CYBER CRIME AND CYBER TERRORISM **(2018). By Robert W. Taylor, Erica J. Fritsch, John Liederbach, Michael R. Saylor and William L. Tafoya, Pearson, New York. Pp 434, Price: Rs.7180/-. ISBN: 978-0-13-484651-4**

A NEW era of millennials, the technology is rapidly growing so fast people are getting relied on. Information technology *i.e.,* the computer - based technology is used by the people in order to gain information, whether it is for organizations, nations or even for the individual needs. However, the information is so enormous that even the terrorist organizations used it to commit crimes *via* cyberspace (internet) which leads to havoc to various organizations as well as the nations. Terrorism is one of the most destructive menaces in a contemporary society.[1] Various efforts have been made to solve such issues, but the perpetrators are having created havoc for various organizations. There could be various reasons why terrorism has become such crucial topic whether it is unemployment or string headed motives behind it.[2] Due to rapid growth in digital technology, various terrorist organizations are misusing the social media and in order to attack the national defense system in the developed countries.[3]

Cyber terrorism is one of the most debatable topics. The word itself talks about the two ingredients which are cyberspace and terrorism. So, it is a deadly combination of digital technology and terrorism. There are numerous national and international regimes which define cyber terrorism. Cyber terrorism is one of the low cost, as it provides for secure communication for the terrorist organizations so that they can carry their terrorist activities and other operations.[4] The main purpose of cyber terrorism is to provoke the violence or fear, by the use of the computer system or programs so that they can target the huge number of audience worldwide.[5]

Cyber terrorism is the most dangerous, destructive, damaging activities that take place in the cyber space. Terrorist group organizations like *Al Qaeda* are considered as one of the most dangerous

[1] Lee Jarvis, Stuart Macdonald and Thomas M.Chen, *Terrorism Online-Politics, Law and Technology* (Routledge Publication, 2017).
[2] *Ibid.*
[3] Thomas Rid, *Cyber War will not take place* (C.Hurst and Co. Publishers Limited, 2016).
[4] Babak Akghar and Ben Brewster, *Combating Cybercrime and Cyber Terrorism: Challenges, Trends and Priorities* (Springer Publication, 2016).
[5] *Ibid.*

group.[6] Cyber attacks in which US officials' data from computers were seized in Afghanistan, denotes that terrorist groups have scouted systems which have control over their communication and other infrastructure.[7] Terrorist organizations remain active and target through the use of internet, launched attacks like Unix Security Guards (USG) which is a pro- Islamic group, Anti India Crew (AIC) which is a Pro Pakistan group launched attacks in India, other groups like World Fantabulas Defacers (WFD) also attacked many Indian sites.[8] The *modus operandi* could be various, but the advantages could be easily accessible, one of the cheapest methods to target a large number of audience, identity remains anonymous, difficulty in tracing out the location due to advanced technology.[9] Coming, to the definition, there is no universally accepted definition, but cyber terrorism has been defined by various authors consist of the same ingredients.[10] However cyber terrorism is different as compared to other computer crime or conventional crime.[11] Every computer crime does not constitute the crime of "cyber terrorism".[12]

The book under review is *Cyber crime and Cyber Terrorism* (2018) written by Robert W. Taylor, Eric J. Fritsch, John Liederbach, Michael R. Saylor and William L. Tafoya and published by Pearson Education. First edition of this book was published in 2013, another edition came in 2014 and the third edition came in 2018 which is divided into four sections. The book brings out the issue of cybercrime and cyber terrorism and it is a compilation of information warfare, various types of crimes committed through criminal hackers, digital hackers, legal strategies used to commit such acts. Apart from the legal issues it also covers technical issues as well. The book brings etiology of cyber terrorism, as the term "terrorism" is very difficult to define. The editor rightfully asserted on cyber terrorism as an adjunct attack and which covers *Al Qaeda*, the Islamic state which is quite appreciable. Section I is "The Etiology of Cyber Crime and Cyber Terrorism" Section II "Cyber Crime: Types, Nature, and Extent". Section III "Controlling Cyber Crime:

[6] *Supra* note 1.
[7] K Mani, *Legal Framework on Cybercrimes* (ITU Publication, 2012).
[8] M Das Gupta, *Cybercrime in India* (Eastern Law House Publication, 2012).
[9] *Ibid.*
[10] Tehrani Pardis Moslemzadeh, *Cyber-Terrorism-The Legal Enforcement Issues* 105 (World Scientific Pub Co Inc, 2017).
[11] F Cassim "Addressing the Spectre of Cyber Terrorism: A Comparative Perspective" May 2017, *available at:* https://www.ajol.info/index.php/pelj/article/view/81295 (last visited on Feb. 21, 2020).
[12] *Ibid*.

Legislation, Law Enforcement, and Investigation" and Section IV "The Future of Cyber Crime and Cyber Terrorism: Prevention and Trends".

Part I elaborated into five chapters *viz*., chapter one is 'Introduction And Overview Of Cybercrime And Cyber Terrorism', chapter two is 'Cyber Terrorism And Information Warfare', chapter three is the 'Criminology Of Computer Crime', chapter four is 'Hackers' and chapter five is 'Sophisticated Cyber Criminal Organizations'. Introduction reveals the current issues, trends and problems in cyber crime and cyber terrorism. Chapter begins with defining the term "cybercrime" and "cyber terrorism" and developmental perspective on growing problems. Chapter two explores the more about website defacement and technological facilitation. The chapter also deals with data hiding and cryptography and further discuss about the funding and financing of the terrorist organizations and how recruitment videos are on the internet by the terrorist organization like *ISIS, Al Qaeda*. Chapter three examines the tenets of the choice theory including routine activities theory and its applicability to the cybercrime. As the chapter focuses on the causes of cybercrime, it also postulates over the past 100 years how crime evolved and there is an emerging body of research attempting to apply these concepts to cybercrimes. According to the choice theory the individual commits crime as he or she makes a rational choice to do so by weighing the risks and benefits of committing the act. With the help of various major criminological theories the author analyses how and why do individuals commit cybercrime. The author made a distinction between computer crime, criminal hacking and non-criminal hacking, which explores the possibility of techniques of hacking and does not hold any sound and sensible justification. As there are important reasons to understand the hacker subculture while considering computer crime and India is far behind with the techniques used in other countries. The author further discusses in the chapter the use of social media like twitter, linkedIn, facebook *etc* by the criminal groups. The chapter also entails a deep web which is very common in today's world as it remains untraceable and difficult to access for the regular internet users and even law enforcement, which allows a large criminal domain to thrive.

Part two consists of introduction and four chapters on 'Various types of crime that are committed using digital technology'. Chapter six is 'White Collar Crimes'. Chapter seven is 'Viruses and Malicious Code'. Chapter eight is 'Sex Crimes, Victimization, and Obscenity on the World Wide Web'. Chapter nine is on 'Anarchy and Hate on the World Wide Web'.

The book illuminates various ways in which the digital era has taken place and the influence of technology lead to creation of various computer crimes like money laundering, fraud, corporate espionage *etc*. Chapter seven gave a brief description of viruses and other types of malicious code. It also entails the categorical analysis of various threats. Chapter eight focuses on the crime conducted against the person by using the internet which includes obscenity, stalking, exploitation. It gives a brief analysis of various types of offences and the offender who commits such types of crime. The author discuss about the *Ashcroft* v. *Free Speech Coalition*[13] case in which provisions of the child pornography reviewed by the Supreme Court of United States, as they curtail the freedom to engage in substantial amount of lawful speech. New provisions were added in the CPPA[14] 1996 as the morph or alter images were used for child pornography. The two provisions of *Communication Decency Act, 1996* was examine in the case of *Reno* v. *American Civil Liberties Union*[15] in which various issues of censorship, online expression and content based restriction have been discussed by the author. Chapter nine provides the extremist views or ideologies creating online hate content on the world wide web with the growth of the internet. The author opined that fake news can be dispersed through social media and consequences can be more. The hate content the learned author elaborated, asks debatable questions - whether commercial Internet service providers (ISP's) prevent the use of their services by extremists? Or why can't the government ban use of the internet to spread hateful and racist ideology in the United States?

Part three "Controlling Cyber Crime: Legislation, Law Enforcement, and Investigation" is divided into four chapters. Chapter ten is 'Digital Laws and Legislation' Chapter eleven is on 'Law Enforcement Roles and Responses'. Chapter twelve is on 'The investigation of Computer-Related Crime'. Chapter thirteen is on 'Digital Forensics'. Chapter ten learned authors review the laws and legislation which applies in case of collection of evidence as well prosecution of cyber crime. The chapters give an overview on digital evidence, searches and warrants and searches without warrants. Second, collection of digital evidence, electronic surveillance law has been discussed along with the federal criminal statutes. Third, issues related to authentication and hearsay under the digital evidence at the trial have been discussed. *United States* v. *Jones*[16] was a landmark case

[13] 535 U.S 234 (2002).
[14] The Child Pornography Prevention Act, 1996.
[15] 521, U.S. 844, 1997.
[16] 565 U.S 400.

in which the United States Supreme Court discussed the "search" under the fourth amendment. The author has discussed in the book another landmark case *Riley* v. *California*[17] which laid down emphasis on whether the law enforcement bodies can search the content of a person's cell phone after the arrest without the warrant. The author has discussed the case with different angles with regard to search warrants.

The most crucial part of the book is part three, the editors have dealt with, where theoretical and practical aspects of law enforcement agencies concerning cybercrimes and interagency give a valuable input. Investigation of computer-related crime which explains and understands the search warrant application processes which are appropriate to the electronic evidence. Digital forensic gives an outline on preparation for forensic analysis, explains how the storage system works in the computer and suggests the portable locations for particular types of digital evidence needed for various types of investigation. Although digital forensic is an upcoming topic in India. The digital forensic discussed convincingly argues that cyber forensic facility is inadequate in India due to lack of tools, techniques and facilities is not incompatible within Indian system.

Part IV the author addresses the future of Cyber Crime and Cyber Terrorism: Prevention and Trends, which underlines the cost effective security technologies, backups, firewalls and wireless network systems. Pointing out these factors, countries like the United States and United Kingdom have such infrastructure and tools which do not exist in India. Interestingly author argument is not complete without mentioning the conventions and international forums dealing with the understanding the cyber terrorism whilst supporting current and future methods of prevention.

On the whole, the book is full of knowledge on a lot of important and complex issues, deliberated by various other co-authors. It is written in a systematic way and entails "Cyber crime and Terrorism" gives an overview of the digital threats trends occurring in the world. It is admirable how the author has covered both sides- criminal justice material as well as computer science legalities and various issues regarding investigation and information warfare, computer and computer related technology. Issues mentioned in the book consist of various types of crime and terrorist acts committed by the use of computer technology, types of digital criminal's tactics and strategies used by the criminals. Further it lays emphasis on impact of cybercrimes and cyber

[17] 537 U.S 2473.

terrorism which are likely to happen in the future and also deals with in what way responses the criminal justice system and other governmental agencies should adopt measures to tackle with the problem of cybercrime and cyber terrorism happens in the future. The book also additionally illuminates new pedagogical features to aid and help the academics, lawyer, judges, researchers and for the researchers who are on the path of learning what research is all about, by providing them various modern tools. Each chapter covers quick facts, summary, review questions, critical thinking exercises and endnotes as well, this indicates that a detailed analysis of each chapter has been made by the author. The chapter includes:

- Chapter objectives which talks about the core elements.
- Boxes which highlight the case studies or examples of the subject matter.
- Quick Facts give you a relevant situation taking place in the world to enhance the student's knowledge.
- Summary discuss the crux of each chapter and give a clear and concise discussion of each chapter.
- Review Questions consist of questions in order to testify the students knowledge.
- Critical Thinking Exercises is given at the end of each chapter which provides students to think on the analytic level and give their opinions and discuss.

Prabha Shree Sain[*]

[*] Assistant Professor, JEMTEC School of Law, Greater Noida & PhD Scholar, Indian Law Institute, New Delhi.