Assessment

(U//FOUO) Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade

IA-0141-09

Office of Intelligence and Analysis
ASSESSMENT

(U//FOUO) Leftwing Extremists Likely to Increase Use of Cyber Attacks over the Coming Decade

26 January 2009

(U) Prepared by the Strategic Analysis Group, Homeland Environment and Threat Analysis Division.

(U) Scope

(U//FOUO) This product is one of a series of intelligence assessments published by the DHS/Office of Intelligence and Analysis (I&A) Strategic Analysis Group to facilitate a greater understanding of the emerging threats to the United States. The information is provided to federal, state, and local counterterrorism and law enforcement officials so they may effectively deter, prevent, preempt, or respond to terrorist attacks against the United States.

(U//FOUO) This assessment examines the potential threat to homeland security from cyber attacks conducted by leftwing extremists, a threat that DHS/I&A believes likely will grow over the next decade. It focuses on the more prominent leftwing groups within the animal rights, environmental, and anarchist extremist movements that promote or have conducted criminal or terrorist activities (see Appendix). This assessment is intended to alert DHS policymakers, state and local officials, and intelligence analysts monitoring the subject so they can better focus their collection requirements and analysis.

(U//FOUO) The key assumptions underpinning this report include:

— (U//FOUO) Cyber attack capabilities will continue to proliferate and be readily available.

— (U//FOUO) Some cyber attack capabilities will continue to outpace countermeasures.

— (U//FOUO) Leftwing extremists will continue to focus on what they consider economic targets.

— (U//FOUO) Economic enterprises and other organizations will become more dependent on advanced information technologies.

(U) Source Summary Statement

(U//FOUO) This assessment reflects primarily intelligence reporting from federal, state, and local agencies at the Unclassified//For Official Use Only level. Key judgments are based largely on field agent reporting considered highly reliable and on law enforcement finished intelligence. By design, the judgments use an estimative analytic approach. DHS subject-matter experts in the areas of domestic leftwing extremism and cyber technologies provided support for threat and trend analysis. In addition, DHS/I&A examined leftwing extremist media for evidence pointing to ideological shifts or changes in motivation and intent. Government crime data specific to leftwing extremist cyber attacks are unavailable, but DHS/I&A assesses that open source and other data accurately frame leftwing extremist goals and motivations, although some of the sources may have provided information intended to deceive or mislead. Other open source information included business journals and research institute reports.

(U) Key Findings

(U//FOUO) DHS/Office of Intelligence and Analysis (I&A) judges that a number of emerging trends point to leftwing extremists maturing and expanding their cyber attack capabilities over the next decade with the aim of attacking targets in the United States.

- ***(U//FOUO) The potential for economic damage, the individually-initiated and anonymous nature of cyber attacks, and the perception that cyber attacks are nonviolent align well with the ideological beliefs, strategic objectives, and tactics of many leftwing extremists.***

- ***(U//FOUO) The increasing reliance of commercial businesses and other enterprises on cyber technologies, including interconnected networks and remote access, creates new and expanding vulnerabilities that technically-savvy leftwing extremists will exploit.***

- ***(U//FOUO) The proliferation of cyber technologies and expertise as well as the public availability of online hacking tools and "hackers-for-hire" offer leftwing extremists incentives to adopt a cyber attack strategy.***

(U) Appeal of Cyber Attacks

(U//FOUO) DHS/I&A assesses that cyber attacks are attractive options to leftwing extremists who view attacks on economic targets as aligning with their nonviolent, "no-harm" doctrine and tactic of "direct action."

- (U//FOUO) Their no-harm doctrine includes claiming to ensure the safety of humans, animals, and the environment even as they attack businesses and associated operations.

- (U//FOUO) Many leftwing extremists use the tactic of direct action to inflict economic damage on businesses and other targets to force the targeted organization to abandon what the extremists deem objectionable. Direct actions range from animal releases, property theft, vandalism, and cyber attacks—all of which extremists regard as nonviolent—to bombings and arson.

- (U//FOUO) The North American Earth Liberation Front Press Office, the media arm of the Earth Liberation Front (ELF), published the following guidance for activists: "By inflicting as much economic damage as possible, the ELF can allow a given entity to decide if it is in their [*sic*] best economic interest to stop destroying life for the sake of profit."

(U//FOUO) Lone wolves and small cells can conduct highly-effective cyber attacks consistent with the strategy of leaderless resistance that many leftwing extremists embrace. ***DHS/I&A assesses that this facet of leftwing extremist operational strategy***

will further encourage some extremists to improve their cyber attack capabilities and possibly encourage recruitment of individuals with sophisticated cyber skills into their trusted circles. Furthermore, extremists can apply their cyber skills in support of a number of different leftwing movements, a capability that is consistent with the frequent shifting of individuals among movements.

(U) Leaderless Resistance

(U//FOUO) Leaderless resistance stresses the importance of individuals and small cells operating independently and anonymously outside of formalized organizational structures or leadership in order to increase operational security and avoid detection. Postings on extremist websites and other online media forums offer guidance on objectives, tactics, and target selection. Followers are encouraged to self-train, promote their own objectives, and conduct attacks on their own initiative.

(U) The most common leftwing extremist cyber attacks (particularly within the animal rights movement) in the past several years have included deletion of user accounts, flooding a company's server with e-mails, and other types of e-mail assaults intended to force businesses to exhaust resources.

— (U//FOUO) On 13 July 2007, an animal rights extremist hacked into a U.S. company's computer system and deleted more than 300 associates' user accounts. To restore the accounts, the perpetrator demanded that the company sell its shares in a corporation that conducts tests using animal subjects.

— (U//FOUO) In October 2005, animal rights extremists launched an e-mail attack against a Milwaukee, Wisconsin firm that held stock in an animal testing laboratory. The firm subsequently sold its shares in the laboratory, with losses it estimated at approximately $1.4 million.

— (U//FOUO) In late April 2005, animal rights extremists overwhelmed a U.S. company's computer server with e-mail, which the company claims resulted in a loss of approximately $1.25 million.

(U) Attractive Strategy for the Future

(U//FOUO) DHS/I&A judges that the cyber attack option will become increasingly attractive to leftwing extremists as companies' reliance on cyber technologies grows. DHS/I&A also assesses that these extremists will improve their cyber attack capabilities by keeping pace with emerging technologies and overcoming countermeasures that develop over the period of this assessment.

(U) Increasing Reliance on Cyber Technologies

(U//FOUO) Businesses and other enterprises rely on interconnected computer networks for operational continuity, storage of vital data, and communications, introducing vulnerabilities that leftwing extremists could exploit. For example, the use of integrated

systems and remote access creates opportunities for computer intrusion and data theft through poorly-monitored or unsecured connections. In this target rich environment, cyber attacks likely will become an increasingly attractive option, particularly on businesses and industries that extremists consider high-priority targets.

— (U) The logging industry, a principal target for environmental extremists and an industry not traditionally associated with cyber technologies, now relies on integrated systems to support forestry operations.

— (U) The farming industry also is experiencing a growth in the use of advanced technologies, such as Global Positioning Systems and remote sensing, to cut costs and manage crop production. The agricultural industry often is a target of environmental extremists who oppose genetically-modified crop production.

(U) Proliferation of Cyber Attack Tools and Expertise

(U//FOUO) DHS/I&A believes that the availability of cyber technologies and expertise such as online hacking tools and hackers-for-hire provides leftwing extremists with resources to augment their own homegrown cyber attack capabilities. Resources and capabilities for successful cyber attacks are becoming more accessible to the public as evidenced by online advertisements for hacking services and software. A simple online search provides users with numerous links to discussion forums and websites that offer hacking tutorials and information regarding exploitable system vulnerabilities.
In addition, illegal file-sharing sites allow pirated copies of hacking software to be freely exchanged.

— (U//FOUO) In October 2007, law enforcement authorities discovered a group advertising hacking services to customers seeking passwords to the e-mail accounts of spouses, employees, and business competitors.

— (U//FOUO) A website identified early in 2008 originating in the United States provided customers the ability to purchase and download hacking tools and malicious codes as well as video tutorials on how to use the software.

(U//FOUO) DHS/I&A believes that the emerging trend exhibited by some leftwing extremists of posting hacking-related materials on their websites signifies their intent to develop more robust cyber strategies over the coming decade.

— (U) *The Anarchist Cookbook*, continually updated and revised in online versions and accessible on numerous anarchist, animal rights, and environmental websites, contains several chapters focusing on hacking techniques and tutorials.

— (U) Popular anarchist Internet groups such as The Hacktivist[USPER] and Internet Liberation Front[USPER] promote hacking as a means of direct action and publish links to hacking resources on their websites.

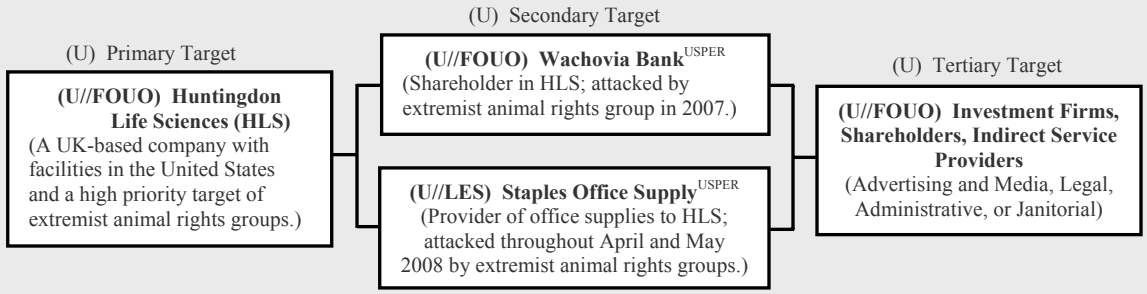
(U) ***Hacktivism*:** The convergence of "hacking" and "activism," using cyber technologies to achieve a political end. Hacktivism includes website defacement, denial-of-service attacks, hacking into the target's network to introduce malicious software, information theft, insider attacks, economic sabotage, and other malicious Internet-based activities.

(U) Potential Targets

(U//FOUO) Based on an analysis of previous limited attacks, both cyber and noncyber, and on the prospective growing advantages of cyber attacks in the future, DHS/I&A judges that potential targets likely will expand to include a broader set of organizations and critical infrastructure that extremists associate with harming animals and degrading the natural environment, as well as icons of capitalism and authority.

— (U//FOUO) In addition, DHS/I&A judges that leftwing extremists will build upon the perceived success of previous, noncyber attacks on secondary targets—organizations with business links to a primary target—and increasingly will attack secondary and possibly tertiary targets. One animal rights extremist website claims that attacks on secondary businesses have resulted in more than 200 companies severing ties with the primary target organization. Secondary targets in previous, noncyber attacks have included financial partners and suppliers associated with the principal target organization.

(U) Potential Range of Target Selection



(U//FOUO) The international nature of many types of cyber attacks means that many more attackers will be available to attack a greater number of distant targets, including those in the United States. A recent study of noncyber attacks demonstrates that a majority of leftwing extremists previously have focused their efforts locally and limited their targeting to within 30 miles of where they live; global connectivity, however, makes the distance between the cyber attacker and the target irrelevant.

— (U) One extremist animal rights group's monthly newsletter stated that

> in today's technological age, computer systems are the real front doors to companies. So instead of chaining ourselves together in the physical doorways of businesses we can achieve the same effect from the comfort [*sic*] our armchairs.

(U) Potential Indicators

(U//FOUO) The following highlight a range of signposts that may expose leftwing extremists' intent—either domestically or abroad—to develop more robust cyber attack strategies:

- (U//FOUO) Increasing number of statements by leftwing extremists advocating the use of cyber attack techniques.
- (U//FOUO) Increasing number of communiques published on leftwing extremist websites claiming credit for cyber attacks.
- (U//FOUO) Suspicious cyber attack activity or increased frequency, creativity, or severity against traditional primary, secondary, and tertiary targets of leftwing extremists.
- (U//FOUO) Evidence that leftwing extremist groups or activists are recruiting or attempting to acquire the services of individuals with cyber capabilities.

(U) Cyber Attack Terms

(U) Cyber attacks are malicious acts that degrade the availability, integrity, or security of data. Cyber attack techniques are constantly evolving; some examples include the following:

- (U) Unauthorized intrusions into computer networks and systems.
- (U) Website defacement or subtle changes to web pages in order to disseminate false information.
- (U) Information theft, computer network exploitation, and extortion.
- (U) Denial-of-service attacks, typically by overwhelming the resources of the system.
- (U) The introduction of malicious software into a computer network.

(U) **Reporting Notice:**

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to DHS and the FBI. The DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@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. The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm. 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 Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.sgov.gov, or IA.PM@dhs.ic.gov.

(U) **Tracked by:** CRIM-040600-01-05, TERR-060100-01-05, TERR-060800-01-05

(U) Appendix: Leftwing Extremists

(U//FOUO) DHS/Office of Intelligence and Analysis defines leftwing extremists as groups or individuals who embrace radical elements of the anarchist, animal rights, or environmental movements and are often willing to violate the law to achieve their objectives. Many leftwing extremist groups are not hierarchically ordered with defined members, leaders, or chain of command structures but operate as loosely-connected underground movements composed of "lone wolves," small cells, and splinter groups.

— (U//LES) ***Animal rights and environmental extremists*** seek to end the perceived abuse and suffering of animals and the degradation of the natural environment perpetrated by humans. They use non-violent and violent tactics that, at times, violate criminal law. Many of these extremists claim they are conducting these activities on behalf of two of the most active groups, the Animal Liberation Front and its sister organization, the Earth Liberation Front. Other prominent groups include Stop Huntingdon Animal Cruelty; and chapters within the Animal Defense League[USPER], and Earth First![USPER].

— (U//FOUO) ***Anarchist extremists*** generally embrace a number of radical philosophical components of anticapitalist, antiglobalization, communist, socialist, and other movements. Anarchist groups seek abolition of social, political, and economic hierarchies, including Western-style governments and large business enterprises, and frequently advocate criminal actions of varying scale and scope to accomplish their goals. Anarchist extremist groups include entities within Crimethinc[USPER], the Ruckus Society[USPER],and Recreate 68[USPER].