Storing of oorlogsdaad?

Ducheine, P.A.L.

Published in:
Militair Rechtelijk Tijdschrift

Bijdrage III
Storing of oorlogsdaad?

Door Brigade-generaal prof. dr. P.A.L. Ducheine[1]

Precies op de dag dat ik aan mijn eerste column voor het MRT begin, dat wil zeggen, mijn gedachten op 'papier' wil zetten, heeft KPN een omvangrijke internetstoring. Vervelend, want in mijn UvA-account zat een mail aan mezelf waarin ik ideeën had genoteerd. Gelukkig kan ik met mijn smartphone wel bij die email. Waar redundantie al niet goed voor is. Kost wat, maar dan heb je ook wat (als back-up). De storing past trouwens perfect bij mijn idee voor deze eerste column, namelijk: de kwalificatie van digitale incidenten.

---

16 In dat kader is het LTC sinds kort ook op internet te vinden: www.updfltc.org

1 Hoogleraar Military Law of Cyber Security & Cyber Operations (OMHP, E 2.15), Universiteit van Amsterdam & Hoogleraar Cyber Operations, Nederlandse Defensie Academie.
NLDA: Hoogleraar Cyber Operations

Ik kwam hierop toen *Vice.com* mij interviewde over 'oorlogsdaden in cyberspace'.[2] De journalist, Wester van Gaal, begon het gesprek met de vraag: "wat is een digitale oorlogsdaad"? 'Goede vraag', dacht ik toen, en ik vroeg hem wat hij er zelf onder verstond. Hij had zich ingelezen en we zaten dicht bij elkaar![3]

Niet ieder digitaal incident is namelijk een 'hack', laat staan een 'aanval' of een 'oorlogsdaad'. Met incidenten bedoel ik een voorval dat de gewenste beschikbaarheid, vertrouwelijkheid of integriteit van ICT verstoort.[4] Dat voorval kan een technische of menselijke oorzaak hebben.

Soms gaat het gewoon om een storing, zoals vandaag dus. Althans dat is wat ik er nu van merk: mijn internet is niet beschikbaar. Wellicht wordt snel duidelijk wat er mankeert: een fysiek technisch mankement, een software probleem, een Hollandse hacker die KPN op de korrel neemt om zijn/haar vaardigheden te testen, een afleidingsmanoeuvre van een criminele groep die ondertussen elders zijn slag slaat, of een niet-bevriende dienst die KPN's beveiliging of (publieke) reacties test. Maar voor hetzelfde geld bestaat er wel een relatie met een oorlog en zit ISIS, een tegenstander in een gewapend conflict, hier achter.[5] Daar ziet het overigens nu gelukkig niet naar uit.

Ik bedoel maar: een incident is niet zo maar een 'oorlogsdaad'. In het Vice-interview bleek dat Wester van Gaal het begrip voor twee verschillende situaties gebruikte. Ten eerste of "Operatie *Olympic Games*, de inzet van *Stuxnet* tegen Iran, als een oorlogsdaad moest worden gezien (A)" en "of het oorlogsrecht wel toegesneden was op deze digitale oorlogsdaden (B)". U herkent in deze tweeslag achterliggende kwesties van rechtsbases en rechtsregimes, van *ius ad bellum* en *ius in bello*.

De kwestie *Stuxnet* (A) raakt het *ius ad bellum*. Moet je *Olympic Games* kwalificeren als een inbreuk op het geweldsverbod van art. 2(4) VN-Handvest? Heeft de auteur van *Stuxnet* met dit 'geweld' het interstatelijke geweldsverbod overtreden? En vervolgens: kan Iran *Stuxnet* aanmerken als een "gewapende aanval" uit artikel 51 VN-Handvest en zich vervolgens beroepen op zelfverdediging als rechtsbasis voor een reactie?[6]

De internationale experts achter de *Tallinn Manual* waren het eens dat *Stuxnet* een vorm van "geweldgebruik" (art. 2(4) VN-Handvest) was.[7] De vervolgvraag verdeelde de groep: een minderheid typeerde de inzet van *Stuxnet* die tot fysieke schade aan de Iraanse nucleaire opwerkingsfaciliteiten leidde, als een "gewapende aanval" (art. 51 VN-Handvest).[8] In dat opzicht een 'oorlogsdaad' dus.

Stuxnet was vanwege de fysieke schade juridisch gezien nog een 'eitje'. Bij louter niet-fysieke gevolgen van een digitale inbreuk worden voorgaande afwegingen lastiger. De *Tallinn Manual* wijst op dit punt naar een uniek Nederlands advies van de AIV en CAVV.[9] Onze regering nam dit advies 'Digitale Oorlogsvoering' (grotendeels) over, inclusief deze kenschets van een digitale gewapende aanval met louter niet-fysieke effecten.

Deze *ius ad bellum* kwesties zijn uiteindelijk politieke keuzes waarin juridische appreciaties van feitelijke gebeurtenissen een belangrijke rol spelen. Althans, meestal. Het is een vraagstuk dat vooraf gaat aan

---

2 Zie <http://motherboard.vice.com/nl/read/cybergeneraal-paul-ducheine-nederland-is-kwetsbaar>

3 Onder andere een (naar mijn gevoel minder geslaagd) interview met de Correspondent <https://decorrespondent.nl/2115/De-online-wapenwedloop-is-begonnen-dus-waar-blijft-het-vredesplan-/102994155-a2e0106b>.

4 Zie de definitie van cyber security in o.a. mijn oratie http://www.militairespectator.nl/thema/recht-cyberoperations/artikel/%E2%80%98je-hoeft-geen-zwaard-en-schild-te-dragen-om-ridder-te-zijn%E2%80%99 of <http://webcolleges.uva.nl/Mediasite/Play/bca07f4a8a77401d96da8bc0e8de090d1d?utm_content=buffer86a43&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer>.

5 Zie T.D. Gill, Classifying the Conflict in Syria, < http://stockton.usnwc.edu/ils/vol92/iss1/11/>.

6 Vooropgesteld natuurlijk dat aan alle andere voorwaarden voor zelfverdediging is voldaan: zelfverdediging is noodzakelijk en proportioneel én Iran weet wie de auteur van de aanval is!

7 M.N. Schmitt (ed.), Tallinn Manual on the International Law applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013, p. 45, zie <https://ccdcoe.org/tallinn-manual.html>.

8 Idem, p. 58.

9 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (AIV & CAVV): Digitale oorlogvoering, Den Haag: AIV no. 77, 2011; CAVV no. 22, zie www.aiv-advice.nl, p. 20.

de inzet van de krijgsmacht.[10] Het gaat om de vraag: wanneer mag de krijgsmacht het (digitale) slagveld betreden?

Pas daarna komt de tweede kwestie van het oorlogsrecht (B) aan de orde: hoe handelt de krijgsmacht op het (digitale) slagveld.[11] Het gaat dan om het rechtsregime, de regels in de (digitale) strijd: i.c. het oorlogsrecht. Iedere commandant en jurist weet bijvoorbeeld dat de oneliner – digitaal kun je alles aanvallen, want alles is met alles verbonden – nonsens is. Technisch gezien wellicht correct, maar net als op het fysieke slagveld dient de militair zijn digitale aanvallen te beperken tot "militaire doelen" (*military objectives*) zoals bedoeld in art. 52(2) AP1.

Zeker, die vertaling van oorlogsrecht is niet eenvoudig en gaat ook niet vanzelf. Vandaar dat we als krijgsmacht officieren onderrichten, militaire juristen inzetten en oefeningen ontwikkelen waarin deze targeting-vraagstukken aan bod komen. Handboeken zoals de *Tallinn Manual* komen hierbij goed van pas.

En ja: ongetwijfeld zal het oorlogsrecht geschonden worden, zoals de journalist kritisch stelde. Die schendingen moeten onderzocht en vervolgd worden, reflecteerde ik, maar het enkele feit dat de norm (soms) overtreden wordt, wil nog niet zeggen dat die norm niet geldt!

Want hoe complex beide kwesties ook zijn: het recht is ook van toepassing op digitale 'oorlogsdaden'. Het *ius ad bellum* en het oorlogsrecht. Maar laten we vooral niet vergeten dat niet iedere storing of hack een oorlogsdaad is.