Cyberterrorism: A Description from Multiple Perspectives

Jonathan Matusitz
University of Central Florida at Seminole State College,
Partnership Center (#UP Center (#UP 3009)
100 Weldon Blvd., Sanford, FL 32773,
matusitz@gmail.com.

Introduction

This paper analyzes cyberterrorism from various perspectives. By and large, cyberterrorism refers to the use of the Internet or information technologies (i.e., computers), from both internal and external networks, to launch electronic attacks. Cyberterrorism involves a premeditated act; its goal is to intentionally take actions – or threaten to use actions – against computers, networks, and other critical infrastructures to inflict damage in order to further ideological, political, or other types of objectives, or to intimidate any person in furtherance of such objectives. This analysis is important because it does not follow a monolithic view of cyberterrorism. Rather, it offers multiple angles to provide a broad-based description of what cyberterrorism actually is.

This paper begins with a detailed definition of the complexity of cyberterrorism, from the origin of the word "cyberterrorism" to its differences from cybercrime, hacktivism, and computer-assisted terrorism. This paper, then, proceeds to describe cyberterrorism in great detail. For example, the authors make the point that hacking, in and of itself, does not constitute cyberterrorism. Another important section of this analysis is a description of cyberterrorism from a communicative and semiotic perspective as well as a description from a legal perspective.

What comes next is an explanation of two specific cases of cyberterrorism: (1) the actions of Titan Rain (a Chinese cyberterrorist group) and (2) the 2007 Estonia cyber attacks. The authors then give an account of what can be done to counter those acts of terror. It was also important to add a section on networks of cyberterrorists (a postmodern organizational design). This paper ends with a discussion section that also offers suggestions for future research.

The Complexity of Cyberterrorism

Despite the fact that cyberterrorism has existed for the past several decades, only a handful of people know what it means. It might prove useful for readers to describe cyberterrorism from various angles. Let us start with a brief description of the origin of the word.

Cyberterrorism: Origin of the Word

Cyberterrorism refers to the use of electronic networks and computer technology as weapons (Dunnigan, 2003; Wacks, 2008). Attacks via the Internet need to have a terrorist component to be called "cyberterrorism." From an historical perspective, the word "cyberterrorism" was coined in the late 1980s when Collin (2006), a senior research fellow at the Institute for Security and Intelligence (ISI) in Stanford, California, coined this innovative techno-phrase by making a portmanteau of two linguistic elements: cyberspace and terrorism.

Difficulty of Defining Cyberterrorism

Almost two decades after the word was invented, cyberterrorism remains difficult to define because it does not possess a straightforward, widely accepted definition. Part of the reason stems from the controversial element of "cyberterrorism" itself: the word consists of "cyber" – a definition for which most people would agree on – and "terrorism" – which, since 1793, has had over two hundred definitions (Schmid, 1984). "Cyber" refers to anything that has to do with computers, computerized items (both real and imagined), and/or automated systems (both in terms of hardware and software). On the other hand, one man's terrorist is another man's freedom fighter. It is not surprising, then, that even prominent scholars and researchers in fields such as communication and information technology cannot agree on a single definition of cyberterrorism. While an e-mail bomb can be an act of pure hacking for some, it can be an act of cyberterrorism for others (Kisielnicki, 2008).

To solve this problem, the authors have chosen a definition that he sticks to throughout the entire analysis. At the same time, the authors deem it important to see how other scholars have defined cyberterrorism and related terms. Such a related term is the word "cyberthreat." Cyberthreats fall into two distinct categories: (1) traditional criminal activities facilitated by computers and the Internet, such as theft of intellectual property, online sexual exploitation of children, and Internet fraud; and (2) threats affecting national security (after the emergence of Internet technology), such as cyberterrorism and computer-aided terrorism (Calder & Watkins, 2008; Kouri, 2005). Based on this definition, several terms have to be differentiated, some of which are "cybercrime" [which refers to the first definition of cyberthreat] and "cyberterrorism" [which refers to the second one].

Cybercrime Is Different from Cyberterrorism

Scholars differentiate cyberterrorism from cybercrime. Although cybercrime and cyberterrorism are both acts of wrongdoing in the cyberworld (Britz, 2004), there is a difference between the two. The difference lies in the motives behind the cyber attacks. Cybercrime refers to an unlawful or criminal act where computer technology is either a tool or a target (or both) (Janczewski & Colarik, 2007). It is a rather new field of criminological inquiry that comes from the area of criminal justice; it encompasses computer crime or computer-related crime (Carter & Katz, 1996) and Internet crime (Wall, 2001). In essence, a cybercriminal is a criminal using computers and/or the Internet to communicate, raise money, recruit new members willing to break the law, and

commit other crimes (Wall, 2007). According to Archick (2003), a cybercriminal offense includes money laundering, as well "fraud and forgery, child pornography, copyright infringements, and security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability" (p. 2). Cyberterrorism is the premeditated use of disruptive activities or the threat of using disruptive activities in the cyberworld (Janczewski & Colarik, 2007). A cyberterrorist act is based on motives that can be social, ideological, religious, political, or of similar intentions. Another objective of the cyberterrorist can be intimidating any person or group in furtherance of those motives (Dunnigan, 2003).

It is indispensable to pay close attention to the very meaning of the word "premeditation." A cyberterrorist act is always premeditated. In contrast, a cybercriminal act does not have to be premeditated to be called "cybercrime." A computer-whiz college student may break into a computer system for various reasons, and these reasons are not necessarily intentional or premeditated. If caught, the computer-whiz college student will still be considered a cybercriminal and will probably go to jail, especially if the act was committed in a country that has cybercriminal laws, such as the United States and many European nations (see Archick, 2003). Yet, the cybercriminal will not be found guilty of cyberterrorism if his or her act is not recognized as an act belonging to one of the categories described as cyberterrorism (as it is explained later in the section on the legal perspective of cyberterrorism). In addition, cyberterrorism is usually intended to be more massive and destructive than cybercrime (Clem, Galwankar, & Buck, 2003).

Hacktivism Is Different from Cyberterrorism

Scholars have highlighted the importance of hacktivism as well. Hacktivism refers to electronic civil disobedience or Internet activism. Hacktivists write codes to promote political ideology (Milone, 2003). They are cyber protesters with political motives and believe that proper use of code will have powerful effects (Dunnigan, 2003). However, they are not cyberterrorists in the sense that they do not cause harm to information systems, Web sites, and other computer-related materials. In other words, hacktivists do not engage in defacing Web sites, launching computer viruses, sending worms, or using malicious computer tools. If they do – and since they have political motives – then they become cyberterrorists.

Computer-Assisted Terrorism Is Different from Cyberterrorism

Cyberterrorism is different from computer-assisted terrorism (Lenzner & Vardi, 2004). Computer technology and the Internet have been used by terrorists (e.g., al-Qaeda members) to assist conventional forms of terrorism like suicide bombings. They can use Web sites to merely communicate, receive orders from their commanders, obtain important information, carry out missions, propagate their messages, or recruit supporters (Robb & Fallows, 2007). In a similar fashion, using email as a medium to communicate information about massive-scale terrorist attacks does not constitute cyberterrorism *per se*. For instance, some experts on terrorism believe that, during the September 11th, 2001 attacks, each of the four groups of hijackers did not know each of the other groups, but

they had communicated with a central "commander" through the Internet. The "commander" might have been a sort of "go-between" or gatekeeper" between those four groups and might have used e-mail (or a Web site) to exchange information, procure and channel funding, and organize and order the launching of the attacks against the Twin Towers in New York City and the Pentagon (Mcdermott, 2005).

Computer-assisted terrorism is not the same as cyberterrorism (Lenzner & Vardi, 2004). Just like "techno-terrorism," computer-assisted terrorism refers to the ample use of computer technology by terrorists because it adds to their conventional operations. Cyberterrorism, on the other hand, pertains to attacks on information systems, on a nation's computer systems, computer-generated infrastructures, and so on (Wacks, 2008). The following sub-section defines cyberterrorism in detail.

What Is Cyberterrorism?

Cyberterrorism has been described from multiple angles and perspectives (Matusitz & O'Hair, 2008). One of the definitions of cyberterrorism tells us that it is the intentional use of threatening and disruptive actions against computers, networks, and the Internet in order to cause harm or further ideological, political, or similar objectives, or to intimidate any person in furtherance of such objectives (Arquilla, Rondfeltd, & Zanini, 1999; Conway, 2002; Kisielnicki, 2008). A similar definition of cyberterrorism is that it is "aimed at coercing a population or its government to accede to certain political or social objectives" (Clem, Galwankar, & Buck, 2003, p. 272). A cyberterrorist act is a cyber attack that endangers life, has the potential to inflict bodily harm, places the public or any section of the public in fear, affects unfavorably the harmony between different national, religious, racial, linguistic, or any social groups or communities, coerces or intimidates the government established by law, and so on. This brings up the question of whether or not a hacker is a cyberterrorist (Dunnigan, 2003; Janczewski & Colarik, 2007; Verton, 1999).

Now the question is, "Are hackers cyberterrorists?" A computer-whiz kid seeking glory and who cripples the entire computer system of a university is not a cyberterrorist if the act of hurting networks is not premeditated (Guttman, 2008). As a result, the term "hacker" does not necessarily imply that he or she is a cyberterrorist. Hackers delve into systems or networks but do not destroy them. Note that, under the U.S. Congress approved law called "Act 2001" (Archick, 2003), if the damage caused by the computer-whiz kid is significant, then he or she might be still get some punishment. No matter what, a cyberterrorist is an intentional, malicious hacker. Hackers with malicious intent are cyberterrorists who use computer systems to achieve their goals (Vegh, 2002; Wacks, 2008). If the hacker just tries to delve into computers with no intention to harm computers, then he or she is plainly a "hacker." In fact, hacking can be a good tool for understanding the threats and vulnerabilities of a user's computer (Calder & Watkins, 2008). The key is to understand that the tools of the cyberterrorist are the tools of the hacker just applied with different motivations.

Cyberterrorism: A Communicative and Semiotic Perspective

There is another crucial distinction to be made between hacking and cyberterrorism. Hackers delve into systems or networks but do not destroy them; they do not even communicate their intention to do so. Cyberterrorism, on the other hand, is like terrorism; it is inherently a communicative process (O'Hair & Heath, 2005). As a public communication channel, the Internet can be used to promote cyberterrorism. As such, cyberterrorism is publicized and perpetuated through new media communication. It is essentially through semiotics and the exploitation of new media that cyberterrorists find success in accomplishing their primary goals. Semiotics is the study of signs (Berger, 1989; Luskin, 1996; Nöth, 1995; Sebeok, 1994). A sign communicates something that stands for something else, or that can be made to represent or symbolize something else (Berger, 1989). We see signs and symbols within a communication context, where the communication of messages is considered essential to the construction of meaning (Fiske, 1982). From this vantage point, meaning is an active process that is subject to continuous transformation. Besides, verbal communication is not the only medium that conveys meaning; semiotics also deals with nonverbal communication (Benford, 1998).

Cyberterrorism is a semiotic act in the form of a message, a symbol, or a new media image. Our contemporary western world is immersed within images, signs, and symbols (Miller, Matusitz, O'Hair, & Eckstein, 2008). It is no surprise, then, that there is a powerful semiotic dimension to cyberterrorism. Indeed, it can involve sending images of fear. For instance, in 1998 cyberterrorists sent a massive flood of e-mails to the Sri Lankan embassy's main Web server with messages that read "We are the Internet Black Tigers and we are doing this to disrupt your communications." The intent was not only to crash the computer systems of the embassy – and they succeeded (Denning, 2000) – the motive was also to send a semiotic message that evoked fear. Cyberterrorism is a semiotic gesture because it aims at creating not only fear, but also *signs* of fear. It is important to consider that, on the whole, cyberterrorist attacks are not successful.

Although, theoretically, cyberterrorists could take down the entire U.S. West Coast if they managed to cripple a few massive power grids, in reality they create fewer casualties than are expected by the magnitude of the news they elicit. Such acts leave compelling signs and images permanently anchored in human minds (Miller et al., 2008). For example, the movie *Firewall*, starring Harrison Ford, showcases this. In the movie, the messages conveyed by cyberterrorist attacks of all sorts have an impact on Harrison Ford because those messages create interference and anxiety in the form of potent psychological noises in his (and his family's) daily life. Likewise, in *Live Free or Die Hard*, a group of cyberterrorists is blocked by a detective (played by Bruce Willis) as they attempt to shut down the whole computer network of the United States.

Just like terrorism is primarily a process of communication between terrorists and target audiences (Tuman, 2003), cyberterrorism has the objective to send a powerful signal whose meaning is intended to frighten and coerce. Cyberterrorism serves a semiotic function in that it communicates a violent political meaning that symbolizes more of an ideological statement than a massive material threat. In 2002, a group of cyberterrorists, known as the World Fantabulous Defacers (WFD), hacked into the

official Web site of Israeli Prime Minister Ariel Sharon and defaced it. As a title, they wrote, "The Face of the World's Biggest Murderer." At the bottom of the Web site, they left a message with the signature of the group. The WFD's hacking into Sharon's official Web site stands out as an example of a cyberterrorist group that was in a position to do far more damage and perhaps cause a national crisis in Israel (Verton, 2003). By gaining such visibility – and sometimes they can infiltrate hundreds of thousands of computers – cyberterrorists are able to spread terror and evoke fear.

Lastly, of equal semiotic relevance is the relationship between cyberterrorism and new media (i.e., the Internet and information technologies). Without these, cyberterrorism would be an ill-fated task. Cyberterrorism news is made to order for the specific requirements of new media. Farnen (1990) already noted this when describing terrorism. As he remarked, "terrorism is different, dramatic, and potentially violent. It frequently develops over a period of time, occurs in exotic locations, offers a clear confrontation, involves bizarre characters, and is politically noteworthy. Finally, it is of concern to the public" (p. 111). The exploitation of communication technologies by cyberterrorists is fundamental to the semiotic cyber struggle. To cause economic chaos, lose of faith (on the part of certain businesses) to do transactions online, and massive overreaction from the public, cyberterrorists rely on those communication technologies to stir up the target population by using images which, once produced, can be evoked again later and reused to new effect (Matusitz, 2008). Now that we have seen the communicative and semiotic perspective of cyberterrorism, let us digress for a moment and focus on its legal perspective.

Cyberterrorism: A Legal Perspective

Within weeks that followed the September 11, 2001 attacks in New York and Washington, the U.S. Congress approved a new antiterrorist law called the "USA Patriot Act" of 2001 (Archick, 2003). The "USA Patriot Act" of 2001 included cyberterrorism as part of the legislative jargon and classified different types of cyberterrorism and wreaking losses to protected computer systems of citizens, juridical persons, and federal and state departments (including offices that coordinate national defense and ensure national security) (Janczewski & Colarik, 2007). Archick (2003) briefly describes those different forms of cyberterrorism. According to Archick, a cyberterrorist act is a cyber attack on critical infrastructure facilities, financial institutions, or government systems that are premeditated and motivated by the goal to (1) intimidate or coerce a government, the civilian population, or any segment thereof and to (2) further political, social, or ideological objectives.

Specific Cases of Cyberterrorism

Two specific cases of cyberterrorism are analyzed in this section: (1) the actions of Titan Rain (a Chinese cyberterrorist group) and (2) the 2007 Estonia cyber attacks. Thornburgh, Forney, Bennett, Burger, and Shannon (2005) tell us about a Chinese group of cyberterrorists called Titan Rain that stole U.S. secrets. Those cyberterrorists are voracious, never hesitating to destroy any parasitic file they could find coming in their

way, attempting to penetrate secure computer networks at the American most sensitive military bases, defense contractors, and aerospace companies. According to the same Thornburgh et al. (2005), those Chinese cyberterrorists work for the government in mainland China and have a political goal. Their cyber attacks come from just three routers that seem to be the first connection point from a local network to the Internet. A TIME investigation into the case reveals how the Titan Rain attacks were uncovered, why they are considered a significant threat now under investigation by the Pentagon, the FBI and the Department of Homeland Security, and why the U.S. government has yet to stop them (Thornburgh et al., 2005).

In the U.S. military, Titan Rain is creating fears. In fact, Titan Rain has the ability to cause widespread havoc as hundreds of computer systems in the Department of Defense have been penetrated by insidious programs such as Trojan horses. Not only could Titan Rain control the DOD hosts, but they could also use the DOD hosts in malicious activity (Thornburgh et al., 2005). The possibility also exists for the perpetrators to shut down each host. Allied nations such as Britain, Canada, Australia, and New Zealand have also been targeted by the Chinese cyberterrorists (Thornburgh et al., 2005).

In 2007, Estonia (a highly wired country) became the target of a massive cyber attack after a Russian World War II war memorial was removed by the Estonian government from downtown Talinn (Estonia's capital city). The attack was carried through a denial-of-service (DOS) attack in which virtually all Estonian government ministry networks, two principal Estonian bank networks, and media Web sites were taken down by the attacks (Howard, 2009). These attacks on Estonia exemplify a case of cyberterrorism (Hanlon, 2007). Not only was it a considerable electronic disruption causing massive network damage and panic in the country; it was also implemented after a political move was made by the Estonian government. As Adrian Blomfield (2007) stated in the *Telegraph*, "If a highly IT country cannot carry out its everyday activities, like banking, it sows terror among the people" (p. A1). It is not clear whether the entire Russian government launched the attacks on Estonia, but three things are certain: it was determined that (1) it was no accident, (2) it was no "simple hacking maneuver" as the targets were vital infrastructures of a country, and (3) the cyber attack was traced to computers housed in the Kremlin (Greenberg, 2008). This cyber attack was both a terrorist act and politically motivated.

Cyberterrorists use various tools to hit their targets and accomplish various objectives. Examples of cyberterror on computers and the Internet are as simple as malicious software such as computer viruses, Trojan horses, vampires, logic bombs, computer network worms, and DOS attacks (see Appendix A).

What Are the Tools against Cyberterrorism?

Computer security experts say that, although the first targets of cyber attacks tend to be government agencies, organizations and businesses that have not established

security measures to protect their systems are also fair game. Some of the tools used against cyberterrorism are firewalls and anti-virus software programs.

Firewall: a computer system with special security precautions. Located between the Internet and a local network, it performs the role of a gateway to prohibit unauthorized or seemingly dangerous material from entering the network and to keep external nodes from accessing, say, an organization's confidential data. From an IT perspective, a firewall can function as a packet filter, which prevents traffic to specific addresses based on the IP address, protocol, or category of application identified by a port number. In practice, a packet filter may permit web traffic on port 75 and block Telnet traffic on port 40. Many packet filters can also determine which IP addresses ask for which ports and allow them or turn them down – based on the security settings of the firewall (Docter, Dulaney, & Skandier, 2009).

Firewalls only allow packets with precise source addresses, source ports, destination addresses, and destination ports to go through them (Baring-Gould, 2009). Major Web sites and corporate computer systems have protected themselves with firewalls. For instance, American power plants have well-protected Internet operations and are well equipped to detect malicious intruders. Yet, they still have soft spots. According to an article entitled "Britain Warns of Trojan Horse Computer Attacks" (2005), firewalls do not give complete protection, and there is no complete mitigation for computers connected to the Internet.

Anti-virus software: a software program that examines the computer memory and disk drives for malicious code. The program notifies the user if a virus is present, and will clean and delete infected files or directories. Another function of anti-virus software is the function of interception mechanism. Such mechanism works to interrupt file system calls and carry out code before returning the result. This code may implement any action desired by the system developer, such as executing direct access to the file systems, exchanging messages across the network, or even declining file operations by returning an error. This example of anti-virus software can be divided into two categories: kernel-based and user-level based. The first runs completely inside the kernel of the operating system. The second only includes a small module that runs in the kernel, intercepting the file system calls and redirects them to user level (Carriço, Baloian, & Fonseca, 2009).

Networks of Cyberterrorists

Cyberterrorists have been known to mostly work alone. Nevertheless, they sometimes feel the need to team up with others as well. In many cases, the now networked cyber attackers claim they are fighting a worthy cause. A few cyberterrorist groups are noticeable as being the "elite," as they have done some of the major attacks around (Zepp, 1999). When cyberterrorists form networks, they network with other factions through various channels of communication. This method reinforces the needs of the community of cyberterrorists without the necessity of creating a large-scale single organization, like a massive conventional terrorist organization. So, cyberterrorists have become involved in Internet social networks (McKenzie, 2004). Some cyberterrorist

groups like to act as cybersurrogate groups in order to help other cyberterrorists – who are really in need of help (i.e., regarding the design of certain malicious software programs, etc.) – increase their chances of striking the right node or hub in the Internet or computer network. This has been proved easy and advantageous (Schwartau, 1996).

Cyberterrorist networks have the innovative characteristics of being self-organized, quick, effective, and flexible (Berger, 1998). This can be an organizational challenge to cyber forensics experts and law enforcement agents in their efforts to locate those responsible for cyber attacks. Indeed, it is hard to dominate the flow of information on the Internet due to decentralized access and the massive volume of information (Matusitz, 2008). Cyberterrorist networks are a form of postmodernism because they traverse and go beyond continental borders within seconds; they have no fixed centers and they depend on the software of ideas, not the hardware of the Army, Navy, or Air Force (Matusitz & O'Hair, 2008). Because the Internet smoothes the progress of easy exchange of information, cyberterrorists can be far away from areas in which they are considered *persona non grata* (that is, "unwelcome") (Matusitz, 2008). Terrorism has transitioned from hierarchical types of models to information-age network designs (Arquilla, Rondfeldt, & Zanini, 1999). This constitutes, again, an organizational challenge because, before cyberterrorist networks existed, cyber forensics experts and law enforcement agents could identify who was who behind terrorist acts (i.e., a government or a leader from a hierarchical terrorist organization). Today, the postmodern type of cyberterrorist network is horizontal and flat, rather than vertical and bureaucratically governed (Matusitz & O'Hair, 2008). It is also an all-channel design (Bavelas, 1950; Leavitt, 1951), implying that any cyberterrorist in the network can be connected to any other cyberterrorist.

Discussion and Future Directions

What this paper has demonstrated is that the look of terrorism is evolving. While cyberterrorism has the same motives as those of conventional terrorism, the world is increasingly confronting new and unique approaches, designs, and weapons. Human lives, those of earthlings, depend greatly on the Internet, networks, and information technology. This is an advantage for cyberterrorists. It gets even more complicated as cyberterrorism has been inadequately considered by many people and does not lead enough to their shared anxieties. For all these reasons, cyberterrorism remains a complex phenomenon that is difficult to define, let alone identify. Nevertheless, one does not need to provide a monolithic view of cyberterrorism in order to effectively describe it in full detail, from all angles, and supported by various factual examples.

An important implication of this analysis is that now readers most likely have a better understanding of the meaning and impact of cyberterrorism. Now, we know that cyberterrorism, unlike hacking, is always premeditated. Although hacking can be a good method for threatening computers or make them more exposed to risks, attacks through the Internet or against networks or systems must have a terrorist component to be labeled "cyberterrorism." Whether causing a disruption in the federal computer network as an act of retaliation or destroying the actual machinery of the information infrastructure, the

objective is to cause harm, inflict damage, or threaten to do so. Hence, the motives of cyberterrorists are the same as those of conventional terrorists; these motives tend to be political, social, ethnic, religious, or ideological. And, as we have seen, cyberterrorism is different from not only hacking, but also from cybercrime, hacktivism, and computer-assisted terrorism. A legal perspective on cyberterrorism was provided in this analysis. While most countries did not have laws against cyberattacks, now they do. It sometimes takes years to realize that cyberterrorist attacks can wreak financial havoc with just a few software programs and keystrokes.

Of equal relevance is the fact cyberterrorism is inherently a communicative and semiotic act. In the same way that terrorism is, first and foremost, a process of communication between terrorists and target audiences (Tuman, 2003), cyberterrorism has, among its many purposes, the goal to send compelling and cogent signals whose meanings are intended to frighten and coerce. Cyberterrorism is a semiotic gesture; it is a message, a symbol, and a new media image. Cyberterrorists, then, seek publicity and communicate their intentions through new media. In essence, it is via semiotics and the exploitation of new media communication that cyberterrorists can accomplish their chief goals successfully. Since western culture is wrapped up with images, signs, and symbols (Sebeok, 1994), it is a breeding ground for effective cyberterrorism. Therefore, there is a powerful semiotic dimension to cyberterrorism.

In line with these contentions, cyberterrorists do not communicate or collaborate among each other through traditional hierarchies (unlike military units and traditional terrorist organizations). Because the Internet is postmodern, collaboration and communication are more horizontal, taking the shape of an all-channel design (Bavelas, 1950; Leavitt, 1951). This facilitates anonymity. Cyberterrorism incidents can go past regional, state, national, and even international boundaries, so much so that the notions of time, space, and geography are no longer necessary. Cyberterrorism becomes an organizational challenge. The challenge also lies in the very fact that cyberterrorists come from all over the world.

For future research, it might prove interesting to further distinguish cyberterrorism from other forms of terror. After all, why was cyberterrorism “invented”? Does cyberterrorism represent an advancement of traditional terrorism or an enrichment of it? By the same token, can traditional terrorism succeed in the postmodern world (i.e., one with no typical organizational structure and totally relying on the Internet, computers, and information technology), or are cyberterrorism and terrorism totally incompatible? Put it another way, what would be better: the use of cyberterrorism alone or a combination of both? No matter what, our vulnerabilities need to be recognized, whether they tend to occur more in the modern world or postmodern world. The Internet and computer networks are unquestionably bringing a major part of our lives to a few mouse clicks away.

All in all, there needs to be “continued progress towards a just and humane world order” (Swazo, 2004, p. 15). Now is the time to act. The threat posed by cyberterrorism is that it has been inadequately and insufficiently taken into account by many. Hopefully,

this in-depth analysis on cyberterrorism will make readers fully cognizant of its reality and growing potential.

References

Archick, K. (2003). Cybercrime: The council of Europe convention. In J. V. Blane (Ed.), *Cybercrime and cyberterrorism* (pp. 1-6). Hauppauge, NY: Novinka Books.

Arquilla, J., Ronfeldt, D., & Zanini, M. (1999). Networks, netwar and information-age terrorism. In I. O. Lesser, B. Hoffman, J. Arquilla, D. F. Ronfeldt, M. Zanini, & B. M. Jenkins (Eds.), *Countering the new terrorism* (pp. 39-88). Santa Monica: RAND.

Baring-Gould, S. (2009). *Sams Teach Yourself Cocoa Touch Programming in 24 hours*. Indianapolis: Sams.

Bavelas, A. (1950). Communication patterns in task-oriented groups. *Journal of the Acoustical Society of America, 22*, 725-730.

Benford, G. (1998). A scientist's notebook. *Fantasy & Science Fiction, 95*, 117-128.

Berger, A. (1989). *Signs in contemporary culture*. Salem, WI: Sheffield.

Blomfield, A. (2007, May 18). Estonia calls for NATO cyber-terrorism strategy. *Telegraph*, p. A1.

Britz, M. (2004). *Computer forensics and cyber crime*. Upper Saddle River, NJ: Prentice Hall.

Calder, A., & Watkins, S. (2008). *It governance: A manager's guide to data security and ISO 27001 / ISO 27002*. Philadelphia, PA: Kogan Page.

Carriço, L., Baloian, N., & Fonseca, B. (2009). *Groupware: Design, implementation, and use*. New York: Springer.

Carter, D., & Katz, A. (1996). Computer crime. *FBI Law Enforcement Bulletin, 4*, 1-8.

Clem, A., Galwankar, S., & Buck, G. (2003). Health Implications of cyber-terrorism. *Prehospital and Disaster Medicine, 18*(3), 272-275.

Collin, B. (1996). *The future of cyberterrorism*. Proceedings of 11th Annual International Symposium on Criminal Justice Issues: The University of Illinois at Chicago.

Conway, M. (2002). What is cyberterrorism? *Current History, 2*, 436-440.

Denning. D. E. (2000). *Information warfare and security*. Boston: Addison-Wesley.

Docter, Q., Dulaney, E., & Skandier, T. (2009). *CompTIA A+ Complete Deluxe Study Guide: Exams 220-701*. New York: Sybex.

Dunnigan, J. F. (2003). *The next war zone: Confronting the global threat of cyberterrorism*. New York: Citadel Press.

Farnen, R. F. (1990). Terrorism and the mass media: A systematic analysis of a symbiotic process. *Terrorism, 13*, 99-143.

Fiske, J. (1982). *Introduction to communication studies*. New York: Methuen.

Greenberg, A. (2008, May 14). When cyber terrorism becomes state censorship. *Forbes*.

Guttman, H. M. (2008). *Great business teams: Cracking the code for standout performance*. New York: Wiley.

Hanlon, M. (2007, May 24). Attack of the cyber terrorists. *Daily Mail*, p. A1.

Howard, R. (2009). *Cyber fraud: Tactics, techniques and procedures*. Auerbach: New York.

Janczewski, L. J., & Colarik, A. M. (2007). *Cyber warfare and cyber terrorism*. Hershey, PA: Idea Group Publishing.

Kisielnicki, J. (2008). *Virtual technologies: Concepts, methodologies, tools, and applications*. Hershey, PA: Information Science Reference.

Kouri, J. (2005, November 18). FBI strategy plan predicts large scale computer attacks. *American Chronicle*, p. A2.

Leavitt, H. J. (1951). Some effects of certain communication patterns on group performance. *Journal of Abnormal and Social Psychology, 46*, 38-50.

Lenzner, R., & Vardi, N. (2004). The next threat. *Forbes, 174*(5), 70-81.

Luskin, B. J. (1996). Toward an understanding of media psychology. *T H E Journal, 23*, 82-85.

Matusitz, J. (2008). Postmodernism and networks of cyberterrorists. *Journal of Digital Forensic Practice, 2*(1), 17-26.

Matusitz, J., & O'Hair, D. (2008). The role of the internet in terrorism. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and rhetorical perspectives* (pp. 383-407). Cresskill, NJ: Hampton Press.

Mcdermott, T. (2005). *Perfect soldiers – The 9/11 hijackers: Who they were, why they did it*. New York: HarperCollins.

McKenzie, W. (2004). *Hacker manifesto*. Cambridge: Harvard University Press.

Miller, C., Matusitz, J., O'Hair, D., & Eckstein, J. (2008). The role of communication and the media in terrorism. In D. O'Hair, R. Heath, K. Ayotte, & G. R. Ledlow (Eds.), *Terrorism: Communication and rhetorical perspectives* (pp. 43-66). Cresskill, NJ: Hampton Press.

Milone, M. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology, & Policy, 16*(1), 75-103.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Indianapolis: Wiley Publishing, Inc.

Nöth, W. (1995). *Handbook of semiotics*. Bloomington, IN: Indiana University Press.

O'Hair, D., & Heath, R. (2005). Conceptualizing communication and terrorism. In D. O'Hair, R. Heath, & J. Ledlow (Eds.), *Community preparedness, deterrence, and response to terrorism: Communication and terrorism* (pp. 1-12). Westport, CT: Praeger.

Robb, J., & Fallows, J. (2007). *Brave new war: The next stage of terrorism and the end of globalization*. New York: Wiley.

Schmid, A. P. (1984). *Political terrorism: A research guide to concepts, theories, data bases, and literature*. Amsterdam: Transaction Books.

Schwartau, W. (1996). *Cyberterrorism: Protecting your personal security in the electronic age*. New York: Thunder's Mouth Press.

Schwartau, W. (2000). *Cybershock: Surviving hackers, phreakers, identity thieves, internet terrorists and weapons of mass disruption*. New York: Thunder's Mouth Press.

Sebeok, T. A. (1994). *Signs: An introduction to semiotics*. Toronto: University of Toronto Press.

Swazo, N. K. (2004). Primacy or world order? The new Pax Americana. *International Journal on World Peace, 21*(1), 15-37.

Thornburgh, N., Forney, M., Bennett, B., Burger, T. J., & Shannon, E. (2005). The invasion of the Chinese cyberspies (and the man who tried to stop them). *Time, 166*(10), 34-39.

Tuman, J. S. (2003). *Communicating terror: The rhetorical dimensions of terrorism*. Thousand Oaks, CA: Sage Publications.

Vegh, S. (2002). Hacktivists or cyberterrorists? The changing media discourse on hacking. *First Monday, 7*(10), 12-25.

Verton, D. (1999, May 3). New cyberterror threatens AF. *Federal Computer Week*, p. A1.

Verton, D. (2003). *Black ice: The invisible threat of cyber-terrorism*. New York: McGraw-Hill.

Wacks, R. (2008). *Law: A very short introduction*. New York: Oxford University Press.

Wall, D. (2001). *Crime and the Internet*. London: Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age*. New York: Polity.

Zepp, C. (1999). Virtuality community: Hackers. *Sociology and the Internet, 4*(3), 1-14.

Appendix A

What Tools Do Cyberterrorists Like to Use?

More surprisingly, examples of cyberterror on computers and the Internet are as simple as malicious software such as computer viruses, Trojan horses, vampires, logic bombs, computer network worms, and DOS attacks.

Virus: a computer virus is a software program that can copy itself (Schwartau, 2000). By self-replicating, it is oftentimes capable to cause massive harm to files or other programs on the same computer. A virus "attaches itself to a legitimate program or document (for example, a Microsoft macro virus is embedded in word processing or spreadsheet files)" (Schwartau, 2000, p. 8). Yet, a virus cannot propagate to another computer without human intervention. A computer virus acts in a way that resembles a biological virus: it proliferates by putting itself into living cells. Not all viruses that target our computer systems are harmful; some are in fact innocuous. Sadly, though, we rarely see those (Dunnigan, 2003). And to show how devastating a computer virus can be, it might be interesting to remind ourselves of the cyberterrorist attempt against the Houston 911 system for widespread disruption. Fortunately, the attempt to send a computer virus failed. Had the virus been successfully activated, it would have had a ripple effect (the possibility was that each infected computer propagated over 2,500 computers simultaneously). It would also have erased the infected computer's hard drive on the nineteenth of the month, creating in effect a massive DOS attack against the 911 emergency system (Verton, 2003).

Trojan horse: a Trojan horse is not a virus; yet, a virus might include a Trojan horse (Schwartau, 2000). A Trojan horse is a software application where users are misled into installing a program that is replete with infected documents. This program is to be downloaded, for instance, through clever e-mails. To make the trick even more realistic, such e-mails sometimes appear to come from friends or colleagues. In other words, a Trojan horse is masqueraded as another legitimate program (Dunnigan, 2003). The goal of the cyberterrorist is to damage the victim's computer or files (Mitnick & Simon, 2002). According to an article entitled "Britain Warns of Trojan Horse Computer Attacks" (2005), central government computers have been the most usual targets of Trojan horses. Corporations and individuals are also at risk, based on a warning given by the British National Infrastructure Security Coordination Center (NISCC). The aim of cyberterrorists appears to be covert gathering and sending of commercially or economically valuable information. In many cases, as Mitnick and Simon (2002) put it, "the reason this technique [sending a Trojan horse] is so effective is that it follows the

theory of killing two birds with one stone: The ability to propagate to other unsuspecting victims, and the appearance that it originated from a trusted person" (p. 96).

Worm: a worm is a type of virus that slowly moves around from computer to computer and, then, slows things down. A worm tends to eat through and at resources (Schwartau, 2000), and does not attach itself to other programs (Dunnigan, 2003).

Logic bomb: it is a hidden software program in a computer system that is executed when certain conditions are met. At that point, what follows is that the program does something usually bad (Dunnigan, 2003). A logic bomb is an unauthorized computer code, sometimes sent by email. When activated, it looks for specific conditions or specific states of the system which triggers the perpetration of a destructive act of sabotage, deletes or corrupts data, and has other harmful effects.

DOS attack: DOS stands for denial-of-service attack; it is an attack against a computer system or network, causing a loss of service to users, usually the loss of connectivity and services by overwhelming the bandwidth of the target's network or congesting the computer-related resources of the target's system (Schwartau, 2000). DOS attacks "flood servers with so many incoming messages that the server can do nothing else but try and deal with the flood" (Dunnigan, 2003, p. 209).

Zombie: sometimes called "bot" or "robot," a zombie is a system that has been taken over using Remote Control Software. In many cases, a zombie is used to send spam or to attack remote servers with an overwhelming amount of traffic. It also enables the cyberterrorist to have easy access to the intruded computer, to launch attacks from that computer, to delve into password-protected chat rooms, and get into the storage for the invader's files (Dunnigan, 2003). A zombie, however, is more likely to be discovered and cleaned out if stored in professionally run Web sites (Dunnigan, 2003).

Vampire: a worm or a virus of which the sole purpose is to run so profusely that the infected computer cannot do anything else. To be more precise, after the vampire starts running, it begins to replicate itself, to such an extent that the victim's server is so active running hundreds of copies of the vampire that it can do nothing else (Dunnigan, 2003). As one can imagine, vampires pose a threat to Internet software and, when activated, they constitute a chance for the cyberterrorists to strike.

The importance of listing and defining those cyberweapons lies in the very fact that they can be used by nasty individuals "to shut down computers, destroy data, and damage the nation's power plants, factories, fuel supplies, communications systems, and even parts of the armed forces" (Dunnigan, 2003, p. 5). Now, it might be interesting to know what tools can be used for protection against cyberterrorism.

Jonathan Matusitz, **Ph.D.**, is an Assistant Professor in the Nicholson School of Communication at the University of Central Florida. Born and raised in Belgium, he earned a B.A. in Translation of Foreign Languages at the International Interpreters' School in Mons (Belgium). In 2000, he moved to the United States and pursued an M.A. in Professional Communication at the University of Alaska Fairbanks. In 2006, he earned a Ph.D. in Communication at the University of Oklahoma. He has published over 45 academic journal articles on communication and globalization, pop culture, and health communication (e.g., in *The International Journal of Strategic Communication* and *The Journal of Information Technology Impact*).

Gerald-Mark Breen, **Ph.D.**, is a Research Associate in the Public Affairs Department at the University of Central Florida. Born in Chicago, he earned a B.A. in Psychology and another B.A. in Criminal Justice at the University of Alaska Fairbanks. He earned an M.A. in Communication at the University of Oklahoma and a Ph.D. in Public Affairs at the University of Central Florida. He specializes in media studies, health communication,

social policy, and organizational communication. He has published three books and about 40 academic articles (e.g., *Health Communication* and *The Journal of Information Technology Impact*).