International Convention for the Peaceful Use of Cyberspace

February 17, 2014

By Edward M. Roche and Michael J. Blaine

Edward M. Roche is an affiliate researcher in the Columbia Institute for Tele-Information, Columbia Business School. **Michael J. Blaine** holds a Ph.D. in international business and writes on a wide range of issues. We would like to thank Susan W. Brenner and Robert Jervis for their comments on an earlier draft of this article.

Abstract: Cyber weapons now are an extension of state power. In hopes of gaining a strategic advantage, many countries including the United States, Russia and China are developing offensive cyber capabilities to disrupt political, economic, and social institutions in competitor nations. These activities have led to a cyber arms race that is spiraling out of control. This imminent global threat challenges the international community to be proactive. The purpose of this article is to propose an international convention to throttle the development, proliferation and use of cyber weapons before they cause electronic Armageddon. We begin by examining three successful efforts in arms control and use the lessons learned to draft a convention that can serve as a starting point for formal multilateral negotiations.

Deployment of cyber weapons now is an extension of state power.[1] The United States has set up a cyber-command authority, bristling with both defensive and offensive capabilities.[2] Similar escalation is occurring in China and Russia, and in many other countries around the world. There is a cyber-arms race.

The United States is under attack. In the spring of 2013, the Mandiant Corporation placed on the Internet a demonstration showing how a hacker

[1] Henry Bakis, *Géopolitique de l'information* (Presses Universitaires de France, 1987), p. 71; Ron Schleifer, "Psyoping Hezbollah: The Israeli Psychological Warfare Campaign During the 2006 Lebanon War," *Terrorism and Political Violence*, 21(2), 2009, pp. 221-238; Nicolas Arpagian, "La cyberguerre," *Réalités Industrielles*, 4, 2010, pp. 23-27.
[2] For an historical discussion of U.S. capabilities, see Edward Hunt, "U.S. Government Computer Penetration Programs and the Implications for Cyberwar," *Annals of the History of Computing*, 34(4), 2012, pp. 4-21.

doi: 10.1016/j.orbis.2014.02.009

organization, controlled by the Chinese Peoples' Liberation Army (PLA), was engaged in cyber espionage against companies in the United States. Governments have hired unconventional computer hackers to learn the tradecraft of cyber warfare. In 2007, after a dispute regarding a statue commemorating Russian loss of life during World War II, Latvia suffered an extensive wave of cyber attacks that brought the government to its knees. A similar incident occurred two years later in the Republic of Georgia[3], and in 2013 South Korea was attacked with North Korean cyber weapons.

These attacks are directed primarily against civilian targets, but not exclusively. Iranian centrifuges enriching uranium were attacked by the Stuxnet virus, widely believed to be of U.S. and Israeli origin. Iran subsequently reacted to this provocation by cyber attacking oil facilities in Saudi Arabia. Regardless of the source of the attacks, these demonstrations of cyber power indicate that governments—and the people they represent—are threatened by cyber-weapons.[4]

The dangers are so great that cyber arms qualify as weapons of mass destruction.[5] What in the past might be accomplished through strategic bombing, now could be handled in a cleaner way with cyber weapons.[6] Loss of important information, disruption of critical infrastructure networks, disabling of weapons systems, a financial catastrophe caused by the crippling of equities, credit, payment and foreign exchange transaction systems—all of these threats are behind the scramble to build defensive capabilities, and offensive weapons to give back what one gets.

The cyber arms race is developing at break-neck speed, and it is completely out of control. The asymmetrical nature of cyber weapons encourages countries to search for first-strike and offensive advantages, leading to the possibility of preemptive spirals following the logic of Thomas Schelling's "reciprocal fear of

[3] Stephen W. Korns and Joshua E. Kasterberg,"Georgia's Cyber Left Hook," *Parameters*, Winter 2008/2009, pp. 60-76. For Kyrgyzstan, see Jose Nazario, "Politically Motivated Denial of Service Attacks," in Christian Czosseck and Kenneth Geers, eds., *The Virtual Battlefield: Perspectives on Cyber Warfare* (Amsterdam: IOS Press, 2009), pp. 163-181.

[4] For popular observers warning about cyber war, see, Richard A. Clarke and Robert K. Knake, *Cyber War: The next threat to national security and what to do about it* (New York: Ecco, 2012); Ronald Deibert and Rafal Rohozinski, "Liberation vs. control: the future of cyberspace," *Journal of Democracy*, 21(4), 2010, pp. 43-57; Brian B. Kelly, "Investing in a centralized cybersecurity infrastructure: why 'hacktivism,' can and should influence cybersecurity reform," *Boston University Law Review* 92(5), 2012, pp. 1663-1711; Nicolas Arpagian, "Les entreprises, complices et victimes de la «cyberguerre»?" *Revue internationale et stratégique* 3, 2012, pp. 65-72.

[5] James P. Farwell and Rafal Rohozinski, "Stuxnet and the future of cyber war," *Survival*, 53(1), 2011, pp. 23-40; Richard Clarke, "War from Cyberspace," *The National Interest*, 104, Nov./Dec. 2009, pp. 31-36; Richard Brust, "Cyber attacks: Computer Warfare Looms as Next Big Conflict in International Law," *ABA Journal*, 98(5), May 2012, p. 40; Samuel Greengard, "The New Face of War," *Communications of the ACM*, 53(12), 2010, pp. 20-22; Thomas Zeitzoff, "Using Social Media to Measure Conflict Dynamics: An Application to the 2008-2009 Gaza Conflict," *Journal of Conflict Resolution*, 55(6), 2011, p. 938.

[6] Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, 9(4), 2010, pp. 384-410.