Ethiek voor Cyberkrijg en Cyberkrijgers

Peter Olsthoorn

ANTW 111 (1): 95–109
DOI: 10.5117/ANTW2019.1.006.OLST

Abstract

Ethics for Cyber War and Cyber Warriors

Although some claim that the term cyber war is merely metaphorical, there are good reasons to see cyber war as a form of warfare – even if it is not war as we have hitherto known it. This poses the question whether the principles of the Just War Tradition, which claims to offer an alternative for pacifism and realism, apply to this specific kind of war too. This article argues that the jus in bello principles of discrimination and proportionality are applicable, and that actually applying them would limit the harm cyber-attacks currently cause. Most cyber-attacks of recent years wrongly target civilians, and this amounts to a serious breach of these principles. The final part of this article looks at those who actually conduct the cyber-attacks, the cyber soldiers – how do they fit into the military profession, and to what extent can we expect them to uphold the principles of Just War?

Keywords: cyber war, discrimination, Just War Theory, proportionality

1. Inleiding – bestaat cyberoorlog?

Wie schrijft over cyberoorlog dient eerst uit te leggen dat het gebruik van de term 'oorlog' op zijn plaats is wanneer men met slechts computers en software de informatiesystemen van een ander land aanvalt (Beard 2013). Dat is nodig sinds de politicoloog Thomas Rid (2012) in een inmiddels redelijk fameus essay met de veelzeggende titel 'Cyber War Will Not Take Place' betoogde dat cyberoorlog niet bestaat. Wie spreekt van een cyberoorlog gebruikt de term oorlog in voornamelijk overdrachtelijke zin, stelt Rid, zoals

we ook spreken van een handelsoorlog of van een oorlog tegen klimaatverandering of obesitas. Waar men in een oorlog doorgaans grossiert in het gebruik van eufemismen – denk aan 'torture lite,' 'enhanced interrogation' 'collateral damage' en 'servicing the target' (zie ook Wolfendale 2009, 53-4) – is hier van het omgekeerde sprake. Zij die denken dat we – politiek en krijgsmacht – ons moeten voorbereiden op een apocalyptisch treffen in cyberspace (de term komt uit het cyperpunk werk van William Gibson uit de jaren tachtig [1984]) hebben dat niet begrepen.

Nu heeft Rid ogenschijnlijk een punt: cyberaanvallen richten zich op computers en netwerken (en dus niet alleen op internet – ook telefonienetwerken en het elektriciteitsnet zijn doelwit), en Rid stelt dat dergelijke aanvallen niet voldoen aan de criteria van oorlogsvoering die de Pruisische generaal en militair denker Carl von Clausewitz in *Vom Kriege* formuleerde: 1) oorlog behelst de toepassing van dodelijk, fysiek geweld om 2) een bepaald doel te bereiken (oftewel: om de eigen wil aan de tegenstander op te leggen) en 3) is uiteindelijk politiek van karakter (en veronderstelt daarmee een politieke actor die op enig moment ook zijn wil communiceert). De tot nu toe bekende cyberaanvallen waren niet gewelddadig (cyberaanvallen die effecten in de fysieke wereld sorteren zijn überhaupt zeldzaam), gezien de geringe effecten niet doeltreffend (ook niet in potentie), en eerder crimineel dan politiek van aard (niet voor niets probeert de aanvaller meestal anoniem te blijven). De meeste cyberaanvallen voldoen aan geen enkele van deze drie criteria, stelt Rid, en niet één voldoet aan alle drie.

Dat nagenoeg alle auteurs over cyberoorlog dezelfde drie of vier voorbeelden aanhalen, nuanceert het beeld van een nakend cyberarmageddon nog verder. Van die voorbeelden is de bekendste en waarschijnlijk meest verstrekkende – omdat het hier een aanval betrof die wel degelijk ook fysieke effecten had – de succesvolle inzet in 2010 van de Stuxnet worm tegen Iraanse kerncentrifuges die het Iraanse atoomprogramma met jaren vertraagde. De daaropvolgende tegenaanval op Amerikaanse financiële instellingen was vermoedelijk afkomstig van de Iraanse staat (zie ook Lucas 2017: 10). Maar ook de Stuxnet aanval komt niet in de buurt van oorlog zoals we ons die normaliter voorstellen. De aanval was geweldloos, en apolitiek in die zin dat niemand de aanval opeiste (en er dus ook geen eisen zijn gesteld). Het is zelfs nooit helemaal duidelijk geworden wie verantwoordelijk voor de aanval was (naar alle waarschijnlijkheid de Verenigde Staten en/of Israël).[1] Cyberoorlog, kortom,

1 Dit is het zogenaamde attributieprobleem: van cyberaanvallen is zelden met zekerheid vast te stellen wie erachter zit.

bestaat niet, en afgaande op Rid komt daarin ook geen verandering. Wat we wel hebben is cybervandalisme en cyberspionage – en alles wat daar tussenin zit, zoals cybersabotage. Heeft Rid gelijk, dan bereiden krijgsmachten die in de cyberruimte een vierde domein naast land, zee en lucht ontwaren zich voor op een cyberoorlog omdat ze de term ten onrechte letterlijk nemen.[2]

Maar Rid staat redelijk alleen, en dat heeft een reden. Rid laat zien dat de cyberaanvallen die we nu zien bij lange na nog geen oorlog zijn in de gebruikelijke zin van dat woord, en dat ook in de toekomst cyberaanvallen waarschijnlijk niet de schaal en intensiteit zullen hebben die we normaal gesproken met de term oorlog associëren.[3] Maar dat gaat slechts op zolang we de negentiende-eeuwse definitie van oorlog blijven hanteren die Von Clausewitz muntte. Het met name in het Westen sindsdien dominante idee dat oorlog bestaat uit een reeks beslissende veldslagen beneemt ons hier echter het zicht op wat oorlog ook kan zijn, en voor het grootste gedeelte van de geschiedenis binnen de meeste culturen ook was: een vorm van strijd zonder duidelijk begin of einde, zonder al te veel risico's voor de deelnemers en zonder beslissende momenten (Lynn 2003). Wellicht zijn de hedendaagse cyberaanvallen nog het beste vergelijkbaar met de chevauchées – plundertochten – in de middeleeuwen (Whetham 2017). Men beoogde daarmee de steun van de vijandelijke bevolking aan haar heer te ondergraven door te laten zien dat deze laatste zijn onderdanen niet de bescherming kon bieden die hij hen, gezien zijn positie en het feit dat hij belasting hief en zich nog een aantal rechten liet aanleunen, wel was verschuldigd.

Dat die bescherming te wensen overliet, toonde een leger aan door burgers te plunderen, te martelen, voor losgeld te ontvoeren, te verkrachten, en te vermoorden. In het beste geval ontsprongen zij de dans door een afkoopsom te betalen. In plaats van non-combattanten te ontzien en een eerlijke veldslag aan te gaan, koos men ervoor van zo'n riskante slag te vermijden en brandschatte men onschuldige burgers. Onder meer in de Honderdjarige Oorlog koos men regelmatig voor deze pragmatische aanpak die nu gaat onder de naam terreur. Een tactiek die zowel wat betreft werkwijze als oogmerk op zijn minst enige overeenkomsten vertoont met hedendaagse

2 Voor wie de kosmos als vierde domein ziet, zoals de Amerikaanse krijgsmacht, is cyber het vijfde domein.

3 Het gebruik van de in het internationaal recht gebruikte term gewapend conflict biedt geen uitweg: het creëert een nieuwe semantische discussie over de vraag of een computer of zelfs software een wapen kan zijn (zie ook Finlay 2018: 360). Het antwoord op die vraag luidt volgens de meeste auteurs overigens bevestigend, omdat wat als wapen telt vooral afhangt van de schade die het kan aanrichten (zie bijvoorbeeld Lucas 2017: 58)

cyberaanvallen, voor zover die door een staat zijn geïnitieerd en op burgerdoelen zijn gericht, en zich uiteindelijk richten op het ondermijnen van het vertrouwen in het eigen bestel. Rest de vraag of de schade die cyberaanvallen veroorzaken ernstig genoeg is om de term oorlog te rechtvaardigen. Doden en gewonden vallen er doorgaans niet. Anderzijds is de schade die cyberaanvallen kunnen veroorzaken aan bijvoorbeeld het bankensysteem of het internet ontwrichtend genoeg, terwijl ook de ondermijning van het geloof in de eigen instituties burgers (en hun vertegenwoordigers) van iets wezenlijks beroofd (zie ook Miller 2015). Je zou zelfs kunnen stellen dat het ontwrichten van een democratische samenleving uiteindelijk veel schadelijker is dan wat conventionele militairen in een oorlogsgebied kunnen aanrichten.

Overigens is irreguliere oorlogsvoering ook nu weer de norm – een klassiek militair treffen tussen twee staten komt nog zelden voor. De in oorlog en vrede gespecialiseerde filosoof Randall Dipert voorspelde al een tijdje terug een koude oorlog (wat dan wel weer een overdrachtelijk gebruik van de term oorlog lijkt te zijn) van cyberspionage, Denial-of-Service (DoS) aanvallen en de corruptie van gegevens (2010: 403). In die zin kunnen we bijvoorbeeld de schermutselingen tussen Rusland en China enerzijds en Amerika en haar bondgenoten anderzijds, maar ook de (waarschijnlijk) Amerikaans-Israëlische actie en (al even waarschijnlijk) Iraanse reactie omtrent de Iraanse kerncentrifuges, wel degelijk als een vorm van (irreguliere) oorlogsvoering beschouwen. Overigens vergen dergelijke aanvallen zoveel kennis en capaciteit dat daar direct of indirect altijd overheden mee zijn gemoeid – waarmee we het domein van de reguliere criminaliteit sowieso zijn ontstegen. Zo bezien kun je niet alleen stellen dat cyberoorlog bestaat, maar ook dat we er wellicht al middenin zitten.

Maar ook als cyberaanvallen op zichzelf geen oorlog vormen, dan is het nog steeds waarschijnlijk dat veel toekomstige oorlogen wel degelijk ook een cybercomponent zullen hebben. Een klassiek voorbeeld daarvan is de oorlog in 2008 tussen Rusland en Georgië (in het digitale domein kan een conflict van tien jaar terug uitstekend 'klassiek' heten) waarbij Rusland de militaire capaciteit van Georgië door een cyberaanval ernstig beperkte (Arquilla 2012). Een jaar eerder slaagde een Israëlische luchtaanval op een nucleaire reactor diep in Syrië (operatie Orchard) mede doordat een cyberaanval de Syrische luchtafweer goeddeels platlegde. Naast dergelijke sabotage zullen we tijdens toekomstige gewapend conflicten steeds vaker ook het door Rid (en anderen) genoemde cyberspionage en cybervandalisme tegenkomen.

Het vervolg van dit artikel gaat eerst in op de vraag onder welk normatief regime cyberaanvallen vallen, waarbij de nadruk ligt op de traditie van de rechtvaardige oorlog; hierboven is al gesteld dat er goede argumenten zijn om cyberoorlog wel degelijk als een vorm van irreguliere oorlogvoering te beschouwen. Dat levert ook wat op, stelt de daaropvolgende paragraaf: de belangrijkste principes uit die traditie, zoals discriminatie en proportionaliteit, zijn goed toepasbaar op het cyberdomein, en de daadwerkelijke toepassing zou de hoeveelheid schade die cyberaanvallen nu veroorzaken ook verminderen. De paragraaf daarna bouwt op die aanname verder en gaat dieper in op hen die zich door die principes moeten laten leiden: hoe passen cybersoldaten in de militaire professie, en aan welke beperkingen dienen zij zich te houden?

2. Rechtvaardigheid in cyberspace

Von Clausewitz stelde niet alleen dat oorlog een voortzetting van de politiek is met andere middelen, de uitspraak die hem roem bracht, maar ook dat beperkingen zoals recht en ethiek wezensvreemd zijn aan wat oorlog is. In de praktijk is oorlogvoering doorgaans wel aan allerlei beperkingen onderhevig. Dat wist Von Clausewitz natuurlijk ook wel, maar anders dan hij meende, maken die restricties in de vorm van regels, taboes en rituelen soms juist de essentie uit van wat oorlog is. Oorlog is vaak een verrassend gereguleerde praktijk.

Er zijn drie regimes waaronder cyberaanvallen kunnen vallen. Ten eerste is er het strafrecht, dat veel cyberaanvallen als cybercrime definieert. Voor wie cyberoorlog beschouwt als metafoor is dit het aangewezen rechtsregime: veel cyberaanvallen bestaan uit diefstal en sabotage; zaken waar het normale strafrecht prima mee uit de voeten kan (zie ook Miller 2015). Wie de term cyberoorlog ziet als (een irreguliere vorm van) oorlog en niet als overdrachtelijk taalgebruik, en cyberaanvallen daarmee als onderdeel van een conflict tussen landen en niet tussen burgers en criminelen, zoekt het eerder bij het oorlogsrecht zoals dat is neergelegd in wetten en verdragen en de principes uit de traditie van de rechtvaardige oorlog die dat oorlogsrecht gedeeltelijk schraagt. Als laatste is er het nogal zwakke 'rechtsregime' dat spionage kenmerkt: hoewel er wel een normatief kader is (zie bijvoorbeeld Goldman 2009), zien de meeste inlichtingendiensten zichzelf als niet of nauwelijks gebonden aan welke wet- en regelgeving dan ook (Lucas 2017: 26, 34).

Omdat het grensoverschrijdende karakter van cyberaanvallen het strafrecht in de praktijk vrijwel tandeloos maakt, zijn van die drie regimes met name het oorlogsrecht en de normatieve principes die op spionage van toepassing zijn relevant. Maar gezien het feit dat veel cyberaanvallen beduidend verder gaan dan het verzamelen van informatie, en gezien het weinig veeleisende karakter van de normen aangaande spionage, zullen de regels van het oorlogsrecht en de traditie van de rechtvaardige oorlog (die overigens ook veel meer toestaan dan het reguliere strafrecht – in oorlog is immers veel geoorloofd dat normaliter is verboden) doorgaans eerder in beeld komen. Dat sluit ook aan bij onze eerdere conclusie dat cyberaanvallen wel degelijk een vorm van oorlog kunnen zijn. Die traditie van de rechtvaardige oorlog is geen wet maar biedt wel een vocabulaire om over oorlog te praten in morele termen, en gaat in tegen Clausewitz' idee dat oorlog streeft naar volledigheid en dat beperkingen er wezensvreemd aan zijn.

De traditie van de rechtvaardige oorlog probeert daarmee een middenweg te bieden voor een niet realistisch (voor politici althans) pacifisme dat oorlog onder geen enkele omstandigheid toestaat en een al te realistisch realisme dat stelt dat in een oorlog alles is geoorloofd. Dat realisme is onder andere gebaseerd op de aanname dat moraal relatief is, en dat we in laatste instantie geen algemeen aanvaard oordeel kunnen vellen over wat wel en niet is toegestaan bij het voeren van een oorlog. De traditie van de rechtvaardige oorlog neemt ook van dat relativisme nadrukkelijk afstand. Uiteindelijk kan iedereen een aantal basisprincipes onderschrijven die het leed dat oorlog veroorzaakt zoveel mogelijk inperken – dat veel van die principes in het Westen zijn 'ontdekt' doet volgens haar aanhangers geen afbreuk aan hun universele geldigheid; min of meer analoog naar de universele geldigheid die mensenrechten volgens sommigen genieten.[4]

4 Waar er overeenstemming bestaat over wat die principes inhouden, is er discussie over de basis van de principes van de rechtvaardige oorlog. De bovengenoemde analogie met mensenrechten suggereert dat het bij de traditie van de rechtvaardige oorlog uiteindelijk om rechten draait, zowel die van burgers als van combattanten. Michael Walzer heeft in zijn *Just and Unjust Wars* (1992) dat standpunt het invloedrijkst verwoord, waarbij hij in dezelfde beweging het utilitarisme als potentieel moreel baken in tijden van oorlog in de ban deed. Volgens Walzer is de onpartijdigheid die het utilitarisme vraagt juist in crises ver te zoeken, omdat in de praktijk politieke en militaire beslissers de kosten-baten analyse toch altijd zó opmaken dat deze in het voordeel van de eigen zijde uitvalt (2004: 39). Het atoombombardement op Hiroshima en Nagasaki is volgens Walzer een voorbeeld van zo'n partijdige utilitaristische afweging die 'the rules of war and the rights they are designed to protect' zouden moeten hebben gestopt (1992: 263-8). Anderzijds verwachten we dat de principes van de rechtvaardige oorlog het oorlogsleed beperken, en volgens sommigen ligt juist in dat nut, en niet in die rechten, de rationale van de traditie van de rechtvaardige oorlog. Politici

3. Toepasbaarheid van de principes van proportionaliteit en discriminatie

De principes van de theorie van de rechtvaardige oorlog reguleren zowel *wanneer* er oorlog mag worden gevoerd (*jus ad bellum*) als *hoe* die oorlog moet worden gevoerd (*jus in bello*). De meeste pleitbezorgers van de traditie van de rechtvaardige oorlog menen dat deze principes voldoende algemeen zijn om ook antwoord te hebben op moderne vraagstukken (zie bijvoorbeeld Beard 2013; Taddeo 2012: 214; zie voor een andere mening Dipert 2010), terwijl ook aard en ernst van de gevolgen van cyberaanvallen voldoende ernstig zijn om de principes van de traditie toe te passen (zie ook Finlay 2018; Lucas 2017; Sleat 2017).[5] Binnen de theorie van de rechtvaardige oorlog is er, in lijn met wat in de inleiding van dit artikel is betoogd, bovendien een tendens om van de klassieke omschrijving van oorlog af te stappen, en in plaats daarvan een omschrijving te hanteren die ook veel kleinschaligere en weinig intensieve conflicten omvat (Finlay 2018: 360).

Het *jus in bello* is hier de interessantste categorie. Als we cyberoorlog zien als irreguliere oorlogvoering zonder duidelijk begin of einde is de vraag naar *ad bellum* rechtvaardigheid weliswaar relevant omdat het ons in staat stelt om een uitspraak te doen over de rechtvaardigheid van die oorlog, maar tegelijkertijd zonder veel praktische consequenties. De twee principes van dat *jus in bello* zijn het discriminatiebeginsel en het proportionaliteitsbeginsel.[6] Het eerste waarborgt de immuniteit van burgers en stelt dat onschuldige burgers nooit het beoogde doel van een aanval mogen zijn. Het tweede principe is dat onbedoelde burgerslachtoffers als nevenschade alleen zijn gerechtvaardigd als die schade proportioneel is: het (verwachte) aantal burgerslachtoffers als gevolg van een legitieme aanval op een militair doel moet in verhouding staan tot de (verwachte) militaire opbrengsten. Beide principes stellen daarmee de bescherming van burgers centraal.

en militairen onderschrijven een aantal basisprincipes – en proberen die ook bij militairen op de grond te internaliseren – omdat die het menselijk lijden beperken, en nemen op de koop toe dat soldaten die principes ook volgen in het enkele geval dat dat niet goed uitpakt (Shaw 2016). Daarnaast hebben bepaalde principes uit de traditie, zoals de proportionaliteitsvereiste en het beginsel dat ook een zelfverdedigingsoorlog alleen mag worden gevoerd als er een kans op succes is, sowieso een utilitaristische achtergrond.

5 Een aantal revisionisten denkt daar anders over, maar wijst eerder op het niet-statelijke karakter van moderne conflicten dan op de opkomst van moderne wapensystemen.

6 Sommige auteurs onderscheiden nog een derde principe: militaire noodzaak. Dit houdt in dat een aanval alleen is toegestaan als het de overwinning dichterbij brengt.

Het voornaamste argument om beide principes van toepassing te verklaren is dat er geen goede redenen zijn om dat *niet* te doen: zowel proportionaliteit en discriminatie zijn zonder al te veel duwen en trekken toe te passen op de cyberaanvallen die we tot nu toe hebben gezien. Nemen we bijvoorbeeld de aanval met de Stuxnet worm, dan is er niets vreemds of kunstmatigs aan de vraag of de aanval de immuniteit van burgers respecteerde en of eventuele voorziene nevenschade aan burgers proportioneel was in het licht van wat de aanval wilde bereiken – op beide vragen valt een duidelijk antwoord te geven, en dat luidt in dit geval overigens bevestigend. Bovendien brengt toepassing van deze principes ook daadwerkelijk inzicht in wat we moeten verdragen en wat niet: de traditie van de rechtvaardige oorlog (en het recht dat daaraan ontspringt) schrijft voor dat cyberaanvallen zich dienen te beperken tot militaire doelen, zoals wapen- of communicatiesystemen (zie ook Dipert 2010). Doemscenario's over cyberoorlog schetsen vaak aanvallen op voor de samenleving vitale infrastructuur, maar juist die zijn niet geoorloofd.

Nu is in veel hedendaagse conflicten het onderscheid tussen strijders en niet-strijders soms moeilijk te maken, bijvoorbeeld omdat de eersten geen uniform dragen en zich regelmatig onder de burgerbevolking begeven. Maar het onderscheid tussen militaire en civiele doelen is juist bij cyberaanvallen vaak redelijk eenduidig (zie Rowe 2016 en Taddeo 2012 voor een andere mening). Nu zullen er ongetwijfeld situaties blijven waarin het verschil wel lastig valt te maken, maar het echte probleem is dat men zich aan dat onderscheid weinig gelegen laat liggen: veel cyberaanvallen zijn er juist op gericht het leven van burgers lastig te maken, of het vertrouwen van diezelfde burgers in hun politici te ondermijnen. Voorbeelden zijn DoS aanvallen (zoals op Estse banken, overheidsinstellingen en media in 2007), het verspreiden van desinformatie (bijvoorbeeld om verkiezingen te beïnvloeden), en het stelen van persoonsgegevens (zoals van Amerikaanse ambtenaren in 2005 door waarschijnlijk China). Net als terrorisme vormen zulke aanvallen op burgerdoelen een flagrante schending van het discriminatiebeginsel dat burgers van aanvallen zou moeten vrijwaren.

We kunnen dit zelfs nog wat aanscherpen: Michael Walzer heeft erop gewezen dat de eis dat burgerslachtoffers onbedoeld en in aantal proportioneel moeten zijn, voor politieke en militaire beslissers nog geen verplichting schept het aantal burgerslachtoffers zoveel mogelijk te beperken. Walzer stelt daarom een additioneel 'due care' principe voor: militaire planners moeten actief hun best doen onbedoelde burgerslachtoffers te vermijden, ook als dit meer risico voor de eigen militairen met zich meebrengt (1992: 156, 319). Een voorbeeld uit de reguliere oorlogsvoering is het

inzetten van grondtroepen in plaats van een aanval uit de lucht. Maar ook voor cyberaanvallen is dit 'due care' principe relevant: zeker bij het ontwikkelen van, bijvoorbeeld, een virus dat als oogmerk heeft militair relevante infrastructuur lam te leggen, kan de nevenschade die dat virus elders aanricht aanzienlijk zijn. De voor Iran bedoelde Stuxnet worm 'ontsnapte' en verspreidde zich naar onder andere Indonesië en India (Miller 2015: 231). Zonder daar overigens schade aan te richten: de worm was zo ontworpen dat het alleen een specifiek model kerncentrifuge onklaar maakte – maar duidelijk is dat de gevolgen van een slordiger ontworpen virus verstrekkend kunnen zijn (zie ook Rowe 2018).

Er zijn, kortom, goede redenen om cyberaanvallen te leggen langs de maatstaf van de rechtvaardige oorlog: cyberoorlog is een vorm van (irreguliere) oorlog, en toepassing van de principes discriminatie en proportionaliteit kunnen de schade daarvan beperken. Overigens zijn westerse landen die relevante delen van die traditie op cyberoorlog van toepassing verklaren daar wel vooral ook zelf aan gehouden – ook als, zeg, Rusland of China zich er weinig aan gelegen laten liggen. Cyberaanvallen zijn vaak het wapen van de zwakkere, en in het licht van de Amerikaanse militaire dominantie is iedere partij dat – China en Rusland incluis (zie ook Lucas 2017, 24). Sommige landen zullen in die asymmetrie een rechtvaardiging vinden voor het gebruik van cyberaanvallen, ook op burgerdoelen. Staten en soldaten die de bovenliggende partij uitmaken verwerven geen extra ruimte als de tegenstander zich niet aan de regels houdt. Dat 'de ander' het toch ook 'doet' legitimeert de eigen misstappen niet.

4. Cyberkrijgers en de militaire professie

Nu wordt reguliere militairen door middel van gedragscodes en ethiekonderwijs met redelijk succes ingeprent zich correct te gedragen en burgers te ontzien, en in die zin maakt dat goede gedrag deel uit van hun professionele militaire ethiek. De vraag is in hoeverre die ethiek zich laat vertalen naar het digitale domein. Clausewitz' idee dat beperkingen wezensvreemd zijn aan oorlog is weliswaar een simplificatie, maar roept wel de vraag op of en hoe zo'n cyberoorlog zich überhaupt laat reguleren. Want als cyberoorlog oorlog is, zijn cyberstrijders dan ook echt krijgers – of *warriors*, zoals ze in het Engelse taalgebied steeds vaker worden genoemd? En zo ja, welke martiale deugden moeten deze strijders dan zoal bezitten, en kan er zoiets als een erecode voor cyberkrijgers bestaan? Die vragen zijn niet zomaar te beantwoorden. Veel cyberstrijders zijn weliswaar in dienst van de staat maar

niet noodzakelijk militair, en houden zich niet bezig met de toepassing van fysiek geweld – en dat laatste is nu net wel datgene wat zogeheten *warrior codes* in goede banen proberen te leiden (Beard 2016). Tot slot zijn cybersoldaten normaliter ook geen object van geweld; zij voeren hun strijd vanuit de relatieve veiligheid van zolderkamer, kantoortuin of defensiekazerne.[7]

Cybersoldaten zijn in dat laatste opzicht wel vergelijkbaar met dronepiloten; beide groepen lopen geen fysieke risico's. Hun groeiende rol past in een ontwikkeling die begon met (kruis)boog en katapult, en waarbij de afstand – fysiek, maar ook psychologisch – tot het gevechtsveld steeds verder toeneemt. Hoewel in oorlog, kunnen cybersoldaten en dronepiloten na het werk naar huis. Politicoloog Peter W. Singer beschrijft hoe piloten van onbemande vliegtuigen iedere relatie met de oorlogswerkelijkheid verliezen: Amerikaanse drone piloten dragen weliswaar een vliegpak, maar verlaten ondertussen de controlekamer in Nevada nooit (2009). De vraag is of dit de drempel om geweld te gebruiken niet verlaagt – je zou kunnen stellen dat de toenemende afstand het dehumaniseren van de tegenstander overbodig maakt (Lifton 1973). Maar het is ook de vraag wat het uitbannen van risico betekent voor de militaire professie. In de beeldvorming is de bereidheid risico's te lopen sterk verbonden met het militaire beroep. Boog, katapult en vuurwapen zijn in het verleden als het wapen voor lafaards afgedaan (maar uiteindelijk altijd omarmd); het bedienen van drones of plegen van cyberaanvallen vergt al even weinig fysieke moed. Desalniettemin is er met name in de Verenigde Staten een toenemende politieke bereidheid ook dronepiloten in aanmerking te laten komen voor dapperheidsonderscheidingen, voornamelijk gebaseerd op het argument dat zij psychologisch belastend werk doen waarbij zij onder tijdsdruk de (moreel) juiste beslissing moeten nemen al dan niet geweld te gebruiken. Die discussie over moed zullen we over cyberstrijders in dienst van defensie wellicht ooit ook moeten voeren.

In een ander opzicht verschilt het werk van drone piloten wel met dat van cybersoldaten. De schaduwzijde van vechten op afstand is dat de kans op burgerslachtoffers soms toeneemt, hoeveel men ook doet om dat te vermijden. Maar waar men het gebruik van onbemande wapensystemen kan zien als een vorm van risktransfer – het verplaatsen van de risico's van de westerse militairen naar de lokale bevolking (Shaw 2005) – is cyberoorlog

7 Singer (2009) stelt dat je een drone piloot in Nevada die deelneemt aan een oorlog volgens het internationaal recht als lid van een krijgsmacht strikt genomen in de straten van San Francisco mag aanvallen. Naar analogie is een cybersoldaat die werkt voor een krijgsmacht ook een legitiem doelwit in zijn of haar kantoortuin. Alleen geestelijken en militaire artsen en verpleegkundigen vormen een uitzondering op deze regel.

dat duidelijk *niet*.[8] Ook in het land of organisatie waarop de aanval zich richt, zijn normaliter geen slachtoffers met schade aan lijf of leden. Cybersoldaten die treinen doen ontsporen of vliegtuigen zich in gebouwen laten boren bestaan tot nu toe alleen in de verbeelding, en alles wijst erop dat dat voorlopig wel zo blijft (zie ook Lucas 2017). Sterker nog, als onderdeel van een traditionele oorlog kunnen cyberaanvallen het bloedvergieten in theorie zelfs inperken, als we ervan uitgaan dat het onklaar maken van militaire systemen eerder mensenlevens spaart dan kost. Daarmee valt op het eerste gezicht de ratio van militaire gedragscodes voor cybersoldaten goeddeels weg: die zijn voornamelijk bedoeld om het geweldgebruik van militairen te reguleren. Maar zoals we in de vorige paragraaf zagen, is ook de schade voor burgers die cyberaanvallen kunnen aanrichten – financieel, moreel, en institutioneel – wel degelijk 'echt,' en zij die cyberaanvallen initiëren of uitvoeren moeten proberen die schade zoveel mogelijk te beperken. Het is de vraag hoe we cybersoldaten in staatsdienst daarvan kunnen overtuigen.

Kijken we naar de traditionele deugdenlijstjes die krijgsmachten hanteren, dan staan daar met name (voornamelijk functionele) deugden op als moed en loyaliteit; niet per se deugden waar een cybersoldaat mee uit de voeten kan. Hoewel lastig is aan te geven welke deugden dan wel moreel relevant zijn voor cybersoldaten, hebben zij gezien de aard van het werk in ieder geval morele moed nodig: de bereidheid de eigen reputatie en carrière voor een hoger doel op het spel te zetten. Het gaat daarbij bijvoorbeeld om het weigeren van opdrachten die manifest illegaal of in strijd met de principes van de rechtvaardige oorlog zijn, of het naar buiten brengen van evidente misstanden. NSA klokkenluider Edward Snowden is mogelijk een voorbeeld van dat laatste, al is er discussie of zijn acties (anders dan zijn intenties) nu echt wel zo moreel zijn (zie bijvoorbeeld Lucas 2017 voor een tegengeluid). Groepsdruk en loyaliteit aan de organisatie maken dat morele moed voor militairen van oudsher een lastige categorie is. Voor cybersoldaten, die normaliter in mindere mate in de krijgsmacht zijn gesocialiseerd en minder aan groepsprocessen onderworpen zijn, zouden die belemmeringen overigens weleens een kleinere rol kunnen spelen.

Een probleem dat moreel handelen voor cybersoldaten juist wel bemoeilijkt is dat van de 'vele handen': in de moderne oorlogsvoering selecteert de een de doelen en wapens, waarna een ander op de knop drukt, daarbij regels en procedures volgend die een derde heeft bedacht. Er is niet alleen weinig ruimte voor een individuele militair om morele afwegingen

8 Het is overigens onduidelijk of de inzet van drones daadwerkelijk leidt tot meer burgerdoden.

te maken; het is ook lastig aan te geven wie verantwoordelijk is als het misgaat. Bovendien *voelt* niemand zich verantwoordelijk als ergens veel mensen bij betrokken zijn – het *bystander* effect dat verklaart waarom een drenkeling minder overlevingskansen heeft naarmate er meer mensen aan de kant staan. Deze problemen zijn inherent aan genetwerkt optreden (waarbij meer informatie over meer mensen wordt gespreid en daarmee de verantwoordelijkheid meestal ook) en doen zich extra nadrukkelijk voor in het digitale domein. Hoewel in de beeldvorming de eenzame hacker vanuit een zolderkamer de digitale infrastructuur van een land kan platleggen, vergt in de echte wereld een cyberaanval de gecoördineerde inspanning van velen (zie ook Lucas 2017), waardoor de ervaren verantwoordelijkheid allicht verwatert. De principieel gekozen dan wel door de situatie gecreëerde anonimiteit van cyberaanvallers helpt daarbij niet. Overigens mogen we de lat voor cybersoldaten desalniettemin best hoog leggen: hoewel zij te maken hebben met een aantal factoren die onethisch gedrag in de hand kunnen werken (geografische en psychologische afstand, relatieve anonimiteit, en over veel mensen gespreide verantwoordelijkheid), hebben zij niet of minder te maken met de veel sterkere krachten die bij reguliere soldaten normvervaging in de hand werken, zoals chaos, slaaptekort, gevaar, groepsdruk en slachtoffers onder nabije collega's.

Ondanks het goeddeels ontbreken van normvervagende factoren, richten cyberaanvallen zich regelmatig op burgerdoelen en voldoen daarmee niet aan de normen van het oorlogsrecht en de traditie van de rechtvaardige oorlog (Lucas 2017: 26). Net zoals bij terrorisme en de eerder beschreven middeleeuwse chevauchées is normloosheid daarbij een weloverwogen keuze die een duidelijk doel dient. Nu kiezen westerse krijgsmachten er tegenwoordig even weloverwogen voor militairen aan duidelijke normen te houden, maar de motieven daarvoor zijn meer functioneel dan moreel: in veel hedendaagse conflicten draait het om het winnen van *hearts and minds*, en dat gaat nu eenmaal beter wanneer je de lokale bevolking correct behandelt. Mede op basis van deze functionele argumenten laten westerse militairen burgers in de regel ongemoeid – normschendingen op middeleeuwse schaal zijn goeddeels uitgebannen. In het cyberdomein geldt dat níet. Het nadeel van functionele argumenten voor ethisch gedrag is dat zij hun kracht verliezen wanneer het aantoonbaar effectiever is om *niet* ethisch op te treden. Dat laatste is bij cyberaanvallen het geval: veel cyberaanvallen richten zich erop *hearts and minds* in een ander land te vervreemden van de overheid van dat land, door aanvallen te plegen waarvan voornamelijk de burgers van dat land hinder ondervinden – inderdaad vergelijkbaar met de middeleeuwse chevauchées.

5. Conclusie

Machiavelli meende dat er weinig is veranderd sinds de antieken, en dat iedere politicus of militair er goed aan doet zijn of haar licht bij hen op te steken. Immers, zo schrijft hij in zijn *Discorsi*, 'alle dingen die wanneer ook gebeuren in de wereld, hebben een parallel in de oude tijden.' De wijze waarop men oorlog voert, was volgens de Florentijn bijvoorbeeld niet aan grote veranderingen onderhevig geweest. Dit bracht Machiavelli ertoe de rol van het vuurwapen – niet veel meer dan een verbeterde versie van de katapult volgens hem – te bagatelliseren. Dat was een vergissing: de opkomst van het vuurwapen bleek voor de oorlogsvoering bijna even ingrijpend als de uitvinding van de stijgbeugel zo'n duizend jaar eerder. De traditie van de rechtvaardige oorlog bleek tegen al die veranderingen overigens prima bestand. Die traditie verbiedt gerichte aanvallen op burgers, en staat alleen onbedoelde schade toe die proportioneel is aan het doel. Dit zijn de principes van discriminatie en proportionaliteit, en hierboven is betoogd dat beide zich goed laten vertalen naar het cyberdomein. Concreet betekent dit dat cyberaanvallen zich moeten richten op militaire doelen, en dat militaire planners, software ontwikkelaars en cybersoldaten zich moeten inspannen eventuele nevenschade zoveel mogelijk te beperken. Dat de naleving van deze principes veel te wensen over laat, doet aan hun geldigheid niets af.

Wat die gebrekkige naleving betreft is het opvallend dat we bij cyberaanvallen meer accepteren dan in traditionele oorlogvoering – morele verontwaardiging over cyberaanvallen op civiele doelen blijft doorgaans beperkt. Nu is dat gezien het ontbreken van doden en gewonden verklaarbaar, maar gerechtvaardigd zijn aanvallen op burgers (waarbij de schade voor burgers het doel is en geen onbedoeld bijeffect) nooit, en verstandig is een lankmoedige houding al helemaal niet. Juist omdat de normen voor wat betreft cyberconflicten zich nog aan het vormen zijn, kan een toegeeflijke houding nu later kostbaar blijken. Het belangrijkste dat we van de traditie van de rechtvaardige oorlog kunnen overnemen zijn niet concrete principes en concepten, ook al laten die zich goed naar het cyberdomein vertalen, maar het idee dat we in morele termen over cyberconflicten kunnen spreken, en dat cyberspace niet een natuurstaat is waarin alles is geoorloofd. Als oorlog een gereguleerde activiteit is, kan cyberoorlog dat ook zijn. Dat veronderstelt wel dat we cyberoorlog als oorlog zien – ook al is het geen oorlog in de klassieke zin – en niet als een vorm van spionage plus (zie ook Lucas 2017).

De redenering dat door staten geïnitieerde cyberaanvallen 'nu eenmaal niet tegen zijn te houden' gaat niet op: de geschiedenis laat bijvoorbeeld

zien dat tal van wapens (van dumdum kogels tot chemische wapens) zijn uitgebannen of gereguleerd, en meestal om goede redenen. Jammer genoeg gebeurt dat soms rijkelijk laat, omdat wet- en regelgeving doorgaans een paar stappen achter de feiten aanlopen.[9] Op dit moment zwijgt het oorlogsrecht en de traditie van de rechtvaardige oorlog nog goeddeels over de ontwikkelingen op het gebied van de inzet van computers als wapen, terwijl hier wel degelijk kwesties liggen.[10] Wie dit soort vraagstukken links laat liggen is als de spreekwoordelijke generaal die zich voorbereidt op de vorige oorlog.

Bibliografie

Arquilla, J. (2012) Cyberwar Is Already Upon Us – But can it be controlled?, *Foreign Policy*, 27 februari.

Beard, M. (2013) Cyberwar and just war theory, *Applied Ethics, Risk, Justice and Liberty*. Edited by the Centre for Applied Ethics and Philosophy, Hokkaido: Hokkaido University Press, Centre for Applied Ethics and Philosophy, pp. 1-12.

Beard, M. (2016) The Code of the Cyber-warrior, in: F. Allhoff, B.J. Strawser en A. Henschke (red.), *Binary Bullets: The Ethics of Cyberwar*. New York: Oxford University Press.

Clausewitz, C. von (2000) *Over de Oorlog*. 's-Hertogenbosch: Voltaire.

Cook, M.L. (2004) *The Moral Warrior: Ethics and Service in the U.S. Military*. Albany: State University of New York Press.

Dipert, R.R. (2010) The Ethics of Cyberwarfare, *Journal of Military Ethics* **9** (4), pp. 384-410.

Finlay, C.J. (2018) Just War, Cyber War, and the Concept of Violence, *Philosophy & Technology* **31** (3), pp. 357-377.

Gibson, W. (1984) *Neuromancer*. New York: Ace.

Goldman, J. (red.) (2009) *The Ethics of Spying: A Reader for Intelligence Professionals*, vol. 2. Lanham: Scarecrow Press.

Lee, P. (2012) Remoteness, Risk and Aircrew Ethos, *Air Power Review* **15** (1), pp. 1-19.

Lifton, R.J. (1973) *Home from the war: Vietnam veterans: Neither victims nor executioners*. New York: Other Press.

Lucas, G. (2017) *Ethics and Cyber Warfare. The Quest for Responsible Security in the Age of Digital Warfare*. Oxford: Oxford University Press.

Lynn, J.A. (2003) *Battle. A History of Combat and Culture*. Boulder Colorado, Westview Press.

Machiavelli, N. (1997) *Discorsi. Gedachten over staat en politiek*. Amsterdam: Ambo.

9 Dat laatste lijkt nu bijvoorbeeld het geval te zijn bij autonome wapensystemen: de technologische ontwikkelingen op dat gebied gaan een stuk sneller dan de regulering ervan.

10 Een uitzondering vormt de *Tallinn Manual on the International Law Applicable to Cyber Warfare*, die uiteenzet op welke wijze het internationaal recht van toepassing is op cyberoorlog (Schmitt et al. 2013). Bindend is dit alles *niet*, en vooral buiten de NATO zal de impact beperkt zijn (zie ook Lucas 2017).

Miller, S. (2015) Cyber-Attacks and 'Dirty Hands': Cyberwar, Cyber-Crimes or Covert Political Action?, in F. Allhoff, B.J. Strawser en A. Henschke (red.), *Binary Bullets: The Ethics of Cyberwar*. New York: Oxford University Press.

Rid, T. (2012) Cyber War Will Not Take Place, *Journal of Strategic Studies* **35** (1), pp. 5-32.

Rowe, N.C. (2017) Challenges of Civilian Distinction in Cyberwarfare, in: M. Taddeo en L. Glorioso (red.), *Ethics and Policies for Cyber Warfare: A NATO Cooperative Cyber Defence Centre of Excellence Initiative, Philosophical Studies Series*, vol. 124. New York: Springer, pp. 33-48.

Rowe, N.C. (2018) Taxonomy of Norms in Cyber conflict for Government Policymakers, *Journal of Information Warfare* **17** (1).

Schmitt, M. et al. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press.

Shaw, M. (2005) *The New Western Way of War*. Cambridge: Polity Press.

Shaw, W.H. (2016) *Utilitarianism and the Ethics of War*. London en New York: Routledge.

Singer, P.W. (2009) *Wired For War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Books.

Sleat, M. (2018) Just cyber war?: Casus belli, information ethics, and the human perspective, *Review of International Studies* **44** (2), pp. 324-342.

Taddeo, M. (2012) An analysis for a just cyber warfare, in: *Cyber conflict 4th international conference on Cyber Conflict* (*CYCON*), pp. 209-218.

Walzer, M. (1992) *Just and Unjust Wars* (New York: Basic Books)

Walzer, M. (2004) *Arguing about War* (New Haven and London: Yale University Press)

Whetham, D. (2016) Cyber Chevauchées: Cyber War Can Happen, in: F. Allhoff, B.J. Strawser en A. Henschke (red.), *Binary Bullets: The Ethics of Cyberwar*. New York: Oxford University Press.

Wolfendale, J. (2009) The Myth of Torture Lite, *Ethics & International Affairs* **23** (1), pp. 47-61.

Over de auteur

Peter Olsthoorn is universitair hoofddocent militair leiderschap en ethiek aan de Nederlandse Defensieacademie. Zijn onderzoek richt zich onder meer op militaire deugden, militaire ethiekeducatie en de ethiek van grensbewaking. Hij schreef onder andere *Honor in Political and Moral Philosophy* (State University of New York Press, 2015) en *Military Ethics and Virtues: An Interdisciplinary Approach for the 21st Century* (Routledge, 2010).