Recht & media arsaequi.nl/maandblad AA20110262

CYBERWAR: THE MEDIUM IS THE MASSACRE

Arno R. Lodder*

Bij mediarecht denk ik in de eerste plaats aan het recht rond omroepen en de pers. Ik was dan ook verrast gevraagd te worden voor de nieuwe rubriek *Recht en Media*. De onderwerpen die de redacteur suggereerde waren echter onderdeel van het internetrecht. Internet is ontegenzeggelijk het belangrijkste medium van de afgelopen tien tot vijftien jaar, dus past het zeker om hierover in deze rubriek te schrijven.

Internet heeft veel gemakken gebracht zoals webwinkelen, online vergunningen aanvragen, vrijwel alle denkbare informatie vinden, downloaden van muziek en films,[1] sociale contacten onderhouden en twitteren.[2] Internet kent echter ook mindere kanten zoals wormen, virussen, *spyware*, *spam* en mede onder toepassing van deze bedreigingen: internetoorlogsvoering.

Bij internetoorlogsvoering wordt internet als medium gebruikt voor handelingen die – mogelijk – onder het oorlogsrecht vallen. Onder de bredere noemer *cyberwar* wordt als elektronische oorlogsvoering begrepen: het gebruik van internet en elektronische wapens om schade aan te richten aan bijvoorbeeld de infrastructuur van een land, verricht met het doel een land te beschadigen of te ontwrichten. In het traditionele volkenrecht is oorlog een conflict tussen staten (of koningen, landheren, stamhoofden) en worden acties van individuen tegen staten niet als object van oorlogsrecht gezien. De situatie die ontstond na acties van terroristen in september 2001, versterkte een al aanwezige trend in het algemene denken over het enkel toepassen van oorlogsrecht op staten.[3] Het internet maakt het mogelijk dat groepen burgers en zelfs individuele burgers handelingen verrichten die zeker zo desastreus kunnen zijn als een aanval met kinetische wapens (bommen, kogels, etc.). Activiteiten op internet die grote schade kunnen aanrichten aan bijvoorbeeld de infrastructuur van een land, verricht met het doel een land te beschadigen of te ontwrichten, brengen voor juristen intrigerende vragen mee, onder andere:

- Kan een actie op internet gelijk worden gesteld aan het gebruik van geweld, een gewapende aanval of zelfs een bedreiging van de internationale vrede en veiligheid die tot ingrijpen van de Veiligheidsraad noopt?[4]
- Kunnen handelingen via internet, al dan niet door staten geïnitieerd, vallen onder oorlogsrecht?[5]
- Welke gevolgen heeft het als we *cyberattacks* gelijkstellen aan meer traditionele vormen van geweldgebruik? Wordt daarmee het onderscheid tussen oorlog en vrede in juridische zin niet ondergraven?[6]
- Welke reactie van een staat is geoorloofd tegen internetacties van individuen? En tegen wie mag deze tegenactie gericht zijn?[7]
- In hoeverre kan een staat verantwoordelijk worden gehouden voor onbedoelde schade (bijv. burgerslachtoffers) bij een overigens juridisch toelaatbaar defensief gebruik van cyber wapens?[8]

In 2010 is aan de Vrije Universiteit de afdeling *Transnational Legal Studies* opgericht alsmede het onderzoeksprogramma *Boundaries of Law* gestart en wordt onder andere onderzoek gedaan naar het recht rond *cyberwar* en onderwijs hierover gegeven. Zoals bij veel internetrechtonderwerpen het geval is, ontstaat in synergie met juristen uit andere disciplines (in casu internationaal recht, Europees recht en rechtsfilosofie) een resultaat dat groter is dan de som der delen. Dat is ook nodig, want er is nog veel onduidelijk op het gebied van *cyberwar*.

Om de genoemde en andere vraagstukken rond *cyberwar* te plaatsen, werd een nuttig referentiekader besproken door Thomas C. Wingfield tijdens een in januari in Amsterdam verzorgde lezing over *cyberwar*.[9] Binnen dit raamwerk kunnen drie lagen onderscheiden worden:

1 The possible;
2 The permissable;
3 The preferable.

Om te beginnen wordt *cyberwar* gekarakteriseerd door alles wat met internettechnologie en ICT mogelijk is, waarbij aan andere zaken dan traditionele, gewapende aanvallen moet worden gedacht. Zo is het mogelijk om een telefoonnetwerk plat te leggen met een worm, het bankverkeer stil te leggen door een virus of elektriciteittoevoer stop te zetten met een *denial-of-service*-aanval. Ook kan met behulp van *spyware* een verkeerscentrale of de besturing van klassieke wapens worden overgenomen.[10]

Het tweede niveau (the permissable) is juridisch van aard en geeft aan wat binnen de technische mogelijkheden juridisch toelaatbaar is. De extremen zijn helder. Zo zal het laten neerstorten van burgervliegtuigen in reactie op het platleggen van het bankverkeer niet toelaatbaar worden geacht. De vraag is vervolgens of dit als een oorlogsmisdrijf of misdaad tegen de menselijkheid[11] kan worden gezien. Vooral lastig is het bijzonder grote grijze gebied. Juristen bieden tot op heden te weinig handvatten aan de hand waarvan bepaald kan worden welke acties onder welke omstandigheden juridisch toelaatbaar zijn.

Het derde niveau betreft de politiek, te weten wat binnen het juridisch toelaatbare politiek de voorkeur heeft. Zo zal men liever met een *joystick en drone*[12] vanuit Amerika een Pakistaanse internetsoldaat fysiek uitschakelen,[13] dan daarnaar af te reizen of de strijd op internet aan te binden. Dit moet echter technisch mogelijk en juridisch toelaatbaar zijn.

Deze drie niveaus kunnen worden gezien als een trechter, aan de hand waarvan handelingen op internet die neigen naar oorlogshandelingen in een kader kunnen worden geplaatst. Meest omvattend zijn de technische mogelijkheden, die worden ingekaderd door de juridische toelaatbaarheid en het speelveld voor de politieke voorkeuren bepalen. Echter, technische ontwikkelingen gaan doorgaans snel en het heeft daarom zin om zowel politiek als juridisch verder te denken dan op dit mo-

Foto © Marten Hoogstraat (whiteframe.nl)

ment technisch mogelijk is, een zogenaamd proactieve benadering. Op die manier kan al nagedacht worden over antwoorden op vragen die later zullen spelen. Daarnaast blijft het natuurlijk van groot belang om de nu spelende vragen zo goed mogelijk te beantwoorden.

De meeste staten zijn bijzonder druk zich voor te bereiden op allerhande *cyberwar*-aanvallen.[14] Ook de Europese Unie[15] en de NAVO zijn actief, onder andere via een in 2008 speciaal opgericht centrum in Letland: *Cooperative Cyber Defence Centre of Excellence*.[16] Deze activiteiten vallen onder de noemer *cyberpreparedness*.[17] Ook hierbij wordt aandacht besteed aan actuele en toekomstige dreigingen en welke maatregelen juridisch toelaatbaar zijn: is vergelding toegestaan en zo ja, in welke mate? Hoe lang moet gewacht worden met tegenacties en welke voorzorgsmaatregelen zijn geoorloofd? Het is hierbij natuurlijk zaak de gevestigde machten kritisch te blijven volgen.

Ieder historisch overzicht van internet begint met het noemen van Arpanet, de voorloper van het huidige internet. Het is ironisch dat het gedistribueerde netwerk dat ooit geïnitieerd is door de Amerikaanse defensie, zo open en makkelijk manipuleerbaar is. De eerste tientallen jaren werd het internet voornamelijk gebruikt door academici die elkaar vertrouwden. De protocollen waren daar toen ook op gebaseerd. Met het opschalen van het internet tot gigantische proporties met inmiddels meer dan een miljard gebruikers vormt de openheid die internet groot maakte, in de huidige tijd de grootste bedreiging.[18]

In die zin is de cirkel rond; het netwerk dat ontwikkeld werd in tijden van ruimtemissies en angst voor massavernietigingswapens, is voor oorlogsvoering een onmisbaar instrument geworden. Er zullen *cyberwar*-acties zijn, reacties daarop en ook de klassieke oorlogsvoering zal vrijwel altijd gepaard gaan met gebruik van informatie- en internettechnologie. Een nieuw en intrigerend onderwerp, waar wij in zowel ons onderzoek als onderwijs (onder andere per januari 2012 is een nieuw vak, *Cybercrime, -war en -terrorism*, hieraan gewijd) aandacht aan besteden. *Ius ad bellum* en *Ius in bello* zullen nooit meer zijn wat zij geweest zijn.

* Mr.dr. A.R. Lodder is universitair hoofddocent Recht en Informatietechnologie aan de afdeling Transnational Studies, Computer/Law Institute van de Vrije Universiteit.

1 Hierover ging een eerdere bijdrage in deze rubriek: B. De Knock, 'Streaming music services: remedie tegen piraterij?', *Ars Aequi* 2011, p. 86-87 (🗁AA20110086).

2 Laatste twee vallen onder de noemer Web 2.0, zie daarover A.R. Lodder, R. van den Hoven van Genderen, A. Engelfriet, D. Mekić e.a, *Recht en Web 2.0*, NVvIR publicatiereeks no. 27, gratis te downloaden via *http://bit.ly/9Rmh4n*.

3 J. Carr, *Inside Cyber Warfare*, Sebastopol: O'Reilly 2010, p. 53.

4 R. van den Hoven van Genderen, 'Gebruik van "cyber-arms" is een oorlogsdaad', *NRC Handelsblad* 20 juni 2009 (Opinie & Debat), p. 9.

5 N. Keijzer, 'Internetoorlog en de Wet internationale misdrijven', in: A.R. Lodder & A. Oskamp (red.) *Caught in the Cyber Crime Act*, Deventer: Kluwer 2009, p. 55-61.

6 J. Meyer, 'The Rules of Cyber War', 14 december 2010, beschikbaar op *http://bit.ly/hFR4PR*.

7 M.N. Schmitt, 'Bellum Americanum: the U.S. View of Twenty-First Century War and Its Possible Implications for the Law of Armed Conflict', *Michigan Journal of International Law* 1998, p. 1051-1090.

8 Cyber War Could Cause Global Collateral Damage, *Internetnews.com* 4 augustus 2009.

9 Zie o.a. T.C Wingfield, 'International Law and Information Operations', in Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz (red.), *Cyberpower and National Security*, Washington, DC: National Defense University, 2009, p. 525-42.

10 Voor een uitgebreid overzicht van mogelijkheden zie: R.A. Clarke & R.K. Knake, *Cyberwar. The next threat to national security and what to do about it*, New York: HarperCollins 2010.

11 Dit is het geval als er sprake is van een 'widespread and systematic attack on the civilian population'.

12 Dit zijn kleine vliegtuigjes die op afstand bestuurbaar zijn.

13 'Drone-aanval VS doodt 18 militanten in Pakistan', *NRC Handelsblad* 27 december 2010.

14 F.D. Kramer, S.H. Starr & L.K. Wentz (red.), *Cyberpower and national security*, Dulles: Potomac books 2009.

15 Commission to boost Europe's defences against cyber-attacks, Brussel, 30 september 2010, IP/10/1239.

16 Zie *www.ccdcoe.org*, met aandacht voor technische, strategische en juridische ontwikkelingen: 'The development of a good legal framework is perhaps the single most pressing need within the domain of computer network defence.'

17 J.B. Michael e.a, 'Integrating Legal and Policy Factors in Cyberpreparedness', *Computer* 2010-4, p. 90-92.

18 Voor een uitstekende analyse zie: J. Zittrain, *The Future of the Internet and How to Stop It*, New Haven: Yale University Press 2008.