Policing Cyber Hate, Cyber Threat and Cyber Terrorism

Edited by Imran Awan and Brian Blackemore

Ashgate Publishing

Dr Clare Chambers-Jones, Associate Professor in Banking and Finance Law

In late August 2012 the Government Forum of Incident Response and Cyber security Teams (GFIRST) gathered in Atlanta to discuss cyber threats and how new realities are emerging and how new forms of regulation are needed. At the same time *Policing cyber hate, cyber threat and cyber terrorism* was published. This comprehensive book brings together a divergent problem and tackles each with a candid exploration. The book has ten chapters and covers aspects such as extortion via the internet, the psychological aspects of cyber hate and terrorism, how cyber terrorism can be policed; how knowledge can be managed in relation to cyber terrorism; the intelligence gathering and police systems and most importantly the challenge of national and international convergence of cyber security strategies.

The book is authored by eminent academics in their specific field. The authors are, Imran Awan , Brain Blackmore, Geoff Coliandris, James Gravelle, Dr jane Prince, Tim read and Dr Colin Rogers.

Despite the increase in cybercrimes in the past decade or so, there is little academic literature in the area. This book brings together for the first time the many multi-discipline approach that is needed to tackle cybercrimes. The book also proffers an insight to the origins of cyber terrorism and how governments have missed an opportunity to tackle it from the beginning.

The book can be seen by the reader as being in two parts. The first part provides a clear and narrative background of cyber hate, crimes, and terrorism. Blackmore opens this debate by providing carefully crafted definitions to what cyberspace actually is. A clear definition of the context in which the book is set is essential for the preceding chapters.

One of the most interesting parts of the book is the way in which Dr Colin Rogers looks at the intelligence cycle of intelligence gathering and application. Rogers examines the cycle and its deficiencies in light of the government response to cyber terrorism. Similarly Tim Read provides a useful and informative chapter on national and international cyber security strategies. Cybercrime has not been taken seriously for many years and only now in recent times the criminal act is being considered a real and credible threat. As such the law and the legislative environment is out of date and unable to cope with the sophisticated techniques of the cyber criminals. Read's chapter analyses the policy guidance in the UK focusing on the interpretation of what is considered a cybercrime. Read's chapter moves on to consider the implication of the international regulatory perspective which is inherently interconnected with every domestic legislative cybercrime provision. Cybercrimes can and do transverse multi-jurisdictions and cause law enforcement agencies problems of sovereignty and jurisdictional basis for criminal acts. The book on the whole concludes that there is no one way to regulate the internet and no one country that can do the job of policing and safeguarding cyberspace. What is needed is a joined up international approach dedicated to stopping cybercrimes, whether these are cyber hate, terrorism or threats.

Awan and Blakemore in the last chapter of the book discuss the policing cyber hate, threats and terrorism and point out that policing is difficult when spanning many different cultures, religions and legal systems. One country may view an act on the internet as a cybercrime, another may view it as fighting for freedom. Human rights will always play an enormous role in shaping policing and legislating the internet. Awan and Blackmore denote this important role human rights can play by critically analysing whether monitoring social networking sites like face book or twitter by law enforcement agencies are an erosion of freedom and a form of oppression. Yet they conclude the chapter by stating that there must be concerted holistic and flexible rapid action both in prevent and response to all cybercrimes.

The most important thing this book does is to provide information. Information and awareness is key to detecting and preventing cybercrime both on a domestic and international arena. The threats of cyber hate and terrorism and the policing and management of cybercrimes is a pertinent and interesting topic. This well researched and authored book is a must for anyone interested in cybercrimes from any discipline. It is comprehensive and factual, up to date and modern. In a fast pace area such as cybercrime I am pleased to see this multi-disciplined book being produced.