International Journal of Cyber Criminology
Vol 7 Issue 2 July - December 2013



# Book Review of Policing Cyber Hate, Cyber Threats and Cyber Terrorism

**Debarati Halder**[1]
Centre for Cyber Victim Counselling, India

*Policing Cyber Hate, Cyber Threats and Cyber Terrorism*. Imran Awan and Brian Blakemore editors, Ashgate, Surrey, England. Pages 201. ISBN: 9781409438168 (hbk)

With the growth of digital communication technology and internet communication technology the world is experiencing huge growth in cyber hate speech, which has also transitioned to cyber threats and cyber terrorism. Many terror organizations have taken to cyber space to recruit individuals, spread terror messages and use the user generated information to locate vulnerable places as targets (Halder, 2011). Problem becomes intense when policing such crime fails due to several essential reasons including lack of awareness among the investigating officers. This book, *Policing cyber hate, cyber treats and cyber terrorism*, edited by Awan and Blakemore addresses this very important issue through ten chapters written by academicians, psychologists, and police officers. The book has chapters dealing with cyber crime, terrorism, policing the cyber space, cyber hate and government strategies.

Even though each chapter deals with essential features which are helpful to understand the subject as a whole, my attention is attracted especially to chapter 4 which discusses about 'cults' and cyber threat and terrorism. Apart from this chapter, other chapters such as chapter 3 and 5 which begin with special personal notes observed by the authors respectively. The author in chapter 3 further takes up the issue of psychological profile of the terrorist in cyber terrorism cases (p. 49), which adds interesting discussions to the book as a whole. This grabs the reader's attention to understand the critical subjects like cyber hate and terrorism. The chapters (6, 7, 8, 9 and 10) dealing with policing strategies successfully provide learning experiences. Often it has been seen that it is not the State alone, but the private individuals also have to face online terrorism and cyber hate. Simultaneously, often private individuals are made of targets of cyber threat which may or may not have direct relation with cyber terrorism. People tend to get confused and skeptical about their privacy and instead of reporting the matter to the police, they may themselves create advantageous position for the terror organizations (Halder, 2011). These five chapters separately address these issues.

[1] Advocate and Managing Director, Centre for Cyber Victim Counselling, 55, Saibaba Colony, 4th Street, T. Nagar, Tirunelveli, Tamil Nadu, India. Email: ccvcindia@cybervictims.org; PhD Alumna, National Law School of India University, Bengaluru, India.

However, the core problem of policing cyber terrorism cases lie in the problem of jurisdiction, constitutional boundaries like freedom of speech and freedom of privacy and 'fear of sharing intelligence' within the departments as well as with other 'partner agencies' (p. 133); Chapter 8 dealing with intelligence gathering, discusses these core issues which are extremely necessary for any police organization. Some of these chapters are equipped with lists, tables and schedules which make the reader understand the issue more practically. However, even though I note that most of the chapters dealing with policing and strategies to tackle the problem are from UK perspective (which limits the book within a specific geographic jurisdiction), chapter 9 broadens the discussions by taking up issues of national and international cyber security strategies. This chapter throws light on importance of cross jurisdictional bilateral treaties, UNODC and European Union strategies to tackle the issues globally. The discussion on the role of NATO (p. 166) is especially mentionable in this context. It definitely provides learning experience for readers belonging to other geographic regions as well. Even though the closing chapter (10) gives the reader an impression that this chapter will also carry forward the discussions held in previous chapters, the author very carefully chose to be different. The chapter deals with problems some of which is now considered as one of the world's most debated issue; police surveillance versus human rights. PRISM system in the US has created hue and cry among privacy rights advocates all over the world. As has been mentioned earlier, perpetrators including terror networks may make private individuals their scapegoats to gather information and this can be done through social networking sites like the Facebook. Police has simultaneously taken to Facebook, Twitter and other popular social networking sites to keep vigil on hate speech, cyber threat and cyber terrorism. As the current debates on global government surveillance suggest, private emails and digital communications are also being targeted. Police being one of the main executing mechanisms in any constitutional setup, often the burden lies on police organizations to carry out the surveillance which may or may or not infringe the privacy rights. This chapter, authored by the editors themselves, finely picks up these issues through paragraphs such as the one titled "policing or oppression" (p. 179). It also addresses social control (p. 184) as a mode to check the problem by the society itself. The book therefore ends with a positive note that society is also developing to cope with the problem at large.

The design of the book deserves special mention; the pages dealing with contents, list of figures and list of tables attracts immediate attention as these predict the extremely interesting discussions that the book holds. The packaging of the book deserves further applause. However, the text fonts could have been made larger to enable readers to have a comfortable reading of the pages. The notes on contributors further says that the book is not limited to contribution by the academics only, but has valuable practical experiences of police officers who may have dealt with the problems directly. The book is a must read for police officers dealing with cyber crimes including online terrorism, cyber hate and threat. It will also be an essential book for lawyers, students of criminology, victimology, and psychologists who are dealing with the problem of cyber hate and threat.

## Reference

Halder, D. (2011). Information Technology Act and Cyber Terrorism: A Critical Review. In P. Madhava Soma Sundaram, & S. Umarhathab, (Eds.), (2011). *Cyber Crime and Digital Disorder* (pp. 75-90). Tirunelveli, India: Publication Division, Manonmaniam Sundaranar University.