Can States Calculate the Risks of Using Cyber Proxies?

May 7, 2016

By Erica D. Borghard and Shawn W. Lonergan

Erica D. Borghard is an Assistant Professor in the Department of Social Sciences and Executive Director of the Grand Strategy Program at the U.S. Military Academy at West Point. **Shawn W. Lonergan** is an Assistant Professor of International Relations in the Department of Social Science at USMA. He previously worked in cyber operations for the U.S. government. The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, Department of the Army, Department of Defense, or the U.S. government.

Abstract: *This article contends that states that employ cyber proxies are confronted with twin dilemmas. First, governments risk a Promethean dilemma when they equip cyber proxies with tools that could be turned against them. Second, governments risk a dilemma of inadvertent crisis escalation by empowering proxies with more expansive, or less restrained, political agendas that may exceed their mandates. The essay explores how states can manage the risks associated with these dilemmas and the conditions under which they are likely to backfire.*

The importance and the risks of the cyber domain for national security have long been recognized by academics and policymakers. A particularly complex and opaque aspect of this domain is the nature of the actors operating within it, and the relationships between them. While the first actors to exploit opportunities for gain (often illicitly) were private actors—criminal networks and the proverbial geeks in their mothers' basements—by the 1990s modern, economically developed states began to recognize the significance of—and develop capabilities to operate in—the cyber domain.[1] Examples abound of states operating in cyberspace to carry out attacks against adversaries or engage in economic warfare. Some of the most notable examples include the allegedly Russian-orchestrated distributed denial-of-service (DDoS) attacks against Estonian networks in 2007, Georgian networks in

[1] Andrew F. Krepinevich, "Cyber Warfare: A 'Nuclear Option?'" *Center for Strategic and Budgetary Assessments* (2012), pp. 18-22. According to recently declassified documents, the U.S. National Security Agency first began to target adversary's computers in 1997. See Jeffrey T. Richelson, "National Security Agency Tasked with Targeting Adversaries' Computers for Attack Since Early 1997, According to Declassified Document," *The National Security Archive* (blog) Sept. 28, 2015, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/.

doi: 10.1016/j.orbis.2016.05.009

2008 (in conjunction with conventional military operations in Georgian territory), and Kyrgyzstan in 2009; alleged Chinese cyber incursions against public and private networks for the purposes of espionage and intellectual property theft—such as Titan Rain in 2002, Aurora in 2009 and, most recently, the U.S. Office of Personnel Management data breach; and Iran's Izz ad-Din al-Qassam Cyber Fighters group's alleged attack in 2012 against U.S. banks and companies (Operation Ababil), in 2013 against Saudi Aramco, and in 2014 against the Sands Casino.[2] In this analysis, we focus on a grossly under-explored aspect of the cyber domain, one with dangerous consequences for the security and stability of the cyber realm: the relationship between state actors and what we term "cyber proxies"—those non-state actors with whom states work to carry out offensive operations against adversaries.

In this analysis, we claim that state actors, recognizing the potential rewards associated with operating in the cyber domain, while also appreciating the risks of utilizing this emerging instrument of power, often form relationships with cyber proxies when they lack an independent ability to conduct cyber operations and/or seek plausibly to deny involvement in a cyber operation.[3] While these dynamics have sparked a budding literature that explores some of the dynamics of these new types of relationships, scholars have yet to define fully their parameters, explore states' motivations for forming them, and assess the potential risks, limitations, and opportunities they pose.

To accomplish this analysis, we first address the definitional problems associated with understanding the various actors in cyberspace. We then turn to existing literature in the field of international relations to derive the concept of a "cyber proxy." Finally, we create a typology of cyber proxies and their state patrons that makes predictions about the nature of the relationships that will form between them and the risks and dilemmas that follow.

Defining the Actors

Governments have worked with a variety of non-state actors in the cyber domain. However, it is difficult to define these actors because they do not operate consistently under state control. Indeed, many of these actors may be cyber criminals, hacktivists, patriotic hackers, online activists or cyber terrorists who only

[2] Krepinevich, "Cyber Warfare," pp. 22-38; Timothy L. Thomas, "Google Confronts China's 'Three Warfares,'" *Parameters,* Summer 2010; Siobhan Gorman, "Georgia States Computers Hit By Cyberattack," *The Wall Street Journal,* Aug. 12, 2008; Jeremy Kirk, "Georgia Cyberattacks Linked to Russian Organized Crime," *PC World*, Aug.16, 2009, http://www.pcworld.com/article/170289/article.html; David Goldman, "Major Banks Hit with Biggest Cyber Attacks in History," CNN Money, Sept. 28, 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/; Nicole Perlroth, "Cyberattack on Saudi Oil Firm Disquiets U.S.," *The New York Times*, Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0. Jose Pagliery, "Iran hacked an American casino, U.S. says," CNN Money, Feb. 27, 2015, http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/.

[3] Krepinevich, "Cyber Warfare," pp. 49-50.