Developed States' Vulnerability to Economic Disruption Online

May 15, 2016

By Christopher Whyte

Christopher Whyte is a Ph.D. candidate in the Schar School of Policy and Government at George Mason University, adjunct professor at American University's School of International Service, and a non-resident fellow with Pacific Forum CSIS. His research focuses on the intersection of technology, political behavior, and international security issues.

Abstract: *Much of the literature on cyberspace and national security has backed away from the idea that cyberwar presents an imminent threat in world politics. However, there remains great concern about the potential for broad-scoped economic disruption prosecuted through digital means. How vulnerable are developed states to cyber economic warfare? Could either a concentrated cyber economic warfare initiative or a scalable disruption effect prove crippling on a large scale? And, most importantly, what are the implications for state policy and international interactions? This article contends that large, advanced industrial states are only superficially more vulnerable to disruption than are other types of systems.*

Digital security is now one of the foremost issues in research on international security.[1] Cyberspace presents new threats that generate unprecedented challenges to political cooperation and technical coordination in states' efforts to secure and ensure national security. Today, top military planners, government officials and civilian researchers debate how digital interconnectedness makes governments, industry and society vulnerable.

For years now, experts have recognized the need to answer broad-scoped questions about the nature of digital dangers and the consequences of certain policies for international security. Recent efforts have tried to link the developmental dynamics of network technologies with policy analyses and academic discussions of

[1] For early work on cyberspace and national security, see Ronald J. Deibert, "Black Code: Censorship, Surveillance, and Militarization of Cyberspace," *Millennium Journal of International Studies*, Dec. 2003, pp. 501–530; Emily O. Goldman, "Introduction: Information Resources and Military Performance," *Journal of Strategic Studies* 27.2 (2004), pp. 195-219; and Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: The (IR)relevant Theory?" *International Political Science Review*, pp. 221–244.

doi: 10.1016/j.orbis.2016.05.008

international politics.[2] In one vein, research in the security studies field focuses on how cyber attacks can be used to prosecute interstate conflict.[3] Here, there is a growing consensus that the idea of large-scale cyberwar is both alarmist and not reflective of strategic realities in international affairs.[4] A limited ability to cause physical disruption relegates cyber assault to a secondary consideration, at least when discussed in the context of major international conflict.[5]

In another vein, some scholars are concerned about the space between political intrusion—meaning intentional sabotage, espionage, etc.—and asymmetric challenges with a digital component, including: criminal operations, non-state and state-sponsored subversive activities, and "hactivism."[6] This focus rightly reflects the reality that most cyber intrusions occur as widespread low-level efforts—i.e., not aimed at major military or national targets, like critical infrastructure—undertaken by a myriad of actors to target a diverse range of social, economic and political functions.

Though scholars have increasingly moved to consider the cyber phenomenon in the past several years, relatively few attempts have been made to apply theories from security studies—or more broadly from political science—to assess the strategic implications of "cyber economic warfare," in which digital dynamics are linked to the social and economic foundations of international political order.[7] This lack encourages rhetoric that is based on premature assumptions. For

[2] See among others, Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012; Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies*, Feb. 2013, pp. 120-124; Mary M. Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly*, June 2010, pp. 381–401; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,", *International Security*, Fall 2013, pp. 7-40; and Timothy Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies*, Vol. 36, No. 1 (2013) pp. 125–133.

[3] See, for instance, Matthew C Waxman, Cyber-Attacks and the Use of Force: Back to the Future, 2(4), 36 (2011); and Thomas G. Mahnken, "Cyber War and Cyber Warfare," in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, D.C.: Center for a New American Security, 2011).

[4] See Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Feb. 2012, pp. 5–32; and Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security,* Fall 2013, pp. 41-73.

[5] Gartzke, "The Myth of Cyberwar."

[6] See, for example, Paul Cornish, David Livingstone, Dave Clemente, and Claire York, "On Cyber Warfare," Chatham House, Nov. 2010; Chintan Vaishnav, and Nazli Choucri, and David D. Clark, Cyber International Relations as an Integrated System, June 14, 2012, MIT Political Science Department Research Paper No. 2012-16; Brandon Valeriano, and Ryan Maness, "A Theory of Cyber Espionage for the Intelligence Community," EMC Conference Paper; and James Lewis, James and Baker, Stewart, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, July 22, 2013).

[7] See Cornish et al. (2010); Lewis & Baker (2013); and Christopher, Whyte, "Power and Predation in Cyberspace," *Strategic Studies Quarterly*, Spring 2015, pp. 100-118.