Sir Daniel Bethlehem QC

THE INTERNET IN BELLO: SEMINAR ON CYBER WAR LAW, ETHICS & POLICY

BerkeleyLaw, University of California
18 November 2011

Daniel Bethlehem

Outline of Remarks

The following is a draft outline of speaking points for purposes of wider discussion. They do not reflect the settled view of the speaker on any given issue.

I. Three Preliminary Points

First

1. Not all "hostile" cyber action (whether by way of "attack" or "defence") properly engages – or should properly engage – a *jus in bello* analysis
   [scale and effects; risks of escalation; is LOAC the appropriate legal framework; LOAC may either be too permissive or too limiting]
2. Not all cyber action that happens within, or touches upon, the geographic space of a "hot" battlefield, or wider space of military action, properly engages – or should properly engage – a *jus in bello* analysis
   [cyber operations against drug lords in Afghanistan; cyber operations Somali pirates; cyber operations undertaken with the consent of the sovereign authority]
3. There may be good reasons not to jump too quickly to a LOAC framework
4. A preliminary and important question is what type of cyber action should properly engage a *jus in bello* analysis
5. Possible elements for consideration as part of a *jus in bello* gateway enquiry (going beyond the simple engagement of a *jus ad bellum* threshold):
   a. action equivalent to, or having consequential, kinetic effects reaching a material threshold; or
   b. action resulting in direct or consequential non-kinetic injury reaching a material threshold; or
   c. action in support of conventional military operations; or
   d. action intended to degrade, or having the foreseeable effect of actually degrading, the target State's military capabilities; or
   e. action intended to cause, or having the foreseeable effect of actually causing, large-scale and materially significant economic or similar damage in the target State; and
   f. action undertaken by persons whose conduct is attributable to the acting State as a matter of law

   [no automaticity from:
   - *the fact of a "hot" conflict between parties;*
   - *the fact of a military infra-structure target;*
   - *a* jus ad bellum *threshold having been engaged;*
   - *the existence of a "hot" war in the same geographic space and/or in which one or more party is engaged]*

Daniel.Bethlehem@legalpolicyinternational.com www.legalpolicyinternational.com

Second

6. Even amongst allies, the world, and the applicable legal framework, looks different depending on where one sits
7. Contrasting national visions of cyber
8. The importance of a (broadly) common analytical framework – the challenges of unilateralism and multilateralism

Third

9. Sources of international law?
10. Who makes international law?
11. Just because it's legal, it doesn't make it wise!
12. The limits of international law?

II. Preparing the Battlefield

Issues (1) - systems and process

13. The challenge of classified systems
14. Taking a direct part in hostilities?
15. Interoperability and de-confliction
16. Cyber "weaponry" and risks of cascading or unintended effects?
17. Command and control – strategic v. operational?
18. Shared operations and the law on State responsibility
    [attribution; aiding and assisting]

Issues (2) - substance: agreed rules and questions of application

19. A changing *jus ad bellum* gateway – new appreciations of threat, imminence and attack?
20. Determining provenance and attribution
21. The presumptive adequacy and application of existing LOAC rules?
22. Is cyber action inherently more LOAC friendly / compliant?
    [Random issues: distinction, proportion, necessity, precautions, ruses, perfidy]
23. Thinking through targeting – who / what, where, when and how?
24. Cyber *in bello* self-defence – where, when, how, who?

Concluding observations

25. How far does / can international law reach into the shadows?
26. The importance of careful and informed State thinking on these matters

---