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.

review is in order. Precision is essential to this task: to understand what cyber-terrorism is we must be able to distinguish it from what it is not.[4]

Cyber-Attack

Beginning with the most general concept, a cyber-attack is a deliberate computer-to-computer attack that disrupts, disables, destroys, or takes over a computer system, or damages or steals the information it contains.[5] There are many methods for conducting cyber-attacks, including infecting computers and networks with viruses and worms that control, slow down or damage computers, exploiting spyware to probe for vulnerabilities or steal data, and conducting denial of service attacks, with or without the assistance of botnets, to overwhelm websites and networks by flooding them with junk communications. Cyber-attacks do not include physical assaults on computers using other weapons, such as destroying computers with hammers or explosives. By definition, cyber-attacks are computer attacks on other computers carried out in cyberspace, including the Internet, telecommunications infrastructures, and computer systems.[6]

The immediate objective of a cyber-attack may be to harm the computer targeted, steal information from it, or simply observe the system to exploit vulnerabilities for a subsequent attack. The key is that the attacker conducts the intrusion with hostile, if not necessarily destructive, intent—without the knowledge or consent of the victim. Beyond these broad parameters, cyber-attacks do not contain many discriminating properties, as one would expect in a broad, genus-level concept. The perpetrators of cyber-attacks can be states or non-state actors, the damage caused by the attack can be extensive or minuscule, and the attack's purpose may be to achieve almost any economic, political, social, or psychological objective.

[4] This article does not analyze cyber-crime, which is typically cast in such broad terms as to include any crime in which a computer is a "facilitator" for acts that are largely carried out offline. For example, see Sarah Gordon and Richard Ford, "On the Definition and Classification of Cybercrime," *Journal in Computer Virology* 2, no. 1, Aug. 2006, p. 14. By including acts that occur outside cyberspace, such definitions place cyber-crime beyond the genus of cyber-attacks, the root concept from which my own analysis proceeds. In excluding cyber-crime from my analysis, I do not mean to suggest that cyber-crime is not a threat to online security. Cyber-crime has reportedly skyrocketed in recent years, with identity theft, online frauds, and other illegal computer intrusions becoming a regular feature of everyday life.

[5] National Research Council, Committee on Offensive Information Warfare, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009), pp. 1 & 10; Richard Kissel, ed., *Glossary of Key Information Security Terms*, NISTIR 7298, Revision 2 (National Institute of Standards and Technology, Gaithersburg, MD, May 2013).

[6] National Research Council, *Committee on Offensive Information Warfare, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 11; Kissel, ed., *Glossary of Key Information Security Terms*, p. 58.

Accurate and reliable counts of cyber-attacks are difficult to estimate given the high number and sheer diversity of computer intrusions, the broad range of public and private systems targeted, and the fact that many cyber-attacks go unreported. What is known is that there have been hundreds of thousands of cyber-attacks in recent years, some of which have caused considerable damage to computer systems and the data they contain. Among the most prominent attacks, the "I Love You" worm reportedly harmed millions of personal computers in 2000, the "Slammer" denial of service worm infected dozens of computer servers in 2003, including a 911 emergency response system in Washington State and the Davis-Besse nuclear power plant in Ohio, and in 2009 the "Conficker" super worm created a massive botnet of millions of Windows-based personal computers that could remotely steal information from other computers.[7]

Cyber-Warfare and Stuxnet

Unlike cyber-attacks, there have been relatively few examples of cyber-war, in which states carry out repeated computer attacks against their adversaries to deny them the ability to use cyberspace effectively, while safeguarding their own ability to do the same.[8] Cyber-warfare refers to offensive computer assaults that seek to damage or destroy adversaries' networks and infrastructures or deter them from waging cyber-attacks of their own. Like conventional warfare, cyber-warfare is instrumental: belligerents seek to impose their will on their enemies by attacking them in pursuit of some political goal or objective.[9] However, in contrast to traditional warfare, cyber-warfare occurs exclusively in cyberspace. "Kinetic" actions that physically destroy virtual networks by bombing computer servers or telecommunications cables are a form of conventional warfare, not cyber-warfare.

Cyber-warfare is largely, but not exclusively, the domain of states. States, and private hackers that act on their behalf, view cyber-warfare as a tool through which they can advance their national interests. This virtual continuation of policy by other means is decidedly less violent than traditional warfare, leading some observers to declare that cyber-warfare is not "real." In one version of this argument, cyber-war is not real war because cyber-weapons lack their "own force or

[7] Sharon Weinberger, "Top Ten Most-Destructive Computer Viruses," *Smithsonian Magazine,* March 20, 2012, http://www.smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html; Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel and Helge Janicke, "SCADA Security in Cyber-Warfare," *Computers and Security,* June 2012, pp. 418-436.

[8] Steven A. Hildreth, "Cyberwarfare," *Congressional Research Service Report for Congress,* June 19, 2001, http://www.fas.org/irp/crs/RL30735.pdf;
Oona A Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel, "The Law of Cyber-Attack," *California Law Review* 100, no. 4, Aug. 2012, pp. 817-885.

[9] Carl von Clausewitz, *On War,* Edited and Translated by Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976); Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs*, Nov./Dec. 2013, pp. 77-87.

energy."[10] Cyber-weapons do not attack directly but indirectly, by exploiting the force or energy in the machinery they target, such as manipulating industrial controllers to make a power generator self-destruct or derail a passenger train.[11] Yet such attacks are still capable of producing real damage and violence, even when the effect is produced indirectly through computer code. Cyber-warfare is not necessarily physically violent or destructive, like conventional warfare, but it can be, as the case of Stuxnet, discussed below, illustrates.

If not necessarily violent, cyber-warfare does involve a campaign of action rather than isolated attacks, and it typically unfolds in the context of larger disputes, including low-intensity conflict and operations other than war. Cyber-attacks that lack these properties, particularly individual assaults on computer systems that occur outside larger conflicts, are usually associated with the broader genus, not the species-level concept.

Although cyber-warfare is less common than cyber-attacks, there have been examples of the former. One such example is the campaign of cyber-attacks against the Georgian government in the run up to the Russian-Georgian war in 2008. Weeks before the fighting broke out, when both countries were still formally at peace with one another, hackers believed to be acting in support of the Kremlin carried out a series of distributed denial of service attacks and website defacements against websites run by the Georgian government. Later, when Russian forces began bombing the country, the computer attacks expanded to other targets, including media and transportation company websites in Georgia. While the online assaults succeeded in temporarily shutting down many websites, the significance of the attacks lay not in the damage they caused, but in their novelty. It was the first time a series of computer attacks acted as a force multiplier for one of the belligerents in active combat, effectively opening another theater of operations in contemporary warfare.[12]

Computer forensic experts uncovered evidence of Russian involvement in the attacks, but the Medvedev Administration denied responsibility, underscoring the clandestine nature of cyber-warfare and the difficulty in determining the perpetrators behind specific attacks. The subterfuge typically involved in cyber-warfare is further illustrated in the recent salvo of computer attacks between Iran and the United States and Israel. In August and September 2012, several major American financial institutions were targeted in a series of cyber-attacks by a group of hackers that called themselves the Izz ad-Din al-Qassam Cyber Fighters. In press

[10] Rid, "Cyberwar and Peace."

[11] Industrial controllers are small computer systems that run mechanical devices such as pumps, valves, motors and thermometers by sending and receiving electrical signals. Rid, "Cyberwar and Peace"; Ralph Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security and Privacy*, May/June 2011, p. 49.

[12] National Research Council, *Committee on Offensive Information Warfare, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 174; John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times*,, Aug. 13, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

releases posted on the Internet, the Cyber Fighters claimed they attacked the banks in retaliation for an offensive video mocking the Prophet Mohammed. However, U.S. officials claim the group is a cover for the Iranian government, which they believe launched the attacks in retaliation for Stuxnet and other computer viruses unleashed by the United States and Israel against Iran's nuclear program. The governments of all three countries—Iran, Israel, and the United States—deny their involvement in these attacks.[13] But if press reports are accurate, the attacks and counter-attacks may be considered cyber-warfare, particularly when seen in the context of the low intensity conflict between the United States and Iran dating back to the Iranian Revolution and the U.S. hostage crisis in the late 1970s.

When states engage in cyber-warfare, whether they acknowledge their involvement or not, their attacks tend to be more complex than cyber-attacks carried out by non-state hackers. The Stuxnet worm, while not as "cutting-edge" as many media reports suggested, set a new standard in weaponized malware. Part of a larger U.S. cyber-warfare program dating back to 2006 called Olympic Games, Stuxnet consisted of a series of computer attacks targeting industrial controllers used at Iran's uranium enrichment facility in Natanz. With Stuxnet, computer programmers created an intricate code capable not only of manipulating the industrial controllers that spun the centrifuges at the enrichment facility, but secretly recording plant operations when the centrifuges were working properly, and replaying these signals back to plant engineers during the attacks, so that they thought the centrifuges were operating normally when they were really spinning out of control.[14]

After programmers developed and tested the Stuxnet worm against a replica of the Iranian facility, individuals with access to the plant deployed the virus through infected jump drives. This allowed the attackers to jump the "air-gap" surrounding the facility, which was not connected to the Internet, presumably for security reasons. Once Stuxnet had infected Natanz's computer systems, programmers periodically activated their cyber-attacks over the course of many weeks in 2009 and 2010, deliberately altering the velocity at which the delicate gas centrifuges spun, ruining many of them in the process.

[13] Nicole Perlroth and David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times*, March 28, 2013, http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html; Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians, Officials Say," *The New York Times*, Jan. 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html; Nicole Perlroth, "JPMorgan and Other Banks Struck by Hackers," *The New York Times,* Aug. 27, 2014, http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html.

[14] Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon"; David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; James P. Farwell and Rafal Rohozinski. "Stuxnet and the Future of Cyber War," *Survival*, Feb.-March 2011, p. 25.

The intermittent nature of the attacks, in which the industrial controllers returned to normal following each round of attacks, confused the plant's engineers, allowing the operation to continue over an extended period of time before Iranian authorities temporarily closed the facility. This delayed their enrichment program by months or even years. Stuxnet marked a watershed in cyber-warfare, not only demonstrating the United States' willingness to engage in offensive cyber-attacks against its most intransigent adversaries, but revealing a level of physical destruction with computer code previously reserved for kinetic bombings and physical sabotage.[15]

Like other acts of cyber-warfare, the United States and Israel deployed Stuxnet to impose their will on their enemy and to advance their respective interests. While private, "patriotic" hackers may actively support one belligerent over another, most cyber-warfare involves state adversaries, either the governments directly involved, or state-sponsored hackers acting on their behalf. Yet, given the secretive nature of such operations, and the challenges facing computer forensics investigators in determining responsibility for specific attacks, cyber-warfare is typically a covert form of statecraft. Herein lies much of cyber-warfare's utility as a weapon: states can attack their adversaries without declaring war against them. With such advantages, it is not surprising that more and more states are interested in these weapons. In addition to the United States, Israel and Iran, numerous other countries have developed offensive cyber-capabilities in recent years—including China, Cuba, France, Germany, India, Japan, Russia, and the United Kingdom. This list likely will continue to grow in the aftermath of Stuxnet, which so dramatically illustrated the virtual firepower of today's most advanced cyber-weapons.

Hacktivism and Anonymous

Hacktivism consists of hostile computer attacks against other computers in cyberspace. While the immediate objective of these attacks may be to disrupt, disable, or control computer systems, or steal the data they contain, hacktivism has additional attributes that distinguish it from cyber-attacks, cyber-warfare, and cyber-terrorism. In particular, hacktivism is a form of "contentious politics" carried out by non-state actors in support of a variety of political, social or religious causes, frequently in opposition to government policy.[16] As Dorothy Denning puts it, hacktivism is "the marriage of hacking and activism."[17] Hacktivists use their knowledge and software tools to gain unauthorized access to computer systems they seek to manipulate or damage not for material gain or to cause widespread

[15] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran"; Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."

[16] Doug McAdam, Sidney Tarrow, and Charles Tilly, *Dynamics of Contention* (New York: Cambridge University Press, 2001).

[17] Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in John Arquilla and David Ronfeldt, eds., *Networks and Netwars* (Santa Monica, CA: RAND, 2001), p. 241.

destruction, but to draw attention to their cause through well-publicized disruptions of select targets.

Of the concepts discussed so far, none are as commonly associated with cyber-terrorism as hacktivism. Anonymous and other hacktivist groups are often portrayed in the media as cyber-terrorists, wreaking havoc by hacking websites, posting sensitive information about their victims, and threatening further attacks if their demands are not met. Yet, hacktivism extends well beyond such "life ruin" pranks to encompass a variety of politically and socially motivated website defacements, distributed denial of service attacks, and data thefts against government agencies, business corporations, and private individuals.

In 1999, after NATO accidentally bombed the Chinese embassy in Belgrade during the Kosovo war, hacktivists from China attacked U.S. government computer networks with denial of service email attacks and website defacements. In 2006, hackers launched denial of service attacks and website defacements against numerous websites in Denmark after the Danish newspaper *Jyllands-Posten* published cartoons lampooning the Prophet Mohammed. Over the years, Anonymous and other pro-Palestinian hackers have repeatedly attacked government and private websites in Israel, most recently after the resumption of violent hostilities between Israel and the Hamas-controlled Gaza Strip in 2012 and 2014.[18]

No collective has pushed the boundaries of this new form of digital activism more forcefully than Anonymous. Along with its numerous spin-off groups, including LulzSec and AntiSec, Anonymous has taken hacktivism to a new level. It has carried out dozens of highly-publicized attacks against an assortment of government agencies, private corporations and individuals. Variously described as a group, gathering, collective, movement, subculture, idea, banner, brand, hive mind, and performance spectacle, Anonymous can also be characterized as a fluid network of loosely affiliated activists, pranksters and hackers from over 20 countries that coordinate their activities on an *ad hoc* basis.[19]

[18] National Research Council, *Committee on Offensive Information Warfare, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 278; Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs*, Sept./Oct 2006, pp. 115-124; Dorothy E. Denning, "Whither Cyber Terror?," *10 Years after September 11: A Social Science Research Council Essay Forum*, 2011, http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/; Isabel Kershner, "2 Israeli Web Sites Crippled as Cyberwar Escalates," *The New York Times*, Jan. 16, 2012, http://www.nytimes.com/2012/01/17/world/middleeast/cyber-attacks-temporarily-cripple-2-israeli-web-sites.html; Dana Liebelson, "Inside Anonymous' Cyberwar Against the Israeli Government," *Mother Jones*, July 22, 2014, http://www.motherjones.com/politics/2014/07/anonymous-cyberattack-israel-gaza.

[19] Carole Cadwalladr, "Anonymous: Behind the Masks of the Cyber Insurgents," *The Observer,* Sept. 8, 2012, http://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents; Gabriella Coleman, "What It's Like to Participate in Anonymous' Actions," *The Atlantic Monthly,* Dec. 10, 2010, http://www.theatlantic.com/technology/archive/2010/12/what-its-like-to-participate-in-anonymous-actions/67860/; Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Little, Brown and Company,

Since its emergence from the online message board 4chan in 2004, Anonymous has evolved from a collection of digital pranksters primarily interested in "trolling," harassing individuals they despise through bullying emails, threatening phone calls, and website hacks, to a transnational network of activists and hackers engaged in serious social and political activism, while remaining true to its mischief-making origins. Anonymous made the jump from trolling to activism in 2008 with "Project Chanology," a coordinated campaign of pranks, denial of service attacks, and real world street protests directed at the Church of Scientology for its perceived malfeasance and censorship.[20] In the years since, "Anons," as members of the hacktivist collective like to call themselves, have attacked a wide range of targets, including the American Israel Public Affairs Committee, the Central Intelligence Agency, the Federal Bureau of Investigation, the Federal Trade Commission, MasterCard, the Motion Picture Association of America, PayPal, the Public Broadcasting Service, the Recording Industry Association of America, Sony, Stratfor, *The Sun* newspaper, the United States Copyright Office, Universal Music, the Vatican, Warner Brothers Music, the White House, and the Westboro Baptist Church.

Anons have also provided technical support to activists from the Arab Spring and Occupy Wall Street movements, and, more recently, protestors from Ferguson, Missouri upset over the killing of Michael Brown. The ideological glue that binds these activities is an eclectic vision that embraces the free flow of information, the protection of human rights, and the "power of the individual" not only to participate in virtual civil disobedience, but to agitate and amuse "just for the lulz," satisfying participants' ironic, self-righteous sense of humor, often at the expense of others.[21] While Anonymous is often characterized as a collection of expert hackers and computer programmers, most of its members have limited technical skills. Significantly, this has not prevented the collective from continuing

2012); David Kushner, "The Masked Avengers: How Anonymous Incited Online Vigilantism from Tunisia to Ferguson," *The New Yorker,* Sept. 8, 2014, pp. 48-59.

[20] Cadwalladr, "Anonymous: Behind the Masks of the Cyber Insurgents"; Gabriella Coleman, "Our Weirdness Is Free, The Logic of Anonymous—Online Army, Agent of Chaos, and Seeker of Justice," *Triple Canopy,* Jan. 13, 2012, http://canopycanopycanopy.com/15/our_weirdness_is_free;
Olson, *We Are Anonymous*; Kushner, "The Masked Avengers," p. 51.

[21] "Lulz" is a mean-spirited derivative of the digital portmanteau LOL ("laugh out loud"). With lulz, the laughter is at the expense, and often deep personal embarrassment, of another. Coleman, "Our Weirdness Is Free, The Logic of Anonymous—Online Army, Agent of Chaos, and Seeker of Justice"; Gabriella Coleman, "Hacker Politics and Publics," *Public Culture* 23, no. 3 (2011), p. 513; Cadwalladr, "Anonymous: Behind the Masks of the Cyber Insurgents"; Olson, *We Are Anonymous*, pp. 32-33; Kushner, "The Masked Avengers," pp. 52, 58-59; and Nicole Perlroth, "Anonymous Hackers' Efforts to Identify Ferguson Police Officer Create Turmoil," *The New York Times,* Aug. 14, 2014, http://www.nytimes.com/2014/08/15/us/ferguson-case-roils-collective-called-anonymous.html.

its contentious politics following the arrest and prosecution of several of its most talented hacktivists.[22]

Attacks carried out by Anonymous and other hacktivists have been disruptive, causing inconvenience, financial damage, and, in some cases, emotional distress to their victims. In one early example, over a two-week period in 1998, a group of hacktivists calling themselves the "Internet Black Tigers" flooded Sri Lankan embassies around the world with eight hundred e-mails a day in support of ethnic Tamil insurgents. While the e-mail "bombings" had little, if any, impact on the war then raging between Tamil rebels and the Sri Lankan army, Dorothy Denning notes the attack "had the desired effect of generating fear in the embassies."[23]

Nine years later, following the removal of a Red Army war monument from the center of Tallinn, the capital of Estonia, hackers used botnets to carry out distributed denial of service attacks against the former Soviet republic. The attacks temporarily blocked Estonians' access to online banking services and government websites. They also prevented people outside Estonia from accessing websites hosted in the country. Speaking at the Center for Strategic and International Studies in Washington, D.C. shortly afterwards, the Estonian Minister of Defense emphasized the "psychological nature" of the attacks, claiming they "caused intimidation… [and] created widespread confusion and miscommunication in the general public."[24] Similarly, after being victimized by distributed denial of service attacks, website defacements, and other pranks carried out by Anonymous in "Project Chanology," the Church of Scientology issued a statement describing the collective as "a group of cyber-terrorists" who are carrying out "illegal assaults on Church web-sites."[25]

While the immediate victims of such attacks are often quick to label them cyber-terrorism, whether such incidents caused the physical damage and widespread fear necessary for cyber-terrorism is questionable. Referring to the Internet Black Tigers attack and other examples she discusses, Denning concludes that none rose to the level of cyber-terrorism because they did not result in "violence or injury to persons, although some may have intimidated their victims."[26] While some Estonians may have been alarmed by the 2007 cyber-attacks, there is no evidence they feared immediate physical harm or that the "intimidation" referred to by the

[22]Olson, *We Are Anonymous*; Kushner, "The Masked Avengers."

[23]Denning, "Activism, Hacktivism, and Cyberterrorism," p. 269.

[24] Jaak Aaviksoo, "Cyberspace: A New Security Dimension at Our Fingertips," public presentation at the Center for Strategic and International Studies, Washington, D.C., Nov. 28, 2007; National Research Council, *Committee on Offensive Information Warfare, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 172.

[25]Olson, *We Are Anonymous*, p. 80; Church of Scientology, "Statement about "Anonymous," Feb. 8, 2008, http://www.newhavenindependent.org/index.php/archives/entry/masked_protesters_picket_scientologists/

[26] Dorothy E. Denning, "Cyberterrorism," Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Defense Minister was widespread. The website disruptions, believed to be carried out by Russian hackers, were short-lived. Online services were quickly restored, and no critical infrastructures in Estonia were targeted. The principal result of the cyber-attacks, concludes the National Research Council in its assessment of the Estonian incident, "was inconvenience."[27] In contrast, violent street protests by Russian Estonians incensed at the war monument's removal left one person dead and dozens more injured.[28]

Similar to the cyber-attacks in Estonia, none of Anonymous' distributed denial of service attacks and website defacements have harmed critical infrastructures or caused widespread physical damage. While individual victims of Anonymous' life ruin attacks may have felt intimidated, no reports suggest that they feared imminent bodily harm from the Anons attacking them or that any intimidation from the attacks spread beyond the immediate victims.

In sum, the cyber-attacks described above are an aggressive form of contentious politics and civil disobedience rather than terrorism. Hacktivists seek to publicize their respective causes by upsetting and embarrassing their victims, rather than terrorizing wider audiences through serious physical damage to property or violence to people. Characterizing hacktivism as cyber-terrorism disregards this essential property, stretching the former so that it includes the latter. There is a real and compelling difference between non-violent denial of service attacks as a form of digital protest politics and computer attacks intended to terrorize large audiences by causing substantial damage to critical infrastructures or financial systems. Both acts are politically motivated, computer-generated attacks on computer systems, but their similarities end there. The first act seeks to communicate through disruption, the second through terror.

Cyber-Terrorism

In common with other species in the cyber-attack genus, cyber-terrorism refers to computer-generated attacks that target other computers in cyberspace or the information they contain. Like cyber-warfare and hacktivism, cyber-terrorism occurs exclusively in cyberspace. It is, in this sense, the "convergence of terrorism and cyberspace," with computer technology serving as both weapon and target.[29] This distinguishes cyber-terrorism from conventional terrorism, including the use of cyberspace by terrorists to prepare for brick-and-mortar attacks. When terrorists use the Internet to research targets for bombings or kidnappings they exploit computer technology as a weapon, not a target. In contrast, a computer-generated

[27] National Research Council, *Committee on Offensive Information Warfare, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, p. 172.

[28] Steven Lee Myers, "After Violent Night, Estonia Removes a Soviet-Era Memorial," *The New York Times,* April 28, 2007, http://www.nytimes.com/2007/04/28/world/europe/28estonia.html.

[29]Denning, "Cyberterrorism"; Barry Collin, "The Future of Cyberterrorism," *Crime and Justice International,* March 1997, pp. 15-18, http://www.cjimagazine.com/archives/cji4c18.html.

attack on an industrial controller or Supervisory Control and Data Acquisition (SCADA) system that regulates critical infrastructure could qualify as cyber-terrorism, as long as the attack contains the other properties of cyber-terrorism.[30]

In contrast to cyber-attacks more generally, perpetrators' motivations are a distinguishing feature of cyber-terrorism. Like hacktivism, cyber-terrorism is a form of digital politics carried out by non-state actors pursuing an assortment of political, social or religious causes, as opposed to an economic one, which is typically associated with cyber-crime.

What distinguishes the contentious politics of cyber-terrorism from hacktivism is that the attack goes beyond inconveniencing its victims to result in physical violence against them or serious damage to property or critical infrastructure. Specific examples would include hacking attacks against SCADA systems and industrial controllers that allow perpetrators to breach a dam, thereby flooding a major urban area; computer attacks that derail passenger trains, causing them to crash; or attacks that wipe out the bank accounts, and life savings, of millions of customers. Critically, such violence and physical damage is not an end in itself but the means by which attackers seek to terrorize people beyond their immediate victims.

The psychological projection of fear and intimidation is the final attribute of cyber-terrorism, the vehicle through which cyber-terrorists publicize their cause to broader audiences, be they governments or societies at large. While cyber-warfare between state actors may also result in physical violence and widespread fear, such effects are incidental to the act, not indispensable, as they are in cyber-terrorism. The objective of cyber-terrorism is to terrorize. There can be no cyber-terrorism without terrorism—and no terrorism without terror.

These four elements—computer generation, political motivation, physical violence, and psychological coercion—are the essential attributes of cyber-terrorism. To qualify as cyber-terrorism, an act must contain all four properties, the combination of which distinguishes it from its broader genus and other cyber-attack species, such as hacktivism and cyber-warfare. Together, these attributes, outlined in Table 1, suggest that cyber-terrorism is defined by its intent *and* its effects, rather than one or the other. The intent of the computer-generated violence must be to achieve some political, social, or religious goal, and its effect must be sufficiently harmful or damaging to generate widespread fear in pursuit of that goal, comparable to conventional terrorism.

The Paucity of Cyber-Terrorism

What is perhaps most striking about cyber-terrorism, particularly given the amount of attention it has received from policymakers and the media, is that it has

[30] Similar to industrial controllers, SCADA systems are computers that run industrial machines. SCADA systems manage electricity grids, regulate temperatures in nuclear power plants, make sure trains run on time, and perform a host of other industrial routines. Nicholson *et al.*, "SCADA Security in Cyber-Warfare," pp. 418-419.

Table 1: Necessary Attributes of Different Cyber Phenomena

Attribute	Cyber-attack	Cyber-warfare	Hacktivism	Cyber-terrorism
Computer attack targeting other computers, computer systems, or the information they contain	✓	✓	✓	✓
Attack in pursuit of political, social, or religious aim		✓	✓	✓
Attack part of broader hostilities between belligerents, usually states or their proxies		✓		
Attack produces physical violence against persons, property or critical infrastructure				✓
Attack causes widespread fear or physical intimidation beyond immediate victims				✓
Examples	"I Love You" worm, "Slammer" denial of service attack, "Conficker" virus	Stuxnet, Russian cyber-attacks on Georgia	Anonymous attacks, "cyber jihad" against Danish newspapers	?

(Adapted from Hathaway *et al.* (2012), p. 833.)

never occurred.[31] Not a single cyber-attack carried out to date contains the four attributes of cyber-terrorism. This includes Anonymous' many operations, Stuxnet, and al Qaeda, which has never carried out a major cyber-attack, despite expressing a desire to do so.[32]

Most cyber-attacks have been *disruptive*, not *destructive*. However, a small number of attacks have resulted in physical damage, at least against property. The most prominent examples are Stuxnet and a separate attack against a water treatment facility in Queensland, Australia in 2000. The Queensland attack was carried out by Vitek Boden, a former employee of the software firm that installed the SCADA system and industrial controllers that regulated the plant's sewage system. After quitting the software firm and being turned down for a similar position on the local government council that ran the treatment plant, Boden used his knowledge of the SCADA system to remotely access and release 800,000 gallons of raw sewage into adjacent rivers, parks and the grounds of a nearby hotel, destroying marine life and creating a nauseating stench for local residents.[33]

Stuxnet and the Boden attacks caused physical damage, in the latter case against critical infrastructure. They also caused confusion among plant operators who struggled to understand what was happening to their facilities. Significantly, neither attack was accompanied by any public statements or admissions of responsibility from perpetrators threatening additional assaults. Such statements would have made the attacks more intimidating, had that been the attackers' intention. "Anons" sometimes threaten additional attacks against their victims but such threats involve promises to release embarrassing information, not engage in physical violence.

What distinguishes cyber-attacks like Stuxnet and Queensland from cyber-terrorism is that the violence of terrorism has an inherently dramatic purpose: to provoke fear, dread and terror in a wider audience, an audience extending beyond the immediate victims of the attack. Stuxnet was meant to disrupt and sabotage the Iranian government's nuclear program, and to signal the Iranian authorities that its efforts to enrich weapons-grade uranium would not be tolerated. Queensland was an act of personal vengeance by a disgruntled insider who wanted to get even with

[31] Maura Conway, "What Is Cyberterrorism?" *Current History* 101, Dec. 2002, pp. 436-442; Denning, "Activism, Hacktivism, and Cyberterrorism"; Dorothy E. Denning, "Stuxnet: What Has Changed?" *Future Internet* 4 (2012), pp. 672-687; Michael Stohl, "Cyber terrorism: a clear and present danger, the sum of all fears, breaking point, or patriot games?" *Crime, Law and Social Change* 46, no. 4 (2006), pp. 223-238; Weimann, "Cyberterrorism: The Sum of All Fears?"

[32] Denning, "Stuxnet: What Has Changed?"; Barton Gellman, "Cyber-Attacks by Al Qaeda Feared: Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *Washington Post* , June 27, 2002, http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html

[33] Marshall Abrams and Joe Weiss, "Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, Australia," *National Institute of Standards and Technology Report,* July 23, 2008, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf; Gellman, "Cyber-Attacks by Al Qaeda Feared."

his former employer and the local government that refused to hire him. Neither attack was intended to terrorize larger audiences.

Recent years have witnessed several complex cyber-attacks by states, many less sophisticated but disruptive attacks by non-state actors like Anonymous, and even more cyber-crimes by economically motivated criminals, but no cyber-terrorism. This does not mean that terrorists and their supporters, including those affiliated with al Qaeda, have not carried out cyber-attacks. In October 2001, a group of hackers announced the formation of the "al Qaeda Alliance" and defaced the Department of Defense website devoted to Operation Enduring Freedom. Several years later, other hackers perpetrated attacks against media websites in Europe under the banner of what is sometimes called "cyber-jihad."[34]

None of these attacks resulted in the violence and widespread fear that are necessary for cyber-terrorism. The distributed denial of service attacks caused, at best, temporary disruptions to public websites, often lasting only a few minutes. The website defacements, which typically posted anti-Western text and photos on the hacked sites, were the online counterpart of spray-painting a building. Users visiting these websites during the attacks may have experienced some frustration because the sites were temporarily unavailable or displayed offensive messages. Notwithstanding exaggerated claims of cyber-terrorism made by some computer security professionals, people trying to access the hacked websites likely did not feel the dread of violence and physical intimidation associated with terrorism.[35]

Some observers have responded to the lack of cyber-terrorism by arguing that the concept itself is flawed and needs to be expanded to include terrorists' use of the Internet. One prominent analyst suggests that "any application of terrorism on the Internet," including posting videos of attacks online and building websites to attract supporters, should be considered cyber-terrorism.[36] A pair of computer security researchers take a similar approach, suggesting that cyber-terrorism targeting computers is "pure" cyber-terrorism, while regular "cyber-terrorism" occurs whenever the terrorist leverages "the other factors and abilities of the virtual world […] to complete his mission," including using the Internet to raise funds and research targets.[37]

In removing the computer-as-target attribute of cyber-terrorism from their definitions, these authors equate terrorists' use of information technology with cyber-terrorism, stretching the concept beyond the species—and the broader genus, as well. As with hacktivism, cyber-warfare, and cyber-attacks more generally, cyber-terrorism occurs exclusively in cyberspace. It refers not only to the convergence of

[34] Kohlmann, "The Real Online Terrorist Threat"; Denning, "Whither Cyber Terror?"; Denning, "Stuxnet: What Has Changed?"; Green, "The Myth of Cyberterrorism."

[35] Denning, "Stuxnet: What Has Changed?," p. 678; Green, "The Myth of Cyberterrorism"; Weimann, "Cyberterrorism: The Sum of All Fears?"

[36] Quoted in Eben Kaplan, "Q&A: Terrorists and the Internet," *The New York Times*, March 6, 2006, http://www.nytimes.com/cfr/international/slot2_030606.html.

[37] Sarah Gordon and Richard Ford, "Cyberterrorism?" *Computers and Security* 21, no. 7 (2002), p. 637.

terrorism and cyberspace, but a convergence in which computer technology is both weapon *and* target. The latter is rare, the former is not.

Terrorists use computers as metaphorical weapons for all sorts of reasons. They exploit the Internet to raise funds, recruit supporters, spread propaganda, and facilitate conventional gun-and-bomb assaults. The overwhelming majority of terrorist activity on the Internet involves such use.[38] Moreover, terrorists exploit a wide variety of communications technologies to facilitate their attacks, not just the Internet. Terrorists routinely use cell phones to communicate with their colleagues, coordinate their activities, and detonate their improvised explosive devices. This is not typically referred to as "cell phone terrorism," nor are fatuous distinctions made between "regular" cell phone terrorism and "pure" cell phone terrorism. Instead, cell phones, along with other communications technologies like GPS devices, satellite phones, and personal digital assistants, are simply seen as "weapons" or tools terrorists use to carry out their activities. Analysts that fail make such distinctions not only stretch the concept to include the many ways terrorists use the Internet instrumentally to advance their interests, they suggest that cyber-terrorism is pervasive when it is anything but.

Moving Beyond Hyperbole

On any given day, the United States and other countries experience thousands of computer attacks on their public and private computer networks. The variety of attacks is enormous, ranging from simple probes to data theft and vandalism to more serious sabotage attacks meant to destroy machines and information. While many of these incidents possess the general properties of cyber-attacks, they do not have the specific, species-level attributes of cyber-terrorism. *In fact, cyber-terrorism has never occurred.* To date, no terrorist organization, including al Qaeda and the Islamic State in Iraq and Syria (ISIS), has carried out a major cyber-attack, nor, apart from Hollywood villains, have terrorists or anybody else engaged in cyber-terrorism. Recent years have seen significant increases in cyber-crime and hacktivism, along with a couple of examples of cyber-warfare, but no cyber-terrorism.

One regrettable, perhaps predictable response to the lack of cyber-terrorism has been to expand the concept so that it includes things that do happen, some of them quite frequently. Whether government officials, security professionals, and other observers exaggerate the threat of cyber-terrorism out of genuine concern for public safety or to advance more parochial interests, such conceptual stretching occurs at the expense of understanding the threat and developing sound policies to counter it. We might be able to say "more" about cyber-terrorism by conflating it with hacktivism, cyber-attacks, and terrorists' conventional use of the Internet, but much of what we say is imprecise, inconsistent, and confusing.[39] If cyber-terrorism

[38] Conway, "What Is Cyberterrorism?" p. 438; Weimann, "Cyberterrorism: The Sum of All Fears?" p. 133.

[39] Giovanni Sartori, "Concept Misformation in Comparative Politics," *American Political Science Review,* Dec. 1970, pp. 1,033-1,053.

is to have any meaning not only for scholars but for security officials and policymakers, we must be able to distinguish it from cyber-attacks, cyber-warfare, hacktivism, and terrorists' use of the Internet.[40] The most effective information security policies are those premised on a realistic awareness of the threat.

Some readers may object that this article sets the definitional bar too high, that the four-properties of cyber-terrorism represent cornerstones for an edifice that cannot be built. Recent developments suggest that such concerns may be misplaced. Cyber-terrorism may not have happened yet, but that does not mean it never will. Stuxnet and other recent cyber-attacks have brought us closer to cyber-terrorism than we were before. To be sure, the purpose of the Stuxnet worm was to sabotage Iran's uranium enrichment program, not spread terror. But the cyber-weapon's demonstration effect was enormous, showing the world how cyber-terrorism could potentially cause substantial physical damage to critical infrastructures by attacking the computer controllers and SCADA systems that regulate industrial machinery.

Perhaps even more troubling, the Stuxnet genie is out of the bottle: its code has spread to computer programmers and hackers around the world. While some observers fear this increases the probability that such cyber-weapons will be deployed, others note that the damage caused by the worm's spread has been minimal because it contained a built-in expiration date and was carefully calibrated to attack only the electrical motors and industrial controllers used at Natanz.[41] It remains largely unknown whether non-state hackers have the capacity and the willingness to modify and learn from the code in Stuxnet and other cyber-weapons developed by states to attack other SCADA systems in similar ways. Such uncertainty is unwise. Policymakers and computer security professionals should devote greater resources to understanding the potential for non-state actors to exploit cyber-weapons developed by states and how to stymie the spread of this malicious code.

To the extent that Stuxnet underscores cyber-terrorism's potential, 20 years of hyperbole surrounding "digital Pearl Harbors," "cyber-Armageddons," and other overwrought scenarios remind us that caution remains in order when assessing the threat today. After Vitek Boden polluted the area around a water treatment plant in Queensland with sewage water in 2000, security specialists sounded the alarm with chilling predictions that terrorists would soon exploit insiders to wage SCADA attacks on critical infrastructures in the United States. While numerous incidents since then have confirmed that poorly protected SCADA systems are vulnerable to cyber-attacks, none of these attacks produced destructive effects anywhere near the doomsday scenarios forecast by many. An important reason for this was that the same computer specialists sounding the alarm were also studying the Boden attack and other incidents to identify—and fix—the vulnerabilities hackers were exploiting.

[40] Mark M. Pollitt, "Cyberterrorism: Fact or Fancy?" *Proceedings of the 20th National Information Systems Security Conference,* Oct.1997, pp. 285-289.

[41] Farwell and Rohozinski, "Stuxnet and the Future of Cyber War."

It also became increasingly apparent that cyber-attacks causing physical damage to industrial machines required substantial expertise, much more than Anonymous and other hackers typically display in their denial-of-service attacks and website defacements. For all the anxieties that Stuxnet has rekindled, the attack has been studied widely by computer security specialists who have developed patches for many of the security flaws the worm exposed. Developing and deploying the Stuxnet worm involved a level of technical expertise that is beyond the capacity of most non-state terrorists today. State hackers and online criminals with the necessary skills and knowledge to exploit Stuxnet's code to malevolent effect are more likely to use such weapons to engage in cyber-espionage against their enemies or line their pockets through cyber-crime than carry out cyber-terrorism.

Conclusion

If the history of contemporary terrorism is any guide, non-state terrorists, including al Qaeda and ISIS, are more likely to carry out flesh-and-blood attacks using simpler, easier-to-acquire conventional weapons—guns, bombs and knives—than complex attacks against SCADA systems and industrial controllers, the fear-inducing capacity of which remains uncertain. While terrorists have increased their use of information technology and social media in recent years, they use these tools instrumentally, to facilitate their own real-world activities, rather than bring the Internet crashing down. The real cyber-threat from non-state terrorists lies in their ability to exploit the Internet to raise funds, research targets, and recruit and radicalize like-minded travelers rather than execute SCADA attacks. Cyber-terrorism may well be in our future, but for now at least, the virtual dangers we face stem more from cyber-crime, hacktivism, and cyber-warfare.