Cyberterrorism: The Silent Threat

Subject Area Electronic Warfare (EW)

EWS 2006

Cyberterrorism: The Silent Threat
Submitted by Capt J. M. Navarro
CG #5, FACAD: Major D. Wright
7 Feb 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberterrorism: The Silent Threat	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps Combat Dev,Marine Corps University, 2076 South Street,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

During the past few years, technology-dependent California has experienced numerous power outages, commonly referred to as “rolling blackouts.” These rolling blackouts have disabled millions of information technology (IT) users as well as crippled technology dependent organizations. Luckily, the rolling blackouts have only created minor monetary setbacks and are far from being classified as catastrophic (Konrad, 2001). A rolling blackout by itself is nothing more than a minor inconvenience; however, imagine a one-two punch of a rolling blackout and an attack on a U.S. infrastructure. Picture an attack orchestrated by cyberterrorists on U.S. infrastructures in conjunction with an attack on an Air Traffic Control Center or perhaps a Nuclear Plant. If a rolling blackout can disrupt the world’s third largest economy, imagine what advanced technology in the hands of terrorists can accomplish. Cyberterrorism is not science fiction. It is a real and growing threat. As American infrastructures, including military, become more techno-centric, a cyberterrorist attack is imminent.

In the Marine Corps, marines are taught to fight in tactical environments by the employment of a combined arms doctrine (air, land, and sea power). However, one of the many tools which enable marines to be so effective in the

battlefield is also the advanced use of technology. Unfortunately, the availability and use of advanced technology is no longer limited only to the most powerful nations or militaries in the world.

The information presented throughout the paper will shed light on how terrorist groups are embracing technology to carry out their missions, as well as illustrate the impact these attacks (i.e. monetary, informational) have on U.S. network infrastructures. In addition, the paper will outline current countermeasures and techniques being utilized by both civilian and government agencies to help mitigate these threats.

Background

The world wide availability and low cost of information technologies is providing new and more effective capabilities for terrorists. When one thinks of a cyber terrorist or hacker, an image of the movie *War Games* (1983) comes to mind.

The main character, played by Matthew Broderick, mischievously accesses a secured Department of Defense (DOD) mainframe and almost starts a nuclear war with the Soviet Union. Although *War Games* was released over two decades ago, it was one of the first times the public was

introduced to the world of hackers and the potential of cyberterrorism.

Advancements in technology have helped shape the military into a more deadly, proficient, and effective force. Because of the complex satellite and network communication systems that have been implemented throughout the world, innovations such as real-time target visualization and battlefield pictures are now reality. However, the lethality gained by our communications and network infrastructure has created a great dependence on the technology itself and has created a new threat for our fighting forces. This new threat is known as cyberterrorism.

Cyberterrorism is the act of exploiting vulnerabilities in an attempt to compromise unsecured and secured networks (Wikipedia, 2005). These vulnerabilities range from information capture to complete shutdown or destruction of a network. Yet, despite the ever growing threat from cyberterrorism, U.S. commercial and DOD networks remain poorly protected and attacks often occur to these networks without any apparent repercussions from the U.S. government.

The proliferation of the information superhighway has paved the way for nefarious organizations to exploit new

resources. Terrorists have moved into cyberspace to facilitate traditional forms of terrorism, such as bombings. They use the Internet to communicate, coordinate events, and advance their agenda (BBC, 2001).

Terrorist cells have devised communication networks that used the Web, email, and even electronic bulletin boards in their coordination efforts (Sieberg, 2001). Osama bin Laden, for example, while conducting terrorist operations out of Afghanistan, was equipped with computers and communications equipment that enabled him to maintain contact with his terrorist cells.

The increased use of information technology (IT) by terrorist organizations has been reported world wide. Israeli security forces have reported that Hamas activists have been using chat rooms and encrypted emails to plan operations and coordinate attacks. In another example of how terrorist organizations are embracing technology, email press releases are utilized by The Revolutionary Armed Forces of Columbia (FARC) in order to formally answer questions from the press (Denning, 2000).

The proliferation of terrorist sponsored web sites and instances of cyberterrorist attacks on U.S. networks has grown at a staggering rate (FBI, 2004). Unfortunately, due to free speech laws the web sites are difficult to

shutdown. Even if a web site is effectively deactivated there is no law that prevents the same web site from being hosted in a country that does not enforce restrictions. In addition, the increased availability and affordability of computer resources also enables nations, enemy and friendly, with limited resources to engage in this new type of warfare.

Threats

Government and DOD networks are often targets of cyber attacks. Detected attacks against unclassified DOD systems rose from 780 in 1997 to 5,844 in 1998, to 75,000 in 2004(Tiboni, 2005).

“An exercise conducted by the DOD in conjunction with the National Security Agency (NSA) took place in 1997. The exercise identified weaknesses in the power grid and found the Emergency 911 systems had weaknesses that could be exploited by an adversary using publicly available tools on the Internet. The findings of the study concluded that service on these systems could be disrupted. The findings also warned that through mutual dependencies and interconnectedness, critical infrastructures could be vulnerable in new ways, and these vulnerabilities were steadily increasing, while the cost of attacks were decreasing” (Denning, 2000).

More recently, attacks on DOD networks by a hacker group known at Titan Rain has raised some concerns about the vulnerability of U.S. IT infrastructure. Titan Rain is the name given to a group of hackers who are allegedly supported by the Chinese government. Thus far, Titan Rain has been able to compromise both corporate and military networks by stealing sensitive data (Thornburgh, 2005). Some experts believe that some of the sensitive military data stolen by Titan Rain has enabled China to leap five years forward in its technology development.

Tools

Although sophisticated tools such as viruses, trojans and worms can be utilized to conduct cyberterrorism, there are other tools that are readily available and in fact are utilized by the everyday personal computer (PC) users. These tools include search engines (i.e. Google, Yahoo), chat groups, and peer to peer (p2p) software and networks. In addition, there are a myriad of web sites that contain vast libraries with tutorials and custom made tools that are free for the taking (Denning, 2000).

Encryption software is another widely-available tool routinely utilized by terrorist organizations to conceal their communications and data files, making it increasingly

difficult for government agencies to monitor their activities.

The U.S. National Security Agency (NSA) has confirmed that organizations such as Al Qaeda and Hamas utilize encrypted internet communications to transmit maps, pictures, and other details pertaining to terrorist attacks (Stout, 2001). For example, the 9/11 hijackers utilized encryption tools to secure files on their laptop computers. The Aum Shinrikyo cult, which gassed the Tokyo subway in 1995 killing twelve people and injuring six thousand more, also used encryption to protect their data, which included plans and intentions to deploy weapons of mass destruction against Japan and the United States (Denning, 2000).

Costs

The cost that a successful cyber attack can have on a national infrastructure is incalculable. For example, the cost for denial of service (DoS) and worm attacks reaches well into the millions of dollars (MacGregor, 2000). A DoS attack is an attack on a computer system or network that causes the loss of network connectivity and services by consuming the bandwidth of the target network or by overloading the computational resources of the victim system. A computer worm is a self-replicating computer program, similar to a computer virus. A virus attaches

itself to, and becomes part of, another executable program (i.e. email, photo attachments, and file executables); a worm, however, is self-contained and does not need to be part of another program to propagate itself (Wikipedia, 2005). DoS and worms are designed to exploit the file transmission capabilities of a target system and often times create backdoors (unauthorized entry ports within a computer connected to a network). These backdoors are exploited by hackers or spammers with the intent to transmit information (.i.e. junk email) or to utilize the resources on the target system.

On a commercial level, DoS and worm attacks can have a devastating monetary impact on an organization; however, they pale in comparison to the damage an organized attack on DOD networks such as the ones recently experienced by Titan Rain.

Countermeasures

The DOD has invested millions of dollars developing and implementing countermeasures in order to mitigate cyberterrorism. According to an article recently published in Wired News entitled "U.S. Military's Elite Hacker Crew", the U.S. military "has assembled the world's most formidable hacker posse: a super-secret, multimillion-dollar weapons program that may be ready to launch

bloodless cyber war against enemy networks. This cyberwar will be launched from electric grids to telephone nets" (Lasker, 2005).

The hacker crew is part of a unit known as the Joint Functional Component Command for Network Warfare (JFCCNW). Very little is known about this unit other than their mission to defend U.S. DOD networks. The unit is believed to be comprised of staff from the Central Intelligence Office (CIA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), the four military branches, and civilian experts and military representatives from allied nations (Lasker, 2005).

Conclusion

The availability and development of cheaper information technology has facilitated a new threat of warfare-cyberterrorism. The United States' growing dependence on technology to function, while advanced and necessary, may prove to be an Achilles' heel to the protection of the nation. The government not only needs to continue developing new methods of defense for land, air and sea, but may also need to develop methods of defense solely for the protection and monitoring of cyberspace. We have only just begun to witness this new method of warfare

and weaponry. Is it really that inconceivable to imagine a cyberterrorist attack on a scale which could both paralyze our nation and our military? Afterall, we never imagined U.S. commercial airliners would be used as missiles as a first strike on a war against America.

WORD COUNT: 1,727

Bibliography

Konrad, Rachel. News.com. California Power outages. <http://news.com.com/2100-1017-251167.html> (18 January 2001)

Wikipedia. Cyberterrorism. <http://en.wikipedia.org/wiki/cyber-terrorism> (2005)

BBC News. U.S. Crackdown on cyberterrorism. <http://news.bbc.co.uk/l/hi/world/americas/594698.stm> (7 (January 2000)

Sieberg, Daniel. CNN.com. Bin Laden exploits technology to suit his needs. <http://archives.cnn.com/2001/us/09/20/inv.terrorist.search/> (21 September 2001)

Denning, D., E. Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> (23 May 2000)

Tiboni, Frank. FCW.com. The New Trojan War. Defense Department finds its networks under attack from China. <http://www.fcw.com/article90262-08-22-05.print> (7 February 2005)

Thornburgh, Nathan. Time. Inside the Chinese hack attack. How a ring of hackers, codenamed Titan Rain by investigators, probed U.S. Government computers. <http://www.time.com/time/nation/printout/0,8816,1098371,00.html> (25 august 2005)

Stout, L., K. Cnn.com. Bin Laden goes low-tech to avoid a trace. <http://archives.cnn.com/2001/BUSINESS/asia/09/13/hk.binladenlowtech/> (14 September 2001)

MacGregor, Maureen. Top Layer. Top Layer Networks Blocks Denial of Service attacks, intrusions. <http://www.toplayer.com/content/cm/pr63.jsp> (9 May 200)

Lasker, John. Insecure.org. U.S. Military's Elite Hacker Crew. <http://seclists.org/lists/isn/2005/apr/0063.html> (18 April 2005)