# Cyberaanvallen en het recht van de gewapende conflicten : bemerkingen bij een juridische primeur in België en de Verenigde Staten

## Frank Franceus (*)



(*) De in deze bijdrage verwoorde opinies zijn enkel deze van de auteur zelf. Zij binden in geen enkele mate de organisatie waaraan de auteur verbonden is.

# 1. Inleiding

Over het fenoneem van de 'cyberwar' is reeds heel wat geschreven[1]. Dat een 'cyberwar' een echte omwenteling in de oorlogsvoering zou vormen, werd reeds bij de start van het publieke internet in de jaren '90 door de Amerikaanse denktank Rand-Corporation, voorspeld : "As an innovation in warfare, we anticipate that cyberwar may be to the 21st century what *blitzkrieg* was to the 20th century" [2].
In een rapport dat in 1998 voor de Amerikaanse minister van Defensie werd opgesteld, wordt een oorlogspel beschreven dat zich in het jaar 2000 in de Perzische Golf en Iran zou afspelen[3]. Een conventionele aanval 'Operation Green Hornet' zou gepaard gaan met een 'geïntegreerd

[1] Naast de vele artikelen die over het onderwerp zijn verschenen en die in deze bijdrage vermeld worden zijn er ook een aantal monografieën die de aandacht weerhouden. De beschikbare literatuur is weliswaar bijna exclusief in het engelstalige domein te vinden.
Vroege werken en rapporten :
- Greenberg, L.T., Goodman, S.E., & Soo Hoo, K.J. (1998). *Information Warfare and International Law*, National Defense University Press. Geraadpleegd op http://www.dodccrp.org/files/Greenberg_Law.pdf
- Schmitt, M.N. (1999). *Computer network attack and use of force in international law, thoughts for a normative framework*. Geraadpleegd op http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993

Recente bronnen :
- Adviesraad Internationale Vraagstukken (AIV) & Commissie voor Advies inzake Volkenrechtelijke vraagstukken (CAVV). (2011). *Digitale oorlogvoering*. (AIV nr. 77 / CAVV nr. 22). Geraadpleegd op http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie_AIV_77_CAVV_22_NL%281%29.pdf.
- Carr, J. (2011). *Inside Cyber Warfare - Mapping the Cyber Underworld*. Sebastopol, CA : O'Reilly Media.
- Clarke, R.A., & Knake, R.K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*, New York, NY : Harper-Collins
- Csosseck, C., Ottis, R., & Ziolkowski, K. (eds). (2012). 2012 4th International Conference on Cyber Conflict Proceedings, Tallinn : Nato CCD COE publications. De CCD-COE is de onder de NATO-vlag opererende en in Tallinn gevestigd Cooperative Cyber Defence Centre of Excellence.
- Libicki, M.C. (2009). *Cyberdeterrence and cyberwar*, Rand Corporation. Geraadpleegd op http://www.rand.org/pubs/monographs/MG877.html
- Melzer, N. (2011). Cyberwarfare and International Law. Unidir Resources - United Nations Institute for Disarmament Research. Geraadpleegd op http://unidir.org/pdf/activites/pdf2-act649.pdf
- Owens, W.A., Dam, K.W., & Lin, H.S. (eds.). (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. National Research Council, Committee on Offensive Information Warfare Computer Science. Geraadpleegd op http://www.nap.edu/catalog.php?record_id=12651#toc
- Raucher, K.F., & Korotkov, A., (principal authors). (2011). *Working towards rules for governing cyber conflicts - Rendering the Geneva and Hague conventions in cyberspace*. EastWest Institute. Geraadpleegd op http://www.ewi.info/working-towards-rules-governing-cyber-conflict
- Roscini, M. (2010). *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*. In von Bogdandy, A., & Wolfrum, R. (eds), Max Planck Yearbook of United Nations Law, vol. 14, p. 85-130. Geraadpleegd op http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf
- Schreier, F. (2012). *On cyberwarfare*. DCAF Horizon 2015 Working Paper. Geraadpleegd op http://www.dcaf.ch/Publications/On-Cyberwarfare
- Tikk, E., Kaska, K., & Vigul, L. (2010). *International Cyber Incidents, Legal considirations*, Tallinn : Nato CCD COE publications.
- Ziolkowski, K. (2010). Computer Network Operations and the Law of Armed Conflict. *Revue de Droit Militaire et de Droit de la Guerre*, 49 (1-2), 47-94.

In het nederlandstalige gebied bestaat bij ons weten enkel de geciteerde studie van de nederlandse AIV en CAVV, en een publicatie van de hand van Lt.Kol De Bruycker, M.L. (2010). Cyber Defense. *Belgisch Militair Tijdschrift*, december, 35-38.

[2] Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is Coming*. National Defense Research Institute – Rand Corporation : http://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf

[3] Molander, R.C., Riddile, A.S., & Wilson, P.A. (1998). *Strategic Information Warfare – A new Face of War, appendix C.* Opgehaald bij Rand Corporation, National Defense Research Institute : http://www.rand.org/pubs/monograph_reports/2005/MR661.pdf

Information-warfare aanvalsplan Net Master'. Dat laatste zou niet enkel als doel hebben de computer- en C3I-infrastructuur (C3I = Command, Control, Communications & Intelligence) te vernietigen, maar ook de burgerlijke ICT-infrastructuur buiten actie te stellen. Een gelijktijdige 'Operation Force Field' moest leiden tot een "information dominance within a 500 km battle cube and in particular render ineffective the key elements of a future regional opponent's tactical reconnaissance, air defense, and C3I systems".
Het verslag van dit oorlogspel dat in de Noord-Atlantische Raad (de Parlementaire Assemblee van de NAVO) werd besproken, wees uit dat het opgestelde scenario niet uit de lucht gegrepen was : een "strategic information warfare can occur without forewarning or escalation of other events'. [4]

Veel recenter, in 2011, hing Leon Panetta in het Amerikaanse Senaat een alarmerend beeld van de virtuele wereld op. Hij stelde : "the next Pearl Harbor that we confront could very well be a cyberattack" [5] [6]. Gelet op de positie van Panetta, als ex-CIA chef en thans Amerikaanse minister van Defensie is dit een mening die van belang is.

Dr. Thomas Rid, expert oorlogsstudies bij het Kings College London stelde begin dit jaar evenwel dat een cyberoorlog nog nooit heeft plaats gevonden en evenmin in de toekomst zal plaats vinden[7]. Rid haalt in zijn artikel belangrijke punten aan gepuurd uit de traditionele oorlogstheorie.
In punt 3 van deze bijdrage gaan we hier nader op in, maar kort gezegd komt zijn stelling er op neer dat de traditionele constitutieve elementen van een oorlog die in de klassieke militaire theorie gangbaar zijn, niet aanwezig zijn bij de 'cyberaanvallen' die tot op heden werden gerapporteerd. De cyberaanvallen, met als schoolvoorbeeld deze op Estland in 2007, hebben niet het 'politieke, instrumentele en dwingend gewelddadige karakter' om van een werkelijke 'oorlog' te kunnen spreken, aldus Rid.

Ook sommige pers is sceptisch ten aanzien de cyberwar-dreiging. In juli 2011 wijdde Michael Hirsh in de National Journal een column aan de problematiek van de cyberoorlog. Onder de titel "Here, there be dragons" betoogt hij dat het gevaar voor een cyberoorlog sterk overdreven wordt en dat de vrees ervoor vooral ingegeven wordt door de onbekendheid met het fenomeen[8]. Net zoals vroegere cartografen bij gebrek aan correcte gegevens de witte vlekken de antieke landkaarten met mooie tekeningen van draken en monsters opvulden, wordt thans de cyberoorlog ten tonele gevoerd [9].

---

[4] NATO Parliamentary Assembly. Science and Technology Committee. (1997). *Information. Warfare and the Millennium bomb*. Geraadpleegd op http://www.iwar.org.uk/iwar/resources/nato/ap237ste.pdf

[5] Ziegeler, R., (2011, june 16). C.I.A. website attacked just days after Panetta warns of a cyber Pearl Harbor, [web log post]. Geraadpleegd op http://blog.foreignpolicy.com/posts/2011/06/16/cia_website_attacked_just_days_after_panetta_warns_of_a_cyber_pearl_harbor

[6] Panetta kan zijn inspiratie voor deze uitspraak hebben gehaald bij een oorlogspel dat door de firma Gartner in 2002 voor U.S. Naval War College werd opgezet onder de naam 'Digital Pearl Harbor'. "Results of a post-game survey indicate that the DPH game experience had a profound impact on the participants: 79 percent of the gamers said that a strategic cyberattack is likely within the next two years". Opgehaald bij Gartner Corporation : Internet : http://www.gartner.com/pages/story.php.id.2727.s.8.jsp

[7] Rid, T. (2012). Cyber War will not take place. *Journal of Strategic Studies*, 35(1), 5-32.

[8] Hirsh, M. (2011, July 23). Here, There Be Dragons. *National Journal*. Geraadpleegd op http://www.nationaljournal.com/magazine/fear-of-cyberattack-may-be-biggest-threat-20110721. De auteur schrijft : "The cyberwar threat is being hyped because of a fear of unknown dangers. The biggest threat of all may come from our own overreaction".

[9] Tot diegenen die denken dat de dreiging wellicht overschat wordt, behoren ook :

Niettemin wordt de cyberdreiging alleszins op militair vlak zeer ernstig genomen en werden in een aantal landen heuse 'cyber-commands' opgericht.[10] Sommige landen hebben ook op wetgevend vlak gereageerd : dit is het geval voor België en de Verenigde Staten. Het is daarover dat deze bijdrage handelt.

# 1 Belgische en Amerikaanse wetgevende initiatieven

## *1.1 De Belgische wetgeving*

In de literatuur met betrekking tot de Belgische inlichtingendiensten werd in de voorbije jaren veel aandacht besteed aan de nieuwe bevoegdheden die de Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens toekende aan de burgerlijke Veiligheid van de Staat (VSSE) en de militaire Algemene Dienst voor Inlichtingen en Veiligheid (ADIV)[11]. Het gaat om de zogenaamde specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, gaande van het achterhalen van oproepgegevens van telefonische gesprekken over het afluisteren van dergelijke gesprekken en het openen van aan de post toevertrouwde brieven, tot het inbreken in computersystemen en het oprichten van fictieve vennootschappen om aldus inlichtingen te kunnen verzamelen.

Bovendien kreeg de ADIV door dezelfde Wet van 4 februari 2010 een nieuwe bevoegdheid toegewezen, in het kader van de zogenaamde 'cyberaanval'. Deze wettelijke bevoegdheidsuitbreiding vormde op internationaal vlak op dat moment bij ons weten een wereldprimeur, maar werd tot op heden niet in de rechtsleer becommentarieerd.

---

- Sommer, P., & Brown, I. (2011). *Reducing systemic cybersecurity risk* (OECD-IFP Project on Future global shocks IFP/WKP/FGS/2010/3). Geraadpleegd op ttp://www.oecd.org/sti/futures/globalprospects/46889922.pdf . In de Executive summary van dit zeer uitgebreid en genuanceerd werk concluderen de auteurs dat "very few single cyber-related events have the capacity to cause a global shock".
- Lawson, S. (2011). Beyond cyber-doom : cyberattack scenarios and the evidence of history (Working paper N° 11-01, Mercatus Center, George Mason University). Geraadpleegd op http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf De auteur schrijft dat "cyber-doom scenarios are more a reflection of long-held, but ultimate incorrect, assumptions and fears about the fragility of modern societies and infrastructure systems than they are a realistic portrayaal of what is possible as a result of cyberattack" (p. 31).
- Cavelty, M.D. (2012). The militarisation of cyberspace : why less may be better. In Czosseck, C., Ottis, R., & Ziolkowski, K. (2012), gecit., p.141-153.

[10] In de Verenigde Staten werd de U.S. Cyber Command opgericht, als onderdeel van de U.S. Strategic Command (USSTRATCOM). Deze USCYBERCOM coördineert de acties van de cyberdivisies van het leger, de zeemacht, de luchtmacht en het marinierscorps. Interessant is dat de het hoofd van de USCYBERCOM ook het hoofd is van de National Security Agency, de Amerikaanse inlichtingendienst die electronische informatie verzamelt. Ook China heeft een cybercapaciteit in zijn leger opgenomen, terwijl ook Israël zich niet onbetuigd laat : de militaire 'unit 8200' houdt zich bezig met electronische inlichtingenverzameling en zou enige duizenden personeelsleden tellen; hoeveel daarvan bij (offensieve) cyberwaractiviteiten betrokken zijn, is onbekend.
Een actueel overzicht van de cybercapaciteit van 27 verschillende landen vindt men bij CARR, J. (2011), p. 243–262.
Zie ook Lewis, J.A. & Timlin, K. (2011). *Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctirne and Organisation.*, Center for Strategic and International Studies, United Nations Institute for Disarmament Research. In dit werk wordt het cyberbeleid van meer dan 60 landen in het kort besproken. Geraadpleegd op http://unidir.org/bdd/fiche-ouvrage.php?ref_ouvrage=92-9045-011-J-en

[11] Wet van 4 februari 2010, BS 10.3.2010, die in belangrijke mate de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna Wet I&V) heeft gewijzigd.

Het artikel 11, § 1, 2° van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (hierna Wet I&V) werd door de Wet van 4 februari 2010 inderdaad als volgt uitgebreid :

> § 1 - De Algemene Dienst inlichting en veiligheid heeft als opdracht : (…) *2°* het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en, *in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten"* (onze cursivering).

De uitbreiding van de bevoegdheid van de militaire inlichtingendienst kwam tot stand ten gevolge van een parlementair initiatief, met name het amendement nr. 83 van Senator Vandenberghe et al. [12]. De verantwoording bij het amendement luidt als volgt :

> *Rekening houdend met de recente wereldwijde toename van cyberaanvallen op overheidssystemen, in het bijzonder op vitale systemen of systemen met gevoelige of geclassificeerde informatie, maakt de voorgestelde wijziging het mogelijk te reageren op dergelijke aanvallen, met indien nodig de mogelijkheid tot inwinnen van inlichtingen via intrusie in informaticasystemen zoals voorzien in het voorgestelde artikel 18/16 (art. 14 van het wetsvoorstel). Een dergelijke actie moet er toe leiden de aanvallers te identificeren en de aanval te neutraliseren.*
>
> *Een cyberaanval op de communicatie- en informatiesystemen van Defensie is elke actie met als doelstelling :*
>
> *— de normale werking ervan te verstoren of te onderbreken*
>
> *— onrechtmatig binnen te dringen om informatie van Defensie te lezen, te wijzigen, toe te voegen of te wissen*
>
> *— onrechtmatig binnen te dringen om de mogelijkheden van het systeem te misbruiken voor het uitvoeren van kwaadaardige acties.*

De indieners van het amendement schreven ook nog dat "deze defensieve mogelijkheid in de opdrachten van de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht aan een aanbeveling van het Vast Comité I (beantwoordt)" [13].

Alhoewel het ontegensprekelijk over een gewichtige materie van 'oorlog en vrede' gaat, heeft het initiatief op het moment van de indiening noch nadien veel ophef verwekt. Tijdens de parlementaire bespreking werden slechts enkele woorden aan deze zaak gewijd [14].
Zo stelde Senator Mahoux de vraag of de zinssnede waarin gewag wordt gemaakt van 'het recht van de gewapende conflicten' betekende dat de ADIV slechts met een eigen cyberaanval

[12] *Parl.St.*, Senaat, 2008-2009, 4-1053/6, blz. 11 e.v. Indieners : Vandenberghe H., Van Parys, T., Van den Driessche, P., de Bethune, S., Vankrunkelsven, P. & Delperée, F.

[13] Zie het jaarverslag van het Vast Comité I, 2006, blz. 11. Deze aanbeveling luidt :

> (…) dat de wet van 30 november 1998 de ADIV de opdracht heeft om de militaire informatica- en verbindingssystemen of de systemen die de minister van Landsverdediging beheert, te beschermen. Om deze opdracht effectief te kunnen waarnemen, is er nood aan het uitwerken van een aanvullend wettelijk kader dat toelaat elke poging van indringing in de computersystemen van de strijdkrachten en van de FOD Landsverdediging te identificeren en te neutraliseren.

[14] *Parl. St.* Senaat, 2008-2009, 4-1053/7, blz. 104-105

mag reageren "*als België in staat van oorlog verkeert*". Senator Vandenberghe antwoordde daarop dat de begrippen 'gewapend conflict' en 'oorlog' geen synoniemen waren.

> *Een gewapend conflict is een feitelijke toestand die door de regering en het Parlement wordt beoordeeld, terwijl oorlog en vrede gekoppeld zijn aan een formele beslissing, zoals een oorlogsverklaring en een vredesverdrag. Bijvoorbeeld, in Afghanistan is er een gewapend conflict, maar België heeft naar aanleiding van zijn militaire interventie aldaar geen oorlogsverklaring aan dat land goedgekeurd.* (…).
>
> En ook :
>
> *De bepaling betreffende het recht van België om met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten, geldt niet alleen wanneer België in staat van oorlog verkeert met een ander land, maar ook wanneer er zich in de wereld gewapende conflicten voordoen die een weerslag hebben op ons land (bijvoorbeeld de Palestijnse kwestie). Het amendement strekt ertoe de bevoegdheid van de Algemene Dienst Inlichtingen en Veiligheid op dit punt te preciseren.*[15]

Het amendement werd in de Senaatscommissie met 7 tegen 2 stemmen bij 1 onthouding aangenomen en nadien zonder meer in de Wet I&V opgenomen.

### *1.2 De National Defense Authorization Act 2012, section 954*

In 2012 gaf ook de Amerikaanse wetgever een wettelijke basis aan het militaire cyberoptreden. In het kader van de National Defense Authorisation Act for fiscal year 2012 (hierna NDAA 2012) machtigde de Amerikaanse wetgever het ministerie van Defensie om onder de leiding van President offensieve cyber-operaties uit te voeren om de Verenigde Staten, zijn belangen maar ook zijn bondgenoten te verdedigen[16].

Sectie 954 van de NDAA 2012 vermeldt :

> *Congress affirms that the Department of Defense has the capability, and upon the direction of the President, may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict, and (2) the War Powers Resolution (50 U.S.C. 1541 et seq.).*

Tijdens de bespreking van deze bepaling, die net zoals in bij haar Belgische tegenhanger bij amendement werd opgenomen, schreef het congres dat militaire activiteiten zich niet langer noodzakelijk tot het fysieke gevechtstheater beperkten en dat het gebruik van militaire cyberactiviteiten een kritisch onderdeel was om zichzelf en de bondgenoten te beschermen en wereldwijd de strijd tegen het terrorisme te voeren.[17]

---

[15] Ook senator Crombe Berton maakte een opmerking in de zin dat ze zich achter het amendement schaarde, maar van oordeel was dat de beperking tot militaire informatica- en verbindingssystemen of systemen van de minister van Landsverdediging te strikt was.

[16] National Defense Authorization Act for fiscal year 2012, sec. 954, H.R. 1540 (112-2012, 5.1.2012). Geraadpleegd op http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf
De bepalingen van de NDAA 2012 zijn door R. SHAWNNA., R. (2012, Februari, 6). *The state of cyberwar in the U.S.* Diplonews. Geraadpleegd op http://www.diplonews.com/pdf/DiploNews_jan_2012_The_State_Of_Cyberwar_In_The_US.pdf.

[17] Het amendement vormde oorspronkelijk sectie 962 van de tekst die in de Senaat voorlag, en als volgt luidde:

> (a) Congress affirms that the Secretary of Defense is authorized to conduct military activities in cyberspace. (b) The authority referred to in subsection (a) includes the authority to carry out a clandestine operation in cyberspace (1) in support of a military operation pursuant to the Authorization of use of military force (50 U.S.C.1541 note, Public Law 107-40) against a target located outside of the United States; or (2) to defend against a cyber attack against an asset of the Department of Defense (…). (d) Nothing in this section shall be construed to limit the authority of the Secretary of Defense to

Wat de precieze draagwijdte van deze bepaling is, is echter niet duidelijk, zoals Robert Chesney opmerkte[18]. De Amerikaanse Senaat bepaalde oorspronkelijk dat het kon gaan om clandestiene operaties, zonder er de aard van te bepalen, en zonder dat dit afbreuk deed aan de bevoegdheid van de minister van Defensie om andere militaire cyberactiviteiten uit te voeren[19].
In het Huis van Afgevaardigden werd de bepaling aangepast in de zin dat het clandestiene karakter van de cyberoperaties werd geweerd maar dat de term 'offensieve' operaties werd ingevoerd. Ook de oorspronkelijke bepaling dat het moest gaan om acties in het kader van militaire operaties tegen een doelwit buiten de Verenigde Staten, verdween.
Voor het overige stelden de Afgevaardigden enkel vast dat er geen historische precedenten te vinden zijn om de cyberoperaties duidelijk af te lijnen in termen van traditionele militaire activiteiten, maar dat er niettemin wel moet worden van uit gegaan dat deze operaties onderworpen zijn aan dezelfde beleidslijnen, principes en juridische normen als deze traditionele kinetische activiteiten [20], dit wil dus zeggen het 'Law of armed conflict'.

### *1.3 Meer vragen dan antwoorden ?*

Alhoewel duidelijk een stap voorwaarts, in de zin dat voor het eerst een (begin van) juridische regeling van de 'cyberwar' tot stand gebracht werd, werpen de Belgische en Amerikaanse wetgevende initiatieven heel veel vragen op.

Een eerste vraag bestaat er in te weten hoe we cyberaanvallen kunnen definiëren en hoe deze nieuwe vorm van 'oorlog' in de militaire en politieke theorievorming ingepast wordt. Hoe kunnen de (dikwijls) anonieme en op het eerste zicht weinig doelgerichte cyberaanvallen met zeer weinig menselijke slachtoffers, worden ingepast in de traditionele theorie over de 'oorlog', en hoe wordt dit alles afgelijnd ten aanzien van andere fenomenen die in de rand van een gewelddadig conflict voorkomen, zoals spionage en sabotage ?

---

conduct military activities in cyberspace" (Geraadpleegd op http://www.gpo.gov/fdsys/pkg/bills-112hr1540rfs/pdf/bills-112hr1540rfs.pdf).

In de Commissie (Committee Issues Mark, Section-by-section summary of the legislative provisions, p. 15-16) werd vermeld : "… As a result, military activities may not be confined to a physical battlefield, and the use of military cyber activities has become a critical part of the effort to protect U.S. and coalition forces and combat terrorism globally".

[18] Professor Chesney van de Universiteit van Texas wijst op de vele vragen die sec. 954 oproept, zowel binnen het Amerikaanse rechtsbestel als op vlak van het internationale recht.

Chesney, R. (2012, December 14). Offensive Cyberspace Operations, the NDAA, and the Title 10-Title 50 Debate [web log post]. Geraadpleegd op http://www.lawfareblog.com/2011/12/cyberoperations/. En zie eveneens

En zie ook Chesney, R. (2011). Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate. *Journal of national security law & policy*, 5, p. 539 et seq. Geraadpleegd op http://ssrn.com/abstract=1945392

[19] Committee Issues Mark, Section-by-section summary of the legislative provisions, gecit. :

> In certain instances, the most effective way to neutralize threats and protect U.S. and coalition forces is to undertake military cyber activities in a clandestine manner. While this section is not meant to identify all or in any way limit other possible military activities in cyberspace, the Secretary of Defense's authority includes the authority to conduct clandestine military activities in cyberspace in support of military operations pursuant to an armed conflict for which Congress has authorized the use of all necessary and appropriate force or to defend against a cyber attack on a Department of Defense asset.

[20] Conference Report on H.R. 1540, H. Rept. 112-329 - Explanatory note.

Het verband tussen cyberaanvallen en het 'recht van de gewapende conflicten' (LoAC) vormt een tweede onderzoeksvraag. Zowel de Belgische als de Amerikaanse wetgeving koppelen cyberaanvallen en cyberoperaties, terug als het ware vanzelfsprekend, aan deze tak van het internationaal recht. Dat de LoAC van toepassing is op dergelijke situaties, en in welke regels dan moeten gevolgd worden, staat echter niet bij voorbaat vast.

Een derde vraag betreft een louter Belgische materie. Wat is het verband tussen het artikel 11, § 1, 2° Wet I&V – de cybertegenaanvallen die de ADIV overeenkomstig het LoAC zou mogen uitvoeren - en de mogelijkheid die dezelfde dienst heeft tot inwinnen van inlichtingen via het binnenbreken in informaticasystemen zoals voorzien in het artikel 18/16 van deze wet.

In deze bijdrage zal blijken dat er veel vragen leven, die niet allemaal volledig beantwoord kunnen worden. Wel proberen we een eerste overzicht te geven van wat ter zake relevant is. Verder stellen we ons ook uitdrukkelijk tot doel via een uitgebreid voetnotenapparaat de belangrijkste bronnen aan te duiden die van belang zijn om de problematiek te doorgronden, zodat andere onderzoekers hierop kunnen voortbouwen.

## 2 Cyberwar en de politiek-militaire theorievorming

Zoals de lezer reeds heeft supra kunnen vaststellen worden zowel in de wetenschappelijke literatuur, als in de vele teksten die inzake 'cyberwar' beschikbaar zijn, de termen 'cyberoorlog' of 'cyberwarfare' en 'cyberaaanvallen gebruikt om allerlei gebeurtenissen te beschrijven, zonder dat er echter duidelijke definities worden gegeven.

In het reeds geciteerde artikel van Thomas Rid, komt de cybersecurity coordinator van het Witte Huis aan bod die stelt terminologische verwarring absoluut moet vermeden worden :

> *Words do matter, Schmidt remarked at a conference in February (2011). When we start throwing out these things, like we're in the midst of a cyberwar, or that cyberwar is around the corner, there's a lot of (those things) that don't actually apply, so we really have to define what it is that we're talking about .*

Dezelfde echo vinden we bij de Nederlandse minister van Defensie: "*(…) Wij weten hier nog te weinig over, wij hebben ons hierin nog te weinig verdiept, wat zijn eigenlijk de definities rondom cyberoperaties ?* " [21]

Te midden van de terminologische verwarring en precies daardoor wordt er soms ook voor gepleit om het fenomeen van de cyberwar in een nieuw veld op te nemen : het zou gaan om een 'other-then-war' fenomeen waar de traditionele denkpatronen en begripscategorieën niet van op toepassing zouden zijn. Dit is althans de conclusie van de gemeenschappelijke Russisch-Amerikaanse studie van het EastWest Institute :

> *It is possible that the binary peace vs. war paradigm is too simple for the complexities of the Internet Age …. Russia and the U.S., along with other willing parties, should explore the value of recognizing a third, 'other than-war' mode in order to clarify the application of existing Conventions and Protocols*[22].

[21] Hillen, J.S.J. (2011, april 13). *Van zwaard naar joystick. De rol van Defensie in de digitale frontlinie.* Toespraak van de minister van Defensie. Geraadpleegd op http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/toespraken/2011/04/13/toespraak-minister-hillen-tijdens-conferentie-cyber-operaties-van-het-koninklijk-instituut-van-ingenieurs/toespraak-cyber-op-geel-1.pdf, blz. 3.

[22] Rauscher, K.F., & A. Korotkov, A. (2011) :

Ook onderzoeker Duncan Hollis en  stelt dat het niet mogelijk is om de bestaande concepten die in het internationaal recht gangbaar zijn per analogie op cyberoperaties toe te passen : het aantal vragen daardoor opgeworpen worden zou te groot zijn[23].  Marco Benatar heeft ook heel wat twijfels (zie verder) en schrijft : "*maybe it is better as a matter of policy not to integrate cyber force in the jus ad bellum"*[24].

De zoektocht naar een goed begrip van cyber warfare is vanzelfsprekend niet nieuw.
Reeds in 1997 noteerde Lord Lyell voor de Noord-Atlantische Raad een aantal definities, waaronder deze van de United States Joint Chiefs of Staff en van de Duitse Bundestag[25]. In 1998 gaven Greenberg et al. geen sluitende beschrijving van het cyberwarfenomeen, maar wel een reeks voorbeelden van wat als '*warfare in the information age*' kon gelden, gaande van een DDoS-aanval[26], tot het buiten actie stellen van militaire elektronische commandosystemen[27].

Ook andere actoren hebben over de jaren heen heel wat definities hebben gegeven, waarbij soms ook andere benamingen, zoals 'Computer Network Attacks' (CNA) werden gebruikt om hetzelfde te beschrijven [28] [29].

---

> *There is no clear, internationally agreed upon definition of what would constitute a cyber war. In fact, there is considerable confusion. Senior government leaders from the same country have incompatible opinions about the most basic aspects of cyber war – its existence now, its reality or likely impact in the future. The current ambiguity is impeding policy development and clouding the application of existing Convention requirements. It is possible that the binary peace vs. war paradigm is too simple for the complexities of the Internet Age. In this recommendation, the joint analysis team offers a fresh approach for a path forward.*

[23] Zie Hollis, D.B. (2007). New Tools, New Rules: International Law and Information Operations. Temple University legal studies research paper series, (NO 2007-1). Geraadpleegd op http://ssrn.com/abstract=1009224.

[24] Benatar, M. (2009). The Use of Cyber Force: Need for Legal Justification?", *Goettingen Journal of International Law*, 1 (3), 375-396. Geraadpleegd op http://d-nb.info/999418149/34

[25] NATO Parliamentary Assembly, Science and Technology Committee. (1997). o.c.:

> The United States Joint Chiefs of Staff have defined information warfare as: Actions taken to achieve information superiority by affecting adversary information, information based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks."
>
> A report by the German Bundestag describes it as: "The comprehensive use of information and communication technology as well as technologies for the disturbance and destruction of hostile information and communications systems (IaC systems) in crisis and conflicts, in order to gain strategic and tactical superiority.

[26] Een Distributed Denial-of-Service aanval heeft tot doel een server of electronische service te overbelasten en zo er voor te zorgen dat deze server of service niet meer toehankelijk is voor de normale gebruikers. 'Distributed' betekent dat de aanval vanuit meerdere punten tegelijkertijd komt.

[27] Greenberg, L.T., Goofman, S.E., & Soo Hoo, K.J. (1998).

[28] Libicki, M.C. (2009) omschrijft een 'cyberattack' zeer algemeen als "the deliberate disruption or corruption by one state of a system of interest to another state".
Owens, W.A., Dam, K.W. & Lin, H.S. (2009) schrijven : "Cyberattack refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."
Deze definitie komt sterk overeen met deze die opgenomen is in de *DOD Dictionary of Military and Associated Terms* (2010 – 2012) onder het trefwoord Computer network operations (CNA): "*Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves"*. Geraadpleegd op http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html
Ook de Nato Glossary of terms and definitions - AAP-6 (2012) omschrijft CNA als een "*Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself*". Geraadpleegd op http://nsa.nato.int/nsa/zPublic/ap/aap6/AAP-6.pdf

De verwarring is dus groot, maar in tegenstelling tot wat de EastWest Institute aanduidt is er ons inziens niet meteen nood aan een volledig nieuw begrippenkader. Er bestaan inderdaad reeds voldoende aangrijpingspunten om duidelijk te bepalen wat onder cyberwar moet begrepen worden en hoe dit in de traditionele militaire theorie kan ingepast worden.

Belangwekkend is bijvoorbeeld wat (reeds) in 1999 in een rapport van de Noord-Atlantische Raad geschreven werd [30].
Op dat moment werd weliswaar nog de term 'Information warfare gehanteerd, en niet het thans meer modieuze 'cyberwar', maar de draagwijdte blijft. Er werd in vastgesteld dat er meerdere definities bestonden, maar uiteindelijk werd voor volgende synthese gekozen :

> *Information warfare could be defined as defensive and offensive operations, conducted by individuals or structured organisations with specific political and strategic goals, for the exploitation, disruption or destruction of data contained in computers or transmitted over the Internet and other networked information systems*[31].

Interessant is dat de Noord-Atlantische Raad daarbij duidelijk de politieke dimensie in rekening brengt.
Zoals reeds in de inleiding vermeld wijst Thomas Rid er op dat het politieke aspect één van de constitutieve elementen van de traditionele oorlogstheorie vormt en dus van belang is om te weten of we al dan niet met een cyberwar te maken hebben.
Ook de Nederlandse AIV en CAVV leggen een duidelijk verband tussen 'operationele cybercapaciteiten' en politieke doelstellingen en schrijven : "*politieke doelstellingen dienen vooraf te gaan aan militaire doelstellingen, of om met de militair theoreticus Von Clausewitz te spreken : oorlog is de voortzetting van de politiek met andere middelen*" [32]. Witte Huis-cybersecurity coordinator Schmidt vat dit op een goede manier samen : "*Information warfare should be limited to 'specific political and strategic goals' to avoid confusion with cybercrime or industrial espionage*" [33].

Deze punten laten toe om een verschil maken met cyberspionage ('cyberexploitatie') en computercriminaliteit (waaronder ook het zogenaamde 'hacktivisme' moet begrepen worden), fenomenen die dikwijls verward worden.

---

[29] Zie ook Wilson, C. (2006). *Information Operations and Cyberwar: Capabilities and Related Policy Issues.* Congressional Research Service. Geraadpleegd op http://www.fas.org/irp/crs/RL31787.pdf

> CNA is defined as effects intended to disrupt or destroy information resident in computers and computer networks. As a distinguishing feature, CNA normally relies on a data stream used as a weapon to execute an attack. For example, sending a digital signal stream through a network to instruct a controller to shut off the power flow is CNA.

[30] Nato parlementary assembly. Science and Technology Committee (rapporteur : Ehlers, V.J.) (1999). *Information Warfare and International Security.* Geraadpleegd op http://www.nato-pa.int/archivedpub/comrep/1999/as285stc-e.asp

[31] Bij cyberwar wordt bijna automatisch het verband met het Internet gelegd. Het feit dat cyberwapens zoals virussen enkel via het internet of fysieke dragers zouden kunnen worden verspreid, is evenwel misschien achterhaald. Zie het artikel van Nakashima, E. (2012, march 2012). *U.S. accelerating cyberweapon research.* Washington Post. Geraadpleegd op http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html?hpid=z1'. Er is sprake is van de zoektocht naar een nieuwe generatie van cyberwapens die ook militaire systemen die helemaal niet met het internet verbonden zijn, zouden kunnen binnendringen (via radiogolven).

[32] AIV/CAVV (2011), o.c., blz. 11. Ook bij de AIV en CAVV vindt men de verwijzing naar de welbekende theorie van Von Clausewitz.

[33] Ehlers, V.J., o.c., voetnoot 6.

Alhoewel cyberspionage inderdaad vanzelfsprekend militaire sytemen kan viseren en de voorbereiding op een (gewapende) aanval kan vormen[34] [35], heeft cyberspionage een volledig ander doel dan een cyberaanval.

Herbert Lin maakt het onderscheid duidelijk[36]. Bij een cyberattack is er :

> *the use of deliberate actions and operations – perhaps over an extended period of time – to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or network*s.

Bij cyberexploitatie gaat het daarentegen om :

> *to the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks. Cyberexploitations are usually clandestine and conducted with the smallest possible intervention that still allows extraction of the information sought*.

En belangrijk : "*they (= cyberexploitations) do not seek to disturb the normal functioning of a computer system or network from the user's point of view, and the best cyberexploitation is one that a user never notices"* .

Met andere woorden, vanuit de traditionele militaire theorievorming begrepen, bevinden we ons slechts in het domein de (cyber)'oorlog' indien (1) de aanvaller een duidelijk politiek en strategisch doel heeft, (2) de intentie bestaat om een Staat te dwingen om te doen wat de aanvaller hem wil opleggen (de 'karakterisering'[37]) en (3) de handelingen (potentieel) gewelddadig zijn.

## 3 Cyber(tegen)aanvallen en het ius ad bellum

Het feit dat cyberaanvallen in traditionele militaire termen al dan niet als 'oorlog' kunnen worden aangemerkt, betekent echter nog niet dat ze volgens het internationaal recht een 'gebruik van gewapend geweld' vormen en het 'recht op zelfverdediging' uitlokken.

---

[34] Wilson, C. (2006).

> Before a crisis develops, DOD seeks to prepare the IO (information operations) battlespace through intelligence, surveillance, and reconnaissance, and through extensive planning activities. This involves espionage, which in the case of IO, is usually performed through network tools that penetrate adversary systems to return information about system vulnerabilities, or that make unauthorized copies of important files. Tools used for CNE (Computer Network Exploitation) are similar to those used for CNA, but configured for intelligence collection rather than system disruption.

[35] Ook het 'Stuxnet' virus dat naar men aanneemt gecreëerd was met de bedoeling de infrastructuren van het Iraanse kernprogramma aan te vallen, is volgens het internetbeveiligheidsbedrijf Symantec met een vorm van spionage gestart. Zie Falliere, N., Murchu, L.O., & Chien, E. (2011). *W32.Stuxnet Dossier*. Symantec Security Respons : "First, the attackers needed to conduct reconnaissance. As each PLC (programmable logic controller) is configured in a unique manner, the attackers would first need the ICS's (industrial control system) schematics".

[36] Lin, H.S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of national security law & policy*, 4, 63-86. Geraadpleegd op http://insct.org/jnslp/wp-content/uploads/2010/08/06_Lin.pdf.
Zelfde redenering bij Owens, W.A., Dam, K.W., & Lin H.S. (2009).

[37] De 'karakterisering' is ook van belang op het niveau van de gewapende handeling op zich. Indien een – bij voorbeeld per abuis – een gewapende handeling wordt gesteld zonder de bedoeling de tegenstander te treffen, dan is in de context van het artikel 51 van het VN-handvest (zie verder) geen tegenaanval gewettigd.

Op dat moment bevinden we ons dus niet langer op het terrein van de militaire theorievorming, maar op het juridische terrein van de 'Law of Armed Conflict'[38].

Zowel de Belgische als de Amerikaanse wetgevers verwijzen expliciet aan de LoAC gekoppeld. De Belgische wetgever legt die koppeling waar het om 'tegenaanvallen' gaat, terwijl de Amerikaanse wetgever dit ook op 'offensive operations' toepast.

Traditioneel omvat het LoAC twee domeinen : het 'ius ad bellum' en het 'ius in bello'. Dit laatste wordt ook soms als het Humanitair oorlogsrecht omschreven en gaat over de oorlogsgebruiken : welke daden mag men stellen, tegen wie ? Wie (personen) en wat (goederen) tijdens de gevechtshandelingen moet worden ontzien, … [39] ? De regels die ter zake van toepassing zijn worden in hoofdzaak gevormd wordt door de verschillende Conventies van Genève. De Conventies van Den Haag leggen dan weer onder andere het gebruik van bepaalde wapens aan banden, en regelen diverse aspecten van de oorlogsvoering [40] [41].

Het ius ad bellum daarentegen - dat we hier verder bespreken - betreft de problematiek van het gewapend optreden op zich : welke omstandigheden wettigen in het internationaal recht dat men een tegenstander gewapend aanvalt of men in het kader van zelfverdediging terugslaat. Internationaalrechtelijk gaat het om de toepassing van de artikelen 2 en 51 van het Charter van de Verenigde Naties. Ook het artikel 5 van het Navo-verdrag moet in dit verband besproken worden[42].

Tenslotte zijn er ook nog de 'rules of engagement' (RoE) die elke Staat voor zijn militairen opstelt en een soort beschrijving vormen van hoe een tegenstander in de praktijk op het slagveld moet worden benaderd ten einde onnodig bloedvergieten te vermijden.

---

[38] In de commentaar bij artikel 2 van de Vierde conventie van Genève betreffende de bescherming van burgers in oorlogstijd, van 12 augustus 1949, wordt het verschil tussen het begrip 'oorlog' en 'gewapend conflict ' verduidelijkt (geraadpleegd op http://www.icrc.org/ihl.nsf/COM/380-600005?OpenDocument) :

> It remains to ascertain what is meant by "armed conflict". (…) It is possible to argue almost endlessly about the legal definition of "war". A State which uses arms to commit a hostile act against another State can always maintain that it is not making war, but merely engaging in a police action, or acting in legitimate self-defence. (…) Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2 (of this treaty), even if one of the Parties denies the existence of a state of war.

Het weze vermeld dat de Conventie van Genève weliswaar het '

[39] Het ius in bello is één van de oudste takken van het publiek recht. Reeds in het klassieke Griekenland bestonden regels die bepaalden met betrekking tot gewapend conflicten, dikwijls van godsdienstige aard.. De bekendste regel was dat er geen oorlog mocht gevoerd worden tijdens religieuze feesten, waaronder de Olympische spelen.

[40] Al deze verdragen zijn per thema te vinden op de website van het Internationaal Rood Kruis (http://www.icrc.org/ihl.nsf/TOPICS?OpenView).

[41] Sommige nationale Staten hebben deze elementen van (vooral) het ius in bello ten behoeve van hun troepen in handleidingen gebundeld.

Bij wijze van voorbeeld : U.S. Department of the Army. (1956 - 1976). *Field Manual 27-10 – The Law of Land Warfare*. Geraadpleegd op http://www.enlisted.info/field-manuals/fm-27-10-the-law-of-land-warfare.shtml

Of ook : U.K. Ministry of Defence - Joint Doctrine & Concepts Centre. (2004). *Joint service manual of the law of armed conflict (*Publication 383). Geraadpleegd op http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf

[42] Voor de volledigheid weze vermeld dat ook het artikel 42 van het Verdrag betreffende de Europese Unie (gemeenschappelijk veiligheids- en defensiebeleid) en het artikel 222 van het Verdrag betreffende de werking van de Europese Unie (solidariteitsclausule) vormen van militair optreden en bijstand voorzien.

Op (civiel) cybervlak richtte de EU de European Network and Information Security Agency (ENISA) op om cyberbedreigingen tegen te gaan. We laten het EU-luik in deze bijdrage evenwel buiten beschouwing.

Aangezien het niet de bedoeling is in deze bijdrage een gedetailleerde studie te maken van de toepassing van de genoemde artikelen in het VN-handvest, trekken we in het kort de aandacht op een aantal elementen.

### *3.1 Verband met het Handvest van de Verenigde Naties*

Het artikel 2 van het Handvest van de Verenigde Naties bepaalt dat de lidstaten zich zullen onthouden van het dreigen met of het gebruik van geweld tegen een andere Staat ('threat or use of force') [43]. De term 'use of force' zelf is artikel 2 van het VN-Handvest niet verder gespecifieerd, maar in artikelen 41 en 46 van hetzelfde Handvest, die over het optreden van de Veiligheidsraad handelen, wordt het kenmerk '*armed*' aan het begrip toegevoegd : 'use of *armed* force' of *gewapend* geweld.

Artikel 51 van hetzelfde handvest zegt verder dat Staten een recht op individuele of collectieve zelfverdediging hebben indien zij het slachtoffer van een gewapende aanval ('armed attack') zijn.

#### 3.1.1 Cyberaanvallen als gewapend geweld

Een eerste vraag die we ons stellen is of een informaticainstrument zoals een computervirus als 'wapen' kan gelden. Het VN-handvest heeft immers niet heeft beschreven wat een 'gewapende' aanval precies betekent. en daarvan afgeleid wat een 'wapen' precies is[44].

Michael Schmitt onderzocht de problematiek reeds in een vroeger stadium van de rechtsleer. Zijn bevinding is dat het VN-handvest niet alleen de inzet van de conventionele fysieke of kinetische wapens verbiedt, maar breder is dan dat [45]. In zijn meest recente bijdrage, in 2012, bevestigt hij dit, want anders zou de toepassing van het VN-verdrag slechts beperkt zijn tot het soort geweld dat kort na WOII technisch mogelijk was, hetgeen niet logisch zou zijn. Hij wordt daarin gevolgd door bijvoorbeeld Benatar die uit de rechtspraak van de Internationaal Hof van Justitie put[46]. Ook de Nederlandse AIV & CAVV spreken zich in dezelfde zin uit :

---

[43] United Nations. *Charter of the United Nations.* (1945). Geraadpleegd op http://www.un.org/en/documents/charter/chapter1.shtml :

> Art. 2. The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles…. (4). All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.
>
> Art. 51. Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.

[44] Het is interessant op te merken dat het geweld dat in artikel 2 van het handvest beschreven staat, zelfs niet noodzakelijk de effectieve inzet van een 'wapen' vereist : het 'dreigen' met geweld is op zich reeds verboden, zonder dat er een wapen wordt gebruikt.

[45] Schmitt, M.N. (1999) :

> The foregoing analysis shows that the prohibition of the threat or use of force includes armed, but not economic or political coercion. However, it does not demonstrate that the borders of 'force' precisely coincide with armed force, i.e., physical or kinetic force applied by conventional weaponry.

[46] Schmitt, M.N. (2012). "Attack as a term of art in international law : the cyber operations context". In Czosseck, C., Ottis, R., & Ziolkowski, K. (2012), gecit., p.311-317.

Idem : Benatar, M. (2009), p. 388. Hij verwijst naar de uitspraak van het ICJ van 8 juli 1996 over het gebruik van nucleaire wapens : *"These provisions [pertaining to the use of force in the UN Charter] do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon"* Geraadpleegd op http://d-nb.info/999418149/34

> *Niets in artikel 51 of het internationale gewoonterecht sluit specifieke soorten wapens of wapensystemen uit…. Er is dan ook geen reden waarom een digitale aanval op een computer- of informatiesysteem niet zou kunnen gelden als een gewapende aanval, indien de gevolgen ervan vergelijkbaar zijn met die van een aanval met conventionele of niet-conventionele wapens*.[47]

Dit sluit goed aan bij wat Thomas Rid en Peter McBurney onder een wapen verstaan, namelijk "*a tool that is used, or designed to be used, or designed to be ustd with the aim of threatening or causing physical, functional, or mental harm to structures, systems or living things*"[48]. Even treffend is wat Schmitt, reeds geciteerd, meegeeft : "*Instrumentalitie sthat produce [specifically physical damage and human injury]are weapons"*.[49]

Met andere woorden : ook cyberinstrumenten kunnen dus 'wapens' zijn of kunnen onder de noemer (dreigen met) 'gewapend' gewapend geweld vallen.

Een tweede vraag is of een aanval met een cyber'wapen', als 'geweld' kan gelden. De inzet van een cyberwapen levert immers weinig directe fysieke dwang op en er is geen bezetting van een grondgebied en geen zichtbare schade aan materieel of mensen, wat Miguel De Bruycker doet twijfelen aan aard ervan[50]. Bovendien zijn de effecten van de 'aanval' niet noodzakelijk onmiddellijk voelbaar, noch zijn de gevolgen die zich het eerst voordoen noodzakelijkerwijze de meest ernstige. Voor Marco Benetar ligt het antwoord niet voor de hand. Op basis van een tekstexegese van het artikel 2 van het Handvest en het onderzoek van voorbereidende werken en de praktijkcasussen, komt hij tot de vaststelling dat de inzet van cyberwapens wel altijd een inbreuk op het internationaal recht vormt, maar dat het niet zeker is of dit in het kader van het Handvest als een 'use of (armed)force' kan worden omschreven[51]. Talbot Jensen daarentegen is meer overtuigd : hij meent dat het gebrek aan fysieke vernielingskracht van een cyberwapen niet uitsluit dat het om een 'use of force' zou gaan [52].

Om over dit vraagstuk meer duidelijkheid te scheppen ontwierp Michael Schmitt een set van 'criteria' aan de hand waarvan bepaald kan worden of een cyberaanval als 'use of force' kan beschouwd worden in de zin van de artikelen 2 en 51 van het VN-handvest. In zijn visie kunnen cyberaanvallen dus wel degelijk als 'geweld' worden beschouwd, maar geldt er geen

---

[47] AIV/CAVV, o.c., blz. 20

[48] Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal*, 157 (1), 6-13. Geraadpleegd op http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354
Lorents & Ottis definieerden op een CCD-COE conferentie een cyberwapen als "an information technology-based system that is designed to damage the structure or operations of some other information technology-based system". Zie Lorents, P., & Ottis, R. (2010). Knowlegde based framework for cyber weapons and conflict. In Czosseck, C., & Podins, K. Conference on cyber conflict proceedings 2010, 129-142. Geraadpleegd op http://www.ccdcoe.org/articles/2010/Lorents_Ottis_KnowledgeBasedFramework.pdf

[49] Schmitt, M.N.. (1999). In zijn meest recente bijdrage - Schmitt, M.N. (2012) – herhaalt hij dit : *"… the act-based threshold of article 51 is but cognitive shorthand for a consequence-based legal regime.*" (p.287).

[50] De Bruycker, M. (2010). p. 37: "Bij internationale spanningen zullen spontane maar ook gerichte cyberaanvallen systematisch tot de eerste acties behoren. … Er vallen niet onmiddellijk slachtoffers en een cyberattack is niet erkend als een gewapende aanval".

[51] Benatar, M. (2009). p. 394-395. : "to claim that cyber force fits article 2(4) and 51 is overreaching".

[52] Zie onder andere Talbot Jensen, E. (2002). Computer attacks on critical national infrastructure : a use of force invoking the right of self-defense, *Stanford Journal of International Law,* 207-240.
De auteur duidt er op dat dit een kwestie is van intensiteit van de aanval : niet alle aanvallen komen over de 'threshold' of the use of force uit. Omgekeerd stelt hij dat het als een cyberaanval geen fysieke vernietiging tot gevolg heeft, dit niet uitsluit dat het toch onder de noemer 'use of force' zou vallen.

algemeen regel : aan de hand van de criteria er moet geval per geval uitgemaakt worden of dit wel degelijk zo is. Schmitt noemt zijn criteria, die international weerklank hebben gevonden, "*factors that can be expected to influence States when making use of force appraisals*"[53].

We citeerden hierboven ook reeds de AIV en de CAVV die geen reden zien waarom een digitale aanval op een computer- of informatiesysteem niet zou kunnen gelden als een gewapende aanval, indien de gevolgen ervan vergelijkbaar zijn met die van een aanval met conventionele of niet-conventionele wapens.[54]

Hierbij komen we aan de zogenaamde 'effects-based' interpretatie van cyberaanvallen, waarbij vooral gekeken worden naar de effecten die een militaire operatie op de tegenstander heeft, eerder dan naar de ingezette middelen en die door de meeste auteurs gedeeld wordt. Schmitt past dit toe in zijn juridische analyse : "*Armed coercion is not defined by whether or not kinetic energy is employed or released, but rather by the nature of the direct results caused, specifically physical damage and human injury*"[55]
Katherina Ziolkowski is dezelfde mening toegedaan :

> *in order to specify the meaning of 'use of [armed] force' conducted by the means of the Internet or other information and communication technologies, an effects-based approach inherent to public international law is surely to be considered appropriate …. Hereby, the comparison of the effects indirectly caused or intended by malicious cyber-activities with the effects usually caused or intended by conventional, biological or chemical weapons (BC-weapons) plays a paramount role*.[56]

En ook Charles Dunlap schrijft : "*cyber events that have violent effects are, therefore, typically the legal equivalent to armed attacks*". Vandaar dus :

> *Of course, a cyber technique can qualify as an armed attack. Cyber methodologies may qualify as "arms" under certain circumstances, and existing LoAC provisions provide ready analogies for construing their use as an 'attack'. Specifically, although cyber techniques may not involve kinetics, as a matter of law an attack may take place even without a weapon that uses them. … The leading view, therefore, among legal experts focuses on the consequences and calls for an effects-based analysis of a particular cyber incident to determine whether or not it equates to an 'armed attack' as understood by Article 51"* [57].

Deze theorie sluit bovendien ook goed aan bij de militaire doctrine waarin het concept 'effects based operations' voorkomt. Dit werd onder andere door David Deptula vorm gegeven. Deptula grijpt terug naar de constitutieve elementen van wat als 'oorlog' geldt – zie het begin van deze bijdrage - en wijst er op dat de bedoeling niet noodzakelijkerwijze is de tegenstander

---

[53] Schmitt, M.N. (2012). p. 314. Deze criteria zijn :severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, responsibility. De criteria warden voor het eerst gepubliceerd in Schmitt, M.N. (1999). Een gedetailleerde bespreking vindt men bij Ziolkowski, K. (2012). Ius at bellum in cyberspace – some thoughts on the 'Schmitt-criteria' for use of force. In Czosseck, C., Ottis, R., & Ziolkowski, K. (2012), gecit., p. 295-310.
En als antwoord daarop : Schmitt, M.N. (2012). The 'use of force' in cyberspace : a reply ot dr. Ziolkowsky'. In Czosseck, C., Ottis, R., & Ziolkowski, K. (2012), gecit., p. 311-317.
[54] AIV & CAVV. (2011).
[55] Schmitt, M.N.. (1999). In zijn meest recente bijdrage - Schmitt, M.N. (2012) – herhaalt hij dit : *"… the act-based threshold of article 51 is but cognitive shorthand for a consequence-based legal regime.*" (p.287).
[56] Schmitt, M.N. (2012). The 'use of force' in cyberspace : a reply to Dr. Ziolkowski. In Czosseck, C., Ottis, R., & Ziolkowski, K. (2012), gecit., p. 283-293.
[57] Dunlap, C.J.Jr. (2011). Perspectives for cyber strategists for law on cyberwar, *Strategic Studies Quarterly*, spring 2011, 81-99.

te vernietingen, maar wel een bepaalde 'political outcome' tot stand te brengen. Indien het mogelijk is een tegenstander op de knieën te krijgen zonder bloedvergieten, dan is dat dit de meest efficiënte manier van het gebruiken van 'force' :

> *Well beyond the activity of destroying an opposing force lies the ultimate purpose of war— to compel a positive political outcome. The use of force to control rather than destroy an opponent's ability to act lends a different perspective to the most effective use of force. Control—the ability to dominate an adversary's influence on strategic events—does not necessarily mean the ability to manipulate individual tactical actions*.[58]

Met andere woorden, er kan van 'use of (armed) force' - in de zin van artikel 2 van het VN-handvest - sprake zijn indien een tegenstrever in het kader van politieke doelstellingen, via ICT-kanalen of –instrumenten militaire of civiele systemen treft of dreigt te treffen, dit wil zeggen vernietigt of al dan niet tijdelijk buiten gebruik stelt. In theorie kan dergelijke aanval dus ook een tegenaanval in het kader van het recht op zelfverdediging, in de zin van artikel 51 van het handvest, rechtvaardigen, voorzover de 'aanval' een bepaalde graad van intensiteit bereikt. In volgende onderdeel wordt dit in meer detail besproken.

### 3.1.2 De intensiteit van een aanval : pearl harbor or a death of a thousand cuts ?

Alhoewel sommigen menen dat een grootschalige aanval van het type 'Pearl Harbor' op komst is, is dit verre van zeker. In dit verband moet de vraag worden gesteld welke 'intensiteit' een cyberaanval moet hebben om een tegenaanval te wettigen.
Voorzover de inzet van cyberwapens niet gepaard gaat met een massieve conventionele aanval, doet de inzet ervan zich immers dikwijls voor als heimelijk en is ze – tot op heden- zelden opvallend agressief.
Dergelijke situatie kan, naar de woorden van Richard Clarke, weliswaar leiden tot een 'death of a thousand cuts', dit wil zeggen een sluipende en slopende vorm van agressie door duizend kleine messneden waarbij elke snede op zich niet fataal is, maar het geheel ervan wel[59].

---

[58] Deptula, D.A. (2001). Effects-based operations : changing in the nature of warfare. Aerospace Education Foundation. Geraadpleegd op http://www.afa.org/mitchell/reports/0901ebo.pdf. De auteur schrijft :

> Centuries of surface warfare created the common view that the intrinsic purpose of military force is the destruction of an enemy's military force.… Well beyond the activity of destroying an opposing force lies the ultimate purpose of war— to compel a positive political outcome. The use of force to control rather than destroy an opponent's ability to act lends a different perspective to the most effective use of force. Control—the ability to dominate an adversary's influence on strategic events—does not necessarily mean the ability to manipulate individual tactical actions.

En :

> As technological innovation accelerates, 'non-lethal' weapons and cyberwar enabled by information operations, will become operative means in parallel war. … Indeed, the ultimate application of parallel war would involve few destructive weapons at all—effects are its objective, not destruction.

Voor een overzicht van de theorie omtrent effects-based-operations, zie Davies, P.K. (2006). *Effects-base operations, a grand challange for the analytical community*, Rand Corporation. Geraadpleegd op http://www.rand.org/pubs/monograph_reports/2006/MR1477.pdf. .

[59] Zie het interview dat Richard Clarke gaf aan Waugh, R. (2012, march 28). "Every major company in the U.S. has been hacked by China': Cyber-espionage warning from U.S security chief who warned of 9/11". The Daily Mail. Geraadpleegd op http://www.dailymail.co.uk/sciencetech/article-2121624/Every-major-company-U-S-hacked-China-Cyber-espionage-warning-U-S-security-chief-warned-9-11.html
Clarke wil echter niet het beeld van 'Pearl Harbor' gebruiken.

> My greatest fear," Clarke says, "is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and

Dit kan trouwens ook tot een welbewuste tactiek vormen, zoals de CCD-COE uitdrukt:

> *In such a volatile environment, by deliberately remaining below the threshold of use of force and at the same time using national policy cover as shield against investigations and prosecution, an attacking entity may believe there is less likelihood of reprisal even if the attacker's identity is suspected.*[60]

De vraag gaat er dus om te weten hoe intens een aanval moet zijn om onder de toepassing van de internationaalrechtelijke regels te vallen en een tegenaanval te wettigen, en of enkel aanvallen met 'fysieke' schade relevant zijn.

In het internationaal recht is het niet nodig dat het geweld per se veel slachtoffers moet maken of veel schade moet veroorzaken. Meer nog : een aanval moet zelfs niet effectief uitgevoerd worden, aangezien het VN-verdrag in artikel 2 niet enkel het geweld op zich verbiedt, maar ook het loutere dreigen ermee. Dunlap stelt in dit verband dat de essentie van een gewapende handeling (of het dreigen ermee) er in bestaat dat lichamelijke en/of materiële schade en vernieling wordt teweeg gebracht, of dat het risico bestaat dat dit het geval zou zijn[61].

Schmitt merkt op dat volgens het internationaal recht op huidig moment de 'physical consequences standard' geldt : enkel aanvallen met fysieke gevolgen mogen als (gewapend) geweld bestempeld worden. Hij voegt er wel aan toe dat deze visie wellicht te eng is [62]. Voor de AIV & CAVV kan een cyberaanval met zekerheid als een gewapende aanval in de zin van het VN-handvest worden beschouwd, wanneer een digitale aanval tot een aanmerkelijk aantal dodelijke slachtoffers leidt of tot grootschalige vernietiging van vitale infrastructuur, militaire platforms of installaties of civiele goederen.
Indien de aanval echter geen fysieke schade aanricht, is dit minder evident, maar ook dat sluiten de AIV & CAVV niet direct uit. Ze menen dat :

> *een serieuze georganiseerde digitale aanval op essentiële functies van de staat kan worden aangemerkt als een 'gewapende aanval' in de zin van artikel 51, indien dit mogelijk of daadwerkelijk leidt tot ernstige verstoring van het functioneren van de Staat of tot ernstige en langdurige gevolgen voor de stabiliteit van de Staat. Hierbij moet sprake zijn van een (aanhoudende poging tot) ontwrichting van de Staat en/of de samenleving en niet slechts een belemmering of vertraging bij het normaal uitvoeren van taken.*

Met andere woorden : de 'eenvoudige' defacing van sites en 'eenvoudige' DDoS-aanvallen vormen geen gewapende aanval die een tegenaanval verantwoorden, maar

> *"een digitale aanval gericht op het gehele financiële stelsel of een aanval waardoor de overheid niet meer in staat zou zijn om essentiële taken uit te voeren – bijvoorbeeld een aanval op het gehele militaire communicatie- en commandonetwerk, waardoor men niet meer in staat zou zijn om de krijgsmacht aan te sturen – moet gelijk gesteld worden met een gewapende aanval"*[63].

---

development stolen by the Chinese. And we never really see the single event that makes us do something about it.

[60] Tikk, E., Kaska, K., & Vigul, L. (2010), p. 103

[61] Dunlap, C.J.Jr. (2011), p. 85.

[62] Schmitt, M.N. (2012) . p.288 :

> In particular, the law's qualitative focus on the type of harm may yield somewhat to a quantitative analysis such that a cyber operation causing serious consequences, such as severe economic effects or significant disruption of societal functions, may be characterized as armed attack even if it does not cause death, injury, damage or destruction. Time will tell.

[63] AIV & CAVV. (2011). p.20.

Het is duidelijk dat dit alles niettemin niet eenvoudig te bepalen is. Zeker is alleszins dat het gebruikte geweld meer dan een simpele 'inconvenience' tot gevolg moet hebben[64], maar wat er onder een 'serieuze aanval', een 'ernstige verstoring', een 'onwrichting' en 'essentiële taken' moet verstaan worden, is voer voor debat.

Ten slotte zijn nog twee elementen van belang.
Volgens de tradionele interpretatie van het artikel 51 van het VN-charter is een (tegen)aanval in het kader van wettige zelfverdediging slechts mogelijk is wanneer de Staat zelf eerst het slachtoffer van een gewapende aanval is geweest. De logica van een 'tegen'aanval is dat er eerst een aanval is geweest. Sean Condron wijst echter op de 'Caroline'-interpretatie, genoemd naar een casus uit 1837 (!). Deze theorie stelt dat het mogelijk is om een vorm van anticipatorische aanval op te zetten, bij wijze van zelfverdediging, indien dit de enige mogelijkheid is om een geplande gewapende aanval op het eigen land te vermijden[65] [66]. Het moet gaan om een situatie waar de aanval imminent is en met geen enkele andere mogelijkheid kan worden afgeslaan. De noodzaak van zelfverdediging moet zijn : "*instant, overwhelming, and leaving no choice of means, and no moment for deliberation*". Wanneer het gaat om een situatie waarin er sprake is van sluipende en slopende aanvallen – de 'death of a thousand cuts' – is het echter wellicht moeilijk om dit als 'overwhelming' te beschouwen.

Een tweede nuance betreft het moment van optreden in het kader van de zelfverdediging. Volgens het internationaal gewoonterecht moet de tegenaanval 'noodzakelijk, proportioneel en onmiddellijk' zijn. Dit laatste betekent dat er moet worden opgetreden op het moment dat de initiele aanval nog bezig is, en niet nadien.
In feite gaat het er echter vooral om dat een 'tegenaanval' reële politiek-militaire doeleinden moet hebben. Dit wil zeggen dat de tegenaanval tot doel en als effect moet hebben om de initiële agressie te doen stoppen. Een tegenaanval die echter in feite een 'represaille' is en tot doel heeft te 'straffen', is in het kader van de zelfverdediging niet toegelaten.[67] Het is in deze zin dat ook het tijdsaspect van de tegenaanval moet worden bekeken.

Inzake cyberaanvallen compliceert dit natuurlijk de zaken eens te meer : door de snelheid van de aanval is het moeilijk om de agressie te stoppen eens ze zich heeft voorgedaan. De term

[64] Dunlap, C.J.Jr. (2011), p. 85

[65] Zie hierover Condron, S.M. (2007). Getting it right : protecting american critical infrastructure in cyberspace, *Harvard Journal of Law and Technology*, 20(2), 403-422. Geraadpleegd op http://www.thefreelibrary.com/Getting+it+right%3A+protecting+American+critical+infrastructure+in...-a0197364705).
Zie ook Van den Hole, L. (2003). Anticipatory self-defence under international law, *American University International Law review*, 69-106. Geraadpleegd op http://auilr.org/pdf/19/19-1-4.pdf. Van den Hole stelt dat het niet vereist is dat een Staat op een aanval moet wachten vooraleer zelf (gewapend) op te treden : "the right of self-defence, inherent in every state, includes logically the right of anticipatory self-defence, ensuring that a defender has sufficient flexibility to take defensive hostile measures without waiting for the attack.".
Hij waarschuwt weliswaar met een citaat van M. Lacy uit diens artikel 'Self-defence or self-denial : the proliferation of weapons of mass-destruction' : "Without the *sine qua non* of necessity, proportionality and immediacy, anticipatory self-defence becomes nothing more than a slippery slope of naked aggression."

[66] Talbot Jensen (2002) gaat zelfs nog verder en stelt een Staat een recht van zelfverdediging heeft en (anticipatorisch) mag optreden zelfs wanneer er helemaal nog geen sprake is van een gewapende aanval. Hij pleit voor een "right to protect themselves with a proportionate response in self-defense, including anticipatory self-defense, even if the attact does not constitute an armed attack".

[67] Van den Hole, L. (2003). P.104. Ook Melzer, N. (2011). p.18

'onmiddellijke' tegenaanval stelt in de praktijk dus problemen. Indien het gaat om een aanval waarvan men met voldoende redenen kan aannemen dat het gaat om één aanval in een serie die nog moet komen, dan hoeft de tegenaanval weliswaar niet noodzakelijk onmiddellijk na de eerste aanval te gebeuren[68], maar of het gewoonterecht buiten dit geval toelaat dat de reactie in de vorm van een tegenaanval pas enige tijd nadien komt, is betwist[69].
Ook inzake dit aspect vormt de cyberoorlog dus een buitenbeentje in het veld van het LoAC.

### 3.1.3 De toewijzing of attributie van de aanval

Met de problematiek van de toewijzing of 'attributie' van de aanval komen we op het wellicht meest delicatie vraagstuk inzake cyberwar uit.
Reeds in 1996 wees een Chinese militaire analist er op dat het bijzonder moeilijk is om uit te maken wie precies een aanval uitvoert :

> *An information war is inexpensive, as the enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from its enemy* [70].

Het CCD COE is van mening dat deze kwestie de grootste struikelblok vormt om de cyberaanvallen in het kader van de bekende LoAC te kunnen inpassen : *"As long as there is no state attribution of cyber attacks, LoAC will offer no remedies and the particular incident must be managed under a different area of law*[71].

De moeilijkheid om de aanval toe te wijzen en de aanvaller precies te kunnen identificeren levert inderdaad meerdere problemen op.

Een eerste probleem heeft te maken met het ontdekken van het politiek-strategische doel van de aanval en de aanvaller. Zoals gezien vormt dit een constitutief element van het fenomeen 'oorlog' en dus ook van cyberoorlog. De identificatie van de tegenstander zal immers een licht werpen op het (politieke) doel van de agressie. Aan een tegenstander die onbekend is en dit ook blijft, kan geen politiek doel worden aangekleefd.

Een tweede probleem betreft het doelwit van de tegenaanval. Om tot de tegenaanval te kunnen overgaan, moet men zich van de identiteit en status van de aanvaller vergewissen.
In het reeds geciteerde artikel zegt Hirsh :

> *One of the things that scares U.S. military officials the most about cyberwar is that, if an attack comes, they may not know who the enemy is. Cyberexperts say the toughest*

---

[68] Van den Hole, L. (2003). p. 104.
[69] Pro : Condron, S.M. (2007). Contra : Melzer, N. (2011) : "It is therefore erroneous to claim that self-defensive action can be taken "after" an armed attack has occurred. Instead, it must be directed "against" an imminent or ongoing attack with the aim of preventing or repelling it" (p.17).
[70] Wei Jinching. (1996, june 25). Information War : a new form of people's war (translated from Chinese version). *Liberation Army Daily*. Geraadpleegd op http://www.fas.org/irp/world/china/docs/iw_wei.htm.
In de film
[71] Tikk., E., Kaska, K., & Vigul, L. (2010) :

> The case closest to the application of LoAC was the Georgian case, where cyber attacks against Georgian governmental websites fell into the timeframe of a nationally declared state of war. We have concluded in the Georgian analysis that it would be highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective evidence of the case is too vague to meet the necessary criteria of both state involvement and gravity of effect. Yet, when looking at the context of when these attacks occurred and how well the desired effect was achieved, if state attribution would be possible, the applicability of LoAC would be much more likely.

> *problem of all is attribution - knowing who's breaking into your grid and where they are if you wish to retaliate.*

Bij cybergebeurtenissen is het dikwijls zeer moeilijk en bovendien tijdrovend om te weten wie de aanvaller precies is. Meer nog, in sommige gevallen komt men tot de vaststelling dat zelfs systemen die zich in het eigen – aangevallen – land bevinden, aan de aanval deelnemen ! Dit was bijvoorbeeld zo bij de gebeurtenissen in Estland, waar de aanvallen konden getraceerd worden naar systemen in Estland zelf, naast 178 (!) andere landen.

Het identificatieprobleem heeft bovendien nog andere belangrijke gevolgen. Onder andere in het kader van de Conventies van Genève moeten de zogenaamde beschermde groepen ontzien worden[72]. Het is derhalve van belang dat oorsprong de aanval duidelijk toegewezen wordt, want een 'blinde' tegenaanval is niet gerechtvaardigd. Bovendien kan de aard van de reactie verschillend zijn naargelang de aanvaller een Staat is of een 'non-state-actor'[73].

Niet alle auteurs vinden dat een Staat die in het kader van een cyberaanval het recht op zelfverdediging inroept, zich door deze moeilijk op te lossen problemen van een tegenaanval moet laten afbrengen.
Talbot Jensen schrijft dat de tijd die nodig is om de tegenstander goed en wel te identificeren, (wellicht) een 'luxe' vormt die niet beschikbaar is bij een cyberaanval[74] :

> *The requirement to attribute an attack before responding is likely to be a time-consuming process, a luxury unavailable in the cyber attack era… As a general principle, therefore, the requirement…. presents a significant gap in a nation's ability to defend itself.*

Hij voegt daaraan toe dat in het geval van cyberaanval, de aangevallen partij zijn reactie mag afstemmen op de aard van de bedreiging en het getroffen doelwit, en niet op de aard van de aanvaller of van de door hem ingezette middelen[75] : ook de goederen van beschermde personen die een cyberaanval zouden inzetten, zouden door een tegenaanval mogen worden getroffen.

Ook Condron stelt dat het niet altijd haalbaar is om de cyberaanvaller te identificeren en de aanval te karakteriseren. Het unieke karakter van de cyberwar laat volgens hem toe dat een Staat, gelet op de snelheid waarop de aanval, een tegenaanval 'te goeder trouw' mag uitvoeren : "*To address the unique nature of cyber warfare, international law should provide a safe harbor for states who initiate a good-faith response to an attack, thus acting in cyber self-defense, without first attributing and characterizing the attack*"[76]. Het overleven van de Staat hangt naar zijn woorden, af van 'onmiddellijke, robuste en agressieve reactie'[77]. Zeker in het geval van een aanval op kritische infrastructuur, zou volgens hem het internationaal recht de aangevallen Staat moeten toelaten om tot een tegenaanval over te gaan, zonder dat de

[72] Hetzelfde is waar voor bepaalde goederen, bijvoorbeeld cultureel erfgoed. Zo kan een bepaalde server ook gegevens bevatten die cultureel immaterieel erfgoed zijn, bijvoorbeeld geluidsopnames. Het is vanzelfsprekend zeer moeilijk dit uit te maken.
[73] Codron, S.M. (2007) : "If the attacker is a state actor, the response must comply with the United Nations Charter and customary international law. On the other hand, if the attacker is a non-state actor, domestic criminal law will likely govern the response".
[74] Talbot Jensen, E. (2002). p. 232.
[75] Idem. p. 235.

[76] Condron, S.M. (2007). p. 415. Dit standpunt wordt ook overgenomen door Hoisington, M. (2009). Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense. *Boston College International and Comparitive Law Review*, 32(2), 439-454. Geraadpleegd op http://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16
[77] Condron, S.M. (2007). p. 415 : : "State survival may depend on an immediate, robust, and aggressive response".

traditionele voorwaarden daartoe zouden vervuld zijn [78]. Dit is een standpunt dat moeilijk verdedigbaar is.

Ten slotte is het nog de problematiek van de neutraliteit van derde Staten. Het respecteren van de neutraliteit van landen en burgers die niet bij een gewapend conflict betrokken zijn, vormt één van de basisprincipes van de LoAC vastgelegd is.
Terug stelt de cyber(tegen)aanval in dit verband problemen. Een aanvaller kan immers gebruik maken van systemen van onschuldige derden die in andere landen gevestigd zijn, of kan zijn aanval laten verlopen via systemen die in andere landen worden beheerd. Door een gans 'leger' van gekaapte systemen in te zetten – een zogenaamd 'Botnet' - vermenigvuldigt de aanvaller zijn kracht en brengt hij de aangevallen Staat bovendien in verwarring zodat de reactie bemoeilijkt wordt. Het bijvoorbeeld bij wijze van tegenaanval buiten actie stellen van een of meer internationale DNS-servers[79] zou het internetverkeer wereldwijd verstoren en eventueel de operaties van en binnen derde landen ernstig in het gedrang kunnen brengen.
Tijdens de bespreking van regelgeving die in de Amerikaanse NDAA 2012- sectie 954 werd opgenomen, kwam dit probleem aan bod en werd dit als een belangrijk struikelblok ervaren :

> *As the public reporting has repeatedly emphasized, the big stumbling block in such operations is the fact that they can have a debilitating impact on servers located in other countries, raising the question whether this amounts to an infringement of that other country's sovereignty or perhaps even its rights as a 'neutral' in an armed conflict*[80].

De verschillende geciteerde problemen wijzen er op dat we de kwestie van de attributie van een cyberaanval inderdaad op de limieten van het internationale recht botsen, aangezien het terugslaan naar (de systemen van) Staten of non-state actors die niet met zekerheid als dader werden geïdentificeerd moeilijk verdedigbaar is. Wellicht is het enkel mogelijk om er voor te zorgen dat de systemen waarmee de aanval wordt uitgevoerd niet langer voor dat doel kunnen worden gebruikt, dus een 'neutralisering' om de aanval te doen stoppen, maar niet meer dan dat.

Ten slotte moet het attributieprobleem echter ook worden genuanceerd.
Dat een aanval die via elektronische kanalen verloopt, in het bijzonder via het internet, moeilijk via elektronische weg te traceren is, is duidelijk. Niettemin is het niet onmogelijk. Op dit punt wordt immers vooruitgang geboekt, bijvoorbeeld door te werken met 'behavior-based algoritmes'[81]. Bovendien is een 'elektronische' identificatie niet noodzakelijk de enige mogelijkheid. Het internationaal recht vergt immers niet dat de attributie zelf elektronisch

[78] Condron, S.M. (2007). p. 421-422 : "International law should not always require a state to fully satisfy the traditional necessity requirements when acting in self-defense of critical infrastructure". Hij voegt er in zijn conclusie ook nog aan toe : "The nature of the threat requires a reversal of the presumption that a cyber attack on critical infrastructure is a criminal matter. The new presumption must be that a cyber attack on critical infrastructure is a national security threat".

[79] DNS-servers zijn Domain Name Servers. Zij regelen belangrijke aspecten van het wereldwijde internetverkeer door de domeinnamen van sites te verbinden met technische internetadressen van servers (IP-adressen).

[80] Chesney, R. (2012, December 14).

[81] Department of Defense Cyberspace Policy Report (2011). *Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934.* Geraadpleegd op http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf
Behavior-based-algoritmen zoeken in de aanval bepaalde kenmerkende patronen of elementen – in feite de modus operandi – die typisch is voor een welbepaalde aanvaller.

gebeurt, wel dat de dader geïdentificeerd wordt. Wanneer het om conventionele aanvallen gaat, is dit veelal duidelijk omdat de aanvaller fysiek optreedt en kentekenen draagt of bepaalde fysieke sporen nalaat. Niettemin zijn er ook conventionele aanvallen waar de aanvaller – weliswaar onregelmatig - geen kentekenen draagt of reeds van het toneel verdwenen is vooraleer hij kan worden geïdentificeerd. Dit belet niet dat hij mogelijkerwijze achteraf via andere middelen, die onder andere tot de sfeer van de inlichtingendiensten behoren, kan worden aangewezen. Bovendien hebben we reeds vermeld dat niet elke aanval een gewapende aanval vormt. Slechts de intense aanvallen vallen onder het LoAC, en voorzover ze niet met een conventionele kinetische aanval gepaard gaan, is de schaal ervan toch zo groot dat het voor een aanvaller moeilijk zal zijn alle sporen uit te wissen.

### 3.1.4 Aanvallen op niet militaire doelwitten of kritische infrastructuur

Zoals gezegd, is het niet zo dat cyberaanvallen zich vooral op militaire doelwitten richten. Deze zijn immers technisch zeer goed beschermd en zijn zomaar aan het Internet gekoppeld. Vandaar dat aanvallers zich ook op niet-militaire doelwitten (zullen) richten. Dergelijke 'asymetrische' aanvallen zijn zeer waarschijnlijk[82]. Dikwijls komt daarbij het thema van aanvallen op civiele infrastructuur zoals elektriciteitscentrales en -netten, watervoorziening en communicatiesystemen aan bod. Deze systemen staan als doelwit hoog op de lijst, niet alleen omdat veel militaire toepassingen (deels) via deze systemen gevoed worden, maar ook omdat het lamleggen er van een zeer grote impact op de economie en de burgers heeft en op het eerste zicht relatief zonder veel bloedvergieten kan verlopen. Dit is niet nieuw : aanvallen op burgerdoelwitten zijn in het LoAC op zich verboden, maar militaire (lucht)operaties nemen dikwijls ook wegen en bruggen tot doelwit om de militaire tegenstander tot staan te brengen, maar treffen daarbij natuurlijk ook door de burgerbevolking die deze infrastructuur gebruikt om zich te verplaatsen, voedsel aan te voeren of zieken te transporteren.

Een aantal auteurs zijn van mening dat cyberaanvallen op de zogenaamde 'kritische infrastructuur' extra waakzaamheid vergen. Zelfs indien ze geen militaire doelen omvatten of er weinige fysieke schade is, moeten ze dergelijke aanvallen toch als bijzonder ernstig worden beschouwd. We citeerden reeds Condron die stelde dat als het gaat om een aanval op kritische infrastructuur, de traditionele voorwaarden om tot een tegenaanval over te gaan, (deels) zouden moeten worden genegeerd. In zijn conclusie voegt hij daar nog aan toe :

> *The nature of the threat requires a reversal of the presumption that a cyber attack on critical infrastructure is a criminal matter. The new presumption must be that a cyber attack on critical infrastructure is a national security threat*"[83].

Met andere woorden : elke aanval op een kritische infrastructuur kan volgens deze doctrine tot een militaire tegenaanval aanleiding geven, ongeacht de doelstelling of aard van de aanvaller, en zelfs indien de aanvaller een non-state-actor die in principe enkel onder het normale criminele rechtssysteem zou vallen en dus niet in het kader van het LoAC zou

[82] In de Amerikaanse Joint publication 3-0 'Joint Operations' van 11.8.2011 is vermeld (Chap. 1, 2, c) :

> Joint operations increasingly occur in urban terrain and in cyberspace. The US homeland and other US interests are potential targets for direct and indirect attack. Adversary actions are likely to follow asymmetric principles. They will avoid "hard"(defended) targets and attack vulnerable ones. Vulnerable targets may include US and partner nation lines of communications (LOCs), ports, airports, staging areas, civilian populations, critical infrastructure, and economic centers.

Geraadpleegd op http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf

[83] Condron,S.M. (2007). p. 421-422.

kunnen aangevallen worden. Deze stelling gaat natuurlijk verder dan wat in het traditionele LoAC gebruikelijk is.
Interessant is evenwel wat Talbot Jensen aan het debat toevoegt. Hij vindt het aangewezen dat aan mogelijke tegenstanders zonder omhaal duidelijk wordt gemaakt welke reactie ze mogen verwachten als ze bepaalde handelingen stellen. Talbot Jensen stelt vanuit Amerikaans perspectief voor dat de Verenigde Staten een lijst van kritische nationale infrastructuur zou opstellen én publiek maken. Op die manier zou duidelijk wordt gemaakt dat het binnendringen in deze systemen quasi automatisch als een aanval in de zin van het LoAC zou worden beschouwd, die met een tegenaanval zou beantwoord worden[84].
Benatar op zijn beurt werpt op dat het weliswaar de individuele Staten zelf zijn die dergelijke lijsten zouden opstellen, zodat ze relatief subjectief zouden zijn : wat precies 'kritisch' is, ligt internationaal immers niet vast[85]. Ook binnen de NAVO is bijvoorbeeld nog geen eenstemmigheid bereikt over de term 'critical infrastructure'[86] [87].

Aangezien de CCD-COE schreef dat de algemene troebelheid van de cyberwar ('general murkiness') en het gebrek aan duidelijke beleidslijnen en procedures, cyberaanvallen aantrekkelijk maken voor wie er zich wil mee inlaten[88], heeft dit voorstel om een lijst van kritische infrastructuur op te stellen en het duidelijk verkondigen van wat de gevolgen van een aanval daarop zijn, alleszins het voordeel van de duidelijkheid.
Weliswaar komt de vraag naar boven of de niét in de lijst opgenomen infrastructuur dan in feite 'vogelvrij' voor aanvallers is ?
Nadeel is bovendien dat een dergelijke lijst de (politieke) beleidsalternatieven ingeval van een aanval verkleint, terwijl het fenomeen 'oorlog' juist rond deze politieke aspecten draait.
In het volgende hoofdstuk betreffende de mogelijke toepassing van het artikel 5 van het NAVO-verdrag wordt geopperd dat het inbouwen van dergelijk 'automatisme' weliswaar het afschrikkingseffect op mogelijke aanvallers zou verhogen – hetgeen na te streven is – maar het tegelijkertijd de opties om op een crisis te reageren zou verminderen. Het idee is niettemin het overdenken waard.

### *3.2 Verband met het NAVO-verdrag*

Hierboven werd aangetoond dat een cyberaanval als gewapend geweld in de zin van het VN-handvest kan beschouwd worden, naargelang de intensiteit ervan.
De vraag die we hier stellen is hoe de NAVO hierover denkt. Het is bijvoorbeeld interessant op te merken dat ten tijde van de cyberaanvallen op Estland in 2007, geen enkele van de NAVO-partners artikel 5 van het NAVO-verdrag van 4 april 1949 heeft ingeroepen. Dit

[84] Talbot Jensen, E. (2002). p.236-237 :
> "an attempt to try to hack into these systems would, in other words, be viewed as a demonstration of hostile intent to which the United States would respond proportionally in anticipatory self-defense. Furthermore, a response will occur once the passive protective measures have been penetrated".

[85] Benetar, M. (2009).
[86] Nato Parliamentary Assembly. Committee reports (rapporteur : Sverre Myrli) (2009). *NATO and Cyber Defence*. (73 DSCFC 09 E bis). Par. 17. Geraadpleegd op http://www.nato-pa.int/default.Asp?SHORTCUT=1782
[87] Een aanzet van een (Belgische) definitie van kritische civiele systemen zou kunnen gevonden worden in artikel 11, § 2, 1° Wet I&V die het heeft over "*bedreigingen die het voorbestaan van de bevolking, het nationale patrimonium of het economisch potentieel van het land in gevaar brengen*". Systemen die voor dit voortbestaan nodig zijn, zijn dan kritische systemen.
[88] Tikk, E., Kaska, K., & Vigul, L. (2011). p. 103

artikel voorziet in een wederzijdse bijstandverplichting ingeval van een 'gewapende'aanval[89]. Op een NAVO-persconferentie werd de vraag gesteld of Estland zelf artikel 5 van het NAVO-verdrag had ingeroepen. De NAVO-woordvoerder verklaarde : "*No, they did not ask for invoking Article 5. They asked, as I said, for solidarity and technical assistance. They got that"*. [90]

Bij gebrek aan formele vraag tot toepassing van artikel 5, kon de NAVO natuurlijk geen formeel antwoord, noch in positieve noch in negatieve zin geven. De kwestie bleef dus onuitgesproken. Wel voegde de NAVO-woordvoerder er nog aan toe :

> *These attacks show that defence has to be understood in a 21st Century context as well. It is not any more just about artillery and tanks. It is about modern defence capabilities. That is why at the Riga summit NATO established a cyber defence capability as NATO.*

De Noord-Atlantische Raad besprak dit punt op een vergadering in 2009 en vroeg zich of het artikel 5 van het verdrag ook ingeval van cyberaanvallen zou kunnen worden ingeroepen. Uit de discussie bleek dat de NAVO van mening was dat er niet voldoende elementen op tafel lagen om een definitief oordeel uit te spreken, en – wellicht vooral – dat dit de opties van de Alliantie ingeval van een crisis teveel zou beperken : "*Cyber defence poses a special problem for NATO policymakers, who are seeking to maximize the deterrend effect of the Alliance in a domain that has a novel combination of limitations* [91]".

Inderdaad, door cyberaanvallen rechtstreeks aan het artikel 5 van het Verdrag te koppelen, zou de alliantie bij een dergelijke aanval in een 'automatische militaire logica' terechtkomen waardoor 'politieke' oplossingen misschien onmogelijk zouden worden gemaakt.

### *3.3 Hoe verhouden de Amerikaanse en Belgische regelgeving zich hiertoe ?*

Er werd reeds op gewezen dat heel wat aspecten van de LoAC vragen oproepen wanneer ze op conflicten in cyberspace worden toegepast.

Daarmee geconfronteerd, definiëren evenwel noch de NDAA 2012, section 954 ('offensive operations in cyberspace'), noch de Wet I&V, artikel 11, § 1, 2° ('cyberaanvallen'), de gebruikte terminologie. Evenmin bepalen ze klaar en duidelijk de voorwaarden duidelijk waaronder een cyberaanval tot een tegenaanval aanleiding kan geven.

---

[89] *North Atlantic Treaty Organisation. (1949). Het Noord-Atlantisch Verdrag.* Geraadpleegd op http://www.nato.int/cps/nl/natolive/official_texts_17120.htm :

> *Art. 5. De partijen komen overeen dat een gewapende aanval tegen een of meer van hen in Europa of Noord-Amerika als een aanval tegen hen allen zal worden beschouwd; zij komen bijgevolg overeen dat, indien zulk een gewapende aanval plaatsvindt, ieder van hen de aldus aangevallen partij of partijen zal bijstaan, in de uitoefening van het recht tot individuele of collectieve zelfverdediging erkend in Artikel 51 van het Handvest van de Verenigde Naties.….*

Het artikel 5 werd tot nog toe slechts éénmaal ingeroepen, met name na de terroristische aanvallen van 11 september 2001.

[90] Persconverentie naar aanleiding van de cyberaanvallen op Estland, 23 mei 2007, door NAVO-woordvoerder Appathurai, J. Geraadpleegd op http://www.nato.int/cps/en/natolive/opinions_8313.htm?selectedLocale=en

[91] Nato Parliamentary Assembly. Committee reports (rapporteur : Sverre Myrli) (2009). Par. 59 – 61 :

> The decision to announce an expansion of Article 5 to encompass cyber attacks may cause potential aggressors to think twice, but would it excessively restrict NATO's options in a crisis management scenario ? How can the danger of misidentifying an aggressor be avoided ? If the source of a cyber attack can be identified with certainty, which forms of cyber attack can NATO consider as direct acts of aggression against a Member or Members, and which constitute indirect acts of aggression? And what is the best way for NATO to deal with the mobilization of informal volunteer groups to carry out deniable cyber attacks on behalf of a non-NATO member government ?

Door dergelijke hiaten bestaat, zoals voormalige Amerikaanse vice-stafchef J.E. Cartwright het omschreef, de aanval vooral 'in het oog van de toeschouwer': "*an act of war in cyberspace (exits) in the eyes of the beholder*"[92].
Bij gebrek aan (inter)nationale juridische concensus over de kwalificatie van de feiten, is het met andere woorden de 'aangevallen' partij die zelf bepaalt of hoe hij de aanval zal definiëren. Of zoals Libicki stelde : *"At the end of the day, the answer to whether a particular attack is an act of war comes down to this: Is it in your interest to declare it so ?"* [93] . Het hoeft niet te worden gezegd dat dergelijke positie (of gebrek daaraan) in een internationale context heel wat onduidelijkheden en zelfs risico's met zich mee brengt [94].

In het kader van de Belgische Wet I&V is het gebrek aan defnitie enigszins ongewoon. In het artikel 3 van deze wet vindt men alle in deze wet gehanteerde termen en begrippen verklaard, maar niet het begrip 'cyberaanval'. Dat de voorbereidende werken wél een definitie bevatten – die eventueel voor verbetering vatbaar is – is juist, maar beter ware het geweest in de wet zelf een omschrijving op te geven, waarbij best ook duidelijk het onderscheid met cyberspionage en cybercriminaliteit zou duidelijk worden gesteld.

Bovendien is het aangewezen om niet alleen in de wetgeving, maar ook in andere officiële beleidsdocumenten duidelijkheid te scheppen. Aangezien sommige Staten ten behoeve van hun troepen het LoAC te boek stellen, ligt het voor de hand om in deze codificaties ook de regels inzake cyberwar te bepalen.
Voor België is dit nog niet het geval, maar op Amerikaans vlak wordt de Amerikaanse Field Manual 27-10 (Law of War Manual) in de toekomst aangepast en zal een hoofdstuk over cyberspace operations bevatten[95]. Deze nieuwe versie van het handboek is echter nog niet gepubliceerd.
Daarnaast, of eventueel in de genoemde Manual geïntegreerd, bestaan er ook zogenaamde 'standing rules of engagement (SRoE), waarin ook een plaats voor cyber operaties kan worden ingeruimd. Wat de USA betreft blikte Clay Wilson reeds 2007 vooruit naar de nieuwe SRoE waar in onder andere de principes van proportionaliteit en het onderscheid tussen militaire en burgers zouden opgenomen worden[96]. Het tot stand brengen van deze SRoE is echter een werk van lange adem. Ook hoe en door wie moet opgetreden worden ter verdediging van militaire en andere doelwitten, van 'critical infrastructure' en zelfs van private ondernemingen zou in dit kader moeten duidelijk worden[97].

Wel blijkt dat de twee wetgevers de drempel om over cyber(tegen)aanvallen en cyberoperaties te kunnen spreken, hoe dan ook heel hoog hebben gelegd.

---

[92] Gecit. door Hirsh, M. (2011, July 23).
[93] Libicki, M.C. (2009). Appendix A, in fine.

[94] *Zie het officiële persbericht gebracht door Pellerin. C. (2012, may 7). U.S., China Must Work Together on Cyber, Panetta Says. American Forces Press Service. Geraadpleegd op* http://www.defense.gov/news/newsarticle.aspx?id=116235 *: "It's extremely important that we work together to develop ways to avoid any miscalculation or misperception that could lead to crisis in this area, Panetta said"*.

[95] Dunlap, C.J.Jr. (2011). Eindnoot 90
[96] Wilson, C. (2006). p. 11.

[97] De SRoE zouden volgens de laatste berichten "*in the next few months*" tot stand komen. Zie het officiële persartikel gebracht door Anoniem. (2012, march 28. van 28 maart 2012. *Cyber Rules of Engagement*. Airforce-magazine.com. Geraadpleegd op http://www.airforce-magazine.com/DRArchive/Pages/2012/March%202012/March%2028%202012/CyberRulesofEngagement.aspx

Doordat zowel sectie 954 van de NDAA 2012 als artikel 11 § 2 Wet I&V een verband met de LoAC leggen, kan een cyberoperatie of cyber(tegen)aanval enkel gevoerd worden in het kader van dit LoAC, en dus in het kader van de artikelen 2 en 51 van het VN-handvest.
Met andere woorden, wanneer de Verenigde Staten of België operaties zouden uitvoeren in toepassing van deze rechtsregels, dan bevinden zich uitdrukkelijk in een hypothese van een gewapend en internationaalrechtelijk conflict met een tegenstrever, wat de 'gewelddrempel' dus zeer zeer hoog legt, zowel voor offensieve cyberoperaties, als voor defensieve in het kader van tegenaanvallen.

Weliswaar leek voormalig Amerikaans vice-stafchef James E. Cartwright in het voorjaar van 2012 met zijn in de pers gerapporteerde uitspraak "*We need to draw a line that we believe is reasonable*", te impliceren dat er een (openlijke) 'demonstratie' van de Amerikaanse cybercapaciteiten klaarblijkelijk ook buiten het kader van een werkelijke gewapend conflict zou kunnen gebeuren : "*Deterrence will require some demonstration of U.S. attack power*" [98]. Met andere woorden : er moet een voorbeeld worden gesteld, ongeacht de kwestie van de LoAC. Dit doet sterk denken aan de reeds geciteerde stelling van Talbot Jensen (2002) die pleit voor een "right to protect themselves with a proportionate response in self-defense, including anticipatory self-defense, even if the attact does not constitute an armed attack"[99]. Maar of een dergelijk idee van het officiële beleid deel uitmaakt is zeer de vraag.

Voorzover ook alle andere juridische vragen inzake aanval en tegenaanval zouden uitgeklaard zijn lijken de mogelijkheden die de Amerikaanse en Belgische wetgevers hebben gecreëerd dus hoe dan ook vooral theoretisch te zijn. Slechts in het kader en als onderdeel van een veel groter internationaal (conventioneel) gewapend conflict lijken ze toepasbaar. In dat geval zullen kwesties zoals het vereiste geweldniveau en attributie en andere problemen die de cyberoorlog met zich meebrengen trouwens in een heel ander licht staan dan nu louter theoretisch kan benaderd worden.

## 4 De cybertegenaanval in het kader van artikel 11 van de wet I&V versus de uitzonderlijke methode bedoeld in het artikel 18/16 van dezelfde wet

In het vorige punt kwamen we tot de vaststelling dat de mogelijkheid die de Belgische wetgever aan de ADIV bood om tot cybertegenaanvallen over te gaan, in de praktijk zelden kan aangegrepen worden, aangezien de gewelddrempel en slechts in het kader van een internationaalrechtelijke context tot uiting kan komen, dus in toepassing van de artikelen 2 en 51 van het VN-handvest.

Evenwel beschikt de ADIV (en trouwens ook de VSSE) over bepaalde actiemogelijkheden in het kader van de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, waarover het in de inleiding van deze bijdrage ging.

---

[98] Fryer-Biggs, Z. (2012, may 7). *Debate Slows New U.S. Cyber Rules.* Defense News (a Gannett Company). Geraadpleegd op http://www.defensenews.com/article/20120507/DEFREG02/305070004/Debate-Slows-New-U-S-Cyber-Rules.

> We (need to) draw a line that we believe is reasonable, but first you put in place the elements of deterrence. In all likelihood, that deterrence will require some demonstration of U.S. attack power, Cartwright said: "At some point, they're going to have to do something that's illustrative, and then communicate.

[99] Talbot Jensen (2002).

Het gaat daarbij om de toepassing van een 'uitzonderlijke methode voor het verzamelen van gegevens', waarbij de inlichtingendiensten gemachtigd kunnen worden om, aldus artikel 18/16 Wet I&V :

> *al dan niet met behulp van technische middelen, valse signalen, valse sleutels of valse hoedanigheden :*
> *1° toegang te krijgen tot een informaticasysteem;*
> *2° er elke beveiliging van op te heffen;*
> *3° er technische voorzieningen in aan te brengen teneinde de door het informaticasysteem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen en te decoderen;*
> *4° er de door het informaticasysteem relevante opgeslagen, verwerkte of doorgestuurde gegevens op eender welke manier van over te nemen.*

Zoals gezien in punt 2.1 legt de verantwoording bij het amendement nr. 83 een verband is tussen de cyberdefensie en deze methode. De verantwoording spreekt immers over de mogelijkheid :

> *te reageren op dergelijke aanvallen, met indien nodig de mogelijkheid tot inwinnen van inlichtingen via intrusie in informaticasystemen zoals voorzien in het voorgestelde artikel 18/16. Een dergelijke actie moet er toe leiden de aanvallers te identificeren en de aanval te neutraliseren.*

Een hieruit voortvloeiende vraag is of deADIV, wanneer ze deze methode bijvoorbeeld toepast ten aanzien van buitenlandse (militaire) systemen die trachten binnen te dringen in Belgische systemen[100], daardoor niet de facto in de hypothese van een cyberaanval in het kader van het LoAC terecht komt.

### *4.1 Kan de methode bedoeld in artikel 18/16 toegepast worden in het kader van de cybertegenaanval die onder het LoAC valt ?*

Op het eerste zicht lijkt inderdaad, zoals de indieners van het amendement nr. 83 stellen, niets te beletten dat de methode die in het artikel 18/16 Wet I&V beschreven is, in het kader van de cybertegenaanval gebruikt wordt.
We hebben er immers op gewezen dat de identificatie van de aanvaller – de attributie - noodzakelijk is om in het kader van de LoAC het recht op zelfverdediging uit te oefenen. De methode waar artikel 18/16 Wet I&V op slaat, is dan in feite een vorm van 'cyberexploitatie'. Cyberexploitatie kan ter voorbereiding een cyber(tegen)aanval dienen, maar maakt op zich er geen deel van uit; het is een vorm van spionage.

Bovendien blijken een aantal bepalingen van 18/16 niet goed met de aard van de cyber(tegen)aanval overeen te stemmen.

---

[100] De vraag of het mogelijk is om artikel 18/16 toe te passen op computersystemen die buiten het Belgische grondgebied gevestigd zijn moet o.i. bevestigend beantwoord worden. In het kader van het toezichtsonderzoek nr. 2007.181 beveelt het Vast Comité I onder andere aan "*dat er ook wordt voorzien in de mogelijkheid (voor de VSSE) om systemen in het buitenland te neutraliseren in geval van aanvallen tegen de informatiesystemen van andere ministeries dan Landsverdediging….*"
Zie Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten. (2011). *Besluiten en aanbevelingen van het onderzoek naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om de informatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland.* (2007.181). Geraadpleegd op http://www.comiteri.be/images/pdf/eigen_publicaties/verslag_181_nl.pdf

Het artikel 18/16 past immers duidelijk in het kader van een zuivere niet-offensieve inlichtingenoperatie, zo mogelijk ongedetecteerd door de tegenstander. De tekst van het artikel stelt :

> *Het binnendringen door de inlichtingen- en veiligheidsdiensten in de informaticasystemen kan enkel het verzamelen van relevante gegevens die erin werden opgeslagen, verwerkt of doorgestuurd tot doel hebben, zonder dat er een onomkeerbare vernietiging of wijziging van deze gegevens gebeurt.*

De bedoeling van het binnendringen in een computersysteem in het kader van de cyberaanval is daardoor heel verschillend van een inlichtingenactie, aangezien een cyberaanval tot doel heeft dwang uit te oefenen. De methode hiertoe kan (deels) gelijklopen – namelijk het binnendringen in het systeem van een tegenstander - maar de ratio en het te bekomen 'effect' is volledig anders.

Verder is er ook het feit dat het toepassen van de methode van artikel 18/16 slechts kan gebeuren na goedkeuring door een administratieve Commissie (de zgn. BIM-commissie).
Nog los van de vraag of een dergelijke administratieve procedure verenigbaar is met de snelheid van een cyber(tegen)aanval, komt het ook vreemd over dat dergelijke militaire actie (zijdelings) zou onderworpen worden aan de goedkeuring van een commissie die verder geen band heeft met het militair apparaat.

Hoe dan leidt de verantwoording van amendement nr. 83 die de methode bedoeld in artikel 18/16 § 1 van de Wet I&V aan de problematiek van de cybertegenaanval koppelt, ons op een gevaarlijk pad.
Per hypothese zou immers, aangezien de cybertegenaanval volgens de regels van de LoAC moet verlopen, het binnendringen in een buitenlands informaticasysteem overeenkomstig artikel 18/16, § 1 binnen ditzelfde kader, zelf deel gaan uitmaken van een gewapend conflict.
Men zou dan kunnen aanvoeren dat, als het ware gevangen door de definitie van de LoAC, de ADIV daardoor de facto een handeling zou stellen die als het gebruik van (niet toegestaan) geweld in de zin artikel 2 van het VN-verdrag zou kunnen beschouwd worden.
Dit gaat zonder twijfel veel verder dan wat oorspronkelijk de bedoeling was.
Vandaar dat het o.i. zeer belangrijk is duidelijk te stellen dat, in tegenstelling tot wat in de verantwoording bij het amendement nr. 83 doet vermoeden, de toepassing van de uitzonderlijke methode die in artikel 18/16 § 1 aan het arsenaal van de Belgische inlichtingendiensten werd toegevoegd – nl. de intrusie in informaticasystemen – als juridisch volledig losstaand van een cyber(tegen)aanval overeenkomstig artikel 11 van dezelfde wet moet worden gezien.
De inzet van de methode bedoeld in artikel 18/16, §1 maakt dus op zich geen deel uit van de (tegen)aanval en valt dus niet onder toepassing van de LoAC, zelfs niet indien ze ermee gelijk lopen of ze zou dienen ter voorbereiding ervan.

### *4.2 Kan artikel 18/16 Wet I&V toch worden toegepast in militaire omstandigheden ?*

Het voorgaande belet dus niet dat de militaire inlichtingendienst de methode van artikel 18/16, § 1 zou kunnen gebruiken in het kader van zijn 'normale' cyberactiviteiten. Dit binnendringen moet dan echter niet begrepen worden als voortvloeiende uit de taak die de ADIV heeft om cyberaanvallen op zich af te slaan (artikel 11, § 1, 2° Wet I&V), als wel als deel uitmakend van de algemene bevoegdheid van de ADIV die vastgelegd is in artikel 11, § 1, 1° juncto artikel 18/9, § 1, 2° Wet I&V.

Deze algemene bevoegdheid van de ADIV is zeer breed en laat hem toe om inlichtingen in winnen, te analyseren en te verwerken met betrekking tot elke activiteit die een bedreiging vormt voor de onschendbaarheid van het nationale grondgebied, de defensieplannen, de vervulling van de taak van de strijdkrachten, enz., inclusief de bescherming van het wetenschappelijk en economisch militair potentieel dat bij privéondernemingen aanwezig is. Zelfs bedreigingen tegen 'kritische infrastructuur' kunnen geacht worden binnen het aandachtsveld van de ADIV te vallen, aangezien artikel 11, § 1, 2° het ook heeft over "*bedreigingen die (met middelen van militaire aard) het voorbestaan van de bevolking, het nationale patrimonium of het economisch potentieel van het land in gevaar brengen*".

In het kader van deze bevoegdheid kan de ADIV dus ten aanzien van een buitenlandse bedreiging via de methode van artikel 18/16 in de systemen binnendringen van waaruit de cyber'aanvallen' georganiseerd worden, los van de vraag of deze als 'gebruik van (gewapend) geweld te catalogeren zijn.
Zelfs indien het enkel mogelijk is om slechts in het aanvallend systeem te gaan 'kijken' – aangezien dit moet gebeuren "*zonder dat er een onomkeerbare vernietiging of wijziging van deze gegevens gebeurt"*, dan toch kan dit binnendringen op zich reeds een effect hebben.
Ofwel is de aanvaller er zich van bewust zijn dat hij gedetecteerd is, en zal dit hem eventueel er toe nopen om zijn acties stil te leggen. De acties die hij onderneemt zijn immers niet alleen illegaal, maar de grootste vijand van een in het donker opererende aanvaller is immers het licht dat op hem wordt gericht.
Indien daarentegen de aanvaller er zich niet van bewust is dat hij ontmaskerd werd, kan de ADIV via diplomatieke of andere kanalen bepaalde acties ondernemen. Indien blijkt dat de aanval verloopt via een gekaapt systeem van een onschuldige derde, dan kan ook deze via discrete kanalen op de hoogte worden gesteld.

Weliswaar vereist de toepassing van artikel 18/16 Wet I&V dat bepaalde procedures gevolgd worden, waaronder zoals reeds vermeld een tussenkomst door de BIM-commissie. Waar we hierboven stelden dat deze tussenkomst vreemd leek in het kader van een militaire cyber(tegen)aanval, wekt dit in het kader van het toepassen van de methode van artikel 18/16 als onderdeel van de algemene taakomschrijving van de ADIV geen verwondering. Het gaat dan gewoon om een methode die binnen de traditionele bevoegdheden van de ADIV toegepast wordt.

Zoals reeds gezegd is de vraag weliswaar ook of deze procedure - die een voorafgaande machtiging door de BIM-commissie vergt - een tijdig optreden mogelijk maakt, gelet op de snelheid waarop cyberaanvallen gebeuren. Wel is een spoedprocedure mogelijk waarbij het diensthoofd van de ADIV veel sneller kan optreden. Belangrijk is ook dat vereiste dat de methode van artikel 18/16 door een 'inlichtingenofficier' moet worden uitgevoerd. De personen die instaan voor het detecteren van cyberaanvallen zouden dus deze hoedanigheid moeten hebben, hetzij door personen met deze hoedanigheid moeten worden bijgestaan.

# 5 Epiloog

Voor de lente 2013 is de publicatie van de 'The Tallinn Manual - Manual on International Law Applicable to Cyber Warfare' in het vooruitzicht gesteld.

Het gaat om de vrucht van zeer intensieve werkzaamheden van het NATO CCD-COE en wordt als een *"authoritative reference on the international law applicable to cyber conflict"* aankondigd [101].
De nakende publicatie is voor de Belgische wetgever wellicht een ideale kans om in het licht ervan, de juridische aspecten van de cyberaanval en -tegenaanval aan bod komen, aan verder onderzoek te onderwerpen. Met deze bijdrage hebben we alvast een aanzet hiertoe willen geven.

* * *

[101] Zie *Internet* : http://www.ccdcoe.org/249.html