INDIAN BAR REVIEW

Vol. 45 (1) 2018

[A Referred Journal]

Editor

VIJAY BHATT

Joint Editor

PRATAP MEHTA

BAR COUNCIL OF INDIA TRUST

NEW DELHI

INDIAN BAR REVIEW

Vol. 45 (1) 2018

[A Referred Journal]

Editor

VIJAY BHATT

Joint Editor

PRATAP MEHTA

BAR COUNCIL OF INDIA TRUST

NEW DELHI

Published by :

Bar Council of India Trust
21, Rouse Avenue Institutional Area
New Delhi-110002
Tel : 91-11-49225045, 49225000
Fax : 91-11-49225011
E-mail : trustbci@gmail.com

Annual Subscription : ₹ 16,000/- (including postage)

TIMES PRESS
23273252

INDIAN BAR REVIEW

VOLUME 45 **JANUARY - MARCH 2018** **NUMBER 1**

CONTENTS

ARTICLES

CYBER TERRORISM : WAR AGAINST THE SECURITY OF THE STATE

Dr. Jayasanakar K.I.*

INTRODUCTION

There are many forms of terrorism on the Internet. Some are not dangerous enough to be deemed a simple spread of information instead of terrorism. They are simple show of skill and are harmless.[1] But the use of information systems, electronic networks, and the entire information technology are playing vital roles in changing the environment dramatically in last decade in expanding and linking all social sectors. Those changes brought significant benefits to individual citizens and to the financial, industrial, business, academic, and service sectors. But, the reliable and safe operation of the myriad of technological solutions, information systems, and support infrastructure requires that far-reaching concerns about security issues should be effectively addressed by governments, business concerns, organizations, and individual users who develop, own, provide, manage, service, and use those information systems, resources, and networks.

It is seemed that the modern civil societies, particularly the advanced developed countries, are mainly depended up on information technologies and systems. But at the same time they themselves turned into another area for illegal activity as criminals and criminal organizations learned to take advantage of information technology for illegal purposes and for indiscriminate violence against civilians and civil institutions with the

---

* Assistant Professor, Department of Law, Central University of Kerala.

1. Saint-Claire S. - 'Overview and Analysis on Cyber Terrorism', School of Doctorial Studies (European Union) Journal-2011.

purpose of causing confusion and unrest, and destroying their faith on leaders, policies, and institutions. Government agencies and military organizations have waged electronic war operations against military institutions and well-defined targets of military tactical or strategic importance. The researcher attempts to make a probe into the impact of cyber terrorism on the security of the state in the modern world the issues which are to be addressed in the present context.

CYBER TERRORISM IN HISTORY

The roots of the idea of cyber terrorism can be traced back to the early 1990s, when the rapid growth in Internet use and the debate on the emerging "information society" generated several studies on the potential risks faced by the highly networked, hightech- dependent USA.

Only in the past decade cyber security threats have surfaced worldwide. Specific targets of cyber terrorism consist of critical infrastructures including transportation, electric power grids, oil and gas distribution, telecommunications, air traffic, and financial institutions. In February 2000, a distributed denial of service attack (DDoS) was launched on popular Internet sites Yahoo, Amazon, e-Bay, CNN, e-Trade, ZDNet, and Datek. Millions of people were unable to access services provided by these companies, resulting in monetary loss and a decline in the sense of security previously offered by these top-tier Web sites.[2] While the focus on the following year became physical terrorism (9/11), an incident involving China and the U.S. in April 2001—the collision between an American surveillance plane and a Chinese fighter aircraft—was the likely culprit that initiated a series of cyber attacks and Web site defacements between the two countries.[3] Following the September 11 attacks, combating cyber terrorism has become not only a highly politicized issue but also an economically rewarding one. An entire industry has emerged to cope with the threat of cyber terrorism: think tanks have launched elaborate projects and issued alarming white papers on the subject, and private companies deployed security consultants and software designers to protect public and private targets. The mass media have added their voice to the chorus,

2. Biegel, Stuart. Beyond Our Control? Controlling the Limits of Our Legal System in the Age of Cyber space. New York: The MIT Press, 2003.
3. Keegan, Christopher. "Cyber-Terrorism Risk." Financial Executive 18.8 (Nov. 2002): 35-37.

running scary front-page headlines, which appeared in the Washington Post in June 2002.[4]

Web site defacement became the most common and extreme visual display of cyber terrorism. It is a form of cyber terrorism because, although the aftermath may not always be violent, it does serve the purpose of intimidation with a political and/or social agenda. Politically motivated Web site defacement has occurred frequently in the past and present. Korean University students defaced Japanese Web sites to protest the content of Japanese textbooks.[5] In protest of the Japanese Prime Minister's visit to the Yasukuni Shrine, pro-Chinese hackers defaced Japanese Web sites. Additionally, the Pakistan-India conflict and the Israel Palestine conflict both involved Web site defacements.

In 2003, Romanian hackers attacked the National Science Foundation's Amundsen-Scott South Pole Station.[6] In 2007, there were several cyberattacks on Estonia, mostly DDoS attacks on police, media, financial, and government Web sites; Estonia claimed that Russia was hacking into their systems.

In August 2008, the Georgia-Russia conflict continued the pattern of Web site defacements between adversarial nations—both countries' Web sites were defaced during the period of tension over South Ossetia.[7] In early 2009, there was a report[8] that the computer systems that controlled the U.S. power grid were penetrated by foreign threats, likely Russia or China, and evidence of signature software was found. Although no monetary damage was done, the implication is inconceivable. There are many control systems (e.g., SCADA)[9] that exist today with both cyber and

4. GELLMAN, Barton: *Cyber-Attacks by Al Qaeda Feared. Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say,* http://www.washingtonpost.com/ac2/wp-dyn/A50765–2002Jun26, June 24, 2007.
5. Bronk, Chris. "Hacking the Nation State: Security, Information Technology and Policies of Assurance." Information Security Journal: A Global Perspective 17.3 (2008): 132-142.
6. "The Case of the Hacked South Pole." Federal Bureau of Investigation Headline Archives. 14 Apr. 2009 .
7. Cluley, Graham. "Conflict Between Russia and Georgia Turns to Cyber Warfare." Weblog post. Sophos. 12 Aug. 2008
8. Ghosh, Bobby. "How Vulnerable is the Power Grid?" Time. 15 Apr. 2009.
9. Supervisory Control and Data Acquisition is a system operating with coded signals over communication channels so as to provide control of remote equipment.

physical vulnerabilities and whose unauthorized control/execution/ destruction would have far-reaching effects. More recently, July 4, 2009, cyber attacks were launched at the U.S. and South Korea. The U.S. targets of the DDoS attacks included the New York Stock Exchange, Pentagon, Treasury, Secret Service, Department of Transportation, and the White House. There has been speculation that the source of the attacks was from North Korea, but there is currently no solid evidence to confirm this allegation Countries such as China, Cuba, Iran, Iraq, Libya, North Korea, Russia, Sudan, and Syria are believed to present a greater threat for potential cyberattacks than other nations.

CYBER TERRORISM DEFINED

There have been several stumbling blocks to creating a clear and consistent definition of the term "cyber terrorism." Much of the discussion of cyber terrorism has been conducted in the popular media, where journalists typically strive for drama and sensation rather than for good operational definitions of new terms. It has been especially common when dealing with computers to coin new words simply by placing the words "cyber," "computer," or "information" before another word. Thus, an entire arsenal of words—cybercrime, cyberwar, infowar, netwar, cyber terrorism, cyber harassment, virtual-warfare, digital terrorism, cybertactics, computer warfare, information warfare, cyber attack, cyberwar, and cyber break-ins—is used to describe what some military and political strategists describe as the "new terrorism" of these times.[10]

Fortunately, some effort has been made to introduce greater semantic precision. Most notably, Dorothy Denning, a professor of computer science, has put forward an admirably unambiguous definition in numerous articles,[11] and in her testimony on the subject before the congressional

10. D. Ronfeldt and J. Arquilla. "Networks, Netwars, and the Fight for the Future." *First Monday* 6(10) (2001); J. Arquilla and D. Ronfeldt. "The Advent of Netwar" (revisited) (2001). In *Networks and Netwars,* edited by J. Arquilla and D. Ronfeldt (Santa Monica: RAND Corporation), pp. 1–25).
11. D. Denning. 1999. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* (Washington, DC: Nautilus, 1999), available at (http://www.nautilus.org/info-policy/workshop /papers/denning.html); D. Denning. 2000a. Testimony before the Special Oversight Panel on Terrorism, U.S. House of Representatives, Committee on Armed Services 23 May 2000a, available at http://www.cs.georgetown. edu/denning/infoset/cyberterror.html.

House Armed Services Committee: Cyber terrorism 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 cyber terrorism, 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, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact.

WHY THE CYBER TERRORISM IS BEING ATTRACTED ?

There is every reason to believe that given the current world situation, terrorism in one form or another will continue to flourish. Most groups will continue to use traditional terrorist methods. These methods have been proven to provide the impact necessary to carry the terrorist message. For those groups that wish to expand their operational repertoire chemical, biological, radiological or nuclear weapons offer a dramatic option. The other option is cyber terror. The widespread vulnerabilities that many studies have previously identified make Cyber terrorism an attractive option by modern terrorists.[12]

There are sevreal reasons for this attraction.[13] First of all, 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.

Secondly, cyber terrorism is more anonymous than traditional terrorist methods. Like many Internet surfers, terrorists use online nick names— "screen names"— or log on to a website as an unidentified "guest user," making it very hard for security agencies and police forces to track down the terrorists' real identity. And in cyberspace there are no physical barriers

D.Denning.2000b."Cyber terrorism." *Global Dialogue* (Autumn), (2000b), available at (http://www.cs.georgetown.edu/ ~denning/infosec/cyberterror-GD.doc); Denning, op. cit.

12. Major Bill Nelson, USAF, 'Cyberterror Prospects and Implications', Center for the Study of Terrorism and Irregular Warfare Monterey, CA.
13. Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears?'*Studies in Conflict & Terrorism,* 28:129–149, 2005.

such as checkpoints to navigate, no borders to cross, no customs agents to outsmart.

Thirdly, the variety and number of targets are enormous. The cyber terrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so on. The sheer number and complexity of potential targets guarantees that terrorists can find weaknesses and vulnerabilities to exploit. Several studies have shown that critical infrastructures, such as electric power grids and emergency 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, cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists. Cyber terrorism requires less physical training, psychological investment, 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, cyber terrorism 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.

CYBER TERRORISM: A THREAT AGAINST THE NATIONAL SECURITY

Cyber terrorism is a threat to national security. It is identified as " the premeditated use of disruptive activities or the threat thereof, in cyber space, with the intention of further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objects". A cyber terrorist is a person who uses the computer system as a means or ends to achieve with various objectives It includes, putting the public or any section of public in fear, or affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities or coercing or overawing the government established by law or endangering the sovereignty and integrity of the nation.

The 21st century has been labeled as the Information Age, where civilians are being able to have unprecedented access to information. However, the information and communication technology (ICT) "revolution" has transformed the way information is used, transmitted and stored not only by the civilian population but also the state military and intelligence agencies. As a result, cyber space has been opted as the a new battlefield . Cyber-conflict and cyber-exploitation are developed as the the new threats to a state's security. And similar to a traditional kinetic conflict

(TKC), both offensive and defensive acts have been taken place in the cyber-arena.[14]

During a cyber-conflict, there are no clear lines between the civilian and military, as civilian computer systems may be used to launch offensive cyber-war against an "enemy" state. Also, the difficulty is determining the perpetrator (which could be state or non-state actors) adds to the confusion in determining the legal course of action once a cyber-attack is discovered. A spate of cyber-attacks have been reported by the media, especially in the last few years: China, Israel and the US are thought to routinely engage in cyber-conflicts with other states in order to siphon confidential business or military information (*i.e.* cyber-exploitation) or prevent/stun rival military systems from functioning properly (*i.e.* cyber-conflict).

Cyber-war is especially a serious threat to the national sovereignty and security because it transcends national borders and involves use of civilian resources. Despite stepped-up security measures in the wake of September 11, a survey conducted by Elon University and the Pew Internet & American Life Project in the fall of 2004, harvested thousands of projections of what has to come in the next decade. Participants included specialists from the Internet 2, Microsoft, Oracle, RAND, AOL, IBM, the FBI, many top universities and hundreds of government and corporate entities.[15] About two thirds (66 percent) of the IT professionals felt that a devastating attack will occur in the next 10 years on the networked information structure or country's power grid, and more than half (55 percent) believe that there will be a major attack on business via the Internet in the next 12 months. Seventy-two percent agreed with the statement "there is a gap between the threat of a major cyber attack and the government's ability to defend against it," and the agreement rate rose to 84 percent among respondents who are most knowledgeable about security.

INDIA AGAINST CYBER TERRORISM

In India, cyber terrorism has emerged as new phenomena. It has to be read with the economic environment of the country. The Indian economy is highly reliant on IT infrastructure. However, the rate of India's

14. Lin, Herbert. 2013. "Cyber Conflict and National Security." In *International Politics: Enduring Concepts and Contemporary Issues*, 11th Edition, edited by Robert Art and Robert Jervis, New York: Pearson.
15. IBM Global Services *Securing a Better Future How To Mitigate Risks, Integrated Technology Services* http://www.pewinternet.org/pdfs/PIP_Future_of_Internet.pdf, June 24, 2007.

development has far outpaced the advancement in IT infrastructure. India is putting more emphasis on the IT infrastructure in recent years, with the technology sector growing by 10.3 percent from 2011 to reach USD 2.05 billion in 2012[16] However, India is still in slow process of moving towards a more efficient model in centralizing its data centres. At the moment, these centres remain distributed and inefficient.

IT infrastructure is not only required in firms and organizations directly related to economic activity. IT is also playing an increasingly important role in households and also in government key sectors such as healthcare and education.

However, there is little support and advancement in infrastructure for these segments and other areas of India's public service.The Indians are known to be tech savvy, using a vast number of devices while harnessing various forms of technology. However, infrastructural support for its tech savvy citizens is not comprehensive. Poor cabling standards have plagued the country. This is due to a lack of awareness and understanding on industrial standards for networking and cabling

LEGISLATIVE ATTEMPT

The Government of India took strong steps to strengthen the cyber security, including prohibition of terrorist activities through cyber space by way of amending the existing Indian information Technology Act, 2000.The provision that was specifically inserted in this legislature for this purpose was section 66F which defines and describes cyber terrorism. Section 66F mentions that

(1) Whoever— (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by – (i) denying or cause the denial of access to any person authorized to access computer resource; or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or (iii) introducing or causing to introduce any Computer Contaminant. and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential

16. Daily The Pak Banker. (2012). Indian IT infra market to reach $2.05b in 2012: Gartner Daily. Retrieved September 26, 2012, from: www.lexisnexis.com

to the life of the community or adversely affect the critical information infrastructure specified under Section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'. From the above definition, it could be inferred that,

And also, Section 69 of the Information Technology Act[17] is a strong legislative measure to counter the use of encryption by terrorists. This

17. Section 69-Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (Substituted Vide ITAA 2008)
    (1) Where the Central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
    (2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(Contd. ...)

section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource[18] Any person who fails to assist the Government agency in decrypting the information[19] sought to be intercepted is liable for imprisonment up to 7 years.

CONCLUSION

We have entered an era of sustained digital attacks from radicals, criminals and cyber adventurers, who will be difficult to control and to deal with at in the 21st century, therefore securing cyberspace is a complex and growing challenge. The absolute defense against terrorism and cyber terrorism is extremely difficult. Although cyber terrorism is currently prevailing mostly in the virtual world, technological advancements make its ability to disrupt our physical world just as possible—if not even more likely. Constantly changing technology advances our quality of life but also changes the landscape of 21st century warfare. Cyberterrorism demonstrates the ability of terrorism to adapt to the modern world and shows why it is important to continue recognizing this threat by minimizing opportunities and devoting resources to its prevention.

* * *

(Contd. from previous page)

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource containing such information; generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

18. The reasons for such an order must be recorded in writing. The order can be made on the following grounds: (1) in the interest of the sovereignty or integrity of India (2) in the interest of the security of the State (3) in the interest of friendly relations with foreign States (4) for preserving public order (5) for preventing incitement to the commission of any cognizable offence .

19. The information referred to in this section would include email messages, password protected files, steganographic images, encrypted information etc.

FOREST PRESERVATION AND LAW AN APPRAISAL

Dr. Shamsher Singh*

INTRODUCTION

Forests are exigent to economic development and the maintenance of all forms of life. It maintains water cycle, preserve soil, landslides, flooding, biodiversity and medicines also. In addition to that forests are congenital recoverable resource and one of the significant assets of the state.

Today, large environmental problems, such as deforestation which is taking place in the world, because of unsustainable pattern of development, consistently degrade the trees and forests. Forests as storehouse of biodiversity are essential to both, preservation of environment and also development. Their destruction means pollution of different types, erosion of biodiversity, degradation of land, drought and desertification, floods, cyclones, depletion of energy sources, ocean and coastal resources, etc. Numbers of policies have been framed at national level for forests conservation like National Forest Policy, 1998,[1] National Conservation Strategy, Policy Statement for Abatement of Pollution and National

* Assistant Professor & Dean, Khalsa College of Law, Amritsar, Punjab.

1. This policy was established to ensure compensatory afforestation, essential environmental safeguards, sustainable utilization, maintenance, restoration, and enhancement of forest areas. It stressed that forests should meet the subsistence requirements of people and was intended to decrease degradation by forest dwellers through better management. (http://www.forestlegality.org/risk-tool/country/india, accessed on 12.12. 2017).