Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 3 Issue 12, December - 2016

Cyberterrorism

Matthew N. O. Sadiku
Electrical & Computer Engineering Dept.
Prairie View A&M University
Prairie View, TX 77446
United States

Adebowale E. Shadare
Electrical & Computer Engineering Dept.
Prairie View A&M University
Prairie View, TX 77446
United States

Sarhan M. Musa
Engineering Technology Department
Prairie View A&M University
Prairie View, TX 77446
United States

Cajetan M. Akujuobi
Office of the Vice President for Research
and Dean of Graduate School
Prairie View, TX 77446
United States

***Abstract*—Cyberterrorism is a premeditated criminal act by agents against information systems to inflict terror and panic. It is a threat to national security and a risk to public safety. It is the use of the Internet for terrorism. It is a pressing security issue facing the U.S. and its allies. This paper introduces the concept of cyberterrorism.**

Keywords—cyberterrorism, cyber security, cyber crime, cyberwar, information warfare

I. INTRODUCTION

The terrorist attacks of September 11, 2001 caught the U.S. by surprise. These attacks on U.S. and those in London and Spain have brought terrorism to a global awareness. Terrorism is the premeditated use of violence against persons to achieve one's objective. It is to coerce a person, a group or a government. Terrorists are often violent extremists who are passionate and determined to achieve their goals and are willing to lose their lives. The most widely used weapons of attack throughout the world are explosives.

In addition to warfare on land, sea, and air, cyberspace has emerged as the new battle field. Cyberspace is a borderless and unique environment. It consists of millions of fiber optic cables connecting computers, servers, routers, and gateways. Its security is an international challenge. The level of sophistication needed to attack cyberspace has decreased dramatically.

II. PROBLEM OF CYBERTERRORISM

Cyberterrorism is the convergence of terrorism and cyberspace. It involves the use of the Internet as both enabler and support mechanism. It has the potential of creating a postmodern state of chaos. It uses computer resources to intimidate or harm or disrupt critical infrastructures such as power grid, transportation, oil and gas, banking and finance, water, and emergency services [1]. Cyberterrorism has the potential to create a postmodern state of chaos, which may refer to a state of extreme disorder and confusion. Cyberterrorists could launch an attack on hospitals, destroying lives, their peacemakers and life-support machines. They could also attack the military, destroying their communications systems [2]. If the target is not critical infrastructure, the attack is not regarded as cyberterrorism. In order to qualify as cyberterrorism, it must occur in cyberspace and use some computer network to carry out the attack [3]. Cyberterrorism is categorized as shown in the Figure 1.

Terrorists are able to cause harm by using several tactics such as fraud, email floods, viruses,Trojans, worms, spam, phishing, identity theft, spyware, and denial-of-service attacks. Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, is credited with coining the word "cyberterrorism" as the combination of cyberspace and terrorism in the 1980s [4]. This form of terrorism is not housed in our country. Although there are known non-Islamic terror groups, cyberterrorism is unequivocally focused on Islamic terrorist actors. For example, Al-Qaeda terrorist groups, who were responsible for the 9/11 attacks, employ computer networks in their operations.

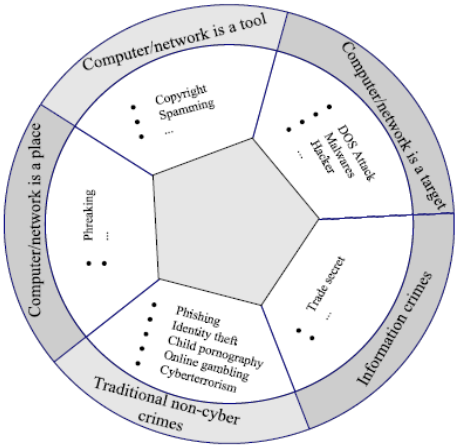

Figure 1. Categorization of cyber crimes [7].

III. PREVENTING CYBERTERRORISM

The term cyberterrorism has been overused and misused. It is an intimidating issue that provokes fear: the fear of technology and the fear of terrorism. Cyber attacks are increasing as Internet is becoming more and more attractive to attackers [5].

Government officials and other professionals often claim that the world is unprepared for cyberterrorism. But what can be done to stop it? Preventives should limit the damaged caused by network intrusions. It should be effective in blocking many forms of cyberterrorism [6]. Critical networks, such sensitive military systems and computer networks for CIA and FBI, are not physically connected to the Internet, making them immune to cyber attack.

With the growth in cyber usage, cyber crime is challenging law enforcement agencies. Although crimes are unavoidable in modern world, they can be minimized through laws, regulations, law enforcement agencies, international cooperation, etc. However, there are no laws to protect users from cyber attacks. Since attacks can happen any day to anyone, we should have basic preparation to protect ourselves. Awareness is perhaps the best defense [7]. Preparedness must begin at the local level since local agents such as the police and military bases will be the first to arrive at the scene of attack and respond to terrorism.

There must be a public education program to let people be aware of cyber threats. Security awareness programs serve as effective countermeasures against cyberterrorism. Also, the private industry must willingly share information with the FBI.

IV. BENEFIT AND CHALLENGES

Cyberterrorism has at least four tactical advantages for the attackers [8-10]. First, using cyber domain makes cyberterrorism less expensive than traditional terrorist tactics. Second, terrorist organizations increase their profits and develop new types of weapons. Third, it is difficult to track down the identity of terrorists. It is almost impossible to know where the attack originated. The odds of their being persecuted are low. Fourth, it can be conducted remotely and the number of potential cyber targets is enormous.

One challenge is defending all critical infrastructures. Traditional security strategies, such as encryption, firewalls, and contingency planning, are not enough to defend critical infrastructure. Computing professionals need to be aware of the whole gamut of vulnerabilities. An effective defense will require a concerted effort from the government and business executives.

Although there is a risk to every size of businesses, high-profile businesses are susceptible to a terrorist attack because people would hear about the attack. Such businesses include IBM, GM, WalMart, GE, and Microsoft [11].

V. CONCLUSION

Cyberterrorism is the term used for terrorists who use Internet to communicate and wreak havoc and paralyze nations. It now ranks with other weapons of mass destruction and weapons of mass disruption in the public awareness. There has been a growing volume of literature suggesting that a cyber attack is imminent. There is a large gap between the presumed threat and reality. Although the U.S. has experienced hundreds of cyber attacks, none of them rose to the level of cyberterrorism. The U.S. Department of Homeland Security recognizes that cyberterrorism is a serious issue. Although cyberterrorism is yet to occur in the U.S., terrorists groups in Sri Lanka and Japan have used cyber attacks against their own governments.

How real is the cyberterrorism threat? Is U.S. vulnerable to cyberterrorism? Waiting for a perceived disaster may be a dangerous strategy. Maybe by preparedness, we have persuaded potential attackers to avoid some courses of action in their own interest. Cyberterrorists can be deterred to some extent. Deterrence activities can lessen the likelihood of cyberterrorism. There is reason for concern but not panic. Fight against cyberterrorism is a continuous struggle.

REFERENCE

[1] J. Matusitz, “Cyberterrorism: Postmodern state of chaos,” *Information Security Journal: A Global Perspective*, vol. 17, no. 4, 2007, pp. 179-187.

[2] A. M. S. Parker, “Cyberterrorism: the emerging worldwide threat,” in D. Canter (ed.), *The Faces of Terrorists: Multidisciplinary Perspectives*, John Wiley & Sons, 2009, pp. 245-255.

[3] N. Ayres and L. A. Maglaras, “Cyberterrorism targeting the general public through social media,” *Security and Communication Networks*, vol. 9, 2016, pp. 2864-2875.

[4] A. M. S. Parker, “Cyberterrorism: an examination of the preparedness of North Carolina local law enforcement,” *Security Journal*, vol. 23, 2010, pp. 159-173.

[5] A. Embar-Seddon, “Cyberterrorism: Are we under siege?” *American Behavioral Scientist*, vol. 45, no. 6, Feb. 2002, pp. 1033-1043.

[6] C. B. Foltz, “Cyberterrorism, computer crime, and reality,” *Information Management & Computer Security*, vol. 12, no. 2, 2004, pp. 154-166.

[7] Y. Zhang et al., “A survey of cyber crimes,” *Security and Communication Networks*, vol. 5, 2012, pp. 422-437.

[8] J. J. Klein, “Detering and dissuading cyberterrorism,” *Journal of Strategic Security*, vol. 8, no. 4, Winter 2015, pp. 23-38.

[9] A. Atalay and G. Sanci, "Cyberterrorism and Turkey's counter-cyberterrorism efforts," *Information & Security: an International Journal*, vol 32, 2015, pp. 3203-2-3203-23.

[10] G. Weimann, "Cyberterrorism: the sum of all fears?" *Studies in Conflict and Terrorism*, vol. 28, no. 2, 2005, pp. 129-149.

[11] T. Singleton and A. Singleton, "Cyberterrorism: are you at risk?" *The Journal of Corporate Accounting and Finance*, 2004, pp. 3-12.

ABOUT THE AUTHORS

Matthew N.O. Sadiku (sadiku@ieee.org) is a professor in the Department of Electrical and Computer Engineering at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Adebowale Shadare (shadareadebowale@yahoo.com) is a doctoral student at Prairie View A&M University, Texas. He is the author of several papers.

Sarhan M. Musa (smmusa@pvamu.edu) is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.

Cajetan M. Akujuobi (cmakujuobi@pvamu.edu) is the vice-president for research and dean of graduate school at Prairie View A&M University, Texas. He is the author of two books and several papers.