Background Briefing #2: Attribution & Repression

Charles H. Pence
Louisiana State University

May 21, 2014 / Cyberwarfare, Ethics, and IHL

Cyberoperations whose effects are publicly felt need to be consistent with the stories that states tell to their citizens and to each other. These stories reflect the narrator's self-chosen status as a victim, an accuser, a retaliator, or an aggressor.

(Libicki (2012), *Crisis and Escalation in Cyberspace,* RAND, 44–5)

Is the difficulty of attribution in the cyber arena a problem for IHL?

What international law applies in cases where attribution is difficult?

Attribution

"The United States Government, to ensure appropriate application of these principles, shall make all reasonable efforts, under circumstances prevailing at the time, to identify the adversary and the ownership and geographic location of the targets and related infrastructure where DCEO or OCEO [Offensive Cyber Effects Operations] will be conducted or cyber effects are expected to occur, and to identify the people and entities, including U.S. persons, that could be affected by proposed DCEO or OCEO."

(US Cyber Operations Policy, 7)

Attribution: A Problem

"More broadly these are *epistemic* problems that have been ignored by most theorists of the morality of war; namely, how much justification or evidence is necessary concerning the threshold conditions for morally going to war?"

(Dipert (2010), *J. Mil. Eth.* 9:393)

"Forensics alone may not carry the narrative. Although a few individuals will understand the forensics, the rest, even among the decisionmaking elite, will have to trust experts, which suggests a problem in letting the normally secretive intelligence community represent the nation's cyberwar expertise."

(Libicki (2012), *Crisis and Escalation in Cyberspace,* RAND, 30)

Attribution: Not A Problem

"Existing resources can address the attribution problems in the cyber domain. Detailed intelligence, coupled with the experience and judgment of the responsible commander, are just as applicable in the cyber domain as in other areas of military operations."

(Phillips (2013), *Joint Forces Quarterly* 70:74)

"Many longstanding strategies, tactics, means, and media of warfare have defied easy application of the JWT.… [W]e can't always identify the agents of violence or their intentions. The Unabomber demonstrated that regrettable fact, as did the corpse on whom the FBI finally pinned the 2001 anthrax attacks."

(Cook (2010), *J. Mil. Eth.* 9:412)

How does the attribution problem interface with the right to self-defense?

Can failure of attribution itself trigger a crisis?

Self-Defense

"The United States Government shall reserve the right to act in accordance with the United States' inherent right of self defense as recognized in international law, including through the conduct of DCEO [Defensive Cyber Effects Operations]."

(US Cyber Operations Policy, 6)

"Russia retains the right to use nuclear weapons first against the means of information warfare, and then against the aggressor state itself."

(Tsymbal (1995), quoted in Arquilla (1999), in Khalilzad *et al., Strategic Appraisal: The Changing Role of Information in Warfare*, RAND, 390)

Self-Defense

"In fact, the interpretation of such expressions in the cyber realm is resolvable under the law if – *and, really, only 'if'* – technology can provide adequate data regarding, for example, the actual harm caused by the supposed 'attack,' as well as sufficient information about who actually did it."

(Dunlap (2013), *Air & Space Power J* 27:24)

Narratives to Defuse Self-Defense

- "We did nothing" (e.g., China's official response to cyber allegations)
- "Patriotic hackers" / "Not on our orders" (e.g., Syrian Electronic Army, organized crime)
- "No hostile intent" (e.g., US International Strategy for Cyberspace)

(Libicki (2012), *Crisis and Escalation in Cyberspace,* RAND, 51–61)

Does the use of deception in cyberwar inherently violate IHL?

Deception

"Notably, [the LOAC] forbid perfidy, such as deception that would draw fire onto non-combatant targets, harming innocent people. […] But deception is the sine qua non of cyberwar. […] Cyberoffenders … elude these detection mechanisms by masquerading as legitimate traffic."

(Libicki (2012), *Crisis and Escalation in Cyberspace,* RAND, 30)

How does the problem of attribution change overall responsibility for cyber attacks?

Responsibility

"In certain circumstances, the conduct of non-State actors may be attributable to a State and give rise to the State's international legal responsibility. Article 8 of the Articles on State Responsibility, which restates customary international law, notes 'the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.'"

(Tallinn Manual, Rule 6, sec. 9)

Which of the core principles of IHL or JWT does failure of attribution challenge?

Just War Theory / IHL Principles

- Just Cause (*casus belli*)
- Proportionality
- Public Declaration by a Proper Authority
- Right Intention

Orend (2013), *The Morality of War,* Broadview, 177–8

FIN

Just War Theory and Attribution

"In summary, it appears that policy perspectives on the just initiation of an information war have left a good part of just war theory in tatters. […] [T]he manner in which the information revolution empowers small groups and individuals to wage information warfare suggests that the notion of duly constituted authority may also have lost meaning."

(Arquilla (1999), in Khalilzad *et al., Strategic Appraisal: The Changing Role of Information in Warfare*, RAND, 394)

Just War Theory: Public Declaration

"The United States Government shall obtain consent from countries in which cyber effects are expected to occur … unless:

[…]

The President … determines that an exception to obtaining consent is necessary, takes into account overall U.S. national interests and equities, and meets a high threshold of need and effective outcomes relative to the risks created by such an exception."

(US Cyber Operations Policy, 7)

Solving Attribution?

- A “red phone” for the cyber realm (Rowe)
- Digital signatures on legitimate cyberweapons (Lin, Allhoff, and Rowe)
- Protocol-level solutions (IPv6, reduction of use of NAT, Tor, botnets)
- International network monitoring arrangements