Office of Intelligence and Analysis
Homeland Security

Homeland Security Assessment

(U//FOUO) Potential Terrorist Threat to the U.S. Information Infrastructure

5 June 2007

(U//FOUO) Prepared by the Critical Infrastructure Threat Analysis Division.

(U) Key Findings

(U//FOUO) DHS assesses that Islamic terrorist groups such as al-Qa'ida, HAMAS, and Hizballah have a growing appreciation of information technology to support their operations, and could parlay their cyber knowledge into attacks on homeland information infrastructure.

(U//FOUO) DHS has no information regarding specific operational planning for cyber attacks by Islamic terrorist groups against the U.S. information infrastructure. Yet, these organizations have expressed interest in capabilities that could exploit cyber vulnerabilities to disrupt provision of services, exact economic costs, and undermine public confidence.

(U//FOUO) Other groups, such as criminal gangs, so-called hacktivists, and lone wolves, also pose a cyber threat to the Homeland.

- ***(U//FOUO) Some hacker groups with the skills to launch cyber attacks are potential talent for hire available to organizations or individuals willing to sponsor cyber attacks.***

- ***(U//FOUO) Individuals or small cells seeking to cause damage by cyber attacks are a challenge for law enforcement and intelligence communities because their activities are often unpredictable and difficult to detect.***

(U//FOUO) The vulnerability of the public network is compounded by the heavy reliance of business and government on open-system protocols and commercial off-the-shelf products to manage networks, and the interconnection of management networks with enterprise networks through the Internet.

(U//FOUO) Islamic Extremists Becoming Computer Savvy

(U//FOUO) Islamic terrorist groups such as al-Qa'ida, HAMAS, and Hizballah incorporate information technology to support their operations and use it for communications, fundraising, propaganda, recruitment, target reconnaissance, and training.

- (U//FOUO) A statement posted on the website azzam.com used by al-Qa'ida-related jihadists urged Muslim Internet professionals to disseminate information through e-mail, online discussion groups, and websites. The statement claimed, "The more websites, the better for us. We must make the Internet our tool."[1]

- (U//FOUO) Islamic extremist groups use websites to provide information on their activities, organization, plans, and political, religious, and social objectives. Groups such as HAMAS and Hizballah and insurgents in Iraq use websites to glorify their violent actions by posting videos and pictures of executions and bombings and statistical updates of daily attacks against the enemy. Many sites publish online exhortations by religious figures encouraging readers to undertake jihad, speeches and declarations of their leaders, and statements and claims of responsibility for attacks.[2]

(U//FOUO) HAMAS and Hizballah are especially technologically savvy with a strong Internet presence and have an interest in collecting information on U.S. infrastructure weaknesses. They routinely use computerized e-mail, encryption to support their operations, and files. They facilitate fundraising and money laundering online by credit card fraud and the establishment of fronts such as charities and technology companies.

(U//FOUO) From Tool to Target

(U//FOUO) In addition to using the Internet to promote their own activities, Islamic extremists have expressed interest in developing the capability to exploit cyber vulnerabilities to disrupt the provision of services, exact economic costs, and undermine public confidence. DHS/I&A lacks information on al-Qa'ida's ability to mount a cyber attack against U.S. infrastructure targets.

- (U//FOUO) An al-Qa'ida operational planner in 2002 explored the possibility of hacking to destabilize banking communications, infrastructures, and power. The development of a specific plan, however, has not been confirmed.[3]

— (U//FOUO) Multiple intelligence reports suggest top-level al-Qa'ida leaders have considered the potential economic and psychological implications of a successful cyber attack on critical infrastructures.

(U//FOUO) Al-Qa'ida Inspired Cyber Jihadists

(U//FOUO) Al-Qa'ida-inspired jihadists use the Internet for the same purposes as core terrorist groups—communications, fundraising, propaganda, recruitment and training, and targeting—but also have demonstrated the capability to disrupt information systems.

— (U//FOUO) The Muslim Hackers Club website provides instructions on how to create and spread viruses, develop code, and devise hacking plans. It includes links to other Islamic extremist and terrorist websites. The site also features links to cyber prankster websites, such as those that purport to disclose sensitive information like code names and radio frequencies used by the U.S. Secret Service.[4,5]

— (U//FOUO) An online community calling itself "Electronic Jihad" in October 2006 claimed it had designed and used an Arabic language hacking program to synchronize a distributed denial-of-service attack against an Israeli website, and that it intended further attacks against "anti-Islamic" websites. The group's website markets itself as a clearinghouse for hackers to network among themselves.[6]

(U//FOUO) Non-Islamic Terrorists

(U//FOUO) According to open source reports Aleph—the Japanese cult and terrorist group formerly known as Aum Shinrikyo that was responsible for the 1995 Tokyo subway sarin attack—has subsequently been involved in developing commercial software, some of which was sold to Japanese firms and government agencies.[7] The cult members probably have the technical expertise to develop software that could be used to launch cyber attacks. DHS is not aware of any intent by the group to target U.S. critical infrastructure.

(U//FOUO) In October 2005 British authorities arrested well-known cyber terrorist Younis Tsouli, known as Irhabi 007 ("terrorist 007"). Tsouli taught hacking techniques and discovered server vulnerabilities. He demonstrated his expertise by hacking a website run by a U.S. state government and a U.S. academic institution. Tsouli maintained contacts with jihadists worldwide, possibly in the United States, the Bahamas, Sweden, and Tunisia, and including Bosnia, Canada, Denmark, Iraq, and the United Kingdom.

(U) Sources:
(U) ACIC Terrorism Summary, 8 June 2006.
(U) SITE Institute, "Irhabi 007 Unveiled: A Portrait of a Cyber-Terrorist," 2006.

(U) Criminal Gangs, Hacktivists, and Lone Wolves

(U//FOUO) Extremist groups focusing on environmental and human rights issues have used cyber attacks to degrade, disrupt, or shut down a target. Known as hacktivists, these operators use denial of service, e-mail floods, website defacement, or malicious code deployment to inflict damage on companies, individuals, and organizations they perceive

as harmful to their cause. They pose a challenge for the law enforcement and intelligence communities because their activities are often unpredictable and difficult to detect.

— (U//FOUO) The Internet Liberation Front (ILF)—an intentional twist on the names of the Earth Liberation Front (ELF) and the Animal Liberation Front (ALF)—says it desires to cause "humiliation or financial disruption to unjust corporations or governments but not harm people."[8]

— (U//FOUO) On at least four occasions in 2005, extremists claiming to represent ALF or Stop Huntingdon Animal Cruelty[USPER] used denial-of-service attacks against U.S. companies' computer and telephone systems to extort money.[9,10,11]

(U//FOUO) Skilled hackers could provide talent for hire that terrorists could use to conduct operations. To date, DHS has not identified any terrorism connection in cyber extortion cases, but the skills hackers use in malicious or criminal activities could suit the agenda of terrorist operatives.

— (U//FOUO) A Miami resident allegedly hired a hacker in June 2006 for $20,000 to discover unprotected computers from which he could route telephone calls and hide his identity. The Miami resident used the hacked computers in a scheme to contract for wholesale bulk minutes of telecommunications time from large telecommunications service providers, sell the bulk time to smaller telecommunications service providers, collect the revenue, and evade paying the original providers.[12]

— (U//FOUO) Hacker groups have gained access to Supervisory Control and Data Acquisition (SCADA) systems of several companies related to the energy sector. In some cases, they exploited vulnerabilities such as absence of passwords on routers or firewalls between the corporate networks and SCADA systems.[13]

(U//FOUO) Hacking software toolkits are available for purchase on the Internet. These tools, already employed in malicious or criminal activities, also could be of use to terrorist operatives planning cyber attacks.

— (U//FOUO) According to online press reports, a Russian website sold a hacking toolkit dubbed "Smartbomb" or the "Web Attacker Toolkit" for between $15 and $20 that has been used on more than 1,000 malicious websites to covertly install software onto a victim's computer that provides access, keystroke logging, and a mechanism for downloading additional code.[14]

— (U//FOUO) According to open source reports, two cyber security firms have discovered a network operating out of Eastern Europe that was distributing customized copies of the data-pilfering Briz.A Trojan for $990. Additional modules were offered for tasks such as hacking into servers to retrieve stolen user names and password information for airlines, banks, hotels, international betting services, and telecommunications companies. Customized modules were also available that compromise File Transfer Protocol sites to store stolen data.[15]

(U) The Insider Threat

(U) Individuals such as contractors, employees, and service providers who have legitimate access to critical computer systems often have detailed operational and security knowledge and physical access that would facilitate a cyber attack.

- ***(U) In 2000 a disgruntled former employee hacked into 300 SCADA nodes that controlled sewage and drinking water in Queensland, Australia and released thousands of gallons of raw sewage into local rivers and parks. Terrorist organizations could try to recruit such insiders to gain their access to a target.***
- ***(U) In August 2006 an Islamic hacktivist in Texas was sentenced to 34 months imprisonment and ordered to pay $44,808 in restitution for using his employee access to a computer data center to hack into a Jewish customer's website.***

(U) Sources:
(U) Duncan Graham-Rowe, *New Scientist*, "Power Play," 15 May 2004.
(U) Department of Justice Press Release, "Former Data Technician at Local Internet Hosting Company and Self-Admitted Supporter of Pro-Jihad Website Sentenced to 34 Months for Attempting to Cause Damage to a Protected Computer." 15 August 2006.

(U) Outlook

(U//FOUO) Businesses and governments' heavy reliance on open-system protocols and commercial off-the-shelf products to manage networks, and the interconnection of management networks through the Internet and with enterprise networks, compound the vulnerability of the public network to cyber attacks by terrorists and other criminals. DHS is working in coordination with Federal, State, and local entities and private sector organizations to improve homeland cyber security. It has established a public-private partnership program among academia, government, and private industry to share information about threats and vulnerabilities and to coordinate responses to cyber attacks. The overall security of the U.S. information infrastructure can be improved by implementing a defense-in-depth strategy, a layered approach based on integrating operations, people, and technology, and balancing protection capabilities against cost, operational impact, and performance.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the National Operation Center (NOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm, and the NOC can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@hq.dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document please contact the DHS/I&A Production Management staff at IA.PM@hq.dhs.gov.

(U) Tracked by: CYBER-010300-02-06, CYBR-040200-02-06, CYBR-010000-02-06, CYBR-010100-02-06, CYBR-010300-02-06, CYBR-020100-02-06, CYBR-020200-01-06, CYBR-040200-02-06

[1] (U) *USA Today*, "Militants Wire Web with Links to Jihad" 10 July 2002.
[2] (U) United States Institute for Peace Press, "Terror on the Internet: The New Arena, The New Challenges," 2006.
[3] (U//FOUO) Tearline, IIS-092-CIA-06.
[4] (U) *Newsweek*, "General: Islamic Cyber Terror; Not a Matter of If But of When," 20 May 2001, OSEC: 24 March 2002.
[5] (U) United States Institute for Peace Press, "Terror on the Internet: The New Arena, The New Challenges," 2006.
[6] (U) Global Issues Report, "Electronic Jihad Group Coordinates Sophisticated Hacking Attacks," 10 October 2006.
[7] (U) Georgetown University, "Is Cyber Terror Next," 2001.
[8] (U) Zone-H, Interview with the Internet Liberation Front, 24 January 2005.
[9] (U) FBI, "Animal Rights Extremists Employing Denial-of-Service Attacks to Achieve Goals," 16 February 2006.
[10] (U) IIR 4 201 4117 05, September 2005.
[11] (U) IIR 4 201 0555 06, October 2005.
[12] (U) DHS/HITRAC Private Sector Note "Voice Over Internet Protocol: A Vulnerable Internet Service," 3 July 2006.
[13] (U//FOUO) Tearline, IIS-101-CIA-06.
[14] (U) TechWeb, "Hacker 'Smartbomb' Toolkit Attacks Unpatched Computers," 24 April 2006.
[15] (U) Tech News World, "Security Firms Bust Malware-For-Sale Racketeers," 4 April 2006.