol I.

4.5.4 De status van virtuele componenten in het humanitair oorlogsrecht

4.5.4.1 Inleiding

Traditioneel gezien kent het humanitair oorlogsrecht een tweedeling in militaire doelen: personen en objecten.¹⁹¹ In het vorige hoofdstuk heb ik geconcludeerd dat het begrip ‘object’ uit de definitie van militair doel zoals weergegeven in artikel 52 Aanvullend Protocol I in traditionele fysieke operaties weinig problemen oplevert.¹⁹² Met object wordt bedoeld op zichtbare en tastbare objecten.¹⁹³ Maar hoe werkt het begrip object uit de definitie van militair doel door in het cyberdomein? Wat is de status van virtuele componenten, die immers niet zichtbaar noch tastbaar zijn, en hebben de verschillende virtuele componenten dezelfde status? Kunnen virtuele componenten een militair doel vormen? Kan de klassieke indeling binnen het humanitair oorlogsrecht gehandhaafd blijven of moet een nieuwe categorie ingebracht worden?

4.5.4.2 Is de indeling personen-objecten voldoende?

Zoals opgemerkt in de inleiding kent het humanitair oorlogsrecht traditioneel gezien twee soorten militaire doelen: personen en objecten. De vraag die opkomt is of deze indeling

187 ICRC 2011, p. 37.

188 Deze methode wordt meestal aangeduid met de Engelse term DOS, *Denial of service*.

189 Harrison-Dinniss 2015, p. 42, Dinstein 2016, p. 143, Schmitt 2014b, p. 297.

190 Boothby in Nasu & McLaughlin 2014, p. 61.

191 Zie bijv. art 48 Aanvullend Protocol I waar als grondregel voor onderscheid een tweedeling wordt gemaakt tussen personen (burgerbevolkingen en combattanten) en objecten (burgerobjecten en militaire doelen). Dinstein 2010, ‘*Lawful targets of attack*’, p. 89-120, de opbouw van de *Tallinn Manual* Hoofdstuk 4 sectie 3 en 4, Mačák 2015, p. 64.

192 Zie Hoofdstuk 3 par. 3.3.3.6.

193 Sandoz, Swinarski & Zimmerman 1987, p. 634.

uitputtend is, of dat nog andere categorieën mogelijk zijn? Beide mogelijke antwoorden op deze vragen leveren problemen op.

Een negatief antwoord op de vraag of binnen het humanitair oorlogsrecht alleen personen en objecten militaire doelen kunnen zijn, betekent dat er nog een, of misschien wel meer, categorieën militaire doelen bestaan. Een van die nieuwe categorieën zou dan de niet-fysieke componenten van het cyberdomein kunnen zijn. Het probleem is dat deze uitleg *“does not sit easily with the underlying dichotomy within the law between people and things.”*¹⁹⁴ Daarnaast zouden voor deze nieuwe categorie, juist omdat hij nieuw is, nog geen regels of criteria bestaan voor wanneer de virtuele componenten een legitiem militair doel vormen.¹⁹⁵ Voor objecten bestaat namelijk de tweeledige eis dat zij naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage moeten leveren tot de krijgsv verrichtingen en dat de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel oplevert.¹⁹⁶ Voor personen volgt het zijn van legitiem militair doel uit de status van combattant¹⁹⁷ of uit de directe deelname aan de vijandelijkheden.¹⁹⁸ Het gegeven dat binnen het humanitair oorlogsrecht tot op heden altijd uitgegaan is van de tweedeling personen-objecten, brengt met zich mee dat nooit criteria zijn vastgesteld waaraan een eventuele nieuwe categorie zou moeten voldoen om een legitiem militair doel te zijn. Introductie van een nieuwe categorie, bijvoorbeeld die van niet-fysieke componenten van het cyberdomein, creëert een categorie militaire doelen waarvan (nog) onduidelijk is wanneer ze legitiem mogen worden aangevallen. Dit maakt de introductie van een nieuwe categorie naar mijn mening vooralsnog onwenselijk.

Afwijzen van een derde categorie militaire doelen heeft als consequentie dat de virtuele componenten van het cyberdomein personen of objecten zouden moeten zijn om de regels voor aanvallen toepasbaar te laten zijn. De virtuele componenten voldoen niet aan de kwalificatie personen,¹⁹⁹ waardoor slechts twee opties open blijven. In de ene optie zijn de virtuele componenten van het cyberdomein objecten in zin van artikel 52 lid 2 Aanvullende

194 Harrison-Dinniss 2015, p. 45-46.

195 Mačák 2015.

196 Aanvullend Protocol I art. 52 lid 2, accentuering toegevoegd.

197 Aanvullend Protocol I art. 43 lid 2, de leden van de strijdkrachten van een partij bij het conflict, die niet zijn medisch personeel of geestelijke verzorgers op wie artikel 33 van het Derde Verdrag betrekking heeft, zijn combattanten en hebben derhalve het recht om rechtstreeks aan de vijandelijkheden deel te nemen.

198 Zie bijvoorbeeld Aanvullend Protocol I art. 51 lid 3 waaruit blijkt dat burgers bescherming genieten behalve indien en zolang zij rechtstreeks aan de vijandelijkheden deelnemen.

199 Dit staat vooralsnog buiten discussie. De huidige groei aan mens-machine interfaces (Duchaine, van Haaster & Harskamp 2017, p 161) kan er echter voor zorgen dat in de (nabije) toekomst de scheiding mens-object minder vanzelfsprekend wordt. Neem de combattant die een zogenaamd exoskelet draagt om zwaardere lasten mee te kunnen nemen. Is een operatie gericht tegen de besturingssoftware van het exoskelet een operatie tegen een object of tegen de combattant? Zolang het een exoskelet betreft lukt het onderscheid nog wel, maar wat als het ondersteunende skelet gedeeltelijk (chirurgisch) is ingebracht? Of als het gaat om op afstand beïnvloedbare nanobots die lichaamsfuncties van een combattant optimaliseren? Dit lijkt allemaal science fiction, maar volgens sommigen, zie bijv. Bostrom 2014, zijn dit soort zaken al gedeeltelijk mogelijk en nog veel verdergaande ontwikkelingen binnen handbereik. De vraag welke juridische implicaties dit mogelijk heeft, niet alleen humanitair oorlogsrechtelijk maar in bredere zin, verdient zeker nader onderzoek. Zie ook Liivoja & Chircop 2018, p. 162, die in dit verband spreken van de *“thingification of warfighters”*.

Protocol I (die legitiem aangevallen mogen worden indien ze voldoen aan de tweeledige eis zoals hierboven genoemd). In dat geval moet afgeweken worden van de visie dat ‘object’ in artikel 52 lid 2 Aanvullend Protocol I verwijst naar zichtbare en tastbare objecten.²⁰⁰ In de andere optie zijn het geen objecten en kunnen de regels met betrekking tot aanval niet toegepast worden. In dat geval moet een manier gevonden worden om recht te doen aan het feit dat militaire cyberoperaties specifiek gericht kunnen worden op virtuele componenten van het cyberdomein.

Een mogelijkheid om virtuele componenten doel van een cyberoperatie te laten zijn zonder deze componenten aan te merken als object, is gevolgd door de samenstellers van de *Tallinn Manual*. De meerderheid van de samenstellers kwam tot de conclusie dat *“the law of armed conflict notion of object should not be interpreted as including data. Data is intangible and therefore neither falls within the ‘ordinary meaning’ of the term object nor comports with the explanation of it offered in the ICRC Additional Protocols Commentary.”*²⁰¹ Ondanks deze conclusie kunnen volgens deze meerderheid de virtuele componenten wél het doelwit zijn van militaire cyberoperaties. Het betreft dan een *“military objective in operational sense, but they do not constitute a military objective in the legal sense.”*²⁰² Indien een dergelijke operatie resulteert in de dood van individuen of schade of vernietiging van fysieke objecten, vormen die individuen of objecten de juridische ‘objects of attack’ en geldt de militaire operatie als een aanval.²⁰³

De conclusie dat de virtuele componenten géén (juridisch) object in de zin van artikel 52 lid 2 Aanvullend Protocol I zijn, werd niet gedeeld door een minderheid van de *Tallinn Manual* expert groep. Deze minderheid was van mening dat *“for the purpose of targeting, data per se should be regarded as an object”*.²⁰⁴ Dit standpunt werd door de meerderheid in 2013 gekwalificeerd als *de lege ferenda*,²⁰⁵ en in 2017 verwoord als: niet in overeenstemming met *“the current state of the law.”*²⁰⁶ Het is de vraag of, en zo ja, hoe lang, deze meerderheidsvisie nog stand houdt. Zo schrijft bijvoorbeeld Schmitt: *“This view is unlikely to endure. Today, the importance of data usually exceeds that of their physical manifestation”*.²⁰⁷

Verschillende schrijvers hebben op andere manieren getracht bovenstaande discrepantie over de status van de virtuele componenten van het cyberdomein op te lossen.

Boothby volgt bijvoorbeeld de redenering dat *“it is the functionality of the target computer system that constitutes the ‘object’”*,²⁰⁸ waarmee hij aanhaakt op de eerder beschreven

■
200 Sandoz, Swinarski & Zimmerman 1987, p. 634.

201 Schmitt 2013, p. 127.

202 Schmitt 2013, p. 126.

203 Schmitt 2013, p. 108.

204 Schmitt 2013, p. 127.

205 Schmitt 2013, p. 127.

206 Schmitt 2017, p. 437.

207 Zie ook Schmitt 2014b, p. 297. Deze opvatting is geheel in lijn met de door Keulen (2018) beschreven trend van *dematerialization*, zie Hoofdstuk 1 par. 1.1.2.

208 Boothby in Nasu & McLaughlin 2014, p. 61.

functionaliteitstest.²⁰⁹ Door de functionaliteit als ‘object’ te bestempelen doet de vervolgvraag zich voor, wanneer is deze functionaliteit beschadigd?²¹⁰ Het antwoord op deze vraag leidt weer tot de uiteenlopende antwoorden zoals beschreven bij de functionaliteitstest.²¹¹

Mačák is in zijn artikel *Military Objectives 2.0* kritisch op de conclusie van de *Tallinn Manual*.²¹² Hij redeneert als volgt. Doordat de *Tallinn Manual* virtuele componenten beziet als niet-tastbaar, waardoor deze niet voldoen aan de betekenis van object uit artikel 52 lid 2 Aanvullend Protocol I, kunnen zij geen militair doel zijn. De belangrijkste consequentie is vervolgens dat cyberoperaties gericht tegen deze virtuele componenten “*would not fall within the ambit of IHL unless it would affect the functionality of a control system resulting in the need to replace its physical components.*”²¹³ Het rechtstreeks gevolg daarvan is dat “*many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace.*”²¹⁴ Dit is volgens hem niet alleen in strijd met een teleologische uitleg van het begrip object uit artikel 52 Aanvullend Protocol I maar ook met “*the object and purpose of the Protocol.*”²¹⁵ Voor Aanvullend Protocol I is een van de belangrijke, zo niet de belangrijkste doelstelling, namelijk “*to improve the protection of victims of armed conflicts compared to that provided by the four Geneva Conventions.*”²¹⁶ Indien twee interpretaties mogelijk zijn, virtuele componenten zijn wel of zijn geen objecten in de zin van artikel 52 Aanvullend Protocol I, “*we must thus choose the one which better serves the identified object and purpose of the Protocol.*”²¹⁷ De visie uit de *Tallinn Manual* “*expands the list of legitimate targets*”²¹⁸ en daarom moet voor de andere interpretatie gekozen worden. Dat wil zeggen, virtuele componenten moeten gezien worden als ‘objecten’ in de zin van artikel 52 lid 2 Aanvullend Protocol I. Deze kunnen kwalificeren als militair doel. Om daadwerkelijk aangemerkt te worden als militair doel moeten de virtuele componenten wel voldoen aan de hiervoor beschreven tweeledige eis die artikel 52 Aanvullend Protocol I daarvoor stelt aan objecten.

Een laatste beschouwing over de status van de virtuele componenten van het cyberdomein die ik hier wil aanhalen is die van Harrison-Dinniss, omdat zij onderscheid maakt in de gevolgen van beschadiging of vernietiging van verschillende vormen van virtuele componenten. In haar bijdrage *The Nature of Objects*²¹⁹ gaat zij in op de definitie van militair

209 Zie par. 4.4.2.

210 Bootby in Nasu & McLaughlin 2014, p. 62.

211 Zie hiervoor par. 4.4.2.

212 Mačák 2015.

213 Mačák 2015, p. 59.

214 Mačák 2015, p. 78. Als voorbeelden noemt hij “*digital records for the functioning of modern-day governments with respect to census taking, the provision of special benefits, voting and taxation.*”

215 Mačák 2015, p. 80.

216 Mačák 2015, p. 80.

217 Mačák 2015, p. 80.

218 Mačák 2015, p. 80.

219 Harrison-Dinniss 2015.

doel uit artikel 52 Aanvullend Protocol I, en concludeert dat deze definitie virtuele componenten niet uitsluit. Het is weliswaar “*indisputable that the dictionary definitions of both the English and French terms, as referred to in the ICRC Commentary, refer to material things that are perceivable by the senses*”,²²⁰ maar dit wordt in de *Commentary* slechts aangehaald om het verschil met de ‘*aim or purpose*’ van een militaire operatie aan te geven en niet specifiek om niet-tastbare objecten uit te sluiten.²²¹ Met andere woorden, virtuele componenten kunnen gewoon een militair doel zijn net als tastbare objecten. Of dit inderdaad het geval is, wordt bepaald door de andere criteria uit de definitie van militair doel.²²²

Deze uitleg heeft echter als consequentie dat alle virtuele componenten binnen het bereik van militair doel komen, wat zij te ruim vindt, omdat “*such an expansive inclusion would take the definition of a military objective too far from its purpose in identifying the legitimate targets of attacks and military operations*.”²²³ Deze te vergaande consequentie beperkt ze op twee manieren.

Als eerste onderscheidt zij twee categorieën virtuele componenten, ‘*content-level data*’²²⁴ en ‘*operational-level data*’,²²⁵ gebaseerd op de soort schade die ontstaat door beschadiging, vernietiging of onbruikbaarmaking van gegevens. Bij ‘*content-level data*’ blijft in dat geval het systeem functioneren, terwijl bij ‘*operational-level data*’ de functionaliteit van het systeem verloren gaat.²²⁶ ‘*Content-level data*’ behoeven geen algemene bescherming, omdat de belangrijkste gegevens al afgedekt zijn door specifieke bescherming²²⁷ en omdat dit het type gegevens is waarvan meestal een back-up wordt aangehouden.²²⁸

De tweede manier om de te vergaande consequenties te beperken, is haar voorstel om bij dual-use objecten²²⁹ het militair doel te definiëren “*in its most minimal form*”.²³⁰ Zij doelt hiermee op de mogelijkheid om het militaire doel te definiëren op “*code, component, system or network level*.”²³¹ Bij de huidige uitleg wordt een object, bijvoorbeeld een netwerk, zodra het voldoet aan de eisen van militair doel uit artikel 52 lid 2 Aanvullend Protocol, in zijn geheel een militair doel. Eventueel civiel gebruik heeft geen invloed op de kwalificatie als militair doel.²³² De consequentie is dat “*any civilian traffic or data that exists purely within the system or network becomes irrelevant to the calculation [proportionalityrule] (as it forms part of the military objective*

220 Harrison-Dinniss 2015, p. 43.

221 Harrison-Dinniss 2015, p. 43. Deze visie wordt gedeeld door Lubell 2013, p. 267.

222 Zoals gegeven in Aanvullend Protocol I art. 52 lid 2.

223 Harrison-Dinniss 2015, p. 42.

224 Harrison-Dinniss 2015, p. 41.

225 Harrison-Dinniss 2015, p. 41. Deze laatste worden ook wel aangeduid als ‘*logical-level data*’ of ‘*program data*’.

226 Harrison-Dinniss 2015, p. 42.

227 Harrison-Dinniss 2015, p. 41. Als voorbeelden worden genoemd medische records en *cultural property*.

228 Indien geen back-up aanwezig is, zal het systeem desondanks blijven functioneren “*albeit with missing data*”. Harrison-Dinniss 2015, p. 41.

229 Dual-use is de aanduiding voor systemen en infrastructuur die zowel militair als civiel gebruikt worden.

230 Harrison-Dinniss 2015, p. 51.

231 Harrison-Dinniss 2015, p. 50.

232 Harrison-Dinniss 2015, p. 50.

and is no longer civilian).²³³ Als echter niet het netwerk, maar een individuele component van dat netwerk of een stuk computercode als militair doel wordt aangewezen, blijft het civiele gebruik van het netwerk en de civiele gegevens buiten het militair doel. Dit civiele gebruik en de civiele gegevens blijven in dat geval civiel en moeten meegenomen worden in de proportionaliteitstest van artikel 52 lid 2 Aanvullend Protocol I.²³⁴

Een verplichting om op basis van onderscheid het militair doel op een zo minimaal mogelijk niveau te definiëren bestaat weliswaar nog niet, maar volgt volgens Harrison Dinniss uit *“the principles of proportionality and the requirement to take all feasible precautions in attack to avoid and at least minimise harm to civilians and civilian objects.”*²³⁵

Uit bovenstaande beschouwing blijkt dat diverse auteurs hebben getracht een compromis tussen de ‘permissieve’ en de ‘restrictieve’ uitleg van aanval te beargmenteren door te kijken naar de status van virtuele componenten binnen het humanitair oorlogsrecht. Deze status ligt echter nog niet onbetwist vast en meningsverschillen zijn blijven bestaan. Een mogelijke onderliggende oorzaak hiervan, namelijk de gevolgen die men toedicht aan het wel of niet voldoen aan het toekennen van de status van object, wil ik hier nog bespreken omdat dit voortborduurt op het verschil in denkrichting²³⁶ over de betekenis van de term ‘onbruikbaarmaking’ in de definitie van militair doel zoals gegeven in artikel 52 Aanvullend Protocol I.

Een denkrichting, bijvoorbeeld toegepast door Dörmann,²³⁷ volgt de redenering dat de definitie van militair doel uit artikel 52 Aanvullend Protocol I onafhankelijk is van de methode van oorlogvoering en geldt voor alle militaire operaties gericht op, of tegen, niet-personen.²³⁸ De argumentatie van deze redenering heb ik al eerder besproken in Hoofdstuk 3 bij het beginsel onderscheid onder objecten en onbruikbaarmaking²³⁹ en komt erop neer dat de opname van ‘onbruikbaarmaking’ in de definitie van militair doel met zich meebrengt dat het niet relevant is of de onbruikbaarheid komt door vernieling of door een andere oorzaak. De onbruikbaarheid is doorslaggevend.²⁴⁰ Militaire operaties en aanvallen zijn in deze visie equivalenten en moeten voldoen aan dezelfde regels. Als een militaire operatie geen aanval is, valt het daarmee buiten de regulering van het humanitair oorlogsrecht.

Toegepast op de status van virtuele componenten komt bijvoorbeeld Mačák tot de conclusie dat als virtuele componenten niet vallen onder ‘objecten’ *“the act of deletion of valuable civilian*

■
233 Harrison-Dinniss 2015, p. 51.

234 Harrison-Dinniss 2015, p. 51.

235 Harrison-Dinniss 2015, p. 54.

236 Zie Hoofdstuk 3, par. 3.3.3.6.

237 Dörmann 2004.

238 Zie par. 4.4.2 voor de ‘restrictieve’ benadering van aanval.

239 Zie Hoofdstuk 3, par. 3.3.3.6.

240 Dörmann 2004, p. 6. Schmitt 2013, p. 127.

datasets would fall outside the scope of application of IHL."²⁴¹ Eenzelfde redenering volgt een minderheid van de samenstellers van de Tallinn Manual: "*failure to do so [data should be regarded as an object] would mean that even the deletion of extremely valuable and important datasets would potentially escape the regulatory reach of the law of armed conflict*";²⁴² al is deze laatste opvatting door de toevoeging van 'in potentie' iets minder uitgesproken.

De andere denkrichting, bijvoorbeeld gevolgd door Harrison-Dinniss,²⁴³ redeneert dat de definitie van militair doel uit artikel 52 Aanvullend Protocol I is gegeven in de context van een aanval. Omdat 'militaire operatie' een breder begrip is dan 'aanval', is het onjuist hieruit conclusies te trekken voor alle militaire operaties omdat daardoor militaire operaties die geen aanval zijn, onterecht onder de noemer 'aanval' worden geschaard. Volgens deze denkrichting kom je pas toe aan de definitie van een militair doel als sprake is van een aanval. De definitie van militair doel mag niet gebruikt worden om een nadere interpretatie van het begrip 'aanval' te geven.²⁴⁴ Met betrekking tot 'onbruikbaarmaking' betekent dit dat onbruikbaarmaking *an sich* niet automatisch leidt tot de kwalificatie van aanval.

Zoals ik in Hoofdstuk 3 al betoogde, volg ik de laatste denkwijze op basis van de volgorde en het taalgebruik van de bepalingen van Aanvullend Protocol I. Daar komt bij dat ik het oneens ben met de visie dat de werking van het humanitair oorlogsrecht beperkt is tot 'aanvallen'. Ook beneden de grens van aanvallen heeft het humanitair oorlogsrecht werking, maar zonder de onderdelen die specifiek toezien op 'aanvallen'.²⁴⁵ Hoe dit uitpakt voor militaire operaties binnen het cyberdomein is onderwerp van het volgende hoofdstuk.

Dit brengt mij terug bij de status van virtuele componenten van het cyberdomein binnen het humanitair oorlogsrecht. Het lijkt erop dat vooralsnog niet getornd gaat worden aan de bestaande dichotomie van personen-objecten. Over de vraag of de virtuele componenten van het cyberdomein gezien kunnen of moeten worden als 'object' in de zin van de definitie van militair doel uit artikel 52 lid 2 Aanvullend Protocol I, en zo ja, of dit dan in gelijke mate geldt voor de verschillende categorieën van virtuele componenten, blijven meningsverschillen bestaan.

Voordat ik een standpunt inneem in de statusdiscussie helpt het misschien te kijken hoe andere (internationale) rechtsgebieden omgaan met de status van virtuele componenten. In de volgende paragraaf zal ik daarom kort bezien hoe strafrecht, zowel nationaal als in internationaal verband, omgaat met virtuele componenten, gevolgd door een rechtsgebied dat al veel langer te maken heeft met ontastbare zaken, namelijk intellectueel eigendom.

■
241 Mažák 2015, p. 59.

242 Schmitt 2013, p. 127.

243 Harrison-Dinniss 2012.

244 Zie bijv. Harrison-Dinniss 2012, p. 198, Schmitt 2013a, p. 95.

245 Zie Hoofdstuk 3. Zie ook bijv. Dinsteijn 2016, p. 143.

4.5.4.3 De status van virtuele componenten in het strafrecht

4.5.4.3.1 Nationaal strafrecht

Een exemplarisch voorbeeld om te beschrijven hoe het Nederlandse strafrecht omgaat met virtuele componenten levert het artikel over diefstal, artikel 310 Wetboek van Strafrecht.²⁴⁶ Het volledige artikel luidt “Hij die enig goed dat geheel of ten dele aan een ander toebehoort wegneemt, met het oogmerk om het zich wederrechtelijk toe te eigenen, wordt, als schuldig aan diefstal, gestraft met gevangenisstraf van ten hoogste vier jaren of een geldboete van de vierde categorie.” Voor dit onderzoek is met name de ontwikkeling van wat verstaan dient te worden onder het bestanddeel “enig goed” van belang.

Ten tijde van de totstandkoming van dit artikel (eind 18e eeuw) werd “algemeen aangenomen dat de wetgever met het begrip ‘goed’ het oog heeft gehad op lichamelijke, althans stoffelijke goederen die fysiek verplaatsbaar zijn.”²⁴⁷ Al in 1921 is door de Hoge Raad in het zogenaamde *Elektriciteitsarrest* uitgesproken dat ook elektriciteit, hoewel onstoffelijk en niet tastbaar, kwalificeert als ‘enig goed’ in de zin van artikel 310 Wetboek van Strafrecht.²⁴⁸ Dit kon omdat elektriciteit voldeed aan een aantal kenmerken, te weten: een zelfstandig bestaan; een overdraagbaarheid door menselijk toedoen; een zekere vermogenswaarde en de mogelijkheid van toe-eigening.²⁴⁹

Een verdere uitbreiding van het begrip ‘enig goed’ vond plaats in het *Giraal geldarrest* arrest.²⁵⁰ In dit arrest, dat handelt over artikel 321 ‘verduistering’ dat ook het bestanddeel ‘enig goed’ bevat,²⁵¹ oordeelt de Hoge Raad dat “onder het wegnemen van geld valt een aantasting in het vermogen van een ander, bijvoorbeeld in het geval van het zonder toestemming tanken van benzine met een tankpas van een ander waardoor een betaling wordt gedaan ten laste van de rekening van die ander.”²⁵² In een latere uitspraak is ook een beschikking van de rechtbank gekwalificeerd als ‘enig goed’.²⁵³ Wat deze uitspraken van de Hoge Raad gemeen hebben is “dat het telkens gaat om een goed dat te individualiseren is. Zodra de één de exclusieve (feitelijke) macht over het goed heeft verkregen, is de ander deze kwijtgeraakt.”²⁵⁴

Dit laatste was anders in het *Pinpasarrest* waarin de Hoge Raad tot de conclusie kwam dat het (onvrijwillig) noemen van een pincode niet aangemerkt kan worden als afgifte

²⁴⁶ Eigenlijk kunnen de artikelen uit het Wetboek van Strafrecht over diefstal (art. 310), afpersing (art. 317) en verduistering (art. 321) hier in een adem genoemd worden, omdat alledrie dezelfde term ‘enig goed’ als bestanddeel hebben.

²⁴⁷ HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251 (concl. A-G Hofstee), par. 17.

²⁴⁸ HR 23 mei 1921, NJ 1921, p. 564 e.v.

²⁴⁹ HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251 (concl. A-G Hofstee), par. 25.

²⁵⁰ HR 11 mei 1982, NJ 1982/583, ECLI: NL: HR: 2013: 2029.

²⁵¹ Artikel 321 Wetboek van Strafrecht luidt: “Hij die opzettelijk *enig goed* dat geheel of ten dele aan een ander toebehoort en dat hij anders dan door misdrijf onder zich heeft, wederrechtelijk zich toe-eigent, wordt, als schuldig aan verduistering, gestraft met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vijfde categorie.”

²⁵² Cleiren, Crijns & Verpalen 2016, p. 1747.

²⁵³ HR 6 oktober 1992, NJ 1993/101, ECLI: NL: HR: 1992: ZC9117, concl. OM.

²⁵⁴ HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251 (concl. A-G Hofstee), par. 26.

van ‘enig goed’, nu “daarvan slechts gesproken kan worden indien door die afgifte de betrokkene de beschikking over het afgegevene verliest.”²⁵⁵ In diezelfde lijn ligt het *Computergegevensarrest*²⁵⁶ waarin de Hoge Raad uitsprak “dat computergegevens niet (meer) als ‘enig goed’ worden aangemerkt omdat degene die de feitelijke macht daarover heeft die niet noodzakelijkerwijs verliest als een ander zich de feitelijke macht erover verschafft.”²⁵⁷ Om dit ‘probleem’ op te lossen heeft de wetgever een nieuw artikel in het Wetboek van Strafrecht geïntroduceerd dat het overnemen, aftappen of opnemen van gegevens strafbaar stelt.²⁵⁸ Onder ‘gegevens’ wordt verstaan “iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken”.²⁵⁹

Voor een antwoord op de vraag of iets onder het begrip ‘enig goed’ valt, is voor de Hoge Raad niet doorslaggevend of het een stoffelijk goed betreft, maar of het dezelfde kenmerken heeft als een stoffelijk goed. Met die redenering kon de Hoge Raad in 2012 ook virtuele voorwerpen aanmerken als ‘enig goed’ in het *RuneScapearrest*.²⁶⁰ Het betrof hier virtuele voorwerpen uit een on-line videospel (een virtueel amulet en masker) waarbij de Hoge Raad overwoog dat “de aangever het virtuele amulet en masker door inspanning en tijdsinvestering heeft verworven, dat dit voor hem een reële waarde had en dat het bezit ervan voor de aangever zowel als voor de verdachte en zijn mededader uiterst begerenswaardig was” en “de aangever door in te loggen op zijn *RuneScape-account* de feitelijke en exclusieve heerschappij had over het virtuele amulet en masker en dat deze door toedoen van de verdachte uit de beschikkingsmacht van de aangever zijn geraakt en in de beschikkingsmacht van de verdachte zijn gekomen en dat de aangever aldus is getroffen in het ongestoorde genot van de beschikkingsmacht die hij bij uitsluiting van een ander over die virtuele objecten had.”²⁶¹

Concluderend is het begrip ‘enig goed’ in het Nederlandse strafrecht door middel van jurisprudentie van de Hoge Raad zodanig uitgebreid dat ook niet-stoffelijke objecten onder het begrip kunnen vallen.²⁶² Hiervoor zijn nadere criteria geformuleerd die aanhaken bij verschillende kenmerken van stoffelijke objecten, waarmee overigens niet alle niet-stoffelijke objecten als ‘enig goed’ kunnen worden gezien. Grensgevallen zullen altijd blijven bestaan, bijvoorbeeld omdat ze zowel kenmerken van ‘enig goed’ als kenmerken van ‘gegevens’ bezitten. In een dergelijk geval is, om met de Hoge Raad te spreken, “de

■
255 HR 13 juni 1995, NJ 1995/365, ECLI: NL: HR:1995:ZDoo64.

256 HR 3 december 1996, NJ 1997/574, ECLI: NL: HR:1996:ZDo584.

257 Cleiren, Crijns & Verpalen 2016, p. 1748.

258 Art. 138ab Wetboek van Strafrecht.

259 Art. 8oquinquies Wetboek van Strafrecht.

260 HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251

261 HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251, r.o. 3.5.

262 In de conclusie van de A-G bij HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251, par. 37-41 maakt A-G Hofstee een rechtsvergelijking op dit onderwerp met de Verenigde Staten, Engeland en Duitsland.

kwalificatie sterk afhankelijk van de omstandigheden van het geval en de waardering daarvan door de rechter.”²⁶³

4.5.4.3.2 Extraterritoriale toepassing van het nationaal strafrecht

Bij de bespreking van strafrecht in internationaal verband past allereerst de opmerking dat als uitgangspunt voor het uitoefenen van strafrecht de jurisdictie wordt geregeld door het nationaal recht binnen de grenzen die het internationaal recht hieraan stelt. Een staat oefent de rechtsmacht uit “*by establishing rules (legislative jurisdiction), by establishing procedures for identifying breaches of the rules and the precise consequences thereof (judicial jurisdiction) and by forcibly imposing consequences such as loss of liberty or property for breaches or, pending adjudication, alleged breaches of the rules (enforcement jurisdiction)*.”²⁶⁴ Dit maakt dat strafrecht in hoofdzaak een nationaal karakter heeft.²⁶⁵ Om het strafrecht ook extraterritoriaal toe te kunnen passen zijn nadere internationale afspraken noodzakelijk. Dit kan bijvoorbeeld in de vorm van een verdrag, zoals het hiervoor al aangehaalde *Cybercrime*-verdrag²⁶⁶ dat op het gebied van virtuele componenten van het cyberdomein een aantal bepalingen bevat.

Na de begripsomschrijvingen in artikel 1 geeft het *Cybercrime*-verdrag in de daarop volgende vijf artikelen een aantal gedragingen die kunnen worden omschreven als *cybercrimes* in enge zin.²⁶⁷ Uit deze artikelen blijkt dat op een aantal plaatsen gepoogd is virtuele componenten een positie te geven vergelijkbaar met fysieke objecten. Zo strekt artikel 3, ‘wederrechtelijke onderschepping’, tot bescherming van de persoonlijke levenssfeer. De door artikel 8 van het Europees Verdrag voor de Rechten van de Mens gegarandeerde vertrouwelijkheid van ‘*correspondence*’ wordt door artikel 3 van het *Cybercrime*-verdrag uitgebreid tot alle vormen van elektronische gegevensoverdracht, bijvoorbeeld door middel van telefoon, fax, e-mail of overdracht van bestanden.²⁶⁸ De bescherming van de persoonlijke levenssfeer bouwt voort op “privacy grondrechten als het huisrecht en het briefgeheim [die] behoren tot onze oudste grondrechten”²⁶⁹ en de uitbreiding ervan was nodig in verband met “de opkomst van nieuwe af luister-, beeld- en geluidstechnieken, een snelle groei in geautomatiseerde gegevensverwerking en de sterke uitbreiding en modernisering van de overheidsadministratie.”²⁷⁰

Een ander voorbeeld geeft artikel 6 van het *Cybercrime*-verdrag, dat handelt over misbruik van technische hulpmiddelen. Lid 1a luidt: “iedere Partij neemt de wetgevende en andere maatregelen die nodig zijn om in haar nationale wetgeving als strafbaar feit aan te merken:

263 HR 31 januari 2012, NJ 2012/536, ECLI: NL: HR: 2012: BQ9251, r.o. 3.6.2.

264 Oxman 2007, onder 3.

265 Zo omschrijft Solis 2016, p. 674, *cybercrime* als “the use of computers in violation of domestic law for criminal purposes.”

266 Zie par. 4.2.1.1.

267 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p 8. Hiermee wordt bedoeld op computerspecifieke delicten, in tegenstelling tot de delicten waarbij de computer als instrument wordt gebruikt of die in een elektronische omgeving kunnen worden begaan, de zogenaamde *cybercrimes* in ruime zin.

268 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p 25.

269 Koekkoek 2000, p. 155.

270 Koekkoek 2000, p. 155.

het opzettelijk en wederrechtelijk vervaardigen, verkopen, verkrijgen voor gebruik, invoeren, verspreiden of anderszins beschikbaar stellen van een technisch hulpmiddel, waaronder begrepen een computerprogramma, dat hoofdzakelijk is ontworpen of geschikt gemaakt voor het plegen van een van de strafbare feiten, bedoeld in de artikelen 2 tot en met 5.²⁷¹ De hulpmiddelen waarop hier gedoeld wordt kunnen bestaan in de vorm van apparaten of toestellen als ook in de vorm van kraakprogramma's, wachtwoorden en toegangscode's.²⁷² Met andere woorden, voor de toepassing van dit artikel worden stoffelijke objecten en virtuele componenten gelijkgesteld. Niet de stoffelijkheid van het object is het criterium voor strafbaarstelling, maar de doelstelling waarvoor het ontworpen of geschikt gemaakt is.

Uit deze twee voorbeelden blijkt dat ook voor de extraterritoriale toepassing van het strafrecht gezocht is naar manieren om virtuele componenten, zoals een e-mail of een computerprogramma, dezelfde status te geven als hun fysieke tegenhanger waarbij de stoffelijkheid van het object geen onderscheidend criterium is.

Voordat ik terugkeer naar het humanitair oorlogsrecht en de status van virtuele objecten daarin, wil ik nog twee aanvullende opmerkingen maken naar aanleiding van het *Cybercrime*-verdrag. Ten eerste is in artikel 5 het verstoren van een computersysteem aangemerkt als zelfstandig strafbaar feit.²⁷³ Hieronder valt het tot stilstand brengen, het uitschakelen maar ook het vertragen of verstoren van het gegevensverwerkend proces.²⁷⁴ Voorwaarde hiervoor is wel dat het moet gaan om ernstige hinder, waarbij echter geen nadere criteria gegeven zijn, ook niet in het *Explanatory Memorandum*, om te bepalen wanneer een verstoring als ernstig aangemerkt moet worden.²⁷⁵ Een vergelijking met de functionaliteitstest binnen het humanitair oorlogsrecht, zoals hiervoor beschreven in paragraaf 4.2, dringt zich op. Ik zal hier later, bij de bespreking van schade aan virtuele componenten, nog op terugkomen.

De tweede opmerking die ik wil maken, is het onderscheid dat het *Cybercrime*-verdrag maakt tussen de aggregatietoestand waarin virtuele componenten zich in een computersysteem kunnen bevinden, namelijk dynamisch en statisch.²⁷⁶ Het gaat hier om het verschil tussen opslag en flow van virtuele componenten. Statisch betekent in deze dat de virtuele componenten zijn vastgelegd op een gegevensdrager, uitschakeling van het computersysteem heeft dan geen gevolgen voor de gegevensbestanden. In de dynamische toestand vindt verplaatsing van de virtuele componenten, oftewel

■
271 Cybercrime-verdrag art. 6 lid 1a, mijn accentuering.

272 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 29.

273 Cybercrime-verdrag art. 5 luidt: "Iedere partij neemt de wetgevende en andere maatregelen die nodig zijn om in haar nationale wetgeving als strafbaar feit aan te merken het opzettelijk en wederrechtelijk ernstig hinderen van de werking van een computersysteem door de invoer, de overdracht, de beschadiging, het wissen, de aantasting, de wijziging of de onderdrukking van computergegevens."

274 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 28.

275 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 28.

276 Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 7.

gegevensoverdracht, plaats. Deze gegevensoverdracht “kan plaatsvinden binnen de grenzen van een enkel computersysteem maar ook in de vorm van elektronische communicatie binnen een computernetwerk, een telecommunicatienetwerk daaronder begrepen.”²⁷⁷ Bij uitschakeling van het systeem gaan de virtuele componenten die zich in de dynamische aggregatietoestand bevinden, in principe verloren. De achtergrond van dit onderscheid is vooral van strafvorderlijke aard. “Een maatregel als inbeslagneming kenmerkt zich door de relatieve openheid ervan, terwijl het afluisteren van bepaalde (tele)communicatie slechts succesvol kan geschieden indien betrokkenen geen kennis dragen van het feit dat de maatregel wordt toegepast.”²⁷⁸ Met andere woorden, bij inbeslagname zal degene van wie iets in beslag genomen wordt daarvan doorgaans op de hoogte zijn, iets wat niet het geval is bij het onderscheppen van bepaalde (tele)communicatie. De voorwaarden en waarborgen onder de nationale wetgeving zullen voor de tweede vorm, vanwege de indringendheid van de betreffende bevoegdheden, daarom zwaarder zijn.

Ondanks de strafvorderlijke achtergrond van het onderscheid, vermeld ik het hier toch omdat ik de indeling naar aggregatietoestand nog niet ben tegengekomen in relatie tot status van virtuele componenten in het humanitair oorlogsrecht, terwijl het wel een criterium op zou kunnen leveren voor de beoordeling van schade. Ik kom hier bij de beantwoording van de vraag wat kwalificeert als schade in de zin van de definitie van cyberaanval nog op terug.²⁷⁹

4.5.4.4 Intellectueel eigendom

Een ander rechtsgebied dat al veel langer te maken heeft met ontastbare zaken is dat van intellectueel eigendom. In dit rechtsgebied had het internationaal recht al lang voor de ontwikkeling en opkomst van het cyberdomein te maken met ontastbare zaken. Al in de *Paris Convention for the Protection of Industrial Property* uit 1883 en de *Berne Convention for the Protection of Literary and Artistic Work* uit 1886 werden multilaterale afspraken gemaakt waarin intellectueel eigendom geregeld werd.²⁸⁰ Intellectueel eigendom wordt wel gedefinieerd als “a set of intangible products of human creativity.”²⁸¹ Alhoewel in een geheel ander rechtsgebied, met hele andere doelstellingen, blijkt hieruit dat staten al veel langer bereid zijn, indien de noodzaak zich daarvoor aandient, rechten en plichten te verbinden aan ontastbare en onzichtbare zaken.

Overigens wordt het gebrek aan aandacht binnen het humanitair oorlogsrecht voor intellectueel eigendom volgens sommigen juist veroorzaakt door het belang dat binnen het humanitair oorlogsrecht traditioneel wordt gehecht aan de stoffelijkheid van objecten. Het humanitair oorlogsrecht zou hierdoor achterblijven bij ontwikkelingen van met name

■
²⁷⁷ Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 8.

²⁷⁸ Kamerstukken II 2004-2005 30036 (R1784) nr. 3, p. 8.

²⁷⁹ Zie par. 4.5.2, een cyberaanval is een cyberoperatie, hetzij offensief of defensief, waarvan redelijkerwijs kan worden verondersteld dat die verwonding of dood van personen of schade of vernieling van objecten veroorzaakt.

²⁸⁰ Abbott 2014, A1.

²⁸¹ Abbott 2014, B2.

de waarde die aan digitale componenten van het cyberdomein gehecht moet worden. *“To a large extent this reflects the current conceptual framework of LOAC, which has not entirely caught up with the development of the concepts of intellectual property and intangible assets”*,²⁸² wat voor de bescherming van intellectueel eigendom heeft geleid tot een *“disparity within [...] two paradigms that are part of one body of rules of international humanitarian law. The protection against property offenses [...] and [...] the protection in the targeting paradigm.”*²⁸³

Beide voorbeelden, het strafrecht, zowel nationaal als bij internationale toepassing, en de internationale erkenning van intellectueel eigendom geven aan dat staten geen principiële bezwaren hebben tegen de behandeling van ontastbare zaken op een zelfde manier als tastbare objecten. Hieruit een directe conclusie trekken voor het humanitair oorlogsrecht gaat te ver, het humanitair oorlogsrecht heeft immers een eigen doel en strekking. Het geeft wel inzicht in de manier van denken van staten die ontastbare zaken niet per definitie uitsluit als objecten.

4.5.4.5 Conclusie status virtuele componenten in het humanitair oorlogsrecht.

De vraag naar de status van virtuele componenten van het cyberdomein binnen het humanitair oorlogsrecht focust zich op de vraag of de term ‘object’ uit artikel 52 Aanvullend Protocol I ook deze virtuele componenten, als niet-zichtbaar en niet-tastbaar, afdekt. In de traditionele opvatting is dat niet het geval, hierbij aanhakend bij de gezaghebbende *Commentary* op Aanvullend Protocol I dat vermeldt dat onder objecten *“visible and tangible”*²⁸⁴ zaken dienen te worden verstaan. Deze traditionele uitleg staat echter onder druk omdat hiermee de virtuele componenten van het cyberdomein lastig binnen de definitie van ‘militair doel’ uit artikel 52 te brengen zijn, terwijl alom erkend wordt, ook door aanhangers van de traditionele opvatting over objecten, dat deze componenten wel het doel van militaire operaties kunnen zijn.²⁸⁵ Hoewel de meningen verdeeld zijn over de huidige status van virtuele componenten wordt vrij algemeen aangenomen dat deze virtuele componenten uiteindelijk tot de term ‘object’ uit artikel 52 Aanvullend Protocol I zullen gaan behoren.²⁸⁶

Mijn conclusie uit de voorgaande analyse is dat virtuele componenten nu al gezien kunnen worden als ‘objecten’ in de zin van artikel 52 Aanvullend Protocol I.²⁸⁷ Virtuele componenten van het cyberdomein kunnen het doel vormen van militaire cyberoperaties en militaire cyberaanvallen (op het onderscheid hiertussen kom ik in de volgende paragraaf

■
282 Liivoja & McCormack 2012, p. 53.

283 Bunk 2016, p. 56.

284 Sandoz, Swinarski & Zimmerman 1987, p. 634.

285 Zie bijvoorbeeld Schmitt 2013, p. 108 en Schmitt 2017, p. 416. *“The limitation in this Rule [definition of cyber attack] to operations against individuals or physical objects should not be understood as excluding cyber operations against data (which are non-physical entities) from the ambit of the term attack.”*

286 Zo schrijft bijvoorbeeld Schmitt, *“the unwillingness to treat data as an object because of it is not tangible, which I believe presently reflects lex lata, is unlikely to survive for long.”* Schmitt 2014a, p. 204.

287 In een eerder stadium was ik nog iets terughoudender en concludeerde *“that there is no clear status of data within LOAC yet.”* Bosch in Duchene en Osinga 2017, p. 271.

terug). Ik voorzie vooralsnog geen uitbreiding van de klassieke dichotomie personen-objecten als militaire doelen met een nieuwe categorie. Als ik virtuele componenten zie als militaire doelen en deze virtuele componenten komen niet in aanmerking voor de status van personen, gebiedt de logica mij om virtuele componenten te accepteren binnen de uitleg van 'objecten'. Voor mij van doorslaggevend belang om deze opvatting als *lex lata* en niet als *lex ferenda*²⁸⁸ te zien, is dat staten, als ultieme 'makers' van het humanitair oorlogsrecht,²⁸⁹ in andere rechtsgebieden geen bezwaar lijken te hebben tegen uitbreiding van het begrip objecten met niet tastbare elementen. Hierbij wordt vooral gekeken naar overeenkomende eigenschappen en veel minder naar de niet-stoffelijkheid van een 'object'. Het is niet zo is dat concepten uit een bepaald rechtsgebied automatisch doorwerken in andere rechtsgebieden. Toch zijn de redenen om niet-fysieke componenten binnen het humanitair oorlogsrecht te beschouwen als objecten, namelijk om eenzelfde bescherming als bij objecten te bieden aan de niet-fysieke componenten van het cyberdomein, gelet op het toegenomen belang van deze niet-fysieke componenten, voor mij dwingender dan de redenen om vast te houden aan de traditionele opvatting.

Deze nieuwe uitleg van het begrip 'object' is gerechtvaardigd door te kijken naar de context en het doel van de bepaling van artikel 52 lid 2 Aanvullend Protocol I.²⁹⁰ De vaak aangehaalde uitleg waarom '*visible and tangible*' voor militaire doelen verwijst naar fysieke objecten,²⁹¹ is namelijk dat dit is om de "*general objective of a military operation*" uit te sluiten.²⁹² Onder '*general objective of a military operation*' zijn namelijk ook abstracte, lees niet-fysieke, begrippen als "*civilian morale*" en "*population's willingness to fight*"²⁹³ te brengen. De virtuele componenten uit het cyberdomein hebben echter veel meer overeenkomsten met fysieke objecten dan met genoemde abstracte begrippen. Zo zijn ze, weliswaar met technische hulpmiddelen zoals een computer met een beeldscherm,²⁹⁴ zichtbaar. Ze kunnen, naar analogie met het strafrecht, overgedragen worden van mens naar computer, tussen computers onderling en van computer naar mens, ze kunnen gekopieerd en gestolen worden en hebben een objectieveerbare (vermogens)waarde. Daarnaast hebben staten nooit principiële bezwaren hebben gehad om rechten en plichten te verbinden aan ontastbare en onzichtbare zaken. Kortom, de virtuele componenten van het cyberdomein vertonen meer overeenkomsten met tastbare objecten dan met de, door de *Commentary* uitgesloten, abstracte, algemene doelstellingen van een militaire operatie. Het humanitair oorlogsrecht is voldoende flexibel, en moet dat ook zijn, om mee te groeien met de voortschrijdende ontwikkeling van methoden en middelen van oorlogvoering, of zoals Bothe, Partsch en Solf

288 Grant & Barker 2009, "*lex ferenda imports the law which is being sought to establish; the law as it 'ought' to be, while lex lata imports the law which is presently in force; the law as it 'is'.*"

289 Schmitt & Watts 2015, p. 193.

290 Art. 31 Verdrag van Wenen, "een verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het Verdrag in hun context en in het licht van voorwerp en doel van het verdrag," mijn accentuering.

291 Sandoz, Swinarski & Zimmerman 1987, p. 634.

292 Sandoz, Swinarski & Zimmerman 1987, p. 634.

293 Harison-Dinniss 2015, p. 44.

294 De gebruikersinterface, categorie 4 (en 4") uit Figuur 5, par 4.2.2.3.

het formuleerden “*objects which may have been military objectives yesterday, may no longer be today and vice versa.*”²⁹⁵

Voordat ik een definitieve positie over de ondergrens van aanval in het cyberdomein inneem keer ik nogmaals terug naar de definitie van een cyberaanval uit de *Tallinn Manual*: “*A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.*”²⁹⁶ Met de conclusie dat virtuele componenten kunnen vallen onder ‘objecten’ in de zin van artikel 52 Aanvullend Protocol I alleen kan ik de vraag naar de ondergrens van een aanval in het cyberdomein echter nog niet beantwoorden. Ik zal ook een standpunt in moeten nemen over wat nu precies schade, en dan met name schade aan virtuele componenten, behelst. Dit vormt het onderwerp van de volgende paragraaf.

4.5.5 Schade aan virtuele componenten

4.5.5.1 Drempel voor schade aan virtuele componenten

Bij het zoeken naar de juiste interpretatie van schade aan virtuele componenten is het goed allereerst terug te gaan naar de definitie van aanval uit artikel 49 Aanvullend Protocol I. “Aanvallen” betekent: daden van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve. Schade in het kader van de definitie van aanval ziet op de gevolgen van daden van geweld.²⁹⁷ Schade in fysieke zin levert hier weinig problemen op, ook niet als die het gevolg is van een cyberoperatie. Zo concludeert bijvoorbeeld het ICRC dat “*cyber operations by means of viruses, worms, etc., that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked could be qualified as “acts of violence”, i.e. as an attack in the sense of IHL.*”²⁹⁸ Volgens de *Tallinn Manual* is voldaan aan het schadecriterium zodra sprake is van meer dan “*de minimis*” aan schade of vernietiging aan objecten²⁹⁹ waarbij opgemerkt moet worden dat de *Tallinn Manual*, in tegenstelling tot mijn conclusie uit de vorige paragraaf, virtuele componenten niet ziet als objecten. Interessant hierbij is dat de *Tallinn Manual* dus ook voor fysieke schade aan fysieke objecten een minimum drempel hanteert voordat sprake is van een cyberaanval zonder verder aandacht te besteden aan de hoogte van de “*de minimis*” schade.

Daar waar fysieke schade aan fysieke objecten als gevolg van een cyberoperatie geen meningsverschillen oplevert, is dit anders bij schade aan virtuele componenten. De discussie over wat schade aan virtuele componenten is, vertoont overeenkomsten met de discussie uit de vorige paragraaf over de status van virtuele componenten binnen het humanitair oorlogsrecht. Ook deze discussie verloopt voornamelijk langs de lijnen van het verschil tussen de ‘permissieve’ en de ‘restrictieve’ benadering van het begrip ‘aanval’.

■
295 Bothe, Partch & Solf 1982, p. 326.

296 Schmitt 2013, p. 106, *Rule 30, definition of cyber attack*. Schmitt 2017, p. 415 *rule 92*.

297 Zie Hoofdstuk 2.

298 ICRC 2011, p. 37.

299 Schmitt 2013, p. 107.

De hiervoor besproken functionaliteitstest³⁰⁰ geeft een goed voorbeeld van een poging een werkbaar compromis tussen de twee benaderingen van aanval te vinden. Als een object niet meer de functie vervult waarvoor het is bestemd, met andere woorden het is defect, kan volgens de *Tallinn Manual* mogelijk gesproken worden van schade in de zin van de definitie van cyberaanval.³⁰¹ Over de vraag wanneer een verstoring in de functionaliteit aangemerkt moet worden als schade bleven de meningen verdeeld, variërend van “it does not”³⁰² tot “the object’s loss of usability constitutes the requisite damage”,³⁰³ respectievelijk corresponderend met de ‘permissieve’ benadering, waarin alleen fysieke schade aan fysieke objecten leidt tot de kwalificatie van aanval en de ‘restrictieve’ benadering, die uitgaat van de opvatting dat het niet uitmaakt hoe, of waardoor, een object onklaar raakt, het feit dat het onbruikbaar is geworden volstaat om de operatie te kwalificeren als ‘aanval’.³⁰⁴ Binnen de groep van experts van de *Tallinn Manual* bestond een meerderheid voor de opvatting dat sprake is van schade als voor het herstel van de functionaliteit vervanging van fysieke componenten noodzakelijk is.³⁰⁵

Diverse andere schrijvers hebben zich uitgesproken in de discussie over wanneer verstoring van virtuele componenten kwalificeert als schade als gevolg van daden van geweld.³⁰⁶ Over fysieke schade is de conclusie eenduidig, fysieke schade als gevolg van een cyberoperatie leidt automatisch tot de kwalificatie van aanval. Aan de andere kant bestaan cyberoperaties, bijvoorbeeld spionage, propaganda of informatie-operaties, die niemand onder de noemer van aanval wil scharen. Waar precies het onderscheid ligt, blijft discussiepunt. Soms wordt de term ‘ongemak’ (*inconvenience*) als onderscheidend criterium voor de gevolgen van een cyberoperatie gebruikt in de zin dat alleen ‘ongemak’ niet leidt tot een kwalificatie van aanval.³⁰⁷ Hiermee wordt echter een nieuw, identiek, probleem geïntroduceerd, namelijk wanneer is iets slechts ‘ongemak’ en wanneer wordt het meer?

Eenzelfde soort gebrek aan onderscheidend vermogen doet zich voor bij Kilovaty die pleit voor “*disruptive cyber operations as a new form of violence*”³⁰⁸ waarbij verstorende (*disruptive*) operaties tegenover destructieve (*destructive*) operaties worden gezet. De eerste

■
300 Zie par. 4.4.2.

301 Schmitt 2013, p. 108.

302 Schmitt 2013, p. 108.

303 Schmitt 2013, p. 109.

304 Deze laatste positie neemt ook het ICRC in, zie bijv. ICRC 2011, p. 37.

305 Schmitt 2013, p. 108.

306 Zie bijv. Melzer 2011a, p. 26, “both arguments [whether the notion of attack also includes cyberoperations aiming merely to capture or neutralize – rather than kill, injure or destroy – the target] have their strong points, neither seems to provide an entirely satisfactory interpretation of the notion of attack in relation to cyberoperations”. Droege 2012, p. 560, “In sum, a cyberoperation can constitute an attack within the meaning of IHL [...] if it interferes with the functioning of an object by disrupting the underlying computer system. However, not all cyberoperations directed at disrupting the functioning of infrastructure amount to attacks”. Lubell 2013, p. 275, “Clearly, cyberoperations that lead to direct physical damage or casualties must be considered attacks. Likewise, those cyberoperations that amount to no more than propaganda and cause no actual harm might lie outside the notion of attack.”

307 Schmitt 2002, p. 372.

308 Kilovaty 2016, p. 123.

veroorzaken, in tegenstelling tot de tweede, geen directe kinetische effecten,³⁰⁹ maar zouden desondanks toch onder de term ‘aanval’ in de zin van artikel 49 API kunnen vallen. “*The interruptive effects need to be of violent nature*”³¹⁰ om de verstorende operatie als aanval te kwalificeren. Of de onderbrekende effecten gewelddadig zijn moet aan de hand van de omstandigheden van het geval worden gezien. De essentie van de onderbroken dienst voor het dagelijks leven van burgers en de omvang en duur van de verstoring zijn de criteria die daarbij in overweging genomen moeten worden.³¹¹ Ondanks de aangereikte criteria blijft ook hier het interpretatieprobleem bestaan wanneer een cyberoperatie gezien moet worden als gewelddadig, en dus gezien moet worden als een aanval, en wanneer niet.

Een andere poging om schade aan de functionaliteit van een systeem te duiden is de hiervoor besproken scheiding tussen ‘*content-level data*’³¹² en ‘*operational-level data*’³¹³ zoals aangebracht door Harrison-Dinniss.³¹⁴ Het onderscheid is gebaseerd op de soort schade die ontstaat door beschadiging, vernietiging of onbruikbaarmaking van de verschillende virtuele componenten. Dit onderscheid lijkt in eerste instantie helder omdat in het geval van verstoring van ‘*content-level data*’ het systeem blijft functioneren terwijl bij ‘*operational level data*’ de functionaliteit van het systeem verloren gaat.³¹⁵ Maar wat nu als het correct functioneren van het systeem mede afhankelijk is van ‘*content-level data*’ zoals bijvoorbeeld een *Global Positioning System* (GPS) dat voor het goed functioneren afhankelijk is van coördinaten. Het systeem functioneert nog, maar de uitkomst is niet datgene wat men normaliter verwacht. Heeft het systeem dan schade volgens de functionaliteitstest? Het geïntroduceerde onderscheid tussen ‘*content-level data*’ en ‘*operational-level data*’ zal de discussie over de functionaliteitstest niet doen verstommen. Toch is bovenstaand onderscheid niet geheel zonder betekenis in de zin dat beschadiging, vernietiging of onbruikbaarmaking van virtuele componenten op het niveau van ‘*operational-level data*’ waarschijnlijk eerder een verlies van functionaliteit tot gevolg heeft dan eenzelfde soort actie gericht op ‘*content-level data*’. Het onderscheid kan daarom verhelderend werken in de discussie over schade, maar zal de discussie niet kunnen beslechten.

Datzelfde kan gezegd worden voor het onderscheid dat gemaakt is in het *Cybercrime*-verdrag, namelijk tussen virtuele componenten in dynamische en statische aggregatietoestand.³¹⁶ Bij uitschakeling van het systeem zullen de virtuele componenten die op dat moment in de dynamische aggregatietoestand zijn, verloren gaan. Afhankelijk van het systeem en de wijze waarop virtuele componenten zijn opgeslagen, kunnen de virtuele componenten vanuit de statische aggregatietoestand relatief eenvoudig worden hersteld naar de toestand

■
309 Kilovaty 2016, p. 123.

310 Kilovaty 2016, p. 124.

311 Kilovaty 2016, p. 124.

312 Harrison-Dinniss 2015, p. 41.

313 Harrison-Dinniss 2015, p. 41. Deze laatste worden ook wel aangeduid als ‘*logical-level data*’ of ‘*program data*’.

314 Zie par. 4.4.3.2.

315 Harrison-Dinniss 2015, p. 42.

316 Zie par. 4.4.3.3.

van voor de uitschakeling van het systeem. Ook dit onderscheid kan verhelderend werken, maar levert geen ‘hard’ criterium dat de discussie over schade aan virtuele componenten kan beslechten omdat ook virtuele componenten in de statische aggregatietoestand verloren kunnen gaan, bijvoorbeeld als gevolg van slechte of afwezige back-ups.

Nu net als bij de status van virtuele componenten niet eenduidig vastligt wat schade aan deze componenten exact behelst, zal ik eerst, net als bij de status, bezien hoe andere rechtsgebieden omgaan met schade aan virtuele componenten.

4.5.5.2 Schade aan virtuele componenten in andere rechtsgebieden

In het strafrecht, bijvoorbeeld in het eerdergenoemde *Cybercrime*-verdrag dat zoals eerder vermeld gericht is op strafbare handelingen zowel binnen als met behulp van computersystemen,³¹⁷ zijn verwijzingen naar schade aan virtuele componenten te vinden, maar deze zijn verre van concreet. Zo geeft bijvoorbeeld artikel 4, Verstoring van computergegevens, de mogelijkheid aan verdragspartijen om in hun nationale wetgeving een voorwaarde voor strafbaarheid van verstoring van computergegevens te stellen, in de zin dat de verstoring ‘ernstige schade’ moet veroorzaken voordat sprake is van een strafbaar feit.³¹⁸ Het verdrag noch de toelichting daarop geeft een nadere omschrijving van wat onder ‘ernstige schade’ verstaan moet worden. De *Explanatory Report to the Cybercrime Convention* laat dit aan de nationale wetgever, maar als een staat het voorbehoud inroept heeft deze de verplichting dat “Parties should notify the Secretary General of the Council of Europe of their interpretation.”³¹⁹ Tot op heden hebben slechts vijf staten gebruik gemaakt van de optie om een voorbehoud te maken, waarbij geen van hen een nadere interpretatie van ‘ernstige schade’ heeft gegeven.³²⁰

Concretere aanwijzingen voor kwalificatie van schade aan virtuele componenten zijn te vinden op het gebied van cyberterrorisme.³²¹ In 2016 kwam de *Study Group on Cybersecurity, Terrorism, and International Law* van de *International Law Association* met een rapport waarin het onderwerp schade, waaronder schade aan virtuele componenten, specifiek aandacht krijgt.³²² Op zoek naar een “*working definition of cyber terrorism*”³²³ concludeerde deze studiegroep dat een “*damage threshold*”³²⁴ in de definitie noodzakelijk was om twee redenen. Allereerst om de definitie onderscheidend te maken. Zonder een drempelwaarde

317 Zie par. 4.2.1.1.

318 *Cybercrime*-verdrag 2001 art. 4 lid 2.

319 *Explanatory Report to the Cybercrime Convention* 2001, par. 64.

320 Stand van zaken april 2018. Deze staten zijn Azerbeidzjan, Chili, Litouwen, Slowakije en Verenigde Staten van Amerika, waarbij alleen de laatste als nadere aanduiding heeft gegeven dat zij “reserves the right to require that the conduct result in serious harm, which shall be determined in accordance with applicable United States federal law.” <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>, onder *reservations and declaration*, laatst geraadpleegd 28 nov 2018.

321 Voor het onderscheid dan wel de overlap tussen cybercrime en cyberterrorisme, zie Saul & Heath in Tsagouria & Buchan 2015, p. 147-167.

322 ILA 2016a.

323 ILA 2016a, p. viii. Waarbij de studiegroep op p. 9 wel opmerkt dat de “*Study Group’s definition of cyber terrorism does not represent international law, nor does it eliminate definitional controversies in the area of cybersecurity.*”

324 ILA 2016a, p. 22.

voor de ernst van de consequenties of hoeveelheid schade zouden ook onbelangrijke consequenties, zoals tijdelijke onderbrekingen van de toegang tot internet, onder de definitie van cyberterrorisme vallen.³²⁵ De tweede reden was dat “*state practice in cyber incidents contains some indications that a definition of cyber terrorism should include a damage threshold*”,³²⁶ gevolgd door een aantal voorbeelden.

De studiegroep keek vervolgens naar een aantal cyberspecifieke vormen van schade zoals “*damage to data, damage to computer-operated machines or equipment and damage to government-provided or privately operated public services*”,³²⁷ om tot de conclusie te komen dat “*states are unlikely to conclude that damage to data, computer-operated machines, or cyberdependent services crosses the threshold into terrorism without such damage causing death, injury, or significant property, economic, or environmental harm*.”³²⁸ Met andere woorden, in het kader van het tegengaan van (cyber) terrorisme komt de studiegroep tot de conclusie dat staten terughoudend zijn in het uitbreiden van het schadebegrip naar schade aan virtuele componenten, als daarnaast niet ook sprake is van de meer ‘traditionele’ vormen van schade zoals dood, verwonding, en/of fysieke schade aan goederen, de economie of het milieu. Het betreft hier het tegengaan van (cyber)terrorisme via strafbaarstelling, waardoor deze visie op schade niet onverkort toepasbaar is op schade in het humanitair oorlogsrecht. Het geeft echter wel een indicatie van de denkrichting over schade door deskundigen op het gebied van internationaal recht.

4.5.5.3 Wanneer zijn fysieke gevolgen mogelijk?

Bovenstaande analyses leveren geen eenduidige criteria op voor wat verstaan kan of moet worden onder schade aan virtuele componenten. Het blijft een subjectieve waardering van de ernst van de niet-fysieke gevolgen die maakt of iets wordt aangemerkt als schade of niet. Wat wel duidelijk is, is dat het objectieve criterium ‘fysieke gevolgen’ van een manipulatie van virtuele componenten, in welke vorm dan ook, binnen het humanitair oorlogsrecht leidt tot de kwalificatie schade, waarmee de manipulatie voldoet aan de definitie van aanval conform artikel 49 Aanvullend Protocol I. Het is daarom zinvol te bezien in welke gevallen manipulatie van virtuele componenten kan leiden tot genoemde fysieke gevolgen.

Om te beoordelen welke manipulaties kunnen leiden tot fysieke gevolgen is de indeling die ontwikkeld is binnen de information security behulpzaam. *Information security* richt zich op “*the adoption of measures to prevent the unauthorized use, misuse, modification, or denial of use of information, knowledge, facts, data, or capabilities*”³²⁹ en berust op een drietal principes, vertrouwelijkheid (*Confidentiality*), integriteit (*Integrity*) en beschikbaarheid (*Availability*)³³⁰ vaak afgekort als, naar de beginletters van de Engelstalige principes, CIA.

■
325 ILA 2016a, p. 23.

326 ILA 2016a, p. 23.

327 ILA 2016a, p. 23.

328 ILA 2016a, p. 24.

329 Talbot & Jakeman 2009, p. 82.

330 Talbot & Jakeman 2009, p. 83.

Deze van oorsprong militaire benaderingswijze was aanvankelijk gericht op de beveiliging van informatie tegen externe dreigingen, zodat de focus vooral lag op de fysieke controle op toegang tot de computers waarop de informatie zich bevond.³³¹ Gaandeweg ontwikkelde de *information security* vanuit deze militaire beveiligingsvisie, onder andere door ook interne bedreigingen te incorporeren, tot het volgende fundament van de *Confidentiality-Integrity-Availability* triade:

Confidentiality: the unauthorized information release where an unauthorized person is able to read and take advantage of information stored in the computer.

Integrity: the unauthorized information modification where an unauthorized person is able to make changes in stored information- a form of sabotage.

*Availability: the unauthorized denial of use: an intruder can prevent an authorized user from referring to, or from modifying information, even though the intruders may not be able to refer to, neither modify the information themselves.*³³²

Deze drie beginselen zal ik toepassen op de verschillende groepen virtuele componenten van het cyberdomein, te weten firmware, besturingsprogramma's, cyberidentiteiten, computerprogramma's en computergegevens.³³³ Als laatste zal ik aandacht besteden aan mogelijke overlappen tussen deze drie beginselen.

4.5.5.3.1 Vertrouwelijkheid

Als ik bovenstaande beschrijving van vertrouwelijkheid toepas op de door mij onderscheiden groepen van virtuele componenten geldt dat een inbreuk op de vertrouwelijkheid waarschijnlijk ongewenst is, maar geen fysieke schade kan veroorzaken. De inbreuk maakt dat informatie over firmware, besturingsprogramma's, cyberidentiteiten, computerprogramma's en computergegevens gelezen³³⁴ kan worden door ongeautoriseerde personen. Uiteraard kan de informatie die zo verkregen is, vervolgens gebruikt worden op een manier waardoor alsnog fysieke schade kan ontstaan of worden veroorzaakt, maar dit laatste is dan het gevolg van de vervolgactie en niet van de inbreuk op de vertrouwelijkheid. Het zal dan van de voorzienbaarheid van en verwevenheid met een eventuele vervolgactie afhangen of een dergelijke operatie alsnog zal kwalificeren als onderdeel van een 'aanval'. De deelconclusie hieruit is dat inbreuk op alleen de vertrouwelijkheid van virtuele componenten geen fysieke gevolgen kan hebben.

■
331 Samonas & Coss 2014, p. 23.

332 Samonas & Coss 2014, p. 24.

333 Zie par. 4.2.2.3.

334 Kopiëren en vervolgens meenemen valt hier ook onder, zolang de oorspronkelijke informatie maar in dezelfde vorm aanwezig en beschikbaar blijft.

4.5.5.3.2 Integriteit

Inbreuk op de integriteit komt voor als een vervolgstap op de inbreuk op de vertrouwelijkheid en als zelfstandige inbreuk. In het eerste geval vindt de schending van de integriteit plaats nadat eerst de vertrouwelijkheid geschonden is door ongeautoriseerde toegang tot de virtuele componenten te verkrijgen. In het tweede geval is de toegang tot bepaalde virtuele componenten wel geautoriseerd maar het wijzigen ervan niet.³³⁵ Het onderscheid is met name van belang vanuit beveiligingsperspectief³³⁶ en ik zal daarom hieraan verder geen aandacht besteden. Bij de inbreuk op integriteit zal ik de indeling en volgorde van categorieën virtuele componenten uit paragraaf 4.2.2.3 aanhouden, namelijk firmware, besturingsprogramma's, cyberidentiteiten, computerprogramma's en computergegevens.

De eerste categorie is de firmware. Zoals eerder aangegeven is de firmware het virtuele gedeelte van de interface-categorie en fungeert als een soort schakelaar tussen de fysieke en niet-fysieke componenten.³³⁷ Omdat de firmware deel uitmaakt van deze interface-categorie en omdat fysieke gevolgen door middel van niet-fysieke componenten alleen te realiseren zijn indien ergens gebruik gemaakt wordt van de interface-categorie, is de kortste weg³³⁸ naar genoemde fysieke gevolgen via firmware. Door veranderingen aan te brengen in de firmware kan fysieke schade worden veroorzaakt. Zo maakte het veranderen van de firmware (*uploading malicious firmware*) deel uit van de *Black Energy attack* op het elektriciteitssysteem van Oekraïne in 2015.³³⁹ Het is daarbij niet de manipulatie van de firmware die kwalificeert als schade, maar de fysieke gevolgen daarvan, waardoor de manipulatie van de firmware voldoet aan de voorwaarden voor aanval. Dit betekent echter ook dat niet elke integriteitsschending van firmware aangemerkt kan worden als aanval³⁴⁰ maar de mogelijkheid bestaat wel.

De tweede categorie bevat de besturingsprogramma's. Tezamen met de firmware, specifiek voor elk onderdeel van de hardware, zorgt het besturingsprogramma er voor dat de verschillende hardwarecomponenten (bijvoorbeeld harde schijf, processor of intern geheugen) of randapparatuur (bijvoorbeeld een muis, een beeldscherm of een toetsenbord) met elkaar één werkend geheel vormen.³⁴¹ Manipulatie van het besturingsprogramma zal doorgaans niet direct fysieke schade tot gevolg hebben, maar kan er wel voor zorgen dat

335 Een voorbeeld hiervan is een *read-only* tekstbestand. Men mag dit bestand wel lezen, maar men kan er niets in veranderen.

336 Vanuit een beveiligingsperspectief moet bij de beveiliging van de integriteit onderscheid gemaakt worden tussen insiders, die wel toegang tot de informatie hebben maar geen autorisatie tot wijzigen, en outsiders, die geen toegang tot de informatie hebben en dus ook geen autorisatie tot wijzigen.

337 Zie par. 4.2.2.2.

338 Kortste is hier gebruikt in de zin van de minste tussenschakels. Dit betekent niet dat deze methode daarmee ook automatisch het eenvoudigst of het snelst zal zijn.

339 Lee, Assante & Conway 2016, p. 10. Het betrof hier een samengestelde aanval op meerdere componenten waar de verandering van de firmware van een aantal apparaten in sub-stations onderdeel van uitmaakte. Voor andere voorbeelden, zie par. 4.2.2.2.

340 Zo zal het veranderen van de firmware waardoor een camera of microfoon wordt aangezet niet gelden als schade.

341 Zie par. 4.2.2.3.

schadelijke handelingen, aan bijvoorbeeld de firmware, mogelijk zijn, waardoor alsnog fysieke schade ontstaat. Net als bij manipulatie van firmware is het niet de manipulatie van het besturingssysteem die kwalificeert als schade, maar de fysieke gevolgen ervan. Net als bij firmware betekent dit dat niet elke manipulatie van een besturingsprogramma als aanval kwalificeert, maar dat het, afhankelijk van de fysieke gevolgen, wel mogelijk is.

De derde categorie is de cyberidentiteiten. Cyberidentiteiten worden gebruikt door personen of apparaten om toegang te krijgen tot een veelheid van computerprogramma's en computergegevens.³⁴² Aantasting van de integriteit van cyberidentiteiten, bijvoorbeeld door het wijzigen van een wachtwoord, zal als direct resultaat hebben dat onbevoegd toegang gekregen wordt tot computerprogramma's en computergegevens of juist dat bevoegde toegang wordt ontzegd.³⁴³ In het eerste geval is sprake van de hierboven behandelde schending van vertrouwelijkheid. In het tweede geval is sprake van schending van beschikbaarheid. Of dit kan leiden tot fysieke schade zal ik behandelen in de volgende subparagraaf over beschikbaarheid. Schending van alleen de integriteit van cyberidentiteiten kan niet leiden tot fysieke gevolgen.

De vierde categorie virtuele componenten is die van de computerprogramma's. Deze uitgebreide groep, waaronder applicaties, protocollen, maar ook programma's voor tekstbewerking, databases en fotobewerkingsprogramma's vallen,³⁴⁴ bestrijken een breed scala van mogelijkheden om door middel van integriteitsschendingen fysieke schade te veroorzaken, variërend van nauwelijks voor te stellen tot heel reëel voorstelbaar. Ik zal deze categorie behandelen aan de hand van SCADA software,³⁴⁵ de software waarvan vaak gezegd wordt dat ze kwetsbaar zijn voor manipulatie van buitenaf met mogelijk grote fysieke gevolgen.³⁴⁶ Voor andere virtuele componenten binnen deze categorie geldt hetzelfde, alleen is de mogelijkheid om fysieke gevolgen te bewerkstelligen waarschijnlijk kleiner of in sommige gevallen geheel niet voorstelbaar.³⁴⁷

Schending van de integriteit van SCADA software kan direct (grote) fysieke gevolgen hebben. Zo kan bijvoorbeeld de software zo worden veranderd dat bepaalde signalen van *Programmable Logic Controllers* worden genegeerd³⁴⁸ of verkeerd worden geïnterpreteerd,³⁴⁹ waardoor enorme fysieke schade kan ontstaan. Dit is niet alleen theoretisch mogelijk maar

■
342 Zie par. 4.2.2.3.

343 Een combinatie van beide effecten is uiteraard ook mogelijk.

344 Zie par. 4.2.2.2.

345 Zie par. 4.2.2.3.

346 Bijvoorbeeld Harrison-Dinniss 2012, p. 5.

347 Denk hierbij bijvoorbeeld aan een fotobewerkingsprogramma. Veranderingen hierin zullen waarschijnlijk slechts kunnen leiden tot gemanipuleerde foto's.

348 Bijvoorbeeld een temperatuursignaal waardoor niet op tijd gekoeld wordt of een overdruksignaal waardoor een veiligheidsklep niet opent.

349 Bijvoorbeeld een sluis die openstaat wordt door het systeem gezien als gesloten.

is in de praktijk ook al toegepast.³⁵⁰ Een mogelijk voorbeeld is de pijplijnexplosie in Siberië in juni 1982,³⁵¹ die zou zijn veroorzaakt doordat de Amerikaanse CIA erin was geslaagd schadelijk software te implanteren in de SCADA software die door de Sovjet Unie gekocht werd in Canada.³⁵² Een beter voorbeeld, in de zin dat het onbetwist heeft plaatsgevonden en nauwkeurig onderzocht is, is de Maroochy water breach die plaatsvond in maart 2000 in Queensland, Australië. Hier nam een ex-werknemer van de *Maroochy Shire Council* wraak op zijn voormalige werkgever door met een laptop en een radiozender in te breken op het SCADA systeem van het afvalwatersysteem. Hij kon hierdoor de controle overnemen over 150 pompstations en gedurende een periode van drie maanden een miljoen liter ongezuiverd afvalwater op lokale oppervlaktewateren lozen.³⁵³

Bovenstaande voorbeelden zijn weliswaar niet als militaire operatie in het kader van een gewapend conflict uitgevoerd, maar het behoeft weinig fantasie om soortgelijke militaire operaties voor te stellen die wel aan die voorwaarde voldoen. In dat geval zijn die militaire operaties zonder twijfel aan te merken als aanvallen onder het humanitair oorlogsrecht. Ook hier zijn het echter, net als bij manipulatie van firmware, de fysieke gevolgen die maken dat de militaire operatie om de SCADA software te wijzigen, voldoet aan de voorwaarden voor aanval en niet de verandering in de software *an sich*. Zo is verandering van het veiligheidssysteem, gevolgd door plaatsing van software in het SCADA systeem om zo te kunnen observeren hoe het systeem precies werkt, zeker een schending van de integriteit van het systeem, maar kwalificeert (nog) niet als aanval. Ook niet als de informatie later alsnog gebruikt kan worden om fysieke schade toe te brengen. Een dergelijke observatieoperatie vertoont dan overeenkomsten met een schending van de vertrouwelijkheid zoals hiervoor beschreven. Pas als er iets gedaan wordt met de op deze manier verkregen informatie kan mogelijk sprake zijn van een aanval.

Een randgeval levert de situatie waarbij veranderingen in de SCADA software leiden tot een geautomatiseerde *shutdown* waardoor bijvoorbeeld een energiecentrale of gasdistributiesysteem (gedeeltelijk) stil komt te liggen. Een sprekend voorbeeld hiervan is *Black Energy*, waarbij een gedeelte van het elektriciteitsnetwerk van Oekraïne in 2015 werd stilgelegd.³⁵⁴ Het zal dan van de mate en de duur van stillegging en de manier waarop dit

■
350 Applegate 2013 beschrijft een drietal “*experimental validations*” waarbij fysieke schade in een gecontroleerde omgeving is gerealiseerd, een drietal “*real-world validations*” waarbij fysieke schade, inclusief gewonden, is opgetreden in de ‘echte wereld (dus buiten een gecontroleerde testomgeving) en hij benoemt Stuxnet als een “*operational validation*” waarbij fysieke schade is ontstaan.

351 Dit voorval wordt genoemd door Thomas Reed 2004, p. 268-269 maar wordt betwist door Rid 2012, p. 10.

352 Rid 2012, p. 10. De SCADA software zou geprogrammeerd zijn om eerst normaal te functioneren om na verloop van een bepaalde tijd “*to reset pump speed and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds*”.

353 Slay & Miller 2008, p.75. De inbraak op het SCADA systeem leidde uiteindelijk tot een veroordeling van 2 jaar gevangenisstraf.

354 Lee, Assante & Conway 2016, p. 10. Na een uitgebreide fase 1 waarin langdurig het systeem geïnfiltrerd en gemanipuleerd was, startte fase 2, de uitvoering van de operatie, met een “*SCADA hijack with malicious operation to open breakers*.”

gebeurt, gecontroleerd of ongecontroleerd,³⁵⁵ afhangen of fysieke schade op zal treden. Zo zal bij stillegging van een klein deel van een energiecentrale die zich bevindt in een netwerk van energiecentrales het tijdelijk wegvallen waarschijnlijk geen fysieke gevolgen hebben. Naarmate het deel van de energieproductie dat wordt stilgelegd ten opzichte van de totale energieproductie stijgt, en ook naarmate de stillegging langer duurt, zal de kans op fysieke gevolgen stijgen. Ook een ongecontroleerde *shutdown* zal de kans op fysieke schade groter maken.

De vijfde categorie virtuele componenten bevat de computergegevens. Net als de vorige categorie van computerprogramma's, is ook de categorie van computergegevens heel gevarieerd, wat eveneens leidt tot een breed spectrum van mogelijkheden om fysieke gevolgen te bewerkstelligen door veranderingen aan de integriteit van deze gegevens variërend van heel reëel voorstelbaar tot nauwelijks voor te stellen. Drie voorbeelden kunnen dit spectrum verduidelijken.

Als eerste voorbeeld in het spectrum van mogelijkheden om fysieke gevolgen te bewerkstelligen noem ik de database van een bibliotheek. Hierin zitten alle boeken, teksten, artikelen enzovoorts die de bibliotheek bezit. Veranderingen in deze database kunnen zeker leiden tot ongemakken, zoals een boek dat niet terug te vinden is of een artikel dat aan een verkeerde auteur wordt toegeschreven. Het is echter moeilijk voor te stellen dat dit tot fysieke gevolgen zou kunnen leiden.

Neem ik als tweede voorbeeld echter een database van patiëntgegevens, bijvoorbeeld in een ziekenhuis, dan zit dit aan de andere zijde van het spectrum. Het is reëel voorstelbaar, en voorspelbaar, dat een wijziging van patiëntgegevens directe fysieke gevolgen heeft. Denk bijvoorbeeld aan de verandering van medicijnbehoefte, of van bloedgroep of allergiegegevens bij een patiënt die binnenkort een zware operatie moet ondergaan.

Het derde voorbeeld zijn de computergegevens aan de hand waarvan een *Global Positioning System* de positie van een object of een persoon bepaalt. Indien deze gegevens worden gemanipuleerd zodat de plaatsbepaling incorrect wordt uitgevoerd kan dit ongetwijfeld tot ongevallen met fysieke gevolgen leiden, zeker als het Global Positioning System het enige gebruikte systeem is en niet gecontroleerd wordt door bijvoorbeeld menselijke observatie.³⁵⁶

Indien beide laatste voorbeelden plaatsvinden binnen een gewapend conflict om zo een tegenstander uit te schakelen of te verzwakken, zijn dit militaire operaties die voldoen aan

■
³⁵⁵ Bij een gecontroleerde *shutdown* verloopt de stillegging volgens een vooraf vastgesteld en veelal uitgetest protocol waardoor de risico's op onvoorspelbare gevolgen geminimaliseerd zijn. Dit in tegenstelling tot een ongecontroleerde *shutdown*.

³⁵⁶ Denk bijvoorbeeld aan een schip dat op automatische piloot (gestuurd door GPS signalen) vaart en tegen een brugpijler aan vaart of een kruisvluchtwapen dat voor zijn vlucht afhankelijk is van GPS signalen.

de definitie van aanval.³⁵⁷ Net als bij firmware en computerprogramma's is het ook hier niet de aantasting van de integriteit van de computergegevens *an sich*, maar de fysieke gevolgen daarvan die de militaire operatie dan kwalificeren als aanval.

Tot slot van deze paragraaf over integriteit van computergegevens nog een specifieke groep computergegevens, namelijk die via een cyberidentiteit direct te koppelen zijn aan een *persoon*. Personen hebben binnen het humanitair oorlogsrecht een andere bescherming dan objecten³⁵⁸ en de vraag is of dit verschil doorwerkt naar de virtuele componenten van het cyberdomein.

Schending van de integriteit van deze groep computergegevens is eenvoudig voor te stellen. Het veranderen van de profielgegevens op een socialmedia-account, het toevoegen of veranderen van berichten in een dergelijk account of het wijzigen van een spamfilter van een mailaccount waardoor deze volloopt met spam zijn slechts enkele van de talloze mogelijkheden om de integriteit van computergegevens te schenden. Deze veranderingen hebben geen directe fysieke gevolgen, omdat de cyberidentiteiten waaraan de computergegevens zijn gekoppeld ook alleen virtueel bestaan. Ze zijn weliswaar intrinsiek verbonden met hun fysieke tegenhanger,³⁵⁹ maar deze verbondenheid heeft geen fysieke component.³⁶⁰ Dit laatste maakt dat deze cyberidentiteiten niet dezelfde status bezitten als fysieke personen en daarmee ook niet de humanitair oorlogsrechtelijke bescherming krijgen die personen wel genieten.³⁶¹

Schending van de integriteit van de computergegevens kan wel indirecte gevolgen hebben voor de fysieke identiteiten die zij representeren, maar deze zijn te indirect om toegerekend te kunnen worden aan de manipulatie. Ik bedoel hiermee dat de indirecte gevolgen afhankelijk zijn van andere tussenliggende gebeurtenissen, onafhankelijk van de manipulatie van de computergegevens. Ik zal dit verduidelijken met een voorbeeld aan de hand van mijn eerder behandelde indeling van de componenten van het cyberdomein.

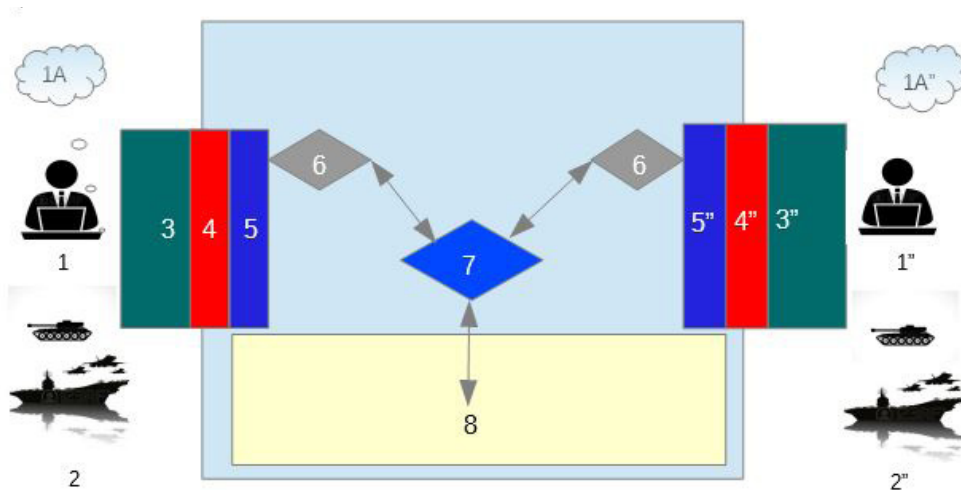
■
357 Het eerste voorbeeld is dan wel een verboden aanval vanwege de beschermde status van medische gegevens. Ik kom daar in het volgende hoofdstuk uitgebreid op terug.

358 Zie Hoofdstuk 3 par. 3.3.3.

359 Ducheine & van Haaster 2014, p. 311.

360 Een fysiek persoon kan zijn haar kleuren, hier een foto van maken en deze foto wel of niet gebruiken als profielfoto op een socialmedia-account (een cyberidentiteit). Andersom heeft het virtueel veranderen van de haarkleur op de socialmedia-account geen directe invloed op de haarkleur van de natuurlijke persoon.

361 Dit betreft de huidige stand van zaken. De groei aan mens-machine interfaces, zie par. 4.5.3.2. voetnoot 791, kan in de (nabije) toekomst herziening van de dichotomie personen-objecten noodzakelijk maken. Dergelijke mens-machine interfaces kunnen waarschijnlijk ook leiden tot fysieke gevolgen bij personen, waardoor deze redenering over cyberidentiteiten aangepast zal moeten worden.



Fysieke componenten

1: fysieke personen/instaties die gebruikmaken van het cyberdomein.

1A: denkbeelden, ideeën en manieren van handelen.

2: militair materieel.

3: fysieke hardware (computers, modems etc.)

Niet-fysieke componenten

4: firmware.

5: besturingsprogramma's.

6: cyberidentiteiten.

7: applicaties, programma's etc.

8: computergegevens (bestanden, foto's, adressen etc.).

Figuur 8 Onderverdeling elementen cyberdomein

De gedachten of de gemoedstoestand van fysieke personen, categorie 1A en 1A" uit figuur 8, kunnen veranderen als gevolg van manipulatie van de computergegevens (8) uit een socialmedia-account (6). Het is voorstelbaar dat dit soort militaire operaties wordt uitgevoerd met deze indirecte gevolgen als primaire doelstelling. Met andere woorden de gedachte- of stemmingsverandering wordt beoogd, bijvoorbeeld om de wil om door te vechten weg te nemen. Wat de persoon vervolgens fysiek doet vanwege die gedachte- of stemmingsverandering (als die doelstelling al gehaald wordt), is mede afhankelijk van vele factoren die losstaan van de manipulatie van de computergegevens.

Dergelijke operaties zijn te kenmerken als een *Psychological Operations*. Dit soort operaties valt onder de noemer van beïnvloedingsoperaties.³⁶² Deze non-kinetische militaire operaties zijn al veel ouder dan het cyberdomein en worden doorgaans niet gerekend tot aanvallen,³⁶³ hetgeen logisch is, gelet op het ontbreken van directe of redelijkerwijs

³⁶² Voor een overzicht en analyse van beïnvloedingsoperaties zie RAND Corporation 2009, *Foundations of Effective Influence Operations*.

³⁶³ Zie bijv. Dinstein 2014, p. 162.

voorzienbare indirecte fysieke gevolgen. Zolang schendingen van de integriteit van deze categorie computergegevens niet leiden tot perfidie, zijn desinformatie en onwaarheden vanuit humanitair oorlogsrechtelijk standpunt toegestaan: “*International Humanitarian Law permits legitimate ruses or deceptions.*”³⁶⁴

De conclusie van deze subparagraaf is dat inbreuk op de integriteit van cyberidentiteiten geen directe fysieke gevolgen zal hebben. Inbreuk op de integriteit van firmware, sturingsprogramma's, computerprogramma's en computergegevens kan directe fysieke gevolgen hebben. Of inderdaad fysieke gevolgen op zullen treden en of deze gevolgen dan zijn aan te merken als schade is afhankelijk van de concrete situatie en varieert van nauwelijks voorstelbaar tot uiterst waarschijnlijk.

4.5.5.3.3. Beschikbaarheid

Een schending van de beschikbaarheid houdt in dat geautoriseerde gebruikers niet meer kunnen beschikken over bepaalde computergegevens of gebruik kunnen maken van bepaalde diensten, waarbij het niet noodzakelijk is dat de veroorzaker van deze schending zelf wel bij de computergegevens kan. Een bekend voorbeeld hiervan is een (*Distributed Denial-of-Service*)³⁶⁵ actie, waarbij een website van een bank met daarop toegang tot een bepaalde dienst, bijvoorbeeld internetbankieren, wordt overladen met verzoeken om informatie. De server van betreffende website loopt daardoor vast, waarna de dienst, in dit voorbeeld het internetbankieren, voor niemand beschikbaar is.

Om de beschikbaarheid aan geautoriseerde gebruikers te ontzeggen, hoeft de veroorzaker niet noodzakelijkerwijs zelf bij de computergegevens of diensten te komen. Dit laatste heeft voor dit onderzoek een aantal consequenties. Als eerste betekent dit dat verstoring van beschikbaarheid door kwaadwillenden relatief eenvoudig te realiseren is.³⁶⁶ De keerzijde van deze medaille is dat door deze beïnvloeding van de beschikbaarheid niets aan het systeem of de daarin opgenomen computergegevens wordt veranderd, waardoor herstel naar de situatie van voor de beïnvloeding ook relatief eenvoudig zal zijn. Daardoor zal de verstoring van beschikbaarheid ook relatief kort duren. Omdat bij deze manier van verstoring van de beschikbaarheid geen veranderingen aan het systeem of aan de daarin ondergebrachte computergegevens wordt aangebracht, lijken fysieke gevolgen als gevolg van het (kortstondig) niet beschikbaar zijn van bepaalde informatie of diensten niet voorstelbaar. Dit gaat echter alleen op indien alle voor het goed functioneren van het systeem benodigde componenten binnen het systeem aanwezig zijn. Met andere woorden, het systeem kan ook functioneren zonder verbinding met bronnen buiten het systeem.

³⁶⁴ Gill & Fleck 2012, p. 405.

³⁶⁵ Deze methode wordt meestal aangeduid met de Engelse term afkorting (D)DoS. Indien bij het overvragen van een website gebruik gemaakt wordt van slechts één computer spreekt men van DoS. Indien gebruik gemaakt wordt van twee of meerdere computers spreekt men van DDoS.

³⁶⁶ Om de vertrouwelijkheid en zeker de integriteit van virtuele componenten te kunnen beïnvloeden zal degene die dit wil doen in het systeem moeten komen. Het systeem zal op enige manier beveiligd/beperkt zijn, anders kan moeilijk gesproken worden van ongeautoriseerde toegang, dus om in het systeem te komen zal een weg om de beveiliging/beperking heen gevonden moeten worden. Omdat dit laatste voor schending van beschikbaarheid niet hoeft is deze schending relatief eenvoudig te realiseren, ook zonder (technische) kennis van het systeem.

De situatie is anders indien een of meerdere componenten, bijvoorbeeld computergegevens, van buiten het systeem moeten komen. Door de verstoring zijn deze computergegevens dan (tijdelijk) niet beschikbaar. Het hangt dan af van de manier waarop het systeem georganiseerd is of fysieke gevolgen op kunnen treden. Ik zal dit aan de hand van een voorbeeld verduidelijken. Een olieraffinaderij heeft het hele raffinageproces geautomatiseerd. Om dit proces goed te laten verlopen is op een aantal plaatsen sensoren geplaatst die continu computergegevens doorgeven aan een centrale computer die het hele proces reguleert. Indien al deze computergegevens via een intern en gesloten netwerk (dus binnen het systeem) verzonden worden, zal dit systeem niet verstoord worden indien de raffinaderij het slachtoffer is van een (*Distributed*) *Denial-of-Service* actie.

Als echter ook computergegevens van buiten het systeem nodig zijn om het proces te laten voortgaan, zullen die gegevens bij een (*Distributed*) *Denial-of-Service* actie niet beschikbaar zijn, waardoor het proces niet naar behoren kan verlopen. Het systeem dat gegevens mist kan zo geprogrammeerd zijn dat het op dat moment alle communicatie met de buitenwereld afsluit, een zogenaamde *fail close procedure*,³⁶⁷ en het proces op een veilige manier stillegt (gecontroleerde *shutdown*). Is het systeem daarentegen geprogrammeerd om bij ontbreken van gegevens het proces gewoon door te laten gaan, dan kan het ontbreken van gegevens tot fysieke schade leiden, bijvoorbeeld doordat een oplopende druk of temperatuur niet of niet tijdig wordt gesignaleerd.

Een dergelijk ontwerp, waarbij fysieke schade kan ontstaan door het niet beschikbaar zijn van (kritieke) computergegevens lijkt in eerste instantie misschien vergezocht, maar “*unfortunately, like other information technologies, most [cyber physical systems referring to the tight conjoining of and coordination between computational and physical resources] were originally designed with little or no security, or security has been added.*”³⁶⁸ Ontbreken van computergegevens (schending van de beschikbaarheid) kan dus directe fysieke schade veroorzaken indien niet, of niet voldoende, is geanticipeerd op het niet beschikbaar zijn van virtuele componenten. Dit geldt voor alle categorieën van virtuele componenten, al zal het vaak ontbrekende computergegevens betreffen. Dit laatste omdat de andere componenten zich vaker binnen de grenzen van het systeem zullen bevinden.

Uiteraard is het ook mogelijk om de beschikbaarheid te verstoren door wel in het systeem te komen, dus op een manier waarbij de veroorzaker wel bij de computergegevens of diensten kan. Er zal dan echter sprake zijn van een overlap met aantasting van de betrouwbaarheid, bijvoorbeeld door aanpassingen waardoor de beveiliging kan worden ontweken, of inbreuk op de vertrouwelijkheid, bijvoorbeeld doordat onder valse voorwendselen ongeautoriseerde toegang tot het systeem is verkregen. Dergelijke overlappingsen komen in de volgende subparagraaf aan de orde.

■
³⁶⁷ “*Fail close: A device or system is set, either physically or via software, to shut down and prevent further operation when failure conditions are detected.*” *Fail Close, Fail Open, Fail Safe and Failover: ABCs of Network Visibility*. Available on: <https://www.ixiacom.com/company/blog/fail-closed-fail-open-fail-safe-and-failover-abcs-network-visibility>, laatst geraadpleegd 28 nov 2018.

³⁶⁸ Applegate 2013, p. 165.

Bij inbreuk op de beschikbaarheid van virtuele componenten is mijn subconclusie dat de mogelijkheden voor fysieke gevolgen sterk afhangen van de manier waarop een systeem omgaat met het ontbreken van bepaalde virtuele componenten. Bij een goed ontworpen systeem zullen fysieke gevolgen voorkomen worden. Bij een minder goed of slecht ontworpen systeem kunnen fysieke gevolgen optreden. Dit geldt voor alle verschillende virtuele componenten.

4.5.5.3.4 Overlappende beginselen

Voor het resultaat van een militaire operatie maakt het niet uit of fysieke schade optreedt als gevolg van schending van de integriteit of van de beschikbaarheid.³⁶⁹ Wanneer fysieke schade optreedt, is het een aanval. Het werkt echter verhelderend te weten in welke gevallen die fysieke schade op *kan* treden. Dit kan de partij die de operatie uitvoert helpen om te bepalen wanneer een dergelijke operatie beschouwd moet worden als een aanval.³⁷⁰ Het is ook van belang voor de partij die zich voorbereidt op of daadwerkelijk verdedigt tegen dergelijke cyberoperaties, om kwetsbaarheden, die fysieke gevolgen kunnen hebben, te onderkennen. Een beter beeld krijgen van wanneer fysieke schade op kan treden is ook de reden van de indeling naar schending van vertrouwelijkheid, integriteit en beschikbaarheid. Zoals hiervoor al aangegeven, is een strikte scheiding tussen de verschillende beginselen niet altijd te handhaven. Als een inbreuk op de integriteit van een computerprogramma gebruikt wordt om de toegang tot bepaalde informatie te ontzeggen, is sprake van zowel inbreuk op de integriteit als de beschikbaarheid. Soms is het lastig een actie eenduidig te benoemen waardoor indeling in één beginsel niet lukt. Een voorbeeld hiervan is het ongeautoriseerd vernietigen van computergegevens, zijn deze dan niet meer beschikbaar of (ernstig) gemodificeerd? Het tegenovergestelde, het toevoegen van computergegevens, levert een soortgelijk probleem. Neem een actie als spoofing, bijvoorbeeld van een GPS signaal. Men spreekt van *spoofing* als gebruik gemaakt wordt van “a malicious signal that overpowers the authentic signal and misleads the receiver to use a forged signal for further processing.”³⁷¹ In tegenstelling tot *jamming*, een inbreuk op de beschikbaarheid waarbij door een overvloed aan andere signalen het originele signaal niet meer herkend wordt en geen plaatsbepaling meer kan plaatsvinden, wordt bij *spoofing* de ontvanger misleid door het toevoegen van gemanipuleerde signalen, waardoor een verkeerde plaatsbepaling wordt berekend.³⁷² Valt het toevoegen van extra signalen onder schending van vertrouwelijkheid, integriteit of beschikbaarheid?

Voor dit onderzoek is bovenstaande indelingsproblematiek bij overlappende beginselen van minder belang. Het onderscheid werkt verhelderend bij de vraag wanneer fysieke

■
369 Het hele CIA concept is namelijk een defensief veiligheidsconcept.

370 En daarmee aan andere regels en voorwaarden moet voldoen dan een militaire operatie die de drempel van aanval niet haalt. Het verschil in regels en voorwaarden is onderwerp van het volgende hoofdstuk.

371 Wen 2005, p.1.

372 Overigens is tussen *jamming* en *spoofing* een mate van overlap mogelijk. Zie bijvoorbeeld de NAVO definitie van *jamming*: AAP-o6 2014, “Deliberate interference, caused by emissions intended to render unintelligible or falsify the whole or part of a wanted signal,” mijn accentuering.

schade kan ontstaan. Waardoor deze fysieke schade ontstaat is daarbij van ondergeschikt belang.

4.5.5.3.5 Samenvatting Confidentiality-Integrity-Availability

Onderstaande tabel geeft een samenvatting van de hiervoor gegeven analyse van de Confidentiality-Integrity-Availability triade op de verschillende categorieën van virtuele componenten van het cyberdomein.

	Vertrouwelijkheid C	Integriteit I	Beschikbaarheid A
Firmware	-	+	+
Besturingsprogramma's	-	+	
Cyberidentiteiten	-	-	
Computerprogramma's	-	+	
Computergegevens	-	+	

Figuur 9 Overzicht CIA triade: mogelijkheid van fysieke gevolgen.

+ : Fysieke schade is mogelijk.

– : Fysieke schade is niet mogelijk.

De conclusie is dat militaire operaties gericht op de integriteit van firmware, besturingsprogramma's, computerprogramma's en computergegevens en de beschikbaarheid van alle virtuele componenten, fysieke gevolgen *kunnen* hebben en kunnen daarmee, in potentie, voldoen aan de voorwaarden van aanval. Of dat ook zo is zal afhangen van de omstandigheden van het geval.

4.5.5.4 Conclusie schade aan virtuele componenten binnen het humanitair oorlogsrecht

Net als bij de status van virtuele componenten binnen het humanitair oorlogsrecht bestaat (nog) geen eenduidige interpretatie van hoe schade aan virtuele componenten uitgelegd moet worden zolang de gevolgen zich beperken tot deze virtuele componenten. Aan de ene zijde is het duidelijk dat niet alle verstoringen aan virtuele componenten direct schade opleveren, wat betekent dat er zoiets moet zijn als een minimum drempel. Aan de andere zijde lijkt het niet acceptabel om grootschalige gevolgen van verstoringen aan virtuele componenten niet te zien als schade. De interpretatieverschillen gaan met name over de hoogte van de drempel voordat verstoring schade wordt.

In tegenstelling tot mijn positie bij de status van virtuele componenten in het humanitair oorlogsrecht ben ik bij de kwalificatie van schade aan virtuele componenten terughoudender om een nieuwe interpretatie, in de zin dat ook zonder fysieke gevolgen sprake kan zijn van schade (en daarmee impliciet sprake is van een aanval), te aanvaarden en wel om een tweetal redenen. Ten eerste zullen grootschalige gevolgen van verstoringen aan virtuele componenten, die geen letsel aan of dood van personen of beschadiging of

vernietiging van fysieke objecten tot gevolg hebben, ‘slechts’ van verstorende aard zijn.³⁷³ Deze verstorende aard kan zeker gevolgen hebben, zoals bijvoorbeeld economische gevolgen of maatschappelijke onrust. Het is echter nooit de bedoeling geweest van het humanitair oorlogsrecht om dit soort gevolgen te reguleren of te beperken en dit heeft het humanitair oorlogsrecht in de praktijk ook nooit gedaan.³⁷⁴ De komst van het cyberdomein als nieuwe mogelijkheid om militaire operaties uit te voeren heeft hierin mijns inziens geen verandering gebracht.

Als tweede lijken staten, zoals eerder vermeld de ultieme ‘makers’ van het humanitair oorlogsrecht,³⁷⁵ in de discussie over schade aan virtuele componenten ook binnen andere rechtsgebieden terughoudend te zijn in uitbreiding van het schadebegrip buiten de ‘traditionele’ opvattingen over schade. Deze opvatting zie ik ook terug in de consensus die de internationale expertgroep bereikte bij de samenstelling van de *Tallinn Manual* over de definitie van ‘cyber attack’.³⁷⁶ De traditionele bestanddelen van schade (*damage or destruction to objects*) leveren geen problemen op. Bij uitbreiding naar de functionaliteit van een object was de meerderheid van mening dat pas sprake was van schade als herstel van de functionaliteit “requires replacement of physical components.”³⁷⁷

4.5.6 De ondergrens van cyberaanval

Na de hierboven beschreven discussies over de status van en schade aan virtuele componenten in het cyberdomein kan ik nu terugkeren naar de ondergrens van cyberaanval. Op basis van mijn conclusies kan ik tot het oordeel komen dat de ondergrens van aanval bij cyberoperaties dezelfde is als bij aanvallen in traditionele zin. Ik doe dit aan de hand van een drietal argumenten.

4.5.6.1 Terug naar het doel van het humanitair oorlogsrecht

Een teleologische redenering levert het eerste argument om de ondergrens van aanval bij cyberoperaties niet anders uit te leggen dan bij militaire operaties in traditionele zin. Dit volgt uit het doel van het humanitair oorlogsrecht.³⁷⁸ Zoals in Hoofdstuk 2 uitgebreid aan de orde kwam, is dat doel tweeledig: enerzijds het reguleren van oorlogvoering en

373 Zie bijv. Nationaal Veiligheidsprofiel 2016, p. 123. Hier wordt, als *worstcase*-scenario van een cyberaanval, de aanval met een verstorende werking op de vitale infrastructuur genoemd, resulterend in fysieke effecten (als voorbeeld wordt genoemd een aanval op de Nederlandse energiesector) die “in potentie net zoveel impact veroorzaken als een fysieke aanval op een vitaal procesonderdeel.” Om vervolgens op te merken “voor cyberaanvallen waarbij de integriteit of vertrouwelijkheid van systemen wordt aangetast, zijn de gevolgen minder evident.”

374 Neem de economische gevolgen. Naarmate een gewapend conflict grootschaliger wordt en/of langer duurt zal dit zeker negatieve gevolgen hebben voor de burgerbevolking en dit kan leiden tot voedseltekorten of verminderde medische voorzieningen met alle negatieve gevolgen van dien. Of neem maatschappelijke onrust wanneer veel militairen omkomen bij een gewapend conflict. Deze reële, maar niet fysieke, gevolgen voor een maatschappij zijn nooit onderwerp geweest binnen het humanitair oorlogsrecht.

375 Schmitt & Watts 2015, p. 193.

376 Schmitt 2013, p. 106, Rule 30.

377 Schmitt 2013, p. 108, mijn accentuering.

378 Hiermee gehoor gevend aan art. 31 Verdrag van Wenen, “een verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het Verdrag in hun context en in het licht van voorwerp en doel van het verdrag.” Mijn accentuering.

anderzijds het beschermen van de slachtoffers van gewapende conflicten.³⁷⁹ Deze dubbele doelstelling wordt uitgewerkt door (het vinden van) een balans tussen militaire noodzaak en humaniteit.³⁸⁰ De discussie over uitbreiding van de definitie van aanval naar niet-fysieke gevolgen wordt ingegeven doordat gefocust wordt op het beginsel onderscheid, dat, zoals eerder is aangegeven, ook weer teruggevoerd kan worden op de balans tussen de grondbeginselen militaire noodzaak en humaniteit.³⁸¹

Het is een gegeven dat het humanitair oorlogsrecht zich in de loop van de afgelopen ruim honderd jaar heeft ontwikkeld en dat daarbij het evenwicht in de balans tot op zekere hoogte is verschoven in het voordeel van humaniteit.³⁸² Door een sterke focus te leggen op humaniteit ligt echter het gevaar op de loer dat het doel van het humanitair oorlogsrecht te eenzijdig wordt belicht. Het doel van het humanitair oorlogsrecht is nooit geweest om de burgerbevolking te vrijwaren van alle effecten van een gewapend conflict.³⁸³ Gegeven het feit dat sprake is van een gewapend conflict, de *sine qua non* voor het van toepassing zijn van het humanitair oorlogsrecht, is het alom aanvaard, en onvermijdelijk, dat de burgerbevolking daarvan negatieve gevolgen ondervindt.³⁸⁴ Het zou een revolutie binnen het humanitair oorlogsrecht betekenen wanneer gesuggereerd werd dat elke verstoring van civiele activiteiten verboden is.³⁸⁵ Waar het humanitair oorlogsrecht zich op richt, is het minimaliseren van de 'rampen van den oorlog, voor zoover de militaire noodzakelijkheid zulks toelaat'.³⁸⁶ Dat heeft in de loop der jaren geresulteerd in een delicaat evenwicht.³⁸⁷

Hieruit volgt een andere, meer tekstuele, redenering ter ondersteuning van hetzelfde argument.³⁸⁸ Zoals weergegeven in Hoofdstuk 2 heeft het evenwicht tussen militaire noodzaak en humaniteit geresulteerd in een uitleg van het begrip 'aanval' die gekoppeld is aan de fysieke gevolgen, met daarnaast militaire operaties zonder fysieke gevolgen die niet vallen onder het begrip 'aanval'. Het feit dat door technologische ontwikkelingen meer mogelijkheden ontstaan om militaire voordelen te behalen, zonder dat dit noodzakelijk fysieke effecten teweegbrengt, heeft hierin geen fundamentele verandering gebracht in de zin dat het noodzakelijk zou worden om het evenwicht te herzien. Het betekent 'slechts' dat de verzameling van militaire operaties die geen aanval zijn, uitgebreid is waarbij

■
379 Zie Hoofdstuk 2 par. 2.3.1.

380 Zie Hoofdstuk 2 par. 2.3.3.

381 Zie Hoofdstuk 2 par. 2.3.1.

382 Wel aangeduid als de "humanisation of IHL", Kolb 2013, p. 52. Zie ook Hoofdstuk 2 par. 3.2.

383 Wat soms wel gesuggereerd wordt. Zie bijvoorbeeld Droege 2012, p. 534, "thus, whether the traditional rules of IHL will provide sufficient protection to civilians from the effects of cyber warfare remains to be seen." Mijn accentuering. Schmitt 203, p. 127, "In their view, failure to do so [...] that the civilian population shall enjoy general protection from the effects of hostilities." Mijn accentuering.

384 Het humanitair oorlogsrecht erkent 'oorlog' als een gegeven, inclusief de negatieve gevolgen die een 'oorlog' heeft of kan hebben.

385 Schmitt 2014b, p. 296.

386 Hague Convention IV 1907, preambule.

387 Schmitt 2010, p. 796.

388 Gebaseerd op art. 31 van het Verdrag van Wenen namelijk dat een verdrag moet worden uitgelegd overeenkomstig de gewone betekenis van de termen van het verdrag. Mijn accentuering.

deze nieuwe mogelijkheden moeten voldoen aan dezelfde regels die altijd al golden voor militaire operaties die geen ‘aanval’ zijn.³⁸⁹ Het begrip ‘aanval’ blijft daarmee op de gangbare manier uitgelegd en gebruikt worden. Het cyberdomein, en de mogelijkheden voor militaire operaties in of via dit domein, geven geen aanleiding om deze gewone betekenis te herzien.

4.5.6.2 *Humanitair oorlogsrecht wordt gemaakt door staten*

Een tweede argument is meer gebaseerd op de context waarin het humanitair oorlogsrecht tot stand komt.³⁹⁰ Ondanks alle veranderingen in de wereld, samenhangend met globalisering en de toegenomen onderlinge afhankelijkheid die samenwerking ‘afdwingt’, is de internationale samenleving een samenleving gebleven van soevereine staten die er slechts in uitzonderingsgevallen toe zijn overgegaan bevoegdheden definitief over te dragen aan een boven of buiten de staten staande instelling.³⁹¹ Dit heeft zijn weerslag op het internationaal recht en daarmee ook op het humanitair oorlogsrecht als onderdeel daarvan. Het zijn alleen staten die de capaciteit bezitten om internationaal recht te maken, door middel van verdragen of door middel van algemeen aanvaarde rechtspraktijk die verwordt tot gewoonterecht³⁹² met andere woorden “*States, and only States ‘make’ IHL.*”³⁹³

Deze staat-centrische benadering is logisch verklaarbaar vanuit de soevereiniteitsgedachte van staten. Op deze manier zijn het alleen staten zelf die bepalen aan welke regels, of juridische uitleg van regels, zij gebonden zijn en blijft het risico om gebonden te worden, *de jure* of *de facto*, aan regels waarmee zij het niet eens zijn, beperkt.³⁹⁴ Het zijn namelijk deze staten die, wanneer zij betrokken zijn bij een gewapend conflict, de mogelijkheid willen behouden om hun belangen veilig te stellen, met andere woorden, het conflict in hun voordeel te beslechten. Door militaire operaties zonder fysieke gevolgen niet te kwalificeren als aanval kunnen misschien strategische doelen behaald worden zonder, of met minder, kinetische aanvallen. Uit een dergelijke overweging blijkt dat het grondbeginsel van humaniteit, waarvoor staten ook verantwoordelijk zijn, niet per se leidt tot een uitbreiding van de kwalificatie aanval voor militaire operaties zonder fysieke gevolgen. Staten zullen oog hebben voor beide zijden van de balans tussen militaire noodzaak en humaniteit. Het zijn namelijk staten die, in tegenstelling tot rechters of de

■ 389 Zie Hoofdstuk 3. Voor de uitwerking naar militaire operaties in het cyberdomein, zie hierna Hoofdstuk 5.

390 Art. 31 Verdrag van Wenen, “een verdrag moet te goeder trouw worden uitgelegd overeenkomstig de gewone betekenis van de termen van het Verdrag in hun context en in het licht van voorwerp en doel van het verdrag.” Mijn accentuering.

391 Kooijmans 2002, p. 3.

392 Art 38 lid 1 Statuut Internationaal Gerechtshof. Zie ook Hoofdstuk 3 par. 3.2.

393 Schmitt & Watts 2015, p. 193. Dit is de huidige stand van zaken, maar de schrijvers verwijzen daarbij wel naar een artikel van Roberts & Sivakumaran ‘*Lawmaking by nonstate Actors: Engaging Armed Groups in the Creation of International Humanitarian law.*’ In dit artikel wordt gesteld dat; “It is worth questioning whether nonstate armed groups can and should be given a role in the creation of the law that governs conflicts to which they are parties.”

394 Schmitt 2010, p. 816.

meest bevoegde schrijvers,³⁹⁵ de praktische gevolgen van een eventuele verschuiving in de balans tussen militaire noodzaak en humaniteit ondervinden.³⁹⁶

Het loslaten van de fysieke gevolgen van letsel en/of schade als onderscheidend criterium voor aanval ten opzichte van militaire operaties die geen aanval zijn, betekent dat meer militaire operaties onder het begrip ‘aanval’ zouden vallen. Dit betekent ook dat meer operaties moeten voldoen aan de stringenter eisen van aanval, waardoor de mogelijkheden voor staten om, via hun strijdkrachten, een gewapend conflict legitiem in hun voordeel te beslechten waarschijnlijk worden beperkt.³⁹⁷ Staten zullen hiertoe bereid zijn indien een substantiële onbalans is ontstaan,³⁹⁸ of dreigt te ontstaan,³⁹⁹ tussen militaire noodzaak en humaniteit. Met het ontstaan van het cyberdomein en de mogelijkheden voor militaire operaties binnen dat domein is van een dergelijke onbalans, naar mijn mening, (nog) geen sprake.

4.5.6.3 Doorwerking verschuiving *jus in bello* naar *jus ad bellum*

Naast de hierboven genoemde consequenties die staten, mogelijk, zullen weerhouden een verruiming van het begrip aanval te accepteren door ook niet-fysieke gevolgen mee te nemen bij de bepaling of een militaire operatie kwalificeert als ‘aanval’, bestaat het gevaar voor een mogelijke doorwerking van deze verruiming naar het *jus ad bellum*. Indien staten accepteren dat de breed aanvaarde betekenis van aanval als een daad van geweld die gericht is op de fysieke consequenties⁴⁰⁰ wordt opgezet om ook niet-fysieke consequenties te omvatten, bestaat het gevaar dat dit gebruikt gaat worden als argument om de discussie over de reikwijdte van het uitgangspunt van het hedendaagse *jus ad bellum*, het verbod op het gebruik van of bedreiging met geweld in internationale betrekkingen,⁴⁰¹ anders te gaan interpreteren. Ik wil hiermee geenszins zeggen dat een dergelijke doorwerking een automatisme is. Het *jus ad bellum* en het *jus in bello* zijn, en blijven, twee gescheiden rechtsgebieden met hun eigen kaders en definities.⁴⁰² Wat ik aangeef is, dat als in het ene rechtsgebied het bereik van het begrip ‘dadens van geweld’ (*acts of violence*) wordt opgerekt, het gevaar bestaat dat een soortgelijke uitbreiding van het begrip ‘geweld’ (*use of force*) als discussiepunt wordt opgebracht. De vraag is echter of staten, vanuit bijvoorbeeld geopolitieke overwegingen, dit wenselijk achten.

■
395 De secundaire bronnen voor internationaal recht zoals genoemd in art. 38 lid 1d Statuut van het Internationaal Gerechtshof.

396 Schmitt 2010, p. 838.

397 Zo mogen civiele objecten wel gebruikt worden voor een militaire operatie, maar niet aangevallen worden, zie Hoofdstuk 3 par. 3.3.3.4. Loslaten van fysieke schade als criterium betekent dat gebruik van civiele objecten eerder aan de regels van ‘aanval’ zal moeten voldoen, waardoor de mogelijkheden voor het gebruik van civiele objecten afnemen.

398 Zo is bijvoorbeeld naar aanleiding van de *carpet bombings* het verbod op niet-onderscheidende aanvallen (art. 51 lid 4 Aanvullend Protocol I) ontstaan.

399 Bijvoorbeeld het verbod op het gebruik van biologische wapens, Verdrag biologische wapens 1972.

400 Zie Hoofdstuk 2 par. 2.5.

401 Art. 4 lid 2 Handvest Verenigde Naties.

402 Zie bijv. Gill in Ducheine, Schmitt & Osinga 2016, p. 102: “They are generally accepted as constituting distinct legal spheres or regimes, both historically and presently in practice and legal opinion.”

4.5.6.4 Conclusie

De ondergrens van cyberaanval kan ik nu op dezelfde manier definiëren als de ondergrens van aanval in traditionele zin, maar dan aangevuld met de definitie van cyberaanval waarmee ik de vraag beantwoord die centraal stond in dit hoofdstuk, namelijk wat de ondergrens van aanval in het cyberdomein is.

De ondergrens wordt dan: de toepassing van cybercapaciteiten door militairen en/of met militaire middelen, die gericht zijn op fysiek letsel of schade of die deze fysieke gevolgen hebben, welke in het kader van een gewapend conflict worden toegepast met als doel een militair voordeel op de tegenstander te behalen in, of door het gebruik van, het cyberdomein.

De ondergrens onderscheidt een cyberaanval, of aanval in het cyberdomein, van andere militaire (cyber)operaties die geen cyberaanval vormen. In de ondergrens is de voorwaarde om fysieke schade of letsel te veroorzaken of deze fysieke gevolgen daadwerkelijk hebben, opgenomen. Hieronder valt ook het verlies van functionaliteit van een object als hiervoor vervanging van fysieke onderdelen noodzakelijk is. Zonder te voldoen aan deze voorwaarde is geen sprake van 'aanval', militaire cyberoperaties die wel aan deze voorwaarde voldoen zijn 'aanvallen' in het cyberdomein in de zin van artikel 49 Aanvullend Protocol I.

Net als bij de ondergrens van aanval in traditionele zin moet ook bij een cyberaanval de fysieke schade voorzienbaar zijn.⁴⁰³ Een nadere beschouwing van de virtuele componenten van het cyberdomein leert dat schendingen van vertrouwelijkheid van virtuele componenten niet kunnen leiden tot fysieke gevolgen. Ook aantasting van de integriteit van cyberidentiteiten kan niet leiden tot fysieke gevolgen. Militaire cyberoperaties gericht op deze beginselen van de *Confidentiality-Integrity-Availability* triade kunnen daarmee geen aanval in de zin van artikel 49 Aanvullend Protocol I opleveren. Aantastingen van de integriteit van firmware, besturingsprogramma's, computerprogramma's en computergegevens en de beschikbaarheid van alle virtuele componenten, *kunnen* wel fysieke gevolgen hebben.

De conclusie dat de ondergrens van aanval in het cyberdomein niet wezenlijk anders is dan voor een aanval in traditionele zin heeft als bijkomend gevolg dat de regels die gelden voor militaire cyberoperaties beneden de grens van aanval⁴⁰⁴ dezelfde zijn als de regels voor andere militaire operaties beneden de grens van aanval. Met andere woorden, de conclusies voor cyberoperaties beneden de grens van aanval kunnen ook worden toegepast op meer traditionele militaire operaties beneden de grens van aanval zoals inlichtingenoperaties of psychologische operaties.

Na de vaststelling van de ondergrens van aanval in het cyberdomein kan ik nu overgaan naar de hoofdvraag van mijn onderzoek, welke regels gelden in het humanitair

■
⁴⁰³Zie Hoofdstuk 2 par. 6.4.

⁴⁰⁴Welke regels dat zijn wordt beantwoord in Hoofdstuk 5.

oorlogsrecht voor militaire cyberoperaties onder de drempel van artikel 49 lid 1 Aanvullend Protocol I en hoe kunnen deze regels worden toegepast?

5

Hoofdstuk 5 Regels uit het humanitair oorlogsrecht voor militaire cyberoperaties onder de drempel van artikel 49 lid 1 Aanvullend Protocol I en hoe deze regels worden toegepast

5.1 Inleiding

In Hoofdstuk 3 heb ik aan de hand van de grondbeginselen van het humanitair oorlogsrecht onderzocht welke regels uit het humanitair oorlogsrecht van toepassing zijn op militaire operaties die de drempel van aanval niet halen. In dit hoofdstuk zal ik de uitkomsten daarvan projecteren op cyberoperaties.¹ Ik zal daarbij de structuur van Hoofdstuk 3 volgen zodat achtereenvolgens de grondbeginselen militaire noodzaak, humaniteit, onderscheid, proportionaliteit en eervol gedrag aan bod komen. Ik zal vervolgens in een samenvattende paragraaf het antwoord op de vraag van dit hoofdstuk formuleren: welke regels gelden in het humanitair oorlogsrecht voor militaire cyberoperaties onder de drempel van artikel 49 lid 1 Aanvullend Protocol I en hoe kunnen deze regels worden toegepast? Dit hoofdstuk besluit ik met een synthese waarin ik in zal gaan op het belang en de toegevoegde waarde van de conclusies van dit onderzoek.

5.2 Militaire noodzaak

In Hoofdstuk 3 heb ik geconcludeerd dat het grondbeginsel van militaire noodzaak ook geldt voor militaire operaties beneden de drempel van aanval met de nuance dat dit alleen geldt als, op basis van het grondbeginsel van onderscheid, negatieve gevolgen voor burgers of burgerobjecten te verwachten zijn als gevolg van de militaire operatie.² Bij de onderstaande bespreking neem ik als uitgangspunt dat negatieve gevolgen te verwachten zijn, en dus dat militaire noodzaak aanwezig moet zijn.³ De nuance dat onder specifieke omstandigheden militaire noodzaak niet vereist is, zal ik wel bij de conclusie terug laten komen.

Als het beginsel militaire noodzaak toegepast wordt op militaire cyberoperaties,⁴ betekent dit dat er een merkbaar militair voordeel ten opzichte van de tegenstander te verwachten

■
1 Een niet ongebruikelijke methode om uitleg te geven over de toepassing van regels die gemaakt zijn voordat een nieuwe techniek zijn intrede deed. Vergelijk DoD Law of War Manual 2016, p. 1013, "Specific law of war rules may apply to cyber operations, even though those rules were developed before cyber operations were possible. When no more specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during cyber operations in armed conflict."

2 Zie Hoofdstuk 3 par. 3.3.1.

3 Nog los van het feit dat het onlogisch en oneconomisch is om een militaire operatie waarvoor geen noodzaak bestaat toch uit te voeren.

4 Zie Hoofdstuk 4 par. 4.3.2, Militaire cyberoperaties: de toepassing van cybercapaciteiten door militairen en/of met militaire middelen om een specifieke doelstelling, namelijk een militair voordeel ten opzichte van de tegenstander, te behalen, in of door het gebruik van het cyberdomein.

moet zijn.⁵ Ik gebruik hier bewust het bijvoeglijke naamwoord ‘merkbaar’ en niet “‘tastbaar en rechtstreeks’ of ‘duidelijk’ zoals deze wel gebruikt worden in artikel 51 respectievelijk 52 Aanvullend Protocol I,⁶ waar in beide gevallen het te behalen militair voordeel in het kader van een aanval geplaatst is.

Zoals ik in Hoofdstuk 2 aangaf werkt de balans tussen militaire noodzaak en humaniteit beide kanten op. Naarmate meer inbreuk op het grondbeginsel humaniteit wordt gemaakt zullen hogere eisen gesteld worden aan de militaire noodzaak om de inbreuk op humaniteit te kunnen rechtvaardigen. Met andere woorden, het te behalen militaire voordeel zal groter moeten zijn. De bijvoeglijke naamwoorden ‘tastbaar en rechtstreeks’ en ‘duidelijk’ bevestigen deze werking. Bij de bescherming van personen moet het militair voordeel ‘tastbaar en rechtstreeks’ zijn, wat betekent dat *“the advantage concerned should be substantial and relatively close, and that advantages which are hardly perceptible and those which would only appear in the long term should be disregarded.”*⁷ Bij de bescherming van objecten moet het militaire voordeel ‘duidelijk’ zijn wat inhoudt dat *“it is not legitimate to launch an attack which only offers potential or indeterminate advantages.”*⁸ Hoewel beide termen *“are roughly equivalent”*,⁹ wordt de lat voor militair voordeel bij ‘tastbaar en rechtstreeks’ net iets hoger gelegd dan bij ‘duidelijk’.¹⁰ Dit bevestigt mijn eerdere constatering dat verschil bestaat tussen de bescherming van personen en objecten die mogelijk te verklaren is doordat het grondbeginsel humaniteit meer gewicht in de schaal legt bij personen dan bij objecten.¹¹

Bij militaire cyberoperaties beneden de grens van aanval zal de inbreuk op het grondbeginsel humaniteit kleiner zijn, er vallen immers geen doden of gewonden noch worden burgerobjecten fysiek beschadigd. Als ik bovengenoemde redenering doorzet betekent dit dat het te behalen militair voordeel ook aan minder stringente eisen zal hoeven te voldoen dan bij een aanval, maar nog steeds aanwezig moet zijn. Door te kiezen voor het bijvoeglijk naamwoord ‘merkbaar’ geef ik aan dat het om een benoembaar militair voordeel moet gaan, een hypothetisch militair voordeel voldoet niet. Door het weglaten van de kwalificatie ‘rechtstreeks’ geef ik aan dat het militaire voordeel verder verwijderd

5 Zie bijv. DoD law of War Manual 2016, p. 1022. *“Nonetheless, such operations [that are not considered attacks] must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary.”*

6 Aanvullend Protocol I art. 51 lid 5 (b): *“aanvallen die, naar kan worden verwacht bijkomend verlies van mensenlevens onder de burgerbevolking, verwonding van burgers, schade aan burgerobjecten of een combinatie daarvan ten gevolge zullen hebben, in een mate die buitensporig zou zijn in verhouding tot het verwachte tastbare en rechtstreekse militaire voordeel”*, respectievelijk Aanvullend Protocol I art. 52 lid 2: *“Aanvallen dienen strikt tot militaire doelen te worden beperkt. Voor zover het objecten betreft, zijn militaire doelen uitsluitend die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel oplevert,”* mijn accentuering.

7 Sandoz, Swinarski & Zimmermann 1987, p. 684. In dezelfde zin Bothe, Partch & Solf 1982 p. 326.

8 Sandoz, Swinarski & Zimmermann 1987, p. 636.

9 Bothe, Partch & Solf 2013 p. 407.

10 Sandoz, Swinarski & Zimmermann 1987, p. 685, *“it should be noted that the words “concrete and direct” impose stricter conditions on the attacker than those implied by the criteria defining in Article 52 (General protection of civilian objects), paragraph 2.”* In dezelfde zin Bothe, Partch & Solf 2013 p. 407, *“Taken together the two words of limitation [concrete and direct] raise the standard set by art. 52.”*

11 Zie Hoofdstuk 3 par. 3.3.3.4.1.

mag liggen van de militaire operatie dan bij een aanval, bijvoorbeeld doordat het langer duurt voordat het militaire voordeel zich aandient.

Dat deze redenering verdedigbaar is, wordt duidelijk als hij wordt toegepast op andere militaire operaties beneden de drempel van aanval. Neem bijvoorbeeld “*non-violent recourse to psychological warfare*.”¹² Het zal niet eenvoudig, en misschien onmogelijk, zijn hiervoor de hoge standaard van ‘tastbaar en rechtstreeks’ militair voordeel aan te tonen. Door alleen de standaard ‘merkbaar’ te hanteren kunnen ook de zeker aanwezige, maar minder directe en langere termijn effecten, meegenomen worden en wordt daarmee voldaan aan het grondbeginsel van militaire noodzaak zodat deze methode van oorlogvoering geoorloofd is.¹³

Het grondbeginsel van militaire noodzaak is onverkort van toepassing beneden de drempel van aanval als er, op basis van het grondbeginsel van onderscheid, negatieve gevolgen voor burgers of burgerobjecten voorzienbaar zijn. Voor militaire cyberoperaties beneden de drempel van ‘aanval’ betekent dit dat er een merkbaar militair voordeel te verwachten moet zijn. Bij de bepaling van de balans tussen de militaire noodzaak en humaniteit worden bij militaire cyberoperaties beneden de drempel van aanval minder stringente eisen gesteld aan het te verwachten militaire voordeel dan bij aanvallen.

5.3 Humaniteit

Humaniteit als grondbeginsel is terug te vinden in vrijwel het gehele humanitair oorlogsrecht en is daarmee van toepassing op alle militaire operaties, ook die beneden de drempel van aanval.¹⁴ Hoe dit uitwerkt voor cyberoperaties beneden de grens van aanval wordt ingevuld door de toepassing van de andere grondbeginselen.¹⁵ Net als in Hoofdstuk 3 zal ik hier een beginsel dat rechtstreeks voortvloeit uit het grondbeginsel humaniteit, namelijk het beginsel van beperking, bespreken en wel aan de hand van de regel dat de keuze van methoden en middelen van oorlogvoering niet onbegrensd is en de regel dat het veroorzaken van overbodig letsel en onnodig leed verboden is.

5.3.1 De keuze van methoden en middelen van oorlogvoering is niet onbegrensd

De plaats en het woordgebruik van de regel, zoals vastgelegd in artikel 35 Aanvullend Protocol I, rechtvaardigt de conclusie dat deze regel algemene gelding heeft binnen het humanitair oorlogsrecht en derhalve ook van kracht is op operaties beneden de drempel van aanval.¹⁶ Voor de toepassing op cyberoperaties beneden de drempel van aanval is deze conclusie van grote invloed.

12 Zie Hoofdstuk 2 par. 2.6.2.

13 Zie bijv. Dinstein 2016, p. 275.

14 Zie Hoofdstuk 3 par. 3.3.2.

15 Zie bijv. DoD law of War Manual 2016, p. 1014. “under the principle of humanity, suffering, injury or destruction unnecessary to accomplish a legitimate military purpose must be avoided in cyber operations.”

16 Zie Hoofdstuk 3 par. 3.3.2.1.

De Tallinn Manual beschrijft *Cyber means of warfare* als “any cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to conduct a cyber attack”¹⁷ wat inhoud dat genoemde middelen “capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects”¹⁸ moeten zijn. “Methods of warfare refers to how cyber operations are mounted, as distinct from the instruments to conduct them.”¹⁹ Zo toegepast zullen de cybermethodes en -middelen van oorlogvoering leiden tot de kwalificatie van aanval en kunnen dus voor dit onderzoek verder buiten beschouwing gelaten worden.

Er bestaan echter ook cyberoperaties die bovenstaande drempel niet halen en toch gezien moeten worden als methode van oorlogvoering.²⁰ Deze cyberoperaties “can be highly useful militarily without generating destructive or injurious effects”.²¹ Tegelijkertijd kunnen deze cyberoperaties “a severe effect on the targeted object by disrupting its functioning, but without causing the physical damage to the object that would occur in traditional warfare”²² hebben. Op dit soort cyberoperaties is de regel dat de middelen en methoden van oorlogvoering niet onbegrensd zijn ook van toepassing, maar wat houdt deze begrenzing dan in? Wat is nog wel toegestaan en wat niet meer?

In een andere context,²³ geeft de Adviesraad Internationale Vraagstukken/Commissie van Advies Inzake Volkenrechtelijke Vraagstukken een voorbeeld van een ernstige maatschappelijke ontwrichting zonder dat sprake is van fysieke schade. Dit is het geval bij “een gecoördineerde aanval op het computernetwerk van het financiële systeem als geheel of op een aanzienlijk deel daarvan, die zou (kunnen) leiden tot langdurige en grootschalige ontwrichting en instabiliteit die niet eenvoudig met behulp van reguliere computerbeveiligingssystemen kan worden afgewend of beperkt.”²⁴ In het advies worden de bestaande volkenrechtelijke regels inzake het gebruik van geweld strikt toegepast op digitale aanvallen. De Nederlandse regering heeft dit advies in grote lijnen overgenomen.²⁵

Of het hierboven gegeven voorbeeld, als het plaats zou vinden binnen een gewapend conflict, wel of geen legitieme methode van oorlogvoering is, zal primair afhangen van de positie die wordt ingenomen in het hiervoor behandelde debat over het wel of niet kwalificeren als aanval van een militaire operatie zonder fysieke gevolgen.²⁶ Aanhangers

17 Schmitt 2013, p. 142.

18 Schmitt 2013, p. 141.

19 Schmitt 2013, p. 142.

20 Schmitt 2013, p. 142, noemt als voorbeeld, “a particular type of cyber operations designed to interfere with the enemy’s capability to communicate may not qualify as an attack (as that term is used in this Manual) but would constitute a method of warfare.”

21 Schmitt 2014b, p. 294.

22 Droege 2012, p. 552.

23 AIV/CAVV Advies Digitale Oorlogvoering, p. 24. De context is of pure cyberoperaties, die niet plaatsvinden in combinatie met conventionele vormen van oorlogvoering, van voldoende ernst kunnen zijn om de drempel van een gewapend conflict te overschrijden.

24 AIV/CAVV Advies Digitale Oorlogvoering, p. 24.

25 Kamerstukken II 2011-2012 33000 X 79, p. 5.

26 Hoofdstuk 4 par. 4.5.3. Dit debat is door Harrison-Dinniss aangeduid als het Schmitt-Dörmann debat.

van de restrictieve benadering zullen de operatie duiden als een aanval die aan de voorwaarden van artikel 52 Aanvullend Protocol I moet voldoen²⁷ om legitiem te kunnen zijn. Aanhangers van de permissieve benadering, waartoe ik mijzelf reken,²⁸ zullen de lat lager leggen, maar zoals ik al eerder betoogde bestaat de lat, in de vorm van bescherming door het humanitair oorlogsrecht, ook beneden de grens van aanval. Allereerst is er het hiervoor behandelde grondbeginsel van militaire noodzaak waaraan voldaan moet worden. Ten tweede zijn, op basis van de regel dat de methoden en middelen van oorlogvoering niet onbegrensd zijn, niet alle militaire (cyber-)operaties beneden de drempel van aanval toegestaan. Hoe de afweging uitvalt hangt af van *“finding the appropriate balance between military necessity and humanitarian concerns in the light of the nature of present day conflict and the values that states wish to protect.”*²⁹

Deze afweging vertoont een overkomst met de proportionaliteitstest uit bijvoorbeeld artikel 51 lid 5(b) en artikel 52 lid 2 van Aanvullend Protocol I waarbij respectievelijk de burgerbevolking en burgerobjecten beschermd worden tegen overmatig militair geweldgebruik. Doordat minder inbreuk wordt gemaakt op het grondbeginsel van humaniteit bij militaire cyberoperaties die beneden de drempel van aanval blijven, zal de balans al bij een geringer militair voordeel gevonden kunnen worden. Ik zou de afweging als volgt willen formuleren: de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan, mogen niet buitensporig zijn in verhouding tot het te verwachten merkbare militaire voordeel van de operatie.³⁰

De formulering van bovenstaande afweging naar analogie van de proportionaliteitstest uit art 51 lid 5(b) en artikel 52 lid 2 heeft als voordeel dat deze afweging aansluit bij een afweging die al bekend is en waarmee militairen en andere besluitvormers ervaring zullen hebben. De manier waarop de afweging gemaakt moet worden, rechtvaardigt de analogie. Zo zijn er net zo min als voor de proportionaliteitstest “abstracte wetmatigheden”³¹ waarmee de uitkomst kan worden bepaald, en zal ook de uitkomst van bovenstaande afweging afhangen van de concrete omstandigheden van het geval. Dat deze afweging een lastige kan zijn, is niet uniek, dat is de proportionaliteitstest ook.³² Dat de uitkomst mede

27 Het financiële systeem moet te beschouwen zijn als object dat naar zijn aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage levert aan de krijgsv verrichtingen en gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking moet, onder de omstandigheden van dat moment, een duidelijk militair voordeel opleveren.

28 Zie Hoofdstuk 4 par. 4.4.3.2.

29 Schmitt 2014b, p. 295.

30 Om te profiteren van de bekendheid van de proportionaliteitsregel, en de manier waarop deze moet worden toegepast, heb ik voor deze analoge manier van formuleren gekozen. Door een lagere eis te stellen aan het te verwachten militaire voordeel, maar gelijke bewoordingen te gebruiken voor de verhouding met de negatieve gevolgen, geef ik aan dat de bescherming tegen de negatieve gevolgen maximaal dezelfde is als bij aanval maar ook minder kan zijn. De bescherming kan echter nooit meer zijn.

31 Ducheine & Pouw 2010, p. 115. Zie ook Hoofdstuk 2 par. 3.2.

32 Zie bijvoorbeeld Sandoz, Swinarski & Zimmermann 1987, p. 684.

berust op het subjectieve oordeel van een commandant deelt de afweging eveneens met de proportionaliteitstest.³³

Juridisch gezien ontbreekt het bij bovenstaande afweging aan een specifieke codificatie die de proportionaliteitsregel wel kent. De juridische verplichting van deze laatste regel wordt nog extra benadrukt doordat overtreding ervan is aangemerkt als een “ernstige inbreuk” (*grave breach*)³⁴ van het humanitair oorlogsrecht. Ondanks het ontbreken van een dergelijke expliciete codificering concludeer ik toch, op basis van de volgende redenering, dat een juridische verplichting bestaat om in voorkomend geval de afweging tussen militair voordeel en humaniteit ook bij militaire operaties beneden de drempel van aanval te moeten maken.

De grondbeginselen van het humanitair oorlogsrecht kunnen worden gezien als “erkende algemene rechtsbeginselen”³⁵ en de Martens Clause bepaalt dat bij gebrek aan specifieke verdragen of overeenkomsten “burgers en combattanten beschermd [blijven] door en onderworpen [blijven] aan de beginselen van het volkenrecht die voortvloeien uit de gevestigde gebruiken, de beginselen van menselijkheid en de eisen van het openbare rechtsbewustzijn.”³⁶ Er bestaat geen specifieke regel voor militaire operaties beneden de drempel van aanval, maar een van de grondregels voor methoden en middelen van oorlogvoering geeft weer dat de methoden en middelen niet onbegrensd zijn.³⁷ Zoals hiervoor aangegeven zijn cyberoperaties beneden de drempel van aanval te kwalificeren als methode van oorlogvoering³⁸ en dus niet onbegrensd. Bovenbeschreven afweging geeft dan de uitwerking van de grens uit artikel 35 Aanvullend Protocol I die berust op de grondbeginselen van militaire noodzaak, humaniteit en onderscheid.³⁹ Gelet op de gewoonterechtelijke verplichting om het humanitair oorlogsrecht na te leven,⁴⁰ kan ik concluderen dat hieruit de juridische verplichting volgt om, in voorkomend geval, de genoemde afweging te moeten maken.⁴¹

De afweging tussen militaire noodzaak en humaniteit beneden de grens van aanval, zoals hierboven geformuleerd, is tevens een methode om de ‘permissieve’ en ‘restrictieve’ benadering van aanval met betrekking tot cyberoperaties te verenigen. De negatieve gevolgen op de burgerbevolking van militaire cyberoperaties beneden de grens van aanval worden meegewogen, terwijl deze militaire cyberoperaties niet gelijkgeschakeld worden

33 Bothe, Partch & Solf 2013, p. 351, “most decisions on the major political, economic, and social affairs of societies as well as major military decisions rest on the subjective judgment of decision makers based on the weighing of factors which cannot be quantified.”

34 Aanvullend Protocol I art. 85 lid 3 (b).

35 Bothe, Partch & Solf 2013 p. 43 “They are general principles of in the sense of Art. 38 of the Statute of the ICJ”

36 Aanvullend Protocol I art. 1 lid 2.

37 Aanvullend Protocol I art. 35 lid 1: “In geen enkel gewapend conflict is het recht van de partijen bij het conflict ten aanzien van de keuze der methoden of middelen van oorlogvoering onbegrensd.”

38 Schmitt 2013, p. 142

39 Het grondbeginsel van onderscheid komt in het vervolg van dit hoofdstuk nog separaat aan bod.

40 Henckarts & Doswald-Beck 2005, Chapter 40 *Compliance with international humanitarian law*, p. 495.

41 De juridische verplichting is wel minder dan bij de proportionaliteitstest in de zin dat niet of onvoldoende toepassen van deze afweging geen “ernstige inbreuk” op het humanitair oorlogsrecht zal opleveren, maar het levert wel een inbreuk op.

met aanvallen en dus ook niet gebonden zijn aan de strengere regels uit het humanitair oorlogsrecht die specifiek gelden voor aanvallen.

Waar in het geval van bovenstaande afweging tussen militaire noodzaak en humaniteit bij militaire cyberoperaties beneden de drempel van aanval de uitkomst komt te liggen, zal afhangen van alle omstandigheden van het geval en van de manier en het tempo waarin de “*humanisation of IHL*”⁴² wel of niet doorzet. Dat is net zo onvoorspelbaar als de toekomst. Resultaten uit het verleden bieden geen garantie voor de toekomst.⁴³ Het grote voordeel van de afweging is dat zij niet geheel nieuw is omdat wordt aangesloten, in bewoordingen en manier van uitvoering, bij de bekende proportionaliteitstest voor aanvallen.

5.3.2 Veroorzaken van overbodig letsel of onnodig leed is verboden

De regel dat het veroorzaken van overbodig letsel en onnodig leed verboden is, geldt ook beneden de drempel van aanval.⁴⁴ Ik roep echter in herinnering dat deze regel bedoeld is om de uitwerking van wapens, wapensystemen en methoden van oorlogvoering te beoordelen en niet om in individuele gevallen nog een afweging te maken tussen militair voordeel en leed of letsel analoog aan de proportionaliteitstest.⁴⁵ Fysiek letsel valt buiten het bereik van dit onderzoek en bij geestelijk leed zou vastgesteld moeten worden dat de doelstelling van een bepaalde methode van oorlogvoering gericht is op het veroorzaken van onnodig leed. Maar hoe onderscheidt het leed van een cyberoperatie zich van het algemene geestelijke leed dat een gewapend conflict sowieso veroorzaakt? Vervolgens is het onvoorspelbaar of het toegevoegde leed in de toekomst wel of niet zal leiden tot klachten.⁴⁶ Neem dit alles tezamen en het zal duidelijk zijn dat deze regel weliswaar van kracht is, maar, zeker bij cyberoperaties beneden de drempel van aanval, in praktische zin geen beperkingen op zal leggen.

5.4 Onderscheid

5.4.1 Het grondbeginsel van onderscheid

Zoals hiervoor al aangegeven volg ik in dit hoofdstuk de structuur van Hoofdstuk 3, waarbij ik de uitkomsten uit dat hoofdstuk zal projecteren op cyberoperaties. Voor deze paragraaf betekent dit dat ik over het algemeen kort kan zijn als de uitkomsten één op één toegepast kunnen worden op cyberoperaties en geen aanleiding geven voor specifieke bijzonderheden.⁴⁷ Dit is bijvoorbeeld het geval met het grondbeginsel van onderscheid

■
42 Kolb 2013, p. 52. Zie ook Hoofdstuk 2 par. 2.3.2.

43 Vrij naar de verplichte mededeling van de Reclame Code Commissie bij reclames voor financiële beleggingsproducten.

44 Zie Hoofdstuk 3 par. 3.3.2.2.

45 Zie Hoofdstuk 3 par. 3.3.2.2.

46 Zo is het ontstaan van een Post Traumatisch Stress Stoornis mede afhankelijk van persoonlijkheidskenmerken en omgevingsfactoren.

47 In Hoofdstuk 3 was er een subparagraaf ‘objecten en onbruikbaarmaking’. Deze onderwerpen zijn al besproken in Hoofdstuk 4 onder respectievelijk de status van virtuele elementen in het humanitair oorlogsrecht en schade aan virtuele elementen en zij keren dus niet terug in deze paragraaf.

in het algemeen. In Hoofdstuk 2 heb ik vastgesteld dat ‘militaire operaties’ een breder begrip betreft dan ‘aanvallen’ zoals gedefinieerd in artikel 49 Aanvullend Protocol I en in Hoofdstuk 3 heb ik vastgesteld dat het grondbeginsel van onderscheid geldt voor *alle* militaire operaties⁴⁸ en daarmee ook voor militaire cyberoperaties beneden de drempel van aanval.

Voordat ik de vraag beantwoord hoe dit uitwerkt voor deze cyberoperaties, aan de hand van de traditionele dichotomie van onderscheid binnen het humanitair oorlogsrecht, in de subparagrafen 5.4.3 voor personen en 5.4.4 voor objecten, zal ik in 5.4.2 allereerst dieper ingaan op de term ‘ontzien en beschermd’, omdat deze term betekenis heeft voor zowel personen als objecten. Als laatste onderwerp bij het grondbeginsel onderscheid zal ik in subparagraaf 5.4.5 het onderwerp voorbereiding bespreken.

5.4.2 ‘Ontzien en beschermd’

De bescherming van personen, instanties en objecten die bedoeld zijn om in een gewapend conflict humanitaire hulp te verlenen, en in het geval van gewonden, zieken en schipbreukelingen te ontvangen,⁴⁹ gaat verder dan alleen bescherming tegen aanvallen.⁵⁰ De term ‘ontzien en beschermd’ wijst op deze bredere bescherming en levert ook bescherming tegen militaire operaties beneden de drempel van aanval, indien deze operaties gericht zijn tegen het humanitair optreden of functioneren, of dit optreden of functioneren negatief beïnvloeden.⁵¹

Deze conclusie heeft zeker gevolgen voor planning, voorbereiding en uitvoering van militaire cyberoperaties. Het verbod op cyberoperaties gericht tegen het humanitair optreden of functioneren zal hierbij nog de minste problemen opleveren. Deze personen, instanties noch hun materieel mogen nimmer het doel van een militaire operatie vormen, niet van een aanval en niet van een cyberoperatie beneden de drempel van aanval.

Lastiger zal het zijn te beoordelen of een militaire cyberoperatie beneden de drempel van aanval het humanitair optreden of functioneren negatief zal beïnvloeden. Moet het verbod absoluut worden uitgelegd, of geldt ook hier een *de minimis* voordat de beïnvloeding onder het verbod valt?⁵² Een analogie met de schade als gevolg van ‘cyber-aanvallen’ ligt hier voor de hand, zodat *de minimis*-verstoring van het humanitair optreden of functioneren niet leidt tot een overtreding van het verbod. De hoogte van de *de minimis*- drempel zal afhangen van de omstandigheden van het geval maar zal, gelet op de specifieke bescherming die de term ‘ontzien en beschermd’ biedt, niet al te hoog liggen, omdat dan deze extra bescherming een lege huls zou blijken te zijn. Een voorbeeld ter verduidelijking.

48 Hoofdstuk 3 par.3.3.3. Uiteraard geldt dit alleen voor militaire operaties binnen het paradigma van oorlogvoering dus de militaire operaties waarop het humanitair oorlogsrecht van kracht is.

49 Geneefse Conventie I art 12 en II art. 12, Aanvullend Protocol I art.10.

50 Zie Hoofdstuk 3 par. 3.3.3.2.

51 Zie Hoofdstuk 3 par. 3.3.3.2.

52 Zie Schmitt 2013, p. 107.

Als door een cyberoperatie de elektriciteitsvoorziening onderbroken wordt en hierdoor moet een ziekenhuis tijdelijk de deuren sluiten of behandelingen uitstellen, dan is dit te kwalificeren als negatief beïnvloeden van het humanitair optreden.⁵³ Schakelt als gevolg van dezelfde cyberoperatie het ziekenhuis over op een noodstroomstelsel waardoor de gezondheidszorg voor minder dan een seconde onderbroken wordt, zal de *de minimis* drempel niet overschreden zijn.

Bovenstaand voorbeeld maakt duidelijk dat de bescherming die de term ‘ontzien en beschermd’ biedt, de lat voor de partij die een militaire cyberoperatie uit wil voeren of uitvoert extra hoog legt, al blijft er ruimte voor grensgevallen.⁵⁴ Ik kom in de subparagraaf ‘voorbereiding’ terug op hoe de verhoogde bescherming vorm krijgt.

5.4.3 Personen

5.4.3.1 Burgerbevolking en afzonderlijke burgers, algemene bescherming

Op basis van het grondbeginsel van onderscheid worden de burgerbevolking en de afzonderlijke burgers beschermd tegen aanvallen en de fysieke gevaren die voortvloeien uit militaire operaties beneden de drempel van aanval.⁵⁵ Militaire cyberoperaties beneden de grens van aanval mogen, zolang ze geen fysieke gevaren veroorzaken, gericht zijn op burgers.⁵⁶ Dit is een van de belangrijke twistpunten uit de discussie over de permissieve versus de restrictieve benadering van aanval.⁵⁷ Zonder de discussie te herhalen, roep ik in herinnering mijn conclusie dat het humanitair oorlogsrecht ook beneden de grens van aanval een beschermende werking heeft. Dat op basis van het grondbeginsel van onderscheid militaire operaties beneden de grens van aanval gericht mogen zijn op burgers, betekent namelijk nog niet dat *alle* militaire operaties beneden de grens van aanval zijn toegestaan. De beperkingen zijn echter mede gebaseerd op andere grondbeginselen uit het humanitair oorlogsrecht.⁵⁸

5.4.3.2 Personen met bijzonder bescherming

De indeling in groepen van personen die ik heb aangebracht in Hoofdstuk 3 gebruik ik ook hier. Personen met alleen bescherming tegen aanval, te weten parachutisten uit een vliegtuig in nood (met uitzondering van luchtlandingseenheden),⁵⁹ personen *hors de*

53 Let wel, indien door de elektriciteitsuitval bijvoorbeeld een hart-longmachine uitvalt (bijvoorbeeld omdat het ziekenhuis geen back-up systeem voor elektriciteitsvoorziening heeft) waardoor een patiënt overlijdt zou de cyberoperatie, als deze gevolgen voorzienbaar zijn, vanwege de gevolgen waarschijnlijk kwalificeren als aanval.

54 Een specifiek voorbeeld wordt gegeven in de *Tallinn Manual*, p 205, waar wordt opgemerkt dat de blokkering van een online uitzending van een religieuze dienst voor troepen verboden is, gevolgd door “*It must be cautioned that the Rule does not extend to situations that occur only incidentally, as in the case of the overall blocking of enemy communications.*”

55 Zie Hoofdstuk 3 par. 3.3.3.3.1.

56 Zie bijv. DoD Law of War Manual 2016, p. 1022. “*Since such operations generally would not be considered attacks under the law of war, they generally would not need to be directed at military objectives, and may be directed at civilians and civilian objects.*”

57 Zie Hoofdstuk 4 par. 4.5.3.

58 Militaire noodzaak in combinatie met onderscheid, zie hiervoor par. 5.2 en de afweging militaire noodzaak versus humanitaire overwegingen, zie hiervoor par. 5.3.1.

59 Aanvullend Protocol I art. 42.

*combat*⁶⁰ (tenzij de buitengevechtstelling het gevolg is van verwonding of ziekte waardoor deze personen ‘ontzien en beschermd’ moeten worden) en parlementairen,⁶¹ hoef ik hier niet verder te bespreken, omdat ze niet beschermd worden tegen cyberoperaties beneden de drempel van aanval.

Vrouwen,⁶² kinderen⁶³ en journalisten⁶⁴ vallen onder dezelfde bescherming tegen cyberoperaties beneden de drempel van aanval⁶⁵ als de hiervoor behandelde burgerbevolking en afzonderlijke burgers in het algemeen, terwijl voor personen met extra bescherming geldt wat hiervoor is besproken onder de term ‘ontzien en beschermd’.

Een laatste opmerking over de uitwerking van het grondbeginsel van onderscheid in relatie tot personen is een herhaling van wat ik eerder in Hoofdstuk 4 opmerkte over cyberidentiteiten. De virtuele componenten van het cyberdomein, en daarmee ook cyberidentiteiten, voldoen niet aan de kwalificatie personen.⁶⁶ Ondanks de komst van mens-machine interfaces die in de (nabije) toekomst herwaardering van de traditionele dichotomie binnen het humanitair oorlogsrecht mogelijk noodzakelijk maken, zal ik cyberidentiteiten behandelen als objecten in de volgende sub-paragraaf.

5.4.4 Objecten

5.4.4.1 Burgerobjecten; algemene bescherming

In Hoofdstuk 3 concludeerde ik dat burgerobjecten, in tegenstelling tot burgers, alleen beschermd zijn tegen aanvallen en gebruikt mogen worden voor militaire operaties beneden de drempel van aanval.⁶⁷ Dit heeft een aantal consequenties voor militaire cyberoperaties beneden de drempel van aanval. Niet alleen mogen burgerobjecten het doel van een dergelijke operatie vormen,⁶⁸ ze mogen hiervoor ook gebruikt worden.⁶⁹ Dit laatste is specifiek van belang omdat ik in Hoofdstuk 4 concludeerde dat de virtuele componenten van het cyberdomein binnen het humanitair oorlogsrecht inmiddels aangemerkt kunnen worden als objecten.⁷⁰ Virtuele componenten van het cyberdomein mogen derhalve niet alleen het doel van militaire cyberoperaties beneden de drempel van aanval zijn, ze mogen hiervoor ook gebruikt worden. Let wel, deze conclusie is slechts geldig op basis van

60 Aanvullend Protocol I art. 41.

61 Haags Verdrag IV(1907) art. 32.

62 Aanvullend Protocol I art. 76.

63 Aanvullend Protocol I art. 77.

64 Aanvullend Protocol I art. 79.

65 Zie Hoofdstuk 3 par. 3.3.3.4.

66 Zie Hoofdstuk 4 par. 4.5.3.2.

67 Zie Hoofdstuk 3 par. 3.3.3.4.1

68 Voor eenzelfde conclusie zie bijv. DoD Law of War Manual 2016, p. 1022. “Since such operations generally would not be considered attacks under the law of war, they generally would not need to be directed at military objectives, and may be directed at civilians and civilian objects.”

69 Zie Hoofdstuk 3 par. 3.3.3.4.1.

70 Hoofdstuk 4 par. 4.4.3.4.

alléén het grondbeginsel van onderscheid. Voor de *overall* juridische toelaatbaarheid van cyberoperaties beneden de drempel van aanval binnen het humanitair oorlogsrecht mag een cyberoperatie niet conflicteren met een van de andere grondbeginselen. De hiervoor beschreven afweging tussen militaire noodzaak en humaniteit⁷¹ biedt hiervoor een praktisch uitvoerbaar handvat.

5.4.4.2 Burgerobjecten; bijzondere bescherming

De eerste categorie die ik bespreek zijn burgerobjecten met een relatief verhoogde bescherming tegen aanval. Deze burgerobjecten kunnen onder voorwaarden nog steeds aangevallen worden, maar de voorwaarden voor het verlies van bescherming liggen hoger dan bij ‘gewone’ burgerobjecten.⁷² Wat betekent dit voor cyberoperaties beneden de drempel van aanval? Neem als voorbeeld ‘werken en installaties die gevaarlijke krachten bevatten.’⁷³ Dit soort werken wordt vaak gecontroleerd door middel van *Supervisory Control and Data Acquisition (SCADA) software*.⁷⁴ De mogelijkheid dat fysieke schade ontstaat door manipulatie van de SCADA software is reëel.⁷⁵ Wanneer een militaire cyberoperatie echter deze fysieke gevolgen heeft, is de drempel van aanval gepasseerd en is de operatie niet langer een militaire operatie beneden de drempel van aanval maar een aanval. Met andere woorden: de relatief verhoogde bescherming tegen aanval heeft geen effect op militaire cyberoperaties beneden de drempel van aanval.

Toch maakt bovenstaande redenering wel iets anders duidelijk. Om te bepalen of een militaire operatie een aanval vormt, moet gekeken worden naar de fysieke schade die ontstaat, of die voorzienbaar kan ontstaan, als gevolg van de operatie.⁷⁶ Met name de schade die voorzienbaar kan ontstaan verdient bij militaire cyberoperaties bijzondere aandacht. Ik kom hier in de subparagraaf ‘voorbereiding’ op terug.

De tweede categorie burgerobjecten met bijzondere bescherming is de categorie culturele goederen. Daar waar burgerobjecten niet beschermd worden tegen militaire operaties beneden de drempel van aanval, ligt de beschermende lat van het humanitair oorlogsrecht hoger voor culturele goederen. Voor culturele goederen geldt dat ze niet gebruikt mogen worden “ter ondersteuning van de militaire inspanning”⁷⁷ omdat de partijen bij het gewapend conflict daarmee deze goederen “aan vernietiging of beschadiging zouden kunnen blootstellen in geval van een gewapend conflict.”⁷⁸ Alhoewel deze bescherming

■
71 Zie par. 5.3.1.

72 Zie Hoofdstuk 3 par. 3.3.3.4.2.

73 Aanvullend Protocol I art. 56.

74 Zie Hoofdstuk 4 par. 4.2.2.2.

75 Zie Hoofdstuk 4 par. 4.4.4.3.2.

76 Zie Hoofdstuk 4 par. 4.4.5.4.

77 Aanvullend Protocol I art 53(b). Militaire inspanning betekent hier: “All military activities connected with the conduct of a war.” Sandoz, Swinarski & Zimmermann 1987, p. 648.

78 Verdrag inzake de bescherming van culturele goederen 1954, art. 4 lid 1.

niet absoluut is,⁷⁹ is het interessant te bezien hoe deze bescherming uitwerkt bij militaire cyberoperaties beneden de drempel van aanval.

Twee vragen rijzen bij militaire cyberoperaties beneden de drempel van aanval in relatie tot culturele goederen. Kunnen virtuele componenten van het cyberdomein, en dan met name computergegevens, culturele goederen zijn? Hierbij valt te denken aan bijvoorbeeld een digitale film van een culturele gebeurtenis, zoals de kroning van koning Willem-Alexander in 2013, of een digitale reproductie van een fysiek cultureel object als het amfitheater in Palmyra in Syrië nadat het fysieke object werd vernietigd door Islamitische Staat begin 2017.

Als de vraag of virtuele componenten culturele goederen kunnen zijn bevestigend wordt beantwoord, hoe ver reikt in dat geval de verhoogde bescherming? Deze twee vragen vertonen een gelijkenis met de vragen over de status van en schade aan virtuele componenten in het humanitair oorlogsrecht.⁸⁰ Ik zal beide vragen bespreken aan de hand van de regel over culturele goederen zoals geformuleerd in de *Tallinn Manual*, die zegt dat “*The parties to an armed conflict must respect and protect cultural property that may be effected by cyber operations or that is located in cyberspace. In particular, they are prohibited from using digital cultural property for military purposes.*”⁸¹

Een tekstuele opmerking vooraf. De *Tallinn Manual* gebruikt de term ‘*respect and protect*’ refererend aan de 1954 *Hague Cultural Property Convention*.⁸² Echter noch de 1954 *Hague Cultural Property Convention*,⁸³ noch Aanvullend Protocol I, dat de bepalingen van de 1954 *Hague Cultural Property Convention* bevestigt,⁸⁴ gebruiken deze term voor culturele goederen, zodat ik de term zoals gebruikt in de *Tallinn Manual* niet op dezelfde manier kan uitleggen als ‘ontzien en beschermd’ die ik hiervoor behandelde.

Ondanks het taalgebruik van *Black letter rule* 82 uit de *Tallinn Manual*, namelijk het verbod van het gebruik van *digital cultural property* voor militaire doeleinden, waren niet alle samenstellers van de *Tallinn Manual* het eens over de vraag of culturele goederen ‘*intangible*’ kunnen zijn. Sommige waren van mening dat, omdat zowel artikel 52⁸⁵ als artikel 53⁸⁶ van Aanvullend Protocol I spreken van ‘*objects*’, de uitleg in beide gevallen hetzelfde moest zijn. Omdat volgens de meerderheid van de *experts* ‘*object*’ in artikel 52 gelezen moet worden

79 Zie Hoofdstuk 4 par. 4.4.4.3.2. Als culturele goederen niet absoluut beschermd zijn tegen aanvallen zijn ze ook niet absoluut beschermd tegen militaire operaties beneden de drempel van aanval. Voor de redenering in deze subparagraaf over de bescherming van culturele goederen ga ik ervan uit dat geen sprake is van de uitzondering genoemd in art. 4 van de het Verdrag inzake de bescherming van culturele goederen 1954, zodat de bescherming niet is opgeheven.

80 De vraag uit respectievelijk par. 4.4.3.4 en 4.4.4 van Hoofdstuk 4.

81 Schmitt 2013, *Black letter rule* no. 82, p. 228.

82 Schmitt 2013, p. 228.

83 1954 *Hague Cultural Property Convention* art. 2: “*the protection of cultural property shall comprise the safeguarding of and respect for such property*”

84 Aanvullend Protocol I art. 53. “Onverminderd de bepalingen van het Verdrag van ‘s-Gravenhage inzake de bescherming van culturele goederen in geval van een gewapend conflict van 14 mei 1954”.

85 Art. 52 Aanvullend Protocol I handelt onder andere over de definitie van objecten als militair doel.

86 Art. 53 Aanvullend Protocol I culturele goederen (*cultural objects*)

als “*visible and tangible*”,⁸⁷ moet dit volgens enkele experts eveneens gelden voor artikel 53.⁸⁸ Anderen daarentegen haken aan bij het gebruik van de term ‘*property*’ uit *Black letter rule* 82 en het feit dat ‘*property*’ niet altijd beperkt wordt tot tastbare zaken. Zij verwijzen daarbij naar intellectueel eigendom dat als zodanig “*is well accepted in international law and that appears in most domestic legal systems*.”⁸⁹ De meningen waren verdeeld, maar uit het feit dat *digital cultural property* wel in de uiteindelijke *Black letter rule* is terechtgekomen, maak ik op dat een consensus onder de samenstellers bestond⁹⁰ dat culturele goederen ook digitaal kunnen zijn.

Voor mijn positie over de vraag of virtuele componenten culturele goederen kunnen zijn, verwijs ik naar mijn conclusie over de status van virtuele componenten uit Hoofdstuk 4. Mijn conclusie dat virtuele componenten inmiddels gezien kunnen worden als objecten binnen het humanitair oorlogsrecht,⁹¹ maakt dat ik, net als de samenstellers van de *Tallinn Manual*, virtuele componenten kan beschouwen als culturele goederen. Welke virtuele componenten daadwerkelijk aangemerkt kunnen worden als culturele goederen die de bescherming van artikel 53 Aanvullen Protocol I genieten hangt af van de definitie van culturele goederen.⁹² Zowel virtuele componenten als fysieke objecten moeten voldoen aan dezelfde definitie om te kwalificeren als culturele goederen.⁹³ De vraag wanneer dit precies het geval is, valt buiten het bereik van dit onderzoek.

Nu ik de vraag of virtuele componenten culturele goederen kunnen zijn positief beantwoord heb, kom ik toe aan de tweede vraag, namelijk hoe ver reikt de verhoogde bescherming van virtuele culturele goederen? In het kader van dit onderzoek bezie ik specifiek de verhoogde bescherming, namelijk niet alleen de bescherming tegen aanval, maar ook tegen militaire cyberoperaties beneden de drempel van aanval, die (virtuele) culturele goederen genieten.

De 1954 *Hague Cultural Property Convention* geeft aan dat partijen zich dienen te onthouden van “ieder gebruik van deze [culturele] goederen en van hun onmiddellijke omgeving of van de middelen voor hun bescherming voor doeleinden, welke deze goederen aan vernietiging

87 Schmitt 2013, p. 126.

88 Schmitt 2013, p. 229.

89 Schmitt 2013, p. 229.

90 Immers. “*The rules reflect consensus among the Experts as to the applicable lex lata.*” Schmitt 2013, p. 5.

91 Hoofdstuk 4 par. 4.4.3.5.

92 Zoals onder meer vastgelegd in artikel 1 van de 1954 *Hague Cultural Property Convention*. In maart 2018 waren 131 landen partij bij deze Conventie. Alhoewel nog niet universeel, worden “*the fundamental principals of protecting and preserving cultural property in the Convention... widely regarded as reflecting customary international law*” Henckaerts & Doswald-Beck 2005, p. 129.

93 Art. 1a van de 1954 *Hague Cultural Property Convention* luidt: “Voor de toepassing van dit Verdrag worden beschouwd als culturele goederen, welke ook hun oorsprong of wie ook hun eigenaar is: a roerende en onroerende goederen, welke van groot belang zijn voor het cultureel erfdeel van ieder volk, zoals monumenten van bouwkunst, kunst of geschiedenis, hetzij van godsdienstige, hetzij van wereldlijke aard; terreinen van oudheidkundig belang; groepen gebouwen, welke als een geheel, uit het oogpunt van kunst van belang zijn; kunstwerken; handschriften, boeken en andere voorwerpen, welke uit het oogpunt van kunst, geschiedenis of oudheidkunde van belang zijn, en voorts wetenschappelijke verzamelingen en belangrijke verzamelingen boeken, archiefbescheiden of afbeeldingen van de hierboven omschreven goederen.”

of beschadiging zouden kunnen blootstellen in geval van een gewapend conflict.⁹⁴ Om te bezien wat onder beschadiging van virtuele culturele goederen moet worden verstaan, is het goed te beseffen waarom de bescherming wordt toegekend. Dit is om te voorkomen dat culturele goederen verloren gaan voor de mensheid.⁹⁵ Daarom noemt artikel 1 van de *Convention* niet alleen allerlei zaken maar ook “*reproductions of the property defined above*”.⁹⁶ Dit levert voor sommige virtuele culturele goederen, zoals bijvoorbeeld de hierboven genoemde digitale film van de kroning van koning Willem-Alexander, een complicatie op. Digitale *reproductions* zijn heel snel, en tegen relatief lage kosten eenvoudig te vervaardigen. Zodra dit gebeurt, verliest een individuele kopie waarschijnlijk de verhoogde bescherming omdat deze bescherming is “*based on the value and irreplaceability of the original work of art, and on the difficulty, time and expense involved in reproducing faithful copies of that original*”.⁹⁷ Met andere woorden, het zal afhangen van de hoeveelheid digitale kopieën, en waarschijnlijk ook van de manier waarop en plaats waar deze bewaard worden, of een individuele digitale kopie nog aangemerkt kan worden als een cultureel goed en daardoor de bijbehorende verhoogde bescherming geniet.

Als onder schade aan virtuele culturele goederen vervolgens wordt verstaan “*any alteration, damage, deletion, or destruction of the data*”,⁹⁸ levert elke inbreuk op de *Confidentiality-Integrity-Availability* triade⁹⁹ een schending van de verhoogde bescherming van culturele goederen op. Het probleem bij virtuele culturele goederen is dan echter tot wanneer digitale kopieën van fysieke culturele goederen, of van digitale kopieën van digitale culturele goederen als deze vanaf het eerste moment digitaal waren, zelf ook nog blijven vallen onder de verhoogde bescherming van culturele goederen. Het antwoord op deze laatste vraag zal weer afhangen van de omstandigheden van het geval, maar zeker is dat het, net als bij de hiervoor besproken burgerobjecten met een relatief verhoogde bescherming tegen aanvallen, extra nadruk legt op de mogelijke voorzienbare gevolgen van een militaire cyberoperatie. Ik kom hier in de subparagraaf ‘voorbereiding’ op terug.

De derde groep van burgerobjecten met bijzondere bescherming zijn de burgerobjecten die beschermd worden door de term ‘ontzien en beschermd’. Hiervoor geldt onverkort hetgeen besproken is bij ‘ontzien en beschermd’. Deze goederen zijn beschermd tegen aanvallen en tegen alle andere militaire operaties gericht op het verstoren van het humanitair optreden of functioneren of dit humanitair optreden of functioneren negatief beïnvloeden.

De vierde en laatste categorie burgerobjecten die ik hier wil bespreken zijn de virtuele componenten van het cyberdomein. Omdat ik de groepen die hieronder vallen, firmware, besturingsprogramma’s, cyberidentiteiten, computerprogramma’s en computergegevens

94 1954 *Hague Cultural Property Convention* art. 4.

95 Woudenberg & Lijnzaad 2010, p. xi. “*the loss of a people’s cultural heritage is a loss for all humanity*.”

96 1953 *Hague Cultural Property Convention* art. 1a.

97 Schmitt 2013, p. 230.

98 Schmitt 2013, p. 230.

99 Zie Hoofdstuk 4 par. 4.4.3.

allemaal classificeer als objecten, volgen zij dezelfde regels als fysieke objecten. Om te bepalen of een virtuele component gezien moet worden als een burgerobject of een militair doel zal afhangen van de tweeledige test uit artikel 52 lid 2 Aanvullend Protocol 1. Als uit deze test blijkt dat het een burgerobject betreft moet vervolgens bezien worden of het een burgerobject is met alleen algemene bescherming, dat wil zeggen alleen tegen aanval, of behoort tot een van drie hiervoor besproken categorieën met een bijzondere bescherming waardoor deze virtuele componenten ook bescherming genieten tegen militaire operaties beneden de drempel van aanval.

5.4.5 Voorbereiding

In Hoofdstuk 3 concludeerde ik dat voorzorgsmaatregelen, zoals gecodificeerd in artikel 57 en 58 Aanvullend Protocol I niet gelden voor militaire operaties beneden de drempel van aanval omdat deze voorzorgsmaatregelen zijn gedefinieerd in termen van ‘aanval’.¹⁰⁰ Toch kan daarmee het onderwerp voorzorgsmaatregelen niet terzijde worden geschoven voor militaire cyberoperaties beneden de drempel van aanval. Om spraakverwarring met de aan ‘aanval’ gekoppelde term ‘voorzorgsmaatregelen’ te voorkomen zal ik in het vervolg de term ‘voorbereiding’ gebruiken als ik het heb over de voorbereiding van militaire operaties beneden de grens van aanval.

Het verschil tussen aanvallen en militaire operaties die geen aanval zijn, ligt in het fysieke letsel of de fysieke schade waarop de actie gericht is of die de actie veroorzaakt, waarbij de fysieke gevolgen voorzienbaar moeten zijn. Juist dit laatste legt een zware last op de voorbereiding van militaire cyberoperaties beneden de drempel van aanval. Uit de voorgaande beschrijving van het grondbeginsel onderscheid blijkt bijvoorbeeld dat in sommige gevallen burgers en burgerobjecten het doel van militaire cyberoperaties mogen zijn, mits deze beneden de grens van aanval blijven. Dezelfde personen of objecten mogen echter niet aangevallen worden. De consequentie hiervan is dat de militaire cyberoperatie beneden de grens van aanval die geoorloofd is, alsnog *kan* veranderen in een verboden aanval op het moment dat fysieke schade of letsel ontstaat en dit laatste voorzienbaar was. Om te garanderen dat de cyberoperatie geoorloofd is en blijft, dient bij de voorbereiding geborgd te worden dat geen (voorzienbare) fysieke gevolgen als gevolg van de operatie op gaan treden.

Hoe ver moet die voorbereiding gaan? Welke mogelijke gevolgen moeten nog worden meegenomen in een situatie van een gewapend conflict waar algemeen erkend is dat absolute zekerheid over de uitkomst van een militaire operatie niet bestaat? De onzekerheid die bestaat, vaak omschreven als de ‘fog of war’, moet zoveel mogelijk ingeperkt worden. Een analogie met artikel 57 en 58 Aanvullende Protocol I ligt hier voor de hand. Deze artikelen, die gerekend worden tot het gewoonterecht,¹⁰¹ beschrijven de voorzorgsmaatregelen die genomen moeten worden bij aanvallen¹⁰² en ter bescherming

■
¹⁰⁰ Zie Hoofdstuk 3 par. 3.3.3.5.

¹⁰¹ Henckaerts & Doswald-Beck 2005, *Black letter rule* 15-24.

¹⁰² Aanvullend Protocol I art. 57.

tegen de gevolgen van aanvallen.¹⁰³ Het is dan logisch eenzelfde maatstaf te hanteren om te voorkomen dat een geoorloofde militaire cyberoperatie alsnog kan veranderen in een (mogelijk) ongeoorloofde cyberaanval.

In zowel artikel 57 als 58 Aanvullend Protocol I wordt de standaard voor te nemen voorzorgsmaatregelen, die zowel gelden voordat een aanval wordt uitgevoerd,¹⁰⁴ als tijdens de uitvoering van een aanval,¹⁰⁵ bepaald op ‘praktisch uitvoerbaar’ (*feasible*). In de *Commentary* bij Aanvullend Protocol I wordt nader ingegaan op de term ‘praktisch uitvoerbaar’. Deze wordt gebruikt om uit te drukken “that no one can be required to do the impossible”¹⁰⁶ en dat de interpretatie “will be a matter of common sense and good faith”¹⁰⁷ waarbij “all the circumstances at the time, including those relevant to the success of military operations” moeten worden meegewogen.¹⁰⁸ ‘Praktisch uitvoerbaar’ houdt tevens een “continuing obligation to assign a high priority to the collection, collation, evaluation and dissemination of timely target intelligence” in.¹⁰⁹

Een analoge toepassing van de standaard ‘praktisch uitvoerbaar’ op militaire cyberoperaties beneden de grens van aanval, betekent dat zowel in de voorbereiding als tijdens de uitvoering alles gedaan moet worden wat ‘praktisch uitvoerbaar’ is om te voorkomen dat een dergelijke militaire cyberoperatie fysieke gevolgen heeft of kan hebben. Naast de aandacht voor de fysieke gevolgen moet in de voorbereiding en tijdens de uitvoering voorkomen worden dat militaire cyberoperaties gericht zijn op het humanitair optreden of functioneren van personen, instanties en objecten die ‘ontzien en beschermd’ moeten worden, of dat het humanitair optreden of functioneren negatief beïnvloed wordt. Daarnaast moet aandacht worden besteed aan de verhoogde bescherming van digitale culturele goederen.

Wat ‘praktisch uitvoerbaar’ is, zal aan de hand van de omstandigheden van het geval te goeder trouw en op basis van gezond verstand moeten worden vastgesteld. Zo zal in de voorbereiding het doel van de militaire cyberoperatie gedegen in kaart gebracht moeten worden. Dit is enerzijds nodig om de zwakheden en kwetsbaarheden van het doel te onderkennen zodat deze uitgebuit kunnen worden om de cyberoperatie uit te voeren. Anderzijds moeten ook de gevolgen van de cyberoperaties, zo goed als mogelijk, in kaart gebracht worden, zodat duidelijk is of wel of geen fysieke gevolgen te voorzien zijn. Indien te veel onzekerheden blijven bestaan is het misschien mogelijk een simulatie van de cyberoperatie uit te voeren in een afgeschermd omgeving, bijvoorbeeld een cyberlab om zo meer duidelijkheid te krijgen en mogelijk onvoorziene gevolgen te onderkennen.

■
103 Aanvullend Protocol I art. 58.

104 Aanvullend Protocol I art. 57 lid 2 (a) (i).

105 Aanvullend Protocol I art. 57 lid 2 (b).

106 Sandoz, Swinarski & Zimmermann 1987, p. 692.

107 Sandoz, Swinarski & Zimmermann 1987, p. 682.

108 Bothe, Partch & Solf 2013, p. 405.

109 Bothe, Partch & Solf 2013, p. 405.

Hoe ver ‘praktisch uitvoerbaar’ reikt zal afhangen van de beschikbare middelen,¹¹⁰ waarbij de factor tijd een belangrijke invloed heeft. Zo zal het in kaart brengen van het doel, zeker als dit gebeurt door het systeem met cybermiddelen binnen te dringen, het risico op detectie met zich mee kunnen brengen. Naarmate dit langer duurt kan het risico van ontdekking groter worden en daarmee de kans om de operatie vervolgens succesvol uit te voeren kleiner. Het optimum zal dan met gezond verstand en te goeder trouw bepaald moeten worden.

Als bij de voorbereiding of tijdens de uitvoering blijkt dat niet (langer) voldaan kan worden aan de hierboven vermelde voorwaarden zijn er twee mogelijkheden. De eerste optie is dat de militaire cyberoperatie niet wordt uitgevoerd of, als de operatie al aan de gang is, wordt beëindigd. De tweede optie is dat de militaire cyberoperatie niet langer gezien mag worden als een cyberoperatie beneden de grens van aanval en in het vervolg dus beoordeeld moet worden aan de hand van de regels die gelden voor aanval in de zin van artikel 49 Aanvullend Protocol I.

5.5 Proportionaliteit

De conclusie over proportionaliteit in Hoofdstuk 3, die specifiek handelde over de proportionaliteitsregel, was dat, vanwege het per definitie ontbreken van fysieke gevolgen bij militaire operaties beneden de drempel van aanval, bijkomende schade of bijkomend letsel niet kan optreden en dus zeker niet buitensporig kan zijn. Met andere woorden, de proportionaliteitsregel geldt niet voor militaire operaties beneden de grens van aanval.¹¹¹ Toch kan ook hier, net als hiervoor bij voorzorgsmaatregelen, het grondbeginsel van proportionaliteit niet terzijde geschoven worden bij militaire cyberoperaties beneden de drempel van aanval.

De proportionaliteitsregel zoals vastgelegd in artikel 51 en 57 Aanvullend Protocol I betreft een uitwerking van het grondbeginsel van proportionaliteit¹¹² en is daarbij van toepassing op ‘aanvallen’ in de zin van artikel 49 Aanvullend Protocol I. Als grondbeginsel is proportionaliteit echter ook van toepassing op de bredere balans tussen militaire noodzaak en humaniteit¹¹³ en speelt het dus ook een rol in de hierboven bij methoden en middelen van oorlogvoering besproken afweging tussen militaire noodzaak en humaniteit.¹¹⁴ Omdat binnen het humanitair oorlogsrecht het grondbeginsel bijna altijd direct gekoppeld is aan de proportionaliteitsregel die geldt voor aanvallen, zal ik de bovenstaande afweging tussen militaire noodzaak en humaniteit niet benoemen als direct gebaseerd op het grondbeginsel

■
¹¹⁰ Denk daarbij aan hoeveel mensen er beschikbaar zijn, of de mogelijkheid bestaat een test uit te voeren in een cyberlab, hoeveel informatie al aanwezig is over het doelwit, hoeveel tijd beschikbaar is etc.

¹¹¹ Zie Hoofdstuk 3 par. 3.3.4.

¹¹² Zie Hoofdstuk 2 par. 2.3.3.

¹¹³ Zie Hoofdstuk 2 par. 2.3.

¹¹⁴ Zie par. 5.3.1.

van proportionaliteit alleen. Enerzijds voorkomt dit spraakverwarring omdat bij de regel volgend uit het proportionaliteitsbeginsel toch veelal aan de proportionaliteitsregel voor aanvallen wordt gedacht. Anderzijds om te benadrukken dat de afweging tussen militaire noodzaak en humaniteit anders is dan bij de proportionaliteitsregel bij aanvallen.¹¹⁵ Dit neemt niet weg dat de afweging, waarbij de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan, niet buitensporig mogen zijn in verhouding tot het te verwachten merkbare militaire voordeel van de operatie, wel mede gebaseerd is op het grondbeginsel van proportionaliteit.¹¹⁶

5.6 Eervol gedrag als grondbeginsel

Eervol gedrag als grondbeginsel is niet beperkt tot daden van geweld en is daarom ook van toepassing beneden de drempel van aanval.¹¹⁷ Hoe dit grondbeginsel uitwerkt bij cyberoperaties beneden de drempel van aanval zal ik bezien aan de hand van de drie regels die ik in Hoofdstuk 3 heb geïdentificeerd als gebaseerd op dit grondbeginsel, namelijk het verbod op perfidie, het ongepast gebruik van erkende kentekenen en het gebruik van bepaalde nationaliteitskentekenen.

5.6.1 Perfidie

Zoals in Hoofdstuk 3 naar voren kwam is binnen het humanitair oorlogsrecht perfidie verboden beneden de drempel van aanval als het leidt tot de gevangenneming van personen.¹¹⁸ Door de brede definitie van perfidie¹¹⁹ zijn andere vormen van perfidie denkbaar, ook beneden de drempel van aanval, die niet verboden zijn, zodat *“a sort of grey area of perfidy which is not explicitly sanctioned as such, in between perfidy and ruses of war”*¹²⁰ bestaat. Ik zal dit toelichten aan de hand van een voorbeeld.

Stel een partij in een internationaal gewapend conflict wil informatie over de tegenstander. Zij zet hiervoor een cyberoperatie op waarbij enkele combattanten zichzelf een cyberidentiteit aanmeten waarbij zij zich uitdrukkelijk presenteren als gewone burgers. Via social media komen ze in contact met burgers van de tegenpartij en verzoeken ze deze burgers om informatie over bijvoorbeeld troepenbewegingen, militaire posities, uitrusting et cetera van de tegenpartij te delen.

Het voorwenden van het bezit van de status van burger of van non-combattant is een van de letterlijk genoemde voorbeelden van perfidie in Aanvullend Protocol I artikel 37,¹²¹ tenzij

■
¹¹⁵ Zie par. 5.3.1.

¹¹⁶ Zie hiervoor par. 5.3.1.

¹¹⁷ Zie Hoofdstuk 3 par. 3.4.5.

¹¹⁸ Zie Hoofdstuk 3 par. 3.3.5.1.

¹¹⁹ Aanvullend Protocol I art. 37 lid 1.

¹²⁰ Sandoz, Swinarski & Zimmermann 1987, p. 433.

¹²¹ Aanvullend Protocol I art. 37 lid 1 (c).

sprake is van de uitzondering genoemd in Aanvullend Protocol I artikel 44 lid 3¹²² welke uitzondering *an sich* al voor de nodige interpretatieproblemen bij cyberoperaties beneden de drempel van aanval zal zorgen. Als de combattanten uit het voorbeeld van de vorige alinea de aangemeten cyberidentiteit gebruiken om het vertrouwen te wekken dat zij de bescherming als burger genieten om op die manier informatie los te krijgen, is voldaan aan de definitie van perfidie. De operatie valt niet onder het verbod op perfidie omdat door de operatie niemand gedood, verwond of gevangen genomen wordt, maar is het een toegestane krijgslist? Talloze complicerende factoren zijn in te brengen, zoals het creëren van een cyberidentiteit waarbij de status bewust vaag, en niet uitdrukkelijk als burger benoemd wordt. Of dat de informatie die uit de operatie (mede) gebruikt wordt voor een beschieting waarbij wel doden en gewonden vallen. Maakt dit verschil bij de bepaling of een cyberoperatie beneden de grens van aanval wel of niet onder het verbod op perfidie valt?

Bovenstaand voorbeeld benadrukt het belang van de voorbereiding van een dergelijke cyberoperatie,¹²³ waarbij het grondbeginsel van eervol gedrag kan helpen bij het verhelderen van het grijze gebied tussen verboden perfidie en toegestane krijgslist. De uiteindelijke uitkomst zal, zoals vrijwel altijd, bepaald worden door alle omstandigheden van het specifieke geval en het subjectieve oordeel van de commandant hierover.¹²⁴

5.6.2 Erkende kentekenen

In tegenstelling tot het verbod op perfidie is het verbod op het ongepast gebruik van erkende kentekenen zoals vastgelegd in Aanvullend Protocol I artikel 38 een absoluut verbod¹²⁵ dat ook geldt voor cyberoperaties beneden de drempel van aanval.¹²⁶ Wat precies onder 'ongepast gebruik' (*improper use*) valt, kan afgeleid worden uit de bedoeling, namelijk de beschermende werking, waarvoor de kentekenen zijn ingesteld. "*In the field of protection, the spirit should support the letter of the law, perhaps more than anywhere else.*"¹²⁷ Met andere woorden, daar waar de beschermende werking die erkende kentekenen verlenen gevaar loopt, is sprake van ongepast gebruik.

Voor militaire cyberoperaties beneden de grens van aanval zullen de genoemde kentekenen als het kenteken van het Rode Kruis, de Rode Halve Maan of de Rode Leeuw en Zon, de parlementaire vlag, het beschermende kenteken van culturele goederen¹²⁸ en het kenteken

122 Aanvullend Protocol I art. 44 lid 3: "Handelingen die voldoen aan de in dit lid neergelegde vereisten worden niet als perfidie in de zin van artikel 37, eerste lid, letter c, beschouwd." De vereisten zijn dat de combattant de wapens openlijk draagt (a) gedurende ieder militair treffen, en (b) gedurende de tijd dat hij zichtbaar is voor de tegenpartij bij het betrekken van militaire posities, voorafgaande aan het inzetten van een aanval waaraan hij moet deelnemen.

123 Zie par. 5.4.5

124 En toont hiermee overeenkomsten met de proportionaliteitstest zoals omschreven in Hoofdstuk 2, par. 3.3. Zie ook Sandoz, Swinarski & Zimmermann 1987, p. 684.

125 Sandoz, Swinarski & Zimmermann 1987, p. 448.

126 Zie Hoofdstuk 3 par. 3.5.2.

127 Sandoz, Swinarski & Zimmermann 1987, p. 449.

128 Aanvullend Protocol I art. 38 lid 1.

van de Verenigde Naties¹²⁹ weinig vraagtekens opwerpen zolang ze op een traditionele manier, dat wil zeggen op een manier die is vastgesteld “als voorzien in de Verdragen of dit Protocol”¹³⁰ kenbaar worden. Maar hoe werkt dit binnen het cyberdomein?

De samenstellers van de *Tallinn Manual* kwamen tot twee verschillende benaderingswijzen waarbij de meningen vooral verschilden over hoever het verbod zich uitstrekt “*beyond the recognized and specified indicators*.”¹³¹ De eerste benaderingswijze gaat uit van een “*strict textual interpretation of the underlying treaty law*”,¹³² waarbij alleen het gebruik van elektronische reproducties van erkende kentekenen uit het humanitair oorlogsrecht valt onder het verbod op ongepast gebruik. In deze benaderingswijze valt bijvoorbeeld het gebruik van een e-mailadres met de extensie ‘icrc.org’ om een filter in een vijandelijk netwerk te omzeilen niet onder het verbod op ‘ongepast gebruik’ omdat het Rode Kruiskenteken niet misbruikt is.¹³³ De tweede benaderingswijze, gebaseerd op een teleologische uitleg, gaat ervan uit dat onder erkende kentekenen ook datgene valt waaraan andere partijen redelijkerwijs een beschermende werking verlenen.¹³⁴ Het gebruik van hetzelfde e-mailadres met de extensie ‘icrc.org’ voor een militaire cyberoperatie valt in deze benaderingswijze wel onder het verbod van artikel 38 Aanvullend Protocol I.

Bovenstaande teleologische benadering vindt steun in de *Commentary I Geneva Convention*. Waar artikel 53 van de eerste Geneefse Conventie specifiek het misbruik van het Rode Kruiskenteken behandelt gaat de *Commentary* een stap verder. “*It is not sufficient, however, to combat misuses that are legally forbidden. [ref. art 53] The emblem must retain its high significance and prestige in all circumstances, and any practice likely to lower it in the eyes of the public must be scrupulously avoided.*”¹³⁵

In deze discussie sta ik aan de zijde van de teleologische benaderingswijze. Naast de hierboven vermelde argumenten baseer ik mijn keuze op het argument dat ik eerder gebruikte bij de term ‘ontzien en beschermd’. Deze term, die ook geldt voor het Rode Kruis, biedt ook bescherming tegen militaire operaties beneden de drempel van aanval, indien deze operaties gericht zijn tegen het humanitair optreden of functioneren, of dit optreden of functioneren negatief beïnvloeden.¹³⁶ De eerste, strikt tekstuele, interpretatie uit de *Tallinn Manual* laat een cyberoperatie toe die het humanitair functioneren van het Rode Kruis zal beïnvloeden, bijvoorbeeld doordat wantrouwen ten opzichte van het Rode Kruis zal ontstaan vanaf het moment dat bekend wordt dat e-mails met de extensie ‘icrc.org’

129 Aanvullend Protocol I art. 38 lid 2.

130 Aanvullend Protocol I art. 38 lid 1. Zo geeft Aanvullend Protocol I, Annex 1 Chapter III de manieren waarop de erkende kentekenen kenbaar gemaakt kunnen worden met licht (art. 7), radiosignalen (art. 8) en elektronische identificatie (art 9).

131 Schmitt 2013, p. 186.

132 Schmitt 2013, p. 187.

133 Schmitt 2013, p. 187.

134 Schmitt 2013, p. 187.

135 Pictet 1952, p. 335.

136 Zie Hoofdstuk 3 par. 3.3.3.2.

zijn gebruikt voor militaire cyberoperaties, wat gezien mijn argumentatie bij ‘ontzien en beschermd’ niet zou mogen.

Los van wie gelijk heeft in de discussie over ‘ongepast gebruik’ van erkende kentekenen, is dit een voorbeeld waarbij het grondbeginsel van eervol gedrag kan helpen bij het vinden van een oplossing in een situatie waar de toepassing van de regels onduidelijkheid oplevert,¹³⁷ waarbij het van alle omstandigheden van het geval af zal hangen hoe de uitkomst uit zal vallen.

5.6.3 Nationaliteitskentekenen

Het verbod op het gebruik van nationaliteitskentekenen geldt voor nationaliteitskentekenen van neutrale staten en staten die geen partij zijn bij het conflict, ook beneden de drempel van aanval. Het verbod op het gebruik van nationaliteitskentekenen van de tegenpartij geldt ook voor militaire operaties beneden de drempel van aanval al wordt deze conclusie niet door iedereen gedeeld.¹³⁸ Hoe deze verboden uitwerken voor militaire cyberoperaties beneden de drempel van aanval, zal ik in deze subparagraaf bespreken.

Het is goed nog even stil te staan bij wat onder nationaliteitskentekenen verstaan moet worden. Artikel 39 Aanvullend Protocol I spreekt van “vlaggen of de militaire kentekenen, onderscheidingstekens of uniformen”¹³⁹ wat verwijst naar “*only the concrete visual aspects*”¹⁴⁰ en verbiedt het gebruik van “*codes, passwords and countersigns to aid military operations*” als krijgslisten niet.¹⁴¹ Het gebruik van dit soort signalen “*has traditionally been regarded as an acceptable form of deception*.”¹⁴² Hoe kan dit vertaald worden naar cyberoperaties beneden de drempel van aanval? Als codes, wachtwoorden en bevestigingstekens van een tegenpartij gebruikt mogen worden als krijgslist, ligt een analoge toepassing op virtuele componenten van het cyberdomein voor de hand. Zo kunnen bijvoorbeeld cyberidentiteiten, computerprogrammatuur of computergegevens ‘vermomd’ worden als afkomstig van de tegenstander om zo een beveiliging te omzeilen. Maar wat als dezelfde virtuele componenten worden ‘vermomd’ als afkomstig van een overheid of (militaire) instantie van een neutrale staat of staat die geen partij is bij het conflict en niet specifiek van een tegenstander?¹⁴³ Komt dit niet in de buurt van het verbod uit lid 1 van artikel 39 Aanvullend Protocol I? Het verbod op nationaliteitskentekenen van neutrale staten of andere partijen die geen partij zijn bij het gewapende conflict is namelijk “*absolute in an armed conflict*”.¹⁴⁴ Mag, gelet op dit absolute karakter van het verbod in relatie tot het geclausuleerde verbod

137 Zie Hoofdstuk 3 par. 3.3.2.2.

138 Zie Hoofdstuk 3 par. 3.3.2.3.

139 Aanvullend Protocol I artikel 39 lid 1 en 2.

140 Bothe, Partch & Solf 2013 p. 246.

141 Bothe, Partch & Solf 2013 p. 246.

142 Watts 2014, p. 166.

143 Een voorbeeld is gebruikmaken van een *top-level* domein naam met de extensie .gov of .mil.

144 Sandoz, Swinarski & Zimmermann 1987, p. 463.

van artikel 39 lid 2¹⁴⁵ de term “vlaggen of de militaire kentekenen, onderscheidingstekens of uniformen”¹⁴⁶ op dezelfde manier worden uitgelegd zodat het gebruik van virtuele componenten ‘vermomd’ als afkomstig van een neutrale staat ook een legitieme krijgslist oplevert?

Zonder deze vraag in absolute zin te kunnen beantwoorden, kan een oplossing gezocht worden in een analoge toepassing van de verbijzondering gegeven in artikel 39 Aanvullend Protocol I, namelijk het gebruik van vlaggen tijdens gewapende conflicten op zee.¹⁴⁷ Als het gaat om het gebruik van vlaggen schrijft de *San Remo Manual* hierover: “*Deception at sea has been a most remarkable feature in naval history. Warships were entitled to disguise themselves if they so wished by, for instance, flying other colors*”¹⁴⁸ om vervolgens verder te gaan met “*the extensive practice of deception in the past has significantly affected the protection of peaceful shipping*.”¹⁴⁹ Een totaal verbod op misleiding werd echter niet opportuun geacht omdat het humanitair oorlogsrecht strijdende partijen toestaat om bijvoorbeeld camouflagemaatregelen te nemen. Uiteindelijk werd de oplossing gevonden in de vorm van “*Ruses of war are permitted. Warships and auxiliary vessels, however, are prohibited from launching an attack whilst flying a false flag and at all times from actively simulating the status of*”¹⁵⁰ gevolgd door een uitputtende lijst van schepen waarvan de status niet gesimuleerd mag worden.¹⁵¹

Het eerste gedeelte, *launching an attack whilst flying a false flag*, ziet op het uitvoeren van een aanval in de zin van artikel 49 Aanvullend Protocol I. Het tweede gedeelte, dat begint met *at all times*, is relevant voor dit onderzoek, omdat deze term ook militaire operaties beneden de drempel van aanval dekt. De relevantie zit in het woord ‘actively’ waarmee wordt aangeduid dat schepen alleen het verbod op simulatie van een beschermd schip overtreden als zij gebruik maken van “*means of communications and terminology reserved for the shipping concerned*”.¹⁵² Met andere woorden, alleen indien gebruik gemaakt wordt van communicatiemiddelen of technologie die is *voorbehouden* aan een schip met een beschermde status betreft het een verboden krijgslist. Het gebruik van communicatiemiddelen en technologie die gebruikt wordt door een schip met een beschermde status, maar ook door schepen van bijvoorbeeld de tegenstander, valt niet onder het verbod en is daarmee een toegestane krijgslist.

■
145 Geclausuleerd in de zin dat het het verbod ‘slechts’ geldt bij: “aanvallen of met het oogmerk militaire operaties te dekken, te begunstigen, te beschermen of te belemmeren.”

146 Aanvullend Protocol I artikel 39 lid 1 en 2.

147 Aanvullend Protocol I, art 39 lid 3 luidt: “Geen enkele bepaling van dit artikel of van artikel 37, eerste lid, letter d, vormt een aantasting van de bestaande, algemeen erkende regels van het volkenrecht, toepasselijk in geval van spionage of het gebruik van vlaggen tijdens gewapende conflicten op zee.”

148 Doswald-Beck 1995, p. 184.

149 Doswald-Beck 1995, p. 184.

150 Doswald-Beck 1995, p. 184.

151 Deze lijst bevat: “a. hospital ships, small coastal rescue craft or medical transports; b. vessels on humanitarian missions; c. passenger vessels carrying civilian passengers; d. vessels protected by the United Nations flag; e. vessels guaranteed safe conduct by prior agreement between the parties, including cartel vessels; f. vessels entitled to be identified by the emblem of the red cross or red crescent; g. vessels engaged in transporting cultural property under special protection. Doswald-Beck 1995, p. 184-185.

152 Doswald-Beck 1995, p. 185.

Bovenstaande redenering kan op een analoge manier worden toegepast op het gebruik van virtuele componenten voor militaire cyberoperaties beneden de drempel van aanval. Wanneer virtuele componenten ‘vermomd’ worden zodat de originele afkomst onduidelijk is, hangt het van de gebruikte methode af of dit is toegestaan. Wordt gebruik gemaakt van een vermomming of technologie die is *voorbehouden* aan een partij die bescherming geniet tegen cyberoperaties beneden de grens van aanval,¹⁵³ dan is de cyberoperatie verboden. Betreft het echter een vermomming of technologie die breder gebruikt wordt, bijvoorbeeld door de tegenstander maar die *ook* door een partij die bescherming geniet tegen cyberoperaties beneden de grens van aanval kan worden gebruikt, is sprake van een geoorloofde krijgslist.

5.7 Regels van humanitair oorlogsrecht van toepassing op militaire cyber operaties beneden de grens van aanval.

Aan het slot van dit hoofdstuk, en van dit onderzoek, is dit de plaats om een samenvatting te geven van de regels en antwoord te geven op de vraag ‘welke regels gelden in het humanitair oorlogsrecht voor militaire operaties onder de drempel van artikel 49 lid 1 Aanvullend Protocol I en hoe kunnen deze regels worden toegepast?’ Samengevat kan ik concluderen dat alle grondbeginselen uit het humanitair oorlogsrecht van kracht zijn op militaire cyberoperaties beneden de grens van aanval. In sommige gevallen werken ze echter wel anders uit dan bij aanvallen waardoor een aantal regels uit het humanitair oorlogsrecht niet van toepassing zijn of tot een andere uitkomst leiden dan bij aanvallen.

5.7.1 Militaire noodzaak

Zodra, op basis van het grondbeginsel van onderscheid, negatieve gevolgen voor burgers of burgerobjecten te voorzien zijn, is het grondbeginsel van militaire noodzaak onverkort van toepassing beneden de drempel van aanval. Voor militaire cyberoperaties beneden de drempel van ‘aanval’ betekent dit dat er een merkbaar militair voordeel te behalen moet zijn. Bij de bepaling van de balans tussen militaire noodzaak en humaniteit worden, bij militaire cyberoperaties beneden de drempel van aanval, lagere eisen gesteld aan het te behalen militaire voordeel dan bij aanvallen.

5.7.2 Humaniteit

Het grondbeginsel van humaniteit is onder meer terug te vinden in de regel dat de keuze voor methoden en middelen van oorlogvoering niet onbegrensd is. Om te bepalen welke methoden en middelen van oorlogvoering nog zijn toegestaan, moet een balans gevonden worden tussen militaire noodzaak en humaniteit. Voor militaire cyberoperaties beneden de drempel van aanval kan deze afweging omschreven worden als: de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan, mogen niet buitensporig zijn in verhouding tot het te verwachten merkbare militaire voordeel van de operatie. Net als bij de

¹⁵³ Bijvoorbeeld neutrale staten of andere partijen die geen partij zijn bij het conflict, maar ook de hiervoor behandelde personen en zaken beschermd door erkende kentekenen.

proportionaliteitsregel voor aanvallen zal de uitkomst van de afweging afhangen van alle omstandigheden van het concrete geval.

5.7.3 Onderscheid

De bescherming die het humanitair oorlogsrecht biedt op basis van het grondbeginsel van onderscheid werkt verschillend voor personen en objecten.

5.7.3.1 Personen

Voor personen geldt op basis van dit grondbeginsel dat militaire cyberoperaties beneden de drempel van aanval gericht mogen worden op zowel de burgerbevolking in zijn geheel als op individuele burgers of specifieke groepen als vrouwen, kinderen en journalisten. De niet-fysieke gevolgen mogen daarbij echter niet buitensporig zijn in verhouding tot het te verwachten merkbare militaire voordeel van de cyberoperatie.

Voor één verzameling personen gaat de bescherming tegen niet-fysieke gevolgen verder. Het betreft personen die humanitaire hulp verlenen, zoals medisch en religieus personeel, personeel ten behoeve van civiele bescherming en personeel dat deelneemt aan hulpverleningsacties, of die humanitaire hulp behoeven, zoals zieken, gewonden en schipbreukelingen. Deze verzameling personen moet 'beschermd en ontzien' worden, wat inhoudt dat militaire cyberoperaties niet gericht mogen zijn op het humanitair optreden of functioneren en dat de niet-fysieke gevolgen dit humanitair optreden of functioneren niet negatief mogen beïnvloeden.

Cyberidentiteiten behoren niet tot de categorie personen.

5.7.3.2 Objecten

Burgerobjecten, inclusief de virtuele componenten van het cyberdomein, mogen, op basis van het grondbeginsel van onderscheid, niet alleen het doel vormen van een militaire cyberoperatie beneden de drempel van aanval, ze mogen hiervoor ook gebruikt worden, tenzij zij behoren tot een van de hierna volgende categorieën objecten met bijzondere bescherming.

Culturele goederen mogen niet gebruikt worden voor militaire cyberoperaties beneden de drempel van aanval,¹⁵⁴ al is dit verbod niet absoluut. Virtuele componenten kunnen ook culturele goederen zijn als zij voldoen aan dezelfde eisen zoals die gelden voor fysieke objecten.

Objecten bedoeld voor humanitaire hulpverlening die vallen onder de bescherming van 'ontzien en beschermd' worden beschermd tegen militaire cyberoperaties beneden de drempel van aanval, voor zover deze cyberoperaties gericht zijn op het humanitair optreden of functioneren of als de niet-fysieke gevolgen het humanitair optreden of functioneren negatief beïnvloeden.

■
¹⁵⁴ Art. 53 Aanvullend Protocol I.

5.7.3.3 Voorbereiding

Net als bij aanvallen moet bij militaire cyberoperaties beneden de drempel van aanval aan een aantal voorwaarden zijn voldaan voordat ze rechtmatig kunnen worden uitgevoerd. Om spraakverwarring met voorzorgsmaatregelen, een term gekoppeld aan aanvallen, te voorkomen gebruik ik de term ‘voorbereiding’ bij militaire operaties beneden de grens van aanval.

Bij de voorbereiding en tijdens de uitvoering van militaire cyberoperaties beneden de grens van aanval moet alles gedaan worden wat ‘praktisch uitvoerbaar’ is om uit te sluiten dat dergelijke militaire cyberoperaties fysieke gevolgen hebben, kunnen hebben of kunnen krijgen. Naast de aandacht voor de fysieke gevolgen moet in de voorbereiding en tijdens de uitvoering voorkomen worden dat deze operaties gericht zijn op het humanitair optreden of functioneren van personen, instanties of objecten die ‘ontzien en beschermd’ moeten worden. Dit houdt tevens in dat dit humanitair optreden of functioneren niet negatief beïnvloed mag worden. Ook moet speciaal aandacht worden besteed aan de verhoogde bescherming van culturele goederen, zowel fysieke als digitale.

5.7.4 Proportionaliteit

Het grondbeginsel van proportionaliteit is ook van kracht beneden de drempel van aanval echter de proportionaliteitsregel zoals die geldt bij aanvallen geldt niet bij militaire cyberoperaties beneden de drempel van aanval. De hierboven beschreven afweging dat ‘de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan, niet buitensporig mogen zijn in verhouding tot het te verwachten merkbare militaire voordeel van de operatie’ is weliswaar mede gebaseerd op het grondbeginsel van proportionaliteit, maar om spraakverwarring met de proportionaliteitsregel te voorkomen duid ik deze aan als afweging tussen militaire noodzaak en humaniteit.

5.7.5 Eervol gedrag

Bij militaire cyberoperaties beneden de drempel van aanval levert het grondbeginsel van eervol gedrag geen juridische verplichtingen op, maar het grondbeginsel kan wel behulpzaam zijn bij de interpretatie van concrete regels. Een voorbeeld hiervan is het beoordelen van het grijze gebied tussen krijgslisten en strafbaar gestelde perfidie.

5.8 Conclusies en synthese

De manier waarop gewapende conflicten worden gevoerd, is van invloed geweest op de ontwikkeling van het humanitair oorlogsrecht. De doelstelling van het humanitair oorlogsrecht is tweeledig: het reguleren, waaronder beperken van de toegestane methoden en middelen van oorlogvoering en het beschermen van personen en objecten die niet, of niet langer, direct betrokken zijn bij het gewapend conflict. Binnen traditionele gewapende conflicten ligt de nadruk op kinetisch optreden,¹⁵⁵ wat is gericht op het toebrengen van fysieke schade of letsel aan de tegenstander. Deze manier van optreden heeft zijn weerslag gevonden in specifieke regels binnen het humanitair oorlogsrecht gericht op het reguleren van dit kinetisch optreden en dan met name op het reguleren van ‘aanvallen’. Aanvallen zijn binnen het humanitair oorlogsrecht gedefinieerd als “dad[en] van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve.”¹⁵⁶ De specifieke regels voor aanvallen dragen bij aan een balans tussen de twee voornaamste grondbeginselen van het humanitair oorlogsrecht, militaire noodzaak en humaniteit.

Relatief minder aandacht is er binnen het humanitair oorlogsrecht geweest voor militaire operaties die niet voldoen aan de criteria van ‘aanval’. Hierbij valt te denken aan psychologische operaties¹⁵⁷ of elektromagnetische operaties.¹⁵⁸ Dit soort operaties bestond wel, maar werd voornamelijk gezien als ondersteunend aan kinetisch militair optreden waarmee het gewapend conflict werd gewonnen.

Twee ontwikkelingen maken dat militaire operaties beneden de drempel van aanval in de afgelopen jaren meer aandacht hebben gekregen. De eerste is de ontwikkeling dat het minder eenvoudig lijkt vast te stellen of, en wanneer sprake is van een gewapend conflict. Dit is met name het geval indien militair optreden onderdeel is van een grotere hybride strategie waarbij een partij gebruik maakt van een mix aan middelen en instrumenten uit de reeks “*diplomatic, information, military, economic, financial, intelligence, legal/law enforcement (DIMEFIL)*”¹⁵⁹ en daarbij “*aim[s] to create ambiguity and blur the lines between peace, crisis, and conflict.*”¹⁶⁰ Bij traditioneel kinetisch optreden zal relatief eenvoudig vastgesteld kunnen

155 De term ‘kinetisch’ verwijst hier naar het militaire optreden gebaseerd op het vrijlaten van kinetische energie in hoofdzaak veroorzaakt door explosies.

156 Art. 49 lid I Aanvullend Protocol I.

157 *Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*, AAP-6 (2014)

158 *Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects*, AAP-6 (2014)

159 Saathof 2018, p. 251.

160 NATO: *Brussels Summit Declaration* 2018, par. 21. Ook Nederland ziet dit als een reële dreiging, “hybride oorlogvoering vormt een reële bedreiging voor open westerse samenlevingen.” Zie de nota “Houvast in een onzekere wereld”, 2017 p.8. Kamerstukken II 1016–2017, bijlage bij 33763 nr. A.

worden of sprake is van een gewapend conflict,¹⁶¹ waarmee het humanitair oorlogsrecht van toepassing is. Bij militaire operaties beneden de drempel van aanval zal dit vaak minder het geval zijn. Partijen kunnen bewust gebruik maken van deze onduidelijkheid.

De tweede ontwikkeling is de opkomst en ontwikkeling van het cyberdomein. De mogelijkheden van steeds meer en snellere verbindingen, rekenkracht en opslagcapaciteit leiden tot meer cybertoeepassingen, ook voor militaire operaties. Er ontstaat een trend van *dematerialization* waarmee wordt bedoeld op “*the elimination of materials altogether for certain functions*.”¹⁶² Dit leidt tot een grotere afhankelijkheid van niet-fysieke of virtuele zaken.¹⁶³ Indien militaire operaties vooral gericht zijn op, of tegen personen en fysieke objecten, is kinetisch optreden vaak de eerste, en soms enige optie om een operatie te laten slagen. Bij militaire operaties tegen virtuele zaken behoren kinetische operaties zeker tot de mogelijkheden,¹⁶⁴ maar bieden *non-violent* of niet-kinetische militaire operaties gericht op of tegen virtuele zaken juist nieuwe mogelijkheden.

Naarmate de afhankelijkheid van de *bits* ten opzichte van de *atoms* toeneemt, zullen ook de mogelijkheden voor niet-kinetische militaire operaties op twee manieren groeien. Ten eerste zal een tegenstander, als gevolg van de toegenomen reken- en opslagcapaciteit van computers, de betere en snellere verbindingsmogelijkheden voor uitwisseling van gegevens en de trend van *dematerialization*, steeds afhankelijker worden van virtuele zaken en dus steeds meer virtuele zaken hebben waarop militaire cyberoperaties gericht kunnen worden. Ten tweede zullen de mogelijkheden om zelf gebruik te maken van niet-fysieke zaken, bijvoorbeeld computerprogramma's, toenemen.

De toegenomen aandacht voor militaire cyberoperaties beneden de drempel van aanval betekent ook dat de vraag, hoe het humanitair oorlogsrecht toegepast moet worden op deze operaties, opportuun is. Het antwoord is namelijk op meerdere manieren relevant. Op maatschappelijk niveau is ook de maatschappij afhankelijker geworden van niet-fysieke zaken. Belangrijke vraag is dan of militaire operaties beneden de drempel van aanval, bijvoorbeeld beïnvloedingsoperaties, gericht mogen zijn op deze niet-fysieke zaken van de burgerbevolking, specifieke groepen of individuele burgers. Indien dit zou mogen, gelden daar dan specifieke regels voor of zijn dergelijke operaties altijd geoorloofd zolang ze maar

■
¹⁶¹ Ik gebruik bewust de aanduiding ‘relatief’ omdat ook bij de vaststelling van een gewapend conflict waarbij sprake is van traditioneel kinetisch geweld waarderingsproblemen op kunnen treden. Zo moet in het geval van een niet-internationaal gewapend conflict aan een tweetal criteria worden voldaan te weten “(1) feitelijke vijandelijkheden van een zekere intensiteit, bestaande uit aan elkaar gerelateerde ‘incidenten’, die (2) uitgevoerd worden door tegenover elkaar staande georganiseerde gewapende groepen die over het vermogen beschikken om over een langere periode militaire operaties te ondernemen.” Duchéine & Pouw 2010, p. 135. Voor concrete toetsing aan deze criteria in een specifiek geval, zie Duchéine & Pouw 2010.

¹⁶² Keulen 2018, p. 24.

¹⁶³ Een eenvoudig voorbeeld kan dit verduidelijken. Indien alle militaire zijn uitgerust en geoefend met een Global Positioning System (GPS) zullen er minder of helemaal geen kompassen en kaarten gebruikt worden voor plaats en routebepaling. Hiermee worden de militairen afhankelijker van de verbindingen met het GPS en de bijbehorende gegevens.

¹⁶⁴ Zie bijv. Applegate, 2013 *The Dawn of Kinetic Cyber*.

beneden de drempel van aanval blijven?¹⁶⁵ Voor militairen is de vraag hoe het humanitair oorlogsrecht toegepast moet worden op operaties beneden de drempel van aanval relevant omdat zij dit soort operaties moeten kunnen uitvoeren¹⁶⁶ waarbij duidelijk moet zijn aan welke regels zij zich moeten houden. Op juridisch wetenschappelijk niveau is met de opkomst van het cyberdomein voor militaire operaties een aantal discussies op gang gekomen die tot soms moeilijk verenigbare denkrichtingen hebben geleid, bijvoorbeeld over wat een cyberaanval is.¹⁶⁷ Duidelijkheid over de toepassing van het humanitair oorlogsrecht beneden de drempel van aanval kan dan helpen bij de vaststelling wat onder het humanitair oorlogsrecht verstaan wordt onder een cyberaanval.

Bovengenoemde ontwikkelingen en de impact die deze kunnen hebben op de manier van oorlogvoering hebben geleid tot de centrale vraag van dit onderzoek: welke regels gelden in het humanitair oorlogsrecht voor militaire cyberoperaties die beneden de drempel van aanval, zoals gedefinieerd in artikel 49 lid 1 Aanvullend Protocol I, blijven?

Om deze vraag te kunnen beantwoorden heb ik als eerste onderzocht waar de drempel van aanval ligt voor traditionele militaire operaties en voor cyberoperaties. Deze zijn met elkaar vergeleken.¹⁶⁸ De grens voor militaire operaties in traditionele zin ligt bij het oogmerk om, of het daadwerkelijk veroorzaken van fysieke schade of letsel.¹⁶⁹ Deze grens is met de opkomst van het cyberdomein en daarmee de mogelijkheden voor militaire operaties in of gebruikmakend van dit cyberdomein, niet veranderd. Zodra een cyberoperatie gericht is op, of voorzienbaar leidt tot, fysieke schade of letsel, is de cyberoperatie een aanval in de zin van artikel 49 Aanvullend Protocol I. Hieruit volgt mijn eerste conclusie dat de grens tussen aanval en militaire operaties beneden de grens van aanval, voor traditionele operaties en cyberoperaties gelijk is. Zolang beide soorten operaties niet gericht zijn op, of leiden tot fysieke schade of letsel zijn het geen aanvallen in de zin van artikel 49 Aanvullend Protocol I en hoeven dus ook niet te voldoen aan de specifieke regels die binnen het humanitair oorlogsrecht gelden voor aanvallen, zoals het verbod op aanvallen van burgers of burgerobjecten.¹⁷⁰

165 Duidelijkheid hierover is gewenst. Denk daarbij aan vragen als; is het toegestaan om social media accounts van familieleden van militairen te gebruiken om zo militairen te beïnvloeden? Mogen met hetzelfde doel bankrekeningen van familieleden of kennissen van militairen (tijdelijk) geblokkeerd worden?

166 Dat dit ook nu al gebeurd blijkt bijv. uit BBC 2018, <http://www.bbc.com/news/technology-43738953>, laatst geraadpleegd 28 nov 2018, waar de directeur van het *Government Communications HQ* UK opmerkte over een UK actie tegen IS: "It is the first time the UK has systematically degraded an adversary's online efforts in a military campaign."

167 Zie bijv. de discussie in de *Tallinn Manual* over de definitie van een *cyber attack*, Schmitt 2013, p. 106-110.

168 Dit is een samenvoeging van de eerste en de derde deelvraag uit mijn onderzoek, respectievelijk "waar ligt de ondergrens van aanval voor militaire operaties in traditionele zin" en "hoe moet de drempelwaarde van aanval geïnterpreteerd worden voor militaire operaties in het cyberdomein".

169 De bedoeling om letsel of schade te veroorzaken levert ook een aanval. Een kogel die wordt afgevuurd om iemand te doden maar die het doel mist is een aanval, ook als er verder geen enkele schade ontstaat.

170 Zoals gecodificeerd in respectievelijk art. 51 en 52 Aanvullend Protocol I.

De logisch daarop volgende vraag is: welke regels uit het humanitair oorlogsrecht gelden voor cyberoperaties beneden de drempel van aanval?¹⁷¹ Om deze vraag te kunnen beantwoorden moest ik eerst een positie innemen over een vraag die al enige tijd voor verdeeldheid in de academische wereld zorgt, namelijk wat is de status van niet-fysieke of virtuele componenten van het cyberdomein binnen het humanitair oorlogsrecht.¹⁷² Deze vraag is zo belangrijk omdat volgens de algemeen geldende interpretatie binnen het humanitair oorlogsrecht twee soorten militaire doelen voor aanvallen bestaan, combattanten (personen) en militaire objecten. Vervolgens geeft het humanitair oorlogsrecht de voorwaarden waaronder deze militaire doelen legitiem aangevallen mogen worden.¹⁷³

De niet-fysieke componenten van het cyberdomein kunnen zeker niet aangemerkt worden als personen, zodat het hooguit objecten kunnen zijn om binnen de algemeen geldende opvatting van militair doel te kunnen vallen. Volgens de tot op heden meest gangbare uitleg van het humanitair oorlogsrecht vallen onder objecten echter alleen zichtbare en tastbare zaken. Dit heeft als consequentie dat de niet-fysieke componenten van het cyberdomein niet zijn te kwalificeren als object in de zin van het humanitair oorlogsrecht. Een aantal argumenten heeft mij doen concluderen dat anno 2019 niet-fysieke componenten van het cyberdomein wel de status van object binnen het humanitair oorlogsrecht bezitten. Als eerste is daar het steeds groter wordende belang van deze niet-fysieke componenten van het cyberdomein voor de hele maatschappij en ook voor militair optreden.¹⁷⁴ Deze niet-fysieke componenten vormen daarmee potentiële militaire doelen in de zin dat het militair voordeel oplevert om deze componenten uit te schakelen, geheel of gedeeltelijk te vernietigen of onbruikbaar te maken. Het tweede en voor mij doorslaggevende argument is dat staten, als ultieme makers van het humanitair oorlogsrecht,¹⁷⁵ in andere rechtsgebieden geen bezwaar hebben tegen uitbreiding van het begrip object met niet-fysieke zaken. Nu is het niet zo is dat concepten uit een bepaald rechtsgebied automatisch doorwerken in andere rechtsgebieden, maar de redenen om niet-fysieke componenten binnen het humanitair oorlogsrecht te beschouwen als objecten, namelijk om een betere bescherming te bieden aan zaken die een cruciale rol binnen de

171 Dit is een samenvoeging van de tweede en vierde deelvraag van mijn onderzoek, respectievelijk "welke regels gelden er in het humanitair oorlogsrecht voor militaire operaties die de drempel van aanval niet halen" en "welke regels gelden er in het humanitair oorlogsrecht voor militaire cyberoperaties beneden de drempel van aanval".

172 De niet-fysieke componenten van het cyberdomein heb ik ingedeeld in vijf categorieën, firmware, besturingssystemen, cyberidentiteiten, computerprogramma's en applicaties, en computergegevens.

173 Voor personen wordt dit bepaald op basis van de status (combattant of burger die rechtstreeks deelneemt aan de vijandigheden en daarmee zijn beschermde status van burger verliest). Voor objecten is dit gecodificeerd in art 52 lid 2 Aanvullend Protocol I dat luidt: "Aanvallen dienen strikt tot militaire doelen te worden beperkt. Voor zover het objecten betreft, zijn militaire doelen uitsluitend die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel oplevert."

174 Een social-media account, een mail account of een bankrekening zijn voorbeelden van niet-fysieke componenten die van belang zijn in het maatschappelijk gebruik die tevens gebruikt kunnen worden als doel van een militaire operatie beneden de drempel van aanval.

175 Schmitt & Watts 2015, p. 193.

hedendaagse maatschappij vertolken, zijn voor mij dwingender dan de redenen om vast te houden aan de traditionele opvatting.

De conclusie dat de niet-fysieke componenten van het cyberdomein objecten zijn in de zin van het humanitair oorlogsrecht, heeft als gevolg dat deze niet-fysieke componenten binnen het bereik van militair doel vallen zoals gedefinieerd in artikel 52 lid 2 Aanvullend Protocol I. Bij de traditionele uitleg van objecten binnen het humanitair oorlogsrecht, namelijk dat alleen zichtbare en tastbare zaken objecten zijn, is dat niet het geval waardoor een hiaat ontstaat. De niet-fysieke componenten van het cyberdomein die een daadwerkelijke bijdrage tot de krijgsv verrichtingen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking een duidelijk militair voordeel opleveren zouden geen legitiem militair doel kunnen vormen omdat het geen objecten zijn. Met de nieuwe uitleg kunnen de niet-fysieke componenten, onder de genoemde voorwaarden van artikel 52 lid 2 Aanvullend Protocol I, een legitiem militair doel voor aanvallen vormen.

Maar wat als een militaire operatie beneden de drempel van aanval blijft? Hiermee ben ik terug bij de vraag: welke regels uit het humanitair oorlogsrecht gelden voor cyberoperaties beneden de drempel van aanval? Deze vraag heb ik beantwoord op het abstractieniveau van de grondbeginselen van het humanitair oorlogsrecht, te weten militaire noodzaak, humaniteit, onderscheid, proportionaliteit en eervol gedrag. Deze grondbeginselen liggen ten grondslag aan vrijwel alle regels binnen het humanitair oorlogsrecht. Mijn conclusie is dat deze grondbeginselen ook van kracht zijn op militaire cyberoperaties beneden de grens van aanval. Ik concludeer echter ook dat deze grondbeginselen in sommige gevallen bij cyberoperaties beneden de drempel van aanval anders uitwerken dan bij aanvallen. Hierdoor gelden voor cyberoperaties beneden de grens van aanvallen wel regels op basis van de grondbeginselen van het humanitair oorlogsrecht, maar dit zijn andere regels dan voor aanvallen.

Het eerste verschil ligt op het niveau van de balans tussen de grondbeginselen militaire noodzaak en humaniteit. Binnen het humanitair oorlogsrecht is het toegestaan om niet-fysieke componenten van het cyberdomein, net als fysieke objecten, te gebruiken voor militaire operaties beneden de drempel van aanval, ook als ze daardoor aan gevaar voor beschadiging of vernietiging worden blootgesteld.¹⁷⁶ Dat gebruik is echter niet onbeperkt. Dit concludeer ik op basis van de grondregel uit het humanitair oorlogsrecht dat de keuze van methoden en middelen van oorlogvoering niet onbegrensd is,¹⁷⁷ gecombineerd met de hiervoor vermelde grondbeginselen militaire noodzaak en humaniteit. Dit komt samen in de verplichting voor en tijdens militaire cyberoperaties beneden de grens van aanval een afweging te maken waarbij de grondbeginselen militaire noodzaak en humaniteit

■
¹⁷⁶ Uitzondering hierop vormen objecten voor godsdienstige verering, culturele goederen en objecten voor humanitaire hulpverlening.

¹⁷⁷ Deze grondregel is gecodificeerd in art. 35 lid 1 Aanvullend Protocol I.

met elkaar in balans gebracht moeten worden.¹⁷⁸ Omdat de inbreuk op humaniteit bij een cyberoperatie beneden de drempel van aanval minder zal zijn dan bij aanvallen, zal de afweging al bij minder militaire noodzaak in balans kunnen zijn. Ik heb deze afweging verwoord als: de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan, mogen niet buitensporig zijn in verhouding tot het te verwachten merkbare militaire voordeel van de operatie. Indien voldaan wordt aan de voorwaarden van deze afweging is de militaire cyberoperatie binnen het humanitair oorlogsrecht toegestaan.

Een ander verschil in regels die gelden tussen militaire cyberoperaties beneden de grens van aanval en aanvallen is dat, in tegenstelling tot aanvallen, militaire cyberoperaties beneden de grens van aanval wel gericht mogen zijn op, of tegen, burgers of burgerobjecten, mits daar voldoende merkbaar militair voordeel tegenover staat. Hiermee kan een belangrijk twistpunt uit de academische discussie tussen de permissieve en restrictieve benadering van aanval in het cyberdomein, opgelost worden. De permissieve benadering stelt dat zolang een cyberoperatie geen fysieke gevolgen heeft, deze cyberoperatie géén aanval is en dus ook niet onder het verbod op aanvallen van burgers of burgerobjecten valt. De restrictieve benadering stelt dat militaire operaties nooit gericht mogen zijn op burgers of burgerobjecten, ook niet als er geen fysieke schade optreedt. De permissieve benadering wordt door de tegenstanders afgewezen omdat daarmee militaire cyberoperaties gericht mogen zijn tegen *alle* niet-fysieke componenten van het cyberdomein, ook als het burgerobjecten zijn. Met andere woorden, *“the permissive approach fails to adequately constrain the effects of cyber operations on the civilian population.”*¹⁷⁹ De restrictieve benadering wordt door tegenstanders juist afgewezen omdat daarmee alle militaire cyberoperaties aan de regels van ‘aanval’, dus ook het verbod op aanvallen van burgerobjecten, moeten voldoen, ook als er geen fysieke schade ontstaat. In de restrictieve benadering zou dan bijvoorbeeld het tijdelijk platleggen van een website van een krant onder het verbod vallen. Zowel aanhangers van de permissieve als de restrictieve benadering zijn het erover eens dat een strikte toepassing van een van beide benaderingen tot onwenselijke resultaten leidt. Er bestaat dus behoefte aan een soort middenweg. Over waar deze middenweg zou moeten liggen, blijven de meningen echter uiteen lopen.

De relevantie van de hierboven geïntroduceerde afweging tussen de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan en het te verwachten merkbare militaire voordeel van de operatie, ligt in het nader tot elkaar brengen van de permissieve en restrictieve benadering. De grens tussen legitiem en in strijd met het humanitair oorlogsrecht, is met deze afweging nog niet ‘hard’ gemaakt in de zin dat deze volledig objectief kan worden bepaald. De grens bepalen blijft immers afhankelijk van alle omstandigheden van het specifieke geval. Een keuze tussen de restrictieve en permissieve benadering is echter niet nodig. Er is één afweging die het voordeel heeft

■
¹⁷⁸ Waarbij de andere grondbeginselen een ondersteunende rol vervullen.

¹⁷⁹ Schmitt 2014a, p. 192.

dat zij overeenkomsten vertoont met een afweging die al veel langer bestaat binnen het humanitair oorlogsrecht en waarmee veel ervaring is opgedaan, namelijk de proportionaliteitstest voor aanvallen.¹⁸⁰ Militairen, en andere besluitvormers, die een afweging moeten maken over de rechtmatigheid van een militaire cyberoperatie beneden de drempel van aanval kunnen bij de geïntroduceerde afweging dus putten uit de kennis en ervaring opgedaan met het plannen en uitvoeren van traditionele aanvallen.

Naast de hierboven vermelde afweging die gemaakt moet worden, is mijn conclusie dat nog een andere regel voor cyberoperaties beneden de drempel van aanval bestaat, namelijk dat in de voorbereiding op, en tijdens de uitvoering van een militaire cyberoperatie beneden de drempel van aanval, alles gedaan moet worden wat ‘praktisch uitvoerbaar’ is om uit te sluiten dat de cyberoperatie fysieke gevolgen heeft, kan hebben of kan krijgen. Deze regel is erop gericht te voorkomen dat een geoorloofde militaire cyberoperatie alsnog verandert in een (mogelijk) ongeoorloofde (cyber)aanval. Wat ‘praktisch uitvoerbaar’ inhoudt, zal aan de hand van de omstandigheden van het geval te goeder trouw en op basis van gezond verstand moeten worden vastgesteld, ook wel aangeduid als de standaard van de *“reasonable military commander”*.¹⁸¹

In mijn onderzoek naar de ondergrens van aanval bij cyberoperaties is mijn conclusie dat deze ondergrens, net als bij traditionele operaties ligt bij de fysieke gevolgen. Dit is relevant omdat ik daarmee de conclusies over militair cyberoperaties beneden de grens van aanval breder kan trekken naar alle militaire operaties zonder fysieke gevolgen. Bovengenoemde afweging tussen de negatieve niet-fysieke gevolgen van operaties voor de burgerbevolking en het te verwachten merkbare militaire voordeel is dan ook toepasbaar op andere militaire operaties beneden de drempel van aanval, zoals inlichtingen- of psychologische operaties. Dit betekent dat binnen het humanitair oorlogsrecht de afweging gemaakt moet worden voor en tijdens *alle* militaire operaties beneden de drempel van aanval. De uitkomsten van dit onderzoek leveren daarmee een bijdrage aan de theorievorming over de toepasselijkheid en toepassing van het humanitair oorlogsrecht op militaire operaties die de drempel van aanval, uit de definitie van artikel 49 Aanvullend Protocol I, niet halen.

Het belang van dit onderzoek zit in de toegevoegde kennis over de toepasselijkheid en zeker ook de toepassing van het humanitair oorlogsrecht op militaire operaties beneden de drempel van aanval. Hiermee kunnen deze operaties binnen een gewapend conflict nadrukkelijker in beeld komen als reëel alternatief voor traditioneel kinetische operaties.

■
¹⁸⁰ De proportionaliteitstest is onder andere gecodificeerd in art. 52 Aanvullend Protocol I en geeft aan dat een aanval verboden is als die aanval: “naar kan worden verwacht bijkomend verlies van mensenlevens onder de burgerbevolking, verwonding van burgers, schade aan burgerobjecten of een combinatie daarvan ten gevolge hebben, in een mate die buitensporig zou zijn in verhouding tot het verwachte tastbare en rechtstreekse militaire voordeel.

¹⁸¹ ICTY, Final Report to the Prosecutor 2000, par. 50.

Op strategisch niveau¹⁸² heeft een staat een aantal machtsmiddelen ter beschikking om zijn belangen te behartigen, waaronder het militaire machtsmiddel: de krijgsmacht.¹⁸³ Deze machtsmiddelen zullen over het algemeen in een mix worden ingezet zodat de toegevoegde kennis op zowel politiek als militair strategisch niveau van belang is. Met het ontstaan van het cyberdomein en de bijbehorende mogelijkheden voor militaire cyberoperaties zijn ook de mogelijkheden toegenomen de krijgsmacht in te zetten zonder dat fysieke schade wordt aangericht. Door duidelijkheid over de toepasselijkheid en toepassing van het humanitair oorlogsrecht beneden de drempel van aanval kan een staat onder wiens verantwoordelijkheid de militaire operaties worden uitgevoerd de verplichting “[to] respect and ensure respect for international humanitarian law by its armed forces and other persons or groups acting in fact on its instructions, or under its direction or control”,¹⁸⁴ gestalte geven. Dit geldt in de gevallen dat duidelijk is dat sprake is van een gewapend conflict en dat het humanitair oorlogsrecht van kracht is. Maar ook, of misschien wel juist ook, in de gevallen dat (nog) geen algemene overeenstemming bestaat over het bestaan van een gewapend conflict maar staten het humanitair oorlogsrecht wel beleidsmatig toepassen.¹⁸⁵

Op operationeel en tactisch niveau geeft duidelijkheid over de toepasselijke regels, maar zeker ook de manier van toepassing, de commandant de mogelijkheid militaire operaties beneden de drempel van aanval te (laten) toetsen aan het humanitair oorlogsrecht. De geïntroduceerde afweging tussen militaire noodzaak en humaniteit geeft daarvoor een praktisch hanteerbare afweging, waardoor militaire operaties beneden de grens van aanval eerder in beeld kunnen komen als reëel alternatief voor ‘aanvallen’.

■
182 Strategisch, en hierna operationeel en tactisch, verwijst naar de drie niveaus van operaties conform NATO AJP-01, 2017. Strategisch: “the level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them.” NATO AJP-01, 2017, p. 1-8. Operationeel: “the level at which campaigns and major operations are planned, conducted and sustained to achieve strategic objectives within theatres or areas of operations.” NATO AJP-01, 2017, p. 1-10. Tactisch: “the level at which activities, battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units.” NATO AJP-01, 2017, p. 1-11.

183 De verschillende machtsmiddelen worden vaak aangeduid onder de afkorting DIMEFIL wat staat voor Diplomacy, Information, Military, Economic, Financial, Intelligence, Legal/law enforcement.

184 Henckaerts & Doswald-Beck 2005, p. 495.

185 Voor Nederland zie bijv. Nationale Defensie Doctrine 2013, p. 55.

Samenvatting

Samenvatting

Oorlog voeren zonder geweld. Onderzoek naar de regels binnen het humanitair oorlogsrecht voor militaire cyberoperaties die de drempel van aanval niet halen.

Het humanitair oorlogsrecht heeft zich gedurende vele jaren ontwikkeld tot het systeem van gecodificeerde en gewoonterechtelijke regels zoals we dat nu kennen. De doelstelling van het humanitair oorlogsrecht was, en is, tweeledig, te weten het reguleren, waaronder beperken, van de toegestane methoden en middelen van oorlogvoering en het beschermen van personen en objecten die niet, of niet langer, direct betrokken zijn bij het gewapend conflict. Dit heeft geresulteerd in een balans tussen de twee voornaamste grondbeginselen van het humanitair oorlogsrecht, militaire noodzaak en humaniteit. De balans is veelal gevonden in het reduceren van de verschrikkingen van de oorlog wat heeft geresulteerd in de definiëring en regulering van een specifieke categorie militaire operaties die genoemde verschrikkingen veelal veroorzaakt, namelijk ‘aanvallen’. Binnen het humanitair oorlogsrecht zijn ‘aanvallen’ gedefinieerd als “daden van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve.”¹ Voor deze categorie van militaire operaties zijn specifieke regels tot stand gekomen. Enkele voorbeelden zijn het verbod op aanvallen van burgers,² het verbod op aanvallen van burgerobjecten³ en het verbod op niet onderscheidende aanvallen,⁴ waaronder ook aanvallen die buitensporig veel bijkomend letsel of bijkomende schade veroorzaken vallen.⁵

Met de aandacht voor aanvallen, is relatief minder aandacht geweest voor militaire operaties die niet voldoen aan de definitie van aanval. Een aantal ontwikkelingen en trends maakt dat militaire operaties beneden de grens van aanval aandacht verdienen. Een daarvan is de opkomst en ontwikkeling van het cyberdomein. De mogelijkheden van steeds meer en snellere verbindingen, rekenkracht en opslagcapaciteit leidt tot meer cybertoeepassingen, niet alleen binnen de maatschappij maar ook voor militaire operaties.⁶ Er ontstaat een trend van *dematerialization* waarmee wordt bedoeld op “*the elimination of materials altogether for certain functions.*”⁷ Een voorbeeld kan dit verduidelijken. Als alle militairen van een eenheid uitgerust zijn met een *Global Positioning System* (GPS) met bijbehorende navigatieapparatuur en ze zijn getraind in het gebruik ervan, zal het aantal kompassen en (land)kaarten binnen die eenheid sterk afnemen of misschien wel helemaal verdwijnen. De afhankelijkheid van niet-fysieke (of virtuele) zaken zoals computergegevens

1 Aanvullend Protocol I art. 49 lid 1.

2 Aanvullend Protocol I art. 51 lid 2.

3 Aanvullend Protocol I art. 52 lid 1.

4 Aanvullend Protocol I art. 51 lid 4.

5 Aanvullend Protocol I art. 52 lid 5.

6 Onder cyberoperaties versta ik de toepassing van cybercapaciteiten door militaire en/of met militaire middelen om een specifieke doelstelling, namelijk een militair voordeel ten opzichte van de tegenstander te behalen, in of door gebruik van het cyberdomein.

7 Keulen 2018, p. 24.

en computerprogramma's voor bijvoorbeeld plaats- of routebepaling, wordt daarmee groter.

Indien militaire operaties vooral gericht zijn op of tegen personen en fysieke objecten, is kinetisch optreden⁸ vaak de eerste, en soms enige optie om een operatie te laten slagen. Bij militaire operaties tegen virtuele zaken hoeft kinetisch optreden niet de enige optie te zijn. Alhoewel kinetische operaties zeker tot de mogelijkheden behoren,⁹ bieden militaire operaties die niet voldoen aan de definitie van aanval, dus niet-gewelddadig of niet-kinetisch, gericht op of tegen virtuele zaken juist nieuwe mogelijkheden. Naarmate de afhankelijkheid van *bits* ten opzichte van *atoms* toeneemt zullen ook de mogelijkheden voor niet-kinetische militaire operaties op twee manieren groeien. Ten eerste zal een tegenstander, als gevolg van de toegenomen reken- en opslagcapaciteit van computers, de betere en snellere verbindingsmogelijkheden voor uitwisseling van gegevens en de trend van *dematerialization*, vaak afhankelijker worden van virtuele zaken en dus meer virtuele zaken hebben waarop militaire cyberoperaties gericht kunnen worden. Ten tweede zullen de mogelijkheden om zelf gebruik te maken van niet-fysieke zaken, bijvoorbeeld computerprogramma's, om een bepaald militair doel te bereiken, toenemen.

Aandacht voor niet-kinetische militaire operaties en de nieuwe mogelijkheden daarvoor binnen het cyberdomein is daarmee opportuun wat de verklaring is voor de centrale onderzoeksvraag van dit onderzoek: welke regels gelden in het humanitair oorlogsrecht voor militaire cyberoperaties die beneden de drempel van aanval, zoals gedefinieerd in artikel 49 lid 1 Aanvullend Protocol I, blijven? Om deze vraag te kunnen beantwoorden is in Hoofdstuk Twee een antwoord gegeven op de vraag waar, binnen het humanitair oorlogsrecht, de grens van aanval in traditionele zin ligt. Het antwoord op deze vraag luidt dat deze ondergrens van aanvallen wordt gevormd door operaties uitgevoerd met militairen en/of militaire middelen, die gericht zijn op fysiek letsel of schade, of die deze fysieke gevolgen hebben, welke in het kader van een gewapend conflict worden uitgevoerd met als doel een militair voordeel op de tegenstander te behalen. Militaire operaties zoals psychologische operaties¹⁰ of elektromagnetische operaties¹¹ die niet gericht zijn op fysiek letsel of schade, en deze fysieke gevolgen ook niet hebben, blijven beneden de drempel van aanval. De specifieke regels voor aanvallen uit het humanitair oorlogsrecht zijn dus ook niet van toepassing op deze militaire operaties.

Vervolgens is in Hoofdstuk Drie onderzocht welke regels uit het humanitair oorlogsrecht wél van kracht zijn op militaire operaties die beneden de drempel van aanval blijven. Hierbij is primair gekeken op het abstractieniveau van de grondbeginselen van het

8 De term 'kinetisch' verwijst hier naar het militaire optreden gebaseerd op het vrijlaten van kinetische energie in hoofdzaak veroorzaakt door explosies.

9 Zie bijv. Applegate, 2013 *The Dawn of Kinetic Cyber*.

10 *Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*, AAP-6 (2014)

11 *Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects*, AAP-6 (2014)

humanitair oorlogsrecht als richtinggevende beginselen voor militaire operaties die ten grondslag liggen aan de meer gedetailleerde en specifieke regels; militaire noodzaak, humaniteit, onderscheid, proportionaliteit en eervol gedrag. Dit leidde tot de volgende conclusies:

Militaire noodzaak geldt, net als bij aanvallen, als vereiste binnen het humanitair oorlogsrecht voor militaire operaties beneden de grens van aanval. Hierop moet wel een uitzondering gemaakt worden. Het vereiste van militaire noodzaak geldt alleen indien negatieve gevolgen voor de burgerbevolking, individuele burgers of burgerobjecten zijn te voorzien.¹²

Het grondbeginsel humaniteit geldt onverkort voor militaire operaties beneden de drempel van aanval. Dit geldt eveneens voor het grondbeginsel onderscheid. Toepassing van dit laatste grondbeginsel leidt bij militaire operaties beneden de drempel van aanval echter wel tot andere uitkomsten dan bij aanvallen. Beneden de grens van aanval treden verschillende gradaties van bescherming van personen en objecten op. Voor de algemene bescherming van burgers geldt dat, in tegenstelling tot aanvallen, militaire operaties beneden de grens van aanval gericht mogen zijn op burgers zolang deze burgers maar niet blootgesteld worden aan fysieke gevaren voortvloeiend uit deze militaire operaties. Daarnaast bestaat een bijzondere bescherming tegen operaties beneden de drempel van aanval voor een aantal categorieën personen met een rol binnen humanitaire hulpverlening, zoals medisch en religieus personeel. Deze categorieën personen zijn beschermd tegen alle militaire operaties beneden de drempel van aanval, die gericht zijn tegen het humanitair optreden of die dit optreden negatief beïnvloeden.

Voor objecten is het verschil in bescherming tussen aanvallen en militaire operaties beneden de drempel van aanval nog groter dan bij personen. Met uitzondering van de hierna genoemde categorieën genieten objecten niet de algemene bescherming tegen uit militaire operaties voortvloeiende fysieke gevaren die wel geldt voor personen. Militaire operaties beneden de drempel van aanval mogen niet alleen gericht zijn op objecten maar objecten mogen ook gebruikt worden voor militaire operaties, ook als deze objecten daardoor aan gevaar voor beschadiging en vernietiging worden blootgesteld. Objecten voor godsdienstige verering en culturele goederen genieten wel meer bescherming tegen militaire operaties beneden de drempel van aanval en mogen niet gebruikt worden als ze daardoor gevaar lopen op beschadiging of vernietiging. Objecten bedoeld voor humanitaire hulpverlening zoals medische formaties, medisch vervoer en instellingen voor civiele bescherming, zijn beschermd tegen militaire operaties beneden de grens van aanval, als deze gericht zijn tegen het humanitair optreden of die dit optreden negatief beïnvloeden.

■
¹² Een voorbeeld van negatieve gevolgen is dat bepaalde diensten zoals vervoersdiensten, tijdelijk niet of minder beschikbaar zijn als gevolg van een verplaatsing van een militaire eenheid waarvoor een bepaald gebied tijdelijk gesloten wordt voor alle verkeer.

De proportionaliteitsregel,¹³ die binnen het humanitair oorlogsrecht veelal gezien wordt als de uitwerking van het grondbeginsel van proportionaliteit, is een balans tussen de grondbeginselen militaire noodzaak en humaniteit, specifiek voor aanvallen. Deze proportionaliteitsregel geldt dus niet voor militaire operaties beneden de drempel van aanval. Door het ontbreken van ‘schade’ in de traditionele zin (fysieke schade), kan ook geen sprake zijn van nevenschade die buitensporig is in verhouding tot het militair voordeel. Eervol gedrag daarentegen geldt als grondbeginsel voor alle militaire operaties. In juridische zin kan dit laatste grondbeginsel een rol spelen bij de interpretatie van bestaande oorlogsrechtelijke regels, bijvoorbeeld bij de beoordeling of perfidie al dan niet verboden is.¹⁴ Daarnaast kan het grondbeginsel een bijdrage leveren bij operationele en morele vraagstukken,¹⁵ ook beneden de drempel van aanval. Het beginsel levert dan echter geen juridisch bindende verplichtingen op.

In Hoofdstuk Vier staat de deelvraag naar de ondergrens van aanval in het cyberdomein centraal. Bij de algemene uitleg over het cyberdomein is duidelijk gemaakt dat het cyberdomein bestaat uit een fysiek en een niet-fysiek deel. In het fysieke deel onderscheid ik fysieke personen en militair materieel die gebruik maken van het cyberdomein en fysieke hardware. Het niet-fysieke deel is door mij ingedeeld in de categorieën firmware, besturingsprogramma's, cyberidentiteiten, computerprogramma's en computergegevens. Deze indeling van de niet-fysieke componenten is aangebracht om te kunnen onderzoeken wat de gevolgen (kunnen) zijn wanneer een bepaalde categorie het doel is van een militaire cyberoperatie. Zodra een cyberoperatie namelijk (ook) fysiek letsel of fysieke schade veroorzaakt valt deze operatie in elk geval onder de definitie van aanval en daarmee buiten het bereik van dit onderzoek.

De constatering dat een cyberoperatie met fysiek letsel of schade als gevolg, een aanval is onder het humanitair oorlogsrecht, is feitelijk onomstreden. Het betreft hier dezelfde uitleg die ook bij aanval in traditionele zin is gehanteerd. Lastiger is de vraag of ook sprake kan zijn van een aanval in humanitair oorlogsrechtelijke zin, als geen fysiek letsel of schade optreedt als gevolg van een cyberoperatie. Het antwoord op deze vraag heb ik gevonden via twee subvragen, wat is de status van niet-fysieke componenten van het cyberdomein

13 Zoals gecodificeerd in bijv. art 51 lid 4 Aanvullend Protocol I: “Niet onderscheidende aanvallen zijn verboden”, gevolgd door lid 5b waarin is omschrijven wat als niet-onderscheidend dient te worden beschouwd: “aanvallen die, naar kan worden verwacht bijkomend verlies van mensenlevens onder de burgerbevolking, verwonding van burgers, schade aan burgerobjecten of een combinatie daarvan ten gevolge zullen hebben, in een mate die buitensporig zou zijn in verhouding tot het verwachte tastbare en rechtstreekse militaire voordeel.”

14 Perfidie is gedefinieerd als: “gedragingen die het vertrouwen wekken bij een tegenstander ten einde deze te doen geloven dat hij gerechtigd is tot bescherming krachtens de regels van het volkenrecht toepasselijk in geval van gewapende conflicten of dat hij verplicht is zodanige bescherming te verlenen, met de bedoeling dat vertrouwen te misbruiken.” Art. 37 Aanvullend Protocol I. In datzelfde art. 37 staat echter ook, “het is verboden een tegenstander te doden, te verwonden of gevangen te nemen door middel van perfidie.” Wat openblijft is de vraag of perfidie die niet leidt tot dood, verwonding of gevangenneming wel of niet is toegestaan.

15 Een voorbeeld is de toepassing van de proportionaliteitsregel bij aanvallen. De juridische verplichting bestaat uit het toepassen van deze regel. Bij het bepalen van de uitkomst, dat wil zeggen beoordelen of het te verwachten bijkomend verlies aan mensenlevens onder de burgerbevolking, verwonding van burgers, schade aan burgerobjecten of een combinatie daarvan niet buitensporig is in verhouding tot het verwachte tastbare en rechtstreekse militaire voordeel, zal de commandant ook operationele en morele argumenten meenemen.

en vervolgens wat moet worden verstaan onder schade aan deze niet-fysieke componenten waardoor de cyberoperatie die dit veroorzaakt kwalificeert als aanval?

De mogelijke antwoorden op de vraag naar de status van niet-fysieke componenten van het cyberdomein hebben geleid tot verschillende stromingen. De verdeeldheid is ingegeven door de vraag of deze componenten wel of niet een militair doel kunnen vormen. Volgens de algemeen aanvaarde opvatting bestaan twee soorten militaire doelen binnen het humanitair oorlogsrecht, combattanten (personen) en objecten. Aangezien niet-fysieke componenten van het cyberdomein in elk geval geen personen zijn, zullen ze hooguit als objecten moeten kwalificeren om een militair doel te kunnen vormen.

De traditionele opvatting is dat objecten zoals genoemd in artikel 52 Aanvullend Protocol I,¹⁶ 'zichtbaar en tastbaar' moeten zijn. Niet-fysieke componenten van het cyberdomein passen niet in deze traditionele opvatting van objecten. Omdat het belang van deze niet-fysieke componenten voor militaire operaties is toegenomen en zal blijven toenemen wordt vrij algemeen aangenomen dat ze uiteindelijk tot de term 'object' uit artikel 52 Aanvullend Protocol I zullen gaan behoren.¹⁷ Deze nieuwe uitleg is in mijn opinie nu al gerechtvaardigd door te kijken naar de context en het doel van de bepaling in artikel 52 Aanvullend Protocol I. De opvatting dat objecten 'zichtbaar en tastbaar' moeten zijn, is bedoeld om abstracte begrippen als "*civilian morale*" en "*population's willingness to fight*"¹⁸ buiten de definitie van militair doel te houden. De niet-fysieke componenten van het cyberdomein hebben echter veel meer overeenkomsten met fysieke objecten dan met genoemde abstracte begrippen. Ze kunnen bijvoorbeeld met behulp van technische hulpmiddelen zoals een computer met beeldscherm 'zichtbaar' gemaakt worden. Ook kunnen ze worden gekopieerd en gestolen.

Naast bovengenoemd argument om niet-fysieke componenten van het cyberdomein te beschouwen als objecten is er nog een ander doorslaggevend argument. Staten, als ultieme makers van het humanitair oorlogsrecht,¹⁹ hebben in andere rechtsgebieden geen bezwaar tegen uitbreiding van het begrip objecten met niet-fysieke zaken. Alhoewel het zeker niet zo is dat concepten uit een rechtsgebied automatisch doorwerken in andere rechtsgebieden, zijn de redenen om niet-fysieke componenten te beschouwen als objecten, namelijk een betere bescherming bieden aan zaken die een cruciale rol binnen de hedendaagse maatschappij vertolken, dwingendere dan de redenen om vast te houden aan de traditionele opvatting. Dit leidt tot mijn conclusie dat niet-fysieke componenten van

■
16 Aanvullend Protocol I, art. 52 lid 2 luidt: "Aanvallen dienen strikt tot militaire doelen te worden beperkt. Voor zover het objecten betreft, zijn militaire doelen uitsluitend die objecten die naar hun aard, ligging, bestemming of gebruik een daadwerkelijke bijdrage tot de krijgsvieringen leveren en waarvan de gehele of gedeeltelijke vernietiging, verovering of onbruikbaarmaking onder de omstandigheden van dat moment een duidelijk militair voordeel oplevert", mijn accentuering.

17 Zo schrijft bijvoorbeeld Schmitt, "*the unwillingness to treat data as an object because of it is not tangible, which I believe presently reflects *lex lata*, is unlikely to survive for long.*" Schmitt 2014a, p. 204.

18 Harrison-Dinniss 2015, p. 44.

19 Schmitt & Watts 2015, p. 193.

het cyberdomein anno 2019, binnen het humanitair oorlogsrecht gezien kunnen worden als objecten zodat de regels uit het humanitair oorlogsrecht aangaande aanvallen ook van toepassing kunnen zijn op niet-fysieke componenten van het cyberdomein.

Ook op de tweede vraag, wat moet worden verstaan onder schade in het humanitair oorlogsrecht om te kwalificeren als aanval, zijn diverse antwoorden mogelijk. Gevolgen in de vorm van fysiek letsel of fysieke schade leiden in elk geval tot kwalificatie als aanval. Na een analyse concludeer ik echter dat niet-fysieke gevolgen, zoals hinder, ongemak maar ook economische schade, niet gezien moeten worden als schade als gevolg van 'dadens van geweld' zoals bedoeld in de definitie van aanval. Hierdoor vallen militaire cyberoperaties die niet gericht zijn op of leiden tot fysieke gevolgen, niet binnen de definitie van aanval uit artikel 49 Aanvullend Protocol I.

Om te bezien wanneer cyberoperaties mogelijk kwalificeren als aanval heb ik, aan de hand van de *Confidentiality-Integrity-Availability* triade, onderzocht wanneer militaire operaties, gericht tegen niet-fysieke componenten van het cyberdomein, kunnen resulteren in fysieke gevolgen. Mijn conclusie luidt dat militaire operaties gericht tegen de integriteit van firmware, besturingsprogramma's, computerprogramma's en computergegevens, en de beschikbaarheid van alle virtuele componenten, fysieke gevolgen *kunnen* hebben. Het gevolg van deze conclusie is dat dergelijke militaire cyberoperaties daarmee, in potentie, kunnen voldoen aan de voorwaarden van aanval. Of inderdaad sprake is van een aanval zal afhangen van de omstandigheden van het geval, namelijk of daadwerkelijk fysieke gevolgen worden beoogd of op zullen treden.

Bovenstaande conclusies leiden ertoe dat het antwoord op de vraag naar de ondergrens van aanval in het cyberdomein als volgt luidt: de toepassing van cybercapaciteiten door militairen en/of met militaire middelen, die gericht zijn op fysiek letsel of schade, of die deze fysieke gevolgen hebben, welke in het kader van een gewapend conflict worden toegepast met als doel een militair voordeel op de tegenstander te behalen in, of door het gebruik van, het cyberdomein.

In Hoofdstuk Vijf staat de laatste deelvraag, en tevens hoofdvraag van dit onderzoek centraal. Welke regels gelden in het humanitair oorlogsrecht voor militaire cyberoperaties beneden de drempel van aanval? Net als in hoofdstuk Drie heb ik deze vraag op het abstractieniveau van de grondbeginselen van het humanitair oorlogsrecht beantwoord.

Het grondbeginsel militaire noodzaak moet aanwezig zijn bij militaire cyberoperaties beneden de grens van aanval zodra negatieve gevolgen voor burgers of burgerobjecten te verwachten zijn als gevolg van de cyberoperatie. Van de operatie moet dan een merkbaar militair voordeel te verwachten zijn om te voldoen aan dit grondbeginsel. Binnen vrijwel het hele humanitair oorlogsrecht is gezocht naar een balans tussen de grondbeginselen militaire noodzaak en humaniteit. Voor aanvallen is deze, zoals hiervoor aangegeven gevonden in de proportionaliteitsregel. Een zelfde soort afweging kan gemaakt worden

bij de bepaling van de balans tussen militaire noodzaak en humaniteit voor militaire cyberoperaties beneden de drempel van aanval. Vanwege het ontbreken van fysieke gevolgen zal, in vergelijking met aanvallen, minder inbreuk gemaakt worden op het grondbeginsel van humaniteit zodat ook minder stringente eisen gesteld hoeven te worden aan het te verwachten militaire voordeel om toch in balans te zijn.

Humaniteit als grondbeginsel is terug te vinden in vrijwel het gehele humanitair oorlogsrecht en is daarmee ook van toepassing op cyberoperaties beneden de grens van aanval. Een regel die (mede) gebaseerd is op dit grondbeginsel is de regel dat de keuze van methoden en middelen van oorlogvoering niet onbegrensd is.²⁰ Deze regel is een bevestiging dat in het hele humanitair oorlogsrecht, en niet alleen bij aanvallen, gezocht moet worden naar een balans tussen de grondbeginselen militaire noodzaak en humaniteit.

Voor het grondbeginsel onderscheid geldt bij de toepassing op cyberoperaties beneden de grens van aanval hetzelfde als voor traditionele militaire operaties. Voor personen betekent dit dat militaire cyberoperaties gericht mogen zijn op burgers zolang deze niet worden blootgesteld aan fysieke gevaren als gevolg van de cyberoperaties. Daarnaast bestaat een bijzondere bescherming tegen cyberoperaties beneden de drempel van aanval voor een aantal categorieën personen met een rol binnen de humanitaire hulpverlening zoals medisch en religieus personeel. Deze categorieën personeel zijn ook beschermd tegen militaire cyberoperaties beneden de grens van aanval die gericht zijn tegen het humanitair optreden of die dit functioneren negatief beïnvloeden.

Ook voor objecten, dit is inclusief de niet-fysieke componenten van het cyberdomein, geldt dat het grondbeginsel onderscheid voor cyberoperaties hetzelfde uitwerkt als voor traditionele militaire operaties beneden de drempel van aanval. Net als bij traditionele operaties kan ik een drietal categorieën onderscheiden. De eerste categorie bestaat uit objecten die geen algemene bescherming genieten tegen de uit militaire operaties voortvloeiende fysieke gevaren en gebruikt mogen worden voor militaire cyberoperaties beneden de drempel van aanval. De tweede categorie omvat objecten voor godsdienstige verering en culturele goederen die niet gebruikt mogen worden voor militaire cyberoperaties als ze daardoor blootgesteld zouden worden aan het gevaar voor vernietiging of beschadiging. De derde categorie zijn objecten bedoeld voor humanitaire hulpverlening, zoals medische formaties, medisch vervoer en instellingen voor civiele bescherming. Deze zijn beschermd tegen militaire cyberoperaties beneden de drempel van aanval als de cyberoperaties gericht zijn tegen het humanitair optreden of dit optreden negatief beïnvloeden.

Het grondbeginsel proportionaliteit is ook van kracht beneden de drempel van aanval. De proportionaliteitsregel, die wel geldt voor aanvallen, geldt echter niet bij militaire cyberoperaties beneden de drempel van aanval. Om toch het grondbeginsel van

■
²⁰ Deze regel is gecodificeerd in Aanvullend Protocol I, art. 35.

proportionaliteit toe te kunnen passen heb ik een afweging geformuleerd die gemaakt moet worden bij cyberoperaties beneden de drempel van aanval. Het doel van deze afweging is de grondbeginselen van militaire noodzaak en humaniteit met elkaar in balans te brengen waarbij de grondbeginselen onderscheid, proportionaliteit en eervol gedrag een ondersteunende rol vervullen. De afweging en de verplichting om deze afweging te maken zijn gebaseerd op de regel dat de keuze van methoden en middelen van oorlogvoering niet onbegrensd is, gecombineerd met de grondbeginselen van het humanitair oorlogsrecht. Deze door mij geformuleerde afweging luidt: de niet-fysieke gevolgen van een militaire cyberoperatie voor de burgerbevolking, individuele burgers, burgerobjecten of een combinatie daarvan, mogen niet buitensporig zijn in verhouding tot het te verwachten merkbare voordeel van de cyberoperatie.

Naast de in de vorige paragraaf geformuleerde afweging tussen de niet-fysieke gevolgen voor de burgerbevolking en het te verwachten militaire voordeel bestaat nog een verplichting, namelijk dat in de voorbereiding op, en tijdens de uitvoering van een militaire cyberoperatie beneden de drempel van aanval, alles gedaan moet worden wat 'praktisch uitvoerbaar' is om uit te sluiten dat de cyberoperatie fysieke gevolgen heeft, kan hebben of kan krijgen. Deze verplichting is erop gericht te voorkomen dat een geoorloofde militaire cyberoperatie alsnog verandert in een (mogelijk) ongeoorloofde (cyber)aanval. Wat 'praktisch uitvoerbaar' inhoudt, zal aan de hand van de omstandigheden van het geval te goeder trouw en op basis van gezond verstand moeten worden vastgesteld, ook wel aangeduid als de standaard van de "*reasonable military commander*".²¹

Bij militaire cyberoperaties beneden de drempel van aanval is het grondbeginsel eervol gedrag van toepassing maar levert geen juridische verplichtingen op. Het grondbeginsel kan wel behulpzaam zijn bij de interpretatie van concrete regels zoals het beoordelen van het grijze gebied tussen krijgslisten en strafbaar gestelde perfidie of de invulling van wat 'praktisch uitvoerbaar' is tijdens de voorbereiding en uitvoering van een cyberoperatie beneden de grens van aanval ter voorkoming van fysieke gevolgen.

Dat de ondergrens van aanval voor cyberoperaties niet anders is dan de ondergrens voor militaire operaties in traditionele zin betekent dat bovenstaande conclusies voor cyberoperaties binnen het humanitair oorlogsrecht ook breder toegepast kunnen worden. Zij zijn van toepassing op alle militaire operaties die de drempel van aanval, zoals gedefinieerd in artikel 49 Aanvullend Protocol I, niet halen. Dus ook op bijvoorbeeld psychologische, inlichtingen- en elektromagnetische operaties.

■
21 ICTY, Final Report to the Prosecutor 2000, par. 50.

Summary

Summary

Fighting a War without Using Violence: A Study of the Rules of International Humanitarian Law Regulating Military Cyber Operations below the Threshold of Attack

Over many years International Humanitarian Law has developed into the system of codified and customary rules that we now know. The purpose of International Humanitarian Law has always been, and continues to be, twofold. On the one hand it regulates hostilities, which includes posing limitations on the permitted methods and means of warfare. On the other hand, International Humanitarian Law protects persons that do not, or no longer participate in hostilities, and objects which do not have a direct military value in armed conflicts. This has resulted in a balance between the two primary principles of International Humanitarian Law, military necessity and humanity. To find this balance, the main focus is on the reduction of the horrors of war. This has resulted in the definition of a specific category of military operations referred to as attacks. Within International Humanitarian Law, attacks are defined as “acts of violence against the adversary, whether in offence or in defence”.²² This category of military operations is regulated by specific rules like the prohibition of attacking civilians,²³ civilian objects²⁴ or conducting indiscriminate attacks²⁵ which includes attacks resulting in disproportionate collateral damage.²⁶

A direct consequence of the focus on attacks is the relative lack of attention for military operations that do not fulfill the conditions for constituting an attack. A number of current developments and trends now mark the need for renewed attention for non-violent (non-kinetic) military operations. One such indicator is the quickly developing cyberdomain. The possibilities for more and better connections, computing power and storage capacity leads to more cyber-applications, not only for society but for military operations²⁷ as well. A mode of dematerialization emerges which can be described as “the elimination of materials altogether for certain functions.”²⁸ An illustrative example is a military unit equipped with Global Positioning System (GPS) devices. When the personnel of this unit is fully trained in using this equipment, the number of compasses and maps within the unit will diminish, and even possibly completely disappear. The dependency on non-physical (or virtual) elements, like computer-data and computer-programs for localization and navigation, will therefore increase.

■
22 Additional Protocol I art. 49 (1).

23 Additional Protocol I art. 51 (2).

24 Additional Protocol I art. 52 (1).

25 Additional Protocol I art. 51 (4).

26 Additional Protocol I art. 51 (5).

27 Cyber-operations are defined as the application of cyber-capabilities by military personnel and/or military means to achieve a specific military advantage over the opponent, in or by the use of the cyberdomain.

28 Keulen 2018, p. 24.

When military operations are directed mainly against persons and physical objects, a kinetic operation²⁹ often is the first, and sometimes the only option for success. For military operations directed against virtual elements, kinetic operations are not the only option. Although kinetic operations may remain one option,³⁰ military operations that do not fulfill the definition of attack, which means the use of non-violent or non-kinetic means, directed at non-physical elements offer new possibilities. With the growing dependency on bits over atoms, the possibilities for non-kinetic operations will increase in two ways. Firstly, as a result of more computing power and storage capacity, better connections for exchanging data and the mode of dematerialization, an opponent will often be more dependent on virtual elements and therefore have more virtual elements that can potentially be targeted by military cyber-operations. Secondly, the possibilities for states and other parties to an armed conflict to apply non-physical elements, like computer-programs themselves, to achieve military goals, will also increase.

Attention for non-kinetic military operations and the new possibilities offered by the cyberdomain is therefore opportune which explains the central question of this research: what rules of International Humanitarian Law apply to military cyber-operations that fall below the threshold of attack as defined in article 49 Additional Protocol I? To answer this question, Chapter Two defines the threshold of attack in International Humanitarian Law for traditional military operations. This threshold is 'operations achieved by military personnel or with military equipment, aimed at physical injury or damage or with these physical consequences, that are performed as part of an armed conflict with the objective to gain a military advantage over the opponent.' Military operations, like psychological operations³¹ or electromagnetic operations,³² that do not intend to have or do not result in physical consequences, remain below the threshold of attack. The specific rules of International Humanitarian Law on attacks do not apply to these military operations.

Chapter Three examines which rules of International Humanitarian Law apply to traditional military operations below the threshold of attack. This is done by looking at the basic principles of International Humanitarian Law which underlie all the more detailed and specific rules; military necessity, humanity, distinction, proportionality and chivalry as guiding principles in all military operations. The study led to the following conclusions.

Military necessity applies equally to attacks and military operations below the threshold of attack. It should be noted that the principle of military necessity is only applicable if negative consequences for the civilian population, individual civilians or civilian objects can be expected.



29 The term 'kinetic' refers to military operations based on the release of kinetic energy, mainly caused by an explosion.

30 Applegate, 2013, *The Dawn of Kinetic Cyber*.

31 *Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives*, AAP-6 (2014)

32 *Military action that exploits electromagnetic energy to provide situational awareness and achieve offensive and defensive effects*, AAP-6 (2014)

The principle of humanity is applicable in full to military operations below the threshold of attack. The same applies for the principle of distinction, but this last principle leads to different outcomes when applied to military operations below the threshold of attack, than with attacks. Below the threshold of attack, there are variations in protection between persons and objects. As far as general protection of the civilian population is concerned, attacks are forbidden but military operations below the threshold of attack may be directed at the civilian population as long as this population is not exposed to physical dangers arising from the military operations.

Besides the general protection, there is special protection for certain categories of persons such as medical and religious personnel. These categories of persons are protected from *all* military operations that are directed at, or have a negative influence on their humanitarian function.

For civilian objects, the difference in protection between attacks and other military operations is even greater than for persons. Civilian objects, with the exemption of the categories mentioned below, do not receive general protection against military operations below the threshold of attack. These operations can not only be directed at civilian objects, civilian objects may also be used for these military operations even if this means that they are exposed to the risk of damage or destruction. Civilian objects like cultural objects and places of worship enjoy more protection and are not allowed to be used for military operations below the threshold of attack if, as a result of these operations, the objects are exposed to the risk of damage or destruction. Civilian objects for humanitarian assistance, such as medical formations, medical transport and installations for civil defence, are protected from *all* military operations directed at, or have a negative influence on their humanitarian function.

The proportionality rule,³³ generally seen as the implementation of the principle of proportionality within International Humanitarian Law, is a balance between the principles military necessity and humanity specifically for attacks. The rule is not applicable to military operations below the threshold of attack. Because there is no damage, there can be no collateral damage that would be excessive in relation to the military advantage. Chivalry, on the other hand, applies to *all* military operations. This principle of International Humanitarian Law can play a legal role in the interpretation of existing rules, for instance in judging whether or not perfidy is prohibited.³⁴ Besides that, it can make a

33 As codified in Additional Protocol I art. 51 (4), "Indiscriminate attacks are prohibited" followed by art. 5b that states that indiscriminate attacks are (among others), "an attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

34 Perfidy is defined in Additional Protocol I art. 37 as: "Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with the intent to betray that confidence." The same art. 37 although also mentions that "it is prohibited to kill, injure or capture an adversary by resort to perfidy." That question that remains is whether perfidy that does not lead to 'kill, injure or capture' is also prohibited or not.

contribution to moral or operational problems³⁵ which are below the threshold of attack. In this last sense, the principle of chivalry will not result in binding legal obligations.

Chapter Four moves on to the cyberdomain and explains what the threshold of attack is in the cyber context. After a general description of the cyber domain, a classification into eight different components is made. In the physical domain persons, military material that uses the cyber domain and physical hardware are distinguished. The non-physical part of the cyberdomain comprises firmware, operating systems, cyber-identities, computer programs and data. This classification is chosen to determine the possible different consequences of military cyber-operations below the threshold of attack directed at certain components of the cyber domain. After all, as soon as a cyber-operation results in physical injury or damage, it will in any case meet the definition of attack and thus falls outside the scope of this research.

The above-mentioned observation that a cyber-operation that results in physical injury or damage qualifies as an attack is basically non-contentious. The reasoning is the same as for attack in traditional sense. More difficult to answer unequivocally is the question whether an attack can be defined according to International Humanitarian Law if there is no physical injury or physical damage as a result from a cyber-operation. To answer this question, two sub-questions are raised: first, what is the status of non-physical components of the cyber domain and second, what should be regarded as damage to these non-physical components in order for the military cyber-operation that caused the damage to qualify as attack?

The first sub-question has led to different opinions. The division is caused by the question: can non-physical components of the cyberdomain be military objectives? According to the well accepted interpretation of International Humanitarian Law, there are two types of military objectives, persons and objects. As non-physical components of the cyber domain are not persons, they have to qualify as objects in order to be a military objective.

The traditional view in International Humanitarian Law is that objects, as mentioned in Additional Protocol I article 52,³⁶ have to be 'visible and tangible'. Non-physical components of the cyberdomain do not fit this traditional view. Because the significance of these non-physical components is increased and will continue to do so, there is a persuasive assumption that these non-physical components will eventually be included

■
35 An example is the proportionality rule for attacks. The legal obligation is the application of this rule. The outcome, the commanders judgment whether or not the incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof is excessive in relation tot the concrete and direct military advantage, will depend operational and moral arguments.

36 Additional Protocol I art. 52: "Attacks shall be limited strictly to military objectives. In so far objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."

in the term ‘object’ as used in Additional Protocol I article 52.³⁷ This is possible by looking at the context and purpose of article 52. The concept that objects have to be ‘visible and tangible’ is to exclude abstract notions like “civilian morale” and “population’s willingness to fight”³⁸ from the definition of military objective. The non-physical components of the cyber domain, however, have far more similarities with physical objects than with such abstract notions. For example, they can be made visible with technical tools like a computer with a screen. They can also be copied or stolen.

On top of this argument, there is another pertinent argument. States, as the ultimate makers of international law,³⁹ do not object to incorporating non-physical elements into the definition of objects in other areas of law. While concepts from one area of law cannot necessarily be automatically applied in other areas, the reasons for including virtual components as objects, so as to provide enhanced protection to elements which play such a crucial role in contemporary society, are more compelling than those in favour of the traditional approach. My conclusion is therefore that in 2019, non-physical components of the cyber domain can be seen as objects in International Humanitarian Law. Therefore, the rules of International Humanitarian Law relating to attacks can apply to virtual components such as data.

The second sub-question as to what should be regarded as damage to non-physical components, can also be answered in different ways. Cyber-operations with consequences like physical injury or damage certainly qualify as attack. After an analysis of the different opinions, the conclusion is that non-physical consequences, like nuisance, inconvenience but also economic loss, do not qualify as damage resulting from acts of violence. This leads to the conclusion that cyber-operations that do not have the intention of causing physical damage or injury, or which result in physical damage or injury do not qualify as an attack under International Humanitarian Law.

To find out when physical damage can be foreseen as a result of a cyber-operation aimed at non-physical components of the cyber domain, the ‘Confidentiality-Integrity-Availability’ triad is used. The conclusion is that military cyber-operations aimed at the integrity of firmware, operating systems, computer programs and data and the availability of all virtual components can result in physical consequences. When seen in this light, these military cyber-operations can potentially fulfill the requirements of an attack. Whether or not this will actually be the case will depend on the aim or actual physical consequences of the operation.

The answers to the two sub-questions lead us to the following description of the threshold for attack in the cyber domain: the application of cyber-capacities by military personnel or

■
37 Schmitt 2014a, p. 204, “the unwillingness to treat data as an object because of it is not tangible, which I believe presently reflects *lex lata*, is unlikely to survive for long.”

38 Harrison-Dinniss 2015, p. 44.

39 Schmitt & Watts 2015, p. 193.

with military means that are aimed at physical injury or damage or lead to those physical consequences, during an armed conflict with the purpose of gaining a military advantage over the adversary in, or by the use of, the cyber domain.

Chapter Five answers the central question of this research namely “what rules of International Humanitarian Law apply to military cyber-operations that fall below the threshold of attack as defined in article 49 Additional Protocol I?” In the same way as in Chapter Three, the question will be answered at the abstraction level of the principles of International Humanitarian Law.

The principle of military necessity becomes applicable to military cyber-operations below the threshold of attack when negative consequences for civilians or civilian objects can be foreseen. A military advantage must be foreseen to fulfill this principle. Almost the entirety of International Humanitarian Law is about finding a balance between military necessity and humanity. For attacks this has resulted, as mentioned before, in the so called proportionality rule. A similar assessment can be made for cyber-operations below the threshold of attack. Because of the missing physical injury or damage, the negative impact will be smaller when compared with attacks. To reach a balance between military necessity and humanity, demands for military advantage will be less austere for military cyber-operations below the threshold of attack than for attacks.

Humanity as a principle is present throughout nearly the entire system of International Humanitarian Law and also applies to cyber-operations below the threshold of attack. One of many rules based on this principle is the rule that choice of methods and means of warfare is not unlimited.⁴⁰ This rule confirms that throughout International Humanitarian Law, and not just in attacks, the balance between military necessity and humanity must be found.

The principle of distinction equally applies to cyber-operations and traditional military operations below the threshold of attack. For persons this means that military cyber-operations can be directed at civilians as long as these civilians are not exposed to physical dangers. In addition to this protection there is a special protection for some specific categories of persons with a humanitarian aid role like medical and religious personnel. These categories personnel are also protected from military cyber-operations that are directed at, or have negative influence on their humanitarian function.

Just as for persons, the principle of distinction works out the same for cyber-operations and traditional military operations below the threshold of attack. As non-physical components of the cyber domain can be considered to be objects under International Humanitarian Law, they follow the classification of objects. As with traditional military operations, three categories can be distinguished. The first category consist of civilian objects that do not have general protection against cyber-operations below the threshold of attack and can be

■
40 This rule is codified in Additional Protocol I art. 35 (1)

used for these cyber-operations. The second category consist of cultural objects and objects for worship. These may not be used for military cyber-operations if, as a consequence of this use, they are exposed to possible damage or destruction. The third category are those objects intended for humanitarian aid like medical formations, medical transport and installations for civilian protection. These objects are protected from military cyber-operations that are directed at, or have negative influence on their humanitarian function.

The principle of proportionality applies, just as with attacks, for military operation below the threshold of attack. The proportionality rule however is limited to attacks. In order to apply the principle of proportionality, a deliberation is introduced with the purpose of balancing military necessity and humanity for cyber-operations below the threshold of attack. The other principles, distinction, proportionality and chivalry play a supporting role. The deliberation and the legal duty to weigh the principles follow from the rule that the methods and means of warfare are not unlimited in combination with the principles of International Humanitarian Law that apply also below the threshold of attack. This determination is expressed as follows: the non-physical consequences of a military cyber-operation for the civilian population, individual civilians or civilian objects or a combination thereof, may not be excessive in relation to the appreciable military advantage anticipated.

In addition to the above mentioned deliberation between the non-physical consequences for the civilian population and the appreciable military advantage there is another obligation. During the planning, preparation and execution of a cyber-operation below the threshold of attack, ‘everything feasible’ should be done to exclude that the cyber-operation has will, or could have physical consequences. This obligation has the purpose to avoid the possibility that a lawful cyber-operation could change into a (possible) illegal attack. What should be understood by ‘everything feasible’ is depending on all circumstances at the time and should be interpreted in good faith and with common sense, sometimes referred to as the standard of the “reasonable military commander.”⁴¹

For military cyber-operations below the threshold of attack, the principle of chivalry is applicable but does not result in legal obligations. This principle can however be helpful when interpreting specific rules of International Humanitarian Law like interpreting the gray area between ruses of war and perfidy, or to give a reasonable interpretation of ‘everything feasible’ during preparation and execution a cyber-operation below the threshold of attack.

Because the threshold of attack in traditional sense is not different from the threshold for cyber-attacks, the conclusions for cyber-operations below the threshold of attack can be implemented more widely and apply to all military operations that do not reach the threshold of attack as defined in article 49 Additional Protocol I, for example psychological, intelligence- and electromagnetic operations.

■
41 ICTY, Final Report to the Prosecutor 2000, par. 50.

Verdragen

Verdragen

Geneva Convention 1864

Convention for the Amelioration of the Condition of the Wounded in Armies in the Field. Geneva, 22 August 1864.

St Petersburg Declaration 1868

Declaration Renouncing the Use, in Time of War, of Certain Explosive Projectiles. Saint Petersburg, 29 November/11 December 1868.

Geneva Convention 1906

Convention for the Amelioration of the Condition of the Wounded in Armies in the Field. Geneva, 6 July 1906.

Hague Convention IV 1907

Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907.

Handvest Verenigde Naties

Handvest van de Verenigde Naties, San Francisco 26 juni 1945.

Statuut van het Internationaal Gerechtshof

Statuut van het Internationaal Gerechtshof, annex tot het Handvest Verenigde Naties, San Francisco 26 juni 1945.

Geneva Convention 1929

Convention for the Amelioration of the Condition of the Wounded in Armies in the Field. Geneva, 27 July 1929.

Verdrag I van Genève 1949

Verdrag van Genève voor de verbetering van het lot der gewonden en zieken, zich bevindende bij de strijdkrachten te velde, Genève 12 augustus 1949.

Verdrag II van Genève 1949

Verdrag van Genève voor de verbetering van het lot der gewonden, zieken en schipbreukelingen van de strijdkrachten ter zee, Genève 12 augustus 1949.

Verdrag III van Genève 1949

Verdrag van Genève betreffende de behandeling van krijgsgevangenen, Genève 12 augustus 1949.

Verdrag IV van Genève 1949

Verdrag van Genève betreffende de bescherming van burgers in oorlogstijd, Genève 12 augustus 1949.

Europees Verdrag voor de rechten van de mens 1950

Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, Rome 4 november 1950.

Cultureel goederen verdrag 1954

Verdrag inzake de bescherming van culturele goederen in geval van een gewapend conflict, Gravenhage 14 mei 1954.

Ruimteverdrag 1967

Verdrag inzake de Beginselen met Betrekking tot de Activiteiten van Staten bij de Verkenning en het Gebruik van de Kosmische Ruimte met inbegrip van de Maan en andere Hemellichamen, Londen, Moskou, Washington 27 januari 1967.

Verdrag van Wenen 1969

Verdrag van Wenen inzake het verdragenrecht, Wenen, 23 mei 1969.

Verdrag biologische wapens 1972

Verdrag tot verbod van de ontwikkeling, de produktie en de aanleg van voorraden van bacteriologische (biologische) en toxinewapens en inzake de vernietiging van deze wapens, Londen, Moskou en Washington, 10 april 1972.

Protocol I 1977

Aanvullend Protocol bij de Verdragen van Genève van 12 augustus 1949, betreffende de bescherming van slachtoffers van internationale gewapende conflicten (Protocol I), van 8 juni 1977.

Conventionele Wapen Verdrag (CCW 1980)

Verdrag inzake het verbod of de beperking van het gebruik van bepaalde conventionele wapens die geacht kunnen worden buitensporig leed te veroorzaken of niet-onderscheidende werking te hebben, Genève, 10 oktober 1980.

Statuut van Rome 1998

Statuut van Rome inzake het Internationaal Strafhof, Rome, 17 juli 1998.

1999 Second Hague Protocol

Second Hague Protocol for the Protection of Cultural Property in the Event of Armed Conflict, van 26 maart 1999.

Cybercrimeverdrag 2001

Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest 23 november 2001.

Protocol III 2005

Aanvullend Protocol III bij de Verdragen van Genève van 12 augustus 1949, betreffende de aanvaarding van een aanvullend onderscheidend embleem (Protocol III), van 8 december 2005.

Uitspraken

Uitspraken

International Court of Justice 1996

ICJ, legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996.

International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991

ICTY, The Prosecutor v. Tadic, IT-94-1-A, 2 oktober 1995.

ICTY, The Prosecutor v. Haradinaj et al., IT-04-84-T, 3 april 2008.

Hoge Raad

HR 23 mei 1921, NJ 1921, Elektriciteits-arrest.

HR 11 mei 1982, NJ 1982, 583, Giraal geld-arrest.

HR 13 juni 1995, NJ 1995, 365, ECLI: NL: HR: 1995: ZD0064, Pinpas-arrest

HR 3 december 1996, NJ 1997/574, ECLI: NL: HR: 1996: ZD0584, Computergegevens-arrest

HR 31 januari 2012, NJ 2012, 536, ECLI: NL: HR: 2012: BQ9251, RuneScape-arrest.

Literatuur

Geraadpleegde literatuur

Abbott 2014

F.M. Abbott, *Intellectual Property, International Protection Law*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2014 (updated).

Applegate 2013

S.D. Applegate, 'The Dawn of Kinetic Cyber', *5th International Conference on Cyber Conflict. Proceedings 2013*. Available on: https://ccdcoe.org/cycon/2013_proceedings/d2r1s4_applegate.pdf.

Arajärvi 2014

N. Arajärvi, *The Changing Nature of Customary International Law: Methods of Interpreting the Concept of Custom in International Criminal Tribunals*, London, Routledge 2014.

Arquilla & Ronfeldt 1997

J. Arquilla & D. Ronfeldt (red), *In Athena's Camp: Preparing for Conflict in the Information Age*, Washington, Rand National Defense Research Institute 1997.

Azarov & Blum 2011

V. Azarov & I. Blum, *Suspension of Hostilities*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2011 (updated).

Barlow 1996

J.P. Barlow, 'A Declaration of the independence of Cyberspace', Davos Switzerland Feb. 1996. Available on <https://www.eff.org/cyberspace-independence>.

Backstrom & Henderson 2012

A. Backstrom & I. Henderson, 'New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 Weapons Reviews', *International Review of the Red Cross* volume 94 number 886 2012, p. 483-531.

Beard 2014

J.M. Beard, 'Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and Target Under International Humanitarian Law', *Vanderbilt Journal of Transnational Law* volume 47 2014, p. 67-144.

Boothby 2009

W.H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford: Oxford university press 2009.

Bostrom 2014

N. Bostrom, *Superintelligence, Paths Dangers Strategies*, Oxford: Oxford university press 2014.

Bothe, Partch & Solf 1982

M. Bothe, K.J. Partch & W.A. Solf, *New Rules for Victims of Armed Conflicts*, The Hague: Martinus Nijhoff Publishers 1982.

Bothe, Partch & Solf 2013

M. Bothe, K.J. Partch & W.A. Solf, *New Rules for Victims of Armed Conflicts second edition*, The Hague: Martinus Nijhoff Publishers 2013.

Bothe 2011

M. Bothe, *Nuclear Weapons Advisory Opinion*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2011 (updated).

Brenner & Clarke 2010a

S.W. Brenner & L.L. Clarke, 'Civilians in Cyberwarfare: Conscripts', *Vanderbilt Journal of Transnational law* 43 (2010). Available at: http://works.bepress.com/susan_brenner/2.

Brenner & Clarke 2010b

S.W. Brenner & L.L. Clarke, 'Civilians in Cyberwarfare: Casualties', *SMU Science & Technology Law Review* 13,3 (2010). Available at: http://works.bepress.com/susan_brenner/3.

Brown & Metcalf 2014

G.D. Brown & A.O. Metcalf, 'Easier Said Than Done: Legal Reviews of Cyber Weapons', *Journal of National Security Law & Policy* volume 7,1 (2014), p. 115-128.

Brown 2016

G.D. Brown, 'Spying and Fighting in Cyberspace: What is Which?', *Journal of National Security Law & Policy* volume 8,3 (2016), p. 1-22.

Brownlie 2003

I. Brownlie, *Principles of Public International Law, Sixth Edition*, Oxford: university press 2003.

Bunk 2016

J.R.H. Bunk, 'The Protection of Intellectual Property in Cyber-Space under International Humanitarian Law during Cyber-Operations', *LLM International Public Law Thesis Leiden Law School*.

Chainoglou 2011

K. Chainoglou, *Psychological Warfare*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2011

Clapham & Gaeta, 2014

A. Clapham & P. Gaeta (red.), *The Oxford Handbook of International Law in Armed Conflict*, Oxford: university press 2014.

Cleiren, Crijns & Verpalen 2016

C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen (red), *Strafrecht tekst & commentaar 11e druk*, Deventer: Wolters Kluwer 2016.

Coolen 1998

G.L. Coolen, *Humanitair oorlogsrecht*, Deventer: Tjeenk Willink 1998.

Dessens 2014

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

Detter 2000

I. Detter, *The law of war (second edition)*, Cambridge: Cambridge university press 2000.

Diamond 2014

E. Diamond, 'Applying International Humanitarian Law to Cyber Warfare', *Institute for National Security Studies* July 2014. Available on <http://www.inss.org.il/uploadImages/systemFiles/05%20Applying.pdf>.

Dinstein 1989

Y. Dinstein (red), *International Law at a Time of Perplexity*, Dordrecht: Martinus Nijhoff Publishers 1989.

Dinstein 2004

Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge: Cambridge university press 2004.

Dinstein 2009a

Y. Dinstein, *Warfare, Methods and means*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2009 (updated).

Dinstein 2009b

Y. Dinstein, *Military Necessity*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2009 (updated).

Dinstein 2010

Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict second edition*, Cambridge: Cambridge university press 2010.

Dinstein 2012

Y. Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts', *Journal of Conflict & Security Law* (2012), Vol. 17 no 2, p. 261-277.

Dinstein 2013

Y. Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference', *International Law Studies – Volume 89* 2013, p. 276-287.

Dinstein 2014

Y. Dinstein, *Non-International Armed Conflicts in International Law*, Cambridge: Cambridge university press 2014.

Dinstein 2016

Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* third edition, Cambridge: Cambridge university press 2016.

Dörmann 2004

K. Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', in Karin Bystrom (red), *Proceedings of the International Experts Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, Stockholm 17-19 november 2004, Swedish National Defence College 2005. Available at: <https://www.icrc.org/eng/resources/documents/misc/68lg92.htm>.

Dörmann 2011

K. Dörmann, *Unlawful Combatants*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2011 (updated).

Doswald-Beck 1995

L. Doswald-Beck (red), *San Remo Manual on International Law applicable to Armed conflicts at sea*, Cambridge: Cambridge university press 2015.

Droege 2012

C. Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians', *International Review of the Red Cross* volume 94 number 886 2012, p. 533-578.

Ducheine 2008

P.A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding*, Nijmegen: Wolf Legal Publishers 2008.

Ducheine 2009

P.A.L. Ducheine, Rechtsregimes tijdens militaire operaties, *Ars Aequi juli/augustus* 2009, p. 490-497.

Ducheine & Pouw 2010

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

Ducheine & Voetelink 2011

P.A.L. Ducheine & J.E.D. Voetelink, Cyberoperaties: naar een juridisch raamwerk, *Militaire Spectator* jaargang 180 nummer 6 2011, p. 273-286.

Ducheine, Osinga & Soeters 2012

P.A.L. Ducheine, F. Osinga & J. Soeters (red), *Cyber Warfare Critical Perspectives*, The Hague: T.M.C. Asser Press 2012.

Ducheine & van Haaster 2013

P.A.L. Ducheine & J. van Haaster, Cyber-operaties en militair vermogen, *Militaire Spectator* jaargang 182 nummer 9 2013, p. 368-388.

Ducheine & van Haaster 2014

P.A.L. Ducheine & J. van Haaster, Fighting Power, Targeting and Cyber Operations, *6th International Conference on Cyber Conflict. Proceedings 2014*. Available on https://ccdcoe.org/cycon/2014/proceedings/dzrlsg_ducheinehaaster.pdf.

Ducheine & Arnold 2015

P.A.L. Ducheine & K. Arnold, Besluitvorming bij cyberoperaties, *Militaire Spectator* jaargang 184 nummer 2 2015, p. 56-70.

Ducheine 2016

P.A.L. Ducheine, oratie uitgesproken op 27 januari 2016. Available on http://www.oratiereeks.nl/upload/pdf/PDF-6825weboratie_Ducheine_-_DEF.pdf.

Ducheine, Schmitt & Osinga 2016

P.A.L. Ducheine, M.N. Schmitt & F.P.B. Osinga (red), *Targeting: The Challenges of Modern Warfare*, The Hague: T.M.C. Asser Press 2016.

Ducheine & Osinga 2017

P.A.L. Ducheine & F.P.B. Osinga (red), *Winning without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, The Hague: T.M.C. Asser Press 2017.

Evans 2010

M.D. Evans (red), *International Law, third edition*, New York: Oxford university press 2010.

Fleck 1973

D. Fleck, 'Ruses of War and Prohibition of Perfidy', *Military Law and the Law of War review* 1974, p. 269-314.

Fleck 2008

D. Fleck (red), *The handbook of international humanitarian law (second edition)*, New York: Oxford university press inc. 2008.

Fleck 2013a

D. Fleck (red), *The handbook of international humanitarian law (third edition)*, Oxford: Oxford university press 2013.

Fleck 2013b

D. Fleck, Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual, *Journal of Conflict & Security Law* (2013), Vol 18, No 2, p. 331-351.

Gervais 2012

M. Gervais, 'Cyber Attacks and the Laws of War', *Berkeley Journal of International Law* Volume 30, Issue 2 2012, p. 524-579.

Gill & Fleck 2012

T.D. Gill & D. Fleck, *The handbook of the international law of military operations*, Oxford: Oxford university press 2012.

Gill & Fleck 2015

T.D. Gill & D. Fleck, *The handbook of the international law of military operations second edition*, Oxford: Oxford university press 2015.

Goodman 2013

R. Goodman, 'The Power to Kill or Capture Enemy Combatants', *The European Journal of International Law* vol. 24 no 3, p. 819-853.

Gosnell Handler 2012

S. Gosnell Handler, 'The New Cyber Face of Battle: Developing a legal Approach to Accomodate Emerging Trends in Warfare', *Stanford Journal of International Law* 48 Winter 2012, p. 209-237.

Grand & Barker 2009

J.P. Grant & J. G. Barker (red), *Encyclopædic Dictionary of International Law, Third Edition*, New York, Oxford University Press 2009.

Gray 2013

C. Gray, *International Law and the Use of Force (third edition)*, Oxford: university press 2013.

Green 2000

L.C. Green, *The contemporary law of armed conflict (second edition)*, Manchester: Manchester University Press 2000.

Greenwood 1983

C. Greenwood, 'The Relationship between ius ad bellum and ius in bello', *Review of International Studies*, Vol. 9, No. 4 1983, p. 221-234.

Haaster, van & Roorda 2016

J. van Haaster & M. Roorda, 'The Impact of Hybrid Warfare on the Traditional Operational Rationale', *Militaire Spectator* jaargang 185 nummer 4 2016, p. 175-185.

Haaster, van 2018

J. van Haaster, *On Cyber*, Ph.D dissertatie Netherlands Defence Academy and University of Amsterdam 2018.

Harold, Libicki & Stuth Cevallos 2016

S.W. Harold, M.C. Libicki & A. Stuth Cevallos, *Getting to Yes with China in Cyberspace*, Washington, Santa Monica, Rand Corporation 2016.

Harrison-Dinniss 2011

H.A. Harrison-Dinniss, 'Attacks and Operations- The Debate over Computer Network 'Attacks'.' Paper presented at the conference :New technologies, Old Law: Applying International Law in a New technological Age, minerva Centre for Human Rights, The Hebrew University of Jerusalem. Available on http://www.academia.edu/4086617/Attacks-and_Operations_The_Debate_over_computer_network_attacks.

Harrison-Dinniss 2012

H. Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge: Cambridge university press 2012.

Harrison-Dinniss 2015

H. Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives', *Israel Law Review Volume 48 Issue 01*, p. 39-54.

Hathaway & Crootof 2012

O.A. Hathaway & R. Crootof, 'The law of Cyber-Attack', *California Law Review* vol. 100 2012, p. 817-886.

Hayashi 2010

N. Hayashi (red), *National Military Manuals on the Law of Armed Conflict (second edition)*, Oslo: Torkel Opsahl Academic Epublisher 2010.

Hayashi 2017

N. Hayashi, *Military Necessity*, PhD dissertatie universiteit van Leiden. Available on: <https://openaccess.leidenuniv.nl/handle/1887/48562>.

Hays Parks 1990

W. Hays Parks, 'Air war and the law of war', *Air Force Law Review* 32 1990, p. 1-225.

Heitschel van Heinegg & Epping 2007

W. Heitschel van Heinegg & Volker Epping (red.), *International Humanitarian Law Facing New Challenges*, Heidelberg: Springer-Verlag 2007.

Henckaerts & Doswald-Beck 2005

J.M. Henckaerts & L. Doswald-Beck, *Customary International Humanitarian Law, volume I: Rules*, Cambridge: Cambridge university press 2005.

Henderson 2009

I. Henderson, *The Contemporary Law of Targeting*, Leiden: Martinus Nijhoff Publishers 2009.

Homan 2005

K. Homan, 'Duel om de ruimte?', *Atlantisch Perspectief*, jaargang 29 no. 2, 2005, p. 17-22.

Ipsen 2010

Knut Ipsen, *Ruses of War*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2010 (updated).

Jachec-Neale 2015

A. Jachec-Neale, *The Concept of Military Objectives in International Law and Targeting Practice*, London: Routledge 2015.

Jensen 2013

E.T. Jensen, 'Cyber attacks: Proportionality and Precautions in Attack', *International Law Studies – Volume 89* 2013, p. 198-217.

Kalshoven & Zegveld 2011

F. Kalshoven & L. Zegveld, *Constraints on the waging of war (4th edition)*, Cambridge: Cambridge university press 2011.

Keulen 2018

R.J.F. van Keulen, *Digital force; disrupting life, liberty and livelihood in the information age*, Ph.D. dissertatie universiteit Leiden 2018. Available on: <https://openaccess.leidenuniv.nl/handle/1887/62050>.

Kilovaty 2016

I. Kilovaty, 'Virtual Vilolence, Disruptive Cyberspace Operations as Attacks under International Humanitarian Law', 23 *Michigan Telecommunications & Technology Law Review* 113, 2016, p. 113-147.

Koekkoek 2000

A.K. Koekkoek (red), *De grondwet, Een systematische en artikelsgewijs commentaar derde druk*, Deventer: W.E.J. Tjeenk Willink 2000.

Koh 2012

H. Koh, 'International Law in Cyberspace', *Harvard International Law Journal Online*, Volume 54 December 2012. Available on http://digitalcommons.law.yale.edu/fss_papers/4854.

Kolb & Hyde 2008

R. Kolb & R. Hyde, *An Introduction to the International Law of Armed Conflict*, Oxford: Hart publishing 2008.

Kooijmans 2002

P.H. Kooijmans, *Internationaal publiekrecht in vogelvlucht (negende druk)*, Deventer, Kluwer 2002.

Kurzweil 2005

R. Kurzweil, *The singularity is Near, When Humans transcend Biology*, London, Duckworth & Co. Ltd. 2005.

Larsen, Cooper & Nystuen 2013

K.M. Larsen, C. G. Cooper & G. Nystuen (red), *Searching for a 'Principle of Humanity' in International Humanitarian Law*, Cambridge: Cambridge University Press 2013.

Lauterpacht 1952

H. Lauterpacht (red), *Oppenheim's International Law, a Treatise vol. II Disputes, War and Neutrality (seventh edition)*, Edinburgh: Longmans 1952.

Lauterpacht 1955

H. Lauterpacht (red), *Oppenheim's International Law, a Treatise vol. I Peace (eighth edition)*, Edinburgh: Longmans 1955.

Lee, Assante & Conway 2016

R.M. Lee, M.J. Assante & T. Conway, 'Analysis of the Cyber Attack on the Ukrain Power Grid, Defence Use Case'. Available on: http://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Levie 1980 Volume 2

H.S. Levie, *Protection of War Victims: Protocol 1 to the 1949 Geneva Conventions Volume 2*, New York: Oceana Publications 1980.

Levie 1980 Volume 3

H.S. Levie, *Protection of War Victims: Protocol 1 to the 1949 Geneva Conventions Volume 3*, New York: Oceana Publications 1980.

Lewis 2014

J.A. Leweis, 'Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms', *Center for Strategic & International Studies*, February 2014. Available on <https://www.csis.org/analysis/liberty-equality-connectivity>

Libicki 2012

M.C. Libicki, 'Cyberspace is not a warfighting domain', *I/S: A Journal of Law and Policy for the Information Society*, volume 8, no 2 Fall 2012, p. 325-340.

Liivoja & McCormack 2012

R. Liivoja & T. McCormack, 'Law in the Virtual Battlespace: The Tallinn Manual and the *Jus in Bello*', *Yearbook of International Humanitarian Law* Volume 15, 2012, p. 45-58.

Liivoja & Chircop 2018

R. Liivoja & L. Chircop, 'Are Enhanced Warfighters Weapons, Means, or methods of Warfare?', *International Law Studies – Volume 94* (2018), p. 160-185.

Lin 2010

H.S. Lin, 'Offensive Cyberoperations and the Use of Force', *Journal of National Security Law & Policy* volume 4,1 (2010), p. 63- 86.

Lodder 2012

A. Lodder, 'De tien geboden van het internet', oratie uitgesproken op 30-03-2012. Beschikbaar op <https://research.vu.nl/en/publications/recht-rond-cyberwar>

Lubell 2013

N. Lubell, 'Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?', *International Law Studies – Volume 89* (2013), p. 252-275.

Mačák 2015

K. Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', *Israel Law Review* Volume 48 Issue 01, p. 55-80.

Matthee, Toebe & Brus 2013

M. Matthee, B. Toebe & M. Brus (red), *Armed Conflict and International Law: In Search of the Human Face*, The Hague: T.M.C. Asser Press 2013.

McCormack 2018

T. McCormack, 'International Humanitarian Law and the Targeting of Data', *International Law Studies – Volume 94* 2018, p. 221-240.

Melzer 2011a

N. Melzer, 'Cyberwarfare and International Law', *United Nations Institute for Disarmament Research (UNIDIR) resources paper*, Geneva 2011. Available on: <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>.

Melzer 2011b

N. Melzer, 'Cyber operations and Jus in Bello', *United Nations Institute for Disarmament Research (UNIDIR) resources paper*, Geneva 2011. Available on: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=143275>.

Nasu & McLaughlin 2014

H. Nasu & R. McLaughlin (red), *New Technologies and the Law of Armed Conflict*, The Hague T.M.C. Asser Press 2014.

Nollkaemper 2014

A. Nollkaemper, *Kern van het internationaal publiekrecht (zesde druk)*, Den Haag: Boom Juridische uitgevers 2014.

Ohlin, Govern & Finkelstein 2015

J.D. Ohlin, K. Govern & C. Finkelstein (red), *Cyberwar, Law and Ethics for Virtual Conflicts*, Oxford: Oxford University Press 2015.

Osinga 2016

F. Osinga, 'Hybrid Warfare en de uitdaging van de nieuwe geopolitieke rivaliteit', *Magazine Nationale veiligheid en crisisbeheersing*, 14e jaargang 2016, p. 16-21.

Owens, Dam & Lin 2009

W.A. Owens, K.W. Dam & H.S. Lin (red), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities*, Washington D.C. National Academies Press 2009.

Oxman 2007

B.H. Oxman, *Jurisdiction of States*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2007 (updated).

Petris 2016

S. Petris, 'Rethinking Proportionality in the Cyber Context', *Georgetown Journal of International Law* 2016, vol 47, p. 1431-1458.

Pictet 1952

J.S. Pictet (red), *Commentary I Geneva Convention for the amelioration of the condition of the wounded and sick in armed forces in the field*, Geneva: International Committee of the Red Cross 1952.

Pictet 1960a

J.S. Pictet (red), *Commentary II Geneva Convention for the amelioration of the condition of the wounded, sick and shipwrecked members of armed forces at sea*, Geneva: International Committee of the Red Cross 1960.

Pictet 1960b

J.S. Pictet (red), *Commentary III Geneva Convention relative to the treatment of prisoners of war*, Geneva: International Committee of the Red Cross 1960.

Pictet 1985

J.S. Pictet, *Development and Principles of International Humanitarian Law*, Dordrecht: Nijhoff 1985.

Pouw 2013

E. Pouw, *International Human Rights Law and the Law of Armed Conflict in the Context of Counterinsurgency, with a Particular Focus on Targeting and Operational Detention*. PhD Dissertatie Available on <http://dare.uva.nl/record/1/399596> Breda repografie NLDA.

Ratziwill 2015

Y. Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law*, Leiden Brill Nijhoff 2015.

Reed 2004

T. Reed, *At the Abyss: An Insider's History of the Cold War*, New York: Presidio Press 2004.

Rid 2012

T. Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, 35-1, p. 5-32.

Rid & McBurney 2012

T. Rid & P. McBurney, 'Cyber-Weapons', *Rusi Journal* 2012 vol 157 no 1, p. 6-13.

Roberts 2008

A. Roberts, 'The Equal application of the Laws of War: A Principle under Pressure', *International Review of the Red Cross* volume 90 number 872 2008, p. 931-962.

Rochester 2016

J.M. Rochester, *The new Warfare, Rethinking rules for an unruly world*, New York: Routledge 2016.

Rogers 2004

A.P.V. Rogers, *Law on the battlefield (Second edition)*, Manchester: Manchester university press 2004.

Rõigas 2015

H. Rõigas, 'An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?', Incyder News, February 10, 2015. Available on: <https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>

Rusinova 2011

V. Rosinova, *Perfidy*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2011 (updated).

Saathof 2018

R. Saathof, 'Chinese oorlogvoering met hybride karakteristieken. Hybride oorlogvoering vanuit een ander perspectief', *Militaire Spectator jaargang 187 nummer 5* 2018, p. 248-263.

Samonas & Coss 2014

S. Samonas & D. Coss, 'The CIA strikes back: Redefining Confidentiality, Integrity and availability in Security', *Journal of information System Security* Volume 10 issue 3 2014, p. 21-45.

Sandoz, Swinarski & Zimmermann 1987

Y. Sandoz, C. Swinarski & B. Zimmermann (red), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva: Martinus Nijhoff Publishers 1987.

Sassoli & Bouvier 2006

M. Sassoli & A.A. Bouvier, *How does Law Protect in War (second, expanded and updated version, volume I)*, International Committee of the Red Cross, Geneva 2006.

Sassoli 2013

M. Sassoli, *Combattants*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2013 (updated).

Schindler 2003

D. Schindler, 'International Humanitarian Law: Its Remarkable Development and its Persistent Violation', *Journal of the History of International Law* 5 2003, p. 165-188.

Schindler & Toman 2004

D. Schindler & J. Toman (red), *The Laws of Armed Conflicts (Fourth revised and completed edition)*, Leiden: Martinus Nijhoff Publishers 2004.

Schmitt 1999

M.N. Schmitt, 'Computer network attack and the use of force in international law: Thoughts on a normative framework', *The Colombia Journal of Transnational Law* 37 1999, p. 885-937.

Schmitt 2002

M.N. Schmitt, 'Wired Warfare: Computer network attack and jus in bello', *International review of the Red Cross* June 2002, vol. 84 p. 365-399.

Schmitt, Harrison-Dinniss & Wingfield 2004

M.N. Schmitt, H.A. Harrison Dinniss & T.C. Wingfield: 'Computers and War: The Legal Battlespace', Background Paper prepared for Informal High-Level Expert Meeting on Current Challenge to International Humanitarian Law, Cambridge June 25-27, 2004. Available on www.hpcrresearch.org/sites/default/files/publications/schmittetal.pdf.

Schmitt, Garraway & Dinstein 2006

M.N. Schmitt, C.H.B. Garraway & Y. Dinstein, *The Manual on the Law of Non-International Armed Conflict With Commentary*, San Remo, International Institute of Humanitarian Law 2006, www.iihl.org.

Schmitt & Pejic 2007

M.N. Schmitt & J. Pejic (red.), *International Law and Armed Conflict: Exploring the Faultlines*, Leiden: Martinus Nijhoff publishers 2007.

Schmitt 2010

M.N. Schmitt, 'Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance', *Virginia Journal of International Law* volume 50 issue 4, p. 795-839.

Schmitt 2012

M.N. Schmitt, *Essays on Law and War at the Fault Lines*, The Hague: T.M.C Asser Press 2012.

Schmitt & Heintschel von Heineg 2012

M.N. Schmitt & W. Heintschel von Heineg, *The Development and Principles of International Humanitarian Law*, Farnham: Ashgate Publishing Limited 2012.

Schmitt 2013

M.N. Schmitt (red.), *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge: Cambridge university press 2013.

Schmitt 2013a

M.N. Schmitt, 'Cyber Operations and the Jus in Bello: Key issues', *International Law Studies – Volume 87 International Law and the Changing Character of War*, p.89-110.

Schmitt 2013b

M.N. Schmitt, 'Wound, Capture, or Kill: A Reply to Ryan Goodman's The Power to Kill or Capture Enemy Combatants', *The European Journal of International Law* vol. 24 no 3, p. 855-861.

Schmitt 2014a

M.N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack', *International review of the Red Cross* June 2014, vol. 96 p. 189-206.

Schmitt 2014b

M.N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?', *Stanford Law and Policy review* 2014 vol 25, p. 269-299.

Schmitt 2015

M.N. Schmitt, 'The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision', *Israel Law Review Volume 48 Issue 01*, p 81-109.

Schmitt & Watts 2015

M.N. Schmitt & S. Watts: 'The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare', *Texas International Law Journal* 2015, Volume 50, Symposium issue 2, p. 189-231.

Schmitt 2017

M.N. Schmitt (red.), *Tallinn Manual 2.0 on the International Law applicable to Cyber Operations*, Cambridge: Cambridge university press 2017.

Schneider & Grinter 1998

B.R. Schneider & L.E. Grinter (red), *Battlefield of the Future, 21st Century Warfare Issues*, Alabama: Air University Press 1998.

Schneier 2014

B. Schneier, 'Sony made it easy, but any of us could get hacked', *The Wall Street Journal*, Dec 19 2014. available on <https://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701>.

Segal 2012

A. Segal, 'China, International Law, and Cyberspace', *The Diplomat*, 8 October 2012. Available on <http://thediplomat.com/2012/china-international-law-and-cyberspace>.

Shaw 2014

M.N. Shaw, *International Law, Seventh Edition*, Cambridge, Cambridge university press 2014.

Slay & Miller 2008

J. Slay & M. Miller, 'Lessons learned from the Maroochy Water Breach', IFIP International Federation for Information Processing, Volume 253, pp. 73-82. Available on <http://www.ifip.org/wcc2008/site/IFIPSampleChapter.pdf>.

Smith 2008

R. Smith, *The Utility of Force: The Art of War in the Modern World*, New York: Vintage books 2008.

Solis 2010

G.D. Solis, *The Law of Armed Conflict*, Cambridge: Cambridge University Press 2010.

Solis 2014

G.D. Solis: 'Cyber Warfare', *Military Law Review* Volume 219 Spring 2014, p. 1-52.

Solis 2016

G.D. Solis, *The Law of Armed Conflict Second Edition*, Cambridge: Cambridge University Press 2016.

Thomas & Cuvelier 1990

F. Thomas & B. Cuvelier, *Inleiding tot het humanitair recht*, Arnhem: Gouda Quint BV 1990.

Talbot & Jakeman 2009

J. Talbot & M. Jakeman, *Security Risk Management Body of Knowledge*, New Jersey: John Wiley & Sons Inc. 2009.

Tsagourias & Buchan 2015

N. Tsagourias & R. Buchan (red), *Research Handbook on International Law and Cyberspace*, Cheltenham, Edward Elgar Publishing 2015.

Valentino-DeVries & Yadron 2015

J. Valentino-DeVries & D. Yadron: 'Cataloging the World's Cyberforces', *Wall Street Journal (online)*. Available on <http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710>

Wang, Wang & Huang 2011

X. Wang, B. Wang & J. Huang., 'Cloud computing and its key techniques', 2011 *IEEE International Conference on Computer Science and Automation Engineering*, Shanghai 2011, p. 404-410.

Warden 1995

J.A. Warden: 'The Enemy As a System', *Airpower Journal* 9, no. 1 (Spring 1995), p. 40-55.

Watkin 2014

K. Watkin: 'Military Advantage: A Matter of "Value", Strategy, and Tactics', *Yearbook of International Humanitarian Law* Volume 17, 2014, p. 277-364.

Watts 2014

S. Watts: 'Law-of-War Perfidy', *Military Law Review* Volume 219 2014, p. 106-175.

Wen 2005

H. Wen et al, 'Countermeasures for GPS signal spoofing', available on http://67.225.133.110/~gbpprorg/mil/gps4/Wen_Spoof.pdf.

Wilmshurst 2012

E. Wilmshurst (red), *International Law and the Classification of Conflicts*, Oxford: Oxford University Press 2012.

Wingfield 2000

T.C. Wingfield, *The Law of Information Conflict, National Security Law in Cyberspace*, Virginia Aegis Research Corporation 2000.

Wolfrum 2011

R. Wolfrum, *Sources of International Law*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2011 (updated).

Woltag 2010

J.C. Woltag, *Cyber Warfare*, Max Planck Encyclopedia of Public International Law, <www.mpepil.com> 2010 (updated).

Woudenberg & Lijnzaad 2010

N. van Woudenberg & L. Lijnzaad (red), *Protecting Cultural Property in Armed Conflict, An Insight into the 1999 Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict*, Leiden, Martinus Nijhoff Publishers, 2010.

Wouters, De Man & Verlinden 2016

Wouters, De Man & Verlinden (red), *Armed Conflicts and the Law*, Cambridge, Intersentia Ltd 2016.

Zhang 2012

L. Zhang: 'A Chinese perspective on cyber war', *International review of the Red Cross* summer 2012, vol. 94 p. 801-807.

Ziolkowski 2013

K. Ziolkowski (red), *Peacetime regime for state activities in cyberspace, International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publications 2013.

Overige publicaties

Overige publicaties

Air and Missile Warfare Manual 2009

Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare*, Harvard University 2009. Available on <http://ihlresearch.org/amw/HPCRManual.pdf>.

AIV/CAVV advies Digitale oorlogvoering 2011

Adviesraad Internationale Vraagstukken advies 77/Commissie van Advies inzake Volkenrechtelijke Vraagstukken advies 22, Digitale Oorlogvoering, december 2011.

Canadian Law of Armed Conflict Manual 2001

Law of Armed Conflict at the operational and tactical levels, B-GJ-005-104/FP-021, aug 2001. Available on https://www.ficnl.org/fileadmin/_migrated/content_uploads/Canadian_LOAC_Manual_2001_English.pdf

CAVV advies identificatie van internationaal gewoonterechtelijk 2017

Commissie van Advies Volkenrechtelijke Vraagstukken advies nr. 29, De identificatie van internationaal gewoonterecht, november 2017.

Commentary on the HPCR Air and Missile Warfare Manual 2010

Program on Humanitarian Policy and Conflict Research, *Commentary on the HPCR Manual on the International Law Applicable to Air and Missile Warfare*, Harvard University 2010. Available on <http://ihlresearch.org/amw/CommentaryontheHPCRManual.pdf>.

DPH 2004

Second Expert Meeting on the Notion of Direct Participation in Hostilities, summary Report. <www.icrc.org>.

DPH 2005

Third Expert Meeting on the Notion of Direct Participation in Hostilities, summary Report. <www.icrc.org>.

DPH 2006

Fourth Expert Meeting on the Notion of Direct Participation in Hostilities, summary Report. <www.icrc.org>.

Explanatory Report to the Convention on Cybercrime 2001

Explanatory Report to the Convention on Cybercrime, European Treaty Series No 185, Budapest, 23 November 2001. Available on <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.

Final Report to the Prosecutor 2000

Final report to the Prosecutor by the committee established to review the NATO bombing campaign against the Federal Republic of Yugoslavia. Available on <http://www.icty.org/sid.10052>.

Handleiding Humanitair Oorlogsrecht 2005

Handleiding humanitair oorlogsrecht, Den Haag.

HCPR 2009A

Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge: Harvard university 2009.

HCPR 2009B

Humanitarian Policy and Conflict Research, *Commentary on the HCPR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge: Harvard university 2009.

ICRC 2011

International Committee of the Red Cross, *International humanitarian law and the challenges of contemporary armed conflicts*, report for the 31th International conference of the Red Cross and Red Crescent, Geneva, October 2011. Available on <http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf>.

ICRC 2012

Occupation and other Forms of Administration of Foreign Territory ICRC report on the Expert meeting, maart 2012 <www.icrc.org/eng/resources/documents/publication/p4094.htm>.

ICRC 2013

International Committee of the Red Cross, *handbook on International Rules governing Military Operations*, Geneva 2013.

ICRC 2015

International Committee of the Red Cross, *International humanitarian law and the challenges of contemporary armed conflicts*, Report Document prepared by the International Committee of the Red Cross, Geneva, October 2015. Available on: <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts>.

IIHL & ICRC 2003

International Institute of Humanitarian Law & International Committee of the Red Cross. *International Humanitarian Law and other Legal Regimes: Interplay in situations of Violence*. Available on https://www.icrc.org/eng/assets/files/other/interplay_other_regimes_nov_2003.pdf.

International Law Association 2000

Final Report of the Committee on Formation of Customary (general) International Law. *Statement of Principles tot the Formation of General Customary International Law*, London Report of the 69th Conference, 2000. pp. 712-777.

International Law Association 2010

Final Report on the meaning of Armed Conflict in International Law. Available on <http://www.ila-hq.org/en/committees/index.cfm/cid/1022>.

International law Association 2016a

Final Report of the Study Group on Cybersecurity, Terrorism, and International Law. Available on <http://www.ila-hq.org/index.php/study-groups>.

International law Association 2016b

Final Report of the Study Group on the Conduct of Hostilities in the 21th Century. Available on <http://www.ila-hq.org/index.php/study-groups?study-group-sID=58>.

Interpretive Guidance 2009

International Committee of the Red Cross, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, International Review of the Red Cross, volume 90 number 872, pp 991-1047.

JP 3-13

Information Operations, 27 November 2012 Incorporating Change 1 20 November 2014. Available on http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

JP 3-60

Joint Targeting, 13 April 2007. Available on https://www.aclu.org/files/dronefoia/dod/drone_dod_jp3_60.pdf.

JSP 383

The Joint Service Manual of the Law of Armed Conflict, edition 2004. Available on www.gov.uk/government/collections/jsp-383.

Juridisch Handboek Commandant 2009

Juridisch Handboek Commandant, Den Haag: Boom Juridische uitgevers, 2009.

Law of War Manual 2015

Department of Defense Law of Warfare Manual 2015. Available on www.defense.gov/Portals/1/Documents/pubs/law-of-war-manual-june-2015.pdf.

Law of War Manual 2016

Department of Defense Law of Warfare Manual 2015, updated dec 2016. Available on http://usnwc.libguides.com/ld.php?content_id=35155368.

LDP-1 2009

Militaire doctrine voor het landoptreden, Den Haag: Ministerie van Defensie 2009.

Lucerne report 1974

International Committee of the Red Cross, Conference of Government Experts on the Use of Certain Conventional Weapons (Lucerne, 24.9-18.10.1974), Geneva 1975.

MCDC 2017

Multinational Capability Development Campaign, Understanding Hybrid Warfare. Available on https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Nationaal Veiligheidsprofiel 2016

Een All Hazard overzicht van potentiële rampen en dreigingen die onze samenleving kunnen ontwrichten. RIVM 2016. Available on [https://www.nctv.nl/binaries/Nationaal Veiligheidsprofiel 2016_tcm31-232083.pdf](https://www.nctv.nl/binaries/Nationaal_Veiligheidsprofiel_2016_tcm31-232083.pdf).

NATO Standard AJP-01 2017

NATO Standard AJP-01 Allied Joint Doctrine Edition E Version 1, February 2017. Available on <https://standards.globalspec.com/std/10266919/ajp-01>

Nederlandse Defensie Doctrine 2013

Nederlandse Defensie Doctrine, Den Haag: Ministerie van Defensie 2013.

Operational Law Handbook 2014

Operational Law Handbook 2014. Available on www.loc.gov/rr/frd/military_law/pdf/operational-law-handbook.

RAND 2009

Foundations of Effective Influence Operations, A Framework for Enhancing Army Capabilities, Rand Corporation 2009. Available on: <https://www.rand.org/pubs/monographs/MG654.html>.

Symantec Security Response 2011

Symantec Security Response, W32.Stuxnet Dossier version 1.4 February 2011. Available on: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

TRADOC 525-7-8

TRADOC Phamplet 525-7-8, *Cyber Operations Concept Capability Plan 2016-2028*. Available on <https://fas.org/irp/doddir/army/pam525-7-8.pdf>.

TRADOC 525-8-6

TRADOC Phamplet 525-8-6, *Cyberspace and Electronic Warfare Operations 2025-2040*. Available on <https://fas.org/irp/doddir/army/pam525-8-6.pdf>.

UN A/C.1/53/3

Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General.

UN A/65/154

United Nations Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security, 20 July 2010.

UN A/66/152

United Nations Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security, 15 July 2011.

UN A/66/359

Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.

UN A/68/98

United Nations Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security, 24 June 2013.

UN A/69/723

Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.

UN A/RES//70/237

United Nations General Assembly Resolution adopted on 23 December 2015.

UN A/71/10

International Law Commission, report on the identification of customary international law chapter V, paras 50-63.

US JP-1

Doctrine for the Armed Forces of the United States, 25 March 2013. Available on www.dtic.mil/doctrine/new_pubs/jp1.pdf.

US JP 1-02

Dictionary of Military and Associated Terms, 8 November 2010 (As Amended Through 15 November 2015). Available on www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

US JP 1-03 (R)

Cyberspace Operations, 5 february 2013. Available on www.dtic.mil/doctrine/new_pubs/jp1_03.pdf.

