State-Sponsored Intrusion

And

Cyber-Terrorism

David J. Swicegood

SANS Track 1 (GSEC) Practical V1.4b

Option 1

Submitted June 22, 2004

EXECUTIVE SUMMARY

This study defends the thesis that despite some experts' opinions, Cyber-Terrorism and state-sponsored hacking not only exist, but the U.S. has the most to lose from these types of attacks. The forensics involved in tracing an attack and using evidence to prosecute offenders proves fruitless in both cases due to lack of ability to establish and enforce law across many national boundaries. This study lists several vulnerabilities and references several U.S. officials who acknowledge the vulnerabilities in our infrastructure and global prosecution, and have been instrumental in getting Congress and private industry to increase their concern and action. The study then discusses several real and potential threats. The study does address criticisms of the "Cyber-terrorism" concept, and flaws in the logic of those criticisms are highlighted. Finally, the study briefly discusses the future of both threat and mitigation to show the direction the argument is taking in the months to come.

Major Findings:

- National Security Advisor, Condoleeza Rice, has labeled the U.S. dependence on IT as our "Achilles' Heel" and "soft underbelly."
- Critical infrastructures have been hacked in the recent past-many attacks will never be discussed due to national security concerns.
- Terrorist organizations have an increasing membership of technologically savvy operatives that use hacking to supply/finance their physical attacks and to spread terror through cyber-attacks.
- Foreign governments have and are training operatives in information warfare and hacking.
- Current forensic practices are still developing in their sophistication in tracking attackers, and regulations and laws that transcend borders (like the Internet does) are even further behind in development.

“Electronic espionage”, “cyber terrorism”, and “information warfare” are just a few of the terms that label some organized threats that exist, and many of their perpetrators or threat agents consider the United States their main target. The FBI and other organizations are heavily engaged in investigation and prosecution of cyber criminals residing in and outside of the U.S.(Dick, 2001). It is well known, however, that countries outside the United States have different levels of interest in preventing cyber crime. Enforcement of unauthorized intrusion and even electronic extortion and robbery varies. To best illustrate this concept, figure 1 represents a spectrum of different levels of interest or participation in enforcing anti-intrusion laws. On one end, there are countries that have laws pertaining to illegal electronic intrusions and the ability to trace, catch, and prosecute intruders. In the middle are the countries that don’t have such capabilities, yet cooperate with more capable countries through apprehension and extradition of such criminals. On the far end, there are countries that fund and train intruders to pursue cyber targets world-wide.

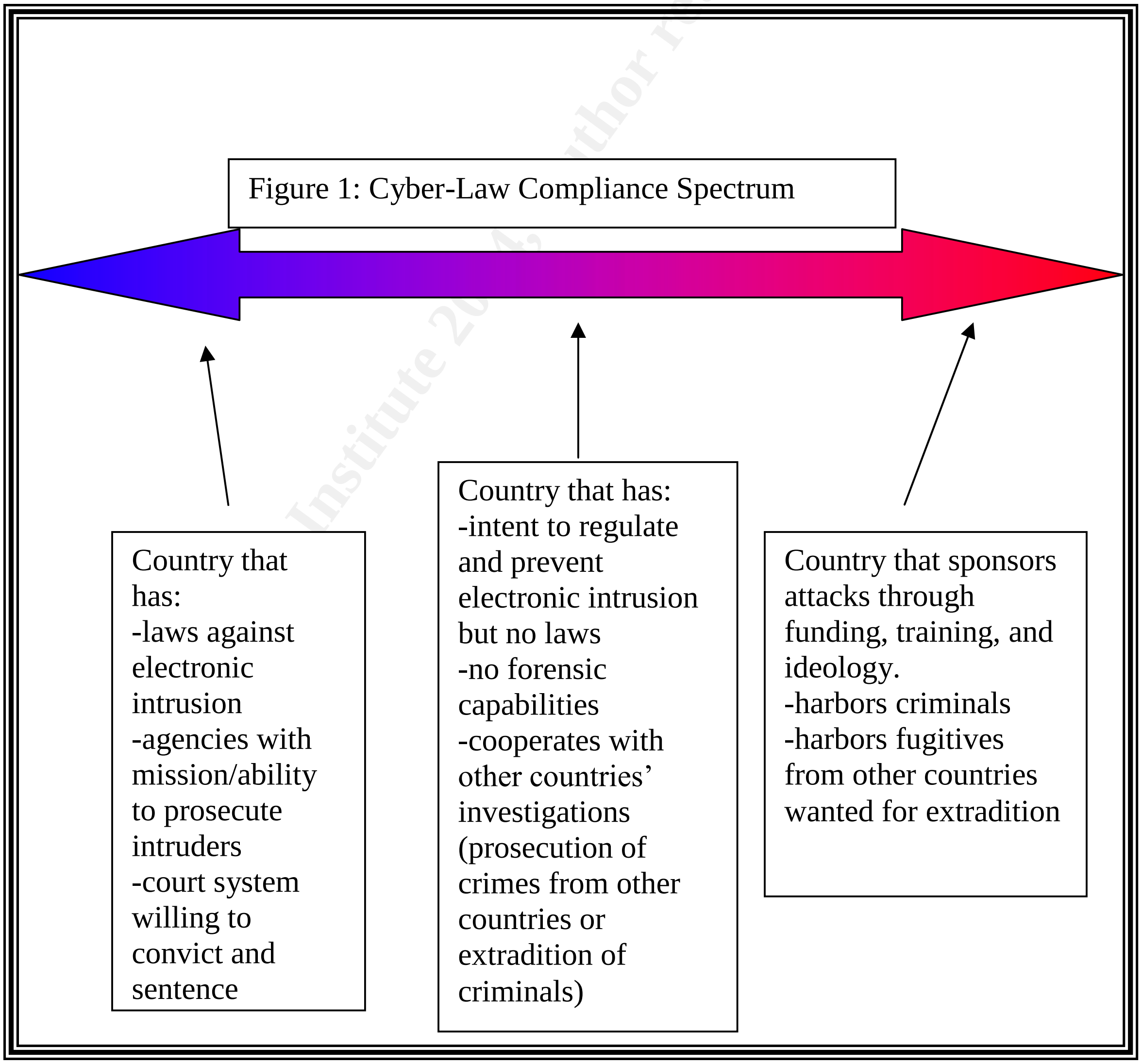

Figure 1: Cyber-Law Compliance Spectrum

Country that has:
-laws against electronic intrusion
-agencies with mission/ability to prosecute intruders
-court system willing to convict and sentence

Country that has:
-intent to regulate and prevent electronic intrusion but no laws
-no forensic capabilities
-cooperates with other countries’ investigations (prosecution of crimes from other countries or extradition of criminals)

Country that sponsors attacks through funding, training, and ideology.
-harbors criminals
-harbors fugitives from other countries wanted for extradition

While some security experts disagree on the presence of such threats and the historical evidence of their impact on security, many see organized and state-sponsored threat agents as being behind recent attacks and, at a minimum, the future wave of the security focus. This paper argues that the potential for state-sponsored crackers and cyber terrorists to exist far outweighs the evidence that states the contrary, and furthermore, establishes the case for hardening against such attacks.

VULNERABILITIES:

In a speech given by the National Security Advisor, Condoleezza Rice, in March of 2001, she explained the significance of the relationship between Information Technology security and the entire U.S. infrastructure. She states, “Virtually every vital service—water supply, transportation, energy, banking and finance, telecommunications, public health—all of these rely upon computers and fiber optic lines, switches and the routers that connect them. Corrupt those networks and you disrupt this nation” (Poulson, 2001). While many of the technicalities of specific vulnerabilities are classified secrets, it doesn’t take much imagination to understand targets of possible attack and the repercussions for such attacks. Attackers can disrupt infrastructure while stealing money to finance other attacks both in and out of the cyber world. In their book, *Hack I.T.*, Klevinsky, Laliberte, and Gupta state that an attacker can steal information such as U.S. deployed troop movements, source code for military software products, medical records, bank account information, and credit card numbers. Attackers can also gain access to systems that allow them to turn off phone systems and raise or lower temperature in important buildings(2002). National Security Advisor, Condoleeza Rice, has labeled the U.S. dependence on IT as our “Achilles’ Heel” and “soft underbelly” (Poulson, 2001). Another description of U.S. vulnerability is described in a report entitled, “Cyber Terrorism or Cyber Crime?” by Deborah H. Juhnke. She writes, “The United States Government has identified several major systems at risk from cyber terrorism and cyber crime. These are: corporate, utilities, transportation, financial, defense, government, space, telecommunications and academics. Disruption of any of these systems would have a significant impact on our economic and/or physical well-being” (2002).

In a SANS study entitled, “Can Hackers Turn Your Lights Off?” (2001), the author states that intruders hacked into a NASA/JPL computer that had FAA information about the configuration of GPS satellites, stealth aircraft operating procedures and locations, and general safety of flight information that shut down communications for several flights. The study specifically states that an honest assessment of our nation’s power grid showed vulnerabilities that Energy Department spokesmen wouldn’t comment on. The author lists specific areas of the Control Center, Substations, and Communications Infrastructure that need hardening. Furthermore, while the Energy Department officially denies the history of ever being hacked, researchers have confirmed that hackers have attacked IT systems in electric utilities and retrieved credit card information, and a radical environmental group was caught hacking in to a electrical IT system at an undisclosed U.S. location(SANS, 2001). During the rolling blackouts of 2001 in California, hackers had gained access to computers at the headquarters for the California Independent Systems Operators (Cal-ISO). For 17 days the attackers worked on gaining what an LA Times source familiar with the attack called "close to a catastrophic breach" (SANS, 2001). While Cal-ISO spokespersons deny the attack had anything to do with the disruption of power that affected almost half of a million residents at any one time, the SANS study calls the denial into doubt.

Vulnerabilities also lie in the defense sector. Intrusions and attacks against the military can not only compromise sensitive information and secrets that affect national security, many weapons and equipment used in the military depend on high-tech computer networks and software products. Intrusions into these systems and malicious code written in this software would not only have devastating consequences, but the true causes, sources, and incident may never reach public knowledge. For security reasons, if this has happened or is happening, the public and many in the military would not be informed. A March 2003 article in Eweek news, however, did report that a web server belonging to the U.S. Army was compromised at least two separate times recently due to vulnerabilities in Microsoft Windows programming that are both well known and extensively used throughout the military (Fisher, 2003).

THREATS:

In a report entitled, "Current and Emerging Threats to Information Technology Systems and Critical Infrastructures" the president of the Terrorism Research Center, Inc., Matthew Devost, states several reasons why cyber terrorism attacks should be viewed as an emerging threat. One of his reasons include the make up of young, technically savvy newcomers that form the current and upcoming generation of terrorist organization members. While there is evidence that young members of terrorist cells have the know-how and motive to launch cyber attacks, it is not clear if their intent is to use their skills to acquire weapons and logistics for physical attacks, or whether they are training for a cyber attack. A second reason that Devost gives for the emergence of cyber terrorism is that travel constraints and the "hardening" of the airline security procedures have made hijacking, border crossing, and escape flights more difficult to achieve; cyber terrorism, however, allows for continued action against enemy targets during periods of heightened travel security.

Supporting Devost's statement that young members of terrorist cells are bringing high tech skills with them as they join is one report in the Baltimore Sun from October 2001. The report, which references a presidential commission, reports that a global army with hacking skills numbers 19 million worldwide who could "reek havoc from a keyboard thousands of miles away"(Shane, 2003). One organized group with a following that makes up part of this "army" runs a popular website named, The Muslim Hackers Club. This site reportedly contains destructive information about Pentagon IT vulnerabilities, Secret Service codewords and frequencies, and other anti-US propaganda(Shane, 2003). According to an Infowar.com article (1998), members of the Muslim Hackers Club include two men who work as spokesmen for Osama bin Laden. One of the men, named Batuta, is the computer expert and web site organizer of the group. Infowar claims it has a reporter that is close to the group who has inside information about the strict requirements for membership, methods of communication, and other methods of operation. Apparently, the group communicates in "the clear" about hacking and virus ideas, and in PGP-encrypted format about organized operations to an exclusive email list. Reportedly, the Muslim Hacker Club is run out of England and has followings primarily in the U.S., U.K., Pakistan, and Malaysia. There was at the time of the article, actual computer training camps in Afghanistan and Pakistan[1]. Whether the club actually is able to cause any substantial damage is debatable, but the fact remains that there exists motive, possibly capability, and certainly enough vulnerability. With a secret membership such as the one at the Muslim Hackers Club, an organized attack could take on the resemblance of an attack being conducted by rogue individuals. Aside from goals of disruption and denial of service, stealing credit card numbers, blackmailing corporations for large sums of cash, and the stealing of other logistical items by diverting shipments could serve to supply necessities and funding to terrorist groups planning physical attacks against U.S. interests. The proliferation of those in the Middle East with Anti-American sentiments is no secret. Due to much of the politics involved with trade and diplomatic relationship building/military alliances many of the details and even reports of organized attacks from that region are shrouded in secrecy. Tom Talleur was chief of NASA's cyber crime unit in 1998. He states that during that time, hackers accessed the NASA/JPL computer[2]. He was able to trace the hackers back to what in public has only been referred to as "an undisclosed location in the Persian Gulf region" (SANS 2001).

It is difficult not to wonder about the motives of many university IT students from inside and outside the U.S. who sympathize with groups that the U.S. government has labeled as terrorist organizations. Just last year, a software engineer in the U.S. pled guilty and turned states witness against the rest of his group who prepared, and somewhat executed a plan to travel through various countries to fight with the Taliban against U.S. and allied troops in Afghanistan(CNN 2003). How difficult would it be to assume that this software engineer had the motive, capability, and perhaps did corrupt software or write malicious code that could fulfill his political agenda that he was willing to fight and die for?

[1] The source at Infowar is reportedly close enough to the Muslim Hacker Club to identify a fictitious email alert about a coordinated cyber attack that made many headlines and caused several warnings in 1998. The Infowar article discusses the Method of Operations in enough detail to lend credibility without compromising the group or the informant's security.
[2] The attack was referenced earlier in this paper also.

In April of 2002, a report by the Newsfactor Network references a CIA report that states that the Chinese military is researching ways to disrupt targeted military and civilian computer infrastructure systems using virus attacks (Lyman 2002). In 2001, The CIA listed China and Russia as countries known to be actively training cyber soldiers. In an address to a Senate subcommittee, Richard Clark, then President Bush's cyber security advisor, later added Iran, Iraq, and North Korea to this list (McDonald, 2002). Furthermore, the director of the CIA acknowledged in Congressional testimony that over 100 nations are currently developing information warfare programs (Devost 2003).
Below is an excerpt from a speech given by the former director of the FBI to the U.S. Senate in 2001 that officially confirms the existence of state-sponsored hackers and cyber terrorists:

> *We believe that foreign intelligence services have adapted to using cyber tools as part of their information gathering tradecraft. While I cannot go into specific cases, there are overseas probes against the U.S. government systems everyday. It would be naïve to ignore the possibility or even probability that foreign powers were behind some or all of these probes. The motivation of such intelligence gathering is obvious.*
>
> *The prospect of " information warfare" by foreign militaries against our critical infrastructure is perhaps the greatest potential cyber threat to our national security. We know that many foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional or "kinetic" weapons, nations see cyber attacks on our critical infrastructure or military operations as a way to hit what they perceive as America's Achilles heel-our growing dependence on information technology in government and commercial operations. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses to counter balance the military power of the United States(FBI, 2001).*

CRITICS:

Security experts agree that in order for there to exist a threat, there must exist a threat agent, a motive, and an outcome(Peltier, 2001). Clearly, the above several examples lay out all three. Arguably, it is the motive that separates terrorist acts from radical militia/political activism or random acts. While any expert familiar with risk analysis would find it foolish to deny the potential for cyber attacks from state sponsored groups and individuals, some security experts are adamant that “cyber terrorism” is merely a catchy buzz-phrase and concept based in fantasy (Juhnke, 2002). Many of these skeptics base their rationale on definitions of cyber terrorism that revolve around the use of violence, outcomes involving grave bodily harm, or loss of life (Juhnke, 2002). Another basis for denial is that the analysis of terrorist objectives reveals that any historical events labeled “cyber terrorism” don’t correspond with the usual creation of graphic pictures and creation of widespread fear that terrorists seems to desire as their outcomes (Sliwa, 2003). Some critics argue that it is precisely the “motive” that distances historical attacks from any type of terrorism. Considering a case like the Oklahoma City Federal Building bombing, the outcome rendered the specific motive and even nationality of the source irrelevant. There are still many unanswered questions about the funding, planning, and relationship between several groups who could be considered benefactors of the Oklahoma bombing objective. Argument on this point is merely a semantics disagreement that distracts from the realization of the overall definition of terms like terrorist and terrorism. Ultimately, a terrorist wants to take his internal struggle and anger/jealousy/sense of injustice, and get the attention of the “unconcerned” who live in places where they are “safe” from these difficulties. The terrorist aims to shatter realms of safety and project a sense of loss of control, loss of predictability, or loss of power to those who would otherwise be unconcerned with his struggle. This mindset causes actions that have secondary repercussions of attracting widespread attention and other indicators that lead scholars to define terrorism so strictly[3] that they quickly divorce the word from being associated with historical or potential cyber attacks.

These critics’ arguments, while not flawed in actual fact, are flawed in logic and attitude. Historically speaking, no terrorist group had ever coordinated a four-plane attack involving almost simultaneous crashes into symbolic and operational targets until September 11, 2001. While unprecedented in history, the planning, preparations, and testing had a vast history only visible through hindsight. The vulnerabilities were there for quite some time, as were the threat agents, the motive, and the prediction of outcome. It is illogical to know the mindset involved with such detailed and patient planning, and not assume that the lessons learned will not be re-applied at another time in another realm. The absence of historical evidence should not outweigh the risk associated with the vulnerabilities, the proliferation of knowledgeable threat agents, and the potential for crippling outcome from a cyber terroristic act. It doesn’t take much imagination to create scenarios where a cyber terror attack could, at a minimum, compliment a physical attack, and at a maximum be the catalyst for wide spread panic and loss of life due to downtime in the 911 system, hospital electricity/electronics, or damn floodwater control.

An additional danger that lies with denial of the existence of cyber terrorism and state-sponsored hacking is a reluctance to focus attention on policy, law-enforcement initiatives, and regulation that reaches out to govern the

[3] See Juhnke, 2002

same borderless world that the Internet operates in. For the forensics expert, each intrusion and especially each large scale incident has to be investigated with the same methodical process whether it be the work of an internal disgruntled employee, an experimenting "script kiddie", an independent criminal, or a cyber soldier/terrorist that is part of a state-sponsored, coordinated attack. It isn't until the investigation reaches a point near termination that the forensics expert is able to tell the magnitude, intention, and source of the attack.[4] The tremendous amount of cooperation and resources available to agencies and contractors working with "homeland defense" initiatives seems to avail itself to greater potential for progressive policy and critical tracking procedures than ever before. The interest in pursuing terrorism in this day and age might be great enough to keep the kinetic energy of interagency cooperation and public interest in passing laws at a sufficient level to make better progress than we have in the past-especially as far as forensic capabilities go[5]. Also, network security investment has always been difficult to sell to top management in organizations and businesses due to its lack of concrete return on investment and widespread ignorance of hacking procedures/method of operation (Peltier, 2001; McClure et al, 2001; Cobb, 2003). It is easier for many corporate executives and agency directors to visualize their company/organization's individual role in forming a collective infrastructure.

THE FUTURE:

In March of 2003, the newly formed Department of Homeland Security issued a press announcement about an initiative called, LIBERTY SHIELD. According to the announcement, LIBERTY SHIELD "is a comprehensive national plan designed to increase protections for America's citizens and infrastructure while maintaining the free flow of goods and people across our border with minimal disruption to our economy and way of life." Amongst many areas, the section applying to Information Technology contains an initiative to aggressively monitor the Internet for "signs of a potential terrorist attack, cyber-terrorism, hacking, and state-sponsored information warfare" (Bespacific, 2003).

In their book *Hack I.T.*, the authors start out their introduction with the following statement:

> "In March 2001, CSI published its "2001 Computer Crime and Security Survey." Which is based on responses from 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions, and universities. Of those organizations surveyed, 91 percent

[4] In the mid 1990's, an attack that was investigated as "solar sunrise" used spoofing addresses that gave the initial impression they were coming from computers in the Middle East. Later in the investigation, the culprits were discovered to be juveniles in California and an Israeli (Sliwa, 2003). The attacks were focused on many Department of Defense networks and corresponded with the U.S. planning attacks against Iraq. The logical conclusion was that of state-sponsored cyber attack. The forensic steps remain the same for all such attacks whether state-sponsored or not.

[5] A significant, if not the main difficulty lies in limitations on tracing/tracking and cross-border apprehension of tracked criminals.

> reported detecting computer security breaches in the last 12 months and 97 percent of those had web sites. Of those web sites, 23 percent reported suffering an attack within the last 12 months and 27 percent did not know if they had experienced an attack."(Klevinsky et al, 2002).

Figures from 2002 and 2003 from the survey reveal similar numbers. "The numbers could actually be bigger because many organizations still aren't equipped to detect security breaches. Only 61 percent of those polled above reported using intrusion detection" (Klevinsky et al, 2002).

With the increase of cable modem, DSL, and other "always on" Internet connections combined with increased home user computing power means more systems out there that could multiply the devastation of Distributed Denial Of Service (DDOS) attacks. Furthermore, the ability to use other addresses to spoof the true source of the attack further complicates the forensics process. The future trend seems to be only an increase of the proliferation of attacks and the severity of their impact. The authors of the book, *Hacking Exposed*, sum up the future of what lies in store for network security professionals who are striving to mitigate the impact of cyber-terrorists and state-sponsored cyber warriors by associating hacking with Moore's Law[6]. They state, "Attackers on the Internet will eventually find and exploit every vulnerability. The more interesting the target, the faster this will occur" (2001).

CONCLUSION:

Security experts disagree on the potential that exists for terrorists and state-sponsored crackers to coordinate attacks against U.S. cyber targets. While some experts see no link or proof that such attacks have or will occur, other experts can't imagine why such attackers wouldn't put their sights on critical U.S. infrastructure. With the Internet's ability to transcend national boundaries, there is no such thing as a safe place, a neutral zone, or a "peaceful cyber neighborhood" that provides the buffer of geographic distance from war-torn, criminal infested, or politically unstable regions. Up until the prolific use of the Internet, a person could choose their neighborhoods by home price or crime rate. Many U.S. citizens could live a lifetime without ever traveling and coming into contact with people from countries and regions that have raised generations who have never known peace. The World Wide Web has brought us the wealth of knowledge that comes from contact with diverse peoples and their information and intelligence, but much like a large city, that exchange of knowledge and metropolitan interaction allows for rubbing shoulders with those whose full time

[6] Moore's law states that the power of computing would double every 18 months(Newton, 2003). The fulfillment of this "prophecy" over time has negated statements like "This encryption is so complicated and secure that it would take the lifetime of the universe to crack it." Considering the improvement of processing speeds of computer chips to rates unimaginable just 10 years earlier, statements about the finality of security, decryption, or exploitation of vulnerabilities can't help but be inaccurate.

job is to scam, rob, or extort. The U.S., once separated from countries with destructive ideologies and dictators by the physical buffers of the ocean, is now existing in a cyber world with no geographic boundaries, few governing laws, and even fewer capabilities to enforce law. Our infrastructure and economy-world renown for stability and predictability-lies an attractive target to the disenchanted.

REFERENCES

Bespacific. (2003). "Homeland Security and Cyber-Attacks." Retrieved on June 1, 2004, from http://www.bespacific.com/mt/archives/002243.html.

Busby, Daniel. (2000). "Peacetime Use of Computer Network Attack." Army War College Review. April 3, 2000. Retrieved on June 1, 2004, from http://www.stormingmedia.us/cgi-bin/42/4267/a426773-142-10t.php.

CNN. (2003). "Arab American Pleads Guilty to Taliban Conspiracy." Retrieved on June 23, 2004, from http://www.cnn.com/2003/LAW/08/06/terror.plea.deal/index.html.

Cobb, Chey. (2003). *Network Security For Dummies.* New York: Wiley Publishing, Inc..

Devost, Matthew. (2003). "Current and Emerging Threats to Information Technology Systems and Critical Infrastructures." Strategic Overview. Retrieved on June 10, 2004 from http://www.devost.net/papers/business-briefing.pdf.

Dick, Ron. (2001). "Speech excerpt from Director FBI to US Senate." Retrieved on June 10, 2004 from http://www.fbi.gov/congress/congress01/rondick.html.

Fisher, Dennis. (2003). "Feds on Guard for Cyber-Attacks." Eweek. March 18, 2003. Retrieved on June 1, 2004, from http://www.eweek.com/print_article/0,3668,a=38866,00.asp.

Infowar. (1998). "Muslim Hackers' Story". Retrieved August 1, 2003, from http://groups.yahoo.com/group/isnet-bl/message/3. Apparently, Infowar had gone off line for a while, or another organization has taken the name. The Internet is full of references to this story and the source at infowar.com. Stories from 1996 to 2001 are no longer available at the site to determine one way or the other. This story could not be confirmed as coming from the current website www.Infowar.com. See www.arabsecurity.8m.com/news/mhc.html for another supporting reference(retrieved June 23, 2004).

Juhnke, Deborah. (2002). "Cyber Terrorism or Cyber Crime?" Retrieved on June 5, 2004, from www.forensics.com.

Klevinsky, T.J., Scott Laliberte, and Ajay Gupta. (2002). *Hack I.T.*. Boston: Pearson Education, Inc.

Lyman, Jay. (2002). "Report: U.S. Expecting Chinese Hack Blitz." Newsfactor Network, April 25, 2002. Retrieved on August 1, 2003, from http://www.newsfactor.com/perl/story/17465.html.

McClure, Stuart, Joel Scambray, and George Kurtz. (2001). *Hacking Exposed: Network Security Secrets and Solutions.* Berkley: Osborne/McGraw Hill.

McDonald, Tim. (2002). "U.S. Cyber Strike Could Earn Military Response." Newsfactor Network, February 14, 2002. Retrieved on May 1, 2004 from http://newsfactor.com/perl/story/16340.html.

Newton, Harry. (2003). *Newton's Telecommunication Dictionary(19th edit).* New York: Miller Freeman, Inc.

Peltier, Thomas. (2001). *Information Security Risk Analysis*. Boca Raton: CRC Press LLC.

Poulsen, Kevin. (2001). "U.S. Hack Attacks Are New Cold War." Security Focus. March 22, 2001. Retrieved on June 1, 2004, from http://www.securityfocus.com/printable/news/177.

Prosise, Chris and Kevin Mandia. (2001). *Incident Response: Investigating Computer Crime.* New York: Osborne/McGraw Hill.

Sans Reading Room. (2001). "Can Hackers Turn Your Lights Off?". Retrieved June 1, 2004, from http://www.sans.org/rr/papers/24/606.pdf

Shane, Scott. (2001). "Web Could Be New Front For U.S. Enemies." Baltimore Sun, October 9, 2001. Retrieved on May 10, 2004, from http://new.blackvoices.com/news/sns-worldtrade-cyber-bal,0,3310225.story?coll=bv-news.

Sliwa, Carol. (2003). "Q&A: Microsoft's Scott Charney on Security in a Time of War." Computerworld. March 20, 2003. Retrieved on June 10, 2004, from http://www.computerworld.com/printhis/2003/0,4814,79554,00.html.