blogs.lse.ac.uk
http://blogs.lse.ac.uk/lsereviewofbooks/2012/12/14/book-review-policing-cyber-hate-cyber-threats-and-cyber-terrorism/

Book review: Policing Cyber Hate, Cyber Threats and Cyber Terrorism

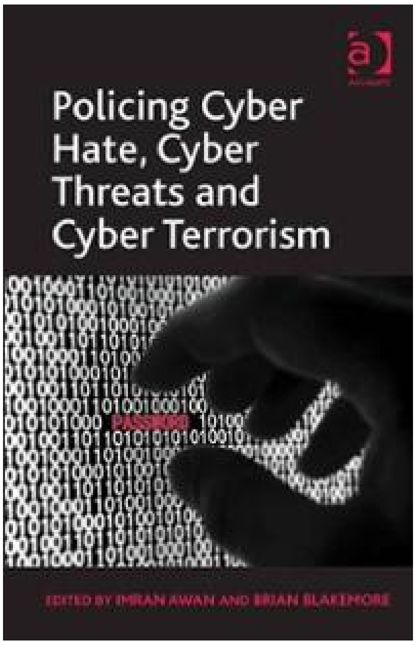
by Blog Admin

December 14, 2012

What are cyber threats? This book brings together a diverse range of multidisciplinary ideas to explore the extent of cyber threats, cyber hate and cyber terrorism. Providing a comprehensive understanding of the range of activities that can be defined as cyber threats, the authors also show how this activity forms in our communities and what can be done to try to prevent individuals from becoming cyber terrorists. ***Stuart Macdonald*** *recommends the book for its useful and thought-provoking material.*

Policing Cyber Hate, Cyber Threats and Cyber Terrorism. Imran Awan and Brian Blakemore. Ashgate. June 2012.

The possibility of a cyber attack is not only to be found in the scripts of popular movies and TV shows such as *Skyfall*, *Die Hard 4.0, Homeland* and *24*. The Government's *National Security Strategy* (2010) lists cyber attack by other states, organised crime or terrorists as one of the four highest priority risks currently facing the UK. Whilst warning that the Government, the private sector and citizens are already under sustained attack, it states that cyber threats could get even worse in the future as cyberspace becomes an ever more integral part of society. The number of global web users has increased from 16 million in 1995 to more than 1.7 billion in 2010, and by 2015 there will be more interconnected devices on the planet than humans. As part of the effort to meet this challenge, a new National Cyber Security Programme was introduced by the Coalition Government in June 2011, accompanied by £650 million of new investment.


Policing Cyber Hate, Cyber Threats and Cyber Terrorism
PASSWORD
EDITED BY IMRAN AWAN AND BRIAN BLAKEMORE

Policing Cyber Hate, Cyber Threats and Cyber Terrorism is a collection of essays edited by Imran Awan and Brian Blakemore (both University of Glamorgan) which examines this threat. Taking an interdisciplinary approach, the book's primary focus is cyber terrorism. It includes: chapters on the psychology of terrorist recruitment using computer-mediated communication and the formation of terrorist groups online; and, chapters on the role of intelligence-led policing and knowledge management within the police and security services. The book also considers other cyber threats, including cyber violence (such as online stalking and harassment), cyber hate (propaganda directed at particular social groups) and cyber crime (such as identity theft).

The book engages with the definitional questions surrounding cyber terrorism, which is important given the diverse ways in which the term is used. Narrow conceptions limit cyber terrorism to acts of serious violence against people or property perpetrated using a computer (computer as means, e.g., penetrating an air traffic control system and causing two planes to collide) and/or to attacks on critical infrastructure (computer as target, e.g., attacking the computer system of a country's financial exchange causing devastating economic damage). By contrast, broader conceptions encompass not only terrorist attacks but also other terrorism-related activities such as recruitment, communication, propaganda and preparation.

The editors prefer the broader conception, arguing that a "wide spectrum approach to defining cyber terrorism" (174) is "more useful in policing terrorism" (34). This results in some counter-intuitive applications of the pejorative label terrorist. For example, in chapter three Bradley Manning – the US soldier charged with passing classified materials to the website *WikiLeaks* – is described as a "well-known contemporary cyber terrorist" (p.51).

The broader conception is also significant when considering the justifiability of many of the criminal offences introduced by the 2000 and 2006 Terrorism Acts (surveyed in chapter six). These offences target a range of preparatory conduct, including: possession of an article for terrorist purposes; collecting information likely to be useful to a terrorist; and encouragement of terrorism. Labelling activities like these cyber terrorism when they are performed online risks obscuring the fact that much of the conduct in question does not cause any direct harm and may be several steps removed from a terrorist act. Respect for individual liberty requires that careful justifications are provided for criminalising preparatory activities, and that the criteria for liability are tightly defined to ensure that innocent activities are excluded. Here, chapter six could have taken a more critical approach to the raft of existing offences.

In terms of the possibility of terrorists committing a cyber attack (the narrow conception), the book emphasises the importance of vigilance. It warns that no country is "immune" from cyber attack (p.98). Technological advances in cyberspace are rapid and frequently "far from perfect", leaving "potential cyber crime opportunities" (p.7). Electronic attacks on air traffic control "are possible, as they are clearly vulnerable" (p.26). And although at present terrorists appear to lack "the skills to use cyber technology" in this manner (p.27), it is possible that they will "actively and deliberately target and recruit the expertise they need to carry out sophisticated acts of terrorism" (p.60).

At the same time, however, it is important to recognise that new information and communication technologies also offer policing opportunities. Websites can be a vital source of intelligence, which is particularly important given the absence of informants in most cases involving Jihadist groups. And not all terrorists are as sophisticated as sometimes assumed; the laptop seized from Mohammed Naeem Noor Khan, for example, was described as a treasure trove for Western intelligence agencies. When discussing the possible regulation of internet use, the book could have engaged in more detail with the security, and not just the liberty, reasons for not closing off modes of communication.

In summary, this book contains some useful and thought-provoking material, a variety of disciplinary perspectives and helpful further reading lists. The editors are correct to describe it as "not an encyclopaedia but … more than an introduction" (p.1).

———————————————————————————-

Stuart Macdonald is a Senior Lecturer at Swansea University. His research interests are criminal law, terrorism laws and policy and the regulation of anti-social behaviour. He is Deputy Director of the Centre for Criminal Justice & Criminology and co-Director of the University's multidisciplinary Cyberterrorism Project (www.cyberterrorism-project.org). You can find Stuart on Twitter at @CTProject_SM and the project at @CTP_Swansea. Read reviews by Stuart.

Related posts:

1. Book Review: Illuminating the Dark Arts of War: Terrorism, Sabotage, and Subversion in Homeland Security and the New Conflict (16.7)
2. Book Review: Terrorism: A Philosophical Enquiry (12.9)
3. Book Review: Media and Terrorism: Global Perspectives, edited by Des Freedman and Daya Kishan Thussa (10.8)
4. Book Review: 9/11 Ten Years After: Perspectives and Problems (10)
5. Book Review: Understanding Terrorist Finance (9.9)