Faculteit Rechtsgeleerdheid
Universiteit Gent

Academiejaar 2015-2016

DE TOEPASSING VAN DE MARTENSCLAUSULE OP CYBEROORLOGEN

"Cyberwar": dringende nood aan regulering of nog sci-fi?

Masterproef van de opleiding
'Master in de rechten'

Ingediend door

Joris Depoorter
(studentennr. 01102324)

Promotor: Prof. Dr. Gert Vermeulen

Commissaris: Prof. Dr. Wendy De Bondt

INHOUDSTAFEL

WOORD VOORAF I

I. INLEIDING 1

II. DE MARTENSCLAUSULE 3
A. OORSPRONG EN BETEKENIS 3
B. GEBRUIK DOORHEEN DE JAREN 8
C. RELEVANTIE VOOR DIT ONDERWERP 13

III. CYBEROORLOG: EEN NIEUW SLAGVELD? 15
A. PROBLEMEN 15
B. DEFINITIES EN PROBLEMEN IN EN VAN DE GANGBARE TERMINOLOGIE 16
1. Gewapend geweld 17
2. Gewapende aanval 19
3. Cyberoorlog 22
4. Cyberspace 24
5. Cyberwapens 27
C. AANNAMES VOOR DEZE MASTERPROEF 28

IV. HET ALGEMEEN VERDRAGSRECHT 29
A. STRUCTUUR 29
B. DE TOEREKENBAARHEID AAN STATEN 30
1. Toerekenbaarheid 30
2. Inbreuk 33
3. Uitsluitingsgronden en herstel 36
4. Conclusie 37
C. HET TRANSNATIONAAL KARAKTER VAN CYBEROORLOGEN 38
1. Neutraliteit 39
2. Niet-internationale gewapende conflicten 40
3. Conclusie 41
D. CYBERAANVALLEN DOOR NIET-STATELIJKE ACTOREN 42
1. Niet-internationale gewapende conflicten 42
2. Niet-statelijke actoren 48
3. Cyberterrorisme 50
4. Conclusie 53
E. SPIONAGE EN DIPLOMATIEKE IMMUNITEIT 54
1. Relevantie 54
2. Spionage 55
a) Interne spionage 55
b) Extraterritoriale spionage 57
3. Diplomatieke immuniteit 60
4. Conclusie 61
F. RAAKVLAKKEN MET CYBERCRIME EN CYBERTERRORISME 62
1. Relevantie 62
2. Cybercrime als sluitstuk voor verschillende problemen 63
3. Conclusie 64

V. HET INTERNATIONAAL HUMANITAIR RECHT 64
A. DE TOEPASBAARHEID VAN HET INTERNATIONAAL HUMANITAIR RECHT 64
1. Ius ad bellum 65

2. Ius in bello *65*
B. DE MOGELIJKHEDEN TOT ZELFVERDEDIGING 66
1. Het recht op zelfverdediging: wanneer? *66*
2. Toegelaten middelen en limieten op het zelfverdedigingsrecht *72*
3. Collectieve zelfverdediging *74*
4. Terrorisme *75*
5. De rol van de VN Veiligheidsraad *77*
6. Conclusie *78*
C. HET GEBRUIK VAN NUCLEAIRE WAPENS 79
1. Probleemstelling *79*
2. Algemene regels rond kernwapens *81*
3. Is dit een reëel probleem? *86*
4. Conclusie *87*
D. VERBOD OP HET GEBRUIK VAN BEPAALDE WAPENS 88
1. Belang *88*
2. Voorbeelden met conventionele wapens *88*
3. Kan een cyberwapen zelf een verboden wapen uitmaken? *92*
4. Conclusie *94*
E. BESCHERMING VAN BEPAALDE GROEPEN PERSONEN EN OBJECTEN 95
1. Waarom worden bepaalde personen en objecten beschermd *95*
2. Relevantie op het vlak van cyberoorlog *95*
a) Personen 95
b) Objecten 99
3. Conclusie *103*

VI. MENSENRECHTEN 104
A. MENSENRECHTEN EN IHL 104
B. MENSENRECHTEN EN CYBEROORLOG 106
1. Afwijkingen van de bescherming geboden door mensenrechtenverdragen *106*
2. Waar houdt IHL op en beginnen de mensenrechten? *109*
3. Conclusie *110*

VII. CONCLUSIE 110
A. VERANTWOORDING VAN DE GEKOZEN THEMA'S 110
B. DE MARTENSCLAUSULE: DE RELEVANTIE VOOR CYBEROORLOG 111
C. EEN CYBERVERDRAG: IS HET NODIG? 111
D. EEN CYBERVERDRAG: IS HET DRINGEND? 113
E. EEN CYBERVERDRAG: IS HET MOGELIJK? 113
F. SLOTBESCHOUWING 114

BIBLIOGRAFIE I
A. WETENSCHAPPELIJKE ARTIKELEN EN LITERATUUR I
B. VERDRAGEN EN ANDERE PRIMAIRE RECHTSBRONNEN I
C. RECHTSPRAAK IV
D. RECHTSLEER VII
1. Artikels, bijdragen in naslagwerken, databanken … ..... *vii*
2. Boeken ..... *xiii*

VIII. BIJLAGEN I

WOORD VOORAF

Een thesis schrijven vergt veel werk, en niet alleen van de student die hem schrijft. Daarom wil ik vooral mijn ouders bedanken, voor alle steun die zij niet alleen tijdens dit onderzoek hebben gegeven, maar voor alles wat zij voor mij hebben gedaan, waardoor ik sta waar ik nu sta.

Verder wil ik ook mijn promotor, professor Gert Vermeulen, bedanken, om steeds snel te antwoorden op elke vraag, hoe dwaas die vraag achteraf ook leek.

Ten slotte kan ik niet anders dan mijn vrienden bedanken, vooral diegenen die samen met mij (figuurlijk) bloed, zweet en tranen hebben gelaten tijdens het schrijven van een masterproef aan de faculteit Rechtsgeleerdheid. Onze gezamenlijke ellende was een steun voor mij.

I. INLEIDING

1. "Cyberoorlog" klinkt voor de leek als een futuristische term, iets wat zich in de verre toekomst ooit kan afspelen, in een tijd van Skynet en Terminators[1]. De waarheid ligt echter veel dichter bij onze tijd: na de afluisterschandalen in 2013 (Het Verenigd Koninkrijk en de Verenigde Staten van Amerika hadden hun bondgenoten afgeluisterd)[2], het hevige debat (vooral in de VSA) tussen overheid en bedrijven zoals Facebook met als inzet de vrijheid van informatie en de bescherming van privacy[3], de vrij recente gevallen van hacking van Belgische, Vlaamse of Waalse regeringswebsites[4] en de sporadische akkoorden in verband met Cyberspace in het algemeen[5] tonen aan dat "cyberoorlog" en in het algemeen een uitbreiding van het recht der gewapende conflicten richting de digitale wereld een probleem vormt dat misschien beter nu wordt aangepakt. Minister van Defensie Vandeput was zelfs van mening dat België zelf cyberaanvallen zou moeten kunnen uitvoeren, wat hij ook in daden omzette door de dienst cyberbeveiliging juist meer mankracht te bieden, in tegenstelling tot besparingen elders[6].

2. Aan de andere kant heeft het Internationaal Publiekrecht al een standaard clausule ingebouwd, die voorziet dat nieuwe ontwikkelingen niet ongeregeld blijven. De zogenaamde "Martensclausule"[7] bepaalt immers dat, in geval een situatie niet geregeld wordt door een specifiek verdrag, het algemeen geldend verdrags- en internationaal recht van toepassing wordt, tot een later verdrag die situatie verder of anders regelt. In het geval dat cyberoorlog niet essentieel zou verschillen van de huidige, "conventionele" oorlogen, zou een specifiek verdrag niet nodig zijn en zou op deze bepaling kunnen teruggevallen worden. De vraag is echter of men nu reeds alle potentiele gevaren of problemen kan voorzien. Men kan zeker niet terugvallen op Statenpraktijk, gezien de recente opkomst van digitale oorlogsvoering[8]. Aangezien zowat alles nu is

[1] Zie *The Terminator*, 1984, James Cameron.
[2] W. DE SMEDT, "De onmacht van de waarschuwing", *De Juristenkrant*, 20 november 2013, 13.
[3] M. UNTERSINGER, "Cybersécurité: Barack Obama tend la main à la Silicon Valley méfiante", *Le Monde*, 13 februari 2015, lemonde.fr.
[4] G. STEVENS, "Website Waalse regering gehackt door Tunesische islamitische groepering", *De Standaard*, 10 april 2015, standaard.be; X, "Des sites gouvernementaux canadiens paralysés par une cyberattaque", *Le Monde*, 17 juni 2015, lemonde.fr.
[5] X, "Washington et Pékin négocient un accord de non-agression dans le cyberspace", *Le Monde*, 20 september 2015, lemonde.fr.
[6] LLO, "Belgisch leger moet ook zelf cyberaanvallen kunnen uitvoeren", *De Standaard*, 7 april 2015, standaard.be.
[7] Zie nr. 6 e.v.
[8] J.-C. WOLTAG, "Cyber Warfare", *Max Planck Encyclopedia of Public International Law*, Oxford Public International Law, mei 2010, opil.ouplaw.com, nr. 5 (hierna afgekort: MPEPIL en OPIL en WOLTAG, "Cyber Warfare").

aangesloten op een of ander digitaal systeem, is het ook mogelijk dat digitale oorlogsvoering op allerhande gebieden een impact heeft, zover zelfs dat de Russische Federatie van mening is dat "informatica-wapens" dezelfde vernietigingskracht zouden kunnen hebben als conventionele massavernietigingswapens[9].

3. Deze masterproef zal daarom deze problematiek onderzoeken. Het zal niet alleen bestuderen waar en hoe cyberoorlog een impact heeft op oorlogsvoering, maar ook op mensenrechten, humanitair recht en algemene, elementaire vraagstukken van internationaal publiekrecht. Deze studie kan evenwel nooit exhaustief zijn. Mede door het plaatsgebrek die deze masterscriptie met zich meebrengt, maar ook door het feit dat onmogelijk alle mogelijke gevolgen kunnen worden voorzien, zal verder onderzoek nodig zijn. Er moet ook worden gewaarschuwd dat er geen duidelijke lijn in de gekozen onderwerpen zit. De elementaire, belangrijkste vraagstukken van internationaal publiekrecht zullen zoveel mogelijk worden behandeld, maar verder zal de keuze afhangen van wat de huidige actualiteit, van wat tijdens het schrijven het meest relevant lijkt. Deze keuze lijkt weinig wetenschappelijk, maar gezien de enorme hoeveelheid gebieden waar cyberoorlog een impact kan op hebben, lijkt het onmogelijk om een eenvormig keuzebeleid te voeren.

4. Dit onderzoek zal voornamelijk aan de hand van klassieke rechtsbronnen gebeuren, met als eerste verdragen, gevolgd door *ius cogens* en statenpraktijk, aangevuld met doctrine. Hier moet meteen een verklaring komen: omdat het net het doel is van deze masterproef om na te gaan of een nieuw verdrag nodig is, zal geen enkel verdrag betreffende cyberoorlog kunnen geciteerd worden. Daarom zullen af en toe deducties moeten gebeuren vanuit de rechtsleer, rechtspraak of algemeen verdragsrecht, in plaats van argumenten te baseren op primair verdragsrecht. Aangezien dit onderwerp een duidelijk voorbeeld van internationaal publiekrecht is, zullen de meeste bronnen Engels- of Franstalig zijn. Vandaar dat er soms Engelstalige woordenschat in deze masterscriptie terug te vinden zal zijn, indien er voor een bepaalde term geen precieze Nederlandstalige vertaling beschikbaar is[10]. Er is een poging ondernomen om aan de hand van interviews met ministeries van defensie, organisaties zoals NAVO en ande-

[9] WOLTAG, "Cyber Warfare", nr. 5.
[10] Waar professor M. KRUITHOF tijdens de lessen Rechtsvergelijking (1ste Master) hard op hamerde: vertalen om te vertalen, zonder dat die vertaling de juiste draagwijdte weergeeft, is volgens hem een zonde.

ren meer inzicht te verwerven in het nut of onnut van een specifiek verdrag, maar door de gevoelige en gespecialiseerde materie zijn deze interviews minder informatief voor deze scriptie. Toch zijn enkele personen geïnterviewd[11].

5. Deze masterproef zal eerst de geschiedenis en de werking van de Martensclausule kort toelichten, om zich daarna op Cyberoorlog te focussen, te beginnen met een aantal definities. Uiteindelijk zal, op basis van de geselecteerde onderwerpen, aangegeven worden of, naar de mening van de schrijver, een specifiek verdrag wenselijk dan wel dringend nodig is, en of een dergelijk verdrag of dergelijke regulering überhaupt haalbaar is. Ten slotte zullen enkele voorstellen gegeven worden, over hoe enkele pijnpunten misschien opgelost kunnen worden.

II. DE MARTENSCLAUSULE

A. Oorsprong en betekenis

6. Tijdens de vredesconferentie van Den Haag in 1899, besprak de Russische diplomaat en advocaat in het internationaal recht Friedrich Martens in zijn verklaring de mogelijkheid om, in geval geen onmiddellijk verdrag tijdens die conferentie werd opgesteld, toch enige regulering van gewapende conflicten door te voeren[12]. Deze clausule was oorspronkelijk bedoeld om een impasse te voorkomen indien de kleinere staten niet tot een overeenkomst kwamen met de grootmachten van die tijd[13]. Voluit leest deze bepaling:

> *"Until a more complete code of the laws of war is issued, the High contracting parties think it is right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain*

[11] Zie correspondentie met: NATHALIE VAN RAEMDONCK, project manager voor het Centrum van Cyber Security België, afgestudeerd aan de Universiteit van Amsterdam als Master in Law and Politics of International Security met een masterproef over cyberoorlog (zie BIJLAGE 1 voor de correspondentie, BIJLAGE 2 voor haar Masterproef met betrekking tot cyberoorlog); de vragen aan de directeur van de Koninklijke Militaire Academie, Luitenant-Kolonel T. DEPREZ, die verwijst naar rechtsleer die hier wordt opgenomen (vooral de *Tallinn-manual*: zie BIJLAGE 3); De vragen aan de Nederlandse Adviesraad voor publiekrecht, die verwijst naar haar eigen advies van de CAVV (zie verder) en de antwoorden van het Ministerie van Defensie (die tot op het moment van printen nog niet ontvangen waren) (zie BIJLAGE 4), en de vragen aan professor SCHMITT, die algemeen wordt geciteerd wanneer het cyberaanvallen betreft, die de eindredactie van de *Tallinn-manual* op zich heeft genomen, maar die jammer genoeg niet kon antwoorden op mijn vragen gezien hij op dit moment aan een tweede versie van de *Tallinn-manual* werkt (zie BIJLAGE 5).

[12] J. VON BERNSTORFF, "Martens Clause", *MPEPIL*, OPIL, december 2009, opil.ouplaw.com, nr. 2 (hierna: VON BERNSTORFF, "Martens Clause").

[13] *Ibid*.

under protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of public conscience."[14]

Het is dus duidelijk dat deze clausule oorspronkelijk enkel bedoeld was om toch enige regulering te voorzien bij dit verdrag. Later is deze bepaling echter ruimer gebruikt,[15] onder andere in recentere verdragen van internationaal humanitair recht[16] en in procedures voor internationaalrechtelijke Hoven[17].

7. Een vrij groot probleem met deze clausule is het feit dat er geen algemeen aanvaarde interpretatie bestaat[18]. Dit verklaart waarom zowel enge als ruime interpretaties van de Martensclausule voorhanden zijn: in de engste vorm wordt deze bepaling gezien als een loutere bevestiging dat internationaal gewoonterecht steeds blijft gelden, terwijl de ruimste interpretatie betekent dat een gewapend conflict ook onder de regels van het algemeen internationaal publiekrecht valt[19]. Een *advisory opinion* van het Internationaal Gerechtshof betreffende nucleaire wapens[20] besteedde heel wat aandacht aan deze clausule, zonder evenwel een duidelijke positie in te nemen. De tussenkomsten van Staten en enkele afwijkende meningen bevestigen echter het debat over de Martensclausule[21]. De volgende paragrafen en ondertitels zullen deze verschillende standpunten toelichten, waarna op basis van deze toelichting een eigen standpunt in het interpretatiedebat zal worden gekozen.

8. De belangrijkste Staten waren over het algemeen niet bereid de Martensclausule een breed toepassingsgebied toe te kennen[22], althans niet op het gebied van nucleaire

[14] Preambule van het Verdrag betreffende de regels en gebruiken tijdens oorlog te land van 1899, Den Haag, par. 9 (hierna: Den Haag, 1899).
[15] VON BERNSTORFF, "Martens Clause", nr. 2.
[16] Zie VON BERNSTORFF, "Martens Clause", nr. 5-7: onder andere het Verdrag betreffende de regels en gebruiken tijdens oorlog te land van 1907, Den Haag (hierna: Den Haag 1907); het Protocol voor het verbod op het gebruik van verstikkende, giftige of andere gassen, en van bacteriologische methoden van oorlogvoering, Genève, 17 juni 1925 (hierna: Gifgasprotocol).
[17] Zie VON BERNSTORFF, "Martens Clause", nr. 8-12: onder andere in Nürembergtribunaal, *United States of America v. Alfried Felix Krupp von Bohlen un Albach et al.*, Nuremberg, 1948.
[18] R. TICEHURST, "The Martens Clause and the Laws of Armed Conflict", *International Review of the Red Cross*, nr. 317, 1997, www.icrc.org (hierna: TICEHURST, "The Martens Clause and the Laws of Armed Conflict")
[19] C. GREENWOOD, "Historical Development and Legal Basis" in D. FLECK (*ed.*), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, 28.
[20] ICJ, Advisory Opinion, *Legality of the threat or use of nuclear weapons*, 8 juli 1996, *I.C.J. Reports* 1996, p. 226 (hierna: *Nuclear Weapons-opinion*).
[21] TICEHURST, "The Martens Clause and the Laws of Armed Conflict".
[22] *Ibid.*

wapens. De Russische Federatie was van mening dat deze clausule overbodig was sinds het invoeren van de Verdragen van Geneve en de protocollen, aangezien die de *"more complete code of laws"* waarvan sprake is in de clausule, uitmaken[23]. Het Verenigd Koninkrijk weigerde aan de Martensclausule enig rechtseffect toe te kennen[24]. Het was van mening dat de clausule enkel kon verwijzen naar internationaal gewoonterecht, maar dat het zelf geen normatieve waarde had[25]. De regering van Nauru daarentegen benadrukte dat de Martensclausule "geen geschiedkundige rariteit" was[26], gesteund door Australië, Mexico, Iran, Maleisië en Zimbabwe[27]. Er kan dus gesteld worden dat de grootmachten in die tijd weinig tot geen waarde aan de Martensclausule toekenden, terwijl de stem van de kleinere Staten toch de clausule leken te erkennen.

9. De *advisory opinion* van het Hof leverde weinig concrete resultaten op betreffende de interpretatie van de clausule. De *dissenting opinions* werpen wel een duidelijker licht op de verschillende standpunten over de clausule. Het Hof zelf vernoemde de clausule onder "het internationaal gewoonterecht"[28], maar vermeldde enkel dat de Martensclausule, als onderdeel van het gewoonterecht, toepasselijk was op nucleaire wapens[29] en dat het een effectieve manier was om de snelle evolutie van oorlogsvoering aan te gaan[30]. De *dissenting opinion* van rechter SHAHABUDDEEN gaat evenwel dieper in op de Martensclausule. Hij is van mening dat het Hof gelijk heeft in de opinie dat die clausule onderdeel uitmaakt van het internationaal gewoonterecht[31]. De opinie van het Verenigd Koninkrijk[32], dat de clausule enkel zou verwijzen naar dat gewoonterecht, wijst de rechter af. Aangezien deze regel volgens het Hof een normatief karakter kent, legt het Staten dus een gedragswijze op. SHAHABUDDEEN merkt op dat het vreemd zou zijn om de clausule zo te interpreteren dat het enkel verwijst naar regels die niet tot de clausule of het verdrag waarin het voorkomt[33]. Het is niet enkel een verwijzing, maar een bepaling die volledig zelfstandig normen creëert.

[23] *Nuclear Weapons-opinion*, Written Statement van de Russische Federatie, 13.
[24] TICEHURST, "The Martens Clause and the Laws of Armed Conflict".
[25] *Nuclear Weapons-opinion*, Written Statement van het Verenigd Koninkrijk, 46-47.
[26] *Nuclear Weapons-opinion*, Written Statement van de overheid van Nauru, aanvraag tot *advisory opinion*, 16.
[27] VON BERNSTORFF, "Martens Clause", nr. 12
[28] *Nuclear Weapons-opinion*, par. 78, 84.
[29] *Ibid*., par. 87.
[30] TICEHURST, "The Martens Clause and the Laws of Armed Conflict"; *Nuclear Weapons-opinion*, par. 78.
[31] *Nuclear Weapons-opinion*, Dissenting opinion Judge Shahabuddeen, 183 (hierna: SHAHABUDDEEN).
[32] Zie *Supra*.
[33] SHAHABUDDEEN, 183.

10. SHAHABUDDEEN merkt op dat de clausule Staten principieel verplicht om de reeds bestaande beschouwingen van menselijkheid toe te passen, zelfs al zijn er geen specifieke bepalingen in enig verdrag terug te vinden[34]. In tegenstelling tot wat het Verenigd Koninkrijk beweert, moeten die verplichtingen niet elders in het humanitair recht worden gezocht na verwijzing door de Martensclausule, maar bevat de clausule zelf die verplichtingen. De rechter illustreert dit door het feit dat de Belgische delegatie op de vredesconferentie van Den Haag in 1899 slechts voor enkele clausules stemde, nadat de Martensclausule werd ingelast. Dit verklaart SHAHABUDDEEN door te verwijzen naar de zelfstandige normatieve kracht van de clausule: omdat die zelf bijkomende bescherming kon bieden, kon de Belgische delegatie met een gerust hart de andere clausules goedkeuren[35].

11. Rechter SHAHABUDDEEN propageerde dus een ruime interpretatie van de Martensclausule. Zijn opinie wordt bovendien bijgestaan door de *International Law Commission*, die ook van mening is dat, zelfs bij gebrek aan enig verdragsrecht, combattanten en burgers nog steeds beschermd worden door gewoonterecht, principes van menselijkheid en van "het dictaat van het publiek geweten"[36]. Indien de clausule irrelevant zou zijn, zoals de Russische Federatie beweerde[37], dan zou die bovendien niet meer herhaald zijn in het Verdrag van Geneve[38] en zijn protocollen[39]. Dit is echter toch het geval, en in het artikelsgewijze commentaar bij deze bepalingen wordt nog eens het belang van de clausule aangehaald, al was het maar om de snel veranderende technologieën van oorlogsvoering bij te blijven[40]. De rechtsleer zelf heeft verschillende standpunten over deze clausule ontwikkeld[41], die echter elk een

[34] SHAHABUDDEEN, 186.
[35] SHAHABUDDEEN, 187.
[36] *Rapport van de International Law Commision over het werk van zijn 46ste Sessie*, 2 mei 1994-22 juli 1994, A/49/10, 317.
[37] Zie nr. 8.
[38] Eerste verdrag van Geneve ter verbetering van de omstandigheden van de gewonden van legers te velde van 12 augustus 1949, Geneve, UNTS 31 (hierna: Verdrag van Geneve I.
[39] Protocol bij het Verdrag van Geneve betreffende de bescherming van slachtoffers van internationale gewapende conflicten van 8 juni 1977, Geneve, *UNTS* 3; Protocol bij het verdrag van Geneve betreffende de bescherming van slachtoffers van niet-internationale gewapende conflicten van 8 juni 1977, Geneve, *UNTS* 609 (hierna: Protocol I en Protocol II).
[40] H.-P. GASSER, S.-S. JUNOD, C. PILLOUD, J. DE PREUX, Y. SANDOZ, C. SWINARSKI, C.F. WENGER, B. ZIMMERMAN, J. PICTET (*voorz.*), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneve, Martinus Nijhoff Publishers, 1987, 38-39 (hierna: *Commentary*); zie ook T. MERON, "The Martens Clause, Principles of Humanity, and Dictates of Public Consience", *The American Journal of International Law*, vol. 94, 2000, 80 (hierna: MERON, "The Martens Clause, Principles of Humanity, and Dictates of Public Consience").
[41] Zie nr. 12.

ruimere interpretatie van de Martensclausule voorstaan[42]. Over het algemeen zou dus gesteld kunnen worden dat de – machtigste – Staten (misschien begrijpelijkerwijs) voorstander zijn van een zo restrictief mogelijke interpretatie van de Martensclausule, terwijl de rechtsleer, (weinige) rechtspraak en de verdragen van Geneve een ruime(re) interpretatie voorstaan.

12. De rechtsleer heeft een aantal verschillende methodes ontwikkeld om deze interpretatieproblematiek aan te pakken[43]. Een van deze methodes ziet de Martensclausule als een bescherming van het humanitair recht: het voorziet in het argument dat wat niet per se verboden wordt door een verdrag, ook niet per se toegelaten is[44]. Bij deze visie moet een opmerking worden geplaatst: dit is in feite het tegenovergestelde van een principe dat in de *Lotus*-zaak werd ingevoerd[45]. In deze zaak werd geoordeeld dat een actie door een Staat, die niet per se wordt verboden, geacht wordt rechtmatig te zijn. De Martensclausule heeft dit principe dus omgedraaid wat betreft internationale gewapende conflicten[46]. In deze eerste opvatting zorgt de Martensclausule ervoor dat, in geval van twijfel, het humanitair recht consistent toegepast wordt met de principes van menselijkheid en de "dictaten van het publiek geweten"[47]. De clausule kan echter niet gebruikt worden om zelfstandig bepaalde praktijken te verbieden of af te keuren[48].

13. Een andere interpretatie ziet deze 'principes van menselijkheid en dictaten van het publiek geweten' als aparte bronnen van internationaal recht, die moeten onderscheiden worden van verdragsrecht of gewoonte. Deze regels zijn dan ontsproten aan oorspronkelijk morele normen, die voordien geen enkele normatieve waarde hadden voor hun 'transformatie' naar geldend recht via de Martensclausule, terwijl hun aanvaarding vaak gebeurt door de herhaalde invoering van die normen in verdragen of

[42] VON BERNSTORFF, "Martens Clause", nr. 13.
[43] *Ibid*.
[44] MERON, "The Martens Clause, Principles of Humanity, and Dictates of Public Consience", 87.
[45] PCIJ, *Frankrijk vs. Turkije*, 1927, ser. A nr. 10 (hierna: *Lotus*-case).
[46] M. BOURBONNIERE, L. HAECK, "Jus in Bello Spatiale", *Air & Space Law*, vol. XXV, 2000, 3.
[47] Voor verdere uitleg bij deze termen: zie MERON, "The Martens Clause, Principles of Humanity, and Dictates of Public Consience". Aangezien zij weinig praktische meerwaarde bieden voor deze Masterproef, wordt hier niet dieper op ingegaan. Het volstaat om het 'publiek geweten' te omschrijven als de algemene consensus van het publiek, de *vox populi*, langs de ene kant, en de *opinio juris*, de statenpraktijk aan de andere kant: het 'geweten', de consensus van wat mag en niet mag bij 'het publiek'. Principes van menselijkheid hoeven weinig extra uitleg, gezien hun aanhoudend benadrukt belang in tijden van oorlog.
[48] MERON, "The Martens Clause, Principles of Humanity, and Dictates of Public Consience", 88.

andere internationaalrechtelijke instrumenten[49]. De clausule voorziet in deze visie dus dat gewoonterecht geldt als er geen specifiek verdrag is, maar apart daarvan ook de werking van deze 'principes en dictaten'. Deze visie werd echter sterk aangevallen door CASSESE, die benadrukt dat geen enkel internationaal gerechtshof zich ooit op deze vermeende bronnen heeft beroepen[50].

14. CASSESE zelf ziet geen nieuwe bronnen van internationaal recht, maar meent dat de Martensclausule binnen de bestaande bronnen de *opinio juris* in het humanitair gewoonterecht sterker benadrukt[51]. Deze benadering wil de vereiste van Statenpraktijk verminderen, om sneller tot internationaal gewoonterecht te kunnen komen bij nieuwe ontwikkelingen op het gebied van oorlogsvoering[52]. CASSESE is van oordeel dat de snelle ontwikkeling van technologieën een enorm gevaar voor burgers kan opleveren, wat het verminderd belang van de statenpraktijk zou rechtvaardigen. Wat betreft de juridische argumenten, baseert hij zich ten eerste op het principe dat elke juridische clausule zo geïnterpreteerd moet worden dat die effect sorteert, wat via deze visie het geval is. Ten tweede meent hij dat, gezien de wijdverspreide internationale aanhang die de clausule kreeg, er enig juridisch gevolg aan moet worden gegeven[53].

B. Gebruik doorheen de jaren

15. In dit deel zal kort worden nagegaan of en waar de Martensclausule überhaupt wordt gebruikt. Dit kan mee het belang (of juist niet) van de clausule aantonen, naast eventuele interpretatievragen in de verschillende conventies. Enige verduidelijking bij de verdragen zal worden gegeven, maar aangezien dit vrij ver buiten de draagwijdte van deze masterproef valt, zal er niet diep op ingegaan worden.

16. De Martensclausule zag zoals gezegd voor het eerst het daglicht in het Verdrag van Den Haag van 1899. Het werd vervolgens identiek overgenomen in de preambule

[49] G. SPERDUTTI, *Lezioni di diritto internazionale*, Milaan, Vari, 1958, 68-74
[50] A. CASSESE, "The Martens Clause: Half a Loaf or Simply Pie in the Sky?", *EJIL*, vol. 11, 2000, 208 (hierna: CASSESE, "The Martens Clause: Half a Loaf or Simply Pie in the Sky?").
[51] VON BERNSTORFF, "Martens Clause", nr. 13; CASSESE, "The Martens Clause: Half a Loaf or Simply Pie in the Sky?", 214.
[52] CASSESE, "The Martens Clause: Half a Loaf or Simply Pie in the Sky?", 214.
[53] CASSESE, "The Martens Clause: Half a Loaf or Simply Pie in the Sky?", 214-215.

van het Verdrag van Den Haag van 1907[54]. Dit is vrij logisch, gezien beide conferenties nauw bij elkaar aanleunden[55]. De clausule werd ook in enigszins gewijzigde en fragmentaire vorm opgenomen in de reeds vernoemde preambule van het Protocol op het verbod van biochemische wapens van 1925[56]. Indien men paragraaf 1 en 3 van deze preambule samen leest, kan men daaruit het principe terughalen dat, aangezien gifgas veroordeeld wordt door de "beschaafde wereld", het verbod deel uitmaakt van het internationaal recht, bindend door de statenpraktijk en 'het geweten':

> *"Whereas the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids materials or devices, has been justly condemned by the general opinion of the civilized world; and […]*
> *To the end that this prohibition shall be universally accepted as a part of international law, binding alike the conscience and the practice of nations;"*[57]

Hoewel dit ver van de oorspronkelijke bewoording van de clausule ligt, kunnen er toch enkele bekende elementen teruggevonden worden, die deze preambule in de lijst van toepassingen verantwoorden. Zo oordeelt de preambule dat het gebruik van gifgas veroordeeld wordt door de opinie van de 'beschaafde wereld', wat uit statenpraktijk en 'het dictaat van publiek geweten'[58] bestaat. Verder stelt de tekst dat het verbod de statenpraktijk uitmaakt, aldus verwijzend naar internationaal gewoonterecht[59]. Hieruit wordt dan wel de Martensclausule afgeleid, maar dit is eigenlijk overbodig, aangezien de preambule zelf aangeeft dat dit al geregeld wordt door het internationaal gewoonterecht. Het kan echter nuttig zijn voor staten die dit protocol niet ratificeren: zij blijven, door de Martensclausule die aangeeft dat bij gebrek aan verdrag gewoonterecht blijft gelden, gebonden aan dat gewoonterecht.

[54] Preambule van Den Haag 1907, par. 8; die samen met de Annex: Reguleringen die de regels en gebruiken tijdens oorlog te land respecteren, het Verdrag van Den Haag IV vormen.
[55] VON BERNSTORFF, "Martens Clause", nr. 5.
[56] Zie nr. 6; voetnoot 16.
[57] www.icrc.org.
[58] Zie nr. 12 e.v.
[59] Art. 38, 1.b van het Statuut betreffende het Internationaal Gerechtshof van 24 oktober 1945, San Francisco.

17. Na de Tweede Wereldoorlog werd de clausule ingeschreven in de problematiek rond opzegging van de Verdragen van Geneve[60]. Hoewel alweer niet letterlijk wordt teruggegrepen naar de oorspronkelijke bewoordingen, komt het opnieuw neer op het gebruik van de clausule:

> *"The denunciation shall have effect only in respect of the denouncing Power. It shall in no way impair the obligations which the Parties to the conflict shall remain bound to fulfil by virtue of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of the public conscience"*[61]

Opnieuw komt dit overeen met een verwijzing naar het internationaal gewoonterecht, in geval van opzegging van dit verdrag. Nog meer dan in het Protocol betreffende het verbod op gifgas vermeldt dit artikel de 'wetten van menselijkheid en de dictaten van het publiek geweten'. Ook hier geldt dus dat het algemeen internationaal gewoonterecht blijft gelden, ook zonder de Verdragen van Geneve. De commentaren bij alle artikels vermelden trouwens dat, hoewel het vanzelfsprekend lijkt, deze clausules toch belangrijk zijn, alhoewel de commentatoren van mening zijn dat deze bepalingen beter in de preambule zouden opgenomen zijn[62].

18. Zoals reeds vermeld[63] werd de Martensclausule ook opgenomen in de Protocollen bij de Verdragen van Geneve:

> *"In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom,*

[60] VON BERNSTORFF, "Martens Clause", nr. 5; Art. 63(4) Verdrag van Geneve I, art. 142(4) Verdrag van Geneve III, art. 158(4) Verdrag van Geneve IV, www.icrc.org. In de aansluitende commentaar van het International Committee of the Red Cross wordt steeds verwezen naar de Haagse vredesconferenties van 1899 en 1907 en aldus de Martensclausule: icrc.org. Voor de gedrukte versie: J.S. PICTET (*ed.*), *Commentary – I Geneva Convention for the amelioration of the condition of the wounded and sick in armed forced in the field*, International Committee of the Red Cross, Geneve, 1952, 413; J.S. PICTET (*ed.*), *Commentary – III Geneva Convention Relative to the treatment of prisoners of war*, International Committee of the Red Cross, Geneve, 1960, 648; J.S. PICTET (*ed.*), *Commentary – IV Geneva Convention Relative to the protection of civilian persons in time of war*, International Committee of the Red Cross, Geneve, 1958, 625.
[61] Zie voetnoot 60, de bewoording is dezelfde in elk artikel.
[62] Zie de commentaren opgelijst in voetnoot 60.
[63] Zie nr. 11.

from the principles of humanity and from the dictates of public conscience."[64]

"Recalling that, in cases not covered by the law in force, the human person remains under the protection of the principles of humanity and the dictates of the public conscience"[65]

Zoals hierboven beschreven, zijn ook hier de nodige elementen terug te vinden: de opmerking dat, bij gebrek aan verdrag, het algemeen internationaal gewoonterecht blijft gelden (Protocol I), net als de 'principes van menselijkheid en de dictaten van het publiek geweten'. Hoewel het gewoonterecht niet wordt vermeld in Protocol II, benadrukt het artikelsgewijze commentaar van het Rode Kruis dat dit niet betekent dat gewoonterecht niet speelt[66]. Men was er in die tijd van overtuigd dat niet-internationale gewapende conflicten te recent waren om al enig gewoonterecht te doen ontstaan[67]. In tegenstelling tot de Verdragen van Geneve wordt de clausule nu echter opgenomen in het Protocol, weliswaar niet in de Preambule van Protocol I, maar wel in het eerste artikel. Het artikelsgewijze commentaar verklaart dit door te benadrukken dat het onmogelijk is een exhaustieve codex van de regels rond oorlogsvoering in te voeren[68], terwijl men in die periode ook al voorzag dat niet alle ontwikkelingen op het gebied van oorlogsvoering te voorzien zijn[69].

19. Ten slotte kan nog het Verdrag betreffende het verbod of beperking op het gebruik van bepaalde conventionele wapens die geacht worden excessief verwondend te zijn of die non-discriminerende effecten hebben worden vermeld[70]. Paragraaf 5 van de preambule verwoordt in opnieuw gelijkaardige termen het volgende:

"Confirming their determination that in cases not covered by this Convention and its annexed Protocols or by other international agreements,

[64] Art. 1(2) Protocol I.
[65] par. 4 Preambule Protocol II.
[66] *Commentary*, 1341.
[67] *Ibid*.
[68] *Commentary*, 39.
[69] *Ibid*.
[70] Verdrag betreffende het verbod of het gebruik van bepaalde conventionele wapens die geacht kunnen worden buitensporig te verwonden of die zonder onderscheid werken van 10 oktober 1980, Geneve, *UNTS* 171 (hierna: Verdrag betreffende het verbod op bepaalde wapens).

> *the civilian population and the combatants shall at all times remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience,"*

Ook hier is het internationaal gewoonterecht terug te vinden, net als de 'principes van menselijkheid en de dictaten van het publiek geweten'.

20. Alle verdragen ten spijt, zou de Martensclausule even goed dode letter kunnen blijven. Indien geen enkel internationaal gerechtshof deze clausule zou erkennen of als argument aanvaarden, zouden die 'principes van menselijkheid en de dictaten van het publiek geweten' geen enkele inbreng hebben in het recht der gewapende conflicten. De clausule wordt echter wel gebruikt, te beginnen in 1948, in de *Krupp*-zaak[71]. De details van deze zaak zou het bestek van deze masterproef te buiten gaan, maar het volstaat om te zeggen dat A. Krupp terechtstond, samen met 11 andere directeurs van de Krupp-groep, voor een reeks feiten, gaande van 'misdaden tegen de vrede' via het plannen en voeren van oorlog (waar lidmaatschap van de S.S. al gezien werd als het plannen van oorlog), het plunderen en stelen van publieke en private eigendommen in bezette gebieden, tot het plegen van oorlogsmisdaden door het gebruik van gifgas en dwangarbeid[72]. Wat betreft de aanklacht van plunderingen, verwijst het Hof naar de Martensclausule, wat het evenwel verkeerdelijk de Mertensclausule noemt en toewijst aan de Belgische diplomaat Mertens:

> *"The preamble [van de Conferenties van 1899 en 1907] is much more than a pious declaration. It is a general clause, making the usages established among civilized nations, the laws of humanity, and the dictates of public conscience into the legal yardstick to be applied if and when the specific provisions of the Convention and the Regulations annexed to it do not cover specific cases occurring in warfare, or concomitant to warfare."*[73]

[71] Zie voetnoot 17.
[72] THE UNITED STATES WAR CRIMES COMMISSION, *Law Reports of Trials of War Tribunals – Volume X The I.G. Farben and Krupp Trials*, Londen, 1949, 6-30 (hierna: *Krupp*-case).
[73] *Krupp*-case, 133.

Het tribunaal verwijst hier, in zijn *obiter dictum*, dus duidelijk, alhoewel deels foutief, naar de Martensclausule, alhoewel het de veroordeling uiteindelijk rechtvaardigt op basis van art. 46 tot 56 van het Verdrag van Den Haag II van 1899[74].

21. Ook het Joegoslaviëtribunaal in Den Haag verwees naar de Martensclausule in de *Martic*-zaak[75]. In eerste aanleg verwees het tribunaal naar de Martensclausule voor de aanduiding van het toepasbaar recht: ook hier werd verwezen naar de 'elementaire overwegingen van menselijkheid'[76]. Opnieuw was dit echter een *obiter dictum*, aangezien het tribunaal de veroordeling steunde op verdrags- en gewoonterecht[77]. Ten slotte dient ook nog de hierboven vermelde *advisory opinion* van het Internationaal Gerechtshof betreffende nucleaire wapens[78] te worden vermeld als laatste voorbeeld van een praktische toepassing van de Martensclausule. Er dient te worden herinnerd aan het feit dat het Hof geen mening gaf over de clausule, maar dat de uitgebreide *dissenting opinion* van rechter SHAHABUDDEEN[79] wel meer licht werpt op de bepaling.

C. Relevantie voor dit onderwerp

22. Is de toepassing van de Martensclausule relevant voor cyberoorlogen? In elk geval wel. Momenteel is er geen enkel verdrag dat cyberoorlog regelt, dus blijft, dankzij de Martensclausule, het internationaal gewoonterecht en 'de principes van menselijkheid en de dictaten van het publiek geweten' toepasbaar. Maar doet de interpretatie van die clausule er dan toe? Volgens de auteur van deze masterproef wel. Indien men zou uitgaan van de meest restrictieve benadering, zou de Martensclausule enkel een omgekeerd *a contrario*-argument aanbieden: omdat cyberoorlog niet geregeld of verboden wordt door een verdrag, is het niet per se toegelaten. Dit is echter onvoldoende. Niet alleen omdat cyberoorlog als feit niet langer onontkoombaar is[80], maar ook omdat men niet over een hele tak van oorlogsvoering kan zeggen dat die verboden is.

[74] *Ibid*.; zie ook VON BERNSTORFF, "Martens Clause", nr. 9.
[75] Joegoslaviëtribunaal*, Prosecuter vs. Martic*, 1996, IT-95-11 (hierna: *Martic*-case).
[76] Zie nr. 13 zoals gevonden op icrc.org, 11 maart 2016.
[77] *Martic*-case; zie ook VON BERNSTORFF, "Martens Clause", nr. 10.
[78] Zie nr. 7 e.v.
[79] zie nr. 10 e.v.
[80] Zie, bijvoorbeeld, J.A RABKIN, A. RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", *Task force on national security and law*, Hoover Institution Stanford University, 2012 (hierna: RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict").

23. Regelgeving kan dus noodzakelijk zijn. Gelet op de rechtsleer, de meerdere weergaven van de clausule in verdragen en de vermeldingen van de bepaling in verschillende zaken, gaat deze masterproef dan ook uit van een ruime interpretatie van de Martensclausule, in navolging van CASSESE[81]: de Martensclausule kan en zou moeten gebruikt worden om de vereiste van Statenpraktijk af te zwakken wat betreft cyberoorlog. Deze manier van oorlogsvoering is relatief nieuw en kan verstrekkende gevolgen hebben. Bovendien evolueert de digitale wereld zo snel, dat het misschien beter is om te rekenen op interpretatie dan op een verdrag, wat starheid zou impliceren[82]. Wachten op een algemeen aanvaarde statenpraktijk zou nefast kunnen zijn. Men kan echter eventueel stellen dat er al bepaalde vormen van statenpraktijk terug te vinden zijn. Een van de meest geciteerde werken en ook aangeraden door de directeur van de Koninklijke Militaire Academie[83], is de *Tallinn-manual*[84]. Deze handleiding werd opgesteld door een team van experts, op vraag van de NAVO. Aangezien SCHMITT nu bezig is aan de redactie van een tweede versie van deze handleiding[85], kan dus gesteld worden dat dit een vrij belangrijke bron is van zowel rechtsleer als (een kiem van) statenpraktijk.

24. Niet iedereen is echter van mening dat interpretatie van de bestaande regels genoeg of zelfs wenselijk is. LEVARSKA meent dat de verschillen tussen cyberoorlog en conventionele oorlogsvoering zo groot zijn, dat een verdrag de enige mogelijke oplossing is[86]. Ze stelt bovendien dat, hoewel er gelijkaardige problemen rijzen voor beide soorten conflicten, de oplossing langs verschillende wegen moet gezocht worden[87]. Enigszins contradictorisch stelt ze wel dat dit hypothetisch verdrag ambigue moet zijn, teneinde de verschillende zienswijzen van staten nader tot elkaar te brengen[88]. Er zou dus sowieso interpretatie nodig zijn. Art. 32 van het Weens Verdragenverdrag stelt bovendien dat verdragen zo geïnterpreteerd moeten worden dat de gevolgen niet

[81] Zie nr. 14.
[82] De zogenaamde Wet van Moore: computertechnologie wordt iedere 18 maand dubbel zo snel en dubbel zo krachtig; N. LEVARSKA, "Regulation of Cyber-Warfare: Interpretation versus Creation"*, ESR*, December 2013, nr. 70, 12 (hierna: LEVARSKA, "Regulation of Cyber-Warfare: Interpretation versus Creation").
[83] Zie BIJLAGE 3.
[84] M.N. SCHMITT (*ed.*), *Tallinn Manual on The International Law Applicable to Cyber Warfare*, Cambridge University press, Cambridge, 2013 (hierna: *Tallinn-manual*).
[85] Zie BIJLAGE 5.
[86] LEVARSKA, "Regulation of Cyber-Warfare: Interpretation versus Creation", 14-15.
[87] LEVARSKA, "Regulation of Cyber-Warfare: Interpretation versus Creation", 14.
[88] LEVARSKA, "Regulation of Cyber-Warfare: Interpretation versus Creation", 13.

manifest absurd of onredelijk zouden zijn[89], wat als een argument pro interpretatie kan worden gezien.

III. CYBEROORLOG: EEN NIEUW SLAGVELD?

A. Problemen

25. Cyberoorlog is een nieuw fenomeen. Er is voor zover bekend nog geen enkel historisch voorbeeld te vinden van cyberoorlog op grote schaal (er zijn wel voorbeelden te vinden van kleinschalige aanvallen, zoals vermeld in de inleiding van deze masterproef). Het fenomeen is zo nieuw, dat sommige rechtsleer nog steeds de discussie aangaat of cyberoorlog wel een actuele situatie is[90] en niet een debat dat in de toekomst moet plaatsvinden[91]. Gelet echter op het grote aantal bijdragen van de rechtsleer (welke in deze masterpref aan bod zullen komen) en de effectieve zorgen die overheden zich erover maken[92], lijkt het dat "cyberoorlog" een aanvaard fenomeen is, of op zijn minst een toekomstig fenomeen dat al het onderwerp van studie zou moeten uitmaken[93].

26. Daarmee is de kous echter niet af. De vraag stelt zich nu hoe cyberoorlog past in het kader van het zogenaamde *jus ad bellum*, het recht der gewapende conflicten. Welke regels zijn er van toepassing, en in welke mate[94]? Valt een cyberaanval onder het verbod op het gebruik van geweld van het Handvest van de VN[95]? Waar vindt cyberoorlog plaats? In iets wat de "cyberspace" heet, of in de echte wereld[96]? Hoe wordt deze ruimte afgebakend[97]? Vanaf wanneer spreekt men van "oorlog"[98]? Wat is een

[89] Verdrag betreffende het verdragenrecht van 23 mei 1969, Wenen (hierna: Weens Verdragenverdrag).
[90] R. HUGHES, "A Treaty for Cyberspace", *International Affairs*, 2010, nr. 2, 533 (hierna: HUGHES, "A Treaty for Cyberspace").
[91] L. VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", *NjW*, 2013, nr. 6, 348-355 (hierna: VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid").
[92] Zie onder andere: Schriftelijke vragen en antwoorden, *Parl.St.* Kamer, 2004-2005, vraag nr. 131.
[93] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 1-3.
[94] VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 356.
[95] Art. 2(4) Handvest van de Verenigde Naties van 26 juni 1945, San Francisco, *UNTS* XVI.
[96] J.-F. KREMER, B. MÜLLER (*eds*.), *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer Press, Berlijn, 2014, 3 (hierna: KREMER, MÜLLER).
[97] *Ibid*.
[98] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 3; VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", die verwijst naar het advies van de AIV/CAVV (Adviesraad Internationale Vraagstukken/Commissie van Advies inzake Volkenrechtelijke Vraagstukken), die stelt dat een digitale oorlog op grote schaal niet in de nabije toekomst zal plaatsvinden, maar aangeeft er toch onderzoek naar te verrichten.

cyberaanval[99]? Al deze vragen tonen aan dat cyberoorlog verre van geregeld is. Daar komt de Martensclausule aan te pas: indien een gebied betreffende cyberoorlog niet geregeld is of niet specifiek onder bestaande regulering valt, zullen het algemeen gewoonterecht, de principes van menselijkheid en de dictaten van het publiek geweten een uitweg bieden.

27. In de volgende secties van dit hoofdstuk zullen eerst enkele elementaire begrippen in verband met cyberoorlog gedefinieerd en afgebakend worden (bijvoorbeeld wat men onder "cyberoorlog" moet begrijpen). Eens dit bestudeerd is aan de hand van de mogelijke bronnen, zal deze thesis aangeven welke (interpretaties van) definities zullen gebruikt worden en hoe verdere terminologie gebruikt dient te worden. Indien dus verder onduidelijkheid in de terminologie zou kunnen bestaan, bijvoorbeeld indien een gangbare term wel toepasselijk is, zullen secties B en C duidelijkheid bieden over hoe bepaalde begrippen geïnterpreteerd moeten worden.

B. Definities en problemen in en van de gangbare terminologie

28. Een masterproef over cyberoorlog schrijven is pas mogelijk indien "**cyberoorlog**" een duidelijk afgebakend gebied vormt. Een eerste probleem rijst wanneer men nagaat wanneer van een "gewapend conflict" sprake is. Art. 2 van het Verdrag van Geneve bepaalt dat de verdragsregels gelden indien staten elkaar de oorlog verklaren. Dit is aanvaardbaar voor conventionele manieren van oorlogsvoering, maar in de digitale wereld ligt dat moeilijker. Het is immers logisch dat staten hun cyberbeveiliging enorm zouden verscherpen indien zij in staat van oorlog verkeren, wat een aanval veel moeilijker zou maken[100]. Ook de rechtspraak biedt niet veel duiding voor dit specifiek gebied. In de zaak *Tadic* oordeelde het Joegoslaviëtribunaal dat van gewapend conflict sprake was wanneer staten onderling naar gewapend geweld teruggrijpen[101]. De vraag stelt zich nu of een digitale aanval wel 'geweld' uitmaakt, en of dit dan gewapend is (aangezien de actie in deze digitale context bijvoorbeeld kan bestaan uit een simpele druk op een toetsenbord, zonder dat er schade aan personen ontstaat, maar

[99] H. NASU, R. MCLAUGHLIN, (*eds*.), *New Technologies and the Law of Armed Conflict*, Asser Press, Den Haag, 2014, 60 (hierna: NASU, MCLAUGHLIN).
[100] Dit is natuurlijk slechts een aanname die deze masterproef maakt. Bij gebrek aan praktijkvoorbeelden, is het onmogelijk om de reacties van staten na te gaan, simulaties daargelaten. Dit kan echter gestaafd worden door de vraag aan de minister van Landsverdediging in Schriftelijke vragen en antwoorden, *Parl.St.* Kamer, 2004-2005, vraag nr. 131: een vermeende dreiging van cyberaanvallen vanuit Noord-Korea lokte de vraag uit of maatregelen zouden worden getroffen.
[101] Joegoslaviëtribunaal, *Prosecutor v. Tadic*, 1995, IT-94-1-A, par. 70 (hierna: *Tadic*-case).

wel het hele defensieapparaat kan worden neergehaald). Daarom dient eerst te worden onderzocht of digitaal geweld mogelijk is, om dan te beslissen of "cyberoorlog" een gepaste term is.

1. Gewapend geweld

29. Art. 2(4) van het VN Handvest verbiedt het gebruik van geweld, niet alleen van gewapend geweld, maar ook van 'elke andere handelswijze die onverenigbaar is met de doelstellingen van de Verenigde Naties'. Toch is de heersende opinie dat dit handvest vooral op gewapend geweld en niet op andere vormen van (politieke of economische) druk slaat[102]. Valt een cyberaanval dan onder *gewapend* geweld? Volgens SCHMITT moeten daarvoor de "kinetische gevolgen" van een cyberaanval overwogen worden[103]. Indien de gevolgen van een cyberaanval gelijkaardig zijn aan de gevolgen van aanvallen met conventionele wapens (bijv. slachtoffers), dan is er sprake van *gewapend* geweld[104] (deze maatstaf zal later nog terugkeren bij het onderzoek naar de kwalificatie als "gewapende aanval[105]). Zo is bijvoorbeeld het op afstand vernietigen van de beveiligingssystemen van kerncentrales op zich geen verboden gebruik van geweld, maar de gevolgen zorgen dat dit wel zo is. Hetzelfde geldt bijvoorbeeld met het in de war sturen van het elektriciteitsnet of het verkeersnet, waardoor verkeersslachtoffers vallen[106].

30. Het feit dat er geen effectief "kinetisch" geweld is[107], doet geen afbreuk aan het label "gewapend geweld"[108]: sinds de ontwikkeling van biologische, chemische en nucleaire wapens[109] is algemeen aanvaard dat deze onder het geweldverbod vallen[110],

[102] Zie bijvoorbeeld de voorbereidende werken bij dit artikel: de meerderheid van de staten stemde tegen een amendement dat niet-gewapende drukkingsmiddelen, zoals *in casu* economische sancties onder deze bepaling zou brengen: M.N. SCHMITT, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *IITA (USAF)*, juni 1999, 5 e.v. (hierna: SCHMITT, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework"); VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 351; later kwam de discussie opnieuw aan bod bij de Verenigde Naties, met hetzelfde gevolg: *Tallinn-manual*, 48.
[103] SCHMITT, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 17-23.
[104] *Tallinn-Manual*, 47.
[105] Zie *infra*.
[106] J. GOLDSMITH, "How Cyber changes the Laws of War", *EJIL*, 2013, vol. 24 nr. 1, 133 (hierna: GOLDSMITH, "How Cyber changes the Laws of War").
[107] Een wetenschappelijke term, slaat op het gebruik van kinetische energie (vb. de ontploffing in de loop van een pistool die de kogel vooruit jaagt) om geweld te plegen.
[108] CAVV, *Cyber Warfare*, december 2011, nr. 77, 20.
[109] Die geen van alle gebruik maken van kinetische energie, i.e. een fysische reactie, maar eerder van chemische en biologische reacties. Nucleaire wapens zijn tweeslachtig: natuurlijk vormt de ontploffing een kinetische aanval, maar de radiatie die nadien vrijkomt, valt eerder als een biologische reactie te beschrijven.

gelet op hun destructieve kracht. Het lijkt dus duidelijk dat er, naargelang de gebruikte technologie in oorlogen evolueert, meer naar de effecten dan naar de middelen wordt gekeken. Toch kunnen niet alle cyberaanvallen als gewapend geweld worden gezien, zoals VAN DEN HERIK aangeeft: dit zou een te groot toepassingsgebied toekennen aan art. 2(4) VN Handvest[111]. Aanvallen die geen 'kinetische' schadelijke gevolgen hebben, zoals spionage of het laten crashen van militaire servers, vallen in elk geval niet onder het geweldverbod[112]. Discussie ontstaat echter nog over wat effectief gewapend geweld uitmaakt: sommigen zijn ervan overtuigd dat elke aanval met kinetische gevolgen gewapend geweld betreft, terwijl anderen echter in zeer uitzonderlijke gevallen tot die kwalificatie willen overgaan[113].

31. Volgens SCHMITT in de *Tallinn-Manual* zullen staten enkele criteria aflopen om na te gaan of een actie een vorm van geweld uitmaakt, waaronder ook cyberoperaties. Hij baseert deze stelling op zijn eerdere werk, waar hij stelt dat die criteria de gevolgen van een operatie bepalen, maar tegelijk ook aangeeft dat dit geen exacte wetenschap is[114] en zelfs niet verdragsrechtelijk of anderzijds legaal onderbouwd[115]. SCHMITT meent dat indien een operatie ernstig genoeg is (i.e. fysiek leed aan personen of eigendom, een *de minimis*-regel), onmiddellijke gevolgen heeft (hoe directer, hoe vaker gekwalificeerd als "gewapend geweld"), directe gevolgen heeft (indien een cyberaanval direct aanwijsbare gevolgen heeft, zal die eerder "gewapend geweld" uitmaken dan een aanval met latente gevolgen), dieper indringt in een Staat of in cybersystemen die vitaal zijn voor die staat (een vuistregel is hier: hoe beter beveiligd, hoe vitaler, hoe sneller de stempel "gewapend geweld" wordt gebruikt), meetbare gevolgen heeft (wat vrij moeilijk is bij cyberoperaties, maar niet onmogelijk: indien het meetbare gevolgen heeft, wordt het sneller als "gewapend geweld" gekwalificeerd), een militair karakter (i.e. doel) heeft, de inmenging van een Staat inhoudt (een operatie bevolen door een overheid zal sneller zo gezien worden dan individuele, 'private' aanvallen) en niet onder de zogenaamde "vermoede legaliteit" valt (de *Lotus*-case

[110] I. BROWNLIE, *International Law and the Use of Force by States*, Clarendon Press, Oxford, 1963, 362; VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 351-352.
[111] VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352.
[112] *Ibid.*; GOLDSMITH, "How Cyber changes the Laws of War", 133.
[113] Zie GOLDSMITH en SCHMITT die de meer uitgebreide interpretatie verdedigen, tegenover VAN DEN HERIK, die een engere zienswijze voorschrijft. Ook WOLTAG is van oordeel dat kinetische schade gewapend geweld kan uitmaken (Woltag, "Cyber Warfare", nr. 8).
[114] SCHMITT, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 18.
[115] *Tallinn-Manual*, 49.

oordeelde dat wat niet verboden is door het internationaal recht *sensu lato*, toegelaten is), die operatie sneller als gewapend geweld zal worden gezien. Deze criteria lijken duidelijk genoeg, hoewel ze toch een zeker mate van discretie overlaten aan de staten zelf, maar door het gebrek aan effectieve (grootschalige) cyberaanvallen kan niet worden nagegaan of deze criteria ook gebruikt (zullen) worden[116].

32. Toch rijzen er nog heel wat praktische problemen, eigen aan het cyberkarakter van de aanvallen. GOLDSMITH geeft dit treffend weer[117]: de stelling dat vernieling of dood ('kinetische' gevolgen) van cyberaanvallen gelijkgesteld worden aan conventioneel geweld, stuit op het probleem dat conventioneel geweld steeds in militaire context wordt gebruikt. Een bommenwerper kan enkel in een militaire context worden gebruikt, bijvoorbeeld. Cyberaanvallen kunnen echter ook buiten het militaire gebruikt worden: een aandelenmarkt die aangevallen wordt kan tot desastreuze economische schade leiden[118], wat op zijn beurt dan weer tot een hoog aantal doden aanleiding kan geven[119]. Bovendien kan, in tegenstelling tot een kinetische aanval (bijvoorbeeld een trekker die wordt overgehaald en een kogel die de kamer verlaat), een cyberaanval een langzaam en omkeerbaar proces uitmaken[120]. Het is niet zeker of dit ook *gewapend* geweld uitmaakt. Deze voorbeelden tonen aan dat, hoewel analogieën getrokken kunnen worden met conventionele oorlogsvoering en conventioneel verdragsrecht, de eigenheid van cyberoorlogen voor problemen zorgen die de grenzen van wat voordien als logisch werd beschouwd, op zijn minst vaag maken, indien het die grenzen zelfs niet doorbreken[121].

2. Gewapende aanval

33. Afgezien van de discussie welke aanvallen precies *gewapend* geweld uitmaken, lijkt de rechtsleer ervan overtuigd dat cyberaanvallen in het algemeen gewapend ge-

[116] Alhoewel kan aangenomen worden dat de NAVO-landen naar deze criteria teruggrijpen, aangezien de *Tallinn-Manual* geschreven is in opdracht van die NAVO.
[117] GOLDSMITH, "How Cyber changes the Laws of War", 133-138.
[118] GOLDSMITH, "How Cyber changes the Laws of War", 133.
[119] M. HAIKEN, "More Than 10.000 Suicides Tied To Economic Crisis, Study Says", *Forbes*, 12 juni 2014, www.Forbes.com; in dit artikel wordt het verband gelegd tussen het aantal zelfmoorden die volgden op de economische crisis van 2008.
[120] GOLDSMITH, "How Cyber changes the Laws of War", 133.
[121] Zo heeft N. VAN RAEMDONCK haar thesis over dit onderwerp geschreven (zie BIJLAGE 2): wat met aanvallen die niet per se een militair karakter hebben, maar wel belangrijke nationale infrastructuur raken?; WOLTAG, "Cyber Warfare", nr. 8.

weld *kunnen* uitmaken[122]. De vraag rijst nu of die cyberaanvallen een gewapende aanval uitmaken, die de scheidslijn tussen incidenten en een volwaardige (cyber)oorlog uitmaakt[123]. Art. 51 VN Handvest vereist specifiek een *gewapende* aanval om het recht op zelfverdediging uit te oefenen. Maar opnieuw is dit niet zo eenvoudig op het gebied van cyberoorlog. Zo moet een gewapende aanval een grensoverschrijdend karakter hebben[124]. Het is echter niet duidelijk of "cyberspace" soevereine grenzen volgt of één grote ruimte is[125]. Verder is het niet altijd duidelijk wie achter een aanval zit[126], is het niet altijd duidelijk wat het doelwit is of kunnen de effecten van de aanval slechts lang na de feitelijke aanval aan het licht komen[127].

34. Aangezien de term niet in het Handvest of in enig ander verdrag wordt gedefinieerd, moet de definitie uit het gewoonterecht worden gehaald, wat in de *Nicaragua*-case is gebeurd[128]. Verder oordeelt het Internationaal Gerechtshof in die zaak dat art. 51 niet op specifieke wapens slaat, maar op elk gebruik van geweld, ongeacht de gebruikte wapens[129]. Er zijn drie factoren van belang om na te gaan of een aanval een *gewapende aanval* in de zin van dit art. 51 uitmaakt[130].

35. In de eerste plaats zijn de middelen van de aanval van belang om de aanval al dan niet onder art. 51 te plaatsen. Indien enkel kinetische wapens in de enge zin onder deze bepaling vallen, kan geen enkele cyberaanval ooit recht op zelfverdediging bieden[131]. Ook daar dient dus een uitbreiding ingevoegd te worden: iedere middel (ook hoogtechnologisch) dat een aanzienlijk verlies van levens en/of eigendom veroorzaakt, moet een gewapende aanval uitmaken[132]. De middelen blijven echter een heikel

[122] H.H. DINNISS, *Cyber Warfare and the Laws of War*, Cambridge University press, Cambridge, 2012, 76-95 (hierna: DINNISS).
[123] *Tallinn-Manual*, 54; VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352.
[124] *Tallinn-Manual*, 54.
[125] Zie *infra*.
[126] GOLDSMITH, "How Cyber changes the Laws of War", 134.
[127] *Ibid.*
[128] K. ZEMANEK, "Armed attack", *MPEPIL*, Oxford Public International Law, oktober 2013, opil.ouplaw.com, nr. 1 (hierna: ZEMANEK, "Armed attack").
[129] PCIJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Verenigde Staten van Amerika)*, 1986, *I.C.J. Reports* 1986, p. 14 e.v. par. 39 (hierna: *Nicaragua*-case).
[130] VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352; *Nicaragua*-case par. 195.
[131] Wat echter het oorspronkelijk idee achter art. 51 was, slechts nadien werden chemische en biologische wapens overwogen: ZEMANEK, "Armed attack", nr. 11.
[132] SCHMITT, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 17-23, VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352, ZEMANEK, "Armed attack", nr. 21.

punt bij deze definitie. Na de aanslagen van 11 september 2001[133] is de discussie evenwel verschoven naar de gevolgen en de omvang van een aanval[134] om uit te maken of het onder het toepassingsgebied van art. 51 valt[135]. Hierdoor heeft het debat over de gebruikte middelen aan belang ingeboet[136].

36. Het Internationaal Gerechtshof was in de *Nicaragua*-case ook van mening dat een onderscheid tussen verschillende aanvallen gemaakt moest worden naargelang het doel, en meer bepaald de 'omvang en gevolgen'[137]. De gevolgen moeten 'ernstig' zijn om "gewapend geweld" de drempel van "gewapende aanval" te laten overstijgen. Helaas gaat het Hof hier verder niet op in. Volgens SCHMITT[138] dienen inderdaad de gevolgen te worden bestudeerd, en niet de gebruikte middelen: indien de gevolgen dezelfde zijn als die welke het gevolg zijn van conventionele, "kinetische" wapens, is er sprake van een gewapende aanval[139]. Zo maakt een aanval die schade aan personen of eigendom veroorzaakt, automatisch een gewapende aanval uit. Verder blijft echter discussie bestaan, in geval van ernstige gevolgen zonder schade aan personen of eigendom. Grote schade aan infrastructuur (publieke eigendom) zou ook als een voldoende ernstig effect worden beschouwd[140]. De Nederlands adviesraad internationaal publiekrecht (CAVV) oordeelt dat een "gewapende aanval" een langdurige of aanhoudende poging tot aanval op de essentiële functies en/of de stabiliteit van een staat inhoudt[141]. Een sluitende, logische redenering lijkt echter niet voorhanden: er is geen overeenstemming welke gevolgen precies in aanmerking moeten worden genomen op het vlak van cyberoperaties[142] en indien de aanval op essentiële functies van een staat (i.e. de noodzakelijke infrastructuur) inderdaad een gewapende aanval zou uitmaken, wat precies onder die essentiële functies moet worden begrepen[143]. Er moet in de huidige stand van zaken dus geval per geval bekeken worden.

[133] *Resolutie 1373 van de Veiligheidsraad van de Verenigde Naties*, 18 september 2001, *Doc. nr.* S/RES/1373; *Resolutie 1386 van de Veiligheidsraad van de Verenigde Naties*, 20 december 2001, *Doc. nr.* S/RES/1386.
[134] ZEMANEK, "Armed attack", nr. 13; VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352.
[135] Wat eigenlijk al gesteld was door het IGH: *Nuclear Weapons-opinion*, par. 39.
[136] VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352.
[137] *Nicaragua*-case, par. 195.
[138] Die met zijn werk door vele auteurs geciteerd wordt; zie o.a. VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 352-353; ZEMANEK, "Armed attack", nr. 13; NASU, MCLAUGHLIN; hij is ook een van de editoren van de zogenaamde 'Tallinn-manual'.
[139] *Tallinn-Manual*, 54.
[140] VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 353.
[141] *Ibid*.
[142] *Tallinn-Manual*, 55-56
[143] VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 353.

37. Er kan echter met zekerheid gesteld worden dat sommige cyberaanvallen wel degelijk onder art. 51 VN Handvest kunnen vallen[144]. Deze conclusie is niet afkomstig van enige primaire rechtsbron of van het internationaal gewoonterecht, maar volgt uit interpretatie en uit de rechtsleer[145]. Dit is van groot belang, aangezien dit artikel het recht op zelfverdediging uitmaakt en dus aan een verdedigende staat het recht geeft om een (proportionele en noodzakelijke)[146] tegenaanval uit te voeren. Dit kan een cyberoorlog ontketenen. Er rijzen echter nog tal van vragen, die later behandeld zullen worden: hoe kan die tegenaanval uitgevoerd worden? Moet dit via een cyberaanval, of mogen conventionele wapens ingezet worden? Hoe ver gaat dit zelfverdedigingsrecht? Tegen wie moet deze aanval gericht zijn? Kunnen niet-statelijke actoren tot gewapende aanvallen overgaan in cyberspace?

3. Cyberoorlog

38. Hoewel *cyberoorlog* nergens specifiek wordt gedefinieerd, kan er wel aangenomen worden dat die bestaat en in de huidige stand van zaken kan uitbreken: indien een cyberaanval de drempel van "gewapende aanval" overschrijdt, kan die onder art. 51 VN Handvest vallen en een zelfverdedigingsreactie uitlokken. Die acties, zowel aanval als verdediging, vallen dan onder de Verdragen van Geneve (via art. 2). Die zienswijze is verdedigbaar, gezien onderlinge gewapende aanvallen een gewapend conflict uitmaken volgens de case-law van het Joegoslaviëtribunaal[147].

39. Aangezien *cyberoorlog* een relatief nieuw begrip is, valt er ook geen algemeen aanvaarde definitie van terug te vinden, maar wordt de term ingevuld naargelang van wat de gebruiker van die term de beste weergave vindt[148]. Enkele voorbeelden:

> *"Information war is […] a confrontation between two or more states in the information space aimed at … undermining political, economic and*

[144] CAVV, 20-21; F. FRANCEUS, "Cyberaanvallen en het recht van de gewapende conflicten: bemerkingen bij een juridische primeur in België en de Verenigde Staten", *BISC*, 19 oktober 2012, 16 (hierna: FRANCEUS).
[145] K. GOMBEER, "Het internationaal juridisch kader voor interstatelijk gebruik van computeraanvallen", *Juridische Meesterwerken*, VUB, 2010-2011, 218 (hierna: GOMBEER, "Het internationaal juridisch kader voor interstatelijk gebruik van computeraanvallen").
[146] *Tallinn-Manual*, 59; *Nicaragua*-case, par. 176, 194.
[147] Zie nr. 26.
[148] KREMER, MÜLLER, 23.

social systems [or] mass psychologic brainwashing to destabilize society and state" (GJELTEN)[149]*;*

"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives" (US Army Training & Doctrine Command)[150]*;*

"Cyber power is the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyber domain" (NYE)[151]*;*

"The use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another state" (SCHAAP)[152]

Er is duidelijk te zien dat de invulling van de term afhangt van wie de term gebruikt: Het leger van de Verenigde Staten ziet het meer als een aanval op de staatsstructuur en ideologie, terwijl bijvoorbeeld NYE een meer wetenschappelijke, abstracte definitie gebruikt. Toch ijveren sommige auteurs voor een eenvormige definitie, aangezien zij van oordeel zijn dat het belangrijk is om deze nieuwe vorm van oorlog duidelijk af te bakenen[153].

40. Het is bovendien noodzakelijk om de definitie van cyberoorlog niet tot een louter interstatelijk gegeven te zien: ook een aanval op een supranationale instelling (zoals de Europese Unie) of een aanval door niet-statelijke actoren (bijvoorbeeld een terro-

[149] The Shanghai Cooperation Organization, zoals geciteerd door T. GJELTEN, "Shadow Wars: Debating Cyber Disarmament", *World Affairs*, 2010, nr. 173, 36.
[150] N.N., *DCSINT Handbook nr. 1.02, Critical Infrastructure Threats and Terrorism*, U.S. Army Training & Doctrine Command, 2006, www.fas.org.
[151] J.S. NYE, "Cyber Power", *Harvard Kennedy School, Belfer Center*, 2010, www.dtic.mil, 3-4 (hierna: NYE, "Cyber Power").
[152] A.J. SCHAAP, "Cyber Warfare Operations: Development and Use under International Law", *Air Force Law Review*, 2009, nr. 64, 127.
[153] M.J. CETRON, O. DAVIES, "Ten Critical Trends for Cyber Security", *The Futurist*, 2009, nr. 45, 47.

ristische organisatie) kan (de start van) een cyberoorlog uitmaken[154]. De meest inclusieve definitie van de vorige voorbeelden (die van SCHAAP) zou dan uitgebreid moeten worden als volgt:

> *"The use of network-based capabilities of a state* ***or non-state actor*** *to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another* ***actor****"*[155]

Deze bezorgdheid om niet-statelijke actoren is niet hypothetisch: *hacktivists* (zoals Anonymous) of zogenaamde *patriotic hackers* tonen aan dat dergelijke groeperingen gemakkelijk toegang vinden tot dit platform[156].

41. **Cyberoorlog** valt dus niet eenduidig te definiëren, alhoewel het een bestaand fenomeen is, waar het recht der gewapende conflicten op van toepassing is[157]. Van alle beschikbare definities in de rechtsleer (rechtspraak en verdrags-of gewoonterecht blijven logischerwijs in gebreke op dit punt) lijkt de aangepaste definitie van SCHAAP[158] de meest inclusieve, daar die alle denkbare gevolgen van een aanval inhoudt, naast de mogelijkheid dat ook niet-statelijke actoren aanvaller of slachtoffer kunnen zijn. Naar de mening van deze auteur kan er echter niet met zekerheid gesteld worden of deze definitie volledig correct is: het lijkt vrij moeilijk om alle denkbare gevolgen en implicaties van een cyberaanval in te schatten, om een allesomvattende definitie van *cyberoorlog* te kunnen afleiden[159].

4. Cyberspace

42. Een tweede belangrijke term is "cyberspace". Cyberspace is overal en verbindt een enorm deel van de menselijke activiteiten en productiviteit: Google, GPS, Ama-

[154] KREMER, MÜLLER, 24.
[155] *Ibid*.
[156] NYE, "Cyber Power", 6
[157] *Tallinn-manual*, 68.
[158] Zie *Supra*.
[159] Dit is natuurlijk slechts de mening van de auteur, maar die is gebaseerd op de volgende analogie: hoewel voor elke grote oorlog (WO I, WO II) reeds verdragen beschikbaar waren die staten bonden op het vlak van oorlog, moest nadien steeds een revisie van die verdragen gebeuren, omdat er onverwachte ontwikkelingen waren: het verdrag op het verbod van gifgas na WO I, de Conventies van Geneve na WO II. Het lijkt dus aannemelijk dat, in het geval een grootschalige cyberoorlog zou uitbreken, nadien ook revisies van de (werk)definities zouden gebeuren. Deze opinie wordt echter ook gesteund door HUGHES, "A Treaty for Cyberspace", 541.

zon, maar ook gewoon mailverkeer behoren tot het dagelijks leven[160]. Dit is evenwel een dubbelsnijdend zwaard: naast enorme mogelijkheden, heeft cyberspace ook voor een nieuwe dreiging gezorgd[161]. Na land, zee en lucht vormen cyberspace en de ruimte de respectievelijk vierde en vijfde dimensie waar oorlog kan uitbreken[162]. Los van het soevereiniteitsvraagstuk moet nagegaan worden *wat* cyberspace precies is en hoe het afgebakend kan worden. Heel wat problemen kunnen zich stellen, zoals een gebrek aan fysieke geografische elementen (in tegenstelling tot bijvoorbeeld land). In cyberspace speelt de effectieve locatie een beperktere rol[163]. Toch moeten de bestaande internationaalrechtelijke principes toegepast kunnen worden, aangezien de effecten in cyberspace wel degelijk effecten in de tastbare wereld teweeg kunnen brengen[164]. De *Tallinn-manual* beschrijft cyberspace als[165]:

> "*The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify and exchange data using computer networks."*

Deze definitie is echter technisch en laat niet toe om enige elementen te onderscheiden die het soevereiniteitsvraagstuk kunnen oplossen, of aangeven welk internationaalrechtelijk regime van toepassing is. Verder onderzoek is dus nodig.

43. Het belang van een afbakening van cyberspace en eventuele territoriale grenzen in dit gebied ligt in het feit dat zo bepaald kan worden waar cyberactiviteiten kunnen en mogen plaatsvinden. Indien cyberspace de geografische grenzen van het klassieke recht der gewapende conflicten volgt, mogen enkel cyberoperaties worden uitgevoerd in en tussen de partijen in een conflict[166]. Omgekeerd zouden in geval van een niet-internationaal gewapend conflict de cyberoperaties beperkt moeten worden tot de staat waar het conflict zich afspeelt[167]. Het is dus van belang om te weten wat cyberspace precies inhoudt, zodat men weet waar en wanneer men cyberoperaties kan inzetten, zoals het geval is met territoriale grenzen en 'klassieke' oorlogsvoering.

[160] KREMER, MÜLLER, 42.
[161] *Ibid.*
[162] NASU, MCLAUGHLIN, 2
[163] GOMBEER, 169.
[164] NASU, MCLAUGHLIN, 75.
[165] *Tallinn-manual*, 211.
[166] *Tallinn-manual*, 71.
[167] *Ibid*.

44. Enkele staten, zoals China en de VSA, zijn onderzoek aan het voeren om cyberspace beter af te kunnen bakenen[168]. Ook Duitsland[169] en de Europese Unie[170] hebben de potentiele gevaren van cyberspace erkend in hun *cyber security strategy*. Dit is te begrijpen, aangezien cyberspace in wezen een onbegrensd domein is: effecten in een ene staat kunnen duizenden kilometers ver weg door een andere staat veroorzaakt zijn, dankzij de connectiviteit in cyberspace[171]. Toch kan voor het fysieke deel van de cyberspace (servers, verbindingen etc.) al gesteld worden dat die onder de soevereiniteit van de staat waar ze zich bevinden vallen[172]. Het moeilijkste deel is te bepalen wat de status of de afbakening van de data is. Die data is snel verplaatsbaar en nutteloos tot het zijn bestemming bereikt. Daarnaast is sinds de ontwikkeling van *cloud-computing* de mogelijkheid ontstaan om data op veel verschillende plaatsen tegelijk op te slaan. Een van de theorieën over cyberspace maakt daarom een analogie met de *global commons*: aangezien data praktisch gezien overal, tegelijkertijd is, zou dit een status zonder territoriale soevereiniteit veroorzaken[173]. Anderen zijn van mening dat cyberspace losstaat van de fysieke wereld, maar dat analogieën mogelijk zijn, terwijl de meest radicale meningen cyberspace als non-territoriaal zien[174], wat rechtsstelsels en regels die gebaseerd zijn op geografische ligging (zoals territoriale soevereiniteit) nutteloos maken[175]. De *Tallinn-manual* is dan weer de eenvoudigste: activiteiten in cyberspace die gebruikmaken van de infrastructuur van een staat, vallen onder de soevereiniteit van die staat[176].

45. Deze theorieën zijn niet zonder discussie. Zo is de theorie om cyberspace als een *global common* te zien moeilijk verenigbaar met het feit dat cyberspace in essentie door de mens is gemaakt, en dus op een zeker tijdstip eigendom van iemand geweest is, en dus onder de soevereiniteit van deze of gene staat lag[177]. Deze zienswijze wordt

[168] S. APPLEGATE, *The Principle of Maneuver in Cyber Operations*, NATO publications, Tallinn, 2012, www.academia.edu; zie ook X, "Washington et Pékin négocient un accord de non-agression dans le cyberspace", *Le Monde*, 20 september 2015, lemonde.fr.
[169] www.bmi.bund.de; KREMER, MÜLLER, 43.
[170] European Commission, *Cybersecurity of the European Union: An open, safe and secure cyberspace*, 7 februari 2013, www.eeas.europa.eu.
[171] NASU, MCLAUGHLIN, 76.
[172] NASU, MCLAUGHLIN ,77.
[173] S. BARNEY, "Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of cyberspace", *Naval Law Review*, nr. 48, 2001, 56-83.
[174] S. KOBRIN, "Territoriality and the governance of cyberspace", *Journal of International Business Studies*, nr. 32, 2001, 688-689.
[175] D. JOHNSON, D. POST, "Law and Borders: the rise of law in cyberspace", *Stanford Law Review*, nr. 48, 1996, 1367.
[176] *Tallinn-manual*, 25.
[177] NASU, MCLAUGHLIN, 79.

dan ook door staten gebruikt: via het eigendomsrecht van personen of entiteiten proberen staten soevereiniteit uit te oefenen. Deze visie kan als een analogie gezien worden met de vlaggenstaat op schepen: wie de eigendom heeft over een stuk data, bepaalt welke staat soevereiniteit kan uitoefenen, ongeacht de locatie (*origin-of-data*-mechanisme)[178]. De theorie dat cyberspace een ruimte op zich is, los van geografische beperkingen, stuit dus op de praktijk dat staten soevereiniteit proberen te verwerven[179]. Aangezien staten ook de data kunnen beperken (bijvoorbeeld de Chinese censuur op bepaalde internetsites)[180], lijkt het dus het best om het probleem van cyberspace pragmatisch op te lossen[181]: **cyberspace** volgt de geografische grenzen van de infrastructuur en eigendomsrechten die de cyberspace vormgeven[182]. Deze praktijkoplossing is echter niet definitief, het debat ligt nog steeds open[183]. Of deze pragmatische definitie enig nut heeft voor de toepassing van internationaal recht, zal verder besproken worden.

5. Cyberwapens

46. Conventionele oorlogen kennen een gebied (lucht, land of zee), kunnen overgaan tot gewapende aanvallen en kennen conventionele wapens. De vraag is nu of die regel ook naar het cyberdomein kan worden doorgetrokken: kunnen cybertoepassingen (software, computers etc.) zo gemaakt worden, dat zij als 'wapen' gedefinieerd kunnen worden?

47. Eerst moet men natuurlijk kijken wat de bestaande definitie van een 'wapen' is. Eén definitie van wapen is de volgende:

> *"[…] a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects."*[184]

[178] *Ibid*.; *Tallinn-manual*, 25.
[179] GOMBEER, 198.
[180] L. JYH-AN, L. CHING-YI, "Forbidden City enclosed by the great firewall: the law and power of internet filtering in China", *Minnesota Journal of Law Science and Technology*, nr. 13(1), 125-151.
[181] DINNISS, 29.
[182] Wat neerkomt op de stelling die in de *Tallin-manual* wordt aangegeven; NASU, MCLAUGHLIN, 80.
[183] NASU, MCLAUGHLIN, 83.
[184] HUMANITARIAN POLICY AND CONFLICT RESEARCH, *Manual on International Law Applicable to Air and Missile Warfare*, Harvard University, Cambridge, 2009, 6 (hierna: HPCR).

Deze studie aan de universiteit van Harvard geeft in de commentaar bij dit werk uitdrukkelijk aan dat de kracht die de schade veroorzaakt niet kinetisch moet zijn[185]. Om als wapen te worden gezien, moet het object/programma wel bedoeld, gemaakt of gebruikt worden om schade toe te brengen[186]. Het commentaar bij de handleiding geeft zelfs een voorbeeld van wat deze handleiding als wapen zou zien: een cyberaanval op de systemen van een luchtverkeerstoren, die vliegtuigen zou laten neerstorten[187]. Indien men dit combineert met de visie van SCHMITT, die stelt dan een cyberaanval redelijkerwijs geacht moet worden om schade, verwondingen of dood toe te brengen[188], lijkt het dus logisch dat een cybertoepassing, die een cyberaanval teweeg brengt met de gevolgen als beschreven, een cyberwapen is[189].

48. Indien de cybertoepassing echter niet redelijkerwijs geacht wordt om schade, verwondingen of dood teweeg te brengen, kan er geen sprake zijn van cyberwapens[190]. Behalve cybertoepassingen die beneden deze drempel vallen, kan echter gesteld worden dat cyberwapens bestaan[191]. Dit heeft belangrijke gevolgen: ingevolge de *Nuclear Weapons*-opinion geldt het internationaal (humanitair) recht ten aanzien van alle soorten wapens, waaronder nu dus ook cyberwapens. Wat dit precies inhoudt, wordt verder besproken.

C. Aannames voor deze Masterproef

49. Hoewel voor beide voorgaande definities en termen (cyberoorlog en cyberspace) geen exacte, unaniem aanvaarde oplossingen te vinden zijn, zal deze masterproef toch enkele aannames maken:

1) cyberoorlog bestaat, door de mogelijkheid dat cyberaanvallen *gewapende aanvallen* in de zin van art. 51 VN Handvest kunnen zijn, en houdt zowel aanvallen *van* niet-statelijke actoren als aanvallen *op* niet-statelijke actoren in;

[185] HUMANITARIAN POLICY AND CONFLICT RESEARCH, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, Harvard University, Cambridge, 2010, 55 (hierna: HPCR, *Commentary*).
[186] W.H. BOOTHBY, *Conflict Law: The Influence of New Weapons, technology, Human Rights and Emerging Actors*, Asser Press, Den Haag, 2014, 67 (hierna: BOOTHBY).
[187] HPCR, *Commentary*, 55.
[188] *Tallinn-manual*, 92
[189] BOOTHBY, 67: de vergelijking met een pistool wordt hier gemaakt, waar, net zoals men door het indrukken van de enter-toets op een toetsenbord de cybertoepassing wordt 'gelanceerd', het overhalen van de trekker de kogel 'lanceert'.
[190] BOOTHBY, 67.
[191] FRANCEUS, 14.

2) cyberspace bestaat en volgt de 'klassieke' soevereiniteitsgrenzen: alles wat geografisch binnen een staat ligt, valt onder diens soevereiniteit, alsook alles wat oorspronkelijk gemaakt is in die staat (*origin-of-data*-mechanisme).
3) cyberwapens bestaan, indien de cybertoepassing die als wapen wordt gezien, bedoeld, gebruikt of gemaakt is om een wapen te zijn, en het gebruik redelijkerwijs schade, verwondingen of dood teweeg kan brengen.

Dit zijn slechts drie aannames, maar om te bepalen hoe de internationaalrechtelijke regels kunnen (of juist niet kunnen) toegepast worden op cyberoorlog, is het vanzelfsprekend eerst noodzakelijk geweest om het bestaan van cyberoorlog te verifiëren, en om het territorium waar het zich afspeelt af te bakenen. Aangezien dit nu is gedaan (alhoewel er geen definitieve oplossing voor de problematiek van cyberspace bestaat en steeds rekening moet worden gehouden dat dit een interim-oplossing is), kan het hoofddeel van deze masterproef, namelijk de toepasbaarheid van het algemeen internationaal recht op cyberoorlogen, bestudeerd worden.

IV. HET ALGEMEEN VERDRAGSRECHT

A. Structuur

50. In dit deel zullen enkele cruciale vraagstukken van het internationaal recht bestudeerd worden, om na te gaan of de voor handen zijnde regels toepasbaar zijn op cyberoorlogen, via de besproken Martensclausule. Die studie zal steeds volgens hetzelfde patroon verlopen:

1) Bespreking en toelichting van het thema: waarover gaat het, waarom komt het aan bod en hoe past het in het kader van cyberoorlog?
2) Hoe regelt het internationaal recht dit onderwerp?
3) Is het toepasbaar in het specifieke kader van cyberoorlogen (via interpretatie van de bestaande regels)?
4) Indien niet, hoe kan dit probleem opgelost worden?

Er dient echter opnieuw te worden benadrukt dat niet *alle* vraagstukken van het internationaal recht behandeld kunnen worden, deels door het plaatsgebrek en deels door

het feit dat het onmogelijk is om alle mogelijke gevolgen van een cyberaanval na te gaan, voor die gevolgen zich gesteld hebben. Daarom zullen in deze masterproef enkele elementaire thema's behandeld worden, naast thema's die een grote actuele waarde hebben (bijvoorbeeld cyberaanvallen van niet-statelijke actoren, cyberspionage etc.).

B. De toerekenbaarheid aan staten

51. Het is niet steeds duidelijk of een cyberaanval het werk is van een staat (een overheid), dan wel van private actoren (*hacktivists*, terroristen). Indien de oorsprong bij private actoren ligt, wordt het vraagstuk van staatsaansprakelijkheid enorm moeilijk[192]. Een groeiende vraag in het internationaal recht bestaat erin om elke cyberaanval toe te rekenen aan het land van herkomst, ongeacht of een aanval publiek dan wel privaat georganiseerd werd. Dit zou een vaak gebruikte techniek van onder andere China en Rusland teniet doen, die erin bestond om de verantwoordelijkheid van aanvallen af te wijzen, daar ze door private actoren werden uitgevoerd[193].

52. Algemeen zijn staten verantwoordelijk voor *internationally wrongful acts*[194]. Art. 2(a) van de DARS zegt eigenlijk niets anders dan dat een staat aansprakelijk is voor foutief gedrag dat toerekenbaar is aan die staat en een inbreuk op de internationaalrechtelijke verplichtingen uitmaakt. Deze twee cumulatief te vervullen vereisten (toerekenbaarheid en inbreuk) zullen dus zo geïnterpreteerd moeten worden, dat zij toepasbaar zijn op cyberaanvallen. Indien dit niet mogelijk blijkt (bijvoorbeeld door technische redenen), zal een andere manier gevonden moeten worden om staten verantwoordelijk te stellen voor cyberaanvallen gepleegd vanuit hun grondgebied.

1. Toerekenbaarheid

53. Over de toerekenbaarheid aan staten bestond al langer een uitgebreide rechtspraak van internationale gerechtshoven. Onder andere in de *Phosphates in Morocco*[195], de *United States Diplomatic and Consular Staff in Tehran*[196] en de *Dickson Car Wheel*

[192] GOLDSMITH, "How Cyber changes the Laws of War", 135; zie ook de correspondentie met VAN RAEMDONCK, BIJLAGE 1
[193] *Ibid*.
[194] *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, Verenigde Naties, 2001, www.legal.un.org (hierna: DARS); *Tallinn-manual*, 35.
[195] PCIJ, *Phosphates in Morocco*, 1938, Series A/B, nr. 74.
[196] PCIJ, *United States Diplomatic and Consular Staff in Tehran*, 1980, *P.C.I.J. Reports 1980*, p. 3 e.v.

Company[197] cases werd beslist dat een staat slechts aansprakelijk kan zijn als er toerekenbaarheid is[198]. Die toerekenbaarheid wordt soms als het 'subjectieve' element in de beoordeling gezien[199]. Sommige activiteiten van staten zullen slechts toerekenbaar zijn indien zij doelbewust of met medeweten van de staten zijn gebeurd. Zo kan men dus argumenteren dat een privaat uitgevoerde cyberaanval, die met medeweten of onder druk of op vraag van een overheid wordt ingezet, toerekenbaar is aan die staat.

54. Niet alleen acties, maar echter ook nalatigheid kan een basis opleveren voor die toerekenbaarheid. Ook dit is reeds langer gekend in de rechtspraak[200]. In de *Corfu Channel*-zaak oordeelde het Internationaal Gerechtshof dat de Albaanse overheid aansprakelijk was voor de opgelopen schade, aangezien het wist of had moeten weten dat er mijnen in de territoriale wateren te vinden waren. Er kan hier ook een analogie worden getrokken: indien een staat weet of had moeten weten dat een cyberaanval vanuit hun grondgebied werd ingezet, zou dit een toerekenbare daad kunnen zijn. Dit zal echter enkel het geval zijn indien de personen die de aanval uitoefenden, personen zijn die namens de staat handelden[201]. Deze problematiek wordt in hoofdstuk II van de Draft Articles on Responsibility of States for Internationally Wrongful Acts (kortweg DARS) behandeld.

55. De meeste bepalingen in dit tweede hoofdstuk vormen geen problemen voor cyberaanvallen. Zo zullen aanvallen die uitgevoerd worden door staatsorganen[202], personen of entiteiten die bepaalde elementen van staatsautoriteit uitoefenen[203] of aanvallen uitgevoerd onder de controle of regie van een staat[204] logischerwijs leiden tot staatsaansprakelijkheid. Zoals gezegd vormt dit echter niet de kern van de problematiek. Aanvallen uitgevoerd door privépersonen, waarvan de overheid ieder medeweten kan ontkennen, kunnen toch door die overheid bevolen of op zijn minst gedoogd worden[205]. Enkel indien een staat nadien de cyberaanval zou opeisen[206], is deze problema-

[197] UNRIAA, *Dickson Car Wheel Company (U.S.A.) v. United Mexican States*, 1931, vol. IV, 669 e.v.
[198] M. DIXON, *Textbook on International Law*, Oxford University press, Oxford, 2013, 257-258 (hierna: DIXON).
[199] *Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentary*, Verenigde Naties, 2001, www.legal.un.org, 34 (hierna: DARS, *commentary*).
[200] Naast de *United States Diplomatic and Consular Staff in Tehran*-case, zie: IGH, *Corfu Channel*, 1949, *ICJ Reports 1949*, p. 4 e.v.
[201] DARS, *commentary*, 35.
[202] Art. 4 DARS.
[203] Art. 5 DARS.
[204] Art. 8 DARS.
[205] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 10; de vergelijking wordt gemaakt met de kapers uit de 17de-18de eeuw, die door de overheid

tiek eenvoudig op te lossen. In principe is een staat immers niet aansprakelijk voor daden van individuen[207], behalve in de voorgaande situatie. Indien er geen opeising gebeurt, zal de aangevallen staat moeten bewijzen dat de privépersonen onder de controle van hun overheid stonden[208]. Dit bewijs is door de razendsnelle evolutie van digitale netwerken echter niet vanzelfsprekend[209].

56. Dat bewijs kan geleverd worden door een feitelijke band tussen de individuen en de staat aan te tonen[210]. Deze situatie is in de rechtspraak voordien al vaak aan bod gekomen en dus algemeen aanvaard[211]. Het probleem blijft echter dat het bewijs leveren moeilijker is in de cyberspace, waardoor het in de praktijk onmogelijk wordt[212]. Zelfs indien een bepaalde schuldige kan worden aangewezen, moet nog bewezen worden dat die volgens de richtlijnen of onder de controle van een staat handelde[213]. Dit bewijs kan lichter of zwaarder uitvallen, naargelang van de omstandigheden van de zaak[214]. Aangezien het bewijs in geval van cyberaanvallen enorm moeilijk is[215], kan geargumenteerd worden dat een lichte bewijslast aanvaardbaar zou zijn, of zelfs een omgekeerde bewijslast: vanaf het redelijkerwijze aannemelijk is dat een aanval uitgevoerd werd onder de controle of op vraag van een staat (bijvoorbeeld af te leiden door het doel van de aanval[216]), zou het aan die staat zijn om te bewijzen dat de aanval *niet* toerekenbaar is[217]. De vraag is natuurlijk of dergelijk voorstel ooit genoeg consensus zou vinden om effectief internationaalrechtelijk afdwingbaar te worden[218]. Een

gemachtigd werden om als privépersoon piraterij te bedrijven. De 21ste-eeuwse 'kapers' kunnen dan privé-entiteiten zijn die cyberaanvallen uitvoeren; *Tallinn-manual*, 37.

[206] Art. 11 DARS.

[207] DIXON, 259-260.

[208] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 11; zij zijn van mening dat dergelijke activiteiten naar alle waarschijnlijkheid regelmatig worden gepland, en dat de overheid (*in casu* de Verenigde Staten van Amerika) daar een gepast antwoord op moet bieden.

[209] V. KUMAR, J. SRIVASTAVA, A. LAZAREVIC (*eds.*), *Managing Cyber Threats – Issues, Approaches and Challenges*, Springer press, New York, 2005, 313-314 (hierna: KUMAR, SRIVASTAVA, LAZAREVIC); deze uitleg is vrij computertechnisch, daarom wordt voor een meer gedetailleerde beschrijving naar het geciteerde werk verwezen.

[210] DARS, *commentary*, 47.

[211] DARS, *commentary*, 47, wat verwijst naar UNRIAA, *Zafiro*, 1925, Vol. VI, p. 160 e.v.; *Lehigh Valley Railroad Company and Others (U.S.A.) v. Germany: "Black Tom" and "Kingsland" incidents*, 1930, Vol. VIII, p. 84 e.v. en p. 1939 e.v.

[212] Zie nr. 55.

[213] DARS, *commentary*, 47.

[214] *Tadic*-case.

[215] CAVV, 22.

[216] Of dat de aanval gebruik maakt van overheidsinfrastructuur; *Tallinn-manual*, 39.

[217] Deze methode lijkt deze auteur meer proportioneel dan het systeem vermeld in GOLDSMITH, waar er een automatische toerekening plaatsvindt vanaf het moment dat er een cyberaanval plaatsvindt. Er kan niet van alle staten verwacht worden dat zij alle internetactiviteit van hun onderdanen volgt om dergelijke aanval te vermijden.

[218] Waarschijnlijk niet, gelet op het feit dat de algemene regels inzake staatsaansprakelijkheid nog steeds officieel een ontwerpversie zijn, hoewel resolutie 56/83 van de Algemene Vergadering van de Verenigde Naties van 12 december 2001 staten aanmoedigde om hun aandacht op deze regels te vestigen. Er moet echter toegevoegd worden dat deze ontwerptekst grote invloed uitoefent op het internationaal recht: J. CRAWFORD, J. PEEL, S. OLLESON,

andere zienswijze stelt dat een staat aansprakelijk zou zijn voor elke cyberoperatie die vanuit diens grondgebied vertrekt[219]. Deze visie is niet alleen erg verstrekkend, maar soms ook ongewenst: staat A kan een groepering in staat B opdracht geven om via een netwerk in staat C een operatie tegen staat D uit te voeren. Staat A zou verantwoordelijk moeten zijn, maar volgens de voorgaande redenering zou dit staat B zijn[220].

57. Het toerekenen van gedragingen van privépersonen zonder een duidelijke affiniteit met een staat wordt expliciet beperkt in het internationaal recht[221]. In de *Tellini*-case besliste de Volkenbond dat staten enkel aansprakelijk zijn voor acties van individuen, indien die staat niet alle redelijke middelen heeft ingezet voor de preventie van die actie (indien ze een misdaad uitmaakt)[222]. Op het vlak van cyberoorlogen betekent dit dus dat staten aan aansprakelijkheid kunnen ontsnappen indien niet bewezen kan worden dat zij de cyberaanval hebben bevolen, gedoogd of anderzijds privépersonen daartoe hebben aangezet, behalve indien die staten geen redelijke maatregelen hebben genomen om dergelijke aanvallen te vermijden of nadien te bestraffen. Deze laatste uitzondering op de principiële niet-toerekenbaarheid, wordt wel sterk benadrukt: staten moeten redelijkerwijs privépersonen op hun grondgebied verhinderen om *internationally wrongful acts* uit te voeren[223].

2. Inbreuk

58. Indien een staat zou kunnen bewijzen dat een cyberaanval toerekenbaar is aan een andere staat, moet die aanval verder een inbreuk op de internationale verplichtingen van de aanvallende staat uitmaken. Gezien een cyberaanval in sommige gevallen gewapend geweld uitmaakt[224] en dit verboden is onder art. 2(4) VN Handvest, zal dit in die gevallen geen probleem opleveren. Maar niet elke cyberaanval overtreft de noodzakelijke drempel om gewapend geweld op te leveren. Spionage door middel van cyberaanvallen (bijvoorbeeld het hacken van overheidsdatabases) is niet verboden onder

"The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading", *EJIL*, 2001, vol. 12 nr. 5, 987-988.
[219] GOLDSMITH, "How Cyber changes the Laws of War", 135.
[220] *Tallinn-manual*, 38.
[221] DARS, *commentary*, 38.
[222] Volkenbond, *Official Journal*, Jaargang 4, nr. 11, 1349.
[223] DARS, *commentary*, 39.
[224] Indien het een bepaalde drempel overschrijdt, zie nr. 29 e.v.

het internationaal recht[225]. Deze 'kleinere' aanvallen zijn dus moeilijker in te delen dan grootschalige cyberaanvallen.

59. Indien die kleinere aanvallen een inbreuk op een verdrag uitmaken, dan is er zeker sprake van een *wrongful act*[226]. In het geval er tussen staten een verdrag bestaat dat bijvoorbeeld spionage verbiedt, zou een cyberaanval gericht op spionage aanleiding geven tot aansprakelijkheid. Er moet wel op gewezen worden dat louter nationaalrechtelijke regels die bijvoorbeeld spionage verbieden de aansprakelijkheid van de aanvallende staat niet in het gedrang brengen: enkel internationaalrechtelijke normen worden in aanmerking genomen[227], wat ook reeds lang in de rechtspraak werd bevestigd[228].

60. Indien de relaties tussen staten niet door een verdrag worden geregeld en de aanval de drempel van gewapend geweld niet overschrijdt, zal het aan de aangevallen staat toekomen om te bewijzen dat de aanvaller ook diens andere internationaalrechtelijke verplichtingen niet te goeder trouw is nagekomen[229]. Dit zou bijvoorbeeld kunnen door een inbreuk op het non-interventiebeginsel aan te tonen[230]: als de aangevallen staat kan aantonen dat de aanval een ongeoorloofde interventie uitmaakt, is dit vanzelfsprekend ook een inbreuk op de internationaalrechtelijke verplichtingen. De kans dat dit bewijs slaagt, hangt ervan af hoe dergelijke interventie wordt gezien: algemeen wordt aangenomen dat een interventie een inmenging in de interne of buitenlandse zaken van een andere staat uitmaakt[231]. In de *Nicaragua*-case werd dit verder uitgelegd: indien de interventie de vrije keuze van een staat in politieke, economische, sociale of culturele overwegingen belemmert, is er sprake van interventie[232]. Als een kleinschalige aanval dus gezien kan worden als dwang die de vrije keuze in die overwegingen belemmert, kan de aanvallende staat aansprakelijk worden gesteld.

[225] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 11.
[226] DARS, *commentary*, 35.
[227] Art. 3 DARS.
[228] Zie o.a. PCIJ, *S.S. "Wimbledon"*, 1923, *P.C.I.J. Series A nr. 1*, p. 15 e.v.
[229] DARS, *commentary*, 37; verwijst naar de oorspronkelijke artikelen inzake staatsaansprakelijkheid: Resolutie 375(IV) van de Algemene Vergadering van de Verenigde Naties van 6 december 1949.
[230] *Tallinn-manual*, 35.
[231] P. KUNIG, "Intervention, Prohibition of", *MPEPIL*, OPIL, april 2008, www.opil.ouplaw.com, nr. 1 (hierna: KUNIG, "Intervention, Prohibition of").
[232] *Nicaragua*-case, par. 205.

61. De inbreuk op een internationaalrechtelijke verplichting moet *in concreto* worden beoordeeld[233]. De bepalingen in hoofdstuk III DARS zijn richtlijnen eerder dan strikte regels, die de casuïstische beoordeling kunnen helpen. Zo bepaalt art. 12 dat de oorsprong of aard van de verplichting er niet toe doet: zowel verdrags- als gewoonterecht kunnen verplichtingen opleggen, net als een uitspraak van een internationaal hof[234]. Er moet dan weer wel voor ogen worden gehouden dat art. 13 staten vrijstelt van aansprakelijkheid indien de verplichting niet bestond ten tijde van de bewuste daad[235]. Vooral in het kader van cyberoorlog kan dit van belang zijn: indien er geen verbod bestaat om cyberaanvallen die geen gewapend geweld uitmaken uit te voeren, dan valt op dit tijdstip niets aan te vangen, ongeacht de schade die de aanval teweeg kan brengen. Op dit punt zou een verdrag of in elk geval een reeks van interstatelijke afspraken soelaas kunnen bieden. Deze eventuele regels zullen evenwel nooit toegepast kunnen worden op de huidige cyberaanvallen[236], waardoor die tussen de mazen van het aansprakelijkheidsnet dreigen te glippen. Dit wordt ook bevestigd in art. 14: de inbreuk wordt vastgesteld op het moment van de daad, ongeacht of de effecten nadien nog voelbaar zijn. *A contrario* geldt dus het volgende: indien dus nu een cyberaanval wordt uitgevoerd, die geen inbreuk uitmaakt, zullen de gevolgen ook geen inbreuk uitmaken, ongeacht of net na die aanval een verdrag zou worden ondertekend en geratificeerd.

62. Er dient nog een kleine kanttekening te worden gemaakt, die verband houdt met wat verder gezegd wordt in verband met de neutraliteit van een staat[237]. Zoals daar verder uitgelegd, verliest een staat enkel zijn neutraal karakter indien het willens en wetens zijn infrastructuur ter beschikking stelde om een cyberoperatie te faciliteren. Het feit dat dergelijke operatie via de netwerken van die staat uitgevoerd werd zonder medeweten van die staat, is geen inbreuk op de neutraliteit[238]. Art. 16 DARS stelt ook dat een staat enkel aansprakelijk is voor hulp of assistentie bij inbreuken op het internationaal recht, indien die staat kennis had van de daad en de daad ten aanzien van die

[233] DARS, *commentary*, 54.
[234] DARS, *commentary*, 55; wat opnieuw ook in de rechtspraak is bevestigd: UNRIAA, *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 1986 between the two States and which related to the problems related to the Rainbow Warrior affair*, 1990, *Vol. XX*, p. 215 e.v.
[235] Wat opnieuw in de rechtspraak en statenpraktijk veelvuldig terugkomt: zie DARS, *commentary*, 57-58 voor de relevante voetnoten en verwijzingen.
[236] DARS, *commentary*, 58.
[237] Zie *infra*.
[238] Zie ook: *Tallinn-manual*, 40.

staat een inbreuk uitmaakt. Staat A die verdragsrechtelijk gehouden is om geen cyberaanvallen uit te voeren op staat B, zou staat C kunnen aanspreken om die aanval uit te voeren: C is niet door een verdrag gebonden en kan, als de aanval kleinschalig genoeg is, door de mazen van het net glippen. Dit wordt door art. 16 uitgesloten: indien het doel van een derde staat was om een effectieve inbreuk te faciliteren, is ook die derde staat aansprakelijk[239].

3. Uitsluitingsgronden en herstel

63. Er moet ook rekening gehouden worden met enkele bepalingen die een staat vrijstellen van aansprakelijkheid. Zo geeft het recht op zelfverdediging staten het recht om een *in se* verboden cyberoperatie uit te voeren, maar die in het kader van zelfverdediging wel te rechtvaardigen is[240]. Nochtans blijven sommige operaties uitgesloten: zo zou het nog steeds verboden kunnen zijn om via een cyberaanval kerncentrales over te nemen en te laten ontploffen[241]. Sommige acties zijn zeker verboden[242]. Ook overmacht kan een uitsluitingsgrond inhouden (art. 23): zo kan bijvoorbeeld een vliegtuig door storm gedwongen worden om in het luchtruim van een staat te vliegen, hoewel dit vliegtuig daar de nodige toestemming niet voor had[243]. Dit is niet noodzakelijk uitgesloten in het kader van cyberoperaties. Hoewel hiervoor geen bronnen te vinden zijn en het voorbeeld volledig aan de fantasie van de auteur is toe te wijzen, kan men de volgende situatie inbeelden: indien bijvoorbeeld een stuwdam elektronisch gecontroleerd wordt, maar die controle plots onmogelijk wordt (een fout in het systeem, een virus van een andere staat, technische stoornissen), kan het gevaar ontstaan dat de dam doorbreekt. Indien een andere staat daarvan het slachtoffer zou kunnen worden, zou die staat in dit geval het recht hebben om op afstand een cyberoperatie uit te voeren, teneinde de controle over de stuwdam te herstellen.

64. Zelfs indien een staat aansprakelijk zou zijn en er geen uitsluitingsgrond voorhanden is, spreekt het herstel voor de gevolgen van dergelijke actie niet voor zich. Zo moet een staat de "gepaste zekerheden en garanties bieden" dat de inbreuk zich niet zal herhalen (art. 30). Hoe die garanties eruit moeten zien op het vlak van cyberoorlog, is zeker niet duidelijk. Indien het al mogelijk is om een staat te linken aan een

[239] DARS, *commentary*, 66.
[240] Art. 21 DARS.
[241] Over die problematiek: zie *infra*.
[242] DARS, *commentary*, 75; *Nuclear Weapons-opinion*, par. 30.
[243] DARS, *commentary*, 77, verwijzing in de daar opgenomen voetnoot 351.

operatie uitgevoerd door privépersonen, zal die staat in het vervolg enkel omzichtiger te werk gaan in het uitvoeren van die operaties. Art. 31 legt de aansprakelijke staat de verplichting op om de schade te herstellen die diens actie veroorzaakt heeft. Ook dit is niet zonder problemen in de digitale context: zo kan na een spionageoperatie moeilijk nog van herstel sprake zijn, indien de gestolen informatie toch al gekend is door de buitenwereld. In dit geval kunnen art. 34 *juncto* art. 36 enige redding brengen, daar het stelt dat, indien reparatie *in natura* niet mogelijk is, compensatie ook een geldige vorm van herstel uitmaakt[244].

4. Conclusie

65. Op het vlak van staatsaansprakelijkheid naar aanleiding van een cyberaanval bevat het internationaal recht nogal wat hiaten. Die zijn eigen aan het karakter van cyberaanvallen: de moeilijkheid om digitale aanvallen te lokaliseren en toe te wijzen, en het gebrek aan statenpraktijk of andere specifieke regels, door de relatieve nieuwheid van het fenomeen. Zoals gezegd, bestaat de grootste moeilijkheid erin om aan te tonen dat privépersonen onder controle of op vraag van overheden aanvallen uitvoerden[245]. Anders is de staat enkel aansprakelijk indien het redelijkerwijs niet de nodige maatregelen heeft genomen om dergelijke aanvallen te vermijden. Deze masterproef stelt daarom voor om de bewijslast voor de aangevallen staat te verlichten: indien er voldoende elementen aanwezig zijn die een andere overheid kunnen incrimineren, zou het aan die overheid zijn om aan te tonen dat zij *niet* achter de cyberaanval zitten[246].

66. Zelfs als deze omgekeerde bewijslast zou helpen met het toerekenen van aanvallen aan staten, moeten deze aanvallen nog inbreuken uitmaken. Dit is ook niet eenvoudig, aangezien enkel aanvallen die de drempel van gewapend geweld overschrijden zeker een inbreuk uitmaken. Andere daden zijn veel moeilijker als inbreuk te zien, behalve als een verdrag die daden verbiedt of indien die daden een inbreuk op het non-interventiebeginsel zouden uitmaken. Dan nog blijven vele cyberoperaties buiten schot (bijvoorbeeld spionage). Een eventueel verdrag of statenpraktijk zou dit probleem verhelpen voor de toekomst, maar huidige cyberoperaties zouden in dat ge-

[244] Wat ook in de rechtspraak terug te vinden is: UNRIAA, *Lusitania*, 1923, *Vol. VII*, p. 32 e.v.; PCIJ, *Factory at Chorzow*, 1927, *P.C.I.J. Series A, nr. 17*, p. 29 e.v.
[245] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 11.
[246] Zie nr. 56.

val buiten schot blijven en dus niet voor aansprakelijkheid vatbaar zijn. Staten zijn dus in zeker zin immuun voor kleinschalige cyberoperaties, die geen grote gevolgen hebben voor de aangevallen staat, maar wel nadelige effecten hebben.

67. Bovenstaande pijnpunten voor wat betreft herstel, tonen aan dat het traditionele internationaal aansprakelijkheidsrecht voor staten tekortschiet op het vlak van cyberoperaties. Hierboven werden slechts enkele voorbeelden, zoals spionage, gegeven, die echter aantonen dat deze frequent voorkomende operaties[247] tussen de mazen van het net glippen: indien dergelijke operatie al tot aansprakelijkheid kan leiden, is het herstel voor die inbreuk nog minder vanzelfsprekend. Enig voorstel tot verbetering aanbieden is moeilijk: de omkering van de bewijslast[248] en het invoeren in verdrag of statenpraktijk van een lijst (al dan niet limitatief) van gedragingen die een inbreuk op de internationale verplichtingen uitmaken, zouden al een stap in de goede richting uitmaken, maar het is maar de vraag of deze voorstellen ooit genoeg consensus zouden vinden om effectief tot positief recht uit te groeien.

C. Het transnationaal karakter van cyberoorlogen

68. Zoals hierboven gesteld, volgt cyberspace de klassieke indeling wat betreft soevereine grenzen, als gevolg van de praktijk die staten erop nahouden. Dat wil daarom niet zeggen dat deze situatie alle gevolgen van een cyberoorlog regelt. Zo beperkt het recht der gewapende conflicten de vijandelijkheden tussen twee of meer staten tot die staten[249]. Op deze manier worden de rechten van neutrale staten gewaarborgd, via deze zogenaamde 'wet van neutraliteit', wat deels door het internationaal gewoonterecht is ontwikkeld en deels gecodificeerd werd in Den Haag 1907[250]. In geval van cyberoorlog stelt zich hier echter een enorm probleem: als staat A een cyberaanval uitvoert op staat C, kan die aanval gebeuren via de digitale infrastructuur van neutrale staat B, die zich daar niet eens van bewust hoeft te zijn[251]. Maar gelet op de pragmatische definitie van cyberspace, valt die infrastructuur onder de soevereiniteit van die neutrale

[247] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 12.
[248] Zoals gezegd in tegenstelling tot een algemene aansprakelijkheid van staten voor elke cyberoperatie vanuit hun grondgebied; dergelijke regel zou te verregaand zijn en waarschijnlijk nooit genoeg steun krijgen om effectief geïmplementeerd te worden; zie voetnoot 217.
[249] H. DUFFY, *The 'War on terror' and the framework of international law*, Cambridge University Press, Cambridge, 2005, 223.
[250] Voornamelijk Conventie V: Verdrag betreffende de rechten en plichten van neutrale mogendheden en personen in geval van oorlog te land.
[251] NASU, MCLAUGHLIN, 82-83.

staat B[252]. De vraag stelt zich dan of van neutraliteit nog sprake kan zijn in de digitale context. Verder stelt de cyberspace de regulering van niet-internationale gewapende conflicten op de proef.

1. Neutraliteit

69. Zoals gezegd ligt het debat over de exacte juridische situatie rond cyberspace nog niet stil. De praktijkoplossing die staten proberen door te voeren en beschreven wordt in de *Tallinn-manual* is slechts een van de mogelijkheden. Indien cyberspace inderdaad een *global common* is, kan de data die voor de aanval gebruikt wordt gerust door de neutrale staat passeren zonder de neutraliteit te schenden, maar indien cyberspace toch onder soevereine controle valt, zou het neutrale karakter van een staat op de helling kunnen komen te staan[253]. In die laatste hypothese moet een onderscheid worden gemaakt tussen het louter versturen van data via die staat, en het effectief gebruik van het territorium of de infrastructuur van de zogenaamd neutrale staat[254].

70. In het eerste geval moet de neutrale staat niet voor zijn status vrezen. In de Haagse Vredesconferentie van 1907 werd al bepaald dat het loutere gebruik van publieke vervoers- en communicatiediensten van een neutrale staat geen schending van die neutraliteit uitmaakt[255]. Aangezien het internet een enorm systeem van datatransmissie is, kan dit gelijkgesteld worden met de telegramlijnen zoals beschreven in de conventie[256]. Deze oefening kan gebruikt worden om de neutraliteit van staten te bewaren, indien zij het onschuldig 'slachtoffer' zijn van datatransmissie door hun netwerken[257]. In het andere geval handelt een staat (of laat het in elk geval handelingen toe), wat duidelijk een schending van de neutraliteit uitmaakt, waar dus ook geen verdere problemen rond rijzen[258].

71. Verder moeten de aanvallers ook de neutraliteit van staten beschermen: indien hun aanval schade of negatieve gevolgen zou teweegbrengen in neutrale staten, is dit ook

[252] Zie nr. 42.
[253] S. KANUCK, "Sovereign Discourse on cyber conflict", *Texas Law Review*, 2010, nr. 88, 1593.
[254] *Ibid*.; NASU, MCLAUGHLIN, 83.
[255] Art. 3, 8, 9 Conventie V van 1907.
[256] NASU, MCLAUGHLIN, 83; E. JENSEN, "Sovereignty and neutrality in cyber conflict", *Fordham International Law Journal*, 2012, nr. 35, 825.
[257] FRANCEUS, 21.
[258] NASU, MCLAUGHLIN, 83.

een inbreuk op de principes van neutraliteit[259]. Deze twee voorgaande punten lijken dan misschien een detailregeling in het grotere geheel van het internationaal recht, maar gezien het onzekere karakter van het rechtsregime van cyberspace, is het van groot belang: waar vroeger staten duidelijk neutraliteit konden afdwingen door niemand toe te laten (men denke aan België in WO I), is de huidige situatie door de datatransmissie veel ingewikkelder geworden. De Haagse Conventies kunnen echter zonder problemen soelaas bieden, via de besproken analogie: het blijft nog steeds verboden om het neutraal karakter van een staat te schenden, terwijl neutrale staten ook geen steun mogen bieden aan een van de partijen[260].

2. Niet-internationale gewapende conflicten

72. Het vraagstuk van de exacte kwalificatie rond cyberoorlog kent een moeilijkere discussie wanneer het gaat over niet-internationale gewapende conflicten. In het geval dat een groepering binnen een staat (*hacktivists*, rebellen, terroristen) een cyberaanval uitvoert tegen de soevereine staat waar zij zich bevindt, hoeven de middelen van die cyberaanval niet noodzakelijk binnen het territorium van die staat liggen[261]. Een van de meest wijdverspreide zienswijzen op deze problematiek volgt uit de zogenaamde *war on terror*: niet de geografische locatie, maar de status van de actoren bepaalt of het over een niet-internationaal gewapend conflict gaat[262]. Deze mening wordt echter niet door iedereen gedeeld, wat SCHMITT ook aangeeft.

73. Deze discussie heeft zijn gevolgen op het vlak van het non-interventiebeginsel. De ene staat kan een niet-statelijke actor in een andere staat (bijvoorbeeld rebellen) steunen via hulp in cyberspace[263]. In het geval van een 'klassiek' niet-internationaal conflict verbiedt het internationaal gewoonterecht de interventie van een staat in de interne zaken van een andere staat[264]. Dit principe is natuurlijk inhoudsloos als in het debat rond cyberspace uiteindelijk beslist wordt dat die cyberspace toch een *global common* is: er is dan immers nooit een inbreuk op de staatssoevereiniteit, en dus nooit een on-

[259] NASU, MCLAUGHLIN, 84; M. BOTHE, "The Law of Neutrality" in D. FLECK (*ed.*), *The Handbook of International Humanitarian Law*, Oxford University press, Oxford, 2013, 549 (hierna: BOTHE, "The Law of Neutrality"); CAVV, 26.
[260] BOTHE, "The Law of Neutrality", 559-562.
[261] NASU, MCLAUGHLIN, 90.
[262] *Tallinn-manual*, 71.
[263] NASU, MCLAUGHLIN, 88.
[264] Reeds beslist in de *Nicaragua*-case; KUNIG, "Intervention, Prohibition of", nr. 7; NASU, MCLAUGHLIN, 88, dat verwijst naar *Verklaring betreffende de ontoelaatbaarheid van interventie en tussenkomst in de interne zaken van Staten*, Algemene Vergadering van de Verenigde Naties, 9 december 1981, *Doc. Nr.* GA RES/36/103.

wettige interventie[265]. Gezien de steeds uitbreidende afhankelijkheid van het internet en cyberspace, lijkt deze positie onhoudbaar, en argumenteren sommigen in de rechtsleer voor een uitbreiding van staatssoevereiniteit naar de mogelijkheid van elementaire beleidsmogelijkheden van die staat. Indien een cyberinterventie die mogelijkheden aantast, is er sprake van een ongeoorloofde interventie[266].

74. Een ander moeilijk en onopgelost vraagstuk rond cyberspace ligt in de *war on terror*. De statenpraktijk van de Verenigde Staten van Amerika houdt in dat territoriale overwegingen overboord worden gegooid en enkel naar de status van de actoren wordt gekeken[267]. Dit betekent dat de Verenigde Staten zich bevoegd achten om gerichte cyberoperaties uit te voeren in soevereine staten tegen terreurdreigingen, indien die soevereine staten niet willen of kunnen helpen, dit terwijl de VS geen partij is in enig gewapend conflict met die bewuste staten[268]. Deze zienswijze biedt duidelijk het voordeel dat de status van de actor (zijnde in conflict met de VS) geldig blijft, ongeacht de locatie van die actor. DASKAL is van oordeel dat, indien de locatie geen beperkende factor is bij de deelname aan de vijandelijkheden (men kan van overal cyberaanvallen uitvoeren), het viseren van die actoren ook niet beperkt zou mogen worden door die locatie[269].

3. Conclusie

75. Het is dus duidelijk dat, in tegenstelling tot de aanname bij deze masterproef, het debat rond cyberspace nog lang niet besloten is. Er zijn talrijke problemen die, wegens de eigenheid van cyberspace, door uiteenlopende oplossingen afgehandeld kunnen worden. Er kan nu enkel met zekerheid gesteld worden dat de statenpraktijk van de VS de status van actoren in rekening brengt om cyberspace af te bakenen, naast de geografische grenzen die er duidelijk nog zijn[270]. De vraag is of deze problematiek via een verdrag kan opgelost worden. De pragmatische definitie uit de *Tallinn-manual*[271]

[265] NASU, MCLAUGHLIN, 88.
[266] R. BUCHAN, "Cyberattacks: unlawful uses of force or prohibited interventions?", *Journal of Conflict and Security Law*, 2012, nr. 17, 223.
[267] J. DASKAL, "The geography of the battlefield: a framework for detention and targeting outside the 'hot' conflict zone", *University of Pennsylvania Law Review*, 2013, nr. 161, 1175 (hierna: DASKAL, "The geography of the battlefield: a framework for detention and targeting outside the 'hot' conflict zone").
[268] *Ibid*.; NASU, MCLAUGHLIN, 89.
[269] DASKAL, "The geography of the battlefield: a framework for detention and targeting outside the 'hot' conflict zone", 1165-1234.
[270] NASU, MCLAUGHLIN, 91.
[271] Zie nr. 45.

lijkt een gemakkelijk haalbare oplossing te bieden, door te stellen dat infrastructuur en origine van de data soevereiniteit in cyberspace afbakenen. Door dit principe te hanteren, kunnen regels in verband met het recht der gewapende conflicten zo geïnterpreteerd worden, dat zij op cyberoorlogen en in cyberspace toepassing vinden[272]. Naar de mening van deze auteur is deze pragmatische toepassing voorlopig te verkiezen, aangezien er geen sprake lijkt van enige consensus die nodig zou zijn om cyberspace af te bakenen in een verdragstekst[273].

D. Cyberaanvallen door niet-statelijke actoren

76. Bij de term "oorlog" denkt men traditioneel aan legers en soldaten, maar ook privépersonen worden en werden ingeschakeld tijdens conflicten tussen staten. Zo werden kapers in de 17de en 18de eeuw gemachtigd om de schepen van een vijandelijke staat aan te vallen[274]. Dit is niet anders op het gebied van cyberoorlog: staten kunnen privé-entiteiten de opdracht geven om cyberoperaties uit te voeren[275]. Daarnaast zijn terrorisme en revolutie/rebellie belangrijke thema's in de huidige wereldpolitiek[276]: actoren zoals de Taliban, IS of de verschillende rebellengroepen in Syrië kunnen in theorie allemaal in aanmerking komen om cyberaanvallen uit te voeren. De vraag stelt zich dan of en hoe het internationaal recht rond niet-internationale gewapende conflicten en niet-statelijke actoren toepasbaar is op cyberoorlogen.

1. Niet-internationale gewapende conflicten

77. Hierboven[277] werd al de problematiek aangehaald dat niet-internationale conflicten door de eigenheid van cyberspace zich veel verder dan (de grenzen van) een staat kunnen uitstrekken. Er moet echter ook nagegaan worden wat precies onder een niet-internationaal gewapend conflict bedoeld wordt in de context van cyberoorlogen. De *Tallinn-manual* oordeelt dat er van een niet-internationaal gewapend conflict sprake is als:

[272] NASU, MCLAUGHLIN, 91.
[273] BOOTHBY, 83.
[274] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 10.
[275] *Ibid*.
[276] *Commentary*, 1325.
[277] Zie nr. 72 e.v.

> *"[…] whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organisation."*[278]

Deze bepaling komt overeen met het gemeenschappelijk art. 3 aan de Conventies van Geneve, dat het recht der gewapende conflicten ook toepasselijk verklaart op niet-internationale gewapende conflicten, naast Protocol II van die Conventies. Deze bepalingen geven echter geen definitie van wat als een dergelijk conflict wordt gezien[279]. Er wordt enkel gesteld dat er een zekere intensiteit voorhanden moet zijn, die hoger ligt dan de drempel om van een internationaal gewapend conflict te spreken[280]. Zo bepaalt art. 1 Protocol II dat de niet-statelijke actoren in een dergelijk conflict een georganiseerd bevel moeten hebben, naast een territorium en de mogelijkheid om aanhoudende en gerichte militaire operaties uit te voeren. Het sluit expliciet sporadische gewelddaden uit. Er dient wel voor ogen te worden gehouden dat indien een situatie in een staat niet voldoet aan de vereisten van art. 1 Protocol II, dit niet noodzakelijk inhoudt dat er geen sprake is van niet-internationale gewapende conflicten. Dit betekent dan dat het conflict onder het gemeenschappelijk art. 3 van de Conventies van Geneve kan vallen[281].

78. Dit algemeen art. 3 (dat eerst wordt besproken, aangezien het als de *lex generalis* kan beschouwd worden[282]) vereist dat er minstens één georganiseerde gewapende groep is[283] en dat de vijandelijkheden een bepaalde graad van intensiteit behalen[284]. Deze organisatiegraad is vereist om ervoor te zorgen dat deze gewapende groep het recht der gewapende conflicten kan toepassen, aangezien er dan sprake kan zijn van 'partijen bij het conflict' (zoals bepaald in art. 3), met bijhorende verantwoordelijkhe-

[278] *Tallinn-manual*, 76.
[279] *Commentary*, 1325.
[280] T. MARAUHN, Z.F. NTOUBANDI, "Armed Conflict, Non-International", *MPEPIL*, OPIL, mei 2011, opil.ouplaw.com, nr. 3-4 (hierna: MARAUHN, NTOUBANDI, "Armed Conflict, Non-International").
[281] BOOTHBY, 32.
[282] *Ibid*.
[283] *Tadic*-case, par. 70; ICC, *Prosecutor v. Thomas Lubanga Dyilo*, 29 januari 2007, ICC-01/04-01/06; BOOTHBY, 32.
[284] Joegoslaviëtribunaal, *Prosecutor v. Limaj*, 30 november 2005, IT-03-66-T, par. 90 (hierna: *Limaj*-case).

den[285]. Indien aan deze voorwaarden is voldaan, moeten de regels in art. 3 worden gevolgd. Indien ook de voorwaarden van art. 1 Protocol II (zie *infra*) voldaan zijn, moet de bescherming van dat protocol samen met Gemeenschappelijk art. 3 toegepast worden[286].

79. De voorwaarden bij art. 1 Protocol II zijn gelijkaardig. Het commentaar bij deze bepalingen geeft aan dat de voorwaarden in art. 1 objectieve criteria zijn, die indien zij vervuld zijn automatisch een conflict als niet-internationaal bestempelen[287]. Het moet ten eerste gaan om een conflict tussen de overheid van een staat en georganiseerde opstandelingen. Een groot minpunt, zeker in de huidige politiek in onder andere Syrië, is dat de situatie wordt uitgesloten waarin enkel gewapende opstandelingen onderling vechten, zonder dat een overheid tussenkomt. Op dit soort conflict is enkel Gemeenschappelijk art. 3 van de Conventies van Geneve van toepassing[288]. Daarnaast moeten deze gewapende groepen een commandostructuur volgen, die zowel plannen kan maken als discipline uitoefenen over de gewapende groepen.

80. Verder moeten die gewapende groepen een deel van het territorium van de staat onder hun *de facto* controle hebben. Hoe groot dit deel moet zijn, is echter niet bepaald[289]. De commentaren beschrijven specifiek de situatie waarin de ene groepering een stadscentrum controleer, terwijl de andere de buitenwijken in bezit heeft. Die controle moet zodanig zijn dat het die groepen in staat stelt om de provisies in het Protocol toe te passen (zoals zorg voor krijgsgevangenen of gewonden). Die controle moet bovendien enigszins stabiel zijn: een constante verandering van territorium zal die controle moeilijk maken, waardoor een conflict niet als niet-internationaal kan worden gezien[290].

81. Zoals gezegd, is de belangrijkste voorwaarde die van de intensiteit van de vijandelijkheden. De aanvallen of operaties moeten "voortdurend en aanhoudend" plaatsvinden, volgens een bepaalde strategie. Intensiteit op zich werd niet toegevoegd, aangezien dit een subjectief element aan de definitie zou toevoegen. Enigszins paradoxaal

[285] S. SIVAKUMARAN, *The law of non-international armed conflict*, Oxford University Press, Oxford, 2012, 177.
[286] BOOTHBY, 35.
[287] *Commentary*, 1351.
[288] *Ibid*.
[289] *Commentary*, 1352.
[290] *Commentary*, 1353.

geeft het commentaar daarna aan dat een voortdurende en aanhoudende militaire operatie een zekere intensiteit inhoudt, wat beoordeeld moet worden om na te gaan of er van voortdurende en aanhoudende militaire operaties sprake zijn[291]. De *Tallinn-manual* kan dus terecht stellen dat een graad van intensiteit vereist is om van een niet-internationaal gewapend conflict te spreken.

82. Dit Protocol kan dus ook op cyberoperaties worden toegepast. Aan de voorwaarden van territorium en overheid versus gewapende opstandelingen kan relatief eenvoudig voldaan worden. Nergens in de Conventies van Geneve of de Protocollen worden conflicten beperkt tot conflicten die met bepaalde wapens worden uitgevochten, dus cyberoperaties alleen kunnen zeker gezien worden als een conflict tussen een overheid en 'gewapende' (met digitale wapens) opstandelingen[292]. Anders oordelen hierover zou juist in strijd zijn met de artikelen in de Protocollen, aangezien die, via de Martensclausule, toekomstige soorten conflicten begrijpen in het recht der gewapende conflicten[293]. Het probleem stelt zich echter bij de vereiste van georganiseerd bevel en intensiteit van de aanvallen.

83. De vereiste van territorium is gemakkelijk te vervullen. Rebellen kunnen een deel van een staat bezetten en van daaruit cyberoperaties uitvoeren tegen de overheid. Er rijst echter opnieuw het probleem van de cyberspace: aanvallen kunnen vanuit een andere locatie dan die bepaalde staat vertrekken[294] (omdat de netwerken daar gelegen zijn, omdat de rebellen hulp krijgen van buitenlandse sympathisanten etc. Syriëstrijders moeten effectief naar Syrië rijzen om daar in het niet-internationaal gewapend conflict te strijden, maar een Syriëstrijder die de Syrische overheidswebsites wil hacken, kan dit in theorie van overal doen). Dit zou een niet-internationaal gewapend conflict onmiddellijk internationaal maken, aangezien er grenzen overschreden worden. Deze zienswijze hanteren zou tot enorme escalaties kunnen leiden, waardoor de mening van de *Tallinn-manual* een meer logische en vooral veiligere interpretatie is: cyberoperaties tijdens een niet-internationaal gewapend conflict vanuit het buitenland ontnemen het karakter van niet-internationaal gewapend conflict niet[295].

[291] *Commentary*, 1353.
[292] *Tallinn-manual*, 76.
[293] Zie nr. 17.
[294] CAVV, 21-22.
[295] *Tallinn-manual*, 76.

84. Indien er echter enkel cyberaanvallen worden uitgevoerd en er geen sprake is van enige territoriale controle, is er volgens de *Tallinn-manual* geen sprake van een niet-internationaal gewapend conflict in de zin van Protocol II[296]. Deze kunnen wel onder Gemeenschappelijk art. 3 van de Conventies van Geneve vallen, maar de bescherming die Protocol II biedt, is dan niet van toepassing[297]. In geval van pure cyberoperaties, zonder enige andere vorm van conflict, zal dus enkel art. 3 van toepassing zijn. Er moet ook rekening worden gehouden dat deze verdragen ondertussen internationaal gewoonterecht zijn geworden. Zelfs als art. 1 Protocol II niet van toepassing is, heeft de statenpraktijk gelijkaardige regels ontworpen[298].

85. Andere voorwaarden leveren echter meer problemen op. De *Tadic*-case werkte de voorwaarde van voortdurende en gerichte aanval verder uit, door die voorwaarde te beoordelen aan de hand van de intensiteit van de aanval en aan de hand van de graad van organisatie van de aanvallende groep[299]. Verdere rechtszaken voor het Joegoslaviëtribunaal kozen de intensiteit van de aanval als voornaamste factor voor de beoordeling[300]. Die intensiteit werd onder andere afgemeten aan de ernst van de aanval, het collectieve karakter van vijandelijkheden, het groeiend aantal overheidstroepen gemobiliseerd in het conflict etc.[301] Cyberoperaties alleen zullen dus zelden de noodzakelijke intensiteit bereiken om als niet-internationaal gewapend conflict te worden gezien. Grootschalige aanvallen die kinetische effecten zouden kunnen hebben (bijvoorbeeld het platleggen van het verkeersnet met verkeersdoden tot gevolg) zullen minder frequent voorkomen bij gewapende groeperingen, terwijl spionage, vernietiging van netwerken en dergelijke niet de vereiste intensiteit bezitten (indien de statenpraktijk dezelfde blijft en dit in de toekomst niet verandert)[302].

86. Naast intensiteit moet de aanval ook uitgevoerd worden door een groepering die in zekere mate georganiseerd is. Cyberaanvallen kunnen echter door individuen of kleine, losse collectieven uitgevoerd worden, waar van organisatie geen sprake is[303]. Het is echter niet uitgesloten dat een collectieve groep hackers onder een commandostruc-

[296] *Tallinn-manual*, 80.
[297] BOOTHBY, 32.
[298] MARAUHN, NTOUBANDI, "Armed Conflict, Non-International", nr. 28.
[299] *Tadic*-case, par. 70.
[300] Joegoslaviëtribunaal, *Prosecutor v. Furundzija*, 10 december 1998, IT-95-17/1-T; *Tallinn-manual*, 77.
[301] Voor de relevante cases, zie de voetnoten in de *Tallinn-manual*, 78, vb. *Limaj*-case, par. 135-137.
[302] *Tallinn-manual*, 78.
[303] *Tallinn-manual*, 79.

tuur werken, het feit dat dit enkel online is, doet hieraan volgens de *Tallinn-manual* geen afbreuk[304]. Dit lijkt logisch, gezien de aard van cyberoorlogen: alles kan in de cyberspace gebeuren, van de aanval tot de gevolgen. Het zou dan weinig zin hebben om van de organisatie te eisen dat zij fysiek controle uitoefenen. Door die eigenheid van cyberspace is het wel zeer moeilijk, zo niet onmogelijk, om het recht der gewapende conflicten toepassing te laten vinden. De *Tallinn-manual* geeft aan dat er argumenten te vinden zijn die dit gebrek zowel negeren als gebruiken om de kwalificatie van organisatie teniet te doen[305]. Dit is begrijpelijk. Enerzijds vereist art. 1 Protocol II dat de gewapende groepering de mogelijkheid heeft om dit recht te implementeren, wil men het conflict als niet-internationaal gewapend conflict bestempelen[306], maar anderzijds heeft het eigen karakter van cyberspace ervoor gezorgd dat sommige bepalingen minder toepasselijk zijn: zo kan men in de cyberspace *an sich* moeilijk krijgsgevangenen nemen of regels volgen in verband met gewonden.

87. Er kan dus gesteld worden dat cyberoperaties een deel van een niet-internationaal gewapend conflict kunnen uitmaken. Het is zelfs in extreme omstandigheden mogelijk dat cyberoperaties op zich een niet-internationaal gewapend conflict veroorzaken. De meeste regels van het recht der gewapende conflicten kunnen via een doelgerichte interpretatie toegepast worden (bijvoorbeeld wat betreft het territorium en het feit dat er *gewapende* groeperingen moeten zijn), maar opnieuw veroorzaakt de eigenheid van de digitale context enkele moeilijkheden. Het lijkt opnieuw weinig waarschijnlijk dat een verdrag ervoor zou zorgen dat alle cyberoperaties de nodige intensiteit bereiken om aan de voorwaarde van art. 1 Protocol II te voldoen, maar de statenpraktijk zou hierin verandering kunnen brengen, zoals aangegeven door de *Tallinn-manual*. Dit lijkt enigszins tegenstrijdig, aangezien die kleinere aanvallen nooit de drempel van gewapend geweld zouden halen die vereist is om van een internationaal gewapend conflict te spreken[307], maar is tegelijk ook logisch daar de beperktere schaal en technische capaciteiten van gewapende groeperingen hen beperken tot deze kleinere aanvallen.

[304] *Ibid*.
[305] *Ibid*.
[306] *Commentary*, 1353.
[307] Zie nr. 85.

2. Niet-statelijke actoren

88. Zoals hierboven gesteld, moet er sprake zijn van niet-statelijke actoren voor men kan spreken van een niet-internationaal gewapend conflict. Deze niet-statelijke actoren omvatten echter een heel gedifferentieerde groep, van *hactivists* die hoogstens losjes georganiseerd zijn, tot terroristen of rebellen[308]. Sommige niet-statelijke actoren bezitten zelfs geen legale status, hoewel hun belang in het internationale toneel enorm is toegenomen[309]. Soms echter kunnen de acties van deze niet-statelijke actoren aan een staat toegerekend worden, indien die staat "effectieve controle" had over de niet-statelijke actoren[310]. Zo zou een cyberaanval door niet-statelijke actoren die onder de controle van een staat staan, aan die staat toerekenbaar zijn, waardoor er zich geen probleem stelt[311]. Maar zelfs indien er sprake zou kunnen zijn van effectieve controle of van algemene controle[312], geldt dit principe niet voor individuen of losse, ongeorganiseerde groeperingen[313].

89. Indien dergelijke individuen (bijvoorbeeld burgers) deelnemen aan de vijandelijkheden, verliezen zij de bescherming die door verschillende bepalingen in de Conventies van Geneve en de Protocollen wordt geboden[314]. Dit is in de discussie rond cyberoorlog en niet-statelijke actoren van belang, gezien deze burgers en individuen dan rechtmatig het doelwit mogen zijn van bijvoorbeeld een cyber-tegenaanval[315]. Dit lost het probleem op van niet-statelijke actoren die niet onder de effectieve controle van een staat staan, of van gewapende groeperingen die niet aan de voorwaarden voldoen om van een niet-internationaal gewapend conflict te spreken: onder "burgers" in de zin van de Protocollen wordt iedereen die geen strijder is verstaan[316]. Hun directe deelname in de vijandelijkheden moet wel een drempel overschrijden[317]: hun daden moeten de militaire operaties of capaciteiten van een partij in het conflict negatief be-

[308] M. WAGNER, "Non-State Actors", *MPEPIL*, OPIL, juli 2013, opil.ouplaw.com, nr. 1 (hierna: WAGNER, "Non-State Actors").
[309] WAGNER, "Non-State Actors", nr. 1-2.
[310] Wat hierboven beschreven werd onder "De toerekenbaarheid aan staten".
[311] *Tallinn-manual*, 37.
[312] *Tadic*-case, wat een lagere vereiste is dan effectieve controle.
[313] *Tadic*-case, graad van beroep, par. 132.
[314] Vb. art. 51(3) Protocol I.
[315] BOOTHBY, 246; *Tallinn-manual*, 90.
[316] Art. 50(1) Protocol I.
[317] DINNISS, 161-162.

invloeden, of hun daad moet de dood, verwonding of vernietiging veroorzaken van personen of objecten die beschermd worden tegen directe aanvallen[318].

90. De vraag blijft dan hoe men moet omgaan met aanvallen die deze drempel niet overschrijden, maar toch hinderlijk kunnen zijn[319]. Een deel van de grootste geniën op het vlak van programmeren en dus ook van hacken is te vinden in de private sector[320]. Een deel van deze problematiek zal nationaalrechtelijk worden opgelost, via de regelgeving rond cybercrime[321] (wat verder aan bod komt onder "F. Raakvlakken met cybercrime en cyberterrorisme"). Welke operaties zij ook uitvoeren, deze niet-statelijke actoren vallen niet onder de bepalingen van het recht der gewapende conflicten, daar dit enkel toepasselijk is voor "partijen in het conflict"[322]. Er is echter gesteld dat sommige bepalingen van Protocol II gewoonterecht zijn geworden die opgenomen zijn in het strafrecht van staten[323], waardoor ook deze niet-statelijke actoren die niet onder het verdragsrecht vallen, enige grenzen aan hun gedrag moeten stellen.

91. Hoewel wat hiervoor werd gesteld (dat zelfs niet-statelijke actoren die niet door enig verdragsrecht worden gebonden, omdat zij geen gewapende groeperingen of burgers die actief deelnemen aan de vijandelijkheden zijn, aan regels gebonden zijn) in theorie op elke cyberoperatie van toepassing is, stelt zich het probleem van terrorisme. Deze vorm van niet-statelijke actoren valt moeilijk te definiëren en te classificeren[324] en zij zullen zich minder geroepen voelen om principes van het recht der gewapende conflicten toe te passen[325]. Dit verantwoordt waarom cyberterrorisme onder een aparte sectie wordt toegelicht, enigszins losstaand van de algemene problematiek rond niet-statelijke actoren.

[318] D. MELZER, *Interpretive guidance on the notion of direct participation in hostilities*, Internationaal Comité van het Rode Kruis, Geneve, 2009, 47.
[319] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 3.
[320] RABKIN, RABKIN, "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", 10.
[321] M. ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", *Max Planck UNYB*, 2010, nr. 14, 91 (hierna: ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force").
[322] Zie de verschillende Conventies van Geneve en de Protocollen in verscheidene bepalingen en andere verdragen in verband met het recht der gewapende conflicten; MARAUHN, NTOUBANDI, "Armed Conflict, Non-International", nr. 36.
[323] MARAUHN, NTOUBANDI, "Armed Conflict, Non-International", nr. 38; Joegoslaviëtribunaal, *Prosecutor v. Akayesu*, 2 september 1998, ICTR-96-4-T, par. 435-447.
[324] BOOTHBY, 36.
[325] Wat de vele oorlogsmisdaden van IS, Al-Qaeda, Boko Haram etc. duidelijk maken.

3. Cyberterrorisme

92. Terrorisme is in de 21ste eeuw een belangrijk *issue* geworden in de wereldpolitiek. Het idee dat terroristen via cyberaanvallen enorme ravage kunnen aanrichten, is zelfs al tot de verbeelding gaan spreken van het publiek: verscheidene Hollywoodfilms (bijvoorbeeld Die Hard 4.0) laten actiehelden de wereld (of vooral de Verenigde Staten van Amerika) redden van een terroristische cyberaanval. De dreiging is echter minder fantasierijk en meer reëel dan men zou denken[326]: de Verenigde Staten en het Verenigd Koninkrijk simuleren al aanvallen op kerncentrales, om de potentiële gevaren te voorzien[327]. De dreiging komt echter niet enkel van terreurgroepen uit het Midden-Oosten, maar ook van politieke *hacktivists*[328]. Zoals hierboven gezegd, moet cyberterrorisme apart worden behandeld. Enerzijds is er het probleem dat deze niet-statelijke actoren niet in een internationaal gewapend conflict zitten en dus onder de jurisdictie van het nationaal strafrecht vallen, maar anderzijds dat hun aanvallen wereldwijd enorme schade kunnen aanrichten[329].

93. Een eerste belangrijke vraag is of er bij terrorisme sprake is of zou moeten zijn van een internationaal conflict, of indien het een niet-internationaal gewapend conflict of gewone misdaad uitmaakt, met alle gevolgen van dien, zoals het principe van non-interventie. Ten eerste moet men herinnerd worden dat het recht der gewapende conflicten enkel geldt ten tijde van oorlog. Terroristische daden gepleegd in vredestijd vallen dus buiten het internationaal humanitair recht[330]. Het verbod van Art. 4 Verdrag van Geneve IV op terroristische daden is dus enkel van toepassing indien er een (niet)internationaal gewapend conflict plaatsvindt. Indien er dus een gewapend conflict is, wordt ook cyberterrorisme uitgesloten. Volgens de *Tallinn-manual* is cyberterrorisme een aanval (of de dreiging daarvan) met als hoofddoel angst onder de bevolking te verspreiden[331]. Dit komt overeen met art. 51(2) Protocol I, dat terrorisme ook omschrijft als daden die als hoofddoel het verspreiden van angst hebben, zonder enig

[326] Zie onder meer D. VERTON, *Black Ice: the invisible threat of cyber-terrorism*, McGraw-Hill, New York, 2003, 1-17 (hierna: VERTON).
[327] H. STEWART, "UK and US to simulate cyber-attacks on nuclear plants to simulate resilience", *The Guardian*, 31 maart 2016, theguardian.com.
[328] T.M. CHEN, L. JARVIS, S. MACDONALD (*eds*.), *Cyberterrorism, Understanding, Assessment and Response*, Springer Press, New York, 2014, 2. (hierna: CHEN, JARVIS, MACDONALD).
[329] M.N. SCHMITT (*ed*.), *Essays on Law and War at the Fault Lines*, Springer Press, Den Haag, 2012, 57 e.v. (hierna: SCHMITT).
[330] N.N., *Fequently Asked Questions on International Law Aspects of Countering Terrorism*, UNODC Wenen, 2009, 64.
[331] *Tallinn-manual*, 104.

substantieel militair voordeel[332]. Volgens die definitie moet de aanval of dreiging dus de drempel van "cyberaanval" overschrijden, wat kleinere aanvallen uitsluit.

94. Maar zelfs als het recht der gewapende conflicten van toepassing is, blijven er problemen bestaan: terroristische organisaties kunnen wereldwijd vertakt zijn en toch geen eigen territorium bezitten[333] (wat hun kwalificatie als niet-statelijke actor bemoeilijkt, zie *supra*). De vraag is dan of de staat waar de terreurorganisatie actief is (bijvoorbeeld de Syrische Arabische Republiek, die strijdt tegen IS) die terreurorganisatie kan aanvallen (met conventionele wapens of via cyberaanvallen) elders dan binnen de grenzen van die staat. Zoals vermeld, bestaat een oplossing hierin door niet-internationale gewapende conflicten niet tot een geografische locatie te beperken, maar uit te breiden tot het buitenland naargelang van de status van de actor[334]. De redenering hierachter is dat (specifiek voor cyberoorlogen) indien de locatie geen belemmering voor deelname vormt, de locatie ook geen belemmering voor het zelfverdediging mag uitmaken, zonder dat het conflict escaleert naar een internationaal gewapend conflict[335].

95. Terroristische groeperingen kunnen dus niet-statelijke actoren in een niet-internationaal gewapend conflict zijn, indien zij aan de voorwaarden van gemeenschappelijk art. 3 van de Conventies van Geneve of art. 1 Protocol II voldoen. Dit is zoals gezegd niet vanzelfsprekend: terreurorganisaties hoeven niet beperkt te zijn tot een staat of moeten niet georganiseerd zijn[336]. Maar indien er geen sprake is van een gewapend conflict, doordat het geweld geen specifieke drempel overschrijdt, de groepering niet genoeg is georganiseerd of doordat het geweld niet aanhoudend genoeg is, zal het recht der gewapende conflicten niet toepasselijk zijn, maar zal men moeten terugvallen op nationaalrechtelijke bepalingen[337]. Dit is ook het geval met cyberterrorisme: indien zij de drempel van "cyberaanval" niet overschrijden[338], zal het nationaal strafrecht deze problematiek behandelen. Men moet de toepasselijke regels wel steeds

[332] *Commentary*, 618.
[333] WAGNER, "Non-State Actors", nr. 26.
[334] DASKAL, "The geography of the battlefield: a framework for detention and targeting outside the 'hot' conflict zone", 1175.
[335] *Tallinn-manual*, 76.
[336] WAGNER, "Non-State Actors", nr. 26.
[337] BOOTHBY, 38.
[338] Voor de definitie wordt nog steeds die gebruikt uit de *Tallinn-manual*, 92; en betekent een vorm van cybergeweld die de drempel van *gewapende aanval* overschrijdt.

bekijken op het moment zelf: kleinschalige terreurdaden kunnen uitgroeien tot volwaardige gewapende conflicten, waardoor een heel ander juridisch systeem van toepassing wordt[339].

96. De Verenigde Naties heeft echter de gevaren van terrorisme onderkend[340] en een tiental verdragen regelt de verantwoordelijkheden van staten in het bestrijden van terrorisme[341]. Ook de Raad van Europa liet zich niet onbetuigd, en heeft met het Cybercrimeverdrag de problematiek opgelost van kleinschalige terroristische aanvallen die niet als een (niet)internationaal gewapend conflict kunnen worden gezien[342]. Dit zijn echter verdragen die eerder in het nationaal strafrecht thuishoren, en de reikwijdte van deze masterproef te buiten gaan.

97. Al deze beschouwingen zijn voor cyberoorlog, cyberoperaties en internationaal recht in het algemeen van belang om verschillende redenen. Zo moet men de precieze rechtssituatie kunnen beoordelen om na te gaan of het non-interventiebeginsel speelt (bijvoorbeeld kunnen de Verenigde Staten van Amerika cyberaanvallen uitvoeren tegen een terreurgroep die actief is in land X, maar ook een dreiging vormt voor de VSA?), of het recht op zelfverdediging geldt (wat nog steeds niet duidelijk is in de situatie van Afghanistan, bijvoorbeeld[343]) en of men moet of mag samenwerken op het nationaal vlak voor wat betreft cybercrime en cyberterrorisme.

98. Een kleine kanttekening is ten slotte nog op zijn plaats. Terrorisme staat bovenaan de huidige politieke agenda, en terroristische aanslagen zijn jammer genoeg een dagelijks gegeven, eentje dat zich bovendien niet alleen in verre landen afspeelt. Daarom leek een sectie over cyberterreur toepasselijk in een thesis over cyberoorlog. De vraag stelt zich nu of cyberterrorisme wel een reëel dreiging is, en niet (nog) meer tot het rijk van de Hollywood-plots behoort dan cyberoorlog in het algemeen. Men moet nog steeds een van de grote factoren van terrorisme in het oog houden: het theatrale karakter ervan. Een cyberaanval kan potentieel verwoestend zijn, en cyberinfrastructuur

[339] BOOTHBY, 39.
[340] *Resolutie 1368 van de Veiligheidsraad van de Verenigde Naties*, 12 september 2001, *Doc.nr.* S/RES/1368.
[341] F.C. GORMAN, *Non-State Actors, Terrorism and the United Nations: A Critical Analysis through Three Case studies Examining the United Nations' Effectiveness in Addressing the Threat Imposed by Violent Non-State Actors*, Thesis aan de Virginia Polytechnic and State University, Virginia, 2009, 24.
[342] Cybercrimeverdrag van de Raad van Europa van 23 november 2001, Budapest (hierna: Cybercrimeverdrag).
[343] SCHMITT, 68.

is door zijn verbondenheid een zwakke schakel[344], maar een aanval in de 'echte' wereld, waar de media op afkomt en die grote littekens in de omgeving slaat (zoals Ground Zero in New York, na de aanslag op de WTC-torens) bezit een veel grotere symbolische waarde[345]. Bovendien is de uitvoering ervan nog steeds moeilijker dan een aanval met conventionele wapens[346]. Om deze redenen is cyberterrorisme wel een theoretisch en mogelijk gevaar, maar zal het in de praktijk minder voorkomen[347].

4. Conclusie

99. Niet-statelijke actoren vormen een heterogeen geheel aan spelers die het veld van het internationaal recht ingewikkeld maken. Ook in de digitale wereld is dit het geval. Deze niet-statelijke actoren kunnen deel uitmaken van een niet-internationaal gewapend conflict, dat in extreme gevallen zelfs een conflict kan zijn dat enkel via cyberaanvallen uitgevochten wordt. Door een doelgerichte interpretatie is het mogelijk om deze cyberaanvallen gelijkaardig te behandelen als conventioneel geweld in dergelijke conflicten, zelfs al zijn er enkele bijzondere situaties, zoals de locatie van de niet-statelijke actoren. Een probleem stelt zich wel wanneer de digitale aanvallen niet ernstig genoeg zijn om cyberaanvallen uit te maken, of indien de niet-statelijke actoren niet aan de vereisten voldoen om partij in een conflict te zijn. In dat geval komt het nationaal (straf)recht rond cybercriminaliteit tussen om deze problematiek aan te pakken.

100. Een bijzondere groep niet-statelijke actoren, die nochtans heel wat aan bod komt in de media, zijn terroristische organisaties. Deze vormen een specifiek probleem, niet alleen in digitale context, maar in het algemene internationaal recht. Niet alleen is het niet steeds duidelijk in welke context een terreurgroep actief is (internationaal gewapend conflict of niet), bovendien is het niet steeds zeker hoe men daartegen op kan treden: heeft men recht op zelfverdediging? Kan men interveniëren, of moet men samenwerken met justitiële autoriteiten van een staat? Dit wordt doorgetrokken naar cyberaanvallen, met de bijkomende factor cyberaanvallen van overal ter wereld uitgevoerd kunnen worden. Cyberterrorisme kent dus dezelfde problemen als het 'conventionele' terrorisme, en wordt gelijkaardig aangepakt. Een kleine kanttekening hierbij

[344] CHEN, JARVIS, MACDONALD, 104.
[345] CHEN, JARVIS, MACDONALD, 118.
[346] CHEN, JARVIS, MACDONALD, 116.
[347] CHEN, JARVIS, MACDONALD, 108.

is dat dit allemaal waarschijnlijk puur hypothetisch is, zoals uitgelegd hierboven: terreur draait om symboliek, en verwoesting in de materiële wereld is veel symbolischer dan verwoesting in de digitale wereld. Daarom blijft cyberterrorisme (voorlopig) een academische denkoefening.

E. Spionage en diplomatieke immuniteit

1. Relevantie

101. Spionage is een wijdverspreide praktijk tijdens elk conflict en daarbuiten. Zelfs in vredestijd bespioneren staten elkaar, om hun buitenlands beleid af te stemmen op wat die spionage te weten komt. De algemene consensus is dat spionage niet verboden is[348]. Volgens SCHALLER is het ook onwaarschijnlijk dat spionage ooit internationaalrechtelijk verboden wordt, en dit lijkt logisch. Spionnen kunnen daarentegen wel streng worden bestraft, afhankelijk van de nationaalrechtelijke bepalingen ter zake[349]: in tegenstelling tot verkenners (die lid zijn van de strijdkrachten van een staat), worden zij niet beschermd als krijgsgevangenen[350]. Behalve deze bepalingen wat betreft spionnen en verkenners in oorlogstijd, is er weinig tot geen regulering[351]. Het is echter noodzakelijk om stil te staan bij spionage tijdens cyberoorlog (en ruimer spionage door middel van cyberoperaties) omwille van de enorme schaal die deze spionage kan bereiken.

102. Dat spionage enorm breed opgevat kan worden, bewees het NSA[352]-debacle, aan het licht gebracht door Edward Snowden[353]. Van Dale omschrijft spionage als "het stiekem onderzoeken en achterhalen van (staats)geheimen", terwijl de Oxford English Dictionary spionage (*espionage*) omschrijft als *"The practice of playing the spy, or of employing spies",* waar het spionnen omschrijft als;

> *"[A] secret agent whose business it is to keep a person, place, etc., under close observation; esp[ecially] one employed by a government in or-*

[348] C. SCHALLER, "Spies", *MPEPIL*, OPIL, september 2015, opil.ouplaw.com, nr. 2 (hierna: SCHALLER, "Spies").
[349] A.J. RADSAN, "The Unresolved Equation of Espionage and International Law", *Michigan Journal of International Law*, 2007, Vol. 28 nr. 595, 601-602 (hierna: RADSAN, "The Unresolved Equation of Espionage and International Law").
[350] Vb. art. 46(2) Protocol I.
[351] RADSAN, "The Unresolved Equation of Espionage and International Law", 602.
[352] National Security Agency, opgericht op 4 november 1952, nsa.gov.
[353] N.N., "Edward Snowden: Leaks that exposed US spy programme", *BBC*, 17 januari 2014, bbc.com.

der to obtain information relating to the military or naval affairs of other countries, or to collect information of any kind."[354].

Dit betekent dus dat onder spionage ook het verzamelen van inlichtingen van eigen burgers valt en niet alleen het bespioneren van vreemde mogendheden. Aangezien het onderwerp van deze masterproef beperkt is tot cyberoorlog, zal vooral spionage besproken worden die gebeurt in oorlogstijd.

103. Nauw verband houdend met spionage is het principe van diplomatieke immuniteit. Het Verdrag van Wenen bepaalt specifiek dat, zelfs in tijden van gewapend conflict, diplomatieke immuniteit nog van toepassing is[355]. Dit strekt zich uit tot de communicatie van de diplomaat[356], waardoor het in feite verboden is om diplomatieke correspondentie te onderscheppen (en dus te spioneren)[357]. Na een bespreking van spionage in het algemeen, zal kort op deze specifieke niche van spionage worden ingegaan.

2. Spionage

a) Interne spionage

104. Deze masterproef wil de toepasbaarheid van het internationaal recht op cyberoorlog bestuderen. Dit houdt vanzelfsprekend in dat er sprake moet zijn van een gewapend conflict. In een gewapend conflict bespioneren staten elkaar, zoals hierboven reeds gezegd. Vooraleer hierop wordt ingegaan, moet er misschien eerst worden nagegaan of ook het bespioneren van de eigen bevolking kan vallen onder spionage ten tijde van oorlog (onder het mom van nationale veiligheid, de *war on terror* of andere voorwendselen). Het vermelde programma van de NSA kwam in feite neer op grootschalige binnenlandse spionage via digitale middelen, waardoor duidelijk is dat cyberoperaties de spionagemogelijkheden enorm hebben uitgebreid. Dit programma werd goedgekeurd via de zogenaamde *Patriot Act*[358], waar het als een cruciaal middel

[354] Zie ook C. FORCESE, "Spies Without Borders: International Law and Intelligence Collection", *Journal of National Security Law & Policy*, 2011, vol. 5 nr. 179, 181 (hierna: FORCESE, "Spies Without Borders: International Law and Intelligence Collection").
[355] Art. 39, 44, 46 Verdrag betreffende diplomatieke relaties van 18 april 1964, Wenen, *UNTS* 95 (hierna: Verdrag van Wenen).
[356] Art. 24 Verdrag van Wenen.
[357] FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 196.
[358] Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes, 26 oktober 2001, nr. 107-56 (beter bekend als *Patriot Act*).

tegen de *war on terror* werd onthaald[359]. Aangezien terrorisme gezien kan worden als een niet-internationaal gewapend conflict[360], of het nu specifiek onder art. 1 Protocol II of enkel onder Gemeenschappelijk art. 3 Conventies van Geneve is[361], kan men stellen dat het NSA-spionageschandaal gebeurde in oorlogstijd. De *Tallinn-manual* beperkt cyberspionage tot het verzamelen van informatie van andere staten. Binnenlandse spionage valt volgens de handleiding dus niet onder cyberspionage[362]. Dit lijkt evenwel tegenstrijdig met de bewoordingen in de *Patriot Act*, waardoor in dit geval het standpunt van de handleiding niet bijgetreden kan worden.

105. Indien dit het geval is (en deze masterproef meent van wel, maar zelfs indien dit niet het geval zou zijn, rechtvaardigt de massale schaal van deze cyberoperatie een bespreking), zal spionage door middel van cyberoperaties vooral geregeld worden door internationale mensenrechten. Deze problematiek werd al onderkend door de Verenigde Naties, dat benadrukte dat privacy ook in de digitale wereld beschermd moet worden[363]. Ook art. 12 van de Universele Verklaring van de Rechten van de Mens[364] bepaalt dat er geen arbitraire inmenging in het privéleven mag zijn, waaronder correspondentie. Een kernelement van die *Patriot Act* is nu juist dat het afluisteren en spioneren niet gemotiveerd moet worden[365]. Er kan dus zeker gesteld worden dat de afluisterschandalen van de NSA twijfelachtig waren wat betreft hun legaliteit. De Verenigde Staten van Amerika is verder gebonden door het BUPO-verdrag[366], dat in art. 17 hetzelfde bepaalt als de (niet-bindende) Universele Verklaring van de Rechten van de Mens. Hoewel de praktijken legaal konden zijn in het nationaal recht van de VS[367], was dit dus niet het geval voor wat betreft het internationaal recht[368].

[359] D.E. SANGER, "White House Begins New Effort to Defend Surveillance Program", *The New York Times*, 23 januari 2003, nytimes.com.
[360] Zie nr. 73 e.v.
[361] Zie ook M. SASSOLI, "Transnational Armed Groups and International Humanitarian Law", *Humanitarian Policy and Conflict Research Harvard University*, 2006, nr. 6, 6.
[362] *Tallinn-manual*, 159.
[363] *Resolutie 68/167 betreffende het recht op privacy in het digitale tijdperk van de Algemene Vergadering van de Verenigde Naties*, 18 december 2013, *Doc.nr.* A/RES/68/167.
[364] Universele Verklaring van de Rechten van de Mens van 10 december 1948, San Francisco.
[365] Titel II *Patriot Act*.
[366] Internationaal Verdrag betreffende de Burgerlijke en Politieke Rechten van 16 december 1966, New York, *UNTS* 171 (beter bekend als het BUPO-verdrag).
[367] Wat niet voor alle delen het geval is, zo blijkt de veroordeling door *District Judge* Ann Aiken: ASSOCIATED PRESS, "Judge rules part of Patriot Act unconstitutional", *NBC News*, 27 september 2009, nbcnews.com.
[368] Z. BAHERI, A.S. FARD, "Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations", *Journal of Scientific Research and Development*, 2015, Vol. 2 nr. 1, 43 (hierna: BAHERI, FARD, "Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations").

106. Een vaak gehoorde verdediging van deze grootschalige cyberspionage is het feit dat deze inbreuk op de privacy gepaard gaat met een grotere bescherming[369]. De vraag is echter of een inbreuk op dergelijke schaal proportioneel is. Een constante in enkele belangrijke mensenrechtenverdragen is de vereiste van proportionaliteit en noodzakelijkheid van inbreuken: art. 4 BUPO-verdrag laat inbreuken toe, voor zover die proportioneel en noodzakelijk zijn[370] , aan art. 17, dat het recht op privacy beschermt[371]. Ook art. 8 van het Europees Verdrag van de Rechten van de Mens[372] bepaalt dat inbreuken op de privacy noodzakelijk moeten zijn in een democratische samenleving ter bescherming van de nationale veiligheid. Hoewel de NSA-praktijken niet onder de bepalingen van het Europees Verdrag vallen, kan, gelet op de dreiging van terrorisme die ook in Europa te voelen is, het nuttig zijn deze te bespreken. Een standaardpraktijk bij inbreuken op art. 8 van dit verdrag is het nagaan of de inbreuk proportioneel is[373]. Het is dus weinig waarschijnlijk dat de dreiging van binnenlands terrorisme een globale surveillance rechtvaardigt, aangezien dit moeilijk proportioneel genoemd kan worden[374].

b) Extraterritoriale spionage

107. Spionage in oorlogstijd (zoals aangenomen werd) van de eigen bevolking is dus moeilijk verenigbaar met enkele basisprincipes van de internationale mensenrechten. Zelfs indien de NSA-praktijken niet als spionage in tijden van oorlog zouden gezien worden, blijven deze cyberoperaties een schending van het recht op privacy. Nu zal echter gekeken worden naar de eventuele legaliteit van cyberspionage van buitenlandse naties tijdens oorlogssituaties. Zoals gezegd, is spionage in theorie legaal. Dit stemt logischerwijs uit de principes van de *Lotus*-case: aangezien spionage niet uitdrukke-

[369] BAHERI, FARD, "Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations", 44.
[370] Y. ARAI-TAKAHASHI, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Intersentia, Antwerpen, 2001, 186; T. BUERGENTHAL, "To Respect and to Ensure: State Obligations and Permissible Derogations" in L. HENKIN (*ed.*), *The International Bill of Rights*, Columbia University Press, New York, 1981, 80-81 (hierna: BUERGENTHAL, "To Respect and to Ensure: State Obligations and Permissible Derogations"; HENKIN).
[371] Wat zich uitstrekt tot de correspondentie van een burger: F. VOLIO, "Legal Personality, Privacy, and the Family" in HENKIN, 197-198.
[372] Europees Verdrag betreffende de Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden van 4 november 1950, Rome (beter bekend als het Europees Verdrag van de Rechten van de Mens of kortweg EVRM).
[373] D. KORFF, "The Standard Approach under Articles 8-11 ECHR and Article 2 ECHR", *European Commission*, ec.europa.eu.
[374] BAHERI, FARD, "Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations", 44.

lijk verboden is door het internationaal recht, moet het toegelaten zijn[375]. Toch zijn er enkele internationaalrechtelijke principes die in conflict komen met spionage, of spionage in elk geval beperken[376]. Hier zal besproken worden of deze beperkingen ook toepassing kunnen vinden in de context van cyberoorlogen en cyberspace.

108. Zoals hierboven is uiteengezet en zoals aangenomen werd voor deze masterproef, volgt cyberspace de territoriale grenzen van staten. Er kan dus gesteld worden dat spionage via een cybertoepassing een inbreuk op de soevereiniteit van een andere staat kan uitmaken. Het is immers verboden om tussen te komen in de binnenlandse zaken van een andere staat, omwille van welke reden ook[377]. Er dienen verschillende situaties in acht te worden genomen om na te gaan of een daad van spionage dan voldoende ernstig is om een interventie uit te maken. FORCESE is bijvoorbeeld van mening dat het passief informatie verzamelen door diplomaten (bijvoorbeeld door publieke bronnen) geen interventie uitmaakt[378]. Gelet op het criterium in de *Nicaragua*-case, dat stelt dat interventies een bepaalde drempel moeten bereik[379]en, lijkt deze stelling logisch. Spionage als voorbereiding van een gewapende aanval brengt ook niet veel problemen: dit is duidelijk een mogelijke inbreuk op het geweldverbod van art. 2(4) VN Handvest[380].

109. Spionage door organen van een staat (andere dan diplomaten), lijkt in tijden van oorlog niet aan regels gebonden. Indien er al een inbreuk op de soevereiniteit zou zijn, is deze inbreuk niet van belang in oorlogstijd, aangezien de partijen in een conflict niet gebonden zijn om elkaars territorium te respecteren[381]. Dit is des te meer het geval voor cyberspionage: indien de aanwezigheid van een fysieke spion geen schending van de fysieke territoriale integriteit uitmaakt, zal de aanwezigheid van een 'digitale spion' (hackers etc.) in cyberspace dat ook niet doen. De legaliteit van spionage in vredestijd ligt veel moeilijker: FORCESE licht de standpunten toe van zowel enkele juristen die menen dat deze spionage illegaal is, als van anderen die van oordeel zijn

[375] SCHALLER, "Spies", nr. 2.
[376] FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 198.
[377] Het zogenaamde non-interventiebeginsel; zie ook KUNIG, "Intervention, Prohibition of"; FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 198.
[378] FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 199.
[379] KUNIG, "Intervention, Prohibition of", nr. 2.
[380] FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 199.
[381] Q. WRIGHT, "Espionage and the Doctrine of Non-Intervention in Internal Affairs" in R. STANGER (*ed.*), *Essays on Espionage and International Law*, Ohio State University Press, Columbus, 11.

dat het toegelaten is[382]. Hoewel de enkele voorbeelden van cyberaanvallen gericht waren op het verkrijgen van informatie (en dus spionage) in vredestijd[383] gaat dit de reikwijdte van deze masterproef (cyber*oorlog*) te buiten.

110. Indien een staat zijn eigen burgers bespioneert, kan het enkele fundamentele mensenrechten schenden. De vraag is nu logischerwijs of deze mensenrechtenbescherming ook geldt indien een staat een andere staat bespioneert. Art. 2 BUPO-verdrag bepaalt dat Lidstaten moeten verzekeren dat de rechten in het verdrag gegarandeerd worden voor individuen onder hun jurisdictie *en* in hun territorium. Aangezien jurisdictie en territorium twee onderscheiden begrippen zijn in het internationaal recht[384], kunnen individuen dus onder de jurisdictie van een staat vallen, zonder dat zij zich in het territorium van die staat bevinden (indien die individuen zich onder de 'effectieve controle' van die staat bevinden)[385]. Indien er dus kan bewezen worden dat individuen zich onder effectieve controle van een staat bevinden (in cybercontext bijvoorbeeld omdat hun computer gehackt wordt en gecontroleerd wordt door die staat), zullen de hierboven beschreven regels in verband met privacy gelden[386]. Er moet echter rekening worden gehouden met wat werd gezegd met betrekking tot de toerekenbaarheid aan staten: het is moeilijk te bewijzen dat een staat achter de cyberaanval zat, waardoor het bewijs dat die bewuste staat mensenrechten heeft geschonden, bemoeilijkt zal worden.

111. Een typerend kenmerk van cyberspionage is dat het een transnationaal karakter heeft: de informatiebron en de ontvanger ervan moeten niet in dezelfde staat verblijven, enkel informatiebron moet zich in het buitenland bevinden. FORCESE maakt een onderscheid tussen extraterritoriale spionage (informatiebron en ontvanger in dezelfde staat) en transnationale spionage, hoewel hij zelf aangeeft dat het, puur internationaal-

[382] FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 203.
[383] Vb. de cyberaanval op de militaire servers van de Verenigde Staten van Amerika in 2008: B. KNOWLTON, "Military Computer Attack Confirmed", *The New York Times*, 25 augustus 2010, nytimes.com.
[384] Zie de beslissing van De Mensenrechtencommissie: Mensenrechtencommissie, *Lopez v. Uruguay*, 1979 (communicatienr. 52/1979), *Doc.nr.* CCPR/C/13/D/52/1979; FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 206.
[385] Zie o.a. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory-opinion*, par. 111; BUERGENTHAL, "To Respect and to Ensure: State Obligations and Permissible Derogations", 74.
[386] Zie nr. 105 e.v.; dit volgt uit het principe dat, tijdens een bezetting, de bezetter verantwoordelijk is voor het respecteren van de mensenrechten in het bezette gebied: C. MCCARTHY, "Human Rights Standards During Military Occupation" IN R. ARNOLD, N. QUÉNIVET (*eds.*), *International Humanitarian Law and Human Rights Law – Towards a New Merger in International Law*, Martinus Nijhoff Publishers, Leiden, 2008, 132 (hierna: ARNOLD, QUÉNIVET); R. WILDE, "Triggering State Obligations Extraterritorially: The Spatial Test in Certain Human Rights Treaties", in ARNOLD, QUÉNIVET, 152-153.

rechtelijk gezien, weinig verschil uitmaakt[387]. Zelfs indien de spion niet in het buitenland verblijft, kan de spionage een verboden interventie in de interne aangelegenheden uitmaken, en de bescherming van de mensenrechten hangt af van het territorium of de jurisdictie (zoals hierboven gezegd), wat niet wezenlijk verandert bij transnationale spionage[388].

112. Toch biedt het cyberkarakter van die transnationale spionage wat meer ruimte voor staten. Staten kunnen passief informatie verzamelen, aangezien het kan dat communicatie door de netwerken in hun staat worden vervoerd, of dat een digitaal signaal opgevangen wordt door een andere staat. Dit zal minder kans maken om als een verboden interventie te worden gezien, aangezien de staat zelf geen bewuste actie heeft ondernomen om te spioneren, maar de informatie eerder in de schoot krijgt geworpen[389]. Dit standpunt wordt ook gesteund door het Verdrag betreffende Internationale Telecommunicatie[390]: art. 22 bepaalt weliswaar dat staten alle mogelijke maatregelen moeten nemen om de geheimhouding van telecommunicatie te verzekeren, maar het bepaalt tegelijk dat de telecommunicatie met de bevoegde autoriteiten mag worden gedeeld, om na te gaan of het nationaal en internationaal recht wordt nageleefd. Passieve onderschepping van communicatie ter bescherming van de openbare orde is dus mogelijk (hoewel actieve onderschepping en spionage meer argwanend worden bekeken)[391].

3. Diplomatieke immuniteit

113. Op het gebied van spionage blijft één soort communicatie altijd beschermd[392]. De diplomatieke immuniteit blijft immers gelden, ook in tijden van gewapende conflicten[393]. Ook de *Tallinn-manual* bepaalt expliciet dat diplomatieke databases en communicatie beschermd worden tegen cyberoperaties[394], terwijl de principiële onschendbaarheid van diplomatieke archieven en communicatie werd bevestigd in de

[387] FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 208.
[388] *Ibid.*
[389] *Ibid*.
[390] Grondwet en Conventie betreffende de Internationale Telecommunicatie-Unie van 6 november 1982, Parijs, *UNTS* 319. (hierna: Verdrag betreffende Internationale Telecommunicatie).
[391] Voor een overzichtelijk schema die het bovenstaande weergeeft: FORCESE, "Spies Without Borders: International Law and Intelligence Collection", 209.
[392] I. BROWNLIE, *Principles of Public International Law*, Oxford University press, Oxford, 1998, 358.
[393] Zie nr. 103.
[394] *Tallinn-manual*, 192.

Teheran-case[395]. Ook ingeval een staat slechts passief informatie verzamelt, aangezien die informatie zijn netwerken passeert, blijft de diplomatieke immuniteit gelden: art. 40(3) Verdrag van Wenen bepaalt dat die communicatie dezelfde bescherming moet genieten als de bescherming die de ontvangende staat garandeert. Zelfs ingeval twee staten dus in conflict zijn, blijft hun diplomatieke communicatie onschendbaar, ook voor cybertoepassingen.

4. Conclusie

114. Spionage is een gebruikelijke praktijk onder staten, zowel in tijden van oorlog als in tijden van vrede. De opkomst van het internet en ruimer, cyberspace, heeft het spionagelandschap echter drastisch veranderd. Waar vroeger in tijden van oorlog vooral in het buitenland werd gespioneerd[396], bewijst het NSA-spionagedebacle dat afluisteren en spioneren op eigen burgers op enorme schaal kan gebeuren, met dank aan cybertechnologie. Deze thesis heeft het standpunt trachten te verdedigen dat dergelijke spionage onder spionage gedurende oorlogstijd kan vallen, door de specifieke rechtvaardiging voor het programma: de strijd tegen de *war on terror*. Dit soort spionage komt in conflict met het fundamentele recht op privacy, gegarandeerd in het BUPO-verdrag en, voor zover dit ooit in Europa zou voorkomen, het EVRM. Een inbreuk op de schaal die door de NSA is toegepast, zal nooit aan de vereisten van noodzakelijkheid en (belangrijker) proportionaliteit kunnen voldoen. Er valt dus te verdedigen dat spioneren in het binnenland (door cybertoepassingen of anderzijds) mag, indien dit binnen de grenzen van de vernoemde verdragen valt. Verdere regels met betrekking tot cyberspionage zijn dus blijkbaar niet nodig, aangezien het bestaande internationaalrechtelijk kader deze problematiek adequaat kan oplossen.

115. Spionage in het buitenland wordt in het algemeen niet verboden. Geen enkele internationaalrechtelijke bepaling verbiedt spionage op zich, waardoor, ingevolge de redenering in de *Lotus*-case, spionage toegelaten is. Dit betekent niet dat spionage ongebreideld toegepast kan worden: het verbod op non-interventie en de privacyrechten van personen beperken de mate waarin gespioneerd kan worden. Dit geldt ook voor cyberoperaties, terwijl zij nog een specifiek karakter kennen: dankzij cybertechnolo-

[395] IGH, *Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, 24 mei 1980, *ICJ Reports 1980*, par. 61-62.
[396] Denk aan de massale spionage gedurende de koude oorlog: D. BARRETT, "Secret files reveal techniques of Cold War Soviet spies", *The Telegraph*, 21 augustus 2015, telegraph.co.uk.

gie kan spionage nu ook transnationaal toepassing vinden. Dit transnationaal karakter betekent ook dat staten gewoon informatie passief kunnen opvangen, doordat die informatie door hun netwerken (digitaal) passeert. Staten moeten in theorie de geheimhouding van berichten garanderen, maar nationale veiligheid kan hierbij primeren, volgens het Verdrag betreffende Internationale Telecommunicatie. Ook hier, bij algemene spionage, zal geen verdrag nodig zijn: aangezien spionage al altijd toegestaan is, lijkt het onwaarschijnlijk dat staten plots cyberspionage zullen willen reguleren, terwijl de bestaande beperkingen op spionage ook toegepast kunnen worden in een cybercontext.

116. Traditioneel wordt diplomatieke communicatie beschermd tegen spionage. Dit is niet anders op het vlak van cyberoorlog en cybertoepassingen. Zelfs indien een staat slechts passief informatie zou verzamelen, verbiedt het Verdrag van Wenen de schending van de communicatie. Aangezien dit specifieker is dan het Verdrag betreffende Internationale Telecommunicatie, kan dit als een *lex specialis*[397] worden beschouwd, waardoor men dus met zekerheid kan stellen dat diplomatieke communicatie beschermd wordt, zelfs in geval van cybertoepassingen.

F. Raakvlakken met cybercrime en cyberterrorisme

1. Relevantie

117. Cybercrime wordt traditioneel op het nationaal vlak geregeld. Er bestaan verdragen rond, zoals het reeds genoemde Cybercrimeverdrag, maar deze verdragen leggen staten eerder verplichtingen op over hoe ze cybercrime op een nationaal vlak dienen aan te pakken en hoe men internationaal daarover dient samen te werken[398]. Op het eerste zicht lijkt dit dus irrelevant voor deze masterproef. Er zijn echter enkele belangrijke principes in het internationaal recht die, voor wat betreft cyberoorlog, nood hebben aan de regels van cybercrime om toepassing te kunnen vinden. De belangrijkste zijn hier al besproken: voor het toerekenen van een cyberaanval aan een staat, zal de nationale cybercrimeregelgeving de verantwoordelijke daders moeten vinden (om ze daarna te kunnen koppelen aan eventueel verantwoordelijke staten). Dit geldt ook voor niet-statelijke actoren: indien een niet-statelijke actor zich in het buitenland be-

[397] S. BORELLI, "The (Mis)-Use of General Principles of Law: *Lex specialis* and the Relationship between International Human Rights Law and the Laws of Armed Conflict" in L. PINESCHI (*ed.*), *General Principles of Law: The Role of the Judiciary*, Springer, New York, 2015, 265 e.v.
[398] Zie preambule van het verdrag.

vindt, zal een conflict daardoor niet internationaal worden, maar zal men op de nationaalrechtelijke cybercrimeregels moeten terugvallen. Ook spionage kan hierbij gerekend worden: het nationaal recht zal beslissen hoe digitale spionnen aangepakt worden.

118. Een korte uitwijding lijkt dus gerechtvaardigd: deze nationaalrechtelijke regels zijn het sluitstuk van enkele internationaalrechtelijke problemen. Om na te gaan of het internationaal recht (via de Martensclausule) aangepast is om de cybercontext te regelen, moeten men ook deze nationale wetten verder bestuderen. Hieronder zal dit kort verder onderzocht worden, zonder evenwel de draagwijdte van deze thesis te overschrijden. De belangrijkste bepalingen uit het cybercrimeverdrag zullen uitgelicht worden, om aan te tonen dat zij van belang zijn voor de hierboven beschreven vraagstukken met betrekking tot cyberoorlog.

2. Cybercrime als sluitstuk voor verschillende problemen

119. Art. 2 van het Cybercrimeverdrag vraagt dat de Lidstaten wetten implementeren die het illegaal toegang verschaffen tot computernetwerken strafbaar stelt. Samen met art. 3 (illegale onderschepping van datatransmissie) en art. 4 (illegale tussenkomst bij datatransmissie) legt dit staten in feite de verplichting op om cyberspionnen strafrechtelijk verantwoordelijk te houden. Hoewel spionage dus toegelaten is, kunnen spionnen bestraft worden. Indien een cyberspion gevat wordt en die blijkt lid te zijn van de strijdkrachten van een staat, kan die toch bestraft worden door het nationaal recht[399], in tegenstelling tot krijgsgevangenen, die in theorie niet bestraft kunnen worden voor deelname in de vijandelijkheden[400]. Zoals gezegd kan het heel moeilijk zijn om aan te tonen dat een bepaalde staat achter de cyberaanval zat, maar via deze bepalingen kan de spion zelf bestraft worden.

120. Naast deze bepalingen die specifiek op spionage van toepassing kunnen zijn, legt art. 5 aan de Lidstaten de verplichting op om aanvallen op systemen strafbaar te stellen. In tegenstelling tot een interventie bij dataverkeer, bepaalt dit artikel dat het beschadigen, veranderen, verwijderen of anderzijds morrelen aan een systeem een mis-

[399] Art. 46(1) Protocol I.
[400] Conventie van Geneve III; N.N., "Prisoners of war and detainees protected under international humanitarian law", *International Committee of the Red Cross*, 29 oktober 2010, icrc.org.

daad uitmaakt. Dit kan natuurlijk ook spionage uitmaken, maar dit artikel zorgt ervoor dat elke cyberaanval (die er in essentie op gericht is een systeem of netwerk te beschadigen of negatief te beïnvloeden) strafbaar is. Hoewel het niet altijd zal lukken om een staat verantwoordelijk te houden, zullen de individuele daders dus bestraft kunnen worden.

3. Conclusie

121. Zoals gezegd lijkt dit onderdeel niet echt thuis te horen in deze masterproef. Toch zijn de bepalingen van het Cybercrimeverdrag van belang, aangezien zij ervoor zorgen dat een van de grote problemen van het internationaal recht met betrekking tot cyberoorlog toch enigszins aangepakt kan worden. Aangezien het immers moeilijk is om cyberaanvallen toe te rekenen aan staten[401], zouden cyberaanvallen in theorie onbestraft kunnen blijven. Door het Cybercrimeverdrag zullen dan wel de uiteindelijke verantwoordelijken (de staten zelf) niet aangepakt kunnen worden, maar zullen de daders zelf aangehouden en veroordeeld worden, wat de gevolgen enigszins verzacht.

V. HET INTERNATIONAAL HUMANITAIR RECHT

A. De toepasbaarheid van het internationaal humanitair recht

122. Het internationaal publiekrecht ken vele takken, waaronder mensenrechten, diplomatiek recht etc. Voor wat betreft cyberoorlog is een tak echter van uitzonderlijk belang. Het internationaal humanitair recht, ook wel het recht der gewapende conflicten genoemd, beheerst en regelt (of tracht in elk geval te regelen) de gewapende conflicten. Deze regels kunnen onderverdeeld worden in twee categorieën: het *ius ad bellum* (regels aangaande de rechtmatigheid van het gebruik van geweld) en het *ius in bello* (de regels die gelden in geval van gebruik van geweld)[402]. Het *ius in bello* vormt het eigenlijke internationaal humanitair recht, maar deze masterproef zal ook ingegaan op het *ius ad bellum*, aangezien cyberoorlog enkele interessante vraagstukken daaromtrent oplevert.

[401] Wat volgens mevr. N. VAN RAEMDONCK het grootste struikelblok vormt om het internationaal recht vlot op cyberoorlogen toe te kunnen passen (zie BIJLAGE 1).
[402] H.-P. GASSER, D. THÜRER, "Humanitarian Law, International", *MPEPIL*, OPIL, maart 2011, opil.ouplaw.com, nr. 1-6 (hierna: GASSER, THÜRER, "Humanitarian Law, International")

123. Men zou zich de vraag kunnen stellen of het recht der gewapende conflicten wel van toepassing is op cyberoorlogen. Het is immers niet zeker of een cyberaanval gebruik van geweld uitmaakt, waardoor het niet zeker is of "cyberoorlog" een bestaand concept is[403]. Deze masterproef gaat uit dat dit wel het geval is, en dus is het internationaal humanitair recht hierop van toepassing. Het is immers irrelevant welke manier van oorlogsvoering gebruikt wordt[404], en dit recht geldt zowel voor internationale als niet-internationale gewapende conflicten[405].

1. Ius ad bellum

124. Deze masterproef zal enkele essentiële vraagstukken betreffende het *ius ad bellum* in de context van cyberoorlogen bestuderen. *Ius ad bellum* (Latijn voor 'het recht naar de oorlog', dus in de zin van het recht die de aanleiding tot oorlog regelt) beheerst de manieren en de momenten waarop staten gerechtvaardigd geweld mogen gebruiken[406]. Als belangrijkste onderdeel hiervan zal deze masterproef het recht op zelfverdediging[407] bestuderen. Verdere vraagstukken rond het gebruik van geweld werden hierboven al besproken, om na te gaan of cyberaanvallen wel gebruik van geweld kunnen uitmaken.

2. Ius in bello

125. Het *ius in bello* (Latijn voor "het recht in de oorlog") regelt de methoden waarop oorlog wordt gevoerd en de wapens die mogen worden gebruikt[408], net als de limieten van oorlogsvoering: welke personen en voorwerpen dienen beschermd te worden en in welke mate?[409] In deze masterproef zal dit aan bod komen door het (eventueel) verbod op het gebruik van kernwapens te bespreken, om dan algemeen na te gaan aan welke voorwaarden cyberwapens moeten voldoen om legaal te zijn. Er zal ook bestudeerd worden in welke mate de bescherming van personen en voorwerpen op het gebied van cyberoorlogen van toepassing kan zijn.

---

[403] Zie de discussie, nr. 28 e.v.
[404] GASSER, THÜRER, "Humanitarian Law, International", nr. 2-3; dit is ook de essentie van de Martensclausule, zoals die ook expliciet is opgenomen in art. 1(2) Protocol I: de oude regels blijven via interpretatie van toepassing op nieuwe ontwikkelingen.
[405] GASSER, THÜRER, "Humanitarian Law, International", nr. 3.
[406] GASSER, THÜRER, "Humanitarian Law, International", nr. 1.
[407] O. DÖRR, "Use of Force, Prohibition of", *MPEPIL*, OPIL, september 2015, opil.ouplaw.com, nr. 6.
[408] Vooral geregeld in de verdragen van Den Haag: N. HORBACH, R. LEFEBER, O. RIBBELINK, *Handboek Internationaal Recht*, Asser Press, Den Haag, 2007, 556-557 (hierna: HORBACH, LEFEBER, RIBBELINK).
[409] Vooral geregeld in de verdragen van Geneve: HORBACH, LEFEBER, RIBBELINK, 556-557.

B. De mogelijkheden tot zelfverdediging

126. Art. 51 en het internationaal gewoonterecht[410] laten een uitzondering op het verbod op gebruik van geweld toe: staten hebben het recht om zichzelf tegen (illegale) aanvallen te verdedigen, of daar collectief tegen op te treden:

> *"[N]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security..."*[411]

De vraag is natuurlijk of dit ook geldt voor cyberoorlogen. Indien wel, stelt zich de vraag in welke mate vergeldend mag worden opgetreden: moet hierbij in de cyberspace gebleven worden, of mag het conflict uit de digitale omgeving naar de materiële wereld gehaald worden, en in welke mate? Verder stellen zich de klassieke vragen in verband met zelfverdediging: hoe zit het met terroristische aanslagen? Wat met preventieve zelfverdediging? Deze vraagstukken zullen hier behandeld worden, waar er zal worden nagegaan, zoals steeds, of het internationaal voldoende adequaat geïnterpreteerd kan worden om het op cyberoorlog van toepassing te verklaren.

1. Het recht op zelfverdediging: wanneer?

127. Er dient vanzelfsprekend eerst nagegaan te worden of er een recht op zelfverdediging bestaat na het gebruik van cyberaanvallen. Uit de definitie van art. 51, moet er ten eerste sprake zijn van een gewapende aanval, wat een hogere drempel is dan het gebruik van geweld uit art. 2(4)[412]. Dergelijk gebruik van geweld kan een reactie van de Veiligheidsraad overeenkomstig art. 39 VN Handvest uitlokken, maar geeft een staat geen recht om zelf geweld te gebruiken in een daad van zelfverdediging[413]. Er moet dus een zeker kinetisch gevolg van verwonding, dood of vernietiging zijn om te kunnen spreken van gewapende aanval[414], indien er enkel cyberaanvallen gebeuren. Indien er cyberaanvallen samenvallen met conventionele aanvallen (bijvoorbeeld een invasie waarbij cyberaanvallen gebruikt worden om radars te verstoren), speelt het

[410] SCHMITT, 3; *Nicaragua*-case.
[411] Art. 51 VN Handvest.
[412] SCHMITT, 38.
[413] SCHMITT, 37.
[414] Zie nr. 29 e.v.

zelfverdedigingsrecht vanzelfsprekend, maar waarschijnlijk eerder op basis van de conventionele aanval dan op basis van de cyberaanval[415]. Evident moet een cyberaanval ook een transnationaal karakter hebben: cyberaanvallen die op de eigen staat worden uitgevoerd, maken hoogstens een niet-internationaal gewapend conflict uit[416].

128. Het is op het cybergebied niet volledig duidelijk wat precies moet worden aangevallen om een zelfverdedigingsreactie te legitimeren. In het traditionele oorlogsrecht vallen aanvallen op burgerlijke (of algemeen niet-militaire) doelwitten onder het toepassingsgebied van art. 51 VN handvest[417], dus is het aannemelijk om deze lijn tot cyberoorlogen door te trekken[418]. De vraag stelt zich nu of *elke* aanval op civiele doelen onder art. 51 valt. Een aanval op Google wordt bijvoorbeeld omschreven als een aanval op de kritieke infrastructuur van de Verenigde Staten van Amerika[419], maar aangezien er geen consensus is over wat als 'kritieke infrastructuur' wordt gezien[420], is dit geen sluitend criterium[421]. Het komt dus aan de staten toe om dit te beoordelen[422], wat ook door de VN is voorgesteld[423]. Voorts geldt een aanval tegen in het buitenland gestationeerde troepen ook als een gewapende aanval die het recht op zelfverdediging doet ontstaan[424].

129. Om te kunnen spreken van een recht op zelfverdediging, moet dus sprake zijn van een gewapende aanval. Deze aanval moet echter niet noodzakelijk uitgevoerd worden door de reguliere strijdkrachten van een staat: de hulp van gewapende groeperingen in het uitvoeren van dergelijke aanvallen volstaat, ingevolge de *Nicaragua*-case[425]. Hetzelfde zou dus in theorie van cyberaanvallen gezegd kunnen worden: indien een staat groeperingen inhuurt om cyberaanvallen uit te voeren, telt dit ook als gewapende aanval, wat een recht op zelfverdediging uitlokt. Rekening houdend met wat gezegd werd over staatsaansprakelijkheid en toerekenbaarheid aan staten, zal dit

[415] SCHMITT, 38.
[416] *Tallinn-manual*, 54.
[417] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 116.
[418] Y. DINSTEIN, "Computer Network Attacks and Self-Defense" in M.N. SCHMITT, B.T. O'DONNELL, (*eds*.), *Computer Network Attack and International Law*, Naval War College, Rhode Island, 2002, 106.
[419] Via een *executive order*: VERTON, 241 e.v.
[420] Zie nr. 35; FRANCEUS, 22-23.
[421] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 117.
[422] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 119.
[423] Zie A/RES/58/199 van 23 december 2003.
[424] C. GREENWOOD, "Self-Defence", *MPEPIL*, OPIL, april 2011, opil.ouplaw.com, nr. 21 (hierna: GREENWOOD, "Self-Defence").
[425] *Nicaragua*-case, par. 195.

echter een zware bewijslast op de verdedigende staat leggen[426]. Voorts maakt het niet uit welke wapens worden gebruikt, zolang de drempel van wat als gewapende aanval wordt gezien, wordt overschreden[427].

130. Ingevolge de *Nicaragua*-case moet deze gewapende aanval bovendien een bepaalde omvang en bepaalde gevolgen bereiken, om dit te onderscheiden van loutere grensincidenten[428]. Er is dus een schemerzone tussen een 'kleine' gewapende aanval en een gewapende aanval die ingevolge de *Nicaragua*-case recht geeft op zelfverdediging. Voor cyberoorlogen zal dit echter minder relevant zijn: grensincidenten zijn sowieso niet denkbaar in de cyberspace, en cyberaanvallen op zich die een grote gewapende aanval uitmaken zullen extreem uitzonderlijk zijn, zoals hierboven is gesteld. Enkele voorbeelden die toch zouden kunnen voorkomen zijn: slachtoffers door het hacken van computergestuurde ademhalingsapparaten, het hacken en laten oververhitten van kerncentrales of het hacken van computergestuurde stuwdammen met grote overstromingen tot gevolg[429]. Bovendien is deze uitspraak van het Hof omstreden[430], waardoor hier verder geen aandacht aan zal worden besteed.

131. Er kan dus aangenomen worden dat cyberaanvallen onder het recht op zelfverdediging van art. 51 VN Handvest vallen. Bovendien kan gesteld worden dat, indien deze interpretatie van art. 51 toch niet zou worden aanvaard, cyberaanvallen onder dit recht vallen ingevolge het gewoonterecht. Het feit dat cyberaanvallen een relatief nieuw fenomeen vormen, doet daaraan geen afbreuk, aangezien gewoonterecht zich in sommige gevallen snel kan ontwikkelen[431]. De vereiste *usus* in de zin van actuele gedragingen na cyberaanvallen ontbreekt echter, maar ook verbale daden van staten kunnen deze *usus* uitmaken (zoals het uitgeven van militaire handboeken of het opstellen van beleidsprincipes)[432]. De meerdere malen geciteerde *Tallinn-manual* alleen geldt voor alle lidstaten van de NAVO, terwijl de Verenigde Staten van Amerika en het Verenigd Koninkrijk gelijkaardige beleidsprincipes hebben uitgevaardigd[433]. Er

[426] Zie nr. 51 e.v.
[427] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 114.
[428] *Nicaragua*-case, par. 195; GREENWOOD, "Self-Defence" nr. 12.
[429] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 115.
[430] GREENWOOD, "Self-Defence", nr. 12.
[431] IGH, *North Sea Continental Shelf*, 1969, *ICJ Reports 1696*, p. 43. par. 74.
[432] ILA, *Report of the Sixty-Ninth Conference*, 2000, 725: Statement of Principles Applicable to the Formation of General Customary International Law.
[433] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 125-129.

kan dus gesteld worden dat het recht op zelfverdediging na cyberaanvallen tot het internationaal gewoonterecht behoort.

132. In de rechtsleer wordt een specifiek maar interessant vraagstuk opgegeven[434]. Er is geen twijfel mogelijk dat een cyberaanval die de vereiste drempel bereikt, recht geeft op zelfverdediging. Indien een cyberaanval samenvalt met conventionele aanvallen, is er ook weinig twijfel mogelijk. Maar wat indien een cyberaanval *voorafgaat aan* een dergelijke conventionele aanval, in voorbereiding daarvan (met hetzelfde voorbeeld maar een andere chronologie: eerst worden de radars digitaal aangevallen, om nadien een invasie uit te voeren)?[435] Het algemeen aanvaarde standpunt is dat een dreiging 'op handen' (*imminent*) moet zijn, vooraleer het recht op zelfverdediging wordt geactiveerd[436]. Deze reactie is echter geen zuivere zelfverdedigingsreactie, maar eerder een anticiperende daad om zichzelf tegen verdere schade te beschermen[437]. Deze standaard werd al aangenomen in het *Caroline*-incident[438] en werd gevolgd in de Nürembergtribunalen[439], maar kwam niet aan bod in zowel de *Nicaragua*-case[440] als de *Congo v. Uganda*-case voor het Internationaal Gerechtshof[441]. Het Hof stelde wel dat preventieve middelen mogelijk moeten zijn, maar onder strikte voorwaarden[442], zoals het 'imminent karakter' van de aanval. Het lijkt ondertussen algemeen aanvaard dat dergelijke preventieve middelen internationaal gewoonterecht zijn geworden[443] en dat een nuttige interpretatie van art. 51 VN Handvest dit toelaat. Dit artikel spreekt weliswaar over een aanval die 'plaatsvindt' (dus niet imminent is), maar art. 32 van het Verdrag van Wenen vereist een interpretatie die niet tot 'manifest absurde of onredelijke' gevolgen zou leiden[444].

[434] Zie onder meer DINNISS, 82-93.
[435] Een voorbeeld hiervan is de invasie van Rusland in Georgië, waar een cyberoorlog aan voorafging; ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 120.
[436] SCHMITT, 39.
[437] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 120.
[438] C. GREENWOOD, "Caroline, The", *MPEPIL*, OPIL, april 2009, opil.ouplaw.com, nr. 5 (hierna: GREENWOOD, "Caroline, The").
[439] Nürembergtribunalen, *Judgement and Sentences*, *American Journal of International Law* 1947, nr. 41.
[440] *Nicaragua*-case, par. 194.
[441] IGH, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, 19 december 2005, *ICJ Reports 2005*, par. 143 (hierna: *Congo v. Uganda*-case).
[442] *Congo v. Uganda*-case, par. 148.
[443] *In Larger Freedom: Towards Development, Security and Human Rights for All*, Rapport van het Secretariaat-Generaal van de Verenigde Naties, 2005, *Doc.nr.* A/59/565, 33.
[444] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 122.

133. De vraag is nu hoe 'imminent' een dreiging moet zijn voor er sprake kan zijn van zelfverdediging, wat neerkomt op de vraag hoe ernstig een voorbereidende cyberaanval moet zijn om art. 51 toepassing te laten vinden. Indien de *Caroline*-standaard in zijn meest extreme vorm moet aangenomen worden, moet de daad van zelfverdediging net voor de gewapende aanval uitgevoerd worden[445]. Het zou misschien, in navolging van SCHMITT, logischer zijn om het principe achter de standaard na te gaan: vredevolle alternatieven zoveel mogelijk kans geven, zonder staten het risico te laten lopen op schade door inertie[446]. In dit geval is 'imminent' relatief, afhankelijk van geval tot geval[447]: een zwakkere staat zal sneller mogen overgaan tot (anticiperende) zelfverdediging dan een sterkere, aangezien deze laatste meer middelen heeft om langer te wachten[448]. In de context van cyberoorlogen betekent dit exact hetzelfde: indien een cyberaanval een voorbereiding uitmaakt, dient een tegenaanval tot het laatste moment uitgesteld te worden. Het imminent karakter hangt ook hier af van geval tot geval, rekening houdend met de intensiteit van de aanval, het doel, de tijd die een succesvolle verdediging zou vergen en de snelheid waarmee een cyberaanval de netwerken kan beschadigen[449]. De aard van de cyberaanval doet er minder toe dan het belang ervan in het licht van de komende aanval: is het de laatste stap in een onomkeerbare kettingreactie of niet[450]? Er moet wel steeds rekening worden gehouden met het feit dat, in deze hypothese, niet de cyberoperatie maar wel de conventionele aanval het recht op zelfverdediging doet ontstaan, waardoor die zelfverdedigingsreactie proportioneel moet zijn aan de conventionele aanval[451] (zie volgende sectie).

134. SCHMITT stelt een schema voor waarlangs kan nagegaan worden of een cyberaanval het recht op zelfverdediging doet ontstaan[452]:

1) Is de cyberaanval (hierna CA) *gewapend* geweld (d.i. met de intentie om directe schade aan personen of materiele voorwerpen toe te brengen)?

[445] SCHMITT, 40.
[446] *Ibid.*; GREENWOOD, "Caroline, The", nr. 7.
[447] *Tallinn-manual*, 60.
[448] SCHMITT, 40.
[449] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 122.
[450] SCHMITT, 41.
[451] SCHMITT, 42.
[452] SCHMITT, 43.

2) Indien *NIET*, is de CA niettemin gebruik van geweld zoals verboden door art. 2(4) VN Handvest? (Dit is het geval indien de aard van de gevolgen dezelfde zijn als bij *gewapend* geweld)
3) Indien de CA gebruik van geweld uitmaakt (gewapend of anderzijds), is dit gebruik overeenkomstig Hoofdstuk VII VN Handvest[453], het principe van zelfverdediging of andere toegelaten vormen?
    a. Indien *WEL*, dan is de CA toegelaten (en dus geen recht op zelfverdediging).
    b. Indien *NIET* en de CA vormt een gebruik van *gewapend* geweld, dan is het in conflict met het gewoonterecht en art. 2(4) VN Handvest (en biedt het dus recht op zelfverdediging).
    c. Indien *NIET* en de CA vormt een gebruik van geweld, maar geen *gewapend* geweld, is er een inbreuk op art. 2(4) VN Handvest (maar geen recht op zelfverdediging, gezien het geen *gewapend* geweld uitmaakt).
4) Indien de CA geen gebruik van geweld uitmaakt, moet er gekeken worden of andere internationaalrechtelijke normen de CA verbieden (bijvoorbeeld het non-interventiebeginsel)

Indien een cyberaanval dan de vereiste drempel overschrijdt, kunnen volgens SCHMITT de volgende reacties (niet alleen zelfverdediging) worden uitgelokt[454]:

1) Indien de CA *gewapend* geweld uitmaakt, kan de Veiligheidsraad deze kwalificeren als een daad van agressie of een inbreuk op de vrede en tegenmaatregelen op basis van art. 42 VN Handvest[455] autoriseren;
2) Indien de CA deze drempel niet overschrijdt, kan de Veiligheidsraad toch gebruik van geweld autoriseren om een eventueel mogelijke inbreuk op de vrede te voorkomen;
3) Staten kunnen ingevolge art. 51 alleen of collectief zichzelf verdedigen tegen een CA, indien deze een *gewapende aanval* uitmaakt;

[453] Art. 39-51 VN Handvest, waardoor de Veiligheidsraad de bevoegdheid krijgt om dreigingen voor de vrede en stabiliteit aan te pakken met o.a. vredesmissies of door het gebruik van geweld toe te staan.
[454] SCHMITT, 43-44.
[455] Wat neerkomt op het recht van de Veiligheidsraad om geweld te (laten) gebruiken om de vrede te herstellen, zowel ter land, ter zee als in de lucht, en met enige interpretatie, ook in de cyberspace.

4) Indien een CA deze drempel niet overschrijdt, kunnen staten eventueel toch alleen of collectief zichzelf verdedigen, indien de CA een integraal onderdeel is van een operatie die moet uitmonden in een gewapende aanval, wanneer:
    a. De CA plaatsvindt op het laatst mogelijke moment voor een tegenaanval, *en*
    b. De CA een onomkeerbare stap is in een imminente en mogelijks onontkoombare aanval (hetzij met conventionele wapens, hetzij een andere CA).

135. Er kan niet anders dan vastgesteld worden dat deze schematisering van het probleem heel afhankelijk is van de invulling van *gebruik van geweld*, *gewapend geweld* en *gewapende aanval*. De kwalificatie van de cyberaanval zal dus altijd afhangen van het doel (vernietiging of verwonding), of, indien dit in de toekomst zou gebeuren, verdragsbepalingen of evoluties in het internationaal gewoonterecht, iets wat SCHMITT zelf ook toegeeft[456]. Bovendien laat deze schematisering toch enkele gevallen buiten beschouwing: wat met een opeenvolging van kleine cyberaanvallen, die elk de drempel niet overschrijden, maar samen wel ernstige nadelige effecten teweegbrengen, of cyberaanvallen die geen materiele vernietiging met zich meebrengen, maar wel ernstig nadeel aan een andere staat berokkenen[457]?

2. Toegelaten middelen en limieten op het zelfverdedigingsrecht

136. Sinds de *Nicaragua*-case[458] en het *Caroline*-incident[459] wordt aangenomen dat een daad van zelfverdediging noodzakelijk en proportioneel moet zijn[460]. Dit werd later bevestigd in de *Oil Platforms*-case[461]. Dit geldt volgens de *Tallinn-manual* ook voor cyberaanvallen[462]. De noodzakelijkheidseis houdt in dat het gebruik van geweld absoluut nodig is om een aanval succesvol af of terug te slaan, hoewel dit niet terug te vinden is in de tekst van art. 51 VN Handvest. Een probleem met beide vereisten is dat dit op voorhand moet nagegaan worden: een staat heeft bijvoorbeeld het recht om

[456] SCHMITT, 44.
[457] *Tallinn-manual*, 55-56.
[458] *Nicaragua*-case, par. 176, 194.
[459] GREENWOOD, "Caroline, The", nr. 6.
[460] CAVV, 22-23.
[461] IGH, *Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, 6 november 2003, *ICJ Reports 2003*, p. 161 e.v., par. 43, 73-74, 76
[462] *Tallinn-manual*, 59.

veroverd gebied terug te eisen, maar het moet nadien aantonen dat de vooraf ingeplande middelen absoluut noodzakelijk en proportioneel waren voor het beoogde doel[463].

137. Om van noodzakelijkheid te kunnen spreken, moeten minstens de daders worden geïdentificeerd, moet worden nagegaan of de aanval geen vergissing uitmaakte (wat in de cybercontext gemakkelijker het geval kan zijn dan met conventionele wapens) en moet de situatie niet op een andere manier kunnen worden opgelost[464]. Maar zoals reeds enkele keren vermeld, is het identificeren van de daders dikwijls niet zo eenvoudig. Enkele auteurs zijn daarom van mening om deze vereiste te laten vallen[465]. Dit lijkt tamelijk verregaand: niet alleen weet men dan niet tegen wie men verdedigt, maar ook niet wie de effecten van de tegenaanval of verdedigingsactie zal voelen[466]. Om het met een (over-)gesimplificeerde analogie te stellen: het zou zijn alsof een blinde willekeurig in het rond slaat bij het voelen van een aanval, in de hoop de aanvaller te treffen[467]. ROSCINI geeft bovendien aan dat, aangezien 'kritieke infrastructuur' niet is gedefinieerd, het niet eens zeker is of een aanval op deze infrastructuur wel recht zou geven op zelfverdediging, laat staan dat die blind zou uitgevoerd worden[468].

138. Proportionaliteit houdt vervolgens in dat rekening moet worden gehouden met de dreiging van de gewapende aanval, en niet noodzakelijk met de effectieve mankracht ervan[469]. GREENWOOD geeft een simpel voorbeeld om dit aan te tonen: Staat A kan door middel van een verrassingsaanval met een relatief kleine troepenmacht een groot deel van staat B veroveren. Indien staat A dit veroverd gebied dan versterkt, met staat B met een veel grotere troepenmacht terugslaan om het gebied te heroveren. Staat B beperken tot de troepenmacht van de initiële aanval zou daarom contraproductief werken. Natuurlijk is dit voorbeeld van bezetting minder relevant voor cyberoorlog,

[463] GREENWOOD, "Self-Defence", nr. 26-27.
[464] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 119.
[465] S.M. CONDRON, "Getting It Right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law and Technology*, 2006-2007, nr. 20, 415-416; M. HOISINGTON, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review*, 2009, nr. 32, 439 e.v.; E.T. JENSEN, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence", *Stanford Journal of International Law*, 2002, nr. 38, 234-235.
[466] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 119.
[467] GOMBEER, 217.
[468] *Ibid*.
[469] GREENWOOD, "Self-Defence", nr. 28.

maar de principes blijven dezelfde: ook cyberaanvallen moeten aan deze voorwaarden voldoen. Het is ten slotte niet steeds mogelijk om cyberaanvallen te gebruiken als zelfverdediging, ofwel omdat de aanvallende staat geen voldoende ontwikkelde infrastructuur heeft om digitale aanvallen uit te voeren[470], ofwel omdat de noodzakelijkheids- en proportionaliteitsvereisten beperkingen opleggen in de gebruikte wapens en methodes[471].

139. Deze laatste vereiste, die de gebruikte wapens en methodes beperkt, is in het geval van cyberoorlogen van belang. Mag een staat conventionele wapens gebruiken om zichzelf tegen een cyberaanval te verdedigen? Mag een cyberaanval gebruikt worden om tegen een conventionele aanval op te treden? Er is alleszins geen vereiste dat geweld met gelijkaardig geweld *moet* worden beantwoord. Een cyberaanval kan dus door een conventionele, 'kinetische' aanval tegemoet worden getreden en *vice versa*[472]. Het zal afhangen van wat in een geval noodzakelijk is (wat geval per geval moet worden nagegaan) en wat proportioneel lijkt. Gezien het feit dat grootschalige, vernietigende cyberaanvallen nog niet zijn voorgekomen, kan er redelijkerwijs gesteld worden dat een conventionele tegenaanval de proportionaliteitstoets nu overschrijdt, al moet dit niet noodzakelijk zo blijven. Een cyberaanval zal waarschijnlijk altijd de proportionaliteitstoets doorstaan, maar men moet toch steeds ervoor zorgen dat de cyber-tegenaanval niet te ver wordt doorgedreven.

3. Collectieve zelfverdediging

140. Art. 51 VN Handvest geeft staten het recht om collectief op te treden tegen aanvallen die een "Lidstaat van de Verenigde Naties" treffen. Deze vereiste, dat een aanval een Lidstaat van de Verenigde Naties moet treffen, is zonder belang komen te staan, aangezien dit recht als internationaal gewoonterecht wordt gezien, dat voor iedere staat toepasselijk is[473]. Voor de *Nicaragua*-case werd aan de bepaling rond collectieve zelfverdediging weinig aandacht besteed[474]. Die case stelde echter wel drie vereisten voorop[475] waaraan een staat (die zelf niet het slachtoffer is van een gewa-

[470] ROSCINI, "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", 120.
[471] GREENWOOD, "Self-Defence", nr. 29; ook erkend in de *Nuclear Weapons*-opinion.
[472] *Tallinn-manual*, 60.
[473] GREENWOOD, "Self-Defence", nr. 7.
[474] GREENWOOD, "Self-Defence", nr. 35.
[475] *Nicaragua*-case, par. 193 e.v.

pende aanval) moet voldoen om rechtmatig het recht op collectieve zelfverdediging te kunnen uitoefenen.

141. Ten eerste (en vrij logisch) moet er sprake zijn van minstens één staat in het collectief die ook recht heeft op individuele zelfverdediging, d.i. er moet minstens één staat zijn die zelf aangevallen wordt. Verder moet volgens de *Nicaragua*-case die staat zich eerst officieel slachtoffer verklaren voor er collectieve zelfverdediging kan plaatsvinden. Ten slotte mogen andere staten slechts tussenkomen indien de slachtofferstaat officieel om een tussenkomst heeft verzocht (wat bijvoorbeeld het geval was voor Koeweit na de invasie door Irak[476]). Het Hof eiste niet het bestaan van een voorafgaand bondgenootschap (zoals NAVO), terwijl JENNINGS in zijn *dissenting opinion* afwijkend van mening was dat de andere staten die tussenkomen ook onder dreiging moeten staan[477]. Dit is zonder problemen toepasbaar op het gebied van cyberoorlogen (al moet steeds nagegaan worden of een cyberoperatie de drempel van gewapende aanval overschrijdt).

4. Terrorisme

142. Opnieuw vormt terrorisme (en dus cyberterrorisme) een uitzonderlijk geval op het recht op zelfverdediging[478]. In theorie vereist art. 51 VN Handvest een transnationaal karakter[479], maar het is niet zeker of de originele aanval van een staat afkomstig moet zijn om dit artikel toepassing te laten vinden[480]. Indien een terroristische aanval op enige wijze de verantwoordelijkheid van een staat is, dan speelt het recht op zelfverdediging (indien die aanval de drempel van gewapende aanval overschrijden)[481]. Het Hof oordeelt daarentegen dat terroristische aanvallen waar geen enkele staat voor verantwoordelijk is, nooit een gewapende aanval kunnen uitmaken[482]. Het *Caroline*-incident beperkte het recht op zelfverdediging echter [483]niet, net zoals art. 51 VN Handvest dat niet doet. Hoewel inderdaad de focus vooral lag op aanvallen *op* staten

[476] GREENWOOD, "Self-Defence", nr. 38.
[477] *Nicaragua*-case, *Dissenting Opinion* van rechter Sir ROBERT JENNINGS.
[478] DINNISS, 95-99.
[479] Zie nr. 127.
[480] GREENWOOD, "Self-Defence", nr. 15.
[481] *Nicaragua*-case; *Congo v. Uganda*-case, 168 e.v.; IGH, *Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 9 juli 2004, *ICJ Reports 2004*, p. 136 e.v. (hierna: *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory-opinion*).
[482] *Congo v. Uganda*-case par. 146; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory-opinion*, par. 139.
[483] GREENWOOD, "Self-Defence", nr. 17.

door staten, is het zeker niet duidelijk of statenpraktijk en *opinio iuris* dan ook het recht op zelfverdediging tot die situaties heeft beperkt[484].

143. In elk geval heeft de Veiligheidsraad van de Verenigde Naties na de aanslagen van 11 september 2001 in de reeds vermelde resoluties 1368 en 1373 het recht op zelfverdediging bevestigd, maar maakte het niet duidelijk of die aanvallen op de een of andere manier aan een staat toe te wijzen moeten zijn. De reactie van de Verenigde Staten en het Verenigd Koninkrijk door Afghanistan binnen te vallen, heeft echter geen protest van de meerderheid van staten uitgelokt, hoewel het op dat moment niet duidelijk was of Afghanistan op de een of andere manier bij de aanslagen was betrokken[485].

144. Het is evident dat een staat mag optreden tegen niet-statelijke actoren (zoals terroristen) die binnen in die staat opereren[486]. De statenpraktijk volgend op de aanslagen van 11 september 2001 lijkt te zijn dat dit een gewapende aanval uitmaakte, wat recht gaf op zelfverdediging[487]. Het Internationaal Gerechtshof lijkt deze mening echter (nog) niet toegedaan te zijn[488]. De meerderheid van experts in de *Tallinn-manual* is echter van oordeel dat de statenpraktijk het recht op zelfverdediging in deze situatie wel erkent en dat dit kan doorgetrokken worden naar cyberaanvallen[489]. Het probleem is echter dat de statenpraktijk zeer divers is geweest in zijn aanpak van terrorisme[490], terwijl het gebruik van geweld verder ging dan loutere zelfverdediging, zoals represailles en de afdwinging van het internationaal recht[491]. TAMS waarschuwt dat een te extensieve interpretatie van het recht op zelfverdediging deze uitzondering op het gebruik van geweld zou kunnen uithollen[492].

145. Zonder de problematiek van terrorisme en zelfverdediging hier volledig te analyseren, wat het doel van deze masterproef ver te buiten zou gaan, kan voor wat betreft cyberterrorisme misschien aangesloten worden bij de tussenoplossing, vooropgesteld

[484] *Ibid.*
[485] *Ibid*.
[486] *Tallinn-manual*, 54.
[487] *Tallinn-manual*, 57.
[488] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory-opinion*, par. 139.
[489] *Tallinn-manual*, 57.
[490] C.J. TAMS, "The Use of Force against Terrorists", *EJIL*, 2009, Vol. 20 nr. 2, 382 (hierna: TAMS, "The Use of Force against Terrorists").
[491] TAMS, "The Use of Force against Terrorists", 382.
[492] TAMS, "The Use of Force against Terrorists", 383.

door TAMS[493]. Hij stelt dat de klassieke premisse (enkel zelfverdediging bij *statelijk* geweld) nog altijd geldt, maar dat er speciale regels gelden in verband met terrorisme (en vooral in verband met toerekenbaarheid van terroristische daden): staten moeten nu zelfverdedigingsreacties in hun territorium dulden indien zij steun hebben geboden, die echter de drempel (van gewapend geweld) van de *Nicaragua*-case niet overschrijdt. Indien die steun de drempel van die case wel te boven gaat, is er vanzelfsprekend gewapend geweld en is een zelfverdediginsreactie logisch.

5. De rol van de VN Veiligheidsraad

146. In het debat rond het recht op zelfverdediging moet ook iets gezegd worden over de rol van de VN Veiligheidsraad in deze situatie. Ten eerste moeten maatregelen genomen ter zelfverdediging gerapporteerd worden aan de Veiligheidsraad[494]. Indien dit niet gebeurt, is er niet alleen sprake van een inbreuk op het Handvest, maar zal het bewijs dat de maatregelen een legitieme vorm van zelfverdediging uitmaakten minder aannemelijk worden[495]. Voorts bepaalt datzelfde art. 51 dat maatregelen ter zelfverdediging enkel mogen uitgevoerd worden totdat de Veiligheidsraad de nodige maatregelen heeft genomen ter vrijwaring van de internationale vrede en veiligheid.

147. Verder wordt het algemeen aanvaard dat uit die rechten die aan de Veiligheidsraad toekomen, ook het recht van die raad voortkomt om wapenstilstanden op te leggen[496]. In dit geval moeten alle vijandelijkheden stoppen, ook die ter zelfverdediging. Niet elke handeling van de Veiligheidsraad is echter zo verregaand, en het loutere uitvaardigen van een resolutie (zelfs een bindende resolutie) maken geen 'maatregelen' in de zin van art. 51 uit[497]. Enkel indien de maatregelen noodzakelijk zijn om de vrede te waarborgen, zal het recht op zelfverdediging ophouden te bestaan. Soms geeft de Veiligheidsraad zelf aan dat een genomen maatregel het recht op zelfverdediging niet aantast[498].

[493] TAMS, "The Use of Force against Terrorists", 385.
[494] Art. 51 VN Handvest.
[495] GREENWOOD, "Self-Defence", nr. 31.
[496] GREENWOOD, "Self-Defence", nr. 33.
[497] *Ibid.*
[498] GREENWOOD, "Self-Defence", nr. 34.

148. In het kader van cyberoorlog en cyberoperaties is het zelfs mogelijk dat de maatregelen die de VN Veiligheidsraad oplegt cyberoperaties zijn[499], bijvoorbeeld als dwangmaatregel ter vrijwaring van de internationale vrede[500]. Zoals GOMBEER stelt, zou dit soort dwangmaatregelen zelfs zeer belangrijk kunnen worden, aangezien cyberspace meer en meer gebruikt wordt en op dagelijkse gebeurtenissen van toepassing is.

6. Conclusie

149. Het recht op zelfverdediging *in se* geeft niet veel problemen voor wat betreft cyberoorlogen. Indien cyberaanvallen de vereiste drempels bereiken, kan een zelfverdedigingsreactie worden uitgelokt. Cyberaanvallen kunnen bovendien een manier van zelfverdediging uitmaken, aangezien er nergens bepaald staat dat zelfverdediging beperkt moet zijn tot sommige manieren van oorlogsvoering. De regels van de collectieve zelfverdediging zijn daarnaast zonder probleem van toepassing. Een heikeler punt vormt het recht op zelfverdediging naar aanleiding van terroristische aanslagen. Net zoals dat bij conventionele 'oorlogsvoering' het geval is, is het eigenlijke bestaan van dit recht in dit geval niet zeker. Gelet op de statenpraktijk kan men echter stellen dat, mits aan bepaalde voorwaarden is voldaan, terrorisme een zelfverdedigingsreactie kan uitlokken. Het is daarom zowel aannemelijk dat die zelfverdediging kan ontstaan na een daad van cyberterreur[501] als dat een cyberoperatie een vorm van zelfverdediging uitmaakt.

150. Een specifiek maar in de praktijk belangrijk geval is de situatie waarin een cyberaanval op zich geen recht geeft op zelfverdediging, maar waarbij die cyberoperatie een voorbereiding is op een conventionele aanval die *wel* daarop recht zou kunnen geven (d.i. die *wel* een gewapende aanval uitmaakt). Hiervan zijn al voorbeelden in de praktijk voorgekomen, zoals de vermelde cyberoperaties van Rusland tegen Georgië. Dit is een geval van anticiperende zelfverdediging. Algemeen wordt aanvaard dat, om rechtmatig te zijn, de 'zelfverdediging' (hoewel het misschien correcter is om in dit geval van een tegenaanval te spreken) moet gebeuren naar aanleiding van een *imminente* dreiging. Dit moet geval per geval nagegaan worden, aangezien verschillende

[499] GOMBEER, "Het internationaal juridisch kader voor interstatelijk gebruik van computeraanvallen", 207-208.
[500] Art. 39 VN Handvest.
[501] Hoewel het onwaarschijnlijk is dat dit snel zal voorkomen, zie nr. 98.

situaties het imminent karakter van een aanval kunnen beïnvloeden. Het schema dat SCHMITT voorstelt om uit te maken of een cyberaanval een zelfverdedigingsreactie kan uitlokken, heeft als voordeel dat het exhaustief is, maar als nadeel dat het steunt op onduidelijke elementen, zoals de invulling van 'gewapend geweld', 'gewapende aanval' en 'imminent karakter'. Er zal dus steeds een analyse van geval per geval moeten gebeuren.

C. Het gebruik van nucleaire wapens

1. Probleemstelling

151. Zoals het non-proliferatieverdrag[502] (weerspiegeld in het internationaal gewoonterecht[503]), de resolutie van de Algemene Vergadering van de Verenigde Naties betreffende een verbod op kernwapens[504] en vooral de *Nuclear Weapons-opinion* (hoewel daar niet expliciet een verbod werd gesteld[505]) aantonen, lijkt er in het algemeen een afkeuring, zo niet een niet-afdwingbaar verbod te bestaan op het gebruik en/of bezit van nucleaire wapens. Enkel in het geval van ultieme zelfverdediging zou een kernwapen gebruikt mogen worden, volgens de *Nuclear Weapons-opinion*[506]. De redenering die het Internationaal Gerechtshof hiervoor volgde, was dat een dergelijke aanval enkele fundamentele principes van het humanitair recht schond: het verbod op non-discriminatoire aanvallen, het verbod op het toebrengen van onnodig leed en de verplichting om burgers en burgerlijke eigendom te beschermen[507]. Bovendien werd de Martensclausule aangehaald om aan te tonen dat, ondanks het gebrek aan specifieke regulering, het algemeen internationaal recht van toepassing blijft[508]. Deze redenering kan zeker bijgetreden worden, gelet op het enorm aantal slachtoffers bij de atoombommen van Hiroshima (minimaal 150 000 directe slachtoffers, ontelbaar veel slachtoffers met gevolgen van radioactieve straling) en Nagasaki (minimaal 75 000 directe slachtoffers)[509].

[502] Verdrag betreffende de non-proliferatie van kernwapens van 1 juli 1968, New York, *UNTS* 161.
[503] M. BOTHE, "Nuclear Weapons Advisory Opinions", *MPEPIL*, OPIL, oktober 2015, opil.ouplaw.com, nr. 23 (hierna: BOTHE, "Nuclear Weapons Advisory Opinions").
[504] *Resolutie 52/39 C van de Algemene Vergadering van de Verenigde Naties*, 31 december 1997, *Doc.Nr.* A/RES/52/39.
[505] BOTHE, "Nuclear Weapons Advisory Opinions", nr. 24.
[506] *Ibid.*
[507] *Nuclear Weapons-opinion*, par. 75 e.v.
[508] Zoals in het eerste deel van deze thesis uitvoerig is aangetoond.
[509] N.N., "Children of the Atomic Bomb – A UCLA Physician's Eyewitness Report and Call to Save the World's Children", *UCLA*, s.d., aasc.ucla.edu.

152. Een *meltdown* of een ontploffing van een kernreactor kent veel minder directe slachtoffers. Dit valt fysisch te verklaren doordat bij een atoombom de onmiddellijke slachtoffers vallen door de kinetische energie die vrijkomt als gevolg van het splitsen van atomen, terwijl een kernreactor daar niet voor gebouwd is: de energie die vrijkomt, wordt juist opgeslagen. Dit komt door het verschil in het gebruikte Uranium[510]. Rampen met kernreactoren zorgen echter voor veel meer onrechtstreekse slachtoffers als gevolg van straling[511]. Er zou dus kunnen gesteld worden dat slechtfunctionerende kernreactoren en kernwapens gelijkaardige effecten hebben, met een gelijkaardige impact op hun slachtoffers, die gelijkaardige bepalingen schenden in het internationaal recht.

153. Deze korte wetenschappelijke uitleg is van belang voor het volgende: indien een cyberaanval een kerncentrale zou treffen, om daar de veiligheidssystemen onderuit te halen, kan een kernreactor in principe oververhit geraken en ontploffen. Een cyberaanval zou ook de codes van kernwapens kunnen achterhalen en die kernwapens lanceren. Bij dit laatste moet evenwel een enigszins grappige maar belangrijke anekdote worden vermeld: blijkbaar bestaat het lanceersysteem van een van de nucleaire grootmachten, de Verenigde Staten van Amerika, uit oude floppydisks (door een gebrek aan updates), waardoor dit oud systeem eigenlijk minder eenvoudig te hacken valt[512]. Deze gevaren zijn niet louter denkbeeldig: op de recente top rond nucleaire wapens werd het gevaar van terroristen in het bezit van een kernwapen benadrukt, maar tegelijk ook aangetoond dat, naar aanleiding van de aanslagen in Brussel, kerncentrales een potentieel doelwit vormen[513]. Om die redenen zal in dit onderdeel onderzocht worden hoe de problematiek rond kernwapens kan of moet ingepast worden in de situatie van cyberaanvallen, waarbij onder 'kernwapens' ook door vijandige systemen overgenomen kerncentrales worden begrepen.

[510] J.M. ARDER, "Nuclear Reactors and Nuclear Bombs: What Defines the Difference?", *PBS*, 6 april 2011, pbs.org.
[511] Zo zou het dodentol van Tsjernobyl opgelopen zijn tot 985 000 slachtoffers; K. GROSSMAN, "Chernobyl Death Toll: 985,000, Mostly from Cancer", *Centre for Research on Globalization*, 4 september 2010, globalresearch.ca.
[512] *Last Week Tonight with John Oliver*, Episode 12, Seizoen 1, *HBO*.
[513] D. SMITH, "Barack Obama at nuclear summit: 'madmen' threaten global security", *The Guardian*, 1 april 2016, theguardian.com.

2. Algemene regels rond kernwapens

154. In tegenstelling tot 'conventionele' wapens, vallen kernwapens onder de zogenaamde massavernietigingswapens (ook vaak WMD – Weapons of Mass Destruction – genoemd)[514]. Deze categorie bestaat verder enkel nog uit chemische en biologische wapens[515], maar kan later nog uitgebreid worden indien nieuwe wapens dezelfde karakteristieken gaan vertonen[516]. Deze kernwapens en het gebruik ervan worden echter door geen enkel specifiek verdrag geregeld (het non-proliferatieverdrag houdt een regulering en beperking in over de bestaande wapens, maar niet over hun gebruik)[517]. Gelet op het feit dat verschillende grootmachten een kernwapenarsenaal hebben, kan men al moeilijk verdedigen dat het bezit van kernwapens *an sich* illegaal is[518].

155. Net zoals het geval is bij cyberoorlog, zal de Martensclausule moeten ingeroepen worden om het algemeen internationaal recht toe te passen op kernwapens[519]. Een eerste bepaling die wordt aangehaald als toepasselijk is het verbod op genocide[520], aangezien de kracht van een kernwapen al snel hele bevolkingsgroepen in een klap kan doden[521]. Hoewel dit op het eerste zicht logisch lijkt, moet deze masterproef KADELBACH bijtreden: om van genocide te kunnen spreken, is de subjectieve wil om een bepaalde bevolking(sgroep) uit te moorden vereist[522]. Aangezien dit subjectieve element moeilijk te bewijzen valt[523], zal het Genocideverdrag waarschijnlijk slechts in uitzonderlijke gevallen spelen.

156. Mensenrechten moeten ten allen tijde worden gerespecteerd, ook in tijden van oorlog. Zo kan er van het recht op leven niet worden afgeweken[524], ook niet in tijden van 'nationale noodtoestanden' (waaronder gewapende conflicten)[525]. Dit art. 4 bepaalt wel dat het recht op leven van art. 6 bekeken moet worden vanuit de toepasselij-

[514] S. KADELBACH, "Nuclear Weapons and Warfare", *MPEPIL*, OPIL, juni 2013, opil.ouplaw.com, nr. 1 (hierna: KADELBACH, "Nuclear Weapons and Warfare").
[515] H.A. STRYDOM, "Weapons of Mass Destruction", *MPEPIL*, OPIL, augustus 2013, opil.ouplaw.com, nr. 1.
[516] *Resolutie 18 van de Veiligheidsraad van de Verenigde Naties*, 12 februari 1947, *Doc.nr.* S/RES/18.
[517] KADELBACH, "Nuclear Weapons and Warfare", nr. 1.
[518] KADELBACH, "Nuclear Weapons and Warfare", nr. 29.
[519] Zoals in het eerste deel van deze Masterproef uitvoerig is toegelicht.
[520] Verdrag betreffende de preventie en de bestraffing van de misdaad van genocide van 9 december 1948, Parijs, *UNTS* 277 (hierna: Genocideverdrag).
[521] KADELBACH, "Nuclear Weapons and Warfare", nr. 33.
[522] Art. 2 Genocideverdrag.
[523] IGH, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro*, 26 februari 2007, *ICJ Reports 1996*, par. 186-201.
[524] Art. 6 BUPO-verdrag.
[525] Art. 4 BUPO-verdrag.

ke *lex specialis*. In tijden van oorlog zal dit het internationaal humanitair recht zijn. Slachtoffers maken kan dus, hoewel de burgerbevolking gespaard moet worden. Daar komen onmiddellijk enkele fundamentele principes bij kijken: het verbod op het gebruik van giftige wapens, het verbod op het toebrengen van onnodig leed en de plicht om de burgerbevolking te beschermen.

157. Den Haag 1907 bepaalt in art. 23(a) dat het gebruik van vergif of giftige wapens verboden is. Aangezien deze verdragen gezien worden als internationaal gewoonterecht, blijft dit tot op de dag van vandaag verboden[526]. Het verbod op het gebruik van giftige wapens is echter nog elders terug te vinden: ook het Gifgasprotocol verbiedt het gebruik van dergelijke wapens. Er kan zeker gesteld worden dat de effecten van een nucleaire *fallout* gelijkgesteld kunnen worden met vergif[527]. De stelling van KADELBACH, dat ingevolge de *Nuclear Weapons-opinion* enkel chemische wapens als giftige wapens gebruikt kunnen worden, kan niet volgens deze auteur niet bijgetreden worden: aangezien ook biologische stoffen gebruikt kunnen worden als vergif[528], zou deze stelling dit soort wapens vrijstellen van het verbod. Puur wetenschappelijk gezien zou radiatievergiftiging als gevolg van een kernwapen dus onder dit verbod moeten vallen.

158. Een ander belangrijk principe in het internationaal humanitair recht, is het verbod om buitensporig leed toe te brengen, wat ondertussen internationaal gewoonterecht is[529]. Al sinds de Haagse Vredesconferenties werd in art. 22 bepaald dat de oorlogvoerende partijen geen onbeperkte keuze hadden in het gebruik van wapens, en art. 23(e) preciseert dit: de partijen mogen geen wapens, projectielen of ander materiaal gebruiken met als doel buitensporig leed te veroorzaken. De *Nuclear Weapons-opinion* past deze bepaling echter niet toe, de opinie oordeelt enkel dat, in geval de radioactieve *fallout* niet het gevolg is van een redelijk strategisch of tactisch doel, deze bepaling

[526] KADELBACH, "Nuclear Weapons and Warfare", nr. 34; , J.-M. HENCKAERTS, L. DOSWALD-BECK, *Internationaal humanitair gewoonterecht*, International Committee of the Red Cross, *s.l.*, *s.d.*, 27 (hierna: HENCKAERTS, DOSWALD-BECK).
[527] Beaamd door Rechter WEERAMANTRY, *Nuclear Weapons-Opinion*, Dissenting Opinion of Judge WEERAMANTRY.
[528] D.R. NELSEN, Z. NISANI, A.M. COOPER, G.A. FOX, E.C. GREN, A.G. CORBIT, W.K. HAYES, "Poisons, toxigens, and venoms: redifining and classifying toxic biological secretions and the organisms that employ them", *Biological Reviews of the Cambridge Philosophical Society*, 2014, vol. 89 nr. 2, ncbi.nlm.nih.gov; het verschil tussen biologische en chemische gassen zit in het feit dat chemische gassen artificieel gemaakt zijn, terwijl biologische wapens gebruik maken van bacteria of virussen: M. BRAIN, S.L. NASR, "How Biological and Chemical Warfare Works", *Science*, 27 september 2001, HowStuffWorks.com.
[529] HENCKAERTS, DOSWALD-BECK, 27.

geschonden kan zijn[530]. KADELBACH geeft aan dat enkele auteurs van mening zijn dat nucleaire wapens niet als doel hebben om onnodig leed te veroorzaken (via de straling), maar dat dit slechts een bijkomend effect is[531]. Of een kernwapenaanval dan onder dit verbod zou vallen, hangt volgens deze auteurs af van de militaire noodzaak en de proportionaliteit[532]. Er kan daarentegen gesteld worden dat een wapen buitensporig leed veroorzaakt, als een ander soort wapen dezelfde resultaten kan bereiken, met minder leed als gevolg (zoals het vernietiging van tanks via ofwel een kernwapen ofwel kleinere, minder 'schadelijke' raketten)[533].

159. Om te weten of een wapen (en hier meer specifiek een kernwapen) onnodig of buitensporig leed veroorzaakt, moet men eerst weten wat als 'buitensporig leed' gezien wordt. De letterlijke tekst van art. 23(e) van de Haagse Vredesconferenties, spreekt van wapens die 'berekend' (*calculated*) zijn om dergelijk leed toe te brengen. Dit werd onder meer uitgelegd als wapens die 'ongeneselijke wonden' toebrengen, net als wapens die de dood van het slachtoffer zeker of aan zekerheid grenzend maken[534]. CASSESE stelt echter andere criteria voorop: ten eerste zouden de medische effecten van het wapen moeten nagegaan worden (de toegebrachte pijn, het blijvend karakter van verwondingen, het verminkend karakter van het wapen), vervolgens moet de graad van medische ontwikkeling van het doelwit worden onderzocht, om ten slotte tot illegaliteit te besluiten als het gebruikte wapen niet noodzakelijk was[535]. Deze criteria lijken logischer en duidelijker dan de oorspronkelijke criteria van Den Haag 1907: er kan het punt gemaakt worden dat alle wapens het oogmerk hebben om zeker om aan zekerheid grenzend te doden, wat alle wapens illegaal zou maken.

[530] *Nuclear Weapons-opinion*, par. 77.
[531] KADELBACH, "Nuclear Weapons and Warfare", nr. 35.
[532] Zie o.a.: N. SITAROPOULOS, "Weapons and superfluous injury or unnecessary suffering in international humanitarian law: human pain in time of war and the limits of law", *Revue Hellénique de Droit International*, 2001, vol. 54, 81 (hierna: SITAROPOULOS, "Weapons and superfluous injury or unnecessary suffering in international humanitarian law: human pain in time of war and the limits of law"); R.M. COUPLAND, "Towards a Determination of Which Weapons Cause 'Superfluous Injury or Unnecessary Suffering'", *International Physicians for the Prevention of Nuclear War*, 1997, ippnw.org (hierna: COUPLAND, "Towards a Determination of Which Weapons Cause 'Superfluous Injury or Unnecessary Suffering'"); HENCKAERTS, DOSWALD-BECK, 19.
[533] KADELBACH, "Nuclear Weapons and Warfare", nr. 35.
[534] SITAROPOULOS, "Weapons and superfluous injury or unnecessary suffering in international humanitarian law: human pain in time of war and the limits of law", 81.
[535] A. CASSESE, "Weapons causing unnecessary suffering: Are they prohibited?", *Rivista di Diritto Internazionale*, 1975, nr. 48, 12-13.

160. De discussie rond het al dan niet verboden karakter van kernwapens aan de hand van het vernoemde principe, ligt dus nog niet stil[536]. KADELBACH meent dat de legaliteit van het gebruik afhangt van de omstandigheden waarin het gebruikt wordt[537]. Enkele medici hebben verder zelf hun criteria opgesteld, in geval een kernoorlog zou uitbreken: COUPLAND stelt voor om wapens aan de hand van de volgende criteria te beoordelen: 1) het wapen veroorzaakt een specifieke ziekte, fysiologische of psychologische staat, specifiek permanent gebrek of verminking, 2) het wapen zorgt voor een sterftecijfer van minstens 25 % in het veld of minstens 5 % in ziekenhuizen, 3) het wapen veroorzaakt wonden van categorie 3[538] en 4) Het wapen veroorzaakt effecten die geen erkende of bewezen remedies hebben[539]. Deze criteria zijn duidelijk meer medisch geïnspireerd. Het belang van deze discussie rechtvaardigt de vermelding hiervan in deze masterproef: het is niet zeker of kernwapens gezien worden als wapens die onnodig leed veroorzaken, doordat het doel van een kernwapen de ontploffing is, en niet de schade door de radioactieve straling[540]. Het is niet zeker of, in het geval van een cyberaanval op een kerncentrale, diezelfde argumentatie ook geldt: de ontploffing van een centrale veroorzaakt minder schade, maar de straling is veel schadelijker[541].

161. Het principe van discriminatie houdt hier nauw mee verband, net de het bescherming van burgers. Volgens het internationaal gewoonterecht[542] en art 48, 51(2) en 52(2) Protocol I hebben staten de praktijk erop nagehouden om hun aanvallen enkel te richten op strijders, wat ook in de *Nuclear Weapons-opinion* werd benadrukt[543]. Dit principe geldt ook wat betreft niet-internationale gewapende conflicten, via art. 13(2) Protocol II en via de statuten van het Internationaal Strafhof te Rome, waar het als oorlogsmisdaad gezien wordt[544]. De specifieke bepalingen in Protocol I leggen staten het verbod op om aanvallen uit te voeren die geen specifiek militair doel heb-

[536] SITAROPOULOS, "Weapons and superfluous injury or unnecessary suffering in international humanitarian law: human pain in time of war and the limits of law", 82.
[537] KADELBACH, "Nuclear Weapons and Warfare", nr. 35.
[538] Volgens een schaal ontwikkeld door het Rode Kruis: R.M. COUPLAND, *The Red Cross Wound Classification*, ICRC, Geneve, 1991, 15 p.
[539] COUPLAND, "Towards a Determination of Which Weapons Cause 'Superfluous Injury or Unnecessary Suffering'", 31.
[540] KADELBACH, "Nuclear Weapons and Warfare", nr. 35.
[541] Zie nr. 152.
[542] Volgens de verzameling regels van het internationaal gewoonterecht van het Rode Kruis, HENCKAERTS, DOSWALD-BECK; ook terug te vinden in verscheidene handleidingen van de strijdkrachten van staten: vb. de handleiding van het Zweeds leger, par. 29.
[543] *Nuclear Weapons-opinion*, par. 434.
[544] Art. 8(2)(e)(i) van het Statuut van het Internationaal Strafhof van 17 juni 1998, Rome, *Doc.nr.* A/CONF.183/9.

ben of die, in verhouding tot het concrete militair voordeel, buitensporige schade aan burgers en/of private eigendom veroorzaken[545]. Het zal waarschijnlijk opnieuw van de omstandigheden afhangen of een kernwapen al dan niet deze bepaling schendt[546]: er kan bijvoorbeeld gedacht worden aan het gebruik van een kernwapen in een afgelegen woestijn, die enkel een militair konvooi raakt[547]. Dit zal met kerncentrales misschien minder het geval zijn, aangezien die niet onmiddellijk een militair doel zijn en naar alle waarschijnlijkheid burgerslachtoffers zullen maken, aangezien zij zich waarschijnlijk in de nabijheid van burgers bevinden.

162. Een laatste verbod dat vooral bij kerncentrales van belang is, is het verbod om wapens te gebruiken die "bedoeld zijn of waarvan verwacht wordt dat zij wijdverspreide, langdurige en ernstige schade aan de natuurlijke omgeving kunnen toebrengen."[548] Hoewel bij een kernwapen radioactieve straling vrijkomt, verdwijnt deze straling vrij snel, aangezien de kenmerkende paddenstoelwolk de radiatie verspreidt. Vandaag zijn Hiroshima en Nagasaki niet meer radioactief dan Gent[549]. Een ramp met een kernreactor laat de radioactiviteit enorm veel meer stijgen: na de ontploffing in Tsjernobyl was er 200 maal meer radioactiviteit dan na de atoombommen[550]. Deze enorme vervuiling zorgde ervoor dat er nu nog steeds een exclusieve zone rond de reactor is, waar slechts recent toeristen voor korte periodes worden toegelaten[551]. Langdurig verblijf is echter verboden, aangezien het stralingsniveau gevaarlijk hoog blijft. Ook grote stukken landbouwgrond in de omgeving blijven nog lange tijd onbruikbaar[552]. Hoewel een kernwapen dus mogelijk gebruikt mag worden, verbiedt Protocol I het gebruik van een kerncentrale als wapen, door de enorme ecologische impact.

[545] KADELBACH, "Nuclear Weapons and Warfare", nr. 37.
[546] KADELBACH, "Nuclear Weapons and Warfare", nr. 40.
[547] Y. DINSTEIN, "Warfare, Methods and Means", *MPEPIL*, OPIL, september 2015, opil.ouplaw.com, nr. 3 (hierna: DINSTEIN, "Warfare, Methods and Means").
[548] Art. 35(3) Protocol I; ook internationaal gewoonterecht: HENCKAERTS, DOSWALD-BECK, 23.
[549] P. TAKASHASHI, "Why worry about Fukushima when Hiroshima and Nagasaki are safe?", *The Huffington Post*, 13 april 2011, huffingtonpost.com (hierna: TAKASHASHI); Hiroshima Peace Memorial Museum Website, FAQ, pcf.hiroshima.jp, geraadpleegd op 20 april 2016;
[550] TAKASHASHI, huffingtonpost.com.
[551] E. PASQUALE, "Terror Tourism: A day at Chernobyl, 26 years later", *The Huffington Post*, 26 april 2012, huffingtonpost.com.
[552] NUCLEAR ENERGY AGENCY, *Chernobyl: Assesment of Radiological and Health Impacts – 2002 Update of Chernobyl: Ten Years On*, OECD, 2002, oecd-nea.org.

3. Is dit een reëel probleem?

163. De vraag is nu of al het voorgaande wel relevant is: kunnen kerncentrales *überhaupt* als kernwapens dienst doen, en is dit een actueel gevaar? Deze masterproef is van mening dat dit wel degelijk het geval is. Tsjernobyl, Fukushima en (dichter bij huis) de scheurtjes in de kernreactoren van Doel en Tihange[553] tonen aan dat schade door kernreactoren immens en langdurig kan zijn en, in het geval van Tsjernobyl[554], op lange termijn meer levens kan eisen dan kernwapens. Die schade kan niet alleen veroorzaakt worden door defecte centrales, maar ook door het hacken van die centrales. In 2009-2010 probeerden de Verenigde Staten van Amerika en Israël via een computeraanval de verrijking van Uranium in Iran schade toe te brengen via "Stuxnet"[555]. Deze aanval moest de centrifuges in een kerncentrale beschadigen[556] en deed dat door de veiligheidssoftware zo te misleiden, dat die enkel positieve waarden kon meten, terwijl de centrifuges veel sneller dan normaal aan het draaien waren[557]. Het virus kon via een USB-stick binnengesmokkeld worden[558].

164. Indien een virus de veiligheidssoftware kan omzeilen, kan dit ook gebruikt worden om de temperatuur in de reactorkern te laten oververhitten. Het Stuxnet-virus kon immers het SCADA-systeem (Supervisory Control and Data Acquisition system)[559] in de Iraanse kerncentrales misleiden[560], dus kan een gelijkaardig virus dit ook doen en dit SCADA-systeem zo misleiden[561] dat het normale waarden voor de reactorkern laat zien, terwijl deze oververhit raakt, met ontploffingsgevaar tot gevolg. Een kerncentrale kan dus zeker als kernwapen worden ingezet. Door het verschil in effect tussen een ontploffende kernbom en een ontploffende kernreactor, moeten de hierboven geschetste principes verschillend worden toegepast: een kernbom kan misschien een militair doel hebben en geen onnodig leed veroorzaken, maar een ontploffende kernreac-

[553] N.N., "'Scheurtjes kernreactor Doel 3 Tihange 2 ernstiger dan gedacht' (FANC)", *Knack*, 13 februari 2015, knack.be.
[554] Zie voetnoot 512.
[555] J. MENN, "Exclusive: U.S. tried Stuxnet-style campaign against North Korea but failed – sources", *Reuters*, 29 mei 2015, reuters.com.
[556] BOOTHBY, 83.
[557] BOOTHBY, 124.
[558] *Ibid*., voetnoot 131.
[559] D. GALEA, "SCADA security: How Britain can reinforce its nuclear and weapons control systems against cyber threats", *International Business Times*, 30 april 2015, ibtimes.co.uk.
[560] D. VELUZ, "Stuxnet Malware Targets SCADA Systems", *Trend Micro*, 1 oktober 2010, trendmicro.com.
[561] B. KESLER, "The Vulnerability of Nuclear Facilities to Cyber Attack", *Strategic Insights Stanford*, 2010, vol. 10 nr. 1, large.stanford.edu.

tor kan dit bijvoorbeeld wel veroorzaken, of niet voldoende onderscheid tussen strijders en burgers maken.

4. Conclusie

165. Kerncentrales kunnen via een cyberaanval gehackt worden en als kernwapen worden ingezet. Dit is geen loutere hypothese, maar is via de Stuxnet-aanval in de praktijk bewezen[562]. Het internationaal recht verbiedt kernwapens echter niet *per se*. Er is geen enkel verdrag ter zake, dus moet de Martensclausule toegepast worden om kernwapens via het algemeen internationaal (humanitair) recht enigszins te reguleren. Vooral het verbod op het gebruik van giftige wapens, de mensenrechten (het recht op leven), het verbod op het gebruik van wapens die onnodig leed veroorzaken en de bescherming van burgers zijn van toepassing: er zal steeds geval per geval nagegaan moeten worden of het gebruik van een kernwapen (hier in de zin van een 'klassieke' atoombom) deze regels niet heeft geschonden. Dezelfde criteria kunnen op gehackte kerncentrales toegepast worden, maar zullen tot andere conclusies leiden: niet alleen zorgt het verschillend effect van centrales en kernbommen of het feit dat kerncentrales minder gebruikt kunnen worden om een specifiek militair doel te bereiken voor een ander resultaat, maar zeker de ecologische impact zal leiden tot een verbod om via cyberoperaties kerncentrales als wapen in te zetten.

166. De vraag is nu of daar een specifiek verdrag rond gesloten moet worden, of indien de Martensclausule van toepassing kan worden verklaard. Het is een vrij complexe situatie: via de Martensclausule kan het internationaal recht met betrekking tot kernwapens toegepast worden op cyberoorlogen (het hacken van kerncentrales), maar de Martensclausule wordt net gebruikt om het algemeen internationaal recht toe te passen op kernwapens. Het lijkt dus onlogisch om deze problematiek voor cyberoorlogen te regelen in een verdrag, zonder dit eerst te doen voor kernwapens. Gezien de vele onduidelijkheden (om te beginnen de verschillende voorstellen voor criteria om na te gaan of een kernwapen al dan niet gebruikt mag worden), lijkt het logisch om een verdrag rond kernwapens te sluiten. Dit zou echter zowel consensus vereisen als

[562] Nu is er een nieuw virus opgedoken, FLAME, wat 20 keer krachtiger zou zijn dan Stuxnet en, naast het aanvallen van bijvoorbeeld nucleaire centrifuges, ook in staat zou zijn om informatie te verzamelen: Schriftelijke vragen en antwoorden, *Parl.St.* Kamer, 2004-2005, vraag nr. 131.

een beperking inhouden voor de nucleaire grootmachten, waardoor dit er naar alle waarschijnlijkheid niet zit aan te komen[563].

D. Verbod op het gebruik van bepaalde wapens

1. Belang

167. Nauw aansluitend op wat hierboven is gezegd, zal in dit onderdeel (kort) worden stilgestaan bij het volgende probleem: nogal wat wapens worden via moderne technologie digitaal bestuurd (raketten, drones, etc.)[564]. Het is dus niet ondenkbeeldig dat, in navolging van wat hierboven werd gezegd in verband met het hacken van kerncentrales, ook deze wapens gehackt zouden worden. Niet al die wapens mogen echter gebruikt worden (bijvoorbeeld kernwapens), terwijl andere wapens misschien wel gebruikt mogen worden in de ene situatie, maar in de andere (zoals door het veroorzaken van onnodig leed[565]) dan weer niet. Dit onderdeel zal kort stilstaan bij verschillende mogelijkheden, aangezien deze bepalingen van toepassing kunnen zijn bij een mogelijke cyberoorlog. Over het al dan niet bestaande verbod rond kernwapens zal hier niets meer gezegd worden: de reële mogelijkheid en dreiging van een kernwapen dat via een cyberaanval gebruikt wordt, leek een aparte bespreking te verantwoorden.

2. Voorbeelden met conventionele wapens

168. Zoals reeds aangegeven in de voorgaande afdeling, worden wapens verboden naargelang zij geen onderscheid kunnen maken tussen burgers en strijders, of indien zij onnodig of buitensporig leed veroorzaken[566]. Het zal dus sowieso verboden zijn om een cyberaanval uit te voeren die als doel heeft een dergelijk wapen te controleren en in te zetten. Het louter aanvallen om een dergelijk wapen te controleren, hoeft echter niet per se verboden te zijn[567]: vaak is het niet de aard van het wapen, maar de wijze waarop het gebruikt wordt die het verbod doen intreden[568]. Sommige wapens kunnen door hun aard echter niet door een cyberaanval gecontroleerd worden, aangezien

[563] KADELBACH, "Nuclear Weapons and Warfare", nr. 29.
[564] NASU, MCLAUGHLIN, 71.
[565] Zie nr. 158 e.v.
[566] DINTEIN, "Warfare, Methods and Means", nr. 2.
[567] NASU, MCLAUGHLIN, 71.
[568] DINSTEIN, "Warfare, Methods and Means", nr. 2.

het loutere bezit van een dergelijk wapen misschien niet verboden is, maar in elk geval sterk afgekeurd wordt[569].

169. Een eerste voorbeeld dat hier wordt aangehaald, is de problematiek rond chemische wapens. Het is niet ondenkbeeldig dat, als een kerncentrale via een cyberaanval overgenomen kan worden, dat ook chemische wapens op afstand kunnen overgenomen en gelanceerd of ingezet worden[570]. Er zijn reeds meerdere aanvallen met chemische wapens voorgekomen, zowel van statelijke actoren[571] als van niet-statelijke actoren (terroristen)[572]. Aangezien de eerste aanvallen met chemische wapens al sedert de 19de eeuw voorkomen[573], is er een uitgebreide regelgeving rond chemische wapens. De vraag stelt zich nu of die eenvoudig met cyberaanvallen verzoend kunnen worden.

170. Er is weinig discussie mogelijk dat chemische wapens onnodig leed kunnen toebrengen en door hun eigen karakter geen onderscheid *kunnen* maken tussen burgers en strijders[574]. Een cyberaanval die de controle verschaft over een chemisch wapen, zou op de aanvallende staat dus de last leggen om dit wapen enkel te gebruiken indien dit geen burgers kan treffen en geen onnodig leed veroorzaakt[575]. Indien dit wapen echter iets anders zou doen dan verdoven of tijdelijk verlammen[576], zou deze cyberaanval in principe enkel gebruikt kunnen worden om het chemisch wapen buiten de controle van de vijandelijke staat te stellen: het Gifgasprotocol van 17 juni 1925 verbiedt immers het gebruik van dergelijke wapens, net zoals het internationaal gewoon-

[569] Bijvoorbeeld chemische wapens, waar inspanningen zijn gedaan om dit soort wapens te bannen: T. MARAUHN, "Chemical Weapons and Warfare", *MPEPIL*, OPIL, juni 2010, opil.ouplaw.com, nr. 36 (hierna: MARAUHN, "Chemical Weapons and Warfare").
[570] MARAUHN, "Chemical Weapons and Warfare", nr. 15: in sommige wapens worden chemische elementen gescheiden gehouden tot aan het punt van impact, waarna zij gemengd worden en vrijkomen. Het is niet onredelijk om aan te nemen dat deze wapens op afstand bestuurde raketten kunnen zijn, die dus overgenomen kunnen worden.
[571] Het gebruik van chemische wapens tijdens de burgeroorlog in Syrië, vermoedelijk in opdracht van het overheidsregime: A. DEUTSCH, "Exclusive: Chemical Weapons used by fighters in Syria – sources", *Reuters*, 6 november 2015, reuters.com.
[572] De aanval van de sekte Aum Shinrikyo in maart 1995 in Japan: MARAUHN, "Chemical Weapons and Warfare", nr. 12.
[573] Toen de Engelse troepen artillerieprojectielen in zuur doopten tijdens de Boerenopstand in Zuid-Afrika: MARAUHN, "Chemical Weapons and Warfare", nr. 6.
[574] MARAUHN, "Chemical Weapons and Warfare", nr. 23.
[575] Opnieuw kan de hypothese gemaakt worden van een chemisch wapen dat in een afgelegen woestijn tegen een militair konvooi wordt gebruikt, zie nr. 161.
[576] Wat gebruikt wordt in ordehandhavingsoperaties: traangas, gas dat gebruikt wordt om mensen tijdelijk in te laten slapen e.d.: MARAUHN, "Chemical Weapons and Warfare", nr. 13. Dit zou door de Russische ordediensten gebruikt zijn in 2002, toen ze een theater in Moscow bestormden na een gijzeling van Tsjetsjeense rebellen: P.M. WAX, C.E. BECKER, S.C. CURRY, "Unexpected 'gas' casualties in Moscow: a medical toxicology perspective", *Annals of Emergency Medicine*, 2003, vol. 41 nr. 5, 700 e.v.

terecht dit doet[577]. Recent komt de controle/het bezit van chemische wapens ook onder vuur: het CWC (Chemical Weapons Convention[578]) verbiedt immers, zoals de naam aanduidt, het bezit van chemische wapens.

171. Waar het gifgasprotocol nog de zogenaamde reservaties voor wederkerigheid kende, is dit niet het geval voor het CWC[579]. Deze reservaties betekenen dat, indien een staat het protocol heeft ondertekend, aangevallen wordt met een chemisch wapen, die ondertekenende staat toch chemische wapens ter verdediging mag inzetten[580]. Daarentegen is het Gifgasprotocol te beschouwen als internationaal gewoonterecht, waardoor het ook staten bindt die geen lid zijn, terwijl dit misschien nog niet het geval is voor het CWC, aangezien dit (vrij) recent is[581]. Aangezien er momenteel 192 lidstaten zijn voor het CWC[582], moet deze stelling in de rechtsleer misschien aangepast worden. Omdat bijna alle staten ter wereld lid zijn, en het CWC bepaalt dat de vernietiging van *alle* chemische wapens voltooid moet zijn 10 jaar na het inwerkingtreden van het verdrag (mogelijk te verlengen tot 15 jaar)[583], zouden alle chemische wapens al vernietigd moeten geweest zijn in 2012. Het louter controleren van een chemisch wapen via een cyberaanval is dus een schending van het internationaal recht.

172. Wat hierboven voor chemische wapens werd uiteengezet, geldt ook voor biologische wapens. Ook deze wapens werken door hun aard zonder onderscheid en kunnen vanop afstand bestuurd worden[584], waardoor ze kwetsbaar zijn voor een cyberaanval. Ook deze wapens mogen niet gebruikt worden ingevolge het Gifgasprotocol, maar ook het bezit is tegenwoordig verboden ingevolge het BWC[585]. Hiervan zijn echter maar 174 staten lid[586], hoewel het BWC als internationaal gewoonterecht wordt

[577] MARAUHN, "Chemical Weapons and Warfare", nr. 22; HENCKAERTS, DOSWALD-BECK, 27.
[578] Verdrag betreffende het verbod op de ontwikkeling, productie, bewaring en het gebruik van chemische wapens en betreffende hun vernietiging van 13 januari 1993, New York/Parijs, *UNTS* 317 (hierna: CWC).
[579] M. BOTHE, N. RONZITTI, A. ROSAS (*eds*.), *The New Chemical Weapons Convention: Implementation and Prospects*, Martinus Nijhoff Publishers, Leiden, 1998, 454 (hierna: BOTHE, RONZITTI, ROSAS).
[580] MARAUHN, "Chemical Weapons and Warfare", nr. 20.
[581] BOTHE, RONZITTI, ROSAS, 454.
[582] Volgens de Organisatie betreffende het Verbod op Chemische Wapens, opcw.org.
[583] CWC, Bijlage betreffende vernietiging en verificatie, bijlage IV, p. 87; het verdrag trad in 1997 in werking, UNODA, un.org.
[584] D. SVARC, "Biological Weapons and Warfare", *MPEPIL*, OPIL, augustus 2015, opil.ouplaw.com (hierna: SVARC, "Biological Weapons and Warfare").
[585] Verdrag betreffende het verbod op de ontwikkeling, productie en bewaring van biologische en toxische wapens en betreffende hun vernietiging van 26 maart 1975, London/Moscow/Washington D.C., *UNTS* 163.
[586] UNODA, un.org.

gezien[587]. Het BWC bepaalt echter geen uiterste datum voor het vernietigen van biologische wapens. Het via een cyberaanval controleren van een eventueel biologisch wapen is dus ook verboden.

173. Behalve deze massavernietigingswapens[588], worden ook enkele conventionele wapens verboden. Enkele daarvan kunnen via een cyberaanval ingezet worden (opnieuw door het hacken van de installatie). Om te weten of een bepaald wapen (onder invloed van een cyberaanval) gebruikt mag worden, moeten de hierboven beschreven principes van onderscheid en het verbod op het toebrengen van onnodig leed in het achterhoofd gehouden worden[589]. Voor wat betreft het principe van onderscheid is dit eenvoudig: een cyberaanval die een conventioneel wapen bemachtigt, laat de aanvallende staat enkel toe dit te gebruiken tegen een militair doelwit. Zoals reeds eerder vermeld, ligt het verbod op het veroorzaken van onnodig leed moeilijker. Volgens DINSTEIN is het kerncriterium te weten of het gebruikte wapen noodzakelijk was om een legitiem militair doel te bereiken (in navolging van de *Nuclear Weapons-opinion*)[590].

174. Bepaalde beperkingen spelen ook een belang in het kader van cyberoorlogen. Zo is er een beperking op het gebruik van ontvlambare munitie, aangezien dit niet gebruikt mag worden tegen militaire doelen die in gebieden met een hoge concentratie aan burgers liggen[591]. Het is dan aan de staat die een wapen overneemt via een cyberaanval, om die bepalingen te eerbiedigen. Het is echter niet altijd eenvoudig te weten welke bepalingen men moet voldoen: zo zal een staat die een drone hackt, moeten nagaan welke wapens deze drone vervoert, vooraleer die drone ingezet kan worden[592]. Er zal, buiten het geval van massavernietigingswapens, dus steeds geval per geval moeten nagegaan worden of het wapen, dat door een cyberaanval wordt overgenomen, gebruikt mag worden en in welke omstandigheden.

[587] N.A. SIMS, *The Future of Biological Disarmament: Strengthening the Treaty Ban on Weapons*, Routledge, New York, 2009, 43; HENCKAERTS, DOSWALD-BECK, 27.
[588] SVARC, "Biological Weapons and Warfare", nr. 1.
[589] DINSTEIN, "Warfare, Methods and Means", nr. 3-5.
[590] DINSTEIN, "Warfare, Methods and Means", nr. 4.
[591] Protocol betreffende het verbod of de beperking op het gebruik van ontvlambare wapens bij Verdrag betreffende het verbod op bepaalde wapens.
[592] BOOTHBY, 73.

3. Kan een cyberwapen zelf een verboden wapen uitmaken?

175. Wat hierboven werd uiteengezet, heeft op zich niets met cyberoorlog te maken, maar meer met de gevolgen van een cyberaanval, waar ook aan gedacht moet worden. De vraag is echter of een cyberwapen (gelet op de aanname dat "cyberwapens" bestaan) ook eventueel verboden of beperkt wordt[593]. Net zoals bij alle wapens, zullen de principes van onderscheid, het verbod op onnodig leed en (algemeen) de principes van het internationaal humanitair recht gelden. Het zal echter misschien moeilijker zijn om deze toe te passen op cyberwapens, daar er sprake is van *dual-use* doelwitten: doelwitten die op zich een militair karakter kunnen hebben, maar door hun verbondenheid in de cyberspace ook een burgerlijk karakter kennen[594]. Art. 36 Protocol I bepaalt expliciet dat, bij de ontwikkeling van nieuwe wapens, nagegaan moet worden of die soms of altijd verboden moeten worden. Hier wordt een poging daartoe ondernomen.

176. Cyberwapens moeten ook een onderscheid maken tussen burger(doelwitten) en strijders (of militaire doelwitten, zoals servers van het leger), mogen geen onnodig leed veroorzaken en mogen geen andere bepalingen van het internationaal recht schenden[595]. Er is echter niet vereist dat staten alle mogelijke vormen van gebruik van een wapen analyseren: enkel het redelijk voorzienbaar gebruik mag de internationaalrechtelijke bepalingen niet schenden[596]. Dit kan een probleem vormen voor wat betreft cyberwapens: door de grote verbondenheid en het technisch karakter van cyberspace, zal de bevelhebber die groen licht geeft voor de cyberaanval moeten steunen op analyses van technici, die zelf ook niet alle mogelijke gevolgen kunnen voorzien[597]. Er zal dus een meer nauwkeurige analyse nodig zijn in het geval van cyberwapens. Het bezit van deze wapens is niet noodzakelijk verboden, indien zij internationaalrechtelijke bepalingen schenden, enkel het gebruik ervan mag niet[598].

[593] Zie onder meer DINNISS, 258-260.
[594] SCHIMTT, 156.
[595] *Commentary*, 423.
[596] *Commentary*, 424.
[597] BOOTHBY, 68-69.
[598] *Commentary*, 424.

177. Als 'wapen' worden cyberwapens gereguleerd door verdragen en door gewoonterecht[599]. Een principe dat in beide wordt teruggevonden en in deze masterproef al enkele keren werd vermeld, is het verbod op het toebrengen van onnodig leed. De vraag is echter of een cyberwapen onnodig leed kan veroorzaken. Een cyberwapen heeft immers steeds een vooraf vastgesteld doel, en de specifieke programmering van een code heeft een specifieke functie[600]. Zoals hierboven gezegd, moet een wapen berekend zijn op het toebrengen van onnodig leed, om als een verboden wapen gekwalificeerd te worden[601]. Indien een cyberwapen dus niet geprogrammeerd is om onnodig leed toe te brengen, zouden deze wapens buiten het verbod vallen. Het lijkt dan logischer om BOOTHBY te volgen, die stelt dat voor cyberwapens naar de gevolgen van hun gebruik moet worden gekeken[602].

178. Een belangrijker probleem bij cyberwapens is het onderscheid tussen burgers en militaire doelwitten. Computervirussen die zich willekeurig verspreiden in een netwerk van het leger, kunnen zich echter ook verspreiden naar particuliere netwerken en daar schade veroorzaken. Dergelijke wapens zouden dus verboden kunnen zijn. Er moet echter rekening gehouden worden dat een zekere mate van *collateral damage* toegelaten is. Ingevolge art. 51(5) en 57(2) Protocol I mag een aanval schade aan burgers of aan private eigendom veroorzaken, indien die proportioneel blijft. De vraag is echter welke schade precies in aanmerking moet worden genomen om de graad van *collateral damage* te berekenen. Volgens de *Tallinn-manual* moeten directe en indirecte gevolgen bekeken worden, voor zover deze laatste voorzienbaar waren. Een voorbeeld geeft dit duidelijker weer: indien het GPS-net aangevallen zou worden, zullen de directe effecten zijn dat voertuigen hun navigatie verliezen, waardoor daarnaast ongevallen veroorzaakt kunnen worden. De aanval op het GPS-net kan ook verschillende systemen beschadigen, zoals GPS-toestellen of andere navigatiemachines. Deze voorzienbare indirecte effecten zijn *collateral damage*. Indien de aanval echter op onvoorzienbare wijze andere systemen, die niet met het GPS-net zijn verbonden, zou infecteren, ziet de *Tallinn-manual* dit niet als bijkomende schade[603].

[599] BOOTHBY, 68.
[600] *Ibid.*
[601] Zie nr. 159.
[602] BOOTHBY, 68.
[603] *Tallinn-manual*, 133.

179. Het grootste probleem voor het principe van onderscheid zijn echter de *dual*[604]*-use* toepassingen. Ingevolge art. 27 van Den Haag 1907 mogen burgerlijke voorwerpen die voor militaire doelwitten gebruikt worden, aangevallen worden. Voor sommige objecten vormt dit geen probleem, maar andere objecten worden slechts indirect voor militaire doeleinden gebruikt. Ook kan een burgerlijk object slechts voor een beperkte tijd voor militaire doelwitten worden gebruikt. Indien het burgerlijk object dan zijn militair karakter verliest, herkrijgt het de bescherming van het internationaal humanitair recht[605]. Volgens de *Tallinn-manual* verliest een burgerlijk object (meestal een netwerk) zijn bescherming indien het redelijkerwijs mogelijk is dat het een militair gebruik heeft (vergelijk het met wegen: een staat hoeft niet te weten langs waar een militair konvooi reist, maar het is redelijk om aan te nemen dat die weg gebruikt kan worden. Die weg vormt dan een doelwit[606]). Aangezien netwerken bijna altijd voor militaire doeleinden gebruikt kunnen worden, zou het gehele internet een doelwit kunnen vormen. Er zal echter steeds naar gestreefd worden om de schade voor burgers tot een minimum te beperken[607].

4. Conclusie

180. Cyberoorlog zal ook geregeld worden door het recht op het gebruik van bepaalde wapens. Dit zal onrechtstreeks het geval zijn, wanneer een cyberaanval bepaalde wapens vanop afstand kan overnemen, maar ook rechtstreeks, wanneer een cyberoperatie op zich een wapen uitmaakt. Hoe het ook zij, dezelfde principes blijven steeds zonder grote problemen van toepassing. Elk wapen zal geen onnodig leed mogen veroorzaken, en elk wapen moet een onderscheid maken tussen burgers en strijders. Enkel in het geval van cyberwapens ligt dit laatste wat moeilijker, ingevolge de leer van *dual-use* objecten. Aangezien Protocol I staten verplicht om de schade aan burgers en burgerlijke objecten zo miniem mogelijk te houden, wordt dit probleem echter enigszins verzacht, zonder dat het volledig uit de wereld is geholpen. Door de unieke verbondenheid in cyberspace, lijkt hier echter niet zoveel aan te doen: een verdrag dat *dual-use* doelwitten in cyberspace zou verbieden, zou ingaan tegen een regel die al sinds de Haagse Vredesconferentie van 1907 bestaat.

[604] DINNISS, 208-209.
[605] *Tallinn-manual*, 108.
[606] *Tallinn-manual*, 114.
[607] Art. 57(1) Protocol I, *Tallinn-manual*, 52.

E. Bescherming van bepaalde groepen personen en objecten

1. Waarom worden bepaalde personen en objecten beschermd

181. Het internationaal humanitair recht heeft als een van zijn essentiële kenmerken de bescherming van bepaalde groepen van personen (burgers, krijgsgevangenen etc.) en bepaalde objecten (cultureel eigendom, private eigendom etc.)[608]. De bescherming van burgers werd door de Verdragen van Geneve als essentieel gezien[609], terwijl het ook de bescherming van het cultureel erfgoed van de mensheid als een noodzakelijke toevoeging aan het internationaal humanitair recht zag[610]. Deze bescherming focust zich echter op conventionele oorlogen. De vraag die zich nu stelt is of deze bescherming ook toepasselijk is op cyberoorlogen, en of men de regels dient aan te passen of uit te breiden om hetzelfde niveau van bescherming te bieden in deze nieuwe cybercontext.

182. Opnieuw zal de vraag zich stellen naar de gevolgen van een cyberaanval. Moeten burgers beschermd worden tegen digitale gevolgen alleen, of moeten ook de 'kinetische' gevolgen van de aanval in rekening worden gebracht? De *Tallinn-manual* lijkt in elk geval uit te gaan van de tweede stelling[611]. Voor wat betreft de bescherming van objecten moet eerst worden nagegaan of de bescherming zoals voorzien in de Verdragen van Geneve ook geldt voor digitale objecten: kunnen digitale bronnen bijvoorbeeld als cultureel erfgoed gezien worden? Op dit vlak moet deze masterproef gezien worden als een mogelijke oplossing tussen de vele. Over deze problematiek is nog weinig doctrine verschenen, dus zullen eventuele stellingen de loutere (beredeneerde) opinie van de schrijver zijn.

2. Relevantie op het vlak van cyberoorlog

a) Personen

183. Zoals gezegd is dit een van de meest essentiële bepalingen van het internationaal humanitair recht. Dat alleen al rechtvaardigt de bespreking ervan in deze masterproef.

[608] Dit volgt o.a. uit de indeling van deel V van het boek: A. CLAPHAM, P. GAETA, T. HAECK, A. PRIDDY (*eds.*), *The Oxford Handbook of International Law in Armed Conflict*, Oxford University Press, Oxford, 2014, Part V.
[609] *Commentary*, 585-589.
[610] *Commentary*, 640.
[611] *Tallinn-manual*, 97.

Maar ook de prominente plaats in de *Tallinn-manual*[612] geeft aan dat deze oefening niet louter theoretisch is, maar dat cyberaanvallen mogelijks grote effecten op burgers (en andere beschermde personen) kunnen hebben. Deze handleiding (die verwijst naar art. 51(2) Protocol I, art. 13(2) Protocol II en het internationaal gewoonterecht dat geldt voor zowel internationale als niet-internationale gewapende conflicten)[613] geeft ten eerste aan dat burgers niet het doelwit mogen zijn van een cyberaanval. Alle burgers vallen daaronder, voor zover zij niet uitgesloten worden door directe deelname aan de vijandelijkheden[614]. De verboden actie tegen burgers moet wel een bepaalde intensiteit bereiken[615]: art. 49 Protocol I geeft aan dat er van een aanval slechts sprake is bij een militaire actie (dus zowel verdedigende als aanvallende gedragingen) die gebruik van geweld uitmaakt. Deze masterproef heeft reeds meerdere keren gesteld dat er, in de cybercontext, een zekere drempel overschreden moet worden om van gebruik van geweld te kunnen spreken[616]. Er zal dus, zoals eerder werd gesteld, naar de kinetische gevolgen van een aanval gekeken moeten worden.

184. Indien dit tot het uiterste wordt doorgetrokken, zou dit betekenen dat burgers slechts beschermd worden tegen cyberoperaties die de drempel van 'gebruik van geweld' overschrijden[617]. Dit lijkt in strijd met de voorzieningen in de Protocollen van Geneve. Art. 51 is zo uitgebreid, dat het de bedoeling leek om burgers tegen alle mogelijke schadelijke gevolgen van een conflict te beschermen. Art. 51(1) is dan ook ruimer: het geeft aan dat het Protocol burgers wil beschermen tegen *gevaren* die rijzen naar aanleiding van militaire operaties, terwijl art. 51(2) (de dreiging van) terreur tegen burgers verbiedt. Het commentaar bij de Protocollen geeft aan dat het de bedoeling is om burgers tegen elk militair maneuver te beschermen, waardoor het aannemelijk is dat de stelling in de *Tallinn-manual* (dat enkel operaties die een drempel overschrijden van toepassing zijn) te extreem gesteld is en dus bijgesteld moet worden. Het principe van de Martensclausule is immers dat het bestaand internationaal recht *doelgericht* wordt geïnterpreteerd en toegepast[618].

[612] Er wordt een hele sectie aan gewijd: *Tallinn-manual*, 97 e.v.
[613] *Tallinn-manual*, 97.
[614] *Commentary*, 618; zie nr. 89.
[615] *Commentary*, 618, verwijst naar art. 49 voor wat betreft de definitie van 'aanval'.
[616] Nr. 29 e.v.; *Tallinn-manual*, 91 e.v.
[617] Wat ook zo in de *Tallinn-manual* op pagina 97 wordt voorgehouden.
[618] Zie nr. 14.

185. Het is inderdaad een lang gevestigde regel dat burgers niet het doelwit mogen zijn van militaire operaties[619]. Een groter probleem stelt zich echter bij zogenaamde *collateral damage*. Deze problematiek werd al aangehaald in de sectie "D. Verbod op het gebruik van bepaalde wapens", en wordt hier nader onderzocht. Ten eerste sluit dit vanzelfsprekend cyberaanvallen of –operaties uit die van nature geen onderscheid maken of kunnen maken tussen burgers en strijders[620]. Deze regel komt terug in de *Tallinn-manual*[621], maar de handleiding beperkt dit opnieuw tot aanvallen die een bepaalde drempel overschrijden. In dit geval lijkt Protocol I echter de *Tallinn-manual* te volgen: het spreekt enkel van "aanvallen" op burgers[622], niet over elke willekeurige militaire actie, die daarnaast volgens het Protocol zelf ook een bepaalde drempel moeten overschrijden[623]. Dit lijkt logisch, gezien het feit dat er maar van bijkomende schade sprake kan zijn indien er een aanval gebeurt.

186. Indien een cyberaanval wel een onderscheid kan maken, kan er nog steeds sprake zijn van *collateral damage*. Protocol I geeft inderdaad aan dat het niet mogelijk is om burgers in alle gevallen te beschermen: art. 51(5)(b) bepaalt dat enkel aanvallen verboden zijn die *excessieve* schade aan burgers teweeg brengen, in vergelijking met het te behalen militaire voordeel. Voordat een cyberaanval uitgevoerd wordt, moet deze proportionaliteit eerst onderzocht worden: art. 57(2)(a)(iii) en het internationaal gewoonterecht leggen[624] aan de aanvallers een onderzoeksplicht op. Gezien deze proportionaliteitstoets, kan aangenomen worden dat kleine(re) ongemakken die volgen uit een cyberaanval (bijvoorbeeld het tijdelijk onbeschikbaar zijn van websites, kleine of kortstondige storingen in het GPS-net) aanvaardbare *collateral damage* uitmaken[625]. Deze afweging moet *in concreto* gebeuren: de commentaren bij de Protocollen van Geneve geven aan dat bijvoorbeeld de weersomstandigheden (helder zicht of mist) bekeken moeten worden[626].

187. In de cybercontext is dit voorbeeld natuurlijk niet van belang, maar het toont aan dat ook hier geval per geval bestudeerd moet worden. Zo zal een aanval op een net-

[619] Voor zover zij niet deelnemen aan de vijandelijkheden. Over deze problematiek, zie nr. 89.
[620] Art. 51(4); zie nr. 176.
[621] *Tallinn-manual*, 130.
[622] *Commentary*, 619-620.
[623] Art. 49 Protocol I
[624] HENCKAERTS, DOSWALD-BECK, 19-20.
[625] *Tallinn-manual*, 132-133.
[626] *Commentary*, 684.

werk dat naast militair nut ook veel burgerlijke toepassingen kent (zoals het GPS-netwerk) van belang zijn om uit te maken of de incidentele gevolgen excessief zijn. Ook de extreme verbondenheid van de cyberspace zal hier een factor spelen: het valt niet altijd te voorzien dat een aanval op netwerk A gevolgen op netwerk C zal hebben, hoewel die verbonden zijn. Hier wordt vooral gekeken naar de bescherming van personen, maar deze bepalingen gelden ook voor private objecten: zowel schade aan personen als gevolg van *collateral damage* (bijvoorbeeld dodelijke auto-ongevallen als gevolg van een aanval op het GPS-netwerk) als schade aan objecten (zoals ernstige schade aan private computers door toevallige verspreiding van *malware*) komen in aanmerking.

188. Burgers zijn niet de enige personen die beschermd worden door het internationaal humanitair recht. De Verdragen van Geneve en de Protocollen bieden aan heel wat categorieën van personen een bepaald niveau van bescherming: de zieken en gewonden (art. 12 Verdrag van Geneve I), medische eenheden (art. 19 e.v.) en medische transporten (art. 35 e.v.), schipbreukelingen (art. 12 e.v. verdrag van Geneve II) en krijgsgevangenen (art. 4 verdrag van Geneve III). Hoewel deze bepalingen zich eerder focussen op het fysieke welzijn en de fysieke bescherming van deze groepen van personen[627], heeft de moderne technologie ervoor gezorgd dat deze bepalingen ook op cybertoepassingen van toepassing kunnen zijn. Indien zieken en gewonden verzorgd moeten worden, zal het dus verboden zijn om via een cybertoepassing medische apparatuur buiten werking te stellen; als hospitaalschepen onschendbaar zijn, dan zal een cyberaanval op de navigatiesystemen van dat schip niet toegelaten zijn. Er valt dus te beargumenteren dat de beschermde personen die hier werden opgelijst, ook beschermd worden tegen cybertoepassingen, voor zover die cybertoepassingen een gevolg zouden kunnen hebben dat neerkomt op een handeling waartegen het internationaal humanitair recht beschermt[628]. Dit volgt opnieuw logischerwijs uit het feit dat, ingevolge de Martensclausule, het internationaal recht doelgericht geïnterpreteerd moet worden[629].

[627] Vb. art. 12 Verdrag van Geneve 1 focust zich op de humane behandeling van gewonden en zieken, zie ook het nieuwe commentaar van 2016: icrc.org; art. 12 Verdrag van Geneve II bepaalt de principiële onschendbaarheid van hospitaalschepen, zelfs indien er geen gewonden aan boord liggen, zie ook het commentaar van 1960 bij deze bepaling: icrc.org; art. 12(1) Verdrag van Geneve III bepaalt dat krijgsgevangenen met respect behandeld moeten worden.
[628] Dit zullen vooral de kinetische gevolgen zijn van een aanval (vb. op medische apparatuur), maar ook de gewone, 'digitale' gevolgen (vb. de aanval op de navigatie van een hospitaalschip).
[629] Zie nr. 14.

b) Objecten

189. Niet alleen personen, maar ook bepaalde objecten worden (zoveel mogelijk) beschermd tegen de gevolgen van gewapende conflicten. Art. 52(1) Protocol I[630] bepaalt dat burgerlijke objecten niet als doelwit mogen dienen, met de uitzondering dat zij wel aangevallen mogen worden voor zover die objecten voor een militair doel worden gebruikt en dat de aanval erop een duidelijk militair voordeel zou behalen[631]. Dit geldt zowel voor internationale als voor niet-internationale gewapende conflicten en wordt als gewoonterecht aanzien[632]. Art. 52(1) spreekt van aanvallen of represailles, terwijl de *Tallinn-manual* enkel bescherming voorziet in geval een cyberoperatie de drempel van aanval overschrijdt[633]. Opnieuw kan de stelling van de *Tallinn-manual* niet bijgetreden worden. Een doelmatige interpretatie van de verdragsrechtelijke bepalingen in de cybercontext betekent dat ook in deze cybercontext de principiële immuniteit van burgerlijke objecten gegarandeerd moet worden[634]. Vereisen dat burgerlijke doelen enkel beschermd worden tegen operaties die een bepaalde drempel overschrijden, zou heel wat hinderlijke schade in principe toelaten. Bovendien worden sommige burgerlijke objecten altijd beschermd, indien zij onmisbaar zijn voor het overleven van de bevolking (art. 54(2) Protocol I)[635].

190. Net zoals burgers kunnen deelnemen aan de vijandelijkheden, kunnen ook burgerlijke objecten gebruikt worden voor militaire doeleinden (een huis kan als militaire observatiepost gebruikt worden, een netwerk kan gebruikt worden om een virus te verspreiden[636]). Art. 52(2) Protocol I beperkt de bescherming van burgerlijke objecten voor zover die niet *gebruikt* worden voor militaire doeleinden. Dit hoeft niet per se expliciet te zijn: bepaalde burgerlijke objecten kunnen door hun aard een militair nut hebben (de zogenaamde *dual-use*-objecten). Een aanval op dergelijk object zal pas geoorloofd zijn indien het militair voordeel opweegt tegen het verlies voor de burger(s)[637] en indien de objecten ook daadwerkelijk militair gebruikt worden[638]. De *Tal-*

[630] Een bepaling die al teruggaat tot 1868, in de Verklaring betreffende de afkeuring van het gebruik in oorlogstijd van projectielen minder wegend dan 400 gram van 11 december 1868, Sint-Petersburg.
[631] Art. 52(2) Protocol I.
[632] Zie hiervoor de database van het ICRC over het internationaal gewoonterecht, icrc.org.
[633] *Tallinn-manual*, 106.
[634] *Commentary*, 634; ook het internationaal gewoonterecht vergt "bescherming te allen tijde".
[635] DINNISS, 243-244.
[636] *Tallinn-manual*, 109.
[637] *Commentary*, 636.
[638] Volgt uit de redenering die gegeven wordt: *Commentary*, 636.

linn-manual trekt dit bijna letterlijk door voor cyberoperaties[639]. De handleiding argumenteert ook dat de aard van burgerlijke objecten een militair nut kunnen hebben, en dus, indien dit proportioneel is, een gerechtvaardigd militair doel kunnen uitmaken, voor zover die objecten daadwerkelijk gebruikt worden[640].

191. In tijden van oorlog is niet altijd alle informatie beschikbaar en is het dus niet altijd duidelijk of een object burgerlijk dan wel militair van aard is. Indien dit het geval is, legt art. 52(3) de Lidstaten op om die objecten als burgerlijk te zien. Deze bepaling dient om de zogenaamde *shoot first, ask questions later*-mentaliteit wat in te perken[641]. Dit wordt echter niet gevolgd door de *Tallinn-manual*. De handleiding gaat er ook van uit dat onduidelijkheid kan bestaan, maar het argumenteert dat eerder dan een verbod op aanvallen op te leggen, een voorzichtige analyse van het object aangewezen is[642]. De handleiding suggereert dat de onderzoeksplicht voortvloeit uit de bewoordingen van art. 52(3) Protocol I. Het vloeit echter eerder voort uit art. 57 Protocol I, dat aan de strijdkrachten van de Lidstaten de voortdurende verplichting oplegt om zo omzichtig mogelijk op te treden, om schade aan burgers en burgerlijke objecten tot een noodzakelijk minimum te beperken[643]. Dit onderzoek zal niet altijd gemakkelijk zijn, want objecten kunnen bijvoorbeeld tijdelijk voor een militair doel worden gebruikt. Het valt te argumenteren (mede door de opname van de bepalingen van Protocol I) dat dit ook geldt voor cybertoepassingen: ook burgerlijke cybereigendom dient beschermd te worden.

192. Cultureel erfgoed is volgens art. 53 Protocol I een categorie van objecten die een bijzondere bescherming verdient en ondertussen internationaal gewoonterecht is geworden[644]. Inderdaad, zoals de recente ophef rond de vernietiging van de archeologische site van Palmyra door IS duidelijk maakt[645], is cultureel erfgoed een belangrijk symbool dat beschermd moet worden tegen willekeurige en soms opzettelijke aanval-

[639] *Tallinn-manual*, 107.
[640] *Tallinn-manual*, 109.
[641] *Commentary*, 637.
[642] *Tallinn-manual*, 115.
[643] *Commentary*, 638.
[644] HENCKAERTS, DOSWALD-BECK, 22.
[645] I. DE ZWAAN, "VN bevestigt: IS heeft kroonjuweel van Palmyra vernield", *De Morgen*, 31 augustus 2008, demorgen.be.

len[646]. De recente verontwaardiging rond Palmyra[647] rechtvaardigt een korte uitwijding over de volgende problematiek: vallen de bepalingen rond de bescherming van cultureel erfgoed toe te passen op cybertoepassingen, en is daar überhaupt nood aan?

193. Het eerste wat onderzocht moet worden, is of er van cultureel erfgoed sprake kan zijn in het cyberdomein. Art. 1 van het Verdrag van Den Haag van 1954[648] definieert cultureel erfgoed als volgt:

> *[…] (a) movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art or history, whether religious or secular, archeological sites, groups of buildings which, as a whole, are of historic or artistic interest, works of art, manuscripts, books and other objects of artistic, historical or archeological interest, as well as scientific and important collections of books or archives or of reproductions of the property defined above;*
> *(b)[…];*
> *(c) centers containing a large amount of cultural property as defined in sub-paragraphs (a) and (b), to be known as 'centers containing monuments'.*

Art. 53 Protocol I beschermt ook cultureel erfgoed, maar verwijst naar de bovenstaande definitie om dit cultureel erfgoed af te bakenen[649] en verwijst in het artikel zelf naar het Verdrag van Den Haag van 1954, zonder afbreuk hieraan te doen. Er valt dus aan te nemen dat dit verdrag voorrang neemt voor zover het meer bescherming biedt dan Protocol I, aangezien het als *lex specialis* wordt beschouwd.

194. Uit bovenstaande definitie valt af te leiden dat de bescherming van cultureel erfgoed ook voor cybertoepassingen geldt. Zo zou een cyberaanval op de gasleidingen

[646] Hierbij kan verwezen worden naar de doelmatige vernietiging van de Joodse cultuur (en dus cultureel erfgoed) tijdens de Tweede Wereldoorlog: N.N., "Book Burning", *United States Holocaust Memorial Museum*, ushmm.org, geraadpleegd op 27 april 2016.
[647] Zie ook: N.N., "Syria: UNESCO chief condemns destruction of Palmyra's ancient temple", *UN News Centre*, 24 augustus 2015, un.org.
[648] Verdrag betreffende de bescherming van culturele eigendom tijdens gewapende conflicten van 14 mei 1954, Den Haag, *UNTS* 215.
[649] *Commentary*, 642.

van het Louvre[650] een enorme ontploffing kunnen veroorzaken, met enorm verlies aan cultureel erfgoed als gevolg. Ook de vermelding van de bescherming van cultureel erfgoed in de *Tallinn-manual* geeft aan dat deze bescherming ook van toepassing is bij cyberoorlogen[651]. Een interessantere vraag is of digitale data (documenten, films etc.) zelf cultureel erfgoed kunnen uitmaken en dus beschermd worden tegen computeraanvallen. Deze masterproef meent van wel. De bovenstaande definitie beschermt reproducties van bestaand cultureel erfgoed, naast centra waar dit erfgoed op grote schaal verzameld wordt. Indien nu een bepaalde online databank (bijvoorbeeld van UNESCO) een archief van grondplannen van bedreigde archeologische sites zou aanmaken (bijvorrbeeld naar aanleiding van de vernielingen aangericht door IS in Palmyra), lijkt dit onder de definitie te vallen[652]. Deze databank, die enkel in de digitale wereld terug te vinden is, kan dus beschermd worden. Andere gevallen zullen aan de definitie getoetst moeten worden. Zo zal een manuscript van een boek, dat enkel op een laptop terug te vinden is, misschien geen cultureel erfgoed uitmaken, indien het niet 'van groot belang voor het cultureel erfgoed van de mensheid' is, terwijl de aard van digitale date (onder andere de mogelijkheid tot back-ups) kunnen zorgen dat een aanval op een stuk cultureel erfgoed hersteld kan worden, waardoor geen ernstige schending van het recht der gewapende conflicten ontstaat[653].

195. Cultureel erfgoed mag dus niet aangevallen worden ingevolge art. 53(a) Protocol I en art. 2-4 Verdrag van Den Haag 1954. Art. 53(b) bepaalt vervolgens dat cultureel erfgoed ook niet gebruikt mag worden voor militaire doeleinden (zoals het opstellen van een observatiepost in een kerk[654]). Dit lijkt op het eerste zicht niet toepasselijk te zijn in een cybercontext, maar een simpel voorbeeld kan het tegendeel bewijzen. In hierboven beschreven voorbeeld van een online databank, zou een staat die databank kunnen aanvallen en er een virus inplanten, waardoor elke bezoeker dit virus automatisch binnenhaalt[655]. Dit virus zou dan gebruikt kunnen worden op grootschalige

[650] Dit valt onder (c) van de definitie: een centrum dat een grote verzameling aan cultureel erfgoed bevat.
[651] *Tallinn-manual*, 118.
[652] Het is een centrum waar een groot deel van het cultureel erfgoed terug te vinden is, via reproducties van erfgoed dat van groot belang is voor het cultureel erfgoed van de mensheid.
[653] DINNISS, 235.
[654] *Commentary*, 648.
[655] Dit wordt dan een zogenaamd *Botnet*: N.N., "Botnet", *Radware*, security.radware.com, geraadpleegd op 28 april 2016; GOMBEER, 171-171.

DDoS-aanvallen[656] uit te voeren. Dit is geen loutere speculatie, maar harde realiteit: zo zouden in de eerste 2 maanden van 2016 39 geregistreerde DDoS-aanvallen gepleegd zijn tegen de FOD Kanselarij van de Eerste Minister[657]. Dat dit slechts een kleine inbreuk lijkt, die geenszins de vereiste drempel uit de *Tallinn-manual* bereikt, doet er niet toe: art. 53(b) moet ruim begrepen worden, tot zelfs het louter passief voordeel halen uit beschermd cultureel erfgoed[658].

3. Conclusie

196. De bescherming van bepaalde categorieën van personen en objecten is een van de fundamentele principes van het internationaal humanitair recht. Dit is niet anders voor cyberoorlogen. Via doelgerichte interpretatie van de bestaande regels komt men eenvoudig tot de conclusie dat burgers (voor zover zij niet direct deelnemen aan de vijandelijkheden) beschermd moeten worden tegen elk militair maneuver dat tegen burgers gericht wordt. De stelling van de *Tallinn-manual* dat enkel tegen aanvallen wordt beschermd die een bepaalde drempel overschrijden, lijkt in strijd te zijn met de *ratio* achter de relevante artikelen in Protocol I. Indien burgers niet het doelwit mogen zijn, zal dit wat betreft cyberoperaties ook het geval zijn voor hinderlijke operaties tegen burgers, die niet die drempel bereiken.

197. Burgers moeten zoveel als mogelijk ontzien worden, maar er is altijd kans op *collateral damage*. Dit is niet anders in de cybercontext, waar cyberspace zorgt dat militaire en burgerlijke netwerken sterk verbonden zijn. Dergelijke onbedoelde schade is niet per se onwettig, voor zover die schade niet excessief is. De beoordeling hiervan moet geval per geval bekeken worden. Naast burgers zijn er nog andere categorieën personen die beschermd worden, zoals zieken, krijgsgevangenen, medisch personeel en medisch transport. Deze bepalingen spreken redelijk voor zich, en kunnen eenvoudig zo geïnterpreteerd worden dat zij op (de nu voorzienbare gevolgen van) cyberoorlog van toepassing zijn.

[656] Distributed Denial of Service-aanval, waarbij een site gelijktijdig door een groot aantal besmette computers wordt bezocht, waardoor de site crasht: J. MARKOFF, "Distributed Denial of Service", *The New York Times*, 1 april 2013, nytimes.com; zie ook DINNISS, Appendix 2.
[657] Schriftelijke vragen en antwoorden, *Parl.St.* Kamer, 2015-2016, vraag nr. 116.
[658] *Commentary*, 648.

198. Naast burgers worden ook burgerlijke objecten beschermd. Deze objecten mogen niet het doelwit vormen van een aanval, en moeten in principe immuun zijn voor de gevolgen van een conflict. De stelling van de *Tallinn-manual* dat die immuniteit enkel geldt voor aanvallen die een bepaalde drempel overschrijden, lijkt opnieuw strijdig met de bedoeling van deze regels. Indien echter burgerlijke objecten gebruikt worden voor oorlogsdoeleinden, mogen zij wel aangevallen worden. Om deze aanval legaal te laten verlopen, zal echter bij geval van twijfel eerst een onderzoek moeten gebeuren, waarna een aanval pas kan worden ingezet als het militair voordeel voldoende opweegt tegen de eventuele schade aan het burgerlijk object. Dit is ook van toepassing op cyberaanvallen: ook hier zal een onderzoek moeten plaatsvinden bij geval van twijfel, zal de proportionaliteit in acht moeten worden genomen en zullen burgerlijke digitale objecten (databanken etc.) beschermd worden, terwijl burgerlijke fysieke objecten beschermd zijn tegen (de gevolgen van) cyberaanvallen.

199. Een onorthodox maar interessant vraagstuk betreft de bescherming van cultureel erfgoed in geval van cyberoorlog. Dat via een cyberaanval 'kinetische' effecten veroorzaakt kunnen worden die cultureel erfgoed kan aantasten, staat vast. Dit is dan ook verboden, zowel door Protocol I als door het Verdrag van Den Haag 1954. Een moeilijker debat is de vraag of digitale objecten cultureel eigendom kunnen uitmaken. Dat zal aan de hand van de definitie van het vermeld Verdrag van Den Haag 1954 moeten getoetst worden, maar deze masterproef gaat uit van wel (en geeft een voorbeeld daarvan). Ook dit digitaal erfgoed zal dus beschermd worden tegen aanvallen, zal niet gebruikt mogen worden voor militaire doeleinden en zal beschermd zijn tegen represailles, allemaal via doelgerichte interpretatie. Een specifiek verdrag lijkt dus niet nodig.

VI. MENSENRECHTEN

A. Mensenrechten en IHL

200. Met betrekking tot spionage werd al aangegeven dat ook mensenrechten regulerend optreden in de cybercontext. Dit laatste hoofdstuk zal echter dieper ingaan op de algemene mensenrechtelijke principes die spelen in de cybercontext, en dan voornamelijk in tijden van gewapend conflict. Mensenrechten en Internationaal Humanitair

recht kennen echter een bijzondere verhouding, die eerst kort toegelicht zal worden. Eerst en vooral moet worden opgemerkt dat men vaak IHL als de *lex specialis* ziet ten opzichte van mensenrechten. Er is echter minder sprake van prioriteit van de ene rechtstak op de andere, dan wel van een samenwerking van beide, waarmee beoogd wordt om, via de gelijktijdige toepassing van beide sets van regels lacunes op te vullen en de bescherming te optimaliseren[659].

201. Pas sinds 1968 werden mensenrechten en internationaal humanitair recht als wederzijds verbonden rechtstakken gezien, in plaats van exclusieve. In de Conferentie van Teheran voor de Mensenrechten[660] werd voor het eerst afstand gedaan van deze exclusiviteitsvisie, terwijl men in plaats daarvan een visie van integratie en samenwerking voorstelde. De oude theorie was vooral gebaseerd op historische argumenten: beide stelsels zijn uit eigen beweegredenen op verschillende tijdstippen ontstaan[661], terwijl men vreesde dat het IHL gepolitiseerd zou worden door invloeden van mensenrechten[662]. Deze theorie werd dus pas aangevallen na de Conferentie van Teheran, die een meer complementaire visie voorstelde. Dit standpunt vertrekt vanuit het idee dat beide rechtstakken een verschillende oorsprong hebben, maar elkaar aanvullen. Zo zullen de mensenrechten lacunes in het IHL opvangen[663]. Dit lijkt niet onlogisch, aangezien dezelfde bezorgdheden van de mensenrechten het ontstaan van het IHL (mee) hebben beïnvloed[664].

202. De meest inclusieve visie gaat ervan uit dat mensenrechten en IHL tot een gemeenschappelijke rechtstak behoren. Sommige auteurs menen dat IHL een subdivisie is van de mensenrechten, terwijl andere auteurs beide domeinen op gelijke voet plaatsen, waarbij beide rechtstakken gecombineerd worden[665]. In elk geval gaat men in deze visie uit van het standpunt dat beide rechtsgebieden ontstaan zijn uit dezelfde be-

[659] R. KOLB, "Human Rights and Humanitarian Law", *MPEPIL*, OPIL, Maart 2013, opil.ouplaw.com (hierna: KOLB, "Human Rights and Humanitarian Law").
[660] *Resolutie XXIII van de Conferentie van Teheran voor de Mensenrechten van 12 mei 1968,* Teheran, icrc.org.
[661] R. KOLB, "The relationship between international humanitarian law and human rights law: A brief history of the 1948 Universal Declaration of Human Rights and the 1949 Geneva Conventions", *International Review of the Red Cross*, 1998, nr. 400, icrc.org.
[662] KOLB, "Human Rights and Humanitarian Law", nr. 28.
[663] Zoals in deze Masterproef al is gebeurd, met betrekking tot spionage.
[664] N. QUÉNIVET, "The History of the Relationship between International Humanitarian Law and Human Rights Law" in ARNOLD, QUÉNIVET, 9-10 (hierna: QUÉNIVET, "The History of the Relationship between International Humanitarian Law and Human Rights Law").
[665] KOLB, "Human Rights and Humanitarian Law", nr. 30.

hoefte om het menselijk leven en waardigheid te beschermen[666]. Deze discussie is echter van minder belang van deze masterproef. Hier zal enkel bestudeerd worden hoe mensenrechten van toepassing kunnen zijn op cyberoorlogen, wars van het feit of dit nu gebeurt op complementaire basis met het IHL, dan wel op geïntegreerde basis.

B. Mensenrechten en cyberoorlog

1. Afwijkingen van de bescherming geboden door mensenrechtenverdragen

203. Het internationaal recht geldt altijd, eens het van toepassing is. Een conflict kan door zijn aard niet onder (een deel van) het IHL vallen (bijvoorbeeld niet-internationale gewapende conflicten), maar de bepalingen die van toepassing zijn, gelden onverkort[667]. Eventuele nuances zijn mogelijk (zo is schade aan burgerlijke objecten in principe verboden, maar *collateral damage* is toegelaten voor zover dit proportioneel is)[668], maar de principes in het IHL zijn absoluut[669]. Dit is niet het geval voor wat betreft mensenrechten. Art. 4 van het BUPO-verdrag bepaalt dat van sommige rechten afgeweken mag worden in tijden van nationale noodtoestanden. Die afwijkingen moeten wel proportioneel en noodzakelijk zijn. Art. 15 van het EVRM bepaalt ook dat in nationale noodtoestanden van bepaalde rechten afgeweken mag worden (onder dezelfde voorwaarden als het BUPO-verdrag, hoewel het EVRM oorlog vermeldt als noodtoestand, in tegenstelling tot het BUPO-verdrag[670]). Beide verdragen leggen aan de Lidstaat de plicht op om afwijkingen te melden aan respectievelijk het Secretariaat-Generaal van de Verenigde Naties en het Secretariaat-Generaal van de Raad van Europa.

204. Het louter bestaan van een conflict maakt niet noodzakelijk een nationale noodtoestand uit. Het mensenrechtencomité van de Verenigde Naties argumenteerde expliciet dat er enkel mag afgeweken worden van deze rechten indien het voortbestaan van de staat ervan afhangt[671]. Het Europees Hof voor de Rechten van de Mens heeft in

[666] QUÉNIVET, "The History of the Relationship between International Humanitarian Law and Human Rights Law", 5.
[667] Gemeenschappelijk Art. 1 Verdragen van Geneve vereist dat de Lidstaten de bepalingen 'in elke omstandigheid' eerbiedigen: GASSER, THÜRER, "Humanitarian Law, International", nr. 31.
[668] Zie nr. 197 e.v.
[669] GASSER, THÜRER, "Humanitarian Law, International", nr. 30.
[670] Dit werd opzettelijk gedaan, om de VN niet te associëren met oorlog, zelfs impliciet: BUERGENTHAL, "To Respect and to Ensure: State Obligations and Permissible Derogations", 79.
[671] Comité voor de Mensenrechten van de Verenigde Naties, *General Comment 29*, 31 augustus 2001, *Doc.Nr.* CCPR/C/21/Rev.1/Add.11.

gelijkaardige bewoordingen bepaald dat die noodtoestand van art. 12 EVRM de gehele bevolking moet treffen en een dreiging moet vormen voor het georganiseerde leven van de gemeenschap waaruit de staat bestaat[672]. Naast de vraag of mensenrechtenhoven of –comités wel geschikt zijn om te beslissen of er al dan niet sprake is van een gewapend conflict dat een noodtoestand waarborgt[673], lijkt dit zeer problematisch voor cyberoorlogen. De vijand die de hoofdstad omsingelt, kan het voortbestaan van de natie bedreigen. Een cyberaanval kan dit misschien minder. Er is in de rechtsleer geen voorbeeld beschikbaar van een cyberaanval, op welke schaal ook, dat het voortbestaan van de natie in gevaar zou kunnen brengen. De definitie van het EHRM is dan misschien iets ruimer: er moeten aan 4 voorwaarden voldaan zijn (actuele of nakende noodtoestand, die de hele natie moet treffen, invloed moet hebben op het georganiseerde leven van de gemeenschap en niet opgelost kunnen worden door de normale middelen of restricties die in de artikelen zelf zijn terug te vinden[674]). Een cyberaanval kan zo groot zijn, dat het de gehele bevolking treft en het georganiseerd leven van die gemeenschap in gevaar brengt en zo de gehele natie treffen. Zo zou een grootschalige en langdurige verstoring van het verkeersnet of een aanval op de beurs[675] ernstige gevolgen kunnen hebben voor de samenleving. De vraag is of deze zienswijze van het Hof in 1961 nog toepasbaar is of mag zijn voor wat betreft de (hyper-)moderne context van cyberoorlogen.

205. Naast de algemene bepalingen zoals hierboven beschreven, wordt voor sommige rechten in hetzelfde artikel bepaald dat van die rechten afgeweken kan worden. Een van de belangrijkste (in de zin van toepasselijk in de cybercontext) is het recht op leven. Art. 2(2) EVRM bepaalt dat het leven niet beschermd moet worden indien dit gebeurt om rellen of opstanden aan te pakken. Het gebruik van geweld moet wel wettelijk zijn voorgeschreven, wat volgens het EHRM inhoudt[676] dat het nationaal recht het gebruik van geweld moet voorzien[677], dat recht toegankelijk[678] en voorzienbaar[679]

[672] EHRM, *Lawless v. Ireland*, 1 juli 1961, nr. 332/57, par. 28.
[673] G. OBERLEITNER, *Human Rights in Armed Conflict – Law, Practice, Policy*, Cambridge University press, Cambridge, 2015, 172.
[674] ECRM, *Denmark, Norway, Sweden and the Netherlands v. Greece*, 31 mei 1961, nr. 3321/67, 3322/67, 3323/67, 3324/67, echr.coe.int; BUERGENTHAL, "To Respect and to Ensure: State Obligations and Permissible Derogations", 79-80.
[675] Die door VAN DEN HERIK als kritieke infrastructuur worden omschreven: VAN DEN HERIK, "De digitale oorlog: waan of werkelijkheid", 353.
[676] Zie algemeen A.-L. SVENSSON-MCCARTHY, *The International Law of Human Rights and States of Exception*, Martinus Nijhoff Publishers, Den Haag, 1998, 75-92.
[677] EHRM, *Silver and others v. United Kingdom*, 25 maart 1983, Series A, Nr. 61, p. 33 e.v., par. 86 (hierna: *Silver and others*-case).

moet zijn en geen willekeurigheid mag veroorzaken[680]. Dit kan van toepassing zijn op cyberoorlogen: cyberaanvallen mogen gebruikt worden, zelfs als de kinetische gevolgen daarvan dodelijke slachtoffers maakt, indien dit binnen die context valt. Vreemd genoeg wordt deze afwijking niet vermeld in art. 6 BUPO-verdrag. Art. 4, dat de afwijkingen van mensenrechten toelaat, sluit expliciet uit dat het recht op leven zou worden beperkt, alhoewel dat dit verbod niet zou gelden in tijden van oorlog[681].

206. Voor wat België betreft (volgens het EVRM), wordt dit geregeld door art. 37 Wet Politieambt[682], dat bepaalt dat agenten geweld mogen gebruiken indien dit proportioneel en redelijk gebeurt. Lid 3 van dit artikel bepaalt dat de verplichte waarschuwing achterwege mag worden gelaten als het gebruik van geweld dan onwerkbaar zou worden, wat het geval is voor cybertoepassingen. Art. 11, § 1 Wet Inlichtingen- en Veiligheidsdiensten[683] geeft vervolgens expliciet aan dat de Belgische Autoriteiten zelf cyberaanvallen mag uitvoeren indien dit nodig is[684].

207. Andere mensenrechten kennen ook afwijkingen. Zo kan het recht op vrijheid van meningsuiting worden beperkt (art. 10(2) EVRM), net als het recht op (het vormen van een) vereniging (art. 11(2) EVRM). Aangezien deze bepalingen echter minder relevant zijn in de context van cyberoorlogen, zal er niet verder op worden ingegaan. Wel relevant is de beperking op het recht van privacy (art. 8(2) EVRM en art. 17 *juncto* art. 4 BUPO-verdrag). Zoals onder de hoofding "E. Spionage en Diplomatieke immuniteit" werd vermeld, kan binnenlandse spionage via deze artikelen problematisch worden. Het BUPO-verdrag vereist echter dat het voortbestaan van de natie in gevaar moet zijn, wat een hoge eis stelt om spionage toelaatbaar te maken, terwijl het EVRM de legaliteit en de noodzakelijkheid van de maatregelen vereist. Die noodzakelijkheid houdt in dat een maatregel proportioneel moet zijn voor het beoogde

[678] EHRM, *Sunday Times v. United Kingdom*, 25 maart 1983, Series A, Nr. 30, p. 31 e.v., par. 49 (hierna: *Sunday Times*-case), *Silver and others*-case, par. 87.
[679] *Sunday Times*-case, 31-33.
[680] *Silver and others*-case, 33.
[681] Wat ook enigszins logisch is, aangezien dit moeilijk verenigbaar is met het recht op zelfverdediging van een staat: Y. DINSTEIN, "The Right to Life, Physical Integrity, and Liberty" in HENKIN, 120.
[682] Wet van 5 augustus 1992 op het politieambt, *B.S.* 22 december 1992.
[683] Wet van 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten, *B.S.* 18 december 1992.
[684] Wat er pas in 2010, na een amendement bij de wet van 4 februari 2010, is gekomen: FRANCEUS, 5.

doel[685], wat grootschalige surveillance zoals gepleegd door de NSA niet vanzelfsprekend maakt.

2. Waar houdt IHL op en beginnen de mensenrechten?

208. Los van de hierboven beschreven standpunten over de verhouding tussen Internationaal Humanitair Recht en mensenrechten, zal het ook voor cyberoorlog noodzakelijk zijn om te weten wanneer welk recht toegepast moet worden. De rechtsregels zelf bepalen dat mensenrechten ("fundamentele garanties") gerespecteerd (moeten) worden[686]. Het artikel zou als een residuaire bepaling kunnen gezien worden: de tekst bepaalt expliciet dat iemand die niet specifiek beschermd wordt door het Protocol, toch bescherming geniet via mensenrechten[687]. Protocol II stelt vervolgens de regel voorop dat internationale mensenrechtenverdragen ook gelden voor niet-internationale gewapende conflicten[688]. Voor wat betreft protocol II werd zelfs gesteld dat de Verdragen en Protocollen van Geneve dezelfde doeleinden hebben als de verschillende mensenrechtenverdragen, hoewel het aparte rechtsdomeinen, met 'eigen grondbeginselen en mechanismen'[689]. Dit werd bevestigd door het Internationaal Gerechtshof, dat meent dat mensenrechten en IHL soms exclusief optreden, maar soms ook tegelijk toegepast moeten worden[690]. Dit leunt dus eerder naar de complementariteitsvisie[691].

209. Voor wat betreft niet-internationale gewapende conflicten moeten mensenrechten en IHL in elk geval gelijktijdig worden toegepast. Tot op het moment dat de interne onrust een bepaalde drempel bereikt, is het IHL immers niet van toepassing en kan men enkel terugvallen op mensenrechten[692]. Indien de drempel bereikt wordt en er een conflict in de zin van gemeenschappelijk art. 3 Verdragen van Geneve of in de zin van Protocol II ontstaat, blijven mensenrechten intern ook van toepassing[693]. De *war on terror* wordt ook als een niet-internationaal gewapend conflict gezien, maar dan een conflict waarbij men in het buitenland optreedt. Indien het IHL voor bepaalde za-

[685] M. NOWAK, *Introduction to the International Human Rights Regime*, Martinus Nijhoff Publishers, Leiden, 2003, 59.
[686] Art. 75 Protocol I.
[687] GASSER, THÜRER, "Humanitarian Law, International", nr. 35.
[688] Preambule, 3de lid, Protocol II.
[689] *Commentary*, 1340.
[690] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory-opinion*, par. 106.
[691] Zie nr. 190.
[692] GASSER, THÜRER, "Humanitarian Law, International", nr. 39.
[693] GASSER, THÜRER, "Humanitarian Law, International", nr. 38.

ken hiervoor geen antwoordt biedt, moet dan ook gekeken worden naar de mensenrechten (bijvoorbeeld voor de behandeling van gevangenen of verdachten[694]). Dit zal ook in de context van cyberoorlog gelden: mensenrechten (zoals het recht op privacy) en IHL kunnen simultaan worden toegepast.

3. Conclusie

210. Mensenrechten en internationaal humanitair recht kennen een bijzondere onderlinge verhouding. Tegenwoordig ziet men beide rechtstakken minstens als onderling complementair, zodat het één de lacunes in het ander kan aanvullen. Dit zal ook zo zijn voor cyberconflicten. Er is geen enkel voorbeeld in de gevonden rechtsleer terug te vinden dat aangeeft dat cyberoorlog een ander regime zou moeten volgen dan 'conventionele' conflicten wat betreft de verhouding mensenrechten en IHL. Een bijzonder probleem voor de cybercontext vormt evenwel de derogatiemogelijkheid van bepaalde mensenrechten. Zowel het EVRM als het BUPO-verdrag oordelen dat die derogatie enkel kan indien de noodtoestand het voortbestaan van de staat ervan bedreigt. De rechtsleer heeft ook hierover geen voorbeeld gegeven, waardoor het aannemelijk lijkt dat een loutere cyberoorlog of -aanval slechts moeilijk zal kunnen voldoen aan de vereisten om derogaties mogelijk te maken.

VII. CONCLUSIE

A. Verantwoording van de gekozen thema's

211. Zoals bij de inleiding vermeld, komen hier slechts een aantal thema's van het internationaal verdragsrecht, het internationaal humanitair recht en de mensenrechten aan bod. Het is immers onmogelijk om in de beperkte ruimte van deze masterproef alle verschillende problematieken aan te kaarten. De hierboven behandelde thema's zijn dan ook gekozen omwille van hun actuele waarde[695], omwille van het feit dat de rechtsleer bepaalde thema's als essentieel in hun rechtsdomein beschouwt[696], op aan-

[694] M. SASSOLI, "Guantanamo, Detainees", *MPEPIL*, OPIL, mei 2013, opil.ouplaw.com.
[695] De dertigjarige verjaardag van de kernramp in Tsjernobyl: N.N., "Dertig jaar na de ramp: extreem toerisme boomt in Tsjernobyl", *De Standaard*, 26 april 2016, standaard.be; de afluisterschandalen van de NSA en binnenlandse spionage; de problematiek van terrorisme en cyberterrorisme: D. CHAZAN, H. SAMUEL, R. MULHOLLAND, C. TURNER, "Brussels attacks: Nuclear breach fears as two more charged with terror offences", *The Telegraph*, 27 maart 2016, telegraph.co.uk.
[696] Het gebruik van bepaalde wapens, de bescherming van burgers en objecten: GASSER, THÜRER, "Humanitarian Law, International", nr. 32.

geven van enkele experts[697], of omwille van de natuurlijke verbondenheid van het ene thema met het andere[698]. De indeling is dus niet op duidelijke, logische criteria gestoeld, maar dat dan ook onmogelijk: de rechtsleer betreffende cyberoorlogen behandelt slechts een fractie van alle mogelijke problemen ter zake, dus moeten er keuzes gemaakt worden die op andere gronden dan de rechtsleer steunen.

B. De Martensclausule: de relevantie voor cyberoorlog

212. Deze masterproef bestudeerde cyberoorlog aan de hand van de bestaande principes van het internationaal recht. Deze principes werden dus uitvoerig beschreven, zonder dat er altijd sprake was van een cybercontext, behalve in de conclusie. Dit is logisch, gelet op de gebruikte techniek: de Martensclausule laat immers toe om het bestaande recht te interpreteren op nieuwe ontwikkelingen. Daarom is het vanzelfsprekend nodig om het bestaande recht te onderzoeken. Deze masterproef is tot de slotsom gekomen dat de Martensclausule nog altijd gebruikt kan worden. Cyberoorlog lijkt op het eerste zicht grote verschillen te kennen met conventionele oorlog, maar via doelgerichte interpretatie kunnen de meeste problemen opgelost worden. Deze thesis komt dus tot de conclusie dat het internationaal recht voldoende is aangepast om het grootste deel van de problemen rond cyberoorlog aan te pakken.

C. Een cyberverdrag: is het nodig?

213. De centrale vraag bij deze masterproef is of het algemeen internationaal recht, zoals hierboven thematisch bestudeerd, via interpretatie op cyberoorlogen van toepassing kan zijn. Hierboven werd al opgemerkt dat de Martensclausule nuttig is om regelgeving op de cybercontext toe te passen. Niet alle problemen kunnen echter opgelost worden. Deze thesis heeft voor wat betreft elk thema steeds geconcludeerd of er problemen zijn bij de interpretatie of niet. Voor een gedetailleerde bespreking wordt dus best verwezen naar elk onderdeel apart, aangezien dit eenvoudiger te lezen en overzichtelijker is. In de gevallen waarin interpretatie niet kan of moeilijker verloopt, is het de vraag of een (multilateraal) verdrag redding kan bieden. Algemeen kan niet anders dan op deze laatste vraag zowel ontkennend als bevestigend te antwoorden.

[697] Zie N. VAN RAEMDONCK (BIJLAGE 1) die de toerekenbaarheid aan staten als een kernprobleem beschouwt, wat ook in de geciteerde rechtsleer terugkomt: o.a. KUMAR, SRIVASTAVA, LAZAREVIC, 313-314.
[698] Indien men over cyberaanvallen spreekt, zal men het recht op zelfverdediging moeten bekijken; indien men over cyberspace spreekt, zal men het transnationaal karakter van cyberoorlogen moeten bestuderen, indien met over (cyber-)terrorisme spreekt, zal men moeten nagaan of niet-statelijke actoren bestaan in de cybercontext.

214. Voor de meeste behandelde thema's kunnen via doelgerichte interpretatie de vraagstukken worden opgelost. Zo zal het gebruik van kernwapens in de cybercontext redelijkerwijs aangepakt kunnen worden door de toepassing van de bestaande rechtspraak en verdragen. Dit geldt des te meer voor het gebruik van cyberwapens: gelet op de bestaande absolute principes in het internationaal humanitair recht (het principe van onderscheid en het verbod op het veroorzaken van onnodig leed), kan het niet anders dan dat deze ook op cyberwapens van toepassing zijn. Zelfs voor problemen die op het eerste zicht niet internationaalrechtelijk opgelost kunnen worden (cyberterreur, de toerekenbaarheid aan staten), kan men terugvallen op bestaande regels (*in casu* het Cybercrimeverdrag). Het zou dan ook onlogisch zijn om deze problemen op te lossen via een verdrag, aangezien dit starheid zou inhouden, terwijl de bestaande regels (vaak op basis van internationaal gewoonterecht) flexibel genoeg zijn[699] om de snel evoluerende cybercontext (zie bijvoorbeeld de Wet van Moore) aan te pakken.

215. Langs de andere kant kennen enkele cruciale vraagstukken geen oplossing door de specifieke context van cyberoorlogen. N. VAN RAEMDONCK ziet bijvoorbeeld de problematiek van de toerekenbaarheid als een van de grootste struikelblokken voor het toepassen van internationaal recht op cyberoorlogen. Deze masterproef heeft hetzelfde geconcludeerd: de bestaande principes om gedragingen aan staten toe te rekenen, voldoen niet. Een nieuwe bewijsregeling zou dit vlotter kunnen doen verlopen, maar daarvoor zou dus consensus in de internationale gemeenschap moeten bestaan. Verder is het ook niet volledig duidelijk wanneer men nu van een cyberaanval kan spreken, wat men als cyberspace ziet en wat men dus als cyberoorlog kan of moet aanduiden. Dit zijn fundamentele vraagstukken indien het gaat over cyberoorlog. Misschien zal de gewoonte en de statenpraktijk in de toekomst een antwoord bieden, maar indien dit niet het geval is, zal men hierover duidelijkheid moeten scheppen, aangezien de bestaande regels onvoldoende zijn.

216. Voorstellen geven over oplossingen voor alle mogelijke pijnpunten lijkt niet mogelijk te zijn. Enerzijds is er de reeds vermelde situatie dat effectieve regeling doorgaans na de feiten (d.i. na een cyberoorlog) gebeurt, en anderzijds zijn niet alle moge-

[699] J. R. CRAWFORD, "The Identification and Development of Customary International Law", *Foundations and Futures of International Law*, 23 mei 2014, 10.

lijke pijnpunten besproken. Een groot probleem werd echter wel aangepakt: de toerekenbaarheid aan staten. Deze masterproef was van oordeel dat het bewijs van toerekenbaarheid in geval van cybertoepassingen misschien lichter kon worden gemaakt: indien het uit de omstandigheden van de zaak aannemelijk zou zijn dat staat A achter een cyberaanval op staat B zit (direct of via tussenpersonen), dan zou het aan staat A zijn om het tegendeel te bewijzen. Dit lijkt een evenwichtige tussenoplossing te zijn tussen de huidige situatie en de voorstellen om alle cyberaanvallen die vanuit een staat komen, onmiddellijk aan die staat toe te rekenen.

D. Een cyberverdrag: is het dringend?

217. Een andere vraag is dan weer of een dergelijk verdrag er snel moet komen. Aangezien de meeste problemen door interpretatie opgelost kunnen worden, kan men stellen van niet. Men zou de vragen die niet via de Martensclausule beantwoord kunnen worden, kunnen oplossen wanneer ze zich effectief stellen. Het feit dat er nog nooit een cyberoorlog heeft plaatsgevonden en dat grootschalige cyberaanvallen een zeldzaamheid zijn, lijkt te bevestigen dat een verdrag (of andere regelgeving) geen prioriteit is. Langs de andere kant erkent men meer en meer dat de cyberspace een gevaar kan vormen: “So Cyberspace is real. And so are the risks that come with it”, aldus president Barack Obama. Stuxnet en Flame tonen bovendien aan dat cyberwapens reeds bestaan en potentieel enorme schade kunnen toebrengen. Indien een cyberoorlog morgen zou uitbreken, blijven dus enkele cruciale vragen onbeantwoord (zoals de vraag wanneer men juist van een cyberoorlog kan spreken en wat men als gewapende aanval ziet). Deze masterproef is daarom van mening dat een verdrag er best zou komen, niet noodzakelijk in de nabije toekomst, maar toch ook niet te ver in die toekomst.

E. Een cyberverdrag: is het mogelijk?

218. Alle argumentatie ten spijt, is een verdrag (en in het algemeen regelgeving) slechts mogelijk indien daarvoor consensus bestaat in de internationale gemeenschap. Daar zou het wel eens kunnen mislopen, wat hierboven ook herhaaldelijk is opgemerkt. In navolging van wat N. VAN RAEMDONCK meent, is het aannemelijk dat staten cyberoorlog niet geregeld *willen* zien. Uitbreiding van de toerekenbaarheid aan staten zou voor sommige staten bijvoorbeeld betekenen dat zij plots aansprakelijk zouden

kunnen zijn. Politieke overwegingen zullen het dus waarschijnlijk halen op de rechtsbescherming.

219. Geen enkel conflict werd bovendien vooraf geregeld, omdat staten voordien geen beperking op hun soevereiniteit wilden zien. Slechts nadien, toen de gevolgen van het conflict zichtbaar werden, vond men de nodige consensus om op te treden. Dit was het geval met de Verdragen van Den Haag van 1907, het verbod op het gebruik van gifgas na de Eerste Wereldoorlog en de bescherming van burgers na de Tweede Wereldoorlog, via de Verdragen en Protocollen van Geneve. In elk van deze verdragen kan men op de een of andere manier terugvinden dat men "gelet op de schadelijke gevolgen van conflicten in het verleden" wil optreden. Het valt niet te argumenteren dat cyberoorlog anders is. Hoewel de rechtsleer dus kan aandringen op verdragen of regels voorschrijven in handleidingen zoals de *Tallinn-manual*, kan men aannemen dat echte regulering pas zal voorkomen na een effectieve cyberoorlog. Dit is ook enigszins te begrijpen: deze masterproef heeft met behulp van de rechtsleer voorbeelden gegeven van situaties waar cyberoorlog problemen kan geven bij het bestaande internationaal recht. Deze voorbeelden zijn echter beredeneerde speculatie. Indien een cyberoorlog totaal onvoorziene effecten teweeg zou brengen, zou een bestaand verdrag aangepast moeten worden. Het is dan misschien beter om slechts regelgevend op te treden wanneer men de volle invloed van een cyberoorlog in aanmerking kan nemen.

F. Slotbeschouwing

220. Cyberoorlog is een nieuw fenomeen. Het is zo nieuw, dat het nog niet is voorgekomen. De cyberwereld zorgt voor unieke problemen door de unieke kenmerken van die wereld, zoals de verbondenheid van cyberspace en de snelle ontwikkeling van cybertoepassingen. Deze nieuwheid is echter relatief vlot aan te pakken in het internationaal recht: de meeste hierboven beschreven problemen kunnen via doelgerichte interpretatie opgelost worden aan de hand van de bestaande internationaalrechtelijke regels. Enkele fundamentele vraagstukken blijven echter onopgelost (de inhoud van de term *gewapende aanval* in de cybercontext, de afbakening van cyberspace, de inhoud van *cyberoorlog* op zich of de toerekenbaarheid aan staten). De statenpraktijk zal in de toekomst misschien leiden tot internationaal gewoonterecht, maar indien niet, zou een verdrag de hier beschreven probleemgevallen kunnen of moeten aanpak-

ken. De vraag is echter of dit zal gebeuren, aangezien de geschiedenis ons leert dat dergelijke verdragen doorgaans slechts na de feiten opgesteld worden. Wanneer men ook een verdrag wil opstellen, hoopt deze masterproef dat het een steentje, hoe klein ook, heeft kunnen bijdragen aan de regulering en discussie rond cyberoorlog in het internationaal recht.

JORIS DEPOORTER

BIBLIOGRAFIE

A. Wetenschappelijke artikelen en literatuur

COUPLAND, R. M., *The Red Cross Wound Classification*, ICRC, Geneve, 1991, 15 p.

COUPLAND, R. M., "Towards a Determination of Which Weapons Cause 'Superfluous Injury or Unnecessary Suffering'", *International Physicians for the Prevention of Nuclear War*, 1997, ippnw.org

KESLER, B., "The Vulnerability of Nuclear Facilities to Cyber Attack", *Strategic Insights Stanford*, 2010, vol. 10 nr. 1, large.stanford.edu, 15-25.

KUMAR, V., SRIVASTAVA, J., LAZAREVIC A., (*eds.*), *Managing Cyber Threats – Issues, Approaches and Challenges*, Springer press, New York, 2005, xvii + 330 p.

N.N., "Children of the Atomic Bomb – A UCLA Physician's Eyewitness Report and Call to Save the World's Children", *UCLA*, s.d., aasc.ucla.edu.

NELSEN, D. R., NISANI, Z., COOPER, A. M., FOX, G. A., GREN, E. C., CORBIT, A. G., HAYES, W. K., "Poisons, toxigens, and venoms: redifining and classifying toxic biological secretions and the organisms that employ them", *Biological Reviews of the Cambridge Philosophical Society*, 2014, vol. 89 nr. 2, ncbi.nlm.nih.gov.

NUCLEAR ENERGY AGENCY, *Chernobyl: Assesment of Radiological and Health Impacts – 2002 Update of Chernobyl: Ten Years On*, OECD, 2002, oecd-nea.org.

WAX, P. M., BECKER, C. E., CURRY, S. C., "Unexpected 'gas' casualties in Moscow: a medical toxicology perspective", *Annals of Emergency Medicine*, 2003, vol. 41 nr. 5, 700-705.

B. Verdragen en andere primaire rechtsbronnen

Verklaring betreffende de afkeuring van het gebruik in oorlogstijd van projectielen minder wegend dan 400 gram van 11 december 1868, Sint-Petersburg.

Verdrag betreffende de regels en gebruiken tijdens oorlog te land van 1899, Den Haag.

Verdrag betreffende de regels en gebruiken tijdens oorlog te land van 1907, Den Haag.

Protocol voor het verbod op het gebruik van verstikkende, giftige of andere gassen, en van bacteriologische methoden van oorlogvoering, Genève, 17 juni 1925.

Handvest van de Verenigde Naties van 26 juni 1945, San Francisco, *UNTS* XVI.

Statuut betreffende het Internationaal Gerechtshof van 24 oktober 1945, San Francisco.

Verdrag betreffende de preventie en de bestraffing van de misdaad van genocide van 9 december 1948, Parijs, *UNTS* 277.

Universele Verklaring van de Rechten van de Mens van 10 december 1948, San Francisco

Eerste verdrag van Geneve ter verbetering van de omstandigheden van de gewonden van legers te velde van 12 augustus 1949, Geneve, UNTS 31.

Europees Verdrag betreffende de Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden van 4 november 1950, Rome.

Verdrag betreffende diplomatieke relaties van 18 april 1964, Wenen, *UNTS* 95.

Internationaal Verdrag betreffende de Burgerlijke en Politieke Rechten van 16 december 1966, New York, *UNTS* 171.

Resolutie XXIII van de Conferentie van Teheran voor de Mensenrechten van 12 mei 1968, Teheran, icrc.org.

Verdrag betreffende het verbod op de ontwikkeling, productie en bewaring van biologische en toxische wapens en betreffende hun vernietiging van 26 maart 1975, London/Moscow/Washington D.C., *UNTS* 163.

Protocol bij het Verdrag van Geneve betreffende de bescherming van slachtoffers van internationale gewapende conflicten van 8 juni 1977, Geneve, *UNTS* 3.

Protocol bij het verdrag van Geneve betreffende de bescherming van slachtoffers van niet-internationale gewapende conflicten van 8 juni 1977, Geneve, *UNTS* 609.

Verdrag betreffende het verbod of het gebruik van bepaalde conventionele wapens die geacht kunnen worden buitensporig te verwonden of die zonder onderscheid werken van 10 oktober 1980, Geneve, *UNTS* 171.

Verklaring betreffende de ontoelaatbaarheid van interventie en tussenkomst in de interne zaken van Staten, Algemene Vergadering van de Verenigde Naties, 9 december 1981, *Doc. Nr.* GA RES/36/103.

Grondwet en Conventie betreffende de Internationale Telecommunicatie-Unie van 6 november 1982, Parijs, *UNTS* 319.

Verdrag betreffende het verbod op de ontwikkeling, productie, bewaring en het gebruik van chemische wapens en betreffende hun vernietiging van 13 januari 1993, New York/Parijs, *UNTS* 317.

Resolutie 52/39 C van de Algemene Vergadering van de Verenigde Naties, 31 december 1997, *Doc.Nr.* A/RES/52/39.

Statuut van het Internationaal Strafhof 17 juni 1998, Rome, *Doc.nr.* A/CONF.183/9.

Comité voor de Mensenrechten van de Verenigde Naties, *General Comment 29*, 31 augustus 2001, *Doc.Nr.* CCPR/C/21/Rev.1/Add.11.

Resolutie 1368 van de Veiligheidsraad van de Verenigde Naties, 12 september 2001, *Doc.nr.* S/RES/1368.

Resolutie 1373 van de Veiligheidsraad van de Verenigde Naties, 18 september 2001, *Doc. nr.* S/RES/1373.

Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes, 26 oktober 2001, nr. 107-56.

Cybercrimeverdrag van de Raad van Europa van 23 november 2001, Budapest.

Resolutie 1386 van de Veiligheidsraad van de Verenigde Naties, 20 december 2001, *Doc. nr.* S/RES/1386.

Draft Articles on Responsibility of States for Internationally Wrongful Acts, Verenigde Naties, 2001, www.legal.un.org.

Draft Articles on Responsibility of States for Internationally Wrongful Acts with commentary, Verenigde Naties, 2001, www.legal.un.org.

In Larger Freedom: Towards Development, Security and Human Rights for All, Rapport van het Secretariaat-Generaal van de Verenigde Naties, 2005, *Doc.nr.* A/59/565.

CAVV, *Cyber Warfare*, december 2011, nr. 77.

Resolutie 68/167 betreffende het recht op privacy in het digitale tijdperk van de Algemene Vergadering van de Verenigde Naties, 18 december 2013, *Doc.nr.* A/RES/68/167.

C. Rechtspraak

PCIJ, *S.S. "Wimbledon"*, 1923, *P.C.I.J. Series A nr. 1*, p. 15 e.v.

UNRIAA, *Lusitania*, 1923, *Vol. VII*, p. 32 e.v.

UNRIAA, *Zafiro*, 1925, Vol. VI, p. 160 e.v.

PCIJ, *Factory at Chorzow*, 1927, *P.C.I.J. Series A, nr. 17*, p. 29 e.v.

PCIJ, *Frankrijk vs. Turkije*, 1927, ser. A nr. 10.

UNRIAA, *Lehigh Valley Railroad Company and Others (U.S.A.) v. Germany: "Black Tom" and "Kingsland" incidents*, 1930, Vol. VIII, p. 84 e.v. en p. 1939 e.v.

UNRIAA, *Dickson Car Wheel Company (U.S.A.) v. United Mexican States*, 1931, vol. IV, p. 669 e.v

PCIJ, *Phosphates in Morocco*, 1938, Series A/B, nr. 74.

Nürembergtribunaal, *United States of America v. Alfried Felix Krupp von Bohlen un Albach et al.*, Nuremberg, 1948.

IGH, *Corfu Channel*, 1949, *ICJ Reports 1949*, p. 4 e.v.

ECRM, *Denmark, Norway, Sweden and the Netherlands v. Greece*, 31 mei 1961, nr. 3321/67, 3322/67, 3323/67, 3324/67, echr.coe.int.

IGH, *North Sea Continental Shelf*, 1969, *ICJ Reports 1969*, p. 3 e.v.

Mensenrechtencommissie, *Lopez v. Uruguay*, 1979 (communicatienr. 52/1979), *Doc.nr.* CCPR/C/13/D/52/1979.

PCIJ, *United States Diplomatic and Consular Staff in Tehran*, 1980, *P.C.I.J. Reports 1980*, p. 3 e.v.

EHRM, *Silver and others v. United Kingdom*, 25 maart 1983, Series A, Nr. 61, p. 33 e.v.

EHRM, *Sunday Times v. United Kingdom*, 25 maart 1983, Series A, Nr. 30, p. 31 e.v.

PCIJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. Verenigde Staten van Amerika)*, 1986, *I.C.J. Reports* 1986, p. 14 e.v.

UNRIAA, *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 1986 between the two States and which related to the problems related to the Rainbow Warrior affair*, 1990, *Vol. XX*, p. 215 e.v.

Joegoslaviëtribunaal, *Prosecutor v. Tadic*, 1995, IT-94-1-A.

ICJ, Advisory Opinion, *Legality of the threat or use of nuclear weapons*, 8 juli 1996, *I.C.J. Reports* 1996, p. 226 e.v.

Joegoslaviëtribunaal*, Prosecuter vs. Martic*, 1996, IT-95-11.

Joegoslaviëtribunaal, *Prosecutor v. Furundzija*, 10 december 1998, IT-95-17/1-T.

Joegoslaviëtribunaal, *Prosecutor v. Akayesu*, 2 september 1998, ICTR-96-4-T.

IGH, *Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America)*, 6 november 2003, *ICJ Reports 2003*, p. 161 e.v.

IGH, *Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, 9 juli 2004, *ICJ Reports 2004*, p. 136 e.v.

Joegoslaviëtribunaal, *Prosecutor v. Limaj*, 30 november 2005, IT-03-66-T.

IGH, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, 19 december 2005, *ICJ Reports 2005*, p. 168 e.v.

ICC, *Prosecutor v. Thomas Lubanga Dyilo*, 29 januari 2007, ICC-01/04-01/06.

IGH, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro*, 26 februari 2007, *ICJ Reports 1996*, P. 595 e.v.

D. Rechtsleer

1. Artikels, bijdragen in naslagwerken, databanken …

BAHERI, Z., FARD, A. S., "Status of espionage from the perspective of international laws with emphasis on countries' diplomatic and consular relations", *Journal of Scientific Research and Development*, 2015, Vol. 2 nr. 1, 41-45.

BARNEY, S., "Innocent Packets? Applying navigational regimes from the Law of the Sea Convention by analogy to the realm of cyberspace", *Naval Law Review*, nr. 48, 2001, 56-83.

BORELLI, S., "The (Mis)-Use of General Principles of Law: *Lex specialis* and the Relationship between International Human Rights Law and the Laws of Armed Conflict" in PINESCHI, L., (*ed.*), *General Principles of Law: The Role of the Judiciary*, Springer, New York, 2015, 265-294.

BOTHE, M., "The Law of Neutrality" in FLECK, D. (*ed*.), *The Handbook of International Humanitarian Law*, Oxford University press, Oxford, 2013, 549-580.

BOTHE, M., "Nuclear Weapons Advisory Opinions", *MPEPIL*, OPIL, oktober 2015, opil.ouplaw.com, 9 p.

BOURBONNIERE, M., HAECK, L., "Jus in Bello Spatiale", *Air & Space Law*, vol. XXV, 2000, 1-11.

BUCHAN, R., "Cyberattacks: unlawful uses of force or prohibited interventions?" *Journal of Conflict and Security Law*, 2012, nr. 17.

BUERGENTHAL, T., "To Respect and to Ensure: State Obligations and Permissible Derogations" in HENKIN, L. (*ed*.), *The International Bill of Rights*, Columbia University Press, New York, 1981, 72-91.

CASSESE, A., "The Martens Clause: Half a Loaf or Simply Pie in the Sky?", *EJIL*, vol. 11, 2000, 187-216.

CRAWFORD, J. R., "The Identification and Development of Customary International Law", *Foundations and Futures of International Law*, 23 mei 2014, 15 p.

CRAWFORD, J., PEEL, J., OLLESON, S., "The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading", *EJIL*, 2001, vol. 12 nr. 5, 963-991.

CONDRON, S. M., "Getting It Right: Protecting American Critical Infrastructure in Cyberspace", *Harvard Journal of Law and Technology*, 2006-2007, nr. 20, 403-422.

DASKAL, J., "The geography of the battlefield: a framework for detention and targeting outside the 'hot' conflict zone", *University of Pennsylvania Law Review*, 2013, nr. 161, 1165-1234.

DINSTEIN, Y., "The Right to Life, Physical Integrity, and Liberty" in HENKIN, L. (*ed*.), *The International Bill of Rights*, Columbia University Press, New York, 1981, 114-137.

DINSTEIN, Y., "Computer Network Attacks and Self-Defense" in SCHMITT, M. N., O'DONNELL, B. T., (*eds*.), *Computer Network Attack and International Law*, Naval War College, Rhode Island, 2002, 100-119.

DINSTEIN, Y., "Warfare, Methods and Means", *MPEPIL*, OPIL, september 2015, opil.ouplaw.com, 9 p.

DÖRR, O., "Use of Force, Prohibition of", *MPEPIL*, OPIL, september 2015, opil.ouplaw.com, 17 p.

FORCESE, C., "Spies Without Borders: International Law and Intelligence Collection", *Journal of National Security Law & Policy*, 2011, vol. 5 nr. 179, 179-210.

FRANCEUS, F., "Cyberaanvallen en het recht van de gewapende conflicten: bemerkingen bij een juridische primeur in België en de Verenigde Staten", *BISC*, 19 oktober 2012, 30 p.

GASSER, H.-P., THÜRER, D., "Humanitarian Law, International", *MPEPIL*, OPIL, maart 2011, opil.ouplaw.com, 18 p.

GJELTEN, T., "Shadow Wars: Debating Cyber Disarmament", *World Affairs*, 2010, nr. 173.

GREENWOOD, C., "Historical Development and Legal Basis" in FLECK, D. (*ed.*), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, 1-43.

GREENWOOD, C., "Caroline, The", *MPEPIL*, OPIL, april 2009, opil.ouplaw.com, 4 p.

GREENWOOD, C., "Self-Defence", *MPEPIL*, OPIL, april 2011, opil.ouplaw.com, 13 p.

GOLDSMITH, J., "How Cyber changes the Laws of War", *EJIL*, 2013, vol. 24 nr. 1, 129-138.

GOMBEER, K, "Het internationaal juridisch kader voor interstatelijk gebruik van computeraanvallen", *Juridische Meesterwerken*, VUB, 2010-2011, 165-220.

HOISINGTON, M., "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", *Boston College International and Comparative Law Review*, 2009, nr. 32, 439-454.

HUGHES, R., "A Treaty for Cyberspace", *International Affairs*, 2010, nr. 2, 523-541.

ILA, *Report of the Sixty-Ninth Conference*, 2000, 725: Statement of Principles Applicable to the Formation of General Customary International Law.

JENSEN, E., "Sovereignty and neutrality in cyber conflict", *Fordham International Law Journal*, 2012, nr. 35, 815-841.

JENSEN, E. T., "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence", *Stanford Journal of International Law*, 2002, nr. 38, 202-240.

JOHNSON, D., POST, D., "Law and Borders: the rise of law in cyberspace", *Stanford Law Review*, nr. 48, 1996, 1366-1402.

JYH-AN, L., CHING-YI, L., "Forbidden City enclosed by the great firewall: the law and power of internet filtering in China", *Minnesota Journal of Law Science and Technology*, nr. 13(1), 125-151.

KADELBACH, S., "Nuclear Weapons and Warfare", *MPEPIL*, OPIL, juni 2013, opil.ouplaw.com, 21 p.

KANUCK, S., "Sovereign Discourse on cyber conflict", *Texas Law Review*, 2010, nr. 88, p. 1571-1597.

KOBRIN, S., "Territoriality and the governance of cyberspace", *Journal of International Business Studies*, nr. 32, 2001, 687-704.

KOLB, R., "The relationship between international humanitarian law and human rights law: A brief history of the 1948 Universal Declaration of Human Rights and the 1949 Geneva Conventions", *International Review of the Red Cross*, 1998, nr. 400, icrc.org.

KOLB, R., "Human Rights and Humanitarian Law", *MPEPIL*, OPIL, Maart 2013, opil.ouplaw.com, 17 p.

KORFF, D., "The Standard Approach under Articles 8-11 ECHR and Article 2 ECHR", *European Commission*, ec.europa.eu.

KUNIG, P., "Intervention, Prohibition of", *MPEPIL*, OPIL, april 2008, www.opil.ouplaw.com, 15 p.

LEVARSKA, L., "Regulation of Cyber-Warfare: Interpretation versus Creation"*, ESR*, December 2013, nr. 70, 15 p.

MARAUHN, T., "Chemical Weapons and Warfare", *MPEPIL*, OPIL, juni 2010, opil.ouplaw.com, 10 p.

MARAUHN, T, NTOUBANDI, Z. F., "Armed Conflict, Non-International", *MPEPIL*, OPIL, mei 2011, opil.ouplaw.com, 14 p.

MERON, T. "The Martens Clause, Principles of Humanity, and Dictates of Public Consience", *The American Journal of International Law*, vol. 94, 2000, 78-89.

RABKIN, J. A., RABKIN, A., "An Emerging Threats Essay – To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict", *Task force on national security and law*, Hoover Institution Stanford University, 2012, 15 p.

RADSAN, A. J., "The Unresolved Equation of Espionage and International Law", *Michigan Journal of International Law*, 2007, Vol. 28 nr. 595, 595-623.

Rapport van de International Law Commision over het werk van zijn 46ste Sessie, 2 mei 1994-22 juli 1994, A/49/10.

ROSCINI, M., "World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force", *Max Planck UNYB*, 2010, nr. 14, 85-130.

NYE, J. S., "Cyber Power", *Harvard Kennedy School, Belfer Center*, 2010, www.dtic.mil, 24 p.

QUÉNIVET, Q., "The History of the Relationship between International Humanitarian Law and Human Rights Law" in ARNOLD, R., QUÉNIVET, N. (*eds*.), *International Hu-*

manitarian Law and Human Rights Law: Towards a new merger in International Law, Martinus Nijhoff Publishers, Leiden, 2008, 1-14.

SASSOLI, M., "Transnational Armed Groups and International Humanitarian Law", *Humanitarian Policy and Conflict Research Harvard University*, 2006, nr. 6, 43 p.

SASSOLI, M., "Guantanamo, Detainees", *MPEPIL*, OPIL, mei 2013, opil.ouplaw.com, 15 p.

SCHAAP, A. J., "Cyber Warfare Operations: Development and Use under International Law", *Air Force Law Review*, 2009, nr. 64, p. 121-153.

SCHALLER, C., "Spies", *MPEPIL*, OPIL, september 2015, opil.ouplaw.com, 5 p.

SCHMITT, M. N., "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *IITA (USAF)*, juni 1999, 41 p.

SITAROPOULOS, N., "Weapons and superfluous injury or unnecessary suffering in international humanitarian law: human pain in time of war and the limits of law", *Revue Hellénique de Droit International*, 2001, vol. 54, 71-108.

STRYDOM, H. A., "Weapons of Mass Destruction", *MPEPIL*, OPIL, augustus 2013, opil.ouplaw.com, 14 p.

SVARC, D., "Biological Weapons and Warfare", *MPEPIL*, OPIL, augustus 2015, opil.ouplaw.com, 7 p.

TAMS, C. J., "The Use of Force against Terrorists", *EJIL*, 2009, Vol. 20 nr. 2, 359-397.

TICEHURST, R., "The Martens Clause and the Laws of Armed Conflict", *International Review of the Red Cross*, nr. 317, 1997, www.icrc.org.

VAN DEN HERIK, L., "De digitale oorlog: waan of werkelijkheid", *NjW*, 2013, nr. 6, 348-355.

VOLIO, F, "Legal Personality, Privacy, and the Family" in HENKIN, L. (*ed*.), *The International Bill of Rights*, Columbia University Press, New York, 1981, 185-208.

VON BERNSTORFF, J., "Martens Clause", *MPEPIL*, OPIL, december 2009, opil.ouplaw.com, 6 p.

WAGNER, M., "Non-State Actors", *MPEPIL*, OPIL, juli 2013, opil.ouplaw.com, 12 p.

WILDE, R., "Triggering State Obligations Extraterritorially: The Spatial Test in Certain Human Rights Treaties", in ARNOLD, R., QUÉNIVET, N. (*eds*.), *International Humanitarian Law and Human Rights Law: Towards a new merger in International Law*, Martinus Nijhoff Publishers, Leiden, 2008, 133-153.

WOLTAG, J.-C., "Cyber Warfare", *Max Planck Encyclopedia of Public International Law*, Oxford Public International Law, mei 2010, opil.ouplaw.com, 9 p.

WRIGHT, Q., "Espionage and the Doctrine of Non-Intervention in Internal Affairs" in STANGER, R., (*ed.*), *Essays on Espionage and International Law*, Ohio State University Press, Columbus, 3-28.

ZEMANEK, K., "Armed attack", *MPEPIL*, Oxford Public International Law, oktober 2013, opil.ouplaw.com, 8 p.

2. Boeken

ARAI-TAKAHASHI, Y., *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Intersentia, Antwerpen, 2001, xiii + 247 p.

BOOTHBY, W. H., *Conflict Law: The Influence of New Weapons, technology, Human Rights and Emerging Actors*, Asser Press, Den Haag, 2014, xv + 464 p.

BOTHE, M., RONZITTI, N., ROSAS, A. (*eds*.), *The New Chemical Weapons Convention: Implementation and Prospects*, Martinus Nijhoff Publishers, Leiden, 1998, xv + 613 p.

BROWNLIE, I., *International Law and the Use of Force by States*, Clarendon Press, Oxford, 1963, xxviii + 532 p.

BROWNLIE, I., *Principles of Public International Law*, Oxford University press, Oxford, 1998, xlviii + 741 p.

DINNISS, H. H., *Cyber Warfare and the Laws of War*, Cambridge University press, Cambridge, 2012, xix + 331 p.

DIXON, M., *Textbook on International Law*, Oxford University press, Oxford, 2013, xxxii + 393 p.

CHEN, T. M., JARVIS, L., MACDONALD, S. (*eds*.), *Cyberterrorism, Understanding, Assessment and Response*, Springer Press, New York, 2014, xxiii + 215 p.

DUFFY, H., *The 'War on terror' and the framework of international law*, Cambridge University press, Cambridge, 2005, xxxvi + 488 p.

GASSER, H.-P., JUNOD, S.-S., PILLOUD, C., DE PREUX, J., SANDOZ, Y., SWINARSKI, C., WENGER, C. F., ZIMMERMAN, B., PICTET J.(*voorz.*), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneve, Martinus Nijhoff Publishers, 1987, xxxv + 1625 p.

GORMAN, F. C., *Non-State Actors, Terrorism and the United Nations: A Critical Analysis through Three Case studies Examining the United Nations' Effectiveness in Addressing the Threat Imposed by Violent Non-State Actors*, Thesis aan de Virginia Polytechnic and State University, Virginia, 2009, v + 132 p.

HORBACH, N., LEFEBER, R., RIBBELINK, O., *Handboek Internationaal Recht*, Asser Press, Den Haag, 2007, xxii + 946 p.

HUMANITARIAN POLICY AND CONFLICT RESEARCH, *Manual on International Law Applicable to Air and Missile Warfare*, Harvard University, Cambridge, 2009, viii + 56 p.

HUMANITARIAN POLICY AND CONFLICT RESEARCH, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, Harvard University, Cambridge, 2010, vi + 348 p.

KREMER, J.-F., MÜLLER, B. (*eds*.), *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer Press, Berlijn, 2014, xxiv + 284 p.

MELZER, D., *Interpretive guidance on the notion of direct participation in hostilities*, Internationaal Comité van het Rode Kruis, Geneve, 2009, 85 p.

NASU, H., MCLAUGHLIN, R. (*eds*.), *New Technologies and the Law of Armed Conflict*, Asser Press, Den Haag, 2014, xx + 259 p.

NOWAK, M., *Introduction to the International Human Rights Regime*, Martinus Nijhoff Publishers, Leiden, 2003, xv + 365 p.

OBERLEITNER, G., *Human Rights in Armed Conflict – Law, Practice, Policy*, Cambridge University press, Cambridge, 2015, xx + 431 p.

PICTET, J. S. (*ed.*), *Commentary – I Geneva Convention for the amelioration of the condition of the wounded and sick in armed forced in the field*, International Committee of the Red Cross, Geneve, 1952, xvi + 466 p.

PICTET, J. S. (*ed.*), *Commentary – III Geneva Convention Relative to the treatment of prisoners of war*, International Committee of the Red Cross, Geneve, 1960, xxxii + 764 p.

PICTET, J. S. (*ed.*), *Commentary – IV Geneva Convention Relative to the protection of civilian persons in time of war*, International Committee of the Red Cross, Geneve, 1958, xxviii + 660 p.

SCHMITT, M. N. (*ed.*), *Essays on Law and War at the Fault Lines*, Springer Press, Den Haag, 2012, xii + 637 p.

SCHMITT, M. N. (*ed.*), *Tallinn Manual on The International Law Applicable to Cyber Warfare*, Cambridge University press, Cambridge, 2013, 215 p.

SIMS, N. A., *The Future of Biological Disarmament: Strengthening the Treaty Ban on Weapons*, Routledge, New York, 2009, xvii + 216 p.

SIVAKUMARAN, S. *The law of non-international armed conflict*, Oxford University Press, Oxford, 2012, xxiv + 696 p.

SVENSSON-MCCARTHY, A.-L., *The International Law of Human Rights and States of Exception*, Martinus Nijhoff Publishers, Den Haag, 1998, xxiii + 780 p.

VERTON, D., *Black Ice: the invisible threat of cyber-terrorism*, McGraw-Hill, New York, 2003, xxvii + 273 p.

THE UNITED STATES WAR CRIMES COMMISSION, *Law Reports of Trials of War Tribunals – Volume X The I.G. Farben and Krupp Trials*, Londen, 1949, ix + 181 p.

VIII. BIJLAGEN

BIJLAGE 1

14/04/2016 11:56

Nathalie Van Raendom
ik denk dat het praktisch zeker mogelijk is, maar dat het politiek moeilijk ligt

het internationaal recht is veel meer een politieke afspraak dan echt recht in mijn opinie, en de vraag of het toegepast kan worden is meer een vraag van goede wil

al zijn de twee struikelblokken wel zeker dat attributie moeilijk/bijna nmogelijk is, en dat het instrument niet duidelijk te definieren valt, en de interpretatie dus moet schuiven naar de effecten van een cyberaanval, niet de aanval zelf.

Nathalie Van Raendom
mijn eindconclusie was dat we niet kunnen beslissen of zo'n aanvallen nu wel of niet een use of force zijn, omdat dit afhangt hoe de internationale gemeenschap dit zelf wil framen (en welke politiekeincentives de kanten hebben om het enerzijds of anderzijds te framen)

Bijlage 2

Student Award Submission

Summary of thesis

Cyber-Attacks and the Jus ad Bellum:

Spectrum of Legality and Development of the Custom

~

By Nathalie Van Raemdonck

Abstract

This paper investigates the classification of cyber-attacks as a use of force from an instrumental and consequence-based perspective, and looks at the relevance of attacks on targets that are of national interest, or those that are vital for national security. It analyses the desirable classification of such cyber-attacks in predictable situations using a leaked US strategic policy document on cyber as a case-study.

BIJLAGE 3

From: **Deprez Thierry (RSWO)** Thierry.Deprez1@rma.ac.be
Subject: RE: Vraag m.b.t. Masterproef
Date: 26 Apr 2016 07:50
To: Joris Depoorter jorisdepoorter@icloud.com

DT

Beste Joris,

Uw vraag werd voorgelegd aan de dienst inlichtingen en veiligheid (ACOS IS) van Defensie Gelieve hieronder het antwoord te willen vinden met de referenties van de persoon die uw aanvraag heeft behandeld :

Onze legal advisors zijn helaas druk bezet sinds de evenementen van vorige maand,
Wijzelf hebben wel notie van, maar onvoldoende om volledig te kunnen antwoorden op onderstaande ruime vragen,
Graag hadden we bij deze dus verwezen naar andere bronnen die volgens ons goede referenties zijn.

- Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar http://www.nato.int/cps/en/natohq/opinions_118435.htm
- Tallinn Manual https://ccdcoe.org/research.html
- Frank Franceus http://docplayer.nl/2328034-Cyberaanvallen-en-het-recht-van-de-gewapende-conflicten-bemerkingen-bij-een-juridische-primeur-in-belgie-en-de-verenigde-staten-frank-franceus.html
- Masterproef UGent http://lib.ugent.be/fulltxt/RUG01/002/163/282/RUG01-002163282_2014_0001_AC.pdf

De vragen met betrekking tot het beleid kunnen het best afgetoetst worden met de standpunten van onze minister die publiekelijk te vinden zijn,
Antwoorden op de vraag met betrekking tot de cyber'aanvallen' zijn evengoed terug te vinden de notulen van de parlementaire vragen/antwoorden in de Kamer en Senaat.

Indien er alsnog punctuele vragen mochten zijn, stel ik voor om dat door middel van een kort onderhoud te behandelen.

v/r,

E-mails are checked only twice a day
In case of urgent response required, please do contact our service by phone.

Björn Vanneste, OF3
Belgian Defence
General Intelligence and Security Service
Cyber Intelligence

Eversestraat 1
1140 Brussels
Belgium

Phone +32 2 44 17 444
fax + 32 2 44 17 444
E-mail Unclass user1242@qet.be
Public GPG Key upon request // Call me to verify
E-mail Secure bjorn.vanneste@bel.bices.org

In de hoop u hiermee van dienst te zijn geweest,
Vriendelijk groet,

Thierry DEPREZ
Luitenant-Kolonel van het Vliegwezen

Bijlage 4

From: **Informatie Rijksoverheid** noreply@informatierijksoverheid.nl
Subject: E3302863: Vraag met betrekking tot Masterproef
Date: 13 Apr 2016 09:04
To: jorisdepoorter@icloud.com

IR

Geachte heer of mevrouw,

Uw kenmerk is E3303413

Wij beschikken niet over voldoende informatie om uw vraag te kunnen beantwoorden.

Het antwoord op uw vraag kan het beste gegeven worden door een medewerker van het ministerie van Defensie die uitgebreid op de hoogte is van de regels en richtlijnen. Uw vraag hebben wij daarom voor verdere beantwoording doorgestuurd naar dit ministerie.

Met vriendelijke groet,

Informatie Rijksoverheid

Dear Sir/Madam,

Your reference is E3303413

Unfortunately, we do not have enough information to answer your question.

We have forwarded your question to the Ministry of Defence. This Ministry has thorough information on the rules and guidelines for this subject.

Kind regards,

Public Information Service, Government of the Netherlands

BIJLAGE 5

From: **Schmitt, Michael** M.Schmitt@exeter.ac.uk
Subject: Re: Questions regarding the completion of Master's Dissertation
Date: 25 Apr 2016 20:59
To: Joris Depoorter jorisdepoorter@icloud.com

SM

I am terribly sorry, but I am in Estonia for the next weeks working furiously to complete the manuscript for Tallinn Manual 2.0. Unfortunately, it leaves me no time to answer the many requests I get from students around the world.

Regrets,

Michael N. Schmitt
Chairman & Charles H. Stockton Professor, Stockton Center, US Naval War College
Professor of Public International Law, University of Exeter
Francis Lieber Distinguished Scholar, Lieber Institute, USMA at West Point
Fellow, Harvard Law School Program in International Law & Armed Conflict

---

From: Joris Depoorter <jorisdepoorter@icloud.com>
Date: Monday, April 25, 2016 at 21:20
To: Michael Schmitt <mschmitt@law.harvard.edu>
Subject: Questions regarding the completion of Master's Dissertation
Resent-From: Michael Schmitt <mschmitt@law.harvard.edu>

Dear Professor Schmitt

I am currently completing my Master's Disseration at the faculty of Law, Ghent University, Belgium. My topic is the applicability of general international law on cyberwar ('the applicability of the Martens Clause on cyber warfare'). Since your contributions appear to be the main source of citation for most scholars, I hoped I might ask you a few direct questions, which I could use in my conclusion (as to wether or not a treaty on cyberwar would be necessary).

Would it be possible to ask a few questions?

1) Is cyberwar (and cyberterrorism) an actual threat that can occur today, according to you?
2) Is the general international law capable of regulating this relatively new form of warfare?
3) Do you think a treaty (or other forms of specific regulation) would be necessary or feasible?
4) If such a treaty was made, which specific topic or concern (if any) should certainly be addressed, in your opinion?

I apologize for posing the questions immediately, but my thesis advisor only

told me very recently that I should add actual comments from people involved in my dissertation.

If you would need affirmation that these are questions for an actual dissertation, I can refer you to my advisor: prof. dr. Gert Vermeulen, Gert.Vermeulen@Ugent.be.

Thank you in advance, and apologies for the inconvenience.

Sincerely,

Joris Depoorter