Office of Homeland Security & Preparedness

Intelligence Assessment

The Cyber-Terror Threat

Key Findings

- **Thus far, there have been no known successful cyber attacks conducted by al Qaeda sympathizers or affiliates against US national infrastructure.**
- **The federal government has placed increased emphasis on the cyber threat, citing it in the Annual Threat Assessment of the Director of National Intelligence, released in February 2008, and hosting the nation's largest cyber security exercise, Cyber Storm II, in March 2008.**
- **Cyber attacks in New Jersey have been carried out by local animal rights extremists employing low-level techniques targeting Internet sites and e-mail systems of companies and businesses associated with animal research programs.**
- **Cyberterrorism is an attractive option for foreign-born and domestic terrorists who value its anonymity, potential to inflict massive damage, psychological impact and media appeal. As a new, more computer-savvy generation of terrorists comes of age, the threat of cyber-terror attack is likely to increase.**

Definitions

Cybercrime: Criminal activities that specifically target a computer or network for damage or infiltration. The use of computer(s) as a tool to conduct criminal activity.[1]

Terrorism: To coerce a government or its people in furtherance of political or social objectives through the use of violence.

Cyberterrorism: The convergence of cyberspace and terrorism in the effort to conduct a premeditated, politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies.[2]

Cyberterrorism exists as, and can be understood as, any action that falls within guidelines set forth in *Terrorist Capabilities for Cyberattack: Overview and Policy*, produced by the Congressional Research Service. In this publication, Cyberterrorism has occurred when an action's effects or intent produce results greater than that of general crime, regardless of what kind of actor initiated the sequence.

- **Effects-based:** Cyberterrorism exists when computer attacks result in effects that are disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.
- **Intent-based:** Cyberterrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.[3]

The Cyber Attack Continuum

While to the best of our knowledge terrorist groups have not yet employed cyber tools as a weapon against U.S. critical infrastructure on a large scale, their acquisition of computer expertise and reliance on information technology to formulate plans, raise funds, spread propaganda, and engage in secure communications represent clear warning signs.[4] The cyber or digital world is not only a vast resource used and targeted by terrorists, but also criminal gangs, foreign intelligence services, and hackers – individuals whose mission is to break into private, public, or classified network systems. These groups may share some of the same objectives, regardless of their primary motivation. They may seek to acquire sensitive, proprietary or classified information, personal identity information, financial resources, property, and other materials of intrinsic value. Cyber-terrorists have the additional goal of destruction and disruption to critical information infrastructure.

Cyber attacks can be divided into three categories, [5] which help quantify the different skills and resources required to carry out such an attack:

- *Simple-Unstructured:* Simple-Unstructured attacks are the most common. These are amateurish attacks with relatively minimal consequences.

- *Advanced-Structured:* Advanced-Structured attacks are more sophisticated and thus more consequential having greater emphasis on targeting and focus done prior to an attack, the result being a more debilitating attack.

- *Complex-Coordinated:* Complex-Coordinated attacks are the most advanced and most troublesome type of attack where success could mean a network shutdown.

Attacks on computers can come in many forms, but the most likely methods can include any number of the following: 1) disrupting equipment and hardware reliability, 2) changing processing logic, or 3) stealing or corrupting existing data or information.[6] Any category or method can involve:

- Directing conventional kinetic weapons against computer equipment, a computer facility, or transmission lines to create a physical attack that disrupts the reliability of equipment.

- The power of electromagnetic energy, most commonly in the form of an electromagnetic pulse (EMP), can be used to create an electronic attack (EA) directed against computer equipment or data transmissions. By overheating circuitry or jamming communications, EA disrupts the reliability of equipment and the integrity of data.

- Malicious code can be used to create a cyber attack, or computer network attack (CNA), directed against computer processing code, instruction logic, or data. The code can generate a stream of malicious network packets that can disrupt data or logic through exploiting a vulnerability in computer software, or a weakness in the computer security practices of an organization. This type of cyber attack can disrupt the reliability of equipment, the integrity of data, and the confidentiality of communications.[7]

The following are three recent cyber-terror events – one plot and two actual attacks – that illustrate the scope of the threat:

- On *16 January 2008*, a Central Intelligence Agency (CIA) cybersecurity analyst made a statement at a security conference attended by international government officials, engineers, and security managers from North American energy companies and utilities. He discussed attempted cyber intrusions into utilities outside the US which were followed by extortion demands, and in one instance resulted in a power outage affecting multiple cities.[8]

- In *April and May 2007*, pro-Russian hackers launched numerous attacks on servers throughout Estonia in response to the removal of Soviet era statues in the capital of Estonia, Tallinn.[9] Experts stated that they had never before seen cyber attacks of such sophistication, coordination, and scale. This method of attack is commonly known as a DoS attack, or denial-of-service. This tactic targets central servers, flooding them with false requests, eventually overloading the capacity of the processor and leading to a complete downing of all services. Targets included various hosting services, government websites and a large part of the commercial sector. Estonia, ranked as one of the highest users of Internet technology worldwide, is largely dependent on data networks. These attacks crippled vital daily functions.

- In *early 2007*, Scotland Yard uncovered an al Qaeda plot to infiltrate and destroy a high-security Internet hub in the United Kingdom. The Internet facility was undoubtedly an attractive target because it contains numerous servers vital to UK Internet operations and is a clearinghouse for the majority of Internet activity in and out of Britain. In addition, it appears that the terrorists were planning to steal sensitive information located on the servers and then launch a cyber attack designed to undermine the UK's economic and business sectors.[10]

Cyberterrorism in New Jersey

Historically, cyberterrorism in New Jersey has been used by animal rights extremists who have employed low-level techniques including worms, viruses and denial-of-service attacks to target the websites and e-mail systems of companies and businesses associated with animal research programs. In most cases, this form of cyber disruption involves the sending of thousands of emails en masse to corporate email addresses. These attacks typically target a single business, and do not constitute a threat to the safe operation of the Internet as a whole.

New Jersey remains a valuable target as it possesses a wealth of critical information infrastructure, much of which is inherently interdependent. New Jersey is strategically located along a heavy transit corridor for people and goods, and is a major node along the fiber path from the Northeast to Philadelphia and Washington, DC. Furthermore, New Jersey is one of the wealthiest states in the country and is home to many Fortune 500 companies. Any disruption to the State's economy could have a drastic impact on the national economy and thus the nation's economic stability.

Worst Case Scenario

A "worst case" cyber attack scenario would involve either a massive cyber attack or both a physical attack and a cyber attack carried out simultaneously. The federal government has conducted several tests and exercises designed to measure the viability and impact of such an attack:

- In July 2002, the US Naval War College developed a scenario entitled "Digital Pearl Harbor" to examine the effects of a coordinated cyberterrorism event. In this event, computer security experts attacked critical infrastructure systems simulating state-sponsored cyberwarfare. This test showed that the most vulnerable of systems included the Internet itself as well as the computer systems that are part of the financial infrastructure. This test also showed that the US telecommunications infrastructure would be able to withstand such an attack due to the built-in system security redundancy that would prevent widespread damage. It also noted that such an attack on the US "was only a slight possibility."[11]

- In February 2006, the Department of Homeland Security (DHS) held Cyber Storm, the first national cyber exercise. The most important finding from this exercise was the need for better interagency-communication during such attacks. Other key findings included the need for a formal contingency plan of response, better correlation of multiple incident reporting between public and private sectors, public messaging to minimize damage through individual protective responses, and the overall need for better training tools, and processes of response.[12]

- In March 2007, researchers at Idaho National Laboratories (INL) conducted an experiment labeled "Aurora Generator Test." This test was designed to show the effects of a cyber attack on a power network by targeting a power generator. The generator was forced to shut down after receiving malicious commands from an outside source. This test demonstrated that in the event that enough generators were targeted simultaneously, a system failure is possible.[13]

- And in early March 2008, DHS conducted Cyber Storm II, the nation's largest cyber security exercise. Mandated by Congress, the exercise was designed to simulate a coordinated cyber attack on information technology, communications, chemical, and transportation systems and assets. Participants were from federal, state and local governments, the private sector, and the international community. The exercise and the participants: 1) Examined organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects; 2) Exercised strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures; 3) Validated information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and 4) Examined means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.[14]

Examples of potential New Jersey-based "worst-case" cyber attack scenarios:

Attack: Network intrusions penetrate the New Jersey nuclear power plant control system.
Result: While probably one of the most difficult cyber attacks to execute, it could be one of the most disastrous due to the possibility of loss of human life or the release of radioactive material.

Attack: Hackers/Terrorists launch a massive denial of service attack against major financial/state government entities in New Jersey.
Result: Major disruption of New Jersey economy and catastrophic impact on national economy & national security.

Outlook

Based on the recent series of cyber attacks and plots – and the wealth of knowledge likely gained from such activity – potential cyber terrorists may have expanded their intelligence gathering and target development activities, along with their understanding of "what is possible." The al Qaeda plot in the UK indicates that cyber attacks fall well within the group's intent. A large scale cyberterrorism attack could be the means to al Qaeda's oft-stated goal of crippling the US economy. Whether such an attack is commensurate with al Qaeda's capabilities is less clear. Al Qaeda has consistently demonstrated an ability to plan extensively for an attack. A 2007 report by the Congressional Research Service indicates that an Advanced-Structured cyber attack against multiple nodes in the information infrastructure network would necessitate target surveillance and the creation and testing of tools against the network, a process estimated to take two to four years. Planning for a Complex-Coordinated attack may take six to 10 years.[15] Seized computers which belonged to al Qaeda as well as other terrorist organizations have yielded information suggesting that these organizations are familiar with hacking tools that are available on the Internet.[16]

Intelligence suggests that al Qaeda's radicalization and recruitment energies are focused largely on educated youth, especially those in the fields of engineering and information technology (IT), a demographic more likely to have the skills to plan and execute such an operation. Al Qaeda might begin to recruit such an individual during his/her high school years, allowing the individual to develop further technical skills in college or even a technical school.[17] Further consistency with al Qaeda operations include the use of computer networks in the planning of terrorists acts, including Khalid Shaikh Mohammed's use of Internet chat software to communicate with two of the September 11 hijackers. [18]

It is important to note,

> Department of Defense (DOD) officials have stated that, while the threat of cyber attack is "less likely" to appear than conventional physical attack, it could actually prove more

damaging because it could involve disruptive technology that might generate unpredictable consequences that give an adversary unexpected advantages.[19]

Given that, the mostly likely cyberterrorism attack scenarios involve operations that seek to corrupt government databases, disable delivery of essential services, or circumvent a government's cyber security measures in order to extort and hold for ransom access and control of these systems until the attackers' demands are met. The density and interdependency of New Jersey's major critical infrastructure, coupled with various computer systems that support basic needs and economic activity make the State an attractive target for cyberterrorism attacks. New Jersey has two of the largest industrial sectors in America – the pharmaceutical and oil-refinery industries, both of which rely heavily on computers to regulate key tasks.

Suspicious activity involving IT systems should be treated as having a possible nexus to terrorism, and be reported immediately to the New Jersey Office of Homeland Security and Preparedness (OHSP) at 866-4-SAFE-NJ and to local law enforcement authorities.

For further information on this document or other OHSP analytical products, please contact the OHSP Intelligence Bureau at 609-584-4000, ext. 7.

Endnotes

[1] GAO-070705 "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats" June 2007 http://www.gao.gov/new.items/d07705.pdf
[2] Wilson, Clay "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", CRC Report for Congress, 17 October 2003 http://www.fas.org/irp/crs/RL32114.pdf
[3] Rollins, John and Wilson, Clay "Terrorist Capabilities for Cyberattack: Overview and Policy Issues", CRC Reports for Congress, 22 January 2007 http://www.fas.org/sgp/crs/terror/RL33123.pdf
[4] One such example is the case of Younis Tsouli, aka "Irhabi007." Tsouli is a good example of a Jihadi cyber-terrorist who used the Internet to spread the radical, militant ideology that is central to the radicalization, recruitment, and planning stages of domestic and international cells. Tsouli pleaded guilty to "inciting another person to commit an act of terrorism wholly or partly outside the UK which would, if committed in England and Wales, constitute murder" (a crime introduced in the Terrorism Act 2006) and admitted to conspiring together and with others to defraud banks, credit card companies and charge card companies. Tsouli was sentenced to 10 years imprisonment. In Dec 2007, Tsouli's sentence was increased from 10 to 16 years.
[5] Joseph, Kendall "Global Information Systems Threats, Issues in Systems Security in the New Age of Hactivism, Cyberterrorism and Cyberwarfare" August 2003 http://www.savageideas.com/downloads/mba/Global_Information_Systems_Threats.pdf
[6] Wilson, Clay "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" 15 November 2007 http://www.fas.org/sgp/crs/terror/RL32114.pdf
[7] Wilson, Clay "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" 15 November 2007 http://www.fas.org/sgp/crs/terror/RL32114.pdf
[8] "We (CIA) have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We (CIA) suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We (CIA) have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We (CIA) do not know who executed these attacks or why, but all involved intrusions through the Internet."
[9] "A Cyber-riot" The Economist May 2007 http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598
[10] Leppard, David "Al-Qaeda plot to bring down UK Internet" Times Online, 11 March 2007 http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece
[11] Wilson, Clay "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" 15 November 2007 http://www.fas.org/sgp/crs/terror/RL32114.pdf
[12] http://govtsecurity.com/news/cyber-storm-results/
[13] Wilson, Clay "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" 15 November 2007 http://www.fas.org/sgp/crs/terror/RL32114.pdf
[14] http://www.dhs.gov/xprepresp/training/gc_1204738760400.shtm
[15] Wilson, Clay "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" 15 November 2007 http://www.fas.org/sgp/crs/terror/RL32114.pdf
[16] Congressional Research Service. Foreign Affairs, Defense, and Trade Division. Report for Congress. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.* October 17, 2003.
[17] Congressional Research Service. Foreign Affairs, Defense, and Trade Division. Report for Congress. *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.* October 17, 2003.
[18] Clarke, Richard. April 2003, Vulnerability: What are Al Qaeda's Capabilities? PBS Frontline: Cyberwar.
[19] Wilson, Clay "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress" 15 November 2007 http://www.fas.org/sgp/crs/terror/RL32114.pdf