Whither Cyber Terror?

Dorothy E. Denning
Distinguished Professor of Defense Analysis, Naval Postgraduate School

August 19, 2011

Ten years have passed since G-Force Pakistan, a group of Pakistani hackers with a history of defacing websites, announced the formation of the Al-Qaeda Alliance on one of their hacked sites. Declaring that they stood by al-Qaeda, the defacement said they would be attacking major US and British websites and giving confidential data to al-Qaeda authorities. Any speculation that the group might conduct attacks of a terrorist nature, however, was quickly put to rest. Apparently worried about their image, G-Force wrote on a subsequent defaced site that they were "not a group of cyber terrorists," and that "All we ask for is PEACE for everyone." They asked the media to "not leave a bad image of us on readers."

Although G-Force never became a major threat, others emerged to take up the umbrella of what is sometimes called "electronic jihad" or "cyber jihad." Typically, these individuals and groups attack websites that they view as contrary to the values of Islam, either defacing the sites or using software tools such as Electronic Jihad to flood them with traffic in a denial-of-service (DoS) attack. Perhaps the largest attack of this nature came in response to the publication of cartoons satirizing the Prophet Mohammed in the Danish newspaper *Jyllands-Posen*. In early 2006, Islamic hackers defaced thousands of websites in Denmark and launched DoS attacks against *Jyllands-Posen* and sites that had republished the cartoons.

While disruptive, none of the attacks by cyber jihadists meets the threshold for terrorism. A few jihadists have proposed more damaging attacks, but their proposals have not translated to credible threats. One suggested disabling all the electronic networks in the world for a day in order to bring about the total collapse of the West, but demonstrated no knowledge of the enormity of such an endeavor and what it would entail. Another suggested targeting the enemy's "data flow charts" in order to paralyze life in a country or reprogramming enemy missiles so they would go back and hit the enemy. At least he admitted to being clueless about flow charts and programming.

Of course, jihadists and persons associated with or sympathetic to al-Qaeda do not represent the only possible threat of cyber terrorism. But no terrorist group has demonstrated much capability or interest in using cyberspace to incite terror. Rather, they use cyberspace to spread their messages and engage in other activities that support their overall objectives.

This does not mean cyberspace has been free of serious threats. To the contrary, the past decade has shown just how vulnerable it is and how damaging attacks can be. But incidents so far are more properly characterized as acts of cybercrime, espionage, or protest than cyber terrorism.

Cybercrime has skyrocketed, with incidents of identity theft, bank and credit card fraud, computer intrusion, extortion, and DoS attacks taking place every day. Tens of millions of computers worldwide have been compromised and placed on “botnets” where they have been commanded to send out spam, provide confidential data, engage in fraud, and participate in massive distributed DoS attacks against selected targets. Even more have been the victim of viruses, Trojans, keystroke loggers, and other forms of malicious software that harvest information and tamper with data. After surveying cyber executives from critical industries in 14 countries, the security firm McAfee reported that 80% of respondents had been the target of a large-scale DoS attack and 85% of a network infiltration in 2010.

Spies routinely penetrate corporate and government networks, stealing proprietary and sensitive information, and routing it to foreign countries. China is often implicated, and in a recently reported espionage case dubbed Shady RAT (so-named for its use of a remote access tool), data from over 70 victims was said to have made its way to that country during the period 2006-2010.

Protestors, including the cyber jihadists but also patriotic hackers and social hacktivists, frequently deface websites and launch DoS attacks against their chosen targets. Some of these attacks have been quite disruptive, for example, the attacks by patriotic Russian hackers against Estonia in 2007 and Georgia in 2008, both of which affected financial services as well as access to government and media websites. However, the group Anonymous and spin-off LulzSec took this to a new level when they started going after targets with a vengeance and for laughs. While claiming to promote free speech, transparency, and democracy, the groups have posted sensitive information taken from companies and law enforcement agencies, including the personal data of police and their informants, in retaliation for arrests of some of their members.

Cyber attacks rarely produce physical damage, which may be one reason they have not yet become an instrument of terrorism. There are exceptions, however, including one that derailed four Polish trams and injured a dozen passengers in 2008. Perhaps the most noteworthy example is Stuxnet, a worm that spread across Microsoft Windows computers but targeted certain Siemens PCS 7 SCADA systems, the industrial control systems responsible for monitoring and controlling critical infrastructures for such services as electric power, oil and gas, and water. Stuxnet was highly selective in its specific targets, and is believed responsible for damaging centrifuges at Iran’s Natanz nuclear enrichment facility with the goal of setting back Iran’s nuclear weapons program. Although the source of the attack is not known, most fingers point to a nation-state, perhaps Israel or Israel in collaboration with the United States.

Researchers are also demonstrating that many cyber-enabled devices are vulnerable to life-threating attacks. They have found vulnerabilities that would allow potentially lethal attacks against implanted pacemakers and defibrillators as well as insulin pumps. They have found others in automobile computer systems that would allow an attacker to take control of a car’s engine or disable the breaks, all with potentially deadly consequences. They have demonstrated SCADA attacks that blow up power generators and are publishing information that could be used in other SCADA attacks.

Jihadists have taken note of the possibilities of SCADA-based attacks, with a posting on the popular al-Shamukh jihadist forum in late 2010 calling for such attacks and claiming they could be used to shut down electricity in one or more American cities. However, while giving a broad overview of SCADA systems and pointing to Stuxnet and other incidents affecting industrial control systems, the posting offered no details for executing such attacks. Further, the premier jihadist English-language publication, *Inspire*, is focused exclusively on physical acts of violence. Readers can learn how to “Make a bomb in the kitchen of your mom,” but not how to conduct even rudimentary cyber attacks.

Thus, the decade following 9/11 closes in much the same state as it began. Al-Qaeda and other terrorist groups still prefer bombs to bytes, and cyber terrorism remains a hypothetical threat even as the overall threat level in cyberspace has increased.