Corporate Hacking and Technology-Driven Crime:
Social Dynamics and Implications

Thomas J. Holt
Michigan State University, USA

Bernadette H. Schell
Laurentian University, Canada

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey • New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Joel Gamon
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Corporate hacking and technology-driven crime : social dynamics and implications / Thomas J. Holt and Bernadette H. Schell, editors. p. cm.
Includes bibliographical references and index. Summary: "This book addresses various aspects of hacking and technology-driven crime, including the ability to understand computer-based threats, identify and examine attack dynamics, and find solutions"--Provided by publisher. ISBN 978-1-61692-805-6 (hbk.) -- ISBN 978-1-61692-807-0 (ebook) 1. Computer crimes. 2. Computer hackers. I. Holt, Thomas J., 1978- II. Schell, Bernadette H. (Bernadette Hlubik), 1952- HV6773.C674 2011
364.16'8--dc22
2010016447

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Section 4

Marco-System Issues Regarding Corporate and Government Hacking and Network Intrusions

Chapter 9
Cyber Conflict as an Emergent Social Phenomenon

Dorothy E. Denning
Naval Postgraduate School, USA

ABSTRACT

This chapter examines the emergence of social networks of non-state warriors launching cyber attacks for social and political reasons. It examines the origin and nature of these networks; their objectives, targets, tactics, and use of online forums; and their relationship, if any, to their governments. General concepts are illustrated with case studies drawn from operations by Strano Net, the Electronic Disturbance Theater, the Electrohippies, and other networks of cyber activists; electronic jihad as practiced by those affiliated with al-Qa'ida and the global jihadist movement associated with it; and operations by patriotic hackers from China, Russia, and elsewhere.

INTRODUCTION

Warfare is inherently social. Soldiers train and operate in units, fighting and dying for each other as much as for their countries. Cyber conflict is also social, but whereas traditional warriors work and socialize in physical settings, cyber warriors operate and relate primarily in virtual space. They communicate electronically and meet in online forums, where they coordinate operations and distribute the software tools and knowledge needed to launch attacks. Their targets are electronic networks, computers, and data.

DOI: 10.4018/978-1-61692-805-6.ch009

The Emergence of Cyber Conflict, or Hacking for Political and Social Objectives

Although conflict appears throughout human history, its manifestation in cyberspace is a relatively recent phenomenon. After all, digital computers did not appear until the 1940s, and computer networks until the 1960s. Attacks against computers and the data they held emerged in the late 1950s and early 1960s, but they were perpetrated more

for money and revenge than as an instrument of national and international conflict. Typical crimes included bank fraud, embezzlement, information theft, unauthorized use, and vandalism (Parker, 1976). Teenage hacking arrived on the scene in the 1970s, and then grew in the 1980s, as young computer users pursued their desire to explore networks, have fun, and earn bragging rights. By the end of the decade, the single biggest attack on the Internet was a computer worm launched by a college student simply as an experiment. Within this mix of playful hacking and serious computer crime, cyber conflict, or hacking for political and social objectives, emerged, taking root in the 1990s and then blossoming in the 2000s. Now, it accounts for a substantial share of all cyber attacks, as well as some of the highest profile attacks on the Internet, such as the ones perpetrated by patriotic Russian hackers against Estonia in 2007 and Georgia in 2008.

The Hacker Group Phenomenon

From the outset, hackers and cyber criminals have operated in groups. In his examination of early computer-related crime, Donn Parker found that about half of the cases involved collusion, sometimes in groups of six or more (Parker, 1976, p. 51). Youthful hackers met on hacker bulletin boards and formed clubs, one of the earliest and most prestigious being the Legion of Doom (Denning, 1999, p. 49), while serious criminals formed networks to traffic in cyber crime tools and booty, such as stolen credit cards. Today, there are perhaps tens or hundreds of thousands of social networks engaging in cyber attacks. While many of these networks were formed for fun or financial gain, others arose for the purpose of engaging in cyber conflict. Individuals, often already connected through hacker groups or other social networks, came together to hack for a cause.

The Purpose of This Chapter

This chapter examines the emergence of social networks of non-state warriors launching cyber attacks for social and political reasons. These networks support a variety of causes in such areas as human and animal rights, globalization, state politics, and international affairs. This chapter examines the origin and nature of these networks; their objectives, targets, tactics, and use of online forums. It also describes the relationship, if any, to their governments.

THE NATURE OF NON-STATE NETWORKS

Unlike states, non-state networks of cyber soldiers typically operate without the constraints imposed by rigid hierarchies of command and control, formal doctrine, or official rules and procedures. Instead, they operate in loosely-connected networks encouraging and facilitating independent action in support of common objectives--what is sometimes characterized as "leaderless resistance."

However, while the networks are decentralized, they are not actually leaderless. A few individuals, often already connected outside cyberspace or from previous operations, effectively take charge, or at least get things started. They articulate goals and strategy, plan and announce cyber attacks, encourage people to participate, and provide instructions and tools for participating. They manage the online forums--websites, web forums and groups, discussion boards, chat rooms/channels, email lists, and so forth--supporting network activities. They also develop or acquire the automated software tools used by the group. Often, the tools themselves give the leaders some control over the conduct of cyber attacks (e.g., selection of targets and rate of attack), compensating for the lack of a hierarchical command structure over the network players.

The net effect is that non-state cyber warriors are able to mobilize and conduct attacks on relatively short notice, unconstrained by the need to follow time-consuming protocols or wait for an approval process to move through a chain of command. Further, the networks can grow to include thousands of participants, as resources are not needed to pay, train, or relocate individual warriors. Assuming adequate bandwidth, an online forum that supports a small cyber army can just as easily support a large one.

Online forums play a vital social role in the formation, growth, and operation of cyber conflict networks. Participants use the forums to acquire information, discuss issues, and get to know each other. The forums foster a sense of group identity and community, while rhetoric on the forums stirs up emotions, inspires action, and promotes a sense of "us vs. them." Newcomers see that others are engaged in, or planning to engage in, cyber attacks—leading to the overarching perception that such activity is normative for the group. By observing this collective behavior, they are more easily influenced to set aside any personal reservations and go along with the group, especially if they can do so with little risk and exposure, hiding in the cyber crowd behind a veil of relative anonymity. The forums also serve as a support base for operations, providing a means for distributing cyber attack tools and information about how to use the tools and what targets to attack, as well as coordinating the attacks. Participants may be encouraged to compete for recognition or prizes, based on who conducts the most attacks.

THIS CHAPTER'S FOCUS: HACKTIVISM, ELECTRONIC JIHAD, AND PATRIOTIC HACKING

With this background in place, the chapter now examines three areas of cyber conflict: (1) hacktivism, (ii) electronic jihad, and (iii) patriotic hacking. Hacktivism, combining hacking with social and political activism, is the broadest area; it can involve small groups of local activists or large groups crossing international boundaries and coming together over the Internet. Targets are typically government institutions, including both national and international bodies, but they also include businesses and other non-state groups. Electronic jihad refers to cyber attacks conducted in support of the terrorist group al-Qa'ida and the global jihadist movement associated with it. Targets include both government and non-government entities across the globe, but especially in the United States and other Western countries. Patriotic hacking covers state-on-state conflict, but the perpetrators of the cyber attacks are citizens and expatriates rather than governments. Targets are both government and non-government entities in the opposing state.

Although these three areas of conflict are discussed separately, they are not disjoint. Indeed, hacktivism is often used to cover all non-state social and political hacking, and hence could be considered as encompassing the other two areas.

There are some areas of conflict not addressed in this chapter, most notably conflicts involving racists and extremists engaging in hate crimes and terrorism. However, electronic jihad exemplifies this general area of conflict and how it plays out on a large scale across the Internet. Another area not covered is conflict at an individual level. Instead, the chapter focuses on conflicts relating to broader societal issues.

The following sections discuss each area of these three key areas in greater depth. For each type, motives, social networks, and activities are described, and case studies are used to illustrate general principles and historical developments. The final section concludes and discusses implications for the future.

HACKTIVISM

Defined

Hacktivism is the convergence of hacking with activism. It arose when social activists with computer skills began hacking for a cause, usually within networks of other activists.

Cases of Hacktivism

In one of the earliest reported cases of hacktivism, protestors unleashed a computer worm into the National Aeronautic and Space Administration's computer network as a means of protesting nuclear weapons. In addition to spreading, the worm displayed the message "Worms Against Nuclear Killers. Your System Has Been Officially WANKed. You talk of times of peace for all, and then prepare for war." The attack took place in late 1989, while anti-nuclear activists protested NASA's launch of the space shuttle carrying the Galileo probe on its initial leg to Jupiter, as Galileo's booster system was fueled with radioactive plutonium. The protestors failed to stop the launch, but the worm took a month to eradicate from NASA's computers, costing the space agency an estimated half million dollars in wasted time and resources (Denning, 1999, p. 281).

Cyber conflict took off with the introduction of the Web in the 1990's. Websites were not only handy targets to attack, but also visible to the public, making the attacks themselves more visible. In addition, activists could use websites to publicize forthcoming operations, distribute the tools and information needed to participate, and coordinate the actual attacks. Two general types of attack emerged and became commonplace: (i) defacements of websites with political and social messages, and (ii) Denial-of-Service (DoS) attacks--disrupting access to target websites, usually by flooding them with traffic.

One of the first web defacements was performed in 1996 to protest The Communications Decency Act (CDA), a controversial law later ruled unconstitutional by the US Supreme Court. Hackers replaced the US Department of Justice home page with a page that read "Department of Injustice" and included pornographic content censored by the act (Attrition, 1996). Another early defacement was performed by an international group of hackers opposed to nuclear weapons. Called Milw0rm, the group hacked the web site of India's Bhabha Atomic Research Center shortly after India's nuclear weapons tests in 1998, replacing the content with anti-nuclear messages and a picture of a mushroom cloud. The group of six hackers, whose ages ranged from 15 to 19, hailed from four countries: the United States, England, the Netherlands, and New Zealand (Denning, 2001).

Since then, web defacements have become common, and while most are performed for fun and bragging rights, many are motivated by social and political issues. Zone-h, which records and archives web defacements, reported that of the roughly 480,000 defacements recorded in 2007, approximately 31,000 (6.5%) were performed for political reasons and another 28,000 (5.8%) were performed as expressions of patriotism (Zone-h, 2008).

Hacktivists have also "defaced" media other than the Web. In 2007, for example, an art group called Ztohoven tampered with a TV broadcast in the Czech Republic, inserting a mushroom cloud in a landscape scene. A video clip of the transmission was posted to YouTube (Mutina, 2007).

Tactics Used by Hacktivists

The tactic of protesting an organization by flooding its website with traffic was pioneered by an international group of activists called Strano Network. On December 21, 1995, Strano Network organized a one-hour cyber attack against selected websites associated with the French government. At the appointed hour, participants from all over the world were instructed to access the target websites and rapidly hit the "reload" key over and over to clog

the sites with traffic. The objective of the DoS attack was to protest French government policies on nuclear and social issues by disrupting access to key government sites. Following the strike, a posting on the Internet proclaimed it had been effective in shutting off access to some of the sites and drawing media attention. The message also asserted that the strike showed "the existence of a world-wide movement able to counteract world-wide injustice; [and] the capacity to develop [such a] movement in a short time" (Denning, 1989, p.237; Schwartau, 1996, pp.406-408).

A few years later, a New York group called the Electronic Disturbance Theater (EDT) automated Strano Network's innovative method of cyber attack so that participants would not have to continually hit the reload key to generate traffic. Instead, they could visit EDT's website and click on a button signaling their desire to join the protest. Upon doing so, a software program named FloodNet would run on their computer and send a rapid and steady stream of packets with web page requests to the target site. This is sometimes called "HTTP flooding," as the page requests are issued with the web's HTTP protocol. Other Internet protocols have also been used to flood websites, including ICMP through "ping" requests ("ping flooding") and TCP through SYN requests ("SYN flooding").

EDT began using their tools in 1998 to support the Zapatistas in their struggle against the Mexican government. Their first attack, conducted on April 10, targeted Mexican President Zedillo's website, while their second hit US President Clinton's site (because of US support to Mexico). Their third strike was more ambitious, simultaneously targeting the websites of President Zedillo, the Pentagon (because the US military helped train Mexican soldiers carrying out human rights abuses), and the Frankfurt Stock Exchange (because it represented globalization--which EDT claimed was at the root of the problem). EDT estimated that 10,000 people participated in the attacks (Denning, 1999; Denning, 2001). Since then, EDT has sponsored numerous other attacks, which they refer to as "virtual sit-ins," to support a range of issues, including the war in Iraq, health care, and immigration. An attack conducted in collaboration with the borderlands Hacklab in March 2008 struck nanotech and biotech firms, because "their science is driven by the war (in Iraq) and drives the war" (EDT, 2008).

By 1999, the virtual sit-in had become a popular means of protest. That year, over 800 animal rights protestors used EDT's FloodNet software against websites in Sweden, while a British group calling itself the Electrohippies Collective developed its own tools and sponsored a massive sit-in against the website of the World Trade Organization during their meeting in Seattle (which also generated street demonstrations). The Electrohippies estimated that over 452,000 people worldwide joined their three-day strike (Cassel, 2000).

EDT's innovation, which took the form of a website with attack software, allowed thousands of people to join a strike with very little effort. All they needed to do was visit EDT's website and click a button. Mobilizing warriors had never been easier. But a later innovation, the "botnet," would give cyber warriors an even more powerful weapon. Instead of rounding up thousands of volunteers, a single warrior could compromise and take over thousands of computers on the Internet. This botnet, defined as a network of machines running robot-like malicious software (bots), would then be instructed to attack the target website in a robot-like fashion. The resulting attacks are often referred to as Distributed Denial-of-Service (DDoS) attacks, because of the distributed nature of the source of the attack. The term "swarming" is also used to denote the swarm-like fashion in which multiple agents (bots or people) simultaneously strike a common target (Arquilla & Ronfeldt, 2000). Most of the DoS attacks described in this chapter are of this nature.

The Electrohippies used their website to introduce another innovation in networked collaboration--collective decision making. During an

international week of protest against genetically-modified foods in 2000, visitors to their website could vote on whether the final phases of the campaign, which included a virtual sit-in, should go forward. When the final vote was only 42% in favor, with 29% opposed and 29% undecided, they cancelled the rest of the campaign. However, future actions did not include an opportunity to vote, so the Electrohippies may have decided that they had yielded too much power to site visitors, likely including curious onlookers and persons associated with the target.

Cyber activists also use email as a means of attack. In 1997, for example, protestors bombarded the web-hosting company IGC with a flood of email (sometimes called "email bombing"), demanding that IGC pull the site of the *Euskal Herria Journal* on the grounds it supported the Spanish-based terrorist group ETA. The protestors also clogged IGC's website with bogus credit card orders. The effect of the attacks severely impacted IGC's ability to service other customers, leading them to give way to the protestors' demands (Denning, 2001, p. 270).

In what some intelligence authorities characterized as the first known attack by terrorists against a country's computer systems, an offshoot of the Liberation Tigers of Tamil Eelam (LTTE) claimed responsibility for "suicide email bombings" against Sri Lankan embassies. Calling themselves the Internet Black Tigers, the group swamped Sri Lankan embassies with about 800 emails a day over a two-week period in 1998. The messages read, "We are the Internet Black Tigers and we're doing this to disrupt your communications" (Denning, 1999, p. 69).

During the early days of cyber activism in the late 1990s, someone created a Hacktivism email list for persons interested in hacking and activism. Following discussions on the list about "jamming up" the Echelon global surveillance system operated by the US, UK, Canada, Australia, and New Zealand, October 21, 1999, was named Jam Echelon Day. On that day, activists were to send out email messages filled with subversive keywords such as "revolt," causing the messages to be snagged by Echelon's filters—thereby clogging the system with useless intercept data. Word spread around the Internet and generated media attention. But when the day came, the Hacktivism list, along with various political email lists, were the recipients of massive amounts of the nonsense email, leading the news service ZDNet to characterize it as a "spam farce" (Knight, 1999).

The Church of Scientology: Key Target for Cyber Activists

The Church of Scientology has been the target of cyber activists for years, often in response to the Church's efforts to censor leaked information about itself. In January 2008, cyber activists stepped up their assaults, launching Project Chanology to "expel the church from the Internet" and "save people from Scientology by reversing the brainwashing." The project, growing to about 9,000 people, used a DDoS attack to cripple the Scientology website for two weeks. It also published on the Web censored materials and personal information about Church leaders (Fritz, 2008).

The activists behind Project Chanology took advantage of the Internet's relative anonymity by using Anonymous accounts. Other activists, most notably the founders of EDT and the Electrohippies, have operated in the open, revealing their true names and taking responsibility for their actions. However, whereas the relatively small leadership of these groups have disclosed their identities and even spoken at conferences, the thousands of participants in their cyber operations have not.

The Role of Lycos Europe

Another leadership core that revealed its identity was Lycos Europe, an email service provider launching a campaign against spammers in 2004. Participants in the Make Love, Not Spam campaign installed a special screen saver generating

a slow stream of traffic against websites used by spammers. The campaign claimed that 110,000 screensavers irritated 100,000 spam sites over a one-month period (Make Love Not Spam, 2004). It also generated negative publicity, as critics argued the participants were essentially spamming the spammers' websites.

Cautionary Note

Although this section has focused on activists deploying cyber attacks, it is important to emphasize that most activists *do not engage* in cyber attacks. Rather, they use the Internet to publish information about the issues, generate support, sponsor letter writing campaigns and petitions, and coordinate non-cyber activities such as meetings, marches, and street demonstrations.

ELECTRONIC JIHAD

Defined

Electronic jihad refers to cyber attacks conducted on behalf of al-Qa'ida and the global jihadist movement associated with it. This movement is held together largely through the Internet.

History of the Movement

The first appearance of an al-Qa'ida-associated hacker group occurred after the September 11, 2001, terrorist attacks, when GForce Pakistan announced the formation of the Al-Qaeda Alliance Online on a U.S. government website it defaced on October 17, 2001. Declaring that "Osama bin Laden is a holy fighter, and whatever he says makes sense," the group of Pakistani Muslim hackers posted a list of demands and warned that it planned to hit major U.S. military and British websites (McWilliams, 2001b). A subsequent message from the group announced that two other Pakistani hacking groups had joined the alliance: the Pakistan Hackerz Club and Anti India Crew. Collectively, the groups had already defaced hundreds of websites, often with political messages.

Although GForce expressed support for bin Laden, they distanced themselves from terrorism. In an October 27, 2001, defacement of a US military website, they proclaimed that they were "not a group of cyber terrorists." Condemning the attacks of September 11 and calling themselves "cyber crusaders," they wrote, "ALL we ask for is PEACE for everyone." This turned out to be one of their last recorded defacements. GForce Pakistan and all mention of the Al-Qaeda Alliance Online disappeared.

Other hackers, however, have emerged in their place, engaging in what is sometimes called "electronic jihad." Jihadist forums are used to distribute manuals and tools for hacking and to promote and coordinate cyber attacks, including a DoS attack against the Vatican website (triggered by Pope Benedict's comments about the Prophet Mohammad)--which mainly fizzled, and an "Electronic Battle of Guantanamo" attack against American stock exchanges and banks, canceled because the banks had been notified (Alshech, 2007; Gross & McMillan, 2006).

The al-Jinan forum has played a particularly active role, distributing a software tool called Electronic Jihad, used by hackers to participate in DoS attacks against target websites deemed harmful to Islam. The forum even gives awards to the most effective participants, where the objective is to "inflict maximum human, financial and morale damage on the enemy by using the Internet" (Bakier, 2007).

The al-Farouq forum has also promoted electronic jihad, offering a hacker library with information for disrupting and destroying enemy electronic resources. The library held keylogging software for capturing keystrokes and acquiring passwords on compromised computers, software tools for hiding or misrepresenting the hacker's Internet address, and disk and system utilities for erasing hard disks and incapacitating Windows-

based systems. Postings on the forum in 2005 called for heightened electronic attacks against US and allied government websites (Pool, 2005a). On another jihadist forum, a posting in October, 2008, invited youths to participate in an 'electronic jihadist campaign' against US military systems by joining the Tariq Bin-Ziyad Brigades. The recently-formed group was looking to increase its ranks so it could be more effective (OSC, 2008).

In a February, 2006, report, the Jamestown Foundation reported that "most radical jihadi forums devote an entire section to [hacker warfare]." The al-Ghorabaa site, for example, contained information on penetrating computer devices and intranet servers, stealing passwords, and security. It also contained an encyclopedia on hacking websites and a 344-page book on hacking techniques, including a step-by-step guide for "terminating pornographic sites and those intended for the Jews and their supporters" (Ulph, 2006). The forum Minbar ahl al-Sunna wal-Jama'a (The Pulpit of the People of the Sunna) offered a hacking manual said to be written in a pedagogical style and discussed motives and incentives for computer-based attacks, including political, strategic, economic, and individual. The manual discussed three types of attack: (i) direct intrusions into corporate and government networks, (ii) infiltration of personal computers to steal personal information, and (iii) interception of sensitive information, such as credit card numbers in transit (Pool, 2005b).

Younis Tsoulis, who went by the codename Irhabi (Terrorist) 007, also promoted hacking, publishing a 74-page manual "The Encyclopedia of Hacking the Zionist and Crusader Websites" with hacking instructions and a list of vulnerable websites on a website he managed (Jamestown, 2008). Tsoulis was later arrested and sentenced to ten years in prison for inciting terrorist murder on the Internet.

Triggering Events for Electronic Jihad

Electronic jihad, like other acts of cyber protest, is often triggered by particular events. Publication of the Danish cartoons satirizing the Prophet Mohammad, for example, sparked a rash of cyber attacks as violence erupted on the streets in early 2006. By late February, Zone-h had recorded almost 3,000 attacks against Danish websites. In addition, the al-Ghorabaa site coordinated a 24-hour cyber attack against *Jyllands-Posten*, the newspaper that first published the cartoons, and other newspaper sites (Ulph, 2006). A video purporting to document a DoS attack against the *Jyllands-Posten* website was later released on the jihadist site 3asfh.com. The video was in the style of jihadist videos coming out of Iraq, showing that the hackers were emulating the publicity tactics of violent jihadists (Internet Haganah, 2006).

Jihadists often target websites used to actively oppose them. For example, a message posted to a Yahoo! group attempted to recruit 600 Muslims for jihad cyber attacks against Internet Haganah's website. The motive was retaliation against Internet Haganah's efforts to close down terrorist-related websites by reporting them to their service providers. Muslim hackers were asked to register to a Yahoo! group called Jehad-Op (Reynalds, 2004). According to the Anti-Terrorism Coalition (ATC), the jihad was organized by a group named Osama Bin Laden (OBL) Crew, also threatening attacks against the ATC website (ATC, 2004).

The use of electronic jihad to support al-Qa'ida is explicitly promoted in a book by Mohammad Bin Ahmad As-Sālim titled *39 Ways to Serve and Participate in Jihâd*. Initially published on al-Qa'ida's al-Farouq website in 2003 (Leyden, 2003), principle 34 in the book discusses two forms of "electronic *Jihâd*:" (i) discussion boards (for media operations) and (ii) hacking methods, about which the book writes: "this is truly deserving of the term 'electronic *Jihâd*,' since the term carries the meaning of force; to strike and to attack. So,

whoever is given knowledge in this field, then he should not be stingy with it in regards to using it to serve the *Jihâd*. He should concentrate his efforts on destroying any American websites, as well as any sites that are anti-*Jihâd* and *Mujâhidîn*, Jewish websites, modernist and secular websites" (As-Sālim, 2003).

The Value of Inflicting Harm

Al-Qa'ida has long recognized the value of inflicting economic harm on the United States, and electronic jihad is seen as a tool for doing so. After the Electronic Battle of Gauntanomo was canceled, a message posted on an Islamist website stated how "disabling [sensitive economic American websites] for a few days or even for a few hours … will cause millions of dollars worth of damage" (Alshech, 2007). A message on al-Jinan noted that hacking methods could "inflict the greatest [possible] financial damage" on their enemies.

According to Fouad Husseing, economically-damaging cyber attacks are part of al-Qa'ida's long-term war against the United States. In his book, *al-Zarqawi-al-Qaeda's Second Generation*, Husseing describes al-Qa'ida's seven-phase war as revealed through interviews of the organization's top lieutenants. Phase 4, scheduled for the period 2010-2013, includes conducting cyberterrorism against the U.S. economy (Hall, 2005).

Although damages from cyber attacks attributed to al-Qa'ida and associated hackers so far has been minor compared to the damages from al-Qa'ida's violent acts of terror, Husseing's book and other writings suggest that al-Qa'ida may be thinking bigger. A posting in a jihadist forum advocated attacking all the computer networks around the world, including military and telecommunication networks, in order to 'bring about the total collapse of the West' (Alshech, 2007). Of course, the idea of shutting down every single network is utter fantasy, so vision by itself does not translate into a threat.

PATRIOTIC HACKING

Defined

Patriotic or nationalistic hacking refers to networks of citizens and expatriates engaging in cyber attacks to defend their mother country or country of ethnic origin. Typically, patriotic networks attack the websites and email accounts of countries whose actions have threatened or harmed the interests of their mother country.

The cyber attacks against Estonia in 2007, for example, were triggered by the physical relocation of a Soviet-era war memorial, while those against Georgia in 2008 accompanied a military confrontation with Russia. Cyberspace provides a venue whereby patriotic hackers can vent their outrage with little effort and little risk. They can be armchair warriors, safe behind their computers. Through their online social networks, they become part of a cyber force larger than themselves—a force with greater impact than they could have alone, and one that provides cover for their individual acts.

History of Patriotic Hackers

Chinese hackers were among the first to form social networks of patriotic hackers. Beginning with the 1998 riots in Jakarta, Indonesia, when Indonesians committed atrocities against the Chinese living among them, a loose network of Chinese hackers came together under a nationalistic banner. The network, which Scott Henderson (2007) calls the Red Hacker Alliance, and others have called the Honker Union of China, was formed from such hacking groups as the Green Army and China Eagle Union. After gathering on Internet Relay Chat (IRC) channels to set a course of action against Indonesia, the hackers formed the Chinese Hacker Emergency Conference Center and launched coordinated cyber attacks, including web defacements and DoS attacks against Indonesian

websites and government email boxes (Henderson, 2007, pp. 9-12).

According to Henderson (2007, p. 13), the Indonesian cyber attacks served as both the recruiting and training grounds for the alliance's next mission: attacks against US websites in retaliation for the accidental bombing of the Chinese Embassy in Belgrade during the 1999 Kosovo conflict. The Red Hacker Alliance published a manifesto expressing its patriotic mission and including quotes from Mao Zedong, such as "The country is our country; the people are our people; if we don't cry out, who will? If we don't do something, who will?" (Henderson, 2007, p. 14)

Following the embassy-related attacks, the Red Hacker Alliance engaged in a series of cyber attacks against foreign countries. These included attacks against Taiwan in 1999, following Taiwanese President Li Deng-Hui's advocacy for a "two-state-theory," and then in 2000, in conjunction with the Taiwanese elections. Attacks were also aimed at Japan in 2000, relating to Japan's handling of events concerning the Nanjing Massacre during WWII; in 2004, attacks were related to the disputed Diaoyu Islands; and in 2001, attacks were related to the US, following the collision of a US EP-3 reconnaissance plane with a Chinese F-8 fighter jet in late April, 2001, resulting in the fighter pilot's death and China's detaining the US aircrew after an emergency landing (Henderson, 2007).

Most of the attacks became two-sided cyber skirmishes, with hackers from both sides attacking targets associated with the other. Indeed, the 2001 strikes against the US may have been triggered as much by defacements of Chinese web sites in April, 2001, by a hacker perceived to be from the US--as by the spy plane incident itself. All in all, the incidents looked more like the acts of youthful hackers showing off their skills and expressing outrage than state-sponsored activity. Indeed, in 2002, the Chinese government asked their hackers to refrain from further attacks, as the anniversary of the 2001 attacks drew near (Hess, 2002).

By the time the 2001 spy plane incident had died down, the Red Hacker Alliance had grown to an estimated 50,000 to 60,000 members. But most of the members knew little about computer networks and hacking. The attacks were characterized as a "chicken-scratch game of a group of children," "a farcical 'patriotic show'," and the work of "Red Hackers who were totally clueless in terms of technology" (Henderson, 2007, pp. 44-45).

A network of patriotic US hackers also emerged over the spy plane incident. According to iDefense (2001b, p. 40), a coalition of hackers calling itself Project China formed and began defacing Chinese websites on May 1, 2001. The alliance was formed from several prominent hacking groups, including Hackweiser and World of Hell.

After the September 11, 2001, terrorist attacks and invasion of Afghanistan, the network of US hackers regrouped to avenge the attacks. Now called the Dispatchers, the patriotic hackers defaced several hundred websites associated with governments in the Middle East and Palestinian Internet service providers, and planned to hit targets in Afghanistan. Founded by Hackah Jak, a 21-year-old security expert from Ohio and former member of Hackweiser and Project China, the group of 60 hackers included members of World of Hell and even some non-US hackers (Graham, 2001; Peterson, 2001). The group seemed to quietly disappear, however, following appeals from industry leaders to refrain from hacking and the group's defacement of a website belonging to a company having offices in the World Trade Center (WTC) and losing employees on September 11, 2001 (Graham, 2001).

Another group of hackers going by the name "Young Intelligent Hackers Against Terrorism" (YIHAT) also surfaced after the September 11, 2001, attacks. Their objective was to disrupt al-Qa'ida's financial resources. However, claims that the group had penetrated bank accounts associated with Osama bin Laden and al-Qa'ida were unsubstantiated, and the group's website

disappeared following cyber skirmishes with other hacking groups, most notably GForce Pakistan, the group of Pakistani hackers mentioned earlier in conjunction with their post September 11, 2001, web defacements and announcement of the Al Qaeda Alliance Online (McWilliams, 2001a, 2001c).

The Lack of U.S. Patriotic Hackers Post-2001

Since 2001, the United States has not seen a large and active network of patriotic hackers, perhaps because there has not been an international conflict or incident that has seriously threatened the US, or perhaps because Americans are simply not as nationalistic as the Chinese are. During the Iraq war (began in 2003), most of the cyber attacks originated with social activists and foreign hackers from China and elsewhere opposed to the war; however, there were not patriotic US hackers supporting it.

The Emergence of Patriotic Hackers in Other Countries

Patriotic hackers have emerged in other countries and regions, however. Pakistani and Indian hackers have been defacing each other's websites since the late 1990s over Kashmir and, more recently, in 2008 over the Mumbai terrorist attacks. In the early days, the Pakistan Hackerz Club (PHC), one of the other groups forming the Al Qaeda Alliance Online, was among the most prolific web defacement groups worldwide (Christenson, 1999). Armenian and Azerbaijani hackers similarly went after each other's websites in 2000 over the fighting in Nagorno-Karabakh, an ethnic Armenian enclave in Azerbaijan (Williams, 2000).

Israeli and Palestinian/Muslim hackers launched cyber attacks after the second intifada, or uprising, erupted in the Palestinian territories in late September, 2000, following a visit by Ariel Sharon to the Temple Mount and the murder of three Israeli soldiers. Hackers on both sides defaced each other's websites and launched DoS attacks.

By January 2001, over 40 hacker groups/individuals from 23 countries had hit the websites of eight governments, as well as numerous commercial sites, according to iDefense (2001a). Both GForce and PHC joined the loosely-formed network of Muslim hackers defacing Israeli sites. One defacement read: "GForce Declares a War against Israel?…. Ok, GForce Pakistan is back. We really planned not to come back to the defacing scene again, but once again our Muslim brothers needed us" (iDefense, 2001a).

A Cautionary Note

It is important to note that the cyber intifada illustrates that there is no hard line between electronic jihad and patriotic hacking. The attacks can be viewed both as electronic jihad by Muslim hackers against Israel and as patriotic hacking by Israeli and Palestinian hackers (and their external supporters) against each other. In addition, there is no hard line between jihadist and patriotic hacker networks. Groups such as GForce and PHC have used their skills to support the jihad as well as their own countries and other Muslim countries and territories.

Following the 2000 cyber intifada, hackers aligned with Israel or the Palestinians have engaged in repeated cyber skirmishes, often in conjunction with incidents taking place on the ground. Within 48 hours of Israel's bombing of Gaza in December, 2008, more than 300 Israeli websites had been defaced with anti-Israel (and anti-US) messages (Higgins, 2008). The hackers came from several countries, including Morocco, Syria, and Iran. Team Evil, a group of Moroccan hackers with a history of attacking Israeli websites, took over an Israeli domain name server and redirected Ynet's English news site and other websites to phony web pages condemning the Israeli strikes (Paz, 2009). For their part, an Israeli alliance called "Help Israel Win" developed and

distributed a software tool for conducting DDoS attacks against Hamas-friendly sites like qudsnews.net and Palestine-info.info. According to the group, more than 8,000 people had downloaded and installed the Patriot software. With websites in Hebrew, English, Spanish, French, Russian and Portugese, the alliance claims to unite "the computer capabilities of many people around the world" (Shachtman, 2009).

The cyber attacks against Estonia in April/May, 2007, and in Georgia in August, 2008, put Russian hackers on the front page of news sites. However, patriotic Russians have engaged in cyber attacks since at least 1999, when the Russian Hackers Union defaced a US military website during the Kosovo war with anti-NATO messages. But with the Estonian attacks, the level of activity dramatically increased. Just before the 2008 Georgian cyber assault, Russian hackers attacked Lithuanian websites to protest a new law banning the display of Soviet emblems. They also issued a manifesto called "Hackers United Against External Threats to Russia," calling for a expansion of targets to include Ukraine, the rest of the Baltic states, and "flagrant" Western nations supporting the expansion of NATO (Krebs, 2008). Then, in January, 2009, the Russian hackers knocked Kyrgyzstan off the Internet (Keizer, 2009).

The Estonian and Georgian cyber assaults leveraged large social networks, as well as huge botnets of compromised computers scattered all over the world, mostly for DoS and DDoS attacks (Davis, 2007; Naraine & Danchev, 2008). Postings on Russian-language forums exhorted readers to defend the motherland and provided attack scripts to follow and target websites. The scripts, flooding targets with network traffic, allowed participants to join a loose network of cyber warriors knowing little or nothing about hacking. During the Georgian attacks, the Russian website stopgeorgia.ru offered several DoS tools and a list of 36 targets. According to one report, the site traced back to the Russian Business Network (RBN), a cybercrime network based in St. Petersburg, Russia (Georgia Update, 2008).

Psychological Analysis and Other Reasons for Patriotic Hacking

Rosanna Guadagno, Robert Cialdini, and Gadi Evron (2009) offer an interesting social- psychological analysis of the Estonian conflict. They posit that several factors contributed to the assault, including: (i) the loss of status of Estonia's ethnic Russian minority, following the collapse of the Soviet Union and Estonia gaining independence; (ii) the anonymity and resulting sense of depersonalization coming from online interaction; (iii) group membership and adherence to group norms; and (iv) rapid contagion through online forums. Because most Russian-language Internet users were participating in or endorsing the attacks, such behavior became normative and quickly spread.

Despite the ability of non-state actors to inflict considerable damage in cyberspace, many analysts see a government hand in nationalistic cyber attacks, for example, attributing the attacks against Estonia and Georgia to the Russian government. Stephen Blank (2008) of the US Army War College, for example, writes that "the computer attacks … and the other steps taken by Moscow against Estonia were acts sanctioned by high policy and reflected a coordinated strategy devised in advance of the removal of the Bronze Soldier from its original pedestal."

At the same time, there are good reasons to believe that the attacks were primarily, if not entirely, the work of non-state actors. First, some of the attacks have been traced to independent persons and to websites operated and frequented by independent persons. Second, non-state actors are capable of pulling off large-scale attacks such as these on their own. They do not need government resources, including funding. The attacks are cheap, and hackers outside the government have the tools and knowledge to launch them. Third, while the tactics used—including web deface-

ments, web flooding, and botnets of compromised computer—are regularly used by non-state actors, there are good reasons why states would not engage in such attacks. They typically violate domestic crime statutes and cause considerable collateral damage, thereby, also violating law of war principles, such as necessity and proportionality. Fourth, states have other means of dealing with conflict; for example, diplomacy, sanctions, and military operations. Cyber attacks might be deployed as part of military operations, but they would more likely be precision strikes against military targets used for command and control, reconnaissance, and communications rather than mass attacks against civilian websites. However, it is possible that the Russian government played some role in the attacks, for example, by encouraging or condoning them.

Even when attacks can be traced to government computers, it would be presumptuous to conclude that they were launched by the state. The computers may have been compromised by hackers of any nationality. Even if individuals within the government were responsible for the attacks, they may have been operating on their own, not as agents of their government or under direction from their government. About 7.4% of the participants in a cyber attack against the Mexican Embassy's London website in June, 1999, for example, apparently had ".mil" addresses; that is, addresses assigned to the US Department of Defense. However, the attacks were not conducted by the Department of Defence. They were conducted by the Electronic Disturbance Theater (discussed earlier), having a history of attacking the websites of the US and Mexican governments, including the Department of Defence websites. The ".mil" participants likely visited the EDT website used to generate the attacks, becoming unwitting participants.

One participant in the Estonian attacks, Konstantin Goloskokov, was a commissar of the pro-Kremlin youth movement Nashi, but he said that he and a few friends had operated on their own initiative and not under the direction of the Russian government (Clover, 2009).

At least so far, non-state actors appear to be responsible for most cyber conflict, taking advantage of this new medium to conduct rapid, large-scale attacks at low cost.

CONCLUSION

Cyber conflict, at least so far, is predominantly a non-state activity. Networks of civilian cyber warriors come together to hack for a cause. Typically, the networks center around social activism (hacktivism), jihad (electronic jihad), or nationalism (patriotic hacking). Tools and tactics are adopted from those used by other hackers, while online forums provide the principal means of organization and support.

Although cyber attacks launched by non-state networks have been highly disruptive, they have not been lethal or even destructive. Nobody has died, and following an attack, services and data are restored. The attacks look more like the cyber-equivalent of street demonstrations than terrorism or warfare, though even street protests sometimes become destructive and deadly. When Estonia relocated its memorial, for example, riots broke out not only in cyberspace, but also on the streets, the latter leading to one death and 150 injuries (Fritz, 2008, p. 33). Similarly, the street violence that erupted over the Danish cartoons left 139 dead and 823 injured (Cartoon, 2006).

However, even if cyber conflict has not been particularly destructive, some of the attacks have inflicted substantial financial costs on their targets, owing to the disruption of services and the need to devote resources to defense and recovery. One Estonian bank targeted during the cyber assault was said to have lost at least $1 million (Landler & Markoff, 2007).

Whether cyber conflict will evolve to something more destructive is difficult to predict. Clearly, some jihadists would like to cause greater

harm, though they currently lack the knowledge and skills to do so. Other non-state actors may also turn to more destructive cyber attacks, just as they turn to terrorism, insurgency, and other forms of physical violence.

Many critical infrastructures are vulnerable to cyber attacks that could be quite destructive, even deadly. Already, cyber attacks have caused raw sewage overflows, disabled emergency 911 services, and disrupted health care in hospitals. In addition, security researchers have demonstrated how cyber attacks could physically destroy electrical power generators (Meserve, 2007). Thus, in the presence of both motivated actors and vulnerable systems, cyber terrorism could morph from the largely theoretical threat it is today to something all too real.

Still, most activists are more interested in raising awareness about an issue and pressing for change rather than inflicting serious harm. For them, cyber conflict will retain its characteristic of being primarily disruptive. Exact tactics, however, will change as technology evolves and hacking along with it.

REFERENCES

Almeida, M. (2008). *Statistics report 2005-2007, March 5, 2008*. Retrieved March 18, 2008, from www.zone-h.org

Alshech, E. (2007). Cyberspace as a combat zone: The phenomenon of electronic jihad. *MEMRI Inquiry and Analysis Series, 329*. The Middle East Media Research Institute, February 7.

Arguilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*, 141–165. doi:10.1080/01495939308402915

Arquilla, J., & Ronfeldt, D. (2000). *Swarming & the future of conflict*. Santa Monica, CA: RAND.

As-Sālim, M. (2003) *39 Ways to serve and participate in jihâd*. Retrieved June 30, 2008, from http://tibyan.wordpress.com/2007/08/24/39-ways-to-serve-and-participate-in-jihad/.

ATC. (2004). *ATC's OBL crew investigation*. Anti-TerrorismCoalition.

Attrition. (1996). *Attrition mirror*. Retrieved 1996 from http://attrition.org/mirror/attrition/1996.html#dec

Bakier, A. H. (2007). *Forum users improve electronic jihad technology*. Retrieved June 27, 2007, from http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=4256

Blank, S. (2008). Web war I: Is Europe's first information war a new kind of war? *Comparative Strategy*, *27*, 227–247. doi:10.1080/01495930802185312

Cartoon. (2006). *Cartoon body count*. Retrieved April 21, 2009, from http://web.archive.org/web/20060326071135/http://www.cartoonbodycount.com/

Cassell, D. (2000). *Hacktivism in the cyberstreets*. Retrieved May 30, 2000, from http://www.alternet.org/story/9223

Clover, C. (2009). Kremlin-backed group behind Estonia cyber blitz. *Financial Times (North American Edition)*, (March): 11.

CSI. (1998). Email attack on Sri Lanka computers. *Computer Security Alert*, *183*, 8.

Davis, J. (2007). *Web war one*. Retrieved September, 2007, from http://www.wired.com/images/press/pdf/webwarone.pdf

Denning, D. E. (1999). *Information warfare and security*. Reading, MA: Addison-Wesley.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism . In Arquilla, J., & Ronfeldt, D. (Eds.), *Networks and netwars* (pp. 239–288). Santa Monica, CA: RAND.

Drogin, B. (1999). *Russians seem to be hacking into Pentagon*. Retrieved October 7, 1999, from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/1999/10/07/MN58558.DTL

EDT. (2008). *EDT*. Retrieved December 17, 2008, from http://www.thing.net/~rdom/ecd/ecd.html

Electrohippies (2009). *The electrohippies call on people around the globe to celebrate World Intellectual Privateers Day 2009*. Retrieved April 13, 2009, from http://www.fraw.org.uk/ehippies

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala, 8*(1), 28-80. Retrieved 2008 from http://epublications.bond.edu.au/cm/vol8/iss1/2/

Georgia Update. (2008). *Russian invasion of Georgia*. Retrieved October 9, 2008, from www.georgiaupdate.gov.ge

Graham, J. (2001). *Hackers strike Middle Eastern sites*. Retrieved September 26, 2001, from http://www.usatoday.com/tech/news/2001/09/19/hack-attack-launched.htm

Gross, G., & McMillan, R. (2006). Al-*Qaeda 'Battle of Guantanamo' cyberattack a no-show.* Retrieved December 1, 2006, from http://hostera.ridne.net/suspended.page/?currtag=12&currletter=2

Guadagno, R. E., Cialdini, R. B., & Evron, G. (2009). (in press). What about Estonia? A social psychological analysis of the first Internet war. *Cyberpsychology & Behavior*.

Hall, A. (2005). *Al-Qaeda chiefs reveal world domination design*. Retrieved August 24, 2005, from http://www.theage.com.au/news/war-on-terror/alqaeda-chiefs-reveal-world-domination-design/2005/08/23/1124562861654.html

Henderson, S. J. (2007). *The dark visitor: Inside the world of Chinese hackers*. Fort Leavenworth, KS: Foreign Military Studies Office.

Hess, P. (2002). *China prevented repeat cyber attack on US*. Retrieved October 29, 2002, from http://seclists.org/isn/2002/Oct/121

Higgins, K. J. (2008). *Hundreds of Israeli websites hacked in 'propaganda war*.' Retrieved December 31, 2008, from http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212700313

iDefense. (2001a). *Israeli-Palestinian cyber conflict*. Fairfax, VA: Intelligence Services Report.

iDefense. (2001b). *US-China cyber skirmish of April-May 2001*. Fairfax, VA: Intelligence Operations Whitepaper.

Internet Haganah. (2006). *How the brothers attacked the website of Jyllands-Posten*. February 7. Retrieved October 21, 2008, from http://internet-haganah.com/harchives/005456.html

Jamestown. (2008). *Hacking manual by jailed jihadi appears on web*. Retrieved March 5, 2008, from http://www.jamestown.org/programs/gta/single/?tx_ttnews%5Btt_news%5D=4763&tx_ttnews%5BbackPid%5D=246&no_cache=1

Keizer, G. (2009). *Russian 'cybermilitia' knocks Kyrgyzstan offline*. Retrieved January 28, 2009, from http://www.computerworld.com/s/article/9126947/Russian_cybermilitia_knocks_Kyrgyzstan_offline

Knight, W. (1999). *Jam Echelon day descends into spam farce*. Retrieved October 22, 1999, from http://news.zdnet.co.uk/emerging-tech/0,1000000183,2074601,00.htm

Krebs, B. (2008). *Lithuania weathers cyber attack, braces for round 2*. Retrieved July 29, 2008, from http://voices.washingtonpost.com/security-fix/2008/07/lithuania_weathers_cyber_attac_1.html

Landler, M., & Markoff, J. (2007). *Digital fears emerge after data siege in Estonia. RetrievedMay29, 2007*, from http://www.nytimes.com/2007/05/29/technology/29estonia.html

Leyden, J. (2003). *Al-Qaeda: The 39 principles of holy war*. Retrieved September 4, 2003, from http://www.israelnewsagency.com/Al-Qaeda.html

Make Love Not Spam. (2004). *Make Love Not Spam*. Retrieved April 3, 2009, from http://www.makelovenotspam.com/

McWilliams, B. (2001a). *Anti-terror hackers seek government blessing*. Retrieved October 17, 2001, from http://www.infowar.com/hacker/01/hack_101701b_j.shtml

McWilliams, B. (2001b). *Pakistani hackers deface US site with ultimatum*. Retrieved October 17, 2001, from http://lists.jammed.com/ISN/2001/10/0158.html

McWilliams, B. (2001c). *Pro-USA hackers target Pakistani defacement group*. Retrieved December 22, 2009, from http://faculty.vassar.edu/lenevare/91101/

Meserve, J. (2007). *Staged cyber attack reveals vulnerability in power grid*. Retrieved April 22, 2009, from http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

Mutina, B. (2007). *Hacking incident goes on Czech TV*. Retrieved June 19, 2007, to www.zone-h.org

Naraine, R., & Danchev, D. (2008). *Zero Day: Coordinated Russia vs Georgia cyber attack in progress*. Retrieved August 11, 2008, from http://blogs.zdnet.com/security/?p=1670

Onley, D. S., & Wait, P. (2006). *Red storm rising*. Retrieved August 21, 2006, from http://www.gcn.com/Articles/2006/08/17/Red-storm-rising.aspx

OSC. (2008). *Jihadist forum invites youths to join 'electronic jihadist campaign*.' Open Source Center, October 6, 2008.

Parker, D. B. (1976). *Crime by computer*. New York: Scribner.

Paz, S. (2009). *Anti-Israel group wreaks havoc with Israeli web sites*. Retrieved January 4, 2009, from http://www.jpost.com/servlet/Satellite?cid=1230733155647&pagename=JPArticle%2FShowFull

Peterson, S. (2001). *Crackers prepare retaliation for terrorist attack*. Retrieved December 22, 2009, from http://www.gyre.org/news/explore/hacktivism?page=1

Pool, J. (2005a). *New web forum postings call for intensified electronic jihad against government websites*. Retrieved December 22, 2009, from http://www.itac-ciem.gc.ca/pblctns/tc_prsnts/2006-2-eng.asp

Pool, J. (2005b). *Technology and security discussions on the jihadist forums*. Retrieved December 22, 2009, from http://www.comw.org/tct/terror-infowar.html

Reynalds, J. (2004). *Internet 'terrorist' using Yahoo to recruit 600 Muslims for hack attack.* Retrieved October 21, 2008, from http://www.mensnewsdaily.com/archive/r/reynalds/04/reynalds022804.htm

Schachtman, N. (2009). *Wage cyberwar against Hamas, surrender your PC*. Retrieved January 8, 2009, from http://www.wired.com/dangerroom/2009/01/israel-dns-hack/

Schwartau, W. (1996). *Information warfare* (2nd ed.). New York: Thunder's Mouth Press.

Ulph, S. (2006). *Internet mujahideen refine electronic warfare tactics*. Retrieved December 22, 2009, from http://www.jamestown.org/programs/gta/single/?tx_ttnews%5Btt_news%5D=666&tx_ttnews%5BbackPid%5D=239&no_cache=1

Vatis, M. (2001). Cyber terrorism and information warfare: Government perspectives . In Alexander, Y., & Swetnam, M. S. (Eds.), *Cyber terrorism and information warfare. Ardsley: Transnational Publishers, Inc*.

William, S. (2000). *Armenian and Azerbaijani hackers wage war on Internet*. Retrieved February 17, 2000, from http://www.hrea.org/lists/huridocs-tech/markup/msg00417.html