THE INTERNET IN BELLO: SEMINAR ON CYBER LAW, ETHICS & POLICY
FRIDAY, NOVEMBER 18, 2011
BERKELEY LAW

SELECTED BIBLIOGRAPHY

A. *Journal Articles, Papers & Book Chapters*

Wing Commander Duncan Blake & Lieutenant Colonel Joseph S. Imburgia, *Bloodless Weapons"? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them As "Weapons,* 66 A.F. L. REV. 157, 181–203 (2010).

Gary Brown, *Why Iran Didn't Admit Stuxnet was an Attack,* JOINT FORCES Q. (4TH QUARTER, 2011)

Gary Brown, *Cyberwarfar,* MIL.REV. (1999) (COAUTHOR)

Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate***,** J.NAT'L. SEC. L. & POLICY (forthcoming).

Dorothy E. Denning, *Barriers to Entry: Are They Lower for Cyber Warfare?,* IO Journal, Apr. 2009, *available at* http://faculty.nps.edu/dedennin/publications/Denning-BarriersToEntry.pdf.

Lucian E. Dervan, *Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown,* 3 (NO.1) GOETTINGEN J. INT'L L. 373 (2011).

Knut Dormann, *Computer Network Attack and International Humanitarian Law,* International Committee of the Red Cross, May 19, 2001, *available at* http://www.icrc.org/Web/Eng/siteeng0.nsf/html/5P2ALJ.

David E. Graham, *Cyber Threats and the Law of War,* 4 J. NAT'L SECURITY L. & POL'Y 87, 97-102 (2010).

Oona Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, *The Law of Cyber-Attack,* CALIFORNIA. L. R. (FORTHCOMING).

Michael H. Hoffman, *The Legal Status and Responsibilities of Private Internet Users Under the Law of Armed Conflict: A Primer for the Unwary on the Shape of Law to Come,* 2 WASH. U. GLOBAL STUD. L. REV. 415 (2003).

Duncan B. Hollis, *Why States Need an International Law for Information Operations,* 11 LEWIS & CLARK L. REV. 1023–61 (2007).

Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict,* FORDHAM INT'L L.J. (forthcoming).

Eric Talbot Jensen, *President Obama and the Changing Cyber Paradigm,* 37 WM. MITCHELL L. REV. 5049 (2011).

Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533 (2010).

Jeffrey T.G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, 106 MICH. L. REV. 1427–51 (2008).

Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Cyberspace*, PROCEEDINGS OF THE WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS, Oct. 14, 2010, at 327-42, *available at* http://ssrn.com/abstract=1691207.

Michael Nacht, *The Cyber Security Challenge*, POLICY NOTES, GOLDMAN SCHOOL OF PUBLIC POLICY (Spring 2011).

Afroditi Papanastasiou, *Application of International Law in Cyber Warfare Operations*, Social Science Research Network, Sept. 2010, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1673785.

John C. Richardson, Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield, JMR Portfolio Intelligence, July 22, 2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888.

Paul Rosenzweig, *The Evolution of Wiretapping*, ENGAGE: THE JOURNAL OF THE FEDERALIST SOCIETY, VOL. 12, NO. 2, Fall 2011, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1904495.

Michael N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 NAVAL WAR COLLEGE BLUE BOOK 89 (2011).

Scott J. Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 229–46 (2009).

Abraham Sofaer, David Clark & Whitfield Diffie, *Cyber Security and International Arrangements*, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY, NAT'L RESEARCH COUNCIL (2010).

Sharon R. Stevens, *Internet War Crimes Tribunals and Security in an Interconnected World*, 18 TRANSNAT'L L. & CONTEMP. PROBS. 657–712 (2009).

Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303–33 (2010).

Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense*, 87 NAVAL WAR COLLEGE BLUE BOOK 59 (2011).

Sean Watts, *Combatant Status and Computer Network Attack*, 50 VA. J. INT'L L. 391 (2010).

Matthew C. Waxman, *Cyber Attacks as "Force" under UN Charter Article 2(4)*, 87 NAVAL WAR COLLEGE BLUE BOOK 43 (2011).

Mark D. Young, *National Cyber Doctrine: The Missing Link in the Application of American Cyber Power*, 4 J. NAT'L SECURITY L. & POL'Y 173 (2010).

B. *Print and Electronic News*

Spencer Ackerman, *NATO's Newest Bombing Tool: Twitter*, WIRED, June 10, 2011, *available at* http://www.wired.com/dangerroom/2011/06/natos-newest-bombing-tool-twitter.

Ellen Nakashima, *NSA allies with Internet carriers to thwart cyber attacks against defense firms*, WASHINGTON POST, June 16, 2011, *available at* http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring traffic/2011/06/07/AG2dukXH_story.html.

Adam Rawnsley, *Pentagon Wants a Social Media Propaganda Machine*, WIRED, July 15, 2011, *available at* http://www.wired.com/dangerroom/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/.

Jim Wolf, *Update 2 – US Military Better Prepared for Cyberwar – General*, REUTERS, Nov. 16, 2011, *available at* http://www.reuters.com/article/2011/11/17/usa-cyber-military-idUSN1E7AF21C20111117.

No legal vacuum in cyberspace, ICRC, Aug. 8, 2011, *available at* http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm.

Obama hands military new cyber war guidelines, ASSOCIATED PRESS, June 22, 2011, *available at* http://www.cbsnews.com/stories/2011/06/22/scitech/main20073212.shtml.

Experts advised U.S. how to cyber attack Libya, ASSOCIATED PRESS, June 13, 2011, *available at* http://www.cbsnews.com/stories/2011/06/13/scitech/main20070794.shtml?tag=contentMain;contentBody

C. *Books*

JEFFREY CARR, INSIDE CYBER WARFARE (O'Reilly Media 2010).

CHRISTIAN CZOSSECK & KENNETH GEERS, THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE (IOS Press 2009).

ABRAHAM D. SOFAER & SEYMOUR E. GOODMAN, THE TRANSNATIONAL DIMENSION OF CYBER CRIME AND TERRORISM, Hoover National Security Forum Series, (1999).