Cyber-Terrorism in a Post-Stuxnet World

By Michael Kenney

Michael Kenney is Associate Professor of International Affairs, Graduate School of Public and International Affairs at the University of Pittsburgh. He wishes to thank Andrew Conte, Dorothy Denning, David Rapoport, and Wendy Wong for their remarks on an earlier version of this article, and Phil Williams for his support of the presentation that led to this article.

Abstract: Recent cyber-attacks such as Stuxnet and Anonymous' increasingly aggressive digital activism have rekindled fears that cyber-terrorism is an imminent threat. However, the concept remains poorly understood. Confusion over cyber-terrorism stems, in part, from recent attempts to stretch the concept to include hacktivism and terrorists' use of the Internet to facilitate conventional terrorism. Although the United States and other countries have experienced thousands of cyber-attacks in recent years, none have risen to the level of cyber-terrorism. This article seeks to dial down the rhetoric on cyber-terrorism by explaining how it differs from cyber-attacks, cyber-warfare, hacktivism, and terrorists' use of the Internet. The most immediate online threat from non-state terrorists lies in their ability to exploit the Internet to raise funds, research targets, and recruit supporters rather than engage in cyber-terrorism. Cyber-terrorism may well occur in the future, but for now online crime, hacktivism, and cyber-warfare are more pressing virtual dangers.

In a major speech on cyber-security in October 2012, then-Defense Secretary Leon Panetta warned that the United States faced a great danger from violent extremist groups that could use computer attacks to "derail passenger trains… contaminate the water supply in major cities, or shut down the power grid across large parts of the country." The combined effect of such an attack, the Secretary declared, would be nothing less than a "cyber Pearl Harbor" that "would paralyze and shock the nation and create a new, profound sense of vulnerability."[1] While Secretary Panetta was responding to a wave of cyber-attacks against U.S. financial institutions in the months leading up to his speech, similar warnings had been issued in the past. Since the widespread adoption of the Internet in the 1990s, government officials, journalists, and computer security experts frequently have described

[1] Leon E. Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," Oct. 11, 2012, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

doi: 10.1016/j.orbis.2014.11.009

frightening scenarios of "digital Pearl Harbors," in which computer hackers "plunge cities into blackness, open floodgates, poison water supplies, and cause airplanes to crash into each other."[2]

The perpetrators behind these conjectural attacks were often called "cyber-terrorists," a term whose provenance dates to the same period. In popular accounts, cyber-terrorists referred to computer hackers who might cause airplanes to fly into each other, bring down the nation's banking system, or use computers to kill. Either way, warned Tom Ridge, then-White House director of homeland security, the threat of cyber-terrorism was immediate and palpable: "Terrorists can sit at one computer connected to one network and can create worldwide havoc… [they] don't necessarily need a bomb or explosives to cripple a sector of the economy, or shut down a power grid."[3]

These dire warnings never materialized. Although the United States experienced hundreds of thousands of cyber-attacks in the ensuing years, none rose to the level of cyber-terrorism, defined here as politically motivated computer attacks against other computer systems that cause enough physical harm or violence to generate fear and intimidation beyond the immediate victims of the attacks. Instead, during any given year, a motley assortment of hackers and online criminals exploited computer networks to probe for weak spots, steal information, vandalize websites, disrupt online services, and, more recently, sabotage computers and the machines they run. Some attacks were carried out by ideologically motivated hackers engaged in contentious politics. However, these attacks involved website defacements, the virtual equivalent of graffiti, or denial of service attacks that temporarily disrupted websites. None of the thousands of computer attacks physically harmed anybody, provoked fear in larger audiences, or seriously damaged critical infrastructures—such as major transportation and communication systems.

This article seeks to dial down the rhetoric on cyber-terrorism by examining the concept, as well as similar phenomena with which it is often associated. Cyber-terrorism belongs to the same metaphorical class or "genus" of events as cyber-attacks, cyber-war, and "hacktivism." In spite of their similarities, there are essential differences between them, as there are between any species that share a common genus. Unfortunately, many observers have stretched cyber-terrorism's conceptual parameters, equating it with hacktivism, cyber-attacks and terrorists' use of the Internet. In the wake of recent intrusions against American banks and other cyber-attacks, including Stuxnet and Anonymous' pugnacious digital activism, a taxonomic

[2] James A. Lewis, "Cybersecurity and Critical Infrastructure Protection," CSIS working paper, Jan. 2006, Washington, D.C.: Center for Strategic and International Studies, http://csis.org/files/media/csis/pubs/0601_cscip_preliminary.pdf.
[3] Joshua Green, "The Myth of Cyberterrorism," *Washington Monthly* , Nov. 2002), http://www.washingtonmonthly.com/features/2001/0211.green.html; Gabriel Weimann, "Cyberterrorism: The Sum of All Fears?" *Studies in Conflict and Terrorism* 28, no. 2, 2005, p. 131.