Keyboard warrior of cyber-combattant?

De gevolgen van deelname aan online oorlogvoering in het conflict tussen Rusland en Oekraïne

Arjen Vermeer & Kraesten Arnold[1]

Na de Russische inval in Oekraïne vroeg de Oekraïense vicepremier Federov aan IT-experts wereldwijd om zich aan te sluiten bij zijn zojuist opgerichte *IT Army*. Het nationale recht is helder over de status van buitenlandse strijders in dienst van andere landen. Maar is de status van *digitale* strijders die cyberaanvallen uitvoeren net zo duidelijk? Kun je als Nederlander zomaar deelnemen aan gevechtshandelingen in de digitale oorlogsomgeving? Maakt jou dat een legitiem doelwit? Mag je zomaar hacken? In hoeverre geldt het humanitair oorlogsrecht in cyberspace? Ben je als hacker combattant? Dit artikel gaat in op de gevolgen van deelname aan online oorlogvoering door digitale strijders.

Op 24 februari 2022 openbaarde de Oekraïense vicepremier Mykhailo Federov, tevens minister van digitale transformatie, dat hij een 'IT-leger' had opgericht om zijn land te beschermen tegen Russische digitale aanvallen. Hij riep IT-specialisten wereldwijd op om zich aan te sluiten bij dit *IT-Army of Ukraine* (hierna IT-Army),[2] een 'virtuele organisatie' waarvan de leden online met elkaar communiceren via sociale netwerken en chatrooms. Volgens de Oekraïense overheid omvatte het IT-leger in maart 2022 al enkele honderdduizenden digitale strijders.[3] Hoewel initieel bedoeld om de Oekraïense digitale infrastructuur te beschermen, kreeg het IT-leger ook offensieve taken. Ook Nederlandse vrijwilligers sloten zich aan.[4] Een Nederlandse oud-militair, inmiddels gepromoveerd tot 'kolonel van het Oekraïense ICT-leger', lijkt intensief betrokken bij de cyberoorlog tussen Oekraïne en Rusland.[5]

Het IT-leger is een hybride gezelschap: civiel noch militair; van de overheid, noch particulier; lokaal, noch internationaal; niet rechtmatig, maar ook niet onrechtmatig.[6] Federov riep een bonte verzameling softwareprogrammeurs, techneuten, patriottische, activistische en ethische hackers en andere geïnteresseerden op om Russische overheidswebsites, banken en bedrijven aan te vallen.[7] Een soort '*crowd-hacking*' door een collectief van digitale soldaten en parttime virtuele verzetsstrijders. Iedereen met hart voor de Oekraïense zaak, een computer en een netwerkverbinding kon zich aansluiten bij dit IT-vreemdelingenlegioen. Ervaring met hacken was gewenst, maar niet noodzakelijk. Lijsten met doelwitten (vooral Russische overheidswebsites, mediakanalen en staatsbedrijven), bijbehorende handleidingen, aanvalsinstructies en benodigde softwaretools werden online aangeboden.

Iedereen met hart voor de Oekraïense zaak, een computer en een netwerkverbinding kon zich aansluiten bij dit IT-vreemdelingenlegioen

Het humanitair oorlogsrecht (HOR) of *ius in bello* is helder over de status van buitenlandse strijders die, in krijgsdienst van een ander land, deelnemen aan de gewapende strijd. Het HOR beschrijft en begrenst de manieren en middelen van oorlog voeren. Ook beschermt dit recht mensen die niet (meer) deelnemen aan de gewapende strijd, zoals gewonde soldaten, krijgsgevangenen of burgers. Het Internationale Rode Kruis waarschuwde dat er onduidelijkheid bestaat – een '*legal grey area*' – over de status van mensen die digitaal en op afstand deelnemen aan een militair conflict. Deze waarschuwing was voor de

Oekraïense regering aanleiding om een wet te ontwerpen die een eind moet maken aan deze onduidelijkheid, door de formele integratie van het IT-Army in de *Cyber Reserve Force* van het Oekraïense Ministerie van Defensie.[8] Inhoudelijk is vooralsnog niet veel bekend over die nieuwe wet.

Met dit artikel willen we inzicht verschaffen in de onduidelijkheid rond de status van mensen die digitaal en op afstand deelnemen aan een gewapend conflict. Het artikel start met een uitleg van hetgeen onder hacken wordt verstaan en in hoeverre dat strafbaar is gesteld. Dan volgt een korte introductie van het HOR, waarna we drie verschillende categorieën combattanten toelichten, respectievelijk reguliere en irreguliere combattanten en de *levée en masse*. Vervolgens gaan we in op de vier criteria waaraan een strijder moet voldoen om aanspraak te mogen maken op de speciale status van combattant, waarna we de consequenties van rechtstreekse deelname aan de strijd door burgers bespreken. We sluiten af met een conclusie.

Strafbaarheid van hacken

Onder het hacken van een computer of netwerk wordt verstaan: het uitbuiten van kwetsbaarheden en omzeilen van veiligheidsmaatregelen waardoor iemand, zonder de toestemming van de eigenaar of gebruiker, wederrechtelijk toegang krijgt tot die computer of dat netwerk. Dat kan bijvoorbeeld door iemands inloggegevens te achterhalen, of door het sturen van een mail met een computervirus. Zomaar een computer hacken is verboden. Eenieder die zonder toestemming van de eigenaar inbreekt in de computer, het account of netwerk van een ander, is in principe strafbaar. Er is dan sprake van computervredebreuk en dat is in Nederland – net als in vele andere landen – een misdrijf.[9]

Na de eigenlijke computerinbraak kan een hacker uiteenlopende vervolgacties uitvoeren; denk aan digitale spionage of data-diefstal. Een hacker kan ook de werking van hardware of software veranderen; gegevens wijzigen of ontoegankelijk maken, of zelfs compleet en onherstelbaar vernietigen. Ook dergelijke vervolgacties worden doorgaans beschouwd als 'hacken'.

Een eerste aanzet om computercriminaliteit internationaal aan te pakken, betrof de *Convention on Cybercrime* uit 2001.[10] Dit verdrag beoogt onder meer harmonisatie van nationale wetgevingen en bevordering van internationale samenwerking bij strafrechtelijke procedures inzake cybercriminaliteit. Geïnitieerd vanuit de Europese Unie is deze conventie voornamelijk door Westerse democratieën en gelijkgestemden getekend en geratificeerd. Nederland is partij bij dit verdrag sinds 2007. Om uiteenlopende redenen erkennen landen als China, India, Brazilië én Rusland deze conventie echter niet. Dat betekent niet dat Rusland het hacken van computersystemen binnen haar landsgrenzen zomaar toestaat. Ook daar is het wijzigen, blokkeren of vernietigen van computergegevens strafbaar gesteld.[11]

Als niet-statelijke actoren grensoverschrijdende cyberaanvallen uitvoeren, dan is de uitdaging om te bepalen in hoeverre een staat precies verantwoordelijk is voor cyberactiviteiten die vanaf haar territorium ontspringen. Vervolgens rijst de vraag in hoeverre een staat kan worden verplicht daartegen op te treden. Het Internationaal Gerechtshof (IGH) oordeelde dat een staat niet mag gedogen dat zijn territorium wordt gebruikt voor activiteiten die de rechten van andere landen schenden. Staten hebben de verplichting om, volgens internationaal recht illegitieme, activiteiten te voorkomen die ernstige schade veroorzaken aan objecten van een andere soevereine staat (*duty of prevention*).[12] De *Tallinn Manual* vertaalde dit principe naar cyberspace, door te stellen dat een staat niet mag toestaan dat zijn cyber-infrastructuur wordt gebruikt voor buitenwettelijke activiteiten tegen andere staten. In voorkomend geval moet de staat van waaruit de aanval op een andere staat plaatsvindt, actie ondernemen (*due diligence* principe).[13]

Staten mogen onrechtmatige, grensoverschrijdende cyberaanvallen niet oogluikend toestaan. De aanname is dat een staat precies weet wat zich afspeelt in cyberspace en bovendien volledige controle heeft over dergelijke activiteiten. Maar zelfs als een staat de (politieke) wil heeft

De aanname is dat een staat precies weet wat zich afspeelt in cyberspace en bovendien volledige controle heeft over dergelijke activiteiten

Auteurs

1. Mr. drs. A.Vermeer is als Universitair Docent verbonden aan de sectie Militair Recht van de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie te Breda. Lt-kol K.L. Arnold ESMD MSc is als (cyber)onderzoeker en docent verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie te Breda.

Noten

2. twitter.com/FedorovMykhailo/status/1497642156076511233
3. 'Ukraine's "IT army" has hundreds of thousands of hackers, Kyiv says', *Wall Street Journal*, 4 maart 2022, wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX.
4. Andrii Maidanyk, 'Cyberoorlog: Oekraïne houdt hulp hackers liever stil', *Computable* 20 juni 2022, computable.nl/artikel/columns/overheid/7368999/1509086/cyberoorlog-oekraine-houdt-hulp-hackers-liever-stil.html.
5. Huib Modderkolk, 'Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol', *de Volkskrant* 24 september 2022. volkskrant.nl/kijkverder/v/2022/een-internationaal-cyberleger-tegen-rusland-met-een-nederlander-in-de-hoofdrol~v580287/.
6. Stefan Soesanto, *The IT army of Ukraine: structure, tasking, and ecosystem*, Cyberdefense report, Zürich, juni 2022, p. 6.
7. t.me/itarmyofukraine2022/1%20or%20 https://archive.ph/SMt31.
8. Nataliya Tkachuk, Secretary of Ukraine's National Coordination Center for Cybersecurity, newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.
9. Art. 138 ab Sr.
10. *The Budapest Convention (ETS No. 185),* 23/11/2001. coe.int/en/web/cybercrime/the-budapest-convention?ref=hackernoon.com.
11. Art. 207(3), 272-274 Wetboek van Strafrecht, Russische Federatie.
12. Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace,* in: Ziolkowski (ed.) *Peacetime Regime for State Activities in Cyberspace*, 2013, p. 204.
13. Michael N. Schmitt (ed.), *Tallinn manual on the international law applicable to cyber warfare,* Cambridge University Press 2013, Rule 5, p. 26.

© Shutterstock

om actie te ondernemen, dan nog is het de vraag of die staat daadwerkelijk zijn 'nationale deel van cyberspace' kan overzien en invloed daarop kan uitoefenen. Een hoge mate van online anonimiteit, de moeilijkheid om cyberaanvallen snel en met zekerheid te attribueren, en de mogelijkheid om cyberaanvallen zelf, of de verantwoordelijkheid ervoor te ontkennen, bemoeilijken het optreden tegen grensoverschrijdende cyberaanvallen.

Introductie humanitair oorlogsrecht

Het HOR beoogt geweldsexcessen tijdens gewapende conflicten te beperken en een maatstaf te geven die een minimum aan humaniteit waarborgt. Het is van toepassing op het internationaal gewapend conflict tussen Rusland en Oekraïne.[14]

Het HOR verbiedt niet uitdrukkelijk de deelname aan vijandelijkheden door wie dan ook. Een combattant als onderdeel van de krijgsmacht van een land mag deelnemen aan de strijd en daarbij ook (dodelijk) geweld gebruiken tegen vijandelijke deelnemers en andere legitieme doelen, zonder dat die deelname kan worden bestraft. Dit 'combattanten-privilege' geldt echter niet voor burgers die deelnemen aan de vijandelijkheden. De status die een persoon heeft (combattant of burger) bepaalt de mate van bescherming van een deelnemer aan een gewapend conflict. Een combattant is, zolang hij deelneemt aan het gewapend conflict, een legitiem doelwit voor de tegenstander. Een burger die zich afzijdig houdt van die gewapende strijd, is geen legitiem doelwit. Hoewel de status van deelnemers ook in de fysieke wereld soms vragen oproept, zijn deze vragen nog pertinenter in de digitale wereld. Het kwalificeren van de deelnemers aan het IT-Army is daarom niet eenvoudig. We proberen deze situatie te duiden door verschillende categorieën deelnemers te analyseren en te bezien of een of meerdere van toepassing is/zijn op deelnemers aan het IT-Army; en onder welke voorwaarden.

De combattant

De reguliere combattant

De reguliere combattant maakt deel uit van de krijgsmacht van een partij bij een internationaal gewapend conflict.[15] Aan deze combattant wordt ook het krijgsgevangenschap verleend wanneer hij in handen van de vijand valt.[16] Nationaal recht regelt wie deel uitmaakt van de nationale krijgsmacht.[17]

Een Oekraïens Presidentieel decreet maakt mogelijk dat Nederlanders (en alle andere niet-Oekraïners) zich kunnen aanmelden bij de krijgsmacht van Oekraïne.[18] Als niet-Oekraïners zich onder dit decreet aansluiten bij het Oekraïense vreemdelingenlegioen (*International Legion of Territorial Defence of Ukraine)*, dan worden zij deel van de Oekraïense krijgsmacht en daarmee combattant. Op grond van die status mogen zij rechtstreeks deelnemen aan de strijd,[19] dat wil zeggen: zij mogen offensieve en defensieve operaties uitvoeren binnen de grenzen van het HOR, zonder daarvoor te worden vervolgd. Bij gevangenneming hebben zij recht op krijgsgevangenschap.[20] Opmerkelijk genoeg heeft Rusland aangegeven deze niet-Oekraïense leden van de Oekraïense krijgsmacht niet te zien als combattanten en in voorkomend geval niet als krijgsgevangenen te behandelen.[21] In lijn hiermee is te verwachten dat Rusland niet-Oekraïense *cybersoldaten* die zich onder het Presidentieel decreet aansluiten bij het IT-Army, evenmin als combattant ziet.

Leden van het IT-Army vallen *niet* onder het Oekraïens Presidentieel decreet en kwalificeren daarom *niet* als reguliere combattant

Hackers kunnen als 'cybersoldaat' onderdeel uitmaken van een nationale krijgsmacht. Denk bijvoorbeeld aan de hackers van het Nederlandse Defensie Cyber Commando. Echter, leden van het IT-Army vallen *niet* onder het Oekraïens Presidentieel decreet en kwalificeren daarom *niet* als reguliere combattant. Vooralsnog is onbekend of voornoemde, in ontwikkeling zijnde, wet inzake de formele integratie van het IT-Army in de Oekraïense *Cyber Reserve Force* hierin verandering brengt; en voor wie die wet zal gelden (Oekraïners en/of niet-Oekraïners).

De irreguliere combattant

Een andere relevante categorie die in aanmerking komt voor de status van combattant (inclusief geweldsprivilege en bescherming bij krijgsgevangenschap), betreft 'leden van andere militiën en leden van andere vrijwilligerskorpsen, met inbegrip van die van georganiseerde verzetsgroepen, behorend tot een Partij bij het conflict', ook als zij vechten tegen een bezetter.[22] Er is sprake van 'behoren tot een Partij bij het conflict' als de groep vecht namens de Partij bij het conflict en die Partij deze gevechtsfunctie van de groep accepteert.[23] Het gaat hier om een feitelijke relatie tussen de Partij en de groep, geen juridische.[24] Een bepaalde mate van controle over de groep door de Partij is niet vereist. *A contrario*, groepen of collectieven die cyberoperaties uitvoeren tegen een van de Partijen bij het conflict, om welke reden dan ook, maar zelf *niet* behoren tot een Partij bij het conflict, worden *niet* beschouwd als combattanten; zij genieten geen geweldsprivilege en aan hen wordt in voorkomend geval geen krijgsgevangenschap verleend.

Het IT-Army is een samengestelde groep bestaande uit (militair) personeel van de Oekraïense krijgsmacht en inlichtingendiensten, alsook civiele vrijwilligers uit binnen- en buitenland. De groep vecht voor en namens Oekraïne, dat de groep beschouwt als onderdeel van haar verdediging. De Oekraïense overheid levert *target lists* met doelwitten, stelt prioriteiten, levert aanvalsinstructies en bijbehorende software, en coördineert aanvalstijden om effecten van cyberaanvallen te optimaliseren.[25] Het IT-Army lijkt te voldoen aan het vereiste 'Partij bij het conflict'. Een tweede element vinden we impliciet in de definitie van deze categorie zelf. Het moet gaan om een georganiseerde, niet-statelijk gewapende groep individuen,[26] waarbij de groep collectief moet voldoen aan elk van de volgende criteria:

1. onder bevel staan van een persoon die verantwoordelijk is voor zijn ondergeschikten;
2. een vast en op enige afstand herkenbaar onderscheidingsteken hebben;
3. de wapens openlijk dragen;
4. zich in hun handelingen gedragen naar de wetten en gebruiken van de oorlog.[27]

Hieronder beschouwen we in hoeverre het IT-Army als groep voldoet aan elk van de vier criteria.

1e Criterium: bevelsverhouding

Het eerste criterium sluit met name digitaal ongeorganiseerde en zelfs losjes georganiseerde individuen uit van de (irreguliere) combattantenstatus. Dit element sluit nauw aan bij het vereiste dat er een bepaalde organisatiegraad van de groep moet zijn.[28] Volgens de Tallinn Manual maakt dat, in combinatie met het vereiste dat in zo´n organisatie disciplinair moet kunnen worden opgetreden, dat het hoogst onwaarschijnlijk is dat individuen die slechts digitaal georganiseerd zijn, voldoen aan het eerste criterium.[29] Het IT-Army is waarschijnlijk wel georganiseerd voor zover het Oekraïense militairen en inlichtingen-medewerkers betreft. Het is aannemelijk dat er een reguliere bevelsverhouding heerst en dat leidinggevenden verantwoordelijkheid dragen voor cyberoperaties in en tegen Rusland. Voor de Oekraïense civiele deelnemers die geen deel uitmaken van de strijdkrachten, alsook alle internationale vrijwillige cybersoldaten (burgers en/of militairen) ligt dit anders. Deze categorie is waarschijnlijk niet hiërarchisch georganiseerd en wordt vermoedelijk

14. Art. 2 Verdragen van Genève I-IV (1949). Zowel de Russische Federatie als Oekraïne zijn partij bij zowel deze verdragen als het Aanvullend Protocol I (1977).

15. Art. 4(A)(1) Verdrag van Genève III en art. 43(2) Aanvullend Protocol I. Militair medisch en religieus personeel die deel uitmaken van de krijgsmacht zijn echter geen combattant.

16. Art. 4(1) Verdrag van Genève III en art. 44(1) Aanvullend Protocol I.

17. Voor Nederland: art. 1, 1.a.1. Wet ambtenaren Defensie.

18. Presidentieel Decreet van Oekraïne, 10 juni 2016, 'Regulations on passing of military service in the Armed Forces of Ukraine foreigners and stateless persons', cis-legislation.com/document.fwx?rgn=86889#A4OO0GJ839.

19. Art. 43(2) Eerste Aanvullend Protocol (1977).

20. Art. 44(1) Eerste Aanvullend Protocol (1977).

21. Tass, *МО РФ: западные наемники на Украине не будут иметь права на статус военнопленного*, 3-3-2022, tass.ru/armiya-i-opk/13952419?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru.

22. Art. 4(A)(2) Derde Verdrag van Genève (1949).

23. Internationaal Comité van het Rode Kruis (ICRK), *Commentaar bij het Derde Verdrag van Genève* (2020), par. 1006.

24. ICRK, *Commentaar bij het Derde Verdrag van Genève* (1960), p. 57.

25. Soesanto, *The IT Army of Ukraine*, p. 8-12.

26. Hierbij wordt vaak verwezen naar de criteria die aangelegd zijn door de ICTY en ICTR ingeval van niet-Statelijk gewapende groepen. Bijvoorbeeld, *Prosecutor/Jean-Paul Akayesu* (Trial Judgment), ICTR-94-4-T, 2 september 1998, par. 626. Voor elementen die de vereiste organisatiegraad kunnen duiden, zie *Prosecutor/Ljube Boskoski and Johan Tarculovski* (Judgement), IT-04-82-T, 10 juli 2008, par. 199-203. De elementen die hierin worden aangegeven, zoals het hebben van een hoofdkwartier, het gebruik van uniformen en controle over grondgebied lenen zich echter moeilijk voor het digitale domein.

27. Art. 4(A)(2) Derde Verdrag van Genève (1949).

28. *Supra*, noot 16.

29. *Tallinn Manual 2.0*, p. 404-405.

niet aangestuurd onder volledige verantwoordelijkheid van de Oekraïense staat. De Oekraïense militairen en inlichtingen-medewerkers voldoen wel aan dit eerste criterium. Alle internationale vrijwillige cybersoldaten en de Oekraïense civiele deelnemers die geen deel uitmaken van de strijdkrachten voldoen echter *niet* aan dit eerste criterium en zij kwalificeren daardoor *niet* als irregulier combattant. De groep *als geheel* voldoet evenmin aan dit eerste criterium.

2e Criterium: onderscheidingstekens

Combattanten dienen zich (duidelijk) te onderscheiden van de burgerbevolking. In de traditionele militaire domeinen (land, zee en lucht) zijn combattanten door kleding en materieel ook op afstand doorgaans makkelijk te onderscheiden. In het cyberdomein daarentegen, zijn daders, hun locatie en digitale wapens, niet zomaar met het blote oog waarneembaar. Zelfs digitale schade is niet altijd (direct) zichtbaar.

Een inherent kenmerk van de virtuele cyberwereld betreft de hoge mate van anonimiteit van actoren. Anders dan 'echte personen en organisaties in de reële wereld' kent de digitale wereld louter virtuele identiteiten. Door die denkbeeldige identiteiten kan een aanvaller relatief gemakkelijk anoniem blijven, zichzelf anders voordoen, zich uitgeven voor iemand anders, optreden namens een ander of achterliggende intenties maskeren. Hoewel niet onmogelijk, zijn cyberoperaties vaak lastig, of soms helemaal niet, te traceren en/of te attribueren.

Zou een vast en op enige afstand herkenbaar onderscheidingsteken ook moeten gelden voor cyber-combattanten? Sommige Tallinn Manual experts zagen deze gewoonterechtelijke verplichting te allen tijde opgaan, dus ook voor cyber-combattanten die cyberaanvallen uitvoeren op grote afstand van hun militaire doelen.[30] Dit zou inhouden dat als een militaire hacker 'behorend tot een Partij bij het conflict' een digitale aanval uitvoert op een tegenstander, op het moment van de aanval *zelf*, als militair/combattant herkenbaar moet zijn. Ongeacht waar die aanvaller zich bevindt (bijvoorbeeld in een ander werelddeel). Zelfs als de effecten van die cyberaanval pas later optreden of zichtbaar worden. Dit zou een rigide interpretatie van het recht inhouden.

Andere deskundigen beargumenteerden dat de verplichting niet geldt wanneer combattanten zich bevinden op of in een militair doel (zoals een oorlogsschip of jachtvliegtuig). Een derde groep specialisten gaf aan dat de verplichting meer contextafhankelijk is. Dit betekent dat waar zo'n teken niet zou leiden tot een situatie waarin het onderscheid tussen combattanten en burgers redelijkerwijs niet meer te maken is, deze verplichting niet geldt. Aangezien cyberspace, in tegenstelling tot de andere domeinen, geen zichtbare of vastomlijnde grenzen heeft, doet deze contextafhankelijke insteek onzes inziens het meeste recht aan de karakteristieken van oorlog voeren in cyberspace. Een vast en op enige afstand herkenbaar onderscheidingsteken is voor het IT-Army als geheel dan niet vereist.

3e Criterium: wapens openlijk dragen

Het derde criterium betreft het openlijk dragen van wapens. Ook dit element volgt de discussie zoals hierboven weergegeven. De Tallinn Manual experts waren hier kort, maar krachtig over: zelfs als er al een definitie is van een cyberwapen, dan vindt dit element geen toepassing in het cyberdomein.[31] In tegenstelling tot tastbare en zichtbare, kinetische wapens bestaan cyberwapens namelijk uit virtuele, digitale computercode; ofwel voor het menselijk oog 'onzichtbare' wapens.

Als een wapen schuilgaat achter civiele gebruikers kunnen die civiele gebruikers enerzijds worden beschouwd als een – door het HOR verboden – menselijk schild. Bij tegenmaatregelen neemt de kans op nevenschade toe bij die civiele gebruiker. Wanneer de civiele gebruiker de laatst traceerbare schakel is, kan dit anderzijds ook leiden tot de conclusie dat deze daarmee een legitiem militair doelwit is. In beide gevallen druist het gebruik van cyberoperaties in tegen het beginsel van onderscheid.[32]

Aanvullend Protocol I (1977) is echter minder streng met dit vereiste en stelt dat wanneer het 'door de aard van de vijandelijkheden niet mogelijk is zich van de burgerbevolking te onderscheiden', dit criterium slechts geldt (a) gedurende ieder militair treffen, en (b) gedurende de tijd dat hij zichtbaar is voor de tegenpartij bij het betrekken van militaire posities, voorafgaande aan het inzetten van een aanval waaraan hij moet deelnemen.[33] Het openlijk dragen van cyberwapens geldt, naar de maatstaven van Aanvullend Protocol I en de Tallinn Manual, dus niet voor cybersoldaten.

4e Criterium: handelen naar gebruiken en wetten van oorlog

Het laatste criterium gaat over de naleving van het HOR. Voor de irreguliere combattanten is het duidelijk dat deze verplichting geldt voor de groep als geheel.[34] Echter, als de individuele irreguliere combattant zich niet houdt aan het HOR, dan verliest deze niet automatisch zijn combattantenstatus en de daaraan gekoppelde bescherming (krijgsgevangenschap). Het is echter niet geheel duidelijk of dit ook op deze manier van toepassing is op reguliere combattanten.[35]

De levée en masse

Naast de reguliere en de irreguliere combattant is er een derde, bijzondere categorie die in deze context het benoemen waard is, namelijk de *levée en masse*.[36] Het Derde Verdrag van Genève definieert een *levée en masse* als:

> 'de bevolking van een niet-bezet gebied die, bij het naderen van de vijand, uit eigen beweging de wapens opneemt om de invallende troepen te bestrijden, zonder tijd gehad te hebben zich tot geregelde gewapende eenheden te organiseren, mits zij de wapens openlijk draagt en de wetten en gebruiken van de oorlog eerbiedigt.'[37]

Hieronder valt ook de bevolking die, als onderdeel van de *levée en masse,* deelneemt aan het uitvoeren van cyberoperaties.[38] Deze categorie combattanten valt op om twee redenen. Allereerst geeft het Derde Verdrag het recht aan burgers om in gewapend verzet te komen en tegelijk geeft het die burgers de combattantenstatus, met bijbehorende rechten. Ten tweede hoeft deze catego-

rie combattanten niet te voldoen aan alle vier criteria voor die status.

Een voorwaarde waar een *levée en masse* wel aan moet voldoen, betreft 'de bevolking van een niet-bezet gebied die, bij het naderen van de vijand ...'. Voor de niet-Oekraïense cybersoldaten, alsook Oekraïners uit de reeds door Rusland bezette gebieden, is dit een onhaalbaar vereiste. Het is bovendien twijfelachtig of cyberaanvallen gericht tegen (militaire) doelwitten anders dan tegen die binnenvallende troepen zelf (*in casu* het achterland van die strijdmacht), wel als *levée en masse* mogen worden beschouwd.[39]

Hiermee lijkt de mogelijkheid van een *levée en masse* uitgesloten. Het artikel roept overigens nog meer vragen op in de cyber-context, zoals: vallen (alle) cybermiddelen, -methoden en -technieken onder 'wapens' en kun je deze cyberwapens 'openlijk dragen'? Kunnen onder 'invallende troepen' ook massale cyberoperaties door de vijand worden verstaan? De groep internationale experts die zich boog over de toepassing van het internationaal recht op cyberspace, was hierover verdeeld.[40] Gezien de beperkte ruimte kunnen we hier niet verder ingaan op dergelijke vragen. Vermeldingswaardig is wel dat aan het vereiste 'uit eigen beweging' ook wordt voldaan wanneer de overheid oproept tot verzet, zolang het gebied op het moment van verzet – de invasieperiode – niet onder controle van de vijand staat. Na die tijd moeten de deelnemende burgers worden vervangen door reguliere combattanten, of worden ingelijfd als reguliere combattanten door de verdedigende staat. De oproep van Federov om deel te nemen aan het IT-Army staat het vereiste van spontaniteit dus niet in de weg. Volstaan wordt met de conclusie dat in ieder geval niet-Oekraiense deelnemers die niet 'behoren tot de bevolking van niet-bezet gebied in Oekraïne' zich niet onder de categorie van de *levée en masse* kunnen scharen.

Rechtstreekse deelname aan vijandelijkheden door burgers

Burgers in een gewapend conflict zijn beschermd vanwege hun status en mogen derhalve nooit doelwit zijn. Deze bescherming vervalt wanneer en voor zolang burgers handelingen uitvoeren die de drempel halen van rechtstreekse deelname aan de vijandelijkheden.[41] Het HOR specificeert niet wat daarmee precies wordt bedoeld. Daarom heeft het Internationaal Comité van het Rode Kruis een *Interpretive Guidance* opgesteld met drie (algemeen geaccepteerde)[42] criteria die dat concept van rechtstreekse deelname aan vijandelijkheden verder invullen:[43]

Deze bescherming vervalt wanneer en voor zolang burgers handelingen uitvoeren die de drempel halen van rechtstreekse deelname aan de vijandelijkheden

- *Schadedrempel*: het is aannemelijk dat de specifieke handeling de militaire operatie of militaire capaciteit van een partij bij het gewapend conflict negatief beïnvloedt of de dood, verwonding of vernietiging van personen of objecten die beschermd zijn tegen een rechtstreekse aanval tot gevolg heeft.
- *Direct causaal verband*: er moet een direct causaal verband bestaan tussen de specifieke handeling of tussen een gecoördineerde militaire operatie waar die handeling integraal onderdeel van uitmaakt en de redelijkerwijs verwachte schade.
- *Link met een Partij bij het conflict*: de specifieke handeling heeft als doel schade aan te brengen om een partij bij het gewapend conflict te bevoordelen en de andere te benadelen.

De toepassing van deze criteria is op zichzelf al complex in traditionele conflictdomeinen, maar nog complexer in cyberspace. Een belangrijk referentiepunt is Regel 97 van de Tallinn Manual die bevestigt dat de regel uit artikel 51(3) Eerste Aanvullend Protocol (1977) en de drie door het ICRC geformuleerde criteria ook van toepassing zijn in cyberspace.[44] Een operatie met bijvoorbeeld *ransomware*, zoals de 'NotPetya'-cyberaanval uit 2017 die voornamelijk schade aanrichtte bij civiele bedrijven,[45] haalt de drempel opvallend genoeg waarschijnlijk niet. Dat cyberaanvallen kritieke infrastructuur kunnen raken, pleit ervoor een bredere interpretatie van 'schade aan objecten' te hanteren.

Ook zonder fysieke schade toe te brengen, kun je de schadedrempel halen. De *Interpretive Guidance* geeft als voorbeeld cyberaanvallen gericht op het verstoren, uitschakelen, vernietigen of kwaadwillig beheersen van een computeromgeving of infrastructuur, het vernietigen van de integriteit van gegevens, of het stelen van informatie.[46] Sommige experts menen dat de drempel ook wordt gehaald ingeval het gaat om de versterking van de

30. *Tallinn Manual 2.0*, p. 405-406.
31. *Tallinn Manual 2.0*, p. 406.
32. R. Buchan, 'Cyberwarfare and the status of anonymous under international law', *Chinese Journal of International Law* 2016, 15(4), p. 752.
33. Art. 44(3) Eerste Aanvullend Protocol (1977). Art. 44(4) Eerste Aanvullend Protocol (1977) voegt daaraan toe dat bij het schenden van deze voorwaarde de combattant het recht verliest om als krijgsgevangene te worden beschouwd.
34. ICRK, *Commentaar bij het Derde Verdrag van Genève* (2020), par. 1026 en *Tallinn Manual 2.0*, p. 406.
35. Idem, par. 1028-1039.
36. Art. 4(A)(1) Derde Verdrag van Genève (1949).
37. Art. 4(A)(6) Derde Verdrag van Genève (1949).
38. *Tallinn Manual 2.0*, p. 408.
39. *Tallinn Manual 2.0*, p. 409.
40. Ibidem.
41. Art. 51(3) Eerste Aanvullend Protocol (1977).
42. *Tallinn Manual 2.0*, p. 429. Voor een kritische behandeling van de *Interpretive Guidance*, zie *New York University Journal of International Law and Politics* (2010).
43. N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC, 2009).
44. *Tallinn Manual 2.0*, p. 428.
45. US Department of Justice, 'The NotPetya Cyber Attacks', United States district court western district of Pennsylvania, Indictment No. 20-316, oktober 15, 2020, p. 16-23.
46. N. Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (ICRC 2009), p. 48.

eigen capaciteit ten opzichte van de tegenstander.[47] Het tweede criterium lijkt het meest problematisch in de praktijk van de cybercontext, omdat cyberoperaties niet altijd schade opleveren, als deze al zichtbaar wordt. Het maken van malware op zich, of het openbaar delen daarvan, is onvoldoende. Als dit gebeurt in de wetenschap dat het wordt gebruikt in een aanval tegen een voor de ontwikkelaar en/of deler bekend doel, dan kan er wel sprake zijn van een direct causaal verband. Het derde criterium is erop gericht criminele groeperingen/activiteiten uit te sluiten.

Een cyberactie die geen cyber-*aanval* is, kan betekenen dat iemand toch rechtstreeks deelneemt aan vijandelijkheden.[48] Als sprake is van rechtstreekse deelname, dan verliest een burger zijn bescherming. De burger is dan voor de tegenstander een legitiem doelwit wanneer en zolang hij/zij rechtstreeks deelneemt aan de vijandelijkheden (waaronder voorbereidingshandelingen, inlichtingen verzamelen, doelidentificatie, uitvoeringshandelingen en *after action assessment*). De locatie van waaruit deze handelingen worden verricht, maakt voor het oorlogsrecht niet uit. (Cyber)operaties die vanuit Nederland worden opgezet, aangestuurd of uitgevoerd, kunnen evenzeer onder rechtstreekse deelname aan vijandelijkheden vallen.

(Cyber)operaties die vanuit Nederland worden opgezet, aangestuurd of uitgevoerd, kunnen evenzeer onder rechtstreekse deelname aan vijandelijkheden vallen

Conclusie

Het HOR stelt dat een combattant mag deelnemen aan de gewapende strijd en daarbij (dodelijk) geweld mag gebruiken tegen vijandelijke strijders en andere legitieme doelen. Dit combattanten-privilege geldt niet voor burgers die deelnemen aan de vijandelijkheden. Zolang een combattant deelneemt aan het gewapend conflict is deze een legitiem doelwit. Een burger die zich afzijdig houdt van de gewapende strijd is geen legitiem doelwit.

Volgens een Oekraïens Presidentieel decreet kunnen alle niet-Oekraïners zich aansluiten bij hun vreemdelingenlegioen waarna zij deel uitmaken van de Oekraïense krijgsmacht en de combattantenstatus krijgen. Diegenen die zich hebben aangemeld bij het *IT-Army of Ukraine* leger vallen *niet* onder het Presidentieel decreet en kwalificeren *niet* als reguliere combattant. De in ontwikkeling zijnde wet inzake de formele integratie van het IT-Army in de Oekraïense *Cyber Reserve Force* kan hierin verandering brengen.

Om te worden beschouwd als irreguliere combattanten, moet het IT-Army 'vechten namens Ukraine' en bovendien moet dat land deze 'gevechtsfunctie' accepteren. Aan die voorwaarde lijkt voldaan. Daarnaast zou het IT-Army als groep collectief moeten voldoen aan vier specifieke criteria. Een vast en op enige afstand herkenbaar onderscheidingsteken is voor het IT-Army als geheel echter niet vereist en ook het openlijk dragen van cyberwapens geldt niet voor cybersoldaten. Dat het IT-Army als groep wel de regels van het humanitair oorlogsrecht moet naleven is evident. Als de internationale vrijwillige cybersoldaten niet hiërarchisch zijn georganiseerd en evenmin worden aangestuurd onder volledige verantwoordelijkheid van de Oekraïense staat, dan voldoen zij *niet* aan het bevelsverhouding-criterium. Zij kwalificeren dan *niet* als irregulier combattant.

De Oekraïense bevolking van niet-bezet gebied die bij het naderen van de Russische strijdmacht uit eigen beweging cyberoperaties uitvoert om de invallende troepen te bestrijden, zou de combattanten-status kunnen verkrijgen als onderdeel van de *levée en masse*. De niet-Oekraïense deelnemers die niet behoren tot 'de bevolking van niet-bezet gebied in Oekraïne' kwalificeren *niet* als combattant onder de categorie *levée en masse*.

Niet-Oekraïense deelnemers aan het IT-Army kwalificeren op geen enkele manier als combattant. In een gewapend conflict hebben burgers een beschermde status, maar deze bescherming vervalt wanneer en zolang burgers rechtstreeks deelnemen aan de vijandelijkheden. Cyberactiviteiten die niet zijn bedoeld als cyberaanval, kunnen wel degelijk worden beschouwd als rechtstreekse deelname aan vijandelijkheden (zoals voorbereidingshandelingen, inlichtingen verzamelen, doelidentificatie en *after action assessment*). Als een burger rechtstreeks deelneemt aan dergelijke vijandelijkheden, dan verliest deze daarmee zijn beschermde status als burger. Wanneer en zolang die burger rechtstreeks deelneemt aan de vijandelijkheden, is die burger een legitiem doelwit voor de tegenstander.

Als *keyboard-warrior* deelnemen aan de cyberoorlog lijkt gerechtvaardigd en legitiem, maar is het niet. Niet iedereen is positief over deelname van cybersoldaten aan de online strijd. Behalve de AIVD liet ook militair jurist en hoogleraar cyberoperaties BGen Paul Ducheine,[49] zich negatief uit over het hacken van Russen door goedwillende Nederlandse vrijwilligers.[50] Een goede reden om je als Nederlander niet te mengen in de (digitale) strijd, is dat een cyberaanval kan worden gezien als poging om Nederland te betrekken bij de oorlog tussen Rusland en Oekraïne; dat is strafbaar en zou betreffende hacker een gevangenisstraf van tien jaar kunnen opleveren.[51] •

47. *Tallinn Manual 2.0*, p. 429.
48. Idem, p. 430.
49. Brigade-generaal Paul A.L. Ducheine is professor Cyber Operations aan de Nederlandse Defensie Academie (NLDA) en bijzonder hoogleraar Recht en Militaire Cyber Operaties aan de Universiteit van Amsterdam (UvA).
50. cybercrimeinfo.nl/cybercrime/cyberoorlog/861942_aivd-waarschuwt-ga-geen-russen-hacken.
51. Art. 100 Sr; hij die, in geval van een oorlog waarin Nederland niet betrokken is, opzettelijk enige handeling verricht waardoor het gevaar ontstaat dat de staat in een oorlog wordt betrokken, of enig van regeringswege gegeven en bekendgemaakt bijzonder voorschrift tot handhaving van het niet-deelnemen aan de oorlog opzettelijk overtreedt.