ISSN 2278-8808 SJIF 2014 = 4.889
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

LINKAGES BETWEEN CYBER TERRORISM AND NATIONAL SECURITY

Sanju Chaudhary

Asstt. Prof. In Computer Science F.G.M. Govt. College , Adampur

Abstract

During the history of mankind, there have been many events and dangers that threaten the security of states. Those threats caused heavy loss of life, the spread of disease, injuries, destruction of public and private property, displacement of large numbers of people and heavy economic losses. Political unrest on international and local levels, and recent technological developments, are elements that would increase the seriousness of threats against national security.

1. *The concept of security has evolved gradually, especially after a major international transformation: the disintegration of Soviet Union, the end of the Cold War. Thus, it has left behind the impact of the policy of the bipolar world, which gave a blurred image of relations between the states, and made it ambiguous. However, it has given an opportunity to them to understand and identify new threats and emerging conflicts, in addition to many unsolved problems. Simultaneously, globalisation has changed the international rules and norms, in order to facilitate the rapid flow of capital and technology, through the weakening of national barriers. Non-governmental actors have come to play an essential role in international politics, some of them a threat, and others to bridge the gap between communities and nations. In such circumstances, the role of the state began to suffer from the changes; also the accepted traditional concept of power was opposed.*

2 . *Today there is no issue of such concern worldwide, and arousing such a high degree of hot debate at both national and international levels, as terrorism-related issues. The threat of terrorism has never been a prominent as it seems to be at the present time. Terrorism is an old phenomenon that has existed since the emergence of human societies. However, the threat of terrorism has increased steadily over the past 30 years. With the technological and* *technical progress in various areas, the actions of terrorists have become more dangerous and destructive, as the perpetrators of such acts are becoming more elusive. There are few parts of the world that have been left out of the current waves of terrorism, which started in the late 1960s.*

Introduction

The threat posed by cyber terrorism has grabbed the attention of the mass media, the security community, and the information technology (IT) industry. Journalists, politicians, and experts in a variety of fields have popularized a scenario in which sophisticated cyber terrorists electronically break into computers that control dams or air traffic control systems, wreaking havoc and endangering not only millions of lives but national security itself. And yet, despite all the gloomy predictions of a cyber-generated doomsday, no single instance of real cyber terrorism has been recorded. Just how real is the threat that cyber terrorism poses?Because most critical infra-structure in Western societies is networked through computers, the potential threat from cyber terrorism is, to be sure, very alarming. Hackers, although not motivated by the same goals that inspire terrorists, have demonstrated that individuals can gain access to sensitive information and to the operation of crucial services. Terrorists, at least in theory, could thus follow the hackers' lead and then, having broken into government and private computer systems, cripple or at least disable the military, financial, and service sectors of advanced economies. The growing dependence of our societies on information technology has created a new form of vulnerability, giving terrorists the chance to approach targets that would otherwise be utterly unassailable, such as national defence systems and air traffic control systems. The more technologically developed a country is, the more vulnerary-able it becomes to cyber attacks against its infrastructure. Concern about the potential danger posed by cyber terrorism is thus well founded. That does not mean, however, that all the fears that have been voiced in the media, in Congress, and in other public forums are rational and reasonable. Some fears are simply unjustified, while others are highly exaggerated. In addition, the distinction between the potential and the actual dam-age inflicted by cyber terrorists has too often been ignored, and the relatively benign activities of most hackers have been conflated with the sectors of pure cyber terrorism. This report examines the reality of the cyber terrorism threat, present and future. It begins by outlining why cyber terrorism angst has gripped so many people, defines what qualifies as "**cyberterrorism**" and what does not,

About The Institute

The United States Institute of Peace is an independent, nonpartisan federal institution created by Congress to promote the prevention, management, and peaceful resolution of international conflicts. Established in 1984, the Institute meets its congressional mandate through an array of programs, including research grants, fellow-ships, professional training, education programs from high school through graduate school, conferences and workshops, library services, and publications. The Institute's Board of Directors is appointed by the President of the United States and confirmed by the Senate.

Board Of Directors

J. Robinson West (Chair), Chairman, PFC Energy, Washington, D.C.• María Otero(Vice Chair), President, ACCION International, Boston, Mass. • Betty F. Bumpers, Founder and former President, Peace Links, Washington, D.C. • Holly J. Burkhalter, Advocacy Director, Physicians for Human Rights, Washington, D.C. • Chester A. Crocker, James R. Schlesinger Professor of Strategic Studies, School of Foreign Service, Georgetown University • George Mason University • Mora L. McLean ,President, Africa-America Institute, New York, N.Y. • Daniel Pipes, Director, Middle East Forum, Philadelphia, Pa. • Barbara W. Snelling, former State Senator and former Lieutenant Governor, Shelburne, Vt. MEMBERSEXOFFICIO Arthur E. Dewey, Assistant Secretary of State for Population, Refugees, and Migration • Michael M. Dunn, Lieutenant General, U.S. Air Force; President, National Defense University •Peter W. Rodman, Assistant Secretary of Defence for International Security Affairs Richard H. Solomon ,President, United States Institute of Peace (nonvoting)Psychological, political, and economic forces have combined to promote the fear of cyber terrorism. From a psychological perspective, two of the greatest fears of modern time are combined in the term cyber terrorism." The fear of random, violent victimiza-tion blends well with the distrust and outright fear of computer technology. An unknown threat is perceived as more threatening than a known threat. Although cyber terrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the effect of terrorist bombs. Moreover, the most destructive forces working against an understanding of the actual threat of cyber terrorism are a fear of the unknown and a lack of information or, worse, too much misinformation. After 9/11, the security and terrorism discourse soon featured cyber terrorism promi-nently. This was understandable, given that more nightmarish attacks were expected and damage. But there was also a political dimension to the new focus on cyber terrorism. Debates about national security, including the security of cyberspace, always attract political actors with agendas that extend beyond the specific issue at hand—and the debate over cyberterrorism was no exception to this pattern. For instance, Yonah Alexander, a terrorism researcher at the Potomac Institute—a think tank with close links to the Pentagon—announced in December 2001 the existence of an "Iraq Net." This network supposedly consisted of more than one hundred websites set up across the world by Iraq since the mid-nineties to launch denial-of-service (DoS) attacks against U.S. companies (such attacks render computer systems inaccessible, unusable, or inoperable). "Saddam Hussein would not hesitate to use the cyber tool he has. . . . It is not a question of if but when. The entire United States is the front line," Alexander claimed. (See Ralf Bendrath's article "The American Cyber-Angst and the Real World," published in 2003 in Bombs and Bandwith, edited by Robert Latham.) Whatever the intentions of its author, such a state-ment was clearly likely to support arguments then being made for an aggressive U.S. policy toward Iraq. No evidence of an Iraq Net has yet come to light.Combating **cyberterrorism** has become not only a highly politicized issue but also an economically rewarding one. An entire industry has emerged to grapple with the threat of cyberterrorism: think tanks have launched elaborate projects and issued alarming white papers on the subject, experts have testified to cyberterrorism's dangers before Congress, and private companies have hastily deployed security consultants and software designed to protect public and private targets. Following the 9/11 attacks, the federal government requested $4.5 billion for infrastructure security, and the FBI now boasts more than one thousand "cyber investigators."Before September 11, 2001, George W. Bush, then a presidential candidate,warned that "American forces are overused and underfunded precisely when they are confronted by a host of new threats and challenges—the spread of weapons of mass destruction, the rise of cyberterrorism, the proliferation of missile technology." After the 9/11 attacks, President Bush created the Office of Cyberspace Security in the White House and appointed his former counterterrorism coordinator, Richard Clarke, to head it. The warn-ings came now from the president, the vice president, security advisors, and government officials: "Terrorists can sit at one computer connected to one network and can create worldwide havoc," cautioned Tom Ridge, director of the Department of Homeland Security, in a representative observation in April 2003. "[They] don't necessarily need a bomb orexplosives to cripple a sector of the economy or shut down a power grid." These warnings certainly had a powerful impact on the media, on the public, and on the administration. For instance, a survey of 725 cities conducted in 2003 by the National League of Cities found that cyberterrorism ranked alongside biological and chemical weapons at the top of a list of city officials' fears.The mass media have added their voice to the fearful chorus, running scary front-page headlines such as the following, which appeared in the Washington Post in June 2003: "Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say." Cyberterrorism, the media have discovered, makes for eye-catching, dramatic 3Psychological, political, and economic forces have combined to promote the fear of cyberterrorism. Combating cyberterrorism has become not only a highly politicized issue but also an economically rewarding one. Cyberterrorism, the media have discovered, makes for eye-catching, dramatic copy.copy. Screenwriters and novelists have likewise seen the dramatic potential, with movies such as the 1995 James Bond feature, Goldeneyeand 2002's Code Hunterand novels such as Tom Clancy and Steve R. Pieczenik's Netforce popularizing a wide range of cyberterrorist scenarios.

What Is Cyberterrorism?

There have been several stumbling blocks to creating a clear and consistent definition of the term "cyberterrorism." First, as just noted, much of the discussion of cyberterrorism has been conducted in the popular media, where journalists typically strive for drama and sensation rather than for good operational definitions of new terms. Second, it has been especially common when dealing with computers to coin new words simply by placing the word "cyber," "computer," or "information" before another word. Thus, an entire arsenal of words—cyber-crime, infowar, netwar, cyberterrorism, cyberharassment, virtual warfare, digital terrorism, cybertactics, computer warfare, cyberattack, and cyber-break-ins—is used to describe what some military and political strategists describe as the "new terrorism" of our times.Fortunately, some efforts have been made to introduce greater semantic precision. Most notably, Dorothy Denning, a professor of computer science, has put forward an admi-rably unambiguous definition in numerous articles and in her testimony on the subject before the House Armed Services Committee in May 2000:Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explo-sions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. ***Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.It is important to distinguish***

between cyberterrorism and "hacktivism," a term coined by scholars to describe the marriage of hacking with political activism. ("Hacking" is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. Unlike hacktivists, hackers tend not to have political agendas.) Hacktivists have four main weapons at their disposal: virtual blockades; e-mail attacks; hacking and computer break-ins; and computer viruses and worms.A virtual blockade is the virtual version of a physical sit-in or blockade: political activ-ists visit a website and attempt to generate so much traffic toward the site that other users cannot reach it, thereby disrupting normal operations while winning publicity—via media reports—for the protesters' cause. "Swarming" occurs when a large number of individuals simultaneously access a website, causing its collapse. Swarming can also amplify the effects of the hacktivists' second weapon: e-mail bombing campaigns (bombarding targets with thousands of messages at once, also known as "ping attacks"). Maura Conway reported in her essay "Reality Bytes" (First Monday 7, no. 11 [November 2002]) on an e-mail bombing campaign launched in July 1997 against the Institute for Global Com-munications (IGC), a San Francisco–based Internet service provider (ISP) that hosted the web pages of Euskal Herria(in English, the Basque Country Journal), a publication edited 4 It is important to distinguish between cyberterrorismand"hacktivism," a term coined by scholars to describe the marriage of hacking with activism.by supporters of the Basque separatist group ETA. The attackers wanted ETA's site removed from the Internet. They bombarded IGC's website with thousands of e-mails, clogging the system, and threatened to attack other organizations using IGC services. IGC pulled the Euskal Herriasite just a few days later.The Spanish government was suspected of being behind the e-mail bombing, but the identity of the attackers remains uncertain. Whether or not the suspicion is well founded, it underlines the fact that the hacktivists' tools are widely available and can be as easily employed by governments as by small groups of political activists.Many cyberprotesters use the third weapon in the hacktivists' arsenal: web hacking and computer break-ins (hacking into computers to access stored information, communication facilities, financial information, and so forth).

Denning notes that the Computer Emergency Response Team Coordination Center (CERT/CC), a federally funded research and development center operated by Carnegie Mellon University, reported 2,134 cases of computer break-ins and hacks in 1997. The number of incidents rose to 21,756 in 2000 and to almost 35,000 during the first three quarters of 2001 alone. In 2003, CERT/CC received more than half a million e-mail messages and more than nine hundred hotline calls reporting incidents or requesting information. In the same year, no fewer than 137,529 computer security incidents were reported. Given that many, perhaps most, incidents are never reported to CERT/CC or any agency or organization, the actual figures are probably much higher. Moreover, Denning notes that each single incident that is reported involves thousands of victims. This rise in cyberattacks reflects the growing popularity of the Internet, the vast number of vulnerable targets, and the development of sophisticated and easy-to-use hacking tools.The fourth category of hacktivist weaponry comprises viruses and worms, both of which are forms of malicious code that can infect computers and propagate over com-puter networks. Their impact can be enormous. The Code Red worm, for example, infected about a million servers in July 2001 and caused $2.6 billion in damage to computer hard-ware, software, and networks, and the I LOVE YOU virus unleashed in 2000 affected more than twenty million Internet users and caused billions of dollars in damage. Although neither the Code Red worm nor the I LOVE YOU virus was spread with any political goals in mind (both seem to have been the work of hackers, not hacktivists), some computer viruses and worms have been used to propagate political messages and, in some cases, cause serious damage. During the NATO operation to evict Serbian forces from Kosovo, businesses, public entities, and academic institutes in NATO member-states received virus-laden e-mails from a range of Eastern European countries. The e-mail messages, which had been poorly translated into English, consisted chiefly of unsubtle denuncia-tions of NATO for its unfair aggression and defenses of Serbian rights. But the real threat was from the viruses. This was an instance of cyberwarfare launched by Serbian hacktivists against the economic infrastructure of NATO countries.In February 2000, the sites of Amazon.com, e-Bay, Yahoo, and a host of other well-known companies were stopped for several hours due to DoS attacks. On October 22, 2002, the Washington Postreported that “the heart of the Internet network sustained its largest and most sophisticated attack ever.” During the NATO operation to evict Serbian forces from Kosovo,businesses, public entities, and academic institutes in NATO member-states received virus-laden e-mails from a range of Eastern European countries.Hacktivism, although politically motivated, does not amount to cyber terrorism.

The Appeal of Cyber terrorism for Terrorists

Cyber terrorism is an attractive option for modern terrorists for several reasons.

• First, it is cheaper than traditional terrorist methods. All that the terrorist needs is a personal computer and an online connection. Terrorists do not need to buy weapons such as guns and explosives; instead, they can create and deliver computer viruses through a telephone line, a cable, or a wireless connection.

• Second, cyberterrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nicknames—"screen names"—or log on to a website as an unidentified "guest user," making it very hard forsecurity agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers such as checkpoints to navigate, no borders to cross, and no customs agents to outsmart.

• Third, the variety and number of targets are enormous. The cyberterrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth. The sheer number and complexity of potential targets guarantee that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emer-gency services, are vulnerable to a cyberterrorist attack because the infrastructures and the computer systems that run them are highly complex, making it effectively impossible to eliminate all weaknesses.

• Fourth, cyberterrorism can be conducted remotely, a feature that is especially appeal-ing to terrorists. Cyber terrorism requires less physical training, psychological invest-ment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retain followers.• Fifth, as the I LOVE YOU virus showed, cyberterrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

Cyberterrorism

Cyberterrorism is the use of Internet attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Cyber terrorism is a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyber terrorism.

Cyber terrorism can be also defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives Objectives may be political or ideological since this can be seen as a form of terrorism.

There is much concern from government and media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies.

References

Matusitz, Jonathan (April 2005). "Cyber terrorism:". American Foreign Policy Interests ***2****: 137–147.*

"India Quarterly : a Journal of International Affairs". 42-43. Indian Council of World Affairs. 1986. p. 122. The difficulty of defining terrorism has led to the cliche that one man's terrorist is another man's freedom fighter

What is ***cyberterrorism?*** *Even experts can't agree at the Wayback Machine (archived November 12, 2009). Harvard Law Record. Victoria Baranetsky. November 5, 2009.*

"Latest viruses could mean 'end of world as we know it,' says man who discovered Flame", The Times of Israel, June 6, 2012

"Cyber espionage bug attacking Middle East, but Israel untouched — so far", The Times of Israel, June 4, 2013

Harper, Jim. "There's no such thing as cyber terrorism". RT. Retrieved 5 November 2012.

Afroz, Soobia (June 16, 2002). "Cyber terrorism — fact or fiction?". Dawn. Retrieved 2008-08-30.

Cyber terrorism National Conference of State Legislatures.

Gable, Kelly A. "Cyber-Apocalypse Now: Securing the Internet against Cyber terrorism and Using Universal Jurisdiction as a Deterrent" Vanderbilt Journal of Transnational Law, Vol. 43, No. 1

Anderson, Kent (October 13, 2010). "Virtual Hostage: Cyber terrorism and politically motivated computer crime". The Prague Post. Retrieved 2010-10-14.

"Top 10 events that may end the human race". Yahoo News. Oct 27, 2010. Retrieved 2010-11-01.

Perlroth, Nicole; Sanger, David E. (28 March 2013). "Corporate Cyber attacks, Possibly State-Backed, Now Seek to Destroy Data". The New York Times.

"White House shifts Y2K focus to states, CNN (Feb. 23, 1999)". CNN. 23 February 1999. Retrieved 25 September 2011.

Chabrow, Eric. Obama Cyber security Coordinator Resigns. GovInfoSecurity.com, May 17, 2012. Accessed: Feb. 11, 2014.