BELGIAN INTELLIGENCE STUDIES CENTRE BISC

Cyber war – Ius ad bellum

Brussel – 19.11.2012

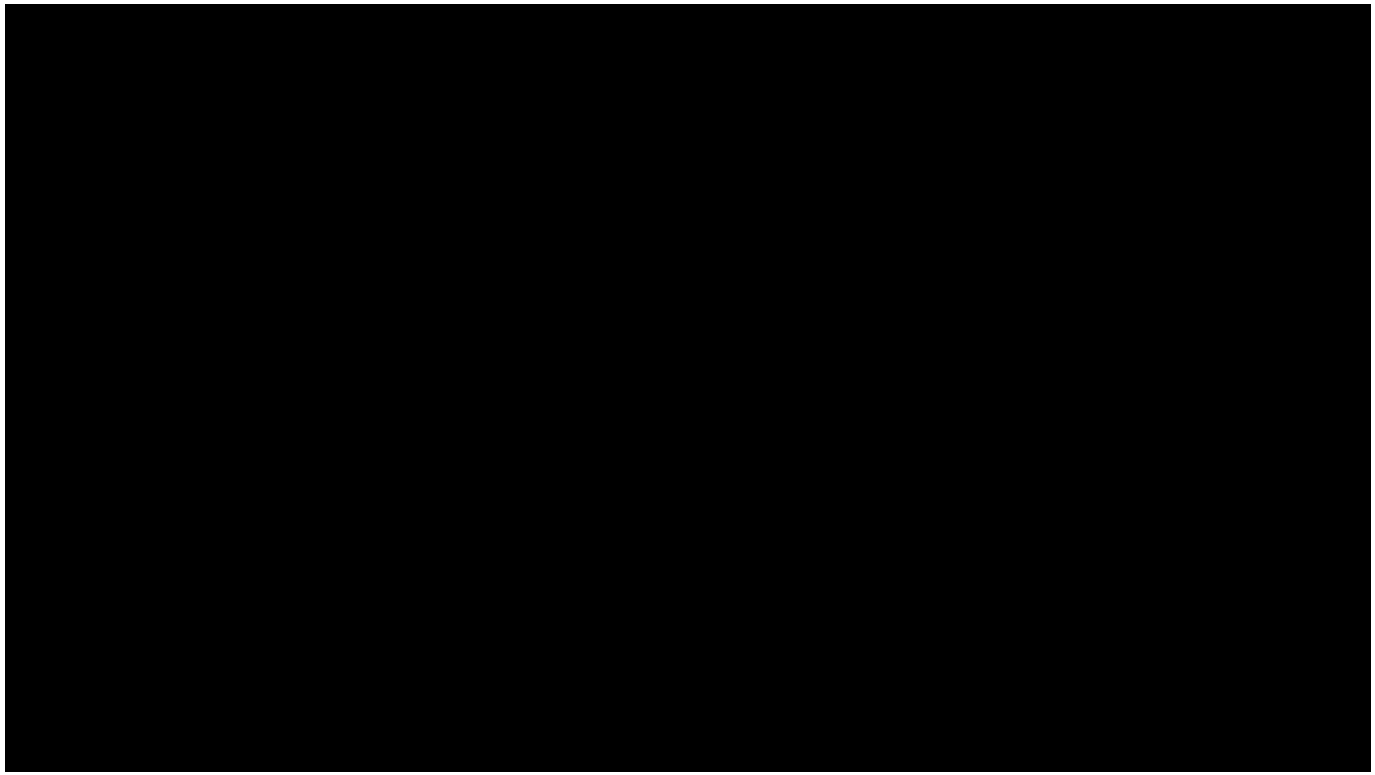
Frank Franceus, Commissaris-auditor
Vast Comité I

Inhoud

- Begripsvorming fenomeen cyber war
- Belgische & US wetgevende initiatieven (2010 / 2012)
- Begrijpen van cyber war : politiek-militaire theorievorming & ius ad bellum
- Verband met artikel 18/16 Wet I&V (1998)

Caveats

- Bindt niet het Vast Comité I
- Zeer omvangrijk onderwerp
- Geen definitieve antwoorden : denkproces
- Referentie naar uitgebreide rechtsleer
- Het ‘laatste’ woord : ‘Tallinn’ manual



« ... does this constitute an act of war ? » (Leon Panetta, 2011)

- 'Believers vs non-believers'
  - *« The next Pearl Harbor could well be a cyberattack »* (Leon Panetta)
  - *« We will instead have this death of a thousand cuts »* (Richard Clarke) = een soort 'koude oorlog'
  - *« There has never been, nor will there ever be a cyberwar » (*Prof. Thomas Rid, Kings College London)

- Cyberdefence = big business : $ 80 – 140 miljard (2015 – Reuters)

- 'Si vis pacem, para bellum'
  - Cyberstrijdkrachten : USA (USCybercom / NSA), Israël (Unit 8200), China (PLA) ... (Carr / Lewis / Temlin)
  - België, USA : wetgevende initiatieven

- Term 'war' (oorlog) = niet adequaat
  - Beter : 'use of force as sanctioned by art. 2 & 51 UNO-charter'
  - Idem term 'aanval'

Wetgevende initiatieven : België, USA

België : Wet 4 februari 2010 (wijziging Wet 1998 I&V)	*USA : National Defense Autorisation Act (NDAA) 2012*
Art. 11, § 1 : De Algemene Dienst Inlichting en Veiligheid heeft als opdracht : (…) ■in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, ■de aanval te neutraliseren en er de daders van te identificeren, ■onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren ■overeenkomstig de bepalingen van het recht van de gewapende conflicten	Sect. 954 : 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.).

Law of Armed Conflict (LoAC) : Ius ad bellum / ius in bello

- Ius ad bellum - « recht tot oorlog » = rechtsregels om tot oorlog over te gaan / om een gewapend conflict te starten (aanval) of om er op te reageren (tegenaanval)
  - UNO-handvest (art. 2 & 51)
  - Gewoonterecht & internationale rechtspraak

- Ius in bello – « recht tijdens de oorlog » = rechtsregels tijdens het voeren van de oorlog
  - Vooral : Conventies van Genève (1947) : humanitair oorlogsrecht
  - Ook : Conventies van Den Haag : inperking van ingezette wapens / methodes
  - + Specifieke internationale conventies

Het fenomeen ‘cyber war’

- Een gevaarlijke begripsverwarring : « *When we start throwing out these things, like we’re in the midst of a cyber war, or that cyber war is around the corner, … we really have to define what it is that we’re talking about* » (Schmidt, White House cybercoordinator, 2011)

- Een groot gebrek aan definities en onderscheiden : term cyber ’war’ gebruikt voor DDoS, cyberspionage, cybersabotage, cyberactivisme (bv.defacing), ...

- Grote juridische onduidelijkheid : « *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 »(Joint US/Russia study, East-West Institute, 2011)*

- ➔ Hoe moeten we ‘cyber war’ begrijpen en welke regels zijn er van op toepassing ?

  Twee referentiekaders : 1° traditioneel politiek-militaire theorievorming
  2° ‘ius ad bellum’ (UNO-handvest & doctrine)

Referentiekader 1 : traditionele politieke-militaire doctrine (a)

- Traditionele politiek-militaire doctrine : ‘functionele’ / instrumentele aspect van ‘oorlog’

  Inadequate term, maar :

  - ‘oorlog is de voortzetting van politiek’ (Von Clausewitz)
  - via dwang een tegenstrever zijn wil opleggen
  - moet een specifiek (politiek) doel hebben
  - eindpunt = wapenstilstand / vrede

- Speelt een belangrijke rol in NAVO-standpunten :

  “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” (Noord-Atlantische Raad, Science/Technological Committee 1999)

- Functionele instrumentele ‘aspect van ‘oorlog’ is primordiaal om cyber’oorlog’ te begrijpen.

Referentiekader 1 : traditionele politieke-militaire doctrine (b)

- Traditionele criteria (politiek instrument, specifiek doel, tegenstrever, dwang, eindpunt) laten toe om een inzicht te verwerven :
  - ‘Estland-incidenten’
  - Hactivisme
  - Cyberterrorisme
  - Cyberspionage
  - Cybersabotage

- ‘Karakterisering’ : niet elke ‘(geweld)daad’ is een ‘oorlogs’daad

- Conclusie voor referentiekader 1 *:*
  - *‘Cyber-X : “When we start throwing out these things, like we’re in the midst of a cyber war, or that cyber war is around the corner, … we really have to define what it is that we’re talking about” (Schmidt)*
  - *« There has never been, nor will there ever be a cyberwar » (*Prof. Thomas Rid, Kings College London)

Referentiekader 2 : UNO-handvest en het LoAC (a)

- Art. 2 (4) UNO-handvest : Verbod van geweld «*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. 41 / 46 UNO-handvest : 'armed' force (security council)

- Geweld = gewapend geweld - maar ook dreigen is ook geweld (cfr. politieke aspect)

- Art. 51 UNO-handvest : Recht op zelfverdediging : «*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* »

Referentiekader 2 : UNO-handvest en het LoAC (b) - vragen

Aanval	Tegenaanval
■Is een cyberinstrument een ‘wapen’ ? ■Is een cyberaanval ‘geweld’ ? Intensiteit van de aanval	■ Quid met toewijzing (‘attributie’) van de aanval ■ Quid snelheid van actie/reactie ■ Quid met Nationale Kritische Infrastructuur

(1) Aanval : ‘wapen’ & ‘geweld’ (a)

- UNO-handvest : WO II = conventioneel geweld.
  - ICJ (1996) : niet beperkt tot in 1945 gekende wapens
  - Bovendien : ook ‘dreigen’ met geweld kan geweld zijn
  - Definitie : *“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*” (Rid / McBurney)

- Geweld-’grens’
  - 7 “Schmitt-criteria” die kans vergroten om over ‘use of force te spreken’ : severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, (state) responsibility = “*factors that can be expected to influence States when making use of force appraisal*s”

- ‘Effects based analysis’
  - Meeste auteurs : “Effects-based analysis of a particular cyber incident to determine whether or not it equates to an (traditional) ‘armed attack’ as understood by Article 51” (Schmitt / Ziolkowski / Dunlap e.a.)
  - Lt Gen Deptula (2001): “*… Indeed, the ultimate application of parallel war would involve few destructive weapons at all—effects are its objective, not destruction”.*
  - Cyber war verwelkomt ‘propere’ oorlog

(1) Aanval : ‘wapen’ & ‘geweld’ (b)

- Niet elk geweld is intens genoeg om UNO art. 2 & 51 toe te passen : ‘death of a thousand cuts’ (maar dit is meestal spionage)

- Indien fysieke / menselijke vernietiging

- Indien geen fysieke vernietiging : meer dan een *louter ‘inconvenience’ :*
  - *“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” (AIV/CAVV)*

  - *“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”* (AIV/CAVV)

(2) Attributie (toewijzing / identificatie)

- *“One of the things that scares … military officials the most about cyberwar is that, if an attack comes, they may not know who the enemy is” (Hirsch)*

- *Wei Jinching (1996) : “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”.*

- Estland-incidenten : 178 landen van oorsprong

- Attributie van belang voor :
  - Doelwit voor de tegenaanval
  - Karakterisering
  - Toepasselijk rechtssysteem (ingeval het om een niet-militair gaat)
  - Respecteren van neutraliteit & vermijden collatoral damage

- Attributieprobleem geen absolute rem (zeker wanneer cyberaanval deel is van conventionele aanval)

(3) Tegenaanval (a)

- Doctrine : tegenaanval = noodzakelijk, proportioneel, onmiddellijk
- Tegenaanval met doel de aanval te stoppen / capaciteit aanvaller te verminderen; geen loutere retaliatie / wraakneming
- Problemen
  - Timing : "*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."* (Talbot Jensen)
  - *Attributie / neutraliteit : "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 " (*Condron)
  - *= betwistbare standpunten*

(3) (Anticipatorische) Tegenaanval (b)

Standpunten :

- Caroline-interpretatie (1837 !) : anticipatorische aanval, bij wijze van zelfverdediging, indien dit de enige mogelijkheid is om een geplande gewapende aanval op het eigen land te vermijden.

- De noodzaak van zelfverdediging moet zijn : "*instant, overwhelming, and leaving no choice of means, and no moment for deliberation*" (quid 'death of a thousand cuts')

- Quid 'demonstration' *: "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."* (James E. Cartwright, reported by defensenews.com, may 2012)

(3) Tegenaanval : Critical national infrastructure (c)

- Welke KNI is ‘kritisch’ ?
- Welke lijst (hangt o.a. af van de economische ontwikkeling)
- Een lijst van ‘NKI’ met oog op ‘automatische’ tegenaanval ?
  - Interessante piste / duidelijkheid
  - “*The new presumption must be that a cyber attack on critical infrastructure is a national security threat*” (Condron)
  - Schept (politieke) beperkingen

NAVO-verdrag, art. 5

- Art. 5 : bijstandsverplichting ingeval van gewapende aanval
- Niet ingeroepen in 2007 (Estland)
- Noord-Atlantische Raad (2009) : *"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 ?"*

Referentiekader 2 - conclusie

- Verwijzing naar LoAC legt ‘geweldgrens’ zeer hoog, en is niet anders te interpreteren dan bij een conventionele aanval

- ‘Tegenaanval’ is gebonden aan zeer veel voorwaarden
  - Voorwaarden van de cybertegenaanval anders interpreteren dan bij een conventionele aanval : gevaarlijk
  - Piste van de (automatische) lijst van NKI : ?

- Conclusie voor referentiekader 2 (ius ad bellum) :
  - de aan de ADIV gegeven bevoegdheid van cyber’tegen’aanval is moeilijk te gebruiken
  - ‘Echte’ cyberaanval zal logischerwijze gepaard gaan met een conventionele aanval ... problemen van karakterisering / attributie / proportionaliteit etc. zullen relatief ‘eenvoudig’ zijn.
  - *« There has never been, nor will there ever be a cyberwar ...*
    - *but if it comes, it will not come alone ...*
    - *and you will easily recognise it »*

Zijn we volledig weerloos ? Verband met art. 18/16 Wet I&V (a)

- *"…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"*

- *Artikel 18/16 Wet I&V : bevoegdheid om :*
  - *"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".*

Zijn we volledig weerloos ? Verband met art. 18/16 Wet I&V (b)

- Behoort tot het ‘normaal’ arsenaal van de ADIV
  - Loskoppelen van het LoAC !

- Specifieke procedures volgen

  - Quid snelheid van optreden (wet I&V)
  - Toezichtprocedures
  - Inlichtingenofficieren

Dank u

Einde van de presentatie

Referenties

- Voor een gedetailleerde uiteenzetting van de in deze presentatie opgenomen standpunten, zie Franceus, F., “Cyberaanvallen en het recht van de gewapende conflicten : bemerkingen bij een juridische primeur in België en de Verenigde Staten”, Cahier Inlichtingenstudies,2012/2, Maklu

- Videoclips (youtube.com) credits to : Loockheed-Martin, CBS News, NATO Channel