



**COMMONWEALTH of VIRGINIA**  
*Department for the Aging*

[Click here to go to the Virginia Department for the Aging Home Page](#)

**TABLE OF CONTENTS**  
**AAA TUESDAY E-MAILING**  
**February 17, 2009**

<b>SUBJECT</b>	<b>VDA ID NUMBER</b>
<a href="#"><u>Older Americans Month - 2009</u></a> (Bill Peterson)	<b>09-63</b>
<a href="#"><u>New Website for Unemployed Older Americans</u></a> (Bill Peterson)	<b>09-64</b>
<a href="#"><u>AHRQ Preventive Health Guides</u></a> (Elaine Smith)	<b>09-65</b>
<a href="#"><u>Resources for Information on Salmonella Typhimurium Outbreak</u></a> (Elaine Smith)	<b>09-66</b>
<a href="#"><u>Poisoning Prevention Train-the-Trainer</u></a> (Elaine Smith)	<b>09-67</b>
<a href="#"><u>National Family Caregiver Support Program</u></a> (Ellen Nau)	<b>09-68</b>
<a href="#"><u>National Alzheimer's Contact Center</u></a> (Tim Catherman)	<b>09-69</b>
<a href="#"><u>Homeland Security Assessment: Likely Increase of Cyber Attacks</u></a> (Deb Loving)	<b>09-70</b>

**Note:** The web addresses (links) in this document may change over time. The Department for the Aging does not attempt to refresh the links once the week has passed. However, this document is maintained on the web for a period of time as a reference. Some links may require registration.

1610 Forest Avenue, Suite 100, Richmond, Virginia 23229  
Toll-Free: 1-800-552-3402 (Voice/TTY) • Phone: 804-662-9333 • Fax: 804-662-9354  
E-mail: [aging@vda.virginia.gov](mailto:aging@vda.virginia.gov) • Web Site: [www.vda.virginia.gov](http://www.vda.virginia.gov)



*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

**MEMORANDUM**

**TO:** Directors  
Area Agencies on Aging

**FROM:** Bill Peterson

**DATE:** February 17, 2009

**SUBJECT:** Older Americans Month - 2009

Each year the Administration on Aging (AoA) issues a theme for Older Americans Month to assist the national aging services network plan for activities that might take place in May or throughout the year. This year's theme is "**Living Today for a Better Tomorrow**" and reflects AoA's continued focus on prevention efforts that are helping older adults have better health as they age and avoid the risks of chronic disease, disability and injury.

AoA encourages everyone to take steps today to ensure healthier and better quality lives tomorrow. For more information about the history of Older Americans Month and Older Americans Month 2009, please visit:

<http://www.aoa.gov/PRESS/Observances/oam/oam.aspx>



*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**FROM:** Bill Peterson

**DATE:** 2/17/09

**SUBJECT:** New Website for Unemployed Older Americans

AARP has launched a new online web portal called [Real Relief](#) to assist Americans during this difficult economic time. This one-stop online site focuses both on jobs and job training, and on financial issues such as money management and investment help.

The Real Relief web portal covers many topics, including:

- Tips for job seekers: job search strategies and resources; help with issues involving self-employment and small businesses.
- Financial advice: tips and resources for protecting investments and cutting expenses.
- Help with taxes and money management: free services to help during tax season, and with bill paying and other money management issues.
- Public benefits: information on public assistance programs, as well as Social Security and Medicare.

Please feel free to share the [Real Relief](#) weblink with your clients or others in your community.



*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**AND:** Nutrition Directors  
Health Promotion and Disease Prevention Coordinators

**FROM:** Elaine S. Smith, MS, RD  
Program Coordinator

**DATE:** February 17, 2009

**SUBJECT:** AHRQ Preventive Health Guides

As reported in the September 2008 *Caregiving Exchange*, the Agency for Healthcare Research and Quality (AHRQ) recently released a checklist for men and one for women that are founded in evidence-based recommendations from the US Preventive Services Task Force regarding screening tests, preventive medicine, and healthy lifestyle behaviors. These checklists are now available in Spanish.

The women's checklist is available here, <http://www.ahrq.gov/consumer/women50sp.pdf> (For English: [www.ahrq.gov/ppip/women50.htm](http://www.ahrq.gov/ppip/women50.htm) or <http://www.ahrq.gov/ppip/women50.pdf> ); and, the men's checklist is available here, <http://www.ahrq.gov/consumer/men50sp.pdf> (For English: [www.ahrq.gov/ppip/men50.htm](http://www.ahrq.gov/ppip/men50.htm) or <http://www.ahrq.gov/ppip/men50.pdf> )

Family caregivers of those 50+ may want to have this checklist to be sure that their loved one is addressing all the necessary healthcare issues. If they are 50+, caregivers themselves should be sure that they are also following the checklist.



*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**AND:** Nutrition Directors

**FROM:** Elaine S. Smith, MS, RD  
Program Coordinator

**DATE:** February 17, 2009

**SUBJECT:** Resources for Information on Salmonella Typhimurium Outbreak

New CDC/FDA Social Media Resources for Information on Salmonella Typhimurium Outbreak are available.

The U.S. Department of Health and Human Services, Food and Drug Administration and Centers for Disease Control and Prevention are working together to provide important information about the recall of certain peanut butter and peanut-containing products that are associated with the recent Salmonella Typhimurium outbreaks.

The latest resource is the new HHS, FDA and CDC social media Web page at <http://www.cdc.gov/socialmedia/> which provides many helpful tools in order to reach as many people as possible.

The social media site makes it easy to obtain automatically updated information on the outbreak and the product recall. The site provides resources for both consumers and partners. Many of these resources are available in both English and Spanish.

Call 1-800-CDC-INFO (1-800-232-4636), 24 hours a day, 7 days a week, for up-to-date information about the recalls and hundreds of other health and safety topics.



**COMMONWEALTH of VIRGINIA**  
*Department for the Aging*

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**AND:** Nutrition Directors  
Health Promotion and Disease Prevention Coordinators

**FROM:** Elaine S. Smith, MS, RD  
Program Coordinator

**DATE:** February 17, 2009

**SUBJECT: Poisoning Prevention Train-the-Trainer**

Passing on Greetings from the Blue Ridge Poison Center!

*Did you know?*

- Each year nearly 80,000 senior citizens in the U.S. are poisoned.
- The most common source of senior poisoning is *medicine*: prescription, over-the-counter, and herbal supplements.
- Though half of all calls to poison centers are about children under age 6, adults are *95 times more likely than children* to die from a poison exposure.

The Public Education Specialists at the Blue Ridge Poison Center will be offering a half-day course for adults who work or volunteer with seniors, and who want to help teach them to stay safe from poisoning. Participants will receive training and all the materials needed to teach seniors about poison safety and prevention. No prior teaching

experience required. Workshops will be held in the following places: **Farmville** (3/13/09), **Bedford** (3/26/09), **Lexington** (4/16/09), and **Winchester** (5/21/09).

The workshop is FREE thanks to a grant from the Division of Injury Prevention at the Virginia Department of Health. Registration is required; space may be limited. For more information or to register, contact:

Kristin Wenger, Education Coordinator  
Blue Ridge Poison Center  
Klw2s@virginia.edu or 434-982-4386.

A registration form follows and materials are also online at  
[www.healthsystem.virginia.edu/brpc/](http://www.healthsystem.virginia.edu/brpc/)

Please feel free to share this with others in your communities.



REGISTRATION:

***“Poison Smarts for Seniors”***  
**Train-the-Trainer Workshop**

YES! I will attend: (check one)

KEYSVILLE, VA  
Friday, March 13, 2009  
Southside Va. Comm. College  
John H. Daniel Campus  
10:00 am—3:00 pm

BEDFORD, VA  
Thursday, March 26, 2009  
Central Va. Comm. College  
Bedford Center  
1:00 pm—4:30 pm

LEXINGTON, VA  
Thursday, April 16, 2009  
Dabney S. Lancaster Comm. College  
10:00 am—3:00 pm

WINCHESTER, VA  
Thursday, May 21, 2009  
Valley Health Wellness & Fitness Ctr.  
1:00 pm—4:30 pm

NAME: \_\_\_\_\_

ORGANIZATION: \_\_\_\_\_

JOB TITLE: \_\_\_\_\_

WORK MAILING ADDRESS: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

WORK PHONE: \_\_\_\_\_ FAX: \_\_\_\_\_

EMAIL: \_\_\_\_\_

**Workshop is free, thanks to a grant from the VA Dept. of Health, but space is limited. If you need to cancel, kindly give us notice so that someone may be offered your spot.**

*More details about workshop location, including directions and parking instructions, will be sent along with confirmation that we've received your registration form.*

**To return registration form, choose from the following:**

- FAX: 434-971-8657 Att. Kristin Wenger, Blue Ridge Poison Center
- EMAIL: Kristin Wenger KLV2S@virginia.edu
- U.S. MAIL: Kristin Wenger  
Blue Ridge Poison Center  
University of Virginia Health System  
Box 800-774  
Charlottesville, VA 22908
- Questions? Call Kristin Wenger 434-982-4386 M-F business hours.



*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**FROM:** Ellen M. Nau

**DATE:** February 17, 2009

**SUBJECT:** National Family Caregiver Support Program

**United Hospital Fund**

On January 13, 2009 the United Hospital Fund of New York launched its Next Step in Care Website: [www.nextstepincare.org](http://www.nextstepincare.org). Guides and checklists are available on the website to aid caregivers of persons with serious illnesses. Suggestions are made to aid patients' transitions between care settings. This website is the Fund's efforts to address a multitude of patient transition issues.

**National Resource Directory (Department of Defense)**

The web-based directory includes resources for wounded, ill and injured service members, veterans, their families, families of the fallen and those who support them. The directory was produced by the Departments of Defense, Labor and Veterans Affairs. Visit:

<https://www.nationalresourcedirectory.org>

**Second African-American Conference: The Journey Continues – Exploring Alzheimer's and Dementia in African-American Families**

The conference will be held Saturday, March 28, 2009 from 8:30 A.M. until 2:30 P.M. at the Fifth Baptist Church at 1415 W. Cary Street in Richmond,

**Subject: National Family Caregiver Support Program**

Page 2 of 2

Virginia. Pre-registration is required. The cost is \$20.00 per person which includes lunch and conference materials. For the conference agenda and registration information, please consult the attachment to this email.



presents

## Second African-American Conference: The Journey Continues - Exploring Alzheimer's and Dementia in African-American Families

Conference Location:

Date/Time:

Fifth Baptist Church  
1415 W. Cary St.  
Richmond, VA 23220

Saturday, March 28, 2009  
8:30 am – 2:30 pm

8:30 am	Registration	
9:00 am	Welcome	Vivian Bagby, Chair African-American Outreach Committee
9:30 am	Dementia and the African-American Family	Arlene Bohannon, M.D.
10:15 am	Stress, Strengths and Dementia	Dr. Joyce Beckett Purnell
10:45 am	The Role of the Church for the Care Partner And the Person with Dementia	Rev. Dr. Patricia Gould-Champ
11:15 am	Questions	
12:00 pm	Lunch	
12:45 pm	Legal and Financial Issues	Christopher McCarthy, Esq.
1:15 pm	Resource Panel Alzheimer's Association, Senior Connections, Veterans Benefits, and PACE	
1:45 pm	Questions for Panel	
2:15 pm	Wrap-Up and Evaluations	

Pre-Registration Required – Cost is \$20 per person which includes Lunch and Materials  
Call 967-2580 to pre-register or complete form  
and mail to Alzheimer's Association at address below.

Second African-American Conference: The Journey Continues - Exploring Alzheimer's and  
Dementia in African-American Families  
March 28, 2009

Name \_\_\_\_\_

Street Address \_\_\_\_\_

City, State, Zip \_\_\_\_\_

Phone Number \_\_\_\_\_

Amount Enclosed \_\_\_\_\_

Alzheimer's Association • 4600 Cox Road, Suite 130 • Glen Allen, VA 23060  
Phone: 804-967-2580 • Fax: 804-967-2588  
[www.alz.org/grva](http://www.alz.org/grva)

*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

February 17, 2009

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**FROM:** Tim Catherman  
Director of Administrative Services

**RE:** National Alzheimer's Contact Center

The following announcement is from AoA.

Thank you to all of you who have supported the National Alzheimer's Contact Center Linking Campaign! Related to this initiative, last year the U.S. Administration on Aging (AoA) and the Alzheimer's Association - National Office offered a series of conference calls that took place during March & early April 2008 to promote the National Alzheimer's Contact Center, for which AoA has been providing funding support since 2003. Each call offered the opportunity to learn about what the Contact Center offers to assist persons with Alzheimer's disease and other dementias, family caregivers, and professionals via:

- 24/7 live telephone support,
- Message boards in English & Spanish on a wide variety of topics,
- Interactive on-line screening tools & resources, and more.

Based on feedback we received, **AoA is again partnering to promote a similar series of conference calls in 2009! All are invited – especially new staff / interns / volunteers, or those just interested in getting a refresher.**

Learn how you can use these resources to complement other aging network programs and initiatives. Individuals with Information & Referral/Assistance, Aging & Disability Resource Centers, Title III-E Family Caregiver Support Program, and/or responsibilities, including those at State Units on Aging, Area Agencies on Aging, Tribes and other organizations, as appropriate, are welcome to participate.

1610 Forest Avenue, Suite 100, Richmond, Virginia 23229  
Toll-Free: 1-800-552-3402 (Voice/TTY) • Phone: 804-662-9333 • Fax: 804-662-9354  
E-mail: [aging@vda.virginia.gov](mailto:aging@vda.virginia.gov) • Web Site: [www.vda.virginia.gov](http://www.vda.virginia.gov)

**National Alzheimer's Contact Center**  
**Page 2 of 3**

To participate in a call, please RSVP to Amy Wiatr, AoA, at [amy.wiatr@aoa.hhs.gov](mailto:amy.wiatr@aoa.hhs.gov) with your name & date of the session you wish to join to ensure the appropriate number of call-in lines are available. Please arrange to be at a computer with internet access to the [www.alz.org](http://www.alz.org) site. Each call will follow the same basic outline to provide a guided tour of some of the on-line Contact Center tools, as well as a brief overview of the Contact Center's history, current operations, and ideas for collaborations.

Please see the schedule with dates and times below. The Dial-in number: 866-316-2054 & Passcode: 2624425328 are the same for all calls.

Date	Time
Tuesday, March 10	2:30 - 4 PM Eastern / 1:30 - 3 PM Central / 12:30 – 2 PM Mountain / 11:30 AM – 1 PM Pacific
Tuesday, March 31	<p>Note: this call is specially scheduled to allow participation from those in relative time zone extremes</p> <p>5 – 6:30 PM Eastern / 4 – 5:30 PM Central / 3 – 4:30 PM Mountain / 2 – 3:30 PM Pacific / 1 – 2:30 PM Alaska / 12 – 1:30 PM Hawaii-Aleutian / 11 AM – 12:30 PM American Samoa</p> <p><i>And 4/1/09 8 – 9:30 AM Chamorro (Guam &amp; CNMI)</i></p>
Wednesday, April 1	3 – 4:30 PM Eastern / 2 – 3:30 PM Central / 1 – 2:30 PM Mountain / 12 – 1:30 PM Pacific

AoA has been providing grant funding support for the National Alzheimer's Contact Center since 2003. The goal of the project is to improve the quality of life of people with Alzheimer's and their caregivers through an integrated network of information specialists and care consultants who provide personalized information, support, care consultation and crisis intervention by telephone and electronically, 24 hours a day, 7 days a week and 365 days a year. The Contact Center operates through one 800 number and provides services throughout the country in partnership with the Association's chapter network. The Contact Center (central location in Chicago) handles over 10,000 calls per month, with an additional over 11,000 calls per month being handled at the local chapters (throughout the country). The Contact Center also offers support via Message Boards and a number of on-line tools.

**National Alzheimer's Contact Center**  
**Page 3 of 3**

Visit [http://www.alz.org/we\\_can\\_help\\_24\\_7\\_helpline.asp](http://www.alz.org/we_can_help_24_7_helpline.asp) to see more about the Contact Center. You may also contact your local Alzheimer's Association chapter for more information.

We look forward to your participation!

Amy Wiatr, MSW  
Aging Services Program Specialist  
U. S. Administration on Aging  
Chicago Regional Support Center  
233 N. Michigan Ave., Suite 790  
Chicago, IL 60601  
Phone: 312-886-8536  
Fax: 312-886-8533  
Email: [amy.wiatr@aoa.gov](mailto:amy.wiatr@aoa.gov)



*COMMONWEALTH of VIRGINIA*  
*Department for the Aging*

**MEMORANDUM**

**TO:** Executive Directors  
Area Agencies on Aging

**FROM:** Deb Loving

**DATE:** February 17, 2009

**SUBJECT:** Homeland Security Assessment: Likely Increase of Cyber Attacks

Please review the attached document from the Department of Homeland Security / Office of Intelligence and Analysis (I&A), and share it with your agency's IT professionals.



# Assessment

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

1/A 0163 09



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

5 February 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 the following:

- (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) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized security personnel without further approval from DHS.

(U) This product contains U.S. person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label <sup>USPER</sup> and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other U.S. person information has been minimized. Should you require the minimized U.S. person information, please contact the DHS/I&A Production Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.gov, or IA.PM@dhs.ic.gov.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

— (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) The 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<sup>USPER</sup>, 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.

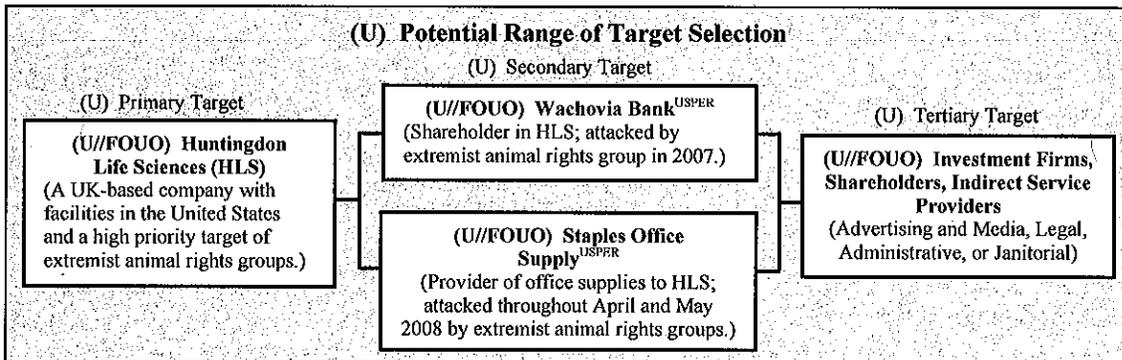
- (U) Popular anarchist Internet groups such as The Hacktivist and Internet Liberation Front <sup>USPER</sup> promote hacking as a means of direct action and publish links to hacking resources on their websites.

(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//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 communiqués 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 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](mailto: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](mailto: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](mailto:IA.PM@hq.dhs.gov), [IA.PM@dhs.gov](mailto:IA.PM@dhs.gov), or [IA.PM@dhs.ic.gov](mailto: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) The 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//FOUO) *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.
- (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.