The Dark Side of Social Media: Review of Online Terrorism

Dr. Geoff Dean, Peter Bell, Jack Newman

Abstract

This paper lays the conceptual foundation for understanding the significant role that social media can and does play in relation to spreading the threat and growth of terrorism, especially 'home-grown' terrorism. The utility of social media applications (eg. Facebook, Twitter, You Tube) to recruit, communicate and train terrorists is explored through the perspective of Knowledge-Managed Policing (KMP). The paper concludes with the implications this conceptual analysis of terrorism as a new dot.com presence on the internet has for law enforcement and the global cyber community.

Introduction

The advent of social media (eg. Facebook, Twitter, You Tube) has created new opportunities for terrorist organisations and brought with it growing challenges for law enforcement and intelligence agencies. Whilst the use of online resources by terrorist organisations is not a new occurrence, what is new is the shift to a broader focus by national intelligence agencies towards the increasing threat of 'home-grown' terrorism (ABC News, 2005, 2011; Johnson, 2010; Silber and Bhatt 2007; Wright 2006). A review of extant literature shows a dearth of research into the connection between theoretical and practical applications of social media by terrorist groups and the strategies available to counteract such use.

This study seeks to address aspects of this conceptual gap in the literature by outlining a framework based on a Knowledge-Managed Policing (KMP) approach to the analysis of social media use by terrorists. Three of the most popular social media applications - Facebook, Twitter and YouTube – are focused on in this study as examples of how 'online terrorism' has become a new dot.com with the potential to harness the power of social media for recruiting, communicating, training and funding 'home-grown' terrorists.

Social Media's Utility for Terrorism

The introduction of Web 2.0 applications—websites based solely on interactive user-generated content, or 'social media', as opposed to more traditional static websites where users can only view content (Tech Pluto, 2009; Vorvoreanu and Kisselburgh, 2010) over the last 10 years has created new opportunities for online engagement. These social media sites effectively create online communities based upon users generating, collaborating on, viewing, and sharing content (Tech Pluto, 2009; Vorvoreanu and Kisselburgh, 2010). Wikipedia, as an example, is a free online encyclopaedia that only contains articles generated, edited and reviewed by its user base (Wikipedia, 2011).

The uptake of social media websites by the general public increased rapidly with the emergence of websites such as MySpace and Facebook, which allowed people to 'connect' online with their friends and family, and encouraged the creation of online communities based on common interests, political ideologies or geographical locations (Wooley et al., 2010). As the statistics began to appear showing the incredible surge in popularity of social media websites, people from all political persuasions quickly realised the value of this new resource (Wooley et al., 2010).

Social media quickly presented itself as a cheap and effective tool for mass-communication, as well as an effective method of specifically targeting key demographics (Earl and Kimport, 2011; Papic and Noonan, 2011; Wooley, et al., 2010). As far back as the 1990's political groups and leaders have used the Internet for political purposes (Earl and Kimport, 2011; Wooley et al., 2010). However, this was largely limited to the use of dedicated websites and e-mailing lists to distribute their campaign messages to constituents (Earl and Kimport, 2011).

With the advent of Web 2.0 technology the use of static forms of social media for political use were transformed into more dynamic and ever-evolving phenomena. For instance, in 2008 the value of social media was evidenced during the US Elections with the then presidential candidate, Barack Obama, investing a significant amount of time developing a Facebook page, Twitter account and YouTube channel (Wooley et al., 2010). However, it soon became apparent that social media could be used for other political purposes, from simply providing a forum for like-minded political dissidents to voice their opinions, to being used for organising and instigating major political riots and even revolutions (Earl and Kimport, 2011; Papic and Noonan, 2011).

Three of the most popular social media sites are Facebook, Twitter, and YouTube (Alexa, 2011b). Whilst these applications use different technologies, one important similarity between them is that any person with a valid email address and who claims to be over 13 years old can register as a user on the site (Facebook, 2011; Parental Guide, n.d; Twitter, 2011; YouTube, 2011)—affording a measure of anonymity to users if they require it. Furthermore, it is notable that recently the most popular social media sites have seen an increase in integration, so that content posted on one social media site will simultaneously appear on all other connected sites (Angelos, 2007; Gannes, 2009; Kelsey, 2010; O'Neill, 2009; Swisher, 2008).

Facebook – Virtual Recruitment Strategy

Facebook falls into the 'social networking' category of social media; its primary function is to build and maintain relationships between people (Alexa, 2011a; Wooley et al., 2010). Users of Facebook create an online profile using their personal

details, add connections to friends or family (or strangers, if desired), and can then post 'status updates' on their page or write messages to other users. Members can also create and join 'groups' based on similar interests such as support for a particular political group or cause (Wooley et al., 2010).

In addition to the inherent advantage of being the most widely used social media site throughout the world, the 'groups' application within Facebook presents itself as an invaluable tool for terrorist groups to organise themselves online, and attract other like-minded people to their cause (Wooley et al., 2010). Groups are public by default, and members of the group can send out invitations to friends to recommend that they also join. In this fashion groups can very quickly increase in size, especially when a political purpose is involved (Wooley et al., 2010). Once a group has its user base, any member can send out notifications or messages to every user who has joined the group instantaneously and free of charge (Wooley et al., 2010).

Facebook provides what is essentially an 'all-in-one' service to any group who knows how to use it. While Facebook is certainly capable of acting as a communication service similar to Twitter, and is capable of hosting videos similar to YouTube, the primary function of Facebook for terrorist organisations is for recruitment purposes (Department of Homeland Security, 2010; Torok, 2010). Traditionally, the online presence of a terrorist organisation consisted primarily of a website and possibly a private forum to facilitate jihadist discussions. The problem with this model, as pointed out by a forum poster on a jihadist website, was that an 'elitist community' was created, with those people on the outside having difficulty accessing the community (Department of Homeland Security, 2010). Facebook allows terrorist organisations to avoid this issue.

The most important and useful Facebook feature for terrorist organisations is the 'groups' function (Torok, 2010). The apparent strategy used by terrorist organisations is to create a Facebook group based on a seemingly innocent ideal, such as supporting Palestinians or Islam in general (Department of Homeland Security, 2010; Torok, 2010). As member numbers for the groups increase, jihadist material can be slowly introduced by members of the organisation to the Facebook group in a way which does not directly condone or encourage jihadist actions, and thus does not constitute a violation of Facebook policy (Department of Homeland Security, 2010; Torok, 2010). From this position, the group can even be directed straight to the website and forums of the terrorist organisation behind the Facebook group.

The threat posed by online recruitment is significant (Stein, 2011; al-Shishani, 2010; Weimann, 2010). There are no borders to be crossed, and no effective methods for intervention (Department of Homeland Security, 2010; Torok, 2010). Facebook

allows terrorist organisations to recruit people from all around the world, without posing any significant threat to the security of the organisation (Department of Homeland Security, 2010; Torok, 2010). Importantly, once people become members of the group, the organisation can then seamlessly transition into the next phase: training.

Twitter –Instant Communication Strategy

Twitter falls into the 'blogging' category of social media; however it is more aptly described as a 'micro-blogging' service (Van der Zee, 2009). Registered users of the site post publicly visible messages on their profile called 'tweets': text-based messages of up to 140 characters (Van der Zee, 2009). Users can subscribe to other users to automatically receive their posts, and can follow specific topics by using 'hashtags' (#), which are used to flag posts as belonging to a certain group or topic (Van der Zee, 2009), for example #terrorism to follow tweets related to the topic of 'terrorism'.

The ability to instantaneously send small bits of information to a virtually unlimited number of people free of charge makes Twitter an extremely valuable tool for political purposes (Papic and Noonan, 2011; Van der Zee,2009). Twitter hashtag groups can function in a similar way to Facebook groups, except without a designated leader, with users often 'retweeting' (re-posting) to ensure the message is spread (Van der Zee, 2009). This is in part where the real value of Twitter lies: in the constantly changing virtual communities that are created almost naturally during major events (Papic and Noonan, 2011; Van der Zee, 2009). Political movements and protests in particular see these online communities thrive, where large amounts of people both directly and indirectly involved in an incident begin flocking to follow the relative hashtag for the event (Papic and Noonan, 2011; Van der Zee, 2009).

The threat posed by Twitter arises from both its ability to send out instant messages to large numbers of people, and from the ability for people to follow particular topics as well as groups (O'Rourke, 2010). Terrorist organisations can utilise Twitter at an operation level, using the service to keep up-to-date on any new information that emerges in the public sphere (Weimann, 2010; O'Rourke, 2010; US 304th Military Intelligence battalion, 2008). The 2008 terrorist attacks in Mumbai present an apt example of how terrorist organisations can utilise social media sites such as Twitter.

The 2008 Mumbai terrorist attacks occurred on 26 November, with more than 10 sites throughout Mumbai targeted by an Islamic terrorist organisation from Pakistan: Lashkar-e-Taiba (O'Rourke, 2010). The attacks killed 164 people and injured over 300. One of the most important issues that arose from the attacks was

the technological sophistication of the attackers. All of the attackers were equipped with BlackBerry smart-phones, and not only utilised VOIP (Voice over Internet Protocol), but also carried multiple SIM cards to switch into the phones if authorities were able to block them (O'Rourke, 2010; US 304th Military Intelligence battalion, 2008).

Post-attack interviews with the sole surviving attacker, combined with information from intercepted phone calls from the attackers during the events indicated that the terrorists were in constant contact with controllers based in Pakistan (O'Rourke, 2010; Rabasa et al., 2009). The controllers were able to keep track of the constant up-to-date flow of information streaming from public Twitter posts and communicate it directly to the attackers (Leggio, 2008; O'Rourke, 2010; Rabasa et al., 2009). This included critical information such as the movements and positioning of the Indian counter-terrorism units planning the assault on the hotel (Lee, 2008; Leggio, 2008; O'Rourke, 2010).

Examples such as Mumbai serve to demonstrate the increasingly advanced technological sophistication of terrorist organisations. In order to effectively combat these groups, robust counter-strategies for social media must be developed and implemented by government agencies as soon as possible.

YouTube – Cyber Training Strategy

YouTube falls into the 'video sharing' category of social media; the primary function of the website is to host videos uploaded by users, which are then publicly viewed and shared around the world (Vergani and Zuev, 2011). Registered users of YouTube are able to upload videos in a wide range of formats up to 15 minutes in length, and in most cases viewers do not need to register (Vergani and Zuev, 2011). Registered members can subscribe to another user's YouTube 'channel', receiving alerts whenever a new video is posted on that channel (Vergani and Zuev, 2011). While there are a range of restrictions over what cannot be uploaded, the 'post-hoc' review system used for YouTube videos means that only those videos which have been 'reported' by viewers will be reviewed and potentially removed by YouTube staff, thus making abuse of the system possible by terrorist groups.

YouTube is free, easy to use, difficult for state authorities to control, and can be used to communicate with a tightly-knit group to the entire world (Vergani and Zuev, 2011). Furthermore, YouTube can provide a more effective means of communication than text-based social media sites such as Facebook and Twitter, simply due to the ability to use sound and video (Vergani and Zuev, 2011).

Like Facebook, YouTube has multiple uses for terrorist organisations (Weimann, 2010; Bergin et al, 2009; George, 2009). Video can be a much more effective means of communicating an issue than plain text, so for this reason alone

YouTube would be an invaluable tool for terrorist organisations (Torok, 2010). For example, Anwar Al Awlaki is a prominent and 'highly dangerous' planner and trainer for 'Al Qaeda and all of its franchises', well known for his utilisation of social media sites such as Facebook and YouTube to spread his extremist messages (Madhani, 2010; Shephard, 2009; Smith, 2009). As of 2010, Awlaki was known to have posted over 5000 videos on YouTube (Torok, 2010). However, more important than simply relaying a message or calling for people to take action is showing them physically how to do it; this is where YouTube's value for terrorist organisations is truly shown (Department of Homeland Security, 2010).

Videos explaining and visually demonstrating practices such as tactical shooting or the field stripping of an AK47 have been identified as examples of training that is effectively communicated over YouTube (Department of Homeland Security, 2010). Additionally, these types of training videos do not actively incite violence, and thus do not contravene YouTube's policy, and will therefore not be deleted (Department of Homeland Security, 2010). Terrorist organisations can also take advantage of YouTube's 'post-hoc' review system by uploading bomb making instructions and other such videos that violate YouTube policy, but which can potentially be viewed hundreds of times before the videos are reported and deleted.

Terrorism: A New Dot.Com

According to Awan (2010) the internet has surpassed all other media forms in becoming the principle arena for terrorist media activity, and the primary platform for the dissemination of jihadism. Furthermore, this review has demonstrated it is not only political activists who see the competitive advantage of using social media, as the three most popular social media sites (Facebook, Twitter, and YouTube) have value-added to terrorism's ability to communicate, organise, recruit, and train would be terrorists (Alexa, 2011b; Weimann, 2006; Wright, 2006). Furthermore, terrorist groups are also using social media for fundraising purposes (Strohm, 2011; Gray, 2009; Caldwell, 2008; Conway, 2006).

This cluster of issues is of particular relevance to countries like Pakistan with large Muslim populations where fertile minds exist for social media to radicalism free of charge. Moreover, countries such as Australia face their own concerns about social media, where the traditional transnational terrorism threat is being replaced by a much more pervasive and difficult to detect 'home-grown' or 'grass-roots' terrorism threat embedded in virtual realities (Johnson, 2010; ABC News, 2005, 2011; Silber and Bhatt, 2007; Wright, 2006).

This review found that whilst the quality of the literature that focused on terrorists' use of social media was generally of a higher quality than that related to political activism in general, the number of articles available on this issue was

limited (Bjelopera and Randol, 2010; Hoffman, 2010; Silber and Bhatt, 2007; Weimann, 2006). Furthermore, many of the articles had been written by, or for, the US military (Mayfield, 2011; McCullar, 2010; Petraeus, 2010; US Joint Forces Command – Joint Warfighting Center, 2010). While the majority of content in these articles was highly relevant, the recommendations presented for strategies to deal with the issues were focused on military applications, as opposed to more generally applicable strategies or those which were specific to government or intelligence agencies.

Those articles which did not focus on military applications debated the effectiveness of the three broad policy approaches that governments can adopt: zero tolerance, encouraging extremist narrative to be challenged through the same social media tools that promote it, and intelligence gathering (Bergin et al, 2009; Caldwell, 2008).

Hence, what is also clear from this review is that governments, law enforcement and intelligence agencies are adapting to this new political and social environment created by Web 2.0 inspired social media and are seeking to find and adopt new policies and strategies to minimize these threats and harness the presented opportunities. For instance, in June 2011, the Joint Select Committee on Cyber-Safety instituted by the Australian Parliament tabled its report on its Inquiry into Cyber-Safety entitled *High-Wire Act: Cyber-Safety and the Young.*

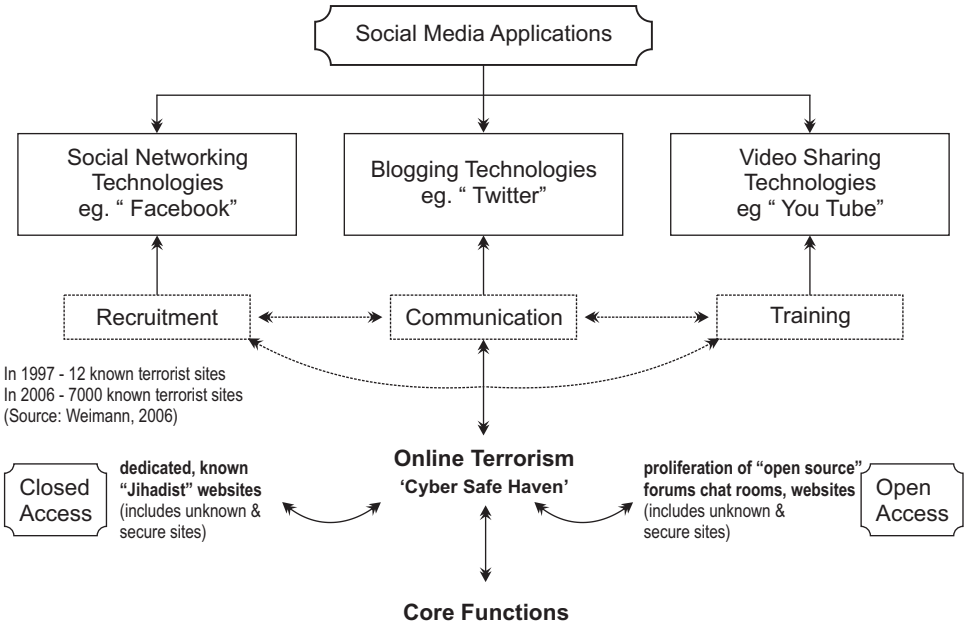
Moreover, there was a rapid expansion and widespread growth of 'Jihadist' websites during the period when Web 2.0 technologies began widely available around 2004 onwards. For instance, research by Weimann (2006) into the use of the Internet by terrorist groups showed that between 1997 and 2006, the number of websites dedicated to terrorist groups rose from only about 12, to over 7000.

Similarly, Stein (2011:3) cites a U.S. State Department report in 1998, that "… there were only 15 Web Sites run by groups defined by US as "terrorist" groups. In 2005, this number increased to more than 4000."

While the terrorist organisations that are advanced enough to have a presence online would traditionally stick to the use of 'jihadist websites' and forums, where most of the users were people already supporting the cause (Department of Homeland Security, 2010), the transition into the more 'open' realm of social media has given them the opportunity to reach significantly larger audiences than was previously possible. For instance, Cohen (2009) found that terrorist groups actively target the large number of social media users among vulnerable populations in impoverished regions in the Middle East, Africa and Asia, and poorly integrated immigrant communities in Western Europe.

Therefore, the conceptual picture which emerges from this review is that Web 2.0 social media technologies have allowed terrorism to become a massive 'dot.com' presence on the internet. Figure 1 below illustrates the virtual pathways utilised by terrorism to carry out its core functions 'online'.

Conceptual Map of Web 2.0 Technologies for Online Terrorism



Information provision (eg. the 3 P's - Publicity, Propaganda, Psychological warfare, including disinformation)
Information gathering (eg. 'data mining' for specific targeting opportunities, intelligence & information sharing)
Networking (eg. decentralized structures, planning & coordination operations, risk mitigation via virtual communities)
Financing (eg. soliciting funds via Jihadist Websites, exploiting e-commerce tools, business, charities, fronts)
Recruitment (eg. recruiting and mobilising followers, sympathizers)

Source: Gray and Head, 2009; Kohlmann, 2008; Conway, 2006;Weimann, 2004

Therefore, the conceptual picture which emerges from this review is that Web 2.0 social media technologies have allowed terrorism to become a massive 'dot.com' presence on the internet. Figure 1 below illustrates the virtual pathways utilised by terrorism to carry out its core functions 'online'.

As can be seen from Figure 1, the conceptual mapping above depicts the phenomenal rise of Jihadist expansion on the web through both closed and open access portals as well as the various configurations of online terrorism. As such, it provides a useful starting point for research but much more work needs to be done before a clearer picture of radicalism and its effectiveness comes into focus.

This is in part due to the very limited amount of scholarly empirical research in the existing literature on the effectiveness of social media by terrorist organisations to radicalise people (Leuprecht and Skillicorn, 2011). Much is anecdotal and based on biased samples. For instance, al-Shishani (2010) reports that "… according to Pakistani authorities, the five young American Muslims arrested in Pakistan last December were recruited online via You Tube and Facebook after the suspects used these sites to reach out to groups such as Lashkar-e-Taiba and Lashkar-e-Jhangyi (*Dawn* [Karachi], December 16)". In addition, there are major issues with the range of quality found in the literature, as well as with the lack of connections made between theory and practical application.

Given such limitations the role of Knowledge Management (KM) in capturing relevant and reliable data, information, intelligence and evidence on which to base policing and law enforcement of social media is still in its infancy. However, KM does have substantial applicability for policing online terrorism. For instance, the notion of 'Knowledge-Managed Policing' (KMP) coined by Dean is a foundational framework for managing, systematically, the application of knowledge to enhance policing effectiveness through harnessing practitioner-based knowledge and integrating such tacit knowledge with KM processes and appropriate IT support systems (Dean and Gottschalk, 2007). Furthermore, the utility of KMP for managing the challenges associated social media must, of necessity, involved a range of Communication Interception Technologies (CIT) by police and other law enforcement agencies. Dean, Bell, and Congram (2010) have previously outlined the significance of KMP as an organising framework for using CIT as an investigative tool for knowledge creation, capture, storage, retrieval, transfer, sharing, application and integration. Moreover, Dean (2007) developed a multi-context model of the terrorism process which is the subject of future work to integrate KMP with this terrorism model in order to expand available counter-terrorism options to police and law enforcement agencies, especially in relation to this dark side of social media.

A special report on *Countering internet radicalisation in Southeast Asia* in 2009 by Bergin, Osman, Ungerer, and Yasin identified three broad policy approaches and/or a combination of them which governments tend to adopt towards dealing with online terrorism. There are as stated in the report (2009:12):

- a hard strategy of *zero tolerance* (blocking sites, prosecuting site administrators, using internet filters)
- a softer strategy of *encouraging internet end users to directly challenge the extremist narrative* (including creating websites to promote tolerance)

- an intelligence-led strategy of *monitoring leading to targeting, investigation, disruption and arrest*.

Essentially, these policy approaches translate into a policing/law enforcement counter-terrorism continuum ranging from prevention to utilisation methodologies.

Prevention Methodologies would include aspects of a '*zero tolerance strategy*' whereby sites are censored, blocked or cut off and aspects of an '*intelligence-led strategy*' of monitoring, targeting, investigating, disrupting and ultimately arresting and prosecuting those involved in terrorist activities. For instance:

- censoring sites, eg. South Korea deletes political content from various social media sites regarded as North Korean propaganda (Eun-jung, 2011)
- blocking sites, eg. 'The Great Firewall of China' where access to websites deemed to be politically sensitive or offensive are blocked (Petraeus, 2010).
- cutting off complete access to the internet for entire regions or countries, eg. during the 2011 revolution in Egypt (Papic and Noonan, 2011)
- Proactive Intelligence monitoring and collection eg. developing risk profiles of potential terrorists through monitoring terrorist-related social media sites, (Norris, 2011)

Utilisation Methodologies would include some aspects of an '*intelligence-led strategy*', mainly that of disinformation, and a softer strategy of *encouraging and challenging extremist narratives.* For instance:

- Disinformation via 'sock puppets', eg. Sock puppets have been used to infiltrate online-based political or terrorist groups, and once inside to spread disinformation about the location and activities of law enforcement to disrupt the plans of the group and/or direct their protest towards a location that can be easily controlled (Norris, 2011; Papic and Noonan, 2011)
- Insider Knowledge' intelligence gathering, eg. tips offs by informers and human assets inside terrorist's cells and sites in order to utilise such knowledge strategically (Norris, 2011)
- Creating alternative websites by moderate Muslim groups, eg. harnessing soical media to promote peace and democracy (Caldwell, 2008); providing alternatives to extremist influence (Cohen, 2009)

All counter-terrorism policy approaches and law enforcement strategic methodologies are depend on and require a substantive investment in a range of resources to counter social media-based radicalisation. The Special report by Bergin et al (2009:13) outlines in broad terms the *technical, human* and *intellectual* resources necessary to deal with online terrorism as follows:

- ***Technical infrastructure***

  The technical requirements are secure, unattributable, superfast (broadband and wireless) ICT systems, and the ability to access and view extremist sites (visibility of the environment is fundamental).

- ***Human resources***

  People with analytical, linguistic and technical skills are essential. They will need adequate training and the support of experts.

- ***Knowledge and intellectual capital***

  It's necessary to stay abreast of the latest trends and industry developments, and governments aren't normally at the forefront of internet-related trends.

This massive investment is ultimately about Knowledge Management and the mobilisation of relevant resources. Since 9/11 and the extraordinary growth of online terrorism, the academic community is also playing a significant role with the emergence of a new interdisciplinary field of study and research known as 'Terrorism informatics' (Chen, Reid, Sinai, Silke, and Ganor, 2008).

According to Chen (2011:1) “Terrorism informatics has been defined as the application of advanced methodologies, information fusion and analysis techniques to acquire, integrate process, analyze, and manage the diversity of terrorism-related information for international and homeland security-related applications.”

Chen notes the wide variety of methods used in 'terrorism informatics' to collect massive amounts of many and varied types of multi-lingual information from multiple sources. Hence, 'terrorism informatics' draws on a diversity of disciplines from Computer Science, Informatics, Statistics, Mathematics, Linguistics, Social Sciences, and Public Policy and their related sub-disciplines to achieve “ Information fusion and information technology analysis techniques, which include data mining, data integration, language translation technologies, and image and video processing, play central roles in the prevention, detection, and remediation of terrorism.” (op. cit).

Conclusion

This review of the extant literature from military, academic and public open sources presents a disturbing picture of the multiple pathways Web 2.0 'social media' technologies provide for terrorists and militant extremists to utilise and develop cyber terrorism into a potent virtual battleground which police and security agencies must confront on a very uneven global playing field.

Furthermore, it is evident from this review that the concept and practice of 'Knowledge-Managed Policing' (KMP) is highly relevant, timely and necessary perspective for policing/law enforcement/security agencies. Adopting a salient Knowledge Management approach can tip the competitive advantage towards policing the multitude of harms and threats that 'online terrorism' presents through the medium of the dark side of social media for Civil Society.

References

ABC News. 2005. ASIO warns of home-grown terror threat. Available from: http://www.abc.net.au/news/stories/2005/11/02/1495641.htm [accessed 04.15.11].

ABC News. 2011. "ASIO sets up cyber-spook unit." Accessed April 16, 2011. Available from: http://www.abc.net.au/news/stories/2011/03/11/3161101.htm

Alexa. 2011a. Facebook.com Site Info. Available from: http://www.alexa.com/siteinfo/facebook.com [accessed 04.04.11].

Alexa. 2011b. Top 500 sites on the web. Available from: http://www.alexa.com/topsites [accessed 04.25.11].

al-Shishani, Murad Batal. 2010. Taking al-Qaeda's Jihad to Facebook. *The Jamestown Foundation: Terrorism Monitor*. 8 (5): 3. Available from: http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=36002 [accessed 08.04.11].

Awan, Akil N. 2010. The Virtual Jihad: An Increasingly Legitimate Form of Warfare. http://www.ctc.usma.edu/posts/the-virtual-jihad-an-increasingly-legitimate-form-of-warfare [accessed 08.04. 2011].

Angelos, A. 2007. Twitter updates now connected to Facebook status. Available from: http://mashable.com/2007/09/30/facebook-Twitter-2/ [accessed 03.30.11].

Barat, J. 2009. Internet Blocked in Uyghur Autonomous Region. Available from: http://www.uighur.nl/Internet-blocked-in-uyghur-autonomous-region/ [accessed 05.05.11].

BBC. 2010. Israeli military 'unfriends' soldier after Facebook leak. Available from: http://news.bbc.co.uk/2/hi/middle_east/8549099.stm [accessed 04.29.11].

Bergin, Anthony; Osman, Sulastri; Ungerer, Carl; Yasin, Nur Auzlin Mohamed. 2009. Countering internet radicalisation in Southeast Asia. *Australian Strategic Policy Institute, Canberra*. Available from: http://www.aspi.org.au/publications/publication_details.aspx?ContentID=202&pubtype=10 [accessed 08.03.11].

Bishop, B. 2010. China's Internet: The Invisible Birdcage. Available from: http://digicha.com/?p=1490 [accessed 05.04.11].

Bjelopera, J., Mark, R. 2010. American Jihadist Terrorism: Combating a Complex Threat. Available from: http://www.fas.org/sgp/crs/terror/R41416.pdf [accessed 05.02.11].

Bray, H. 2009. Finding a way around Iranian censorship. Available from: http://www.boston.com/business/technology/articles/2009/06/19/activists_utilizing_Twitter_web_proxies_to_sidestep_iranian_censorship/?page=2 [accessed 05.01.11].

Bristow, M. 2008. China's Internet 'spin doctors'. Available from: http://news.bbc.co.uk/2/hi/asia-pacific/7783640.stm [accessed 05.07.11].

Chen, Hsinchun; Zhou, Yilu; Reid, Edna F. and Larson, Catherine A. 2011. *Introduction to special issue on terrorism informatics. Information systems frontiers.* 13 (1): 1-3. Available from http://www.springerlink.com.ezp01.library.qut.edu.au/content/p373485141036393/ [accessed 08.01.11].

Chen, H., Reid, E., Sinai, J., Silke, A., & Ganor, B. (Eds.) (2008). Preface. *Terrorism informatics: Knowledge management and data mining for homeland security* (Integrated Series in Information Systems). New York: Springer.

Caldwell, Ingrid. 2008. Terror on YouTube. *Forensic Examiner.* (17)3: 80-83. Availablefrom:http://search.proquest.com.ezp01.library.qut.edu.au/docview/207654544/fulltextPDF/130EDDFAE4C5ACB3E4A/1?accountid=13380 [accessed 08.01.11].

Clayton, R., Murdoch, S., Watson, R. 2006. Ignoring the Great Firewall of China. Available from: http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf [accessed 05.03.11].

Cohen, J. 2009. Diverting the Radicalization Track. *Policy Review*. 154: 51-63. Available from: http://search.proquest.com.ezp01.library.qut.edu.au/docview/216455875/fulltextPDF/130F2EF9BC860766293/1?accountid=13380 [accessed 08.03.11].

Conway, Maura. 2006. Terrorism and the Internet: New Media- New Threat? *Parliamentary Affairs.* 59(2): 283-98. Available from: http://pa.oxfordjournals.org.ezp01.library.qut.edu.au/content/59/2/283.full.pdf+html [accessed 08.01.11].

Crampton, T. 2010. Infographic of Social Media Equivalents in China. Available from: http://www.thomascrampton.com/china/social-media-china/ [accessed 05.04.11].

Crampton, T. 2011. China social networks: cool girls to hipsters. Available from:http://www.thomascrampton.com/china/renren-china/ [accessed 05.04.11].

Cyber-Safety Inquiry Report, *High-Wire Act: Cyber-Safety and the Young.* 2011. A Joint Select Committee on Cyber-Safety tabled its report on Monday 20 June 2011 for the Australian Government. Available from: http://www.aph.gov.au/house/committee/jscc/report.htm [accessed 27.06.11].

Dean, G., Bell, P., and Congram, M. 2010. Knowledge-Managed Policing Framework for Communication Interception Technologies (CIT) in Criminal Justice System. *Pakistan Journal of Criminology*, 2 (4) pp.25-41

Dean, G. 2007. Criminal Profiling in a Terrorism Context. In Kocsis, R. (Ed) *Criminal Profiling: International perspectives in theory, practice & research.* Humana Press.

Dean, G. and Gottschalk, P. 2007. *Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications.* Oxford University Press: UK.

Department of Homeland Security. 2010. Terrorist use of Social Networking Sites: Facebook Case Study. Available from: http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-facebook-case-study/ [accessed 04.20.11].

Earl, J., Kimport, K. 2011. *Digitally Enabled Social Change: Activism in the Internet Age*, Massachusetts Institute of Technology Publishing.

Eun-jung, K. 2011. S. Korean man indicted for pro-Pyongyang postings on Internet, Twitter. Available from: http://english.yonhapnews.co.kr/news/2011/01/10/36/0200000000AEN20110110007200315F.HTML [accessed 05.05.11].

Facebook. 2011. What is the minimum age required to sign up for Facebook? Available from: http://www.facebook.com/help/?page=173#!/help/?faq=13455 [accessed 04.10.11].

Fielding, N. Cobain, I. 2011. Revealed: US spy operation that manipulates social media. Available from: http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks?INTCMP=SRCH [accessed 05.05.11].

Gannes, L. 2009. YouTube integrates Facebook Connect. Available from: http://gigaom.com/video/youtube-integrates-facebook-connect/ [accessed 04.05.11].

Gray, David H. and Head, Albon. 2009. The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven. *European Journal of Scientific Research.* 25 (3): 396-404. Available from: http://www.eurojournals.com/ejsr_25_3_05.pdf [accessed 08.03.11].

Hennock, M. 2009. The Uighur riots in western China are teaching the government how to spin. Available from: http://www.newsweek.com/2009/07/06/bad-press.html [accessed 05.05.11].

Hoffman, B. 2010. Internet terror recruitment and tradecraft: how can we address an evolving tool while protecting free speech? Available from: http://www.homelandsecurity.house.gov/SiteDocuments/20100526101502-95237.pdf [accessed 04.25.11].

Johnson, T. 2010. Threat of Homegrown Islamist Terrorism. Available from: http://www.cfr.org/terrorism/threat-homegrown-islamist-terrorism/p11509 [accessed 04.20.11].

Kelsey, T. 2010. *Social Networking Spaces: From Facebook to Twitter and Everything In Between*, New York: Springer-Verlag.

Kohlmann, Evan F. 2008. Homegrown Terrorists: Theory and Cases in the War on Terror's Newest Front. *The Annals of the American Academy of Political and Social Science. 618(1): 95-109.* Available from: http://ann.sagepub.com.ezp01.library.qut.edu.au/content/618/1/95.full.pdf+html [accessed 08.03.11].

Lee, M. 2008. Blogs feed information frenzy on Mumbai blasts. Available from: http://www.theglobeandmail.com/news/technology/article725225.ece [accessed 04.17.11].

Leggio, J. 2008. Mumbai attack coverage demonstrates (good and bad) maturation point of social media. Available from: http://www.zdnet.com/blog/feeds/mumbai-attack-coverage-demonstrates-good-and-bad-maturation-point-of-social-media/339 [accessed 04.17.11].

Leuprecht. C., and Skillicorn, D. B. 2011. Radicalisation: What (If Anything) is to be Done? When Facts Get in the Way of a Good Story. *Home Team Journal*, Issue 3 pp. 38-46.

Macleod, Hugh. 2011. Syria's young cyber activists keep protests in view. Available from: http://www.guardian.co.uk/world/2011/apr/15/syria-activists-protests-in-view [accessed 04.12.11].

Madhani, A. 2010. Cleric al-Awlaki dubbed 'bin Laden of the Internet'. Available from: http://www.usatoday.com/news/nation/2010-08-25-1A_Awlaki25_CV_N.htm [accessed 04.15.11].

Malkin, B. 2010. Google refuses Australian government request to censor YouTube. Available from: http://www.telegraph.co.uk/technology/google/7212902/Google-refuses-Australian-government-request-to-censor-YouTube.html [accessed 05.04.11].

Mayfield, T. 2011. A Commander's Strategy for Social Media. Available from:http://www.ndu.edu/press/commanders-strategy-social-media.html [accessed 05.01.11].

McCullar, T. 2010. Information Warfare, Media, and Decisiveness in Counterinsurgency. Information Operations Journal. 2(4), 4-7. Available from: http://www.nxtbook.com/nxtbooks/naylor/JEDQ0410/#/0 [accessed 05.03.11].

Merriam Webster. 2011. Sock Puppet. Available from: [accessed 05.15.11].

Michael, George. 2009. Adam Gadahn and Al-Qaeda's Internet Strategy. *Middle East Policy.* 16 (3): 135-152. Available from: http://onlinelibrary.wiley.com.ezp01.library.qut.edu.au/doi/10.1111/j.1475-4967.2009.00409.x/pdf [accessed 08.04.11].

Mi-ju, K. 2010. Pro-North Facebook entries face gov't crackdown. Available from: http://joongangdaily.joins.com/article/view.asp?aid=2929934 [accessed 05.02.11].

Molok, N., Chang, S., Ahmad, A. 2010. Information Leakage through Online Social networking: Opening the Doorway for Advanced Persistence Threats. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1092&context=ism&sei-redir=1 [accessed 05.02.11].

Norris, J. 2011. UK police using Twitter to track protesters. Available from: http://unplugged.rcrwireless.com/index.php/20110210/news/6955/uk-police-using-Twitter-to-track-protesters/ [accessed 05.07.11].

O'Neill, N. 2009. YouTube adds Facebook Connect. Available from: http://www.allfacebook.com/youtube-adds-facebook-connect-2009-06 [accessed 04.05.11].

OpenNet Initiative. 2009. Internet Filtering in China. Available from: http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf [accessed 05.03.11].

OpenNet Initiative. n.d. Social Media Filtering Map. Available from: http://opennet.net/research/map/socialmedia [accessed 05.15.11].

O'Rourke, S. 2010. The Emergent Challenges for Policing Terrorism: Lessons from Mumbai. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1004&context=act [accessed 04.10.11].

Papic, M. Noonan, S. 2011. Social Media as Tool for Protest. Last modified February 3, 2011. Available from: http://www.stratfor.com/weekly/20110202-social-media-tool-protest?utm_source=SWeekly&utm_medium=email&utm_campaign=110203&utm_content=readmore&elq=77ffb64cf0554757abe76e998eb0395b [accessed 09.07.11].

Parental Guide. n.d. Parents Lying to Gain Online Access for Their Kids on Facebook, Twitter, and MySpace. Available from: http://www.parentalguide.org/parentalcontrols_age-requirements-for-facebook-Twitter-myspace.html [accessed 04.11.11].

Petraeus, D. 2010. The Posture of U.S. Central Command. Available from: [accessed 05.05.11].

Rabasa, A., Blackwill, R., Chalk, P., Cragin, K., Fair, C., Jackson, B., Jenkins, B., Jones, S., Shestak, N., Tellis, A. 2009. The Lessons of Mumbai. Available from: http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf [accessed 04.20.11].

Sanchez, R. 2010. Growing number of prosecutions for videotaping the police. Available from: http://abcnews.go.com/US/TheLaw/videotaping-cops-arrest/story?id=11179076&page=1 [accessed 04.13.11].

Schneier, B. 2008. Internet censorship. Available from: http://www.schneier.com/blog/archives/2008/04/Internet_censor.html [accessed 05.03.11].

Shephard, M. 2009. The powerful online voice of jihad. Available from: http://www.thestar.com/news/world/article/711964--the-powerful-online-voice-of-jihad [accessed 04.15.11].

Silber, M. Bhatt, A. 2007. Radicalization in the West: The Homegrown Threat. Available from:http://sethgodin.typepad.com/seths_blog/files/NYPD_Report-Radicalization_in_the_West.pdf [accessed 04.20.11].

Smith, H. 2009. Al-Awlaki May Be Al-Qaeda Recruiter. Available from: http://www.cbsnews.com/8301-503543_162-6039811-503543.html [accessed 04.12.11].

Stein, Yael. 2011. Social Networks – Terrorism's New Marketplace. *Genocide Prevention Now.* Available from: http://www.genocidepreventionnow.org/Portals/0/docs/Al%20Quaeda%20is%20recruiting%20on%20Facebook.pdf [accessed 08.04.11].

Stone, B. Richtel, M. 2007. The Hand That Controls the Sock Puppet Could Get Slapped. Available from: http://www.nytimes.com/2007/07/16/technology/16blog.html?ex=1342238400&en=9a3424961f9d2163&ei=5088&partner=rssnyt&emc=rss [accessed 05.10.11].

Strohm, Chris. 2011. Facebook, YouTube Aid in Al-Qaida's Spread, Study Says. *National Journal.* Available from: http://search.proquest.com.ezp01.library.qut.edu.au/docview/850518421# [accessed 08.02.11].

Swisher, K. 2008. When Twitter Met Facebook: The Acquisition Deal That Fail-Whaled. Available from: http://kara.allthingsd.com/20081124/when-Twitter-met-facebook-the-acquisition-deal-that-fail-whaled/ [accessed 03.30.11].

Tech Pluto. 2009. Core Characteristics of Web 2.0 Services. Accessed April 5, 2011. Available from: http://www.techpluto.com/web-20-services/ [accessed 04.05.11].

Torok, R. 2010. 'Make a Bomb In Your Mum's Kitchen': Cyber Recruiting And Socialisation of 'White Moors' and Home Grown Jihadists. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1005&context=act [accessed 04.20.11].

Twitter. 2011. Twitter Privacy Policy. Available from: https://Twitter.com/privacy [accessed 04.10.11].

US 304th Military Intelligence Battalion. 2008. Sample Overview: alQaida-Like Mobile Discussions & Potential Creative Uses. Available from: http://www.fas.org/irp/eprint/mobile.pdf [accessed 04.28.11].

US Joint Forces Command – Joint Warfighting Center. 2010. Commander's Handbook for Strategic Communication and Communication Strategy. Available from: [accessed 05.07.11].

Van der Zee, B. 2009. Twitter Triumphs. Index on Censorship. 38(4), 97-102. Doi: 10.1080/03064220903392570 [accessed 04.20.11].

Vergani, M. Zuev, D. 2011. Analysis of YouTube Videos Used by Activists in the Uyghur Nationalist Movement: combining quantitative and qualitative methods. *Journal of Contemporary China*. 20(69), 205-229. Doi: 10.1080/10670564.2011.541628

Vorvoreanu, M. Kisselburgh, L. 2010. Web 2.0: A Complex Balancing Act. Available from: http://www.mcafee.com/us/resources/reports/rp-first-global-study-web-2.0-usage.pdf [accessed 04.10.11].

Weimann, G. 2010. Terror on Facebook, Twitter, and Youtube. *The Brown Journal of World Affairs*. 16 (2): 45-54. Available from: http://search.proquest.com.ezp01.library.qut.edu.au/docview/347853609/fulltextPDF/130DF8DC3A413223544/2?accountid=13380 [accessed 07.29.11].

Weimann, G. 2006. *Terror on the Internet: the New Arena, the New Challenges*. Washington, DC: United States Institute of Peace Press.

Wikipedia. 2011. Wikipedia: About. Last modified April 7, 2011. Available from:

http://en.wikipedia.org/wiki/Wikipedia:About [accessed 15.10.11].

Wikipedia. 2011. Web 2.0. Last modified April 7, 2011. Available from:

http://en.wikipedia.org/wiki/Wikipedia:About [accessed 05.10.11].

Williams, M. 2010. South Korea has begun blocking access to a Twitter account operated by a North Korean Web site. Available from: http://www.reuters.com/article/2010/08/20/urnidgns852573c40069388000257785000b-idUS56724690620100820 [accessed 05.02.11].

Woolley, J.K., Limperos, A.M. Beth, M. 2010. The 2008 Presidential Election,

2.0: A Content Analysis of User-Generated Political Facebook Groups. *Mass Communication and Society.* 13(5), 631-652. Doi:10.1080/15205436.2010.516864 [accessed 03.20.11].

Wright, L. 2006. ASIO scans Muslim web surfers. Available from: http://www.news.com.au/national/asio-scans-muslim-web-surfers/story-e6frfkx0-1111112257310 [accessed 04.14.11].

Wright, R. 2009. In Iran, One Woman's Death May Have Many Consequences. Available from: http://www.time.com/time/world/article/0,8599,1906049,00.html [accessed 04.20.11].

Wtwu. 2011. Hints and Tips for Whistleblowers. Available from: https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/ht4w/index.html [accessed 04.25.11].

YouTube. 2011. Teenage Safety. Available from: http://www.google.com/support/youtube/bin/answer.py?hl=en-GB&answer=126262 [accessed 04.11.11].

The author *Dr. Geoff Dean* is Associate Professor in the School of Justice in the Faculty of Law at the Queensland University of Technology in Brisbane, Australia. His current areas of expertise, teaching specialisation and research are in Knowledge-Managed Policing, the cognitive psychology of investigative thinking, criminal and terrorism profiling, global organised crime and international policing. Dr. Dean has extensive publications in international journals and is the principal author of the book *Knowledge Management in Policing and Law Enforcement: Foundations, Structures, Applications* published by Oxford University Press in the UK in 2007. Dr. Dean was principal Guest Editor of a Special Issue on 'Local Research Links to Global Policing' in *Police Practice and Research: An International Journal*, Vol 9, No.4 in 2008. His latest book as principal author is *Organised Crime: Policing Illegal Business Entrepreneurialism* published in UK in 2010 by Oxford University Press.

The author *Dr. Peter Bell* is a Senior Lecturer and the Director of Postgraduate Studies at the School of Justice in the Faculty of Law. He has wide and diverse experience in policing, law enforcement and security including senior analytical and operational positions with the Queensland Police Service, the Australian Bureau of Criminal Intelligence, the Australian Federal Police and the Organised Crime Agency of British Columbia- Canada (OCABC). Dr Bell has written extensively for police/security agencies on topics to do with official corruption, international drug trafficking, terrorism, critical infrastructure security and transnational organised crime.

And the author *Jack Newman* holds a Bachelor of Justice majoring in Policing and Criminology, and Graduate Certificate in Intelligence. He is currently undertaking the Masters of Justice (Intelligence) at Queensland University of Technology. His research interests include the use of social media for political activism and terrorism, censorship, policing and law enforcement, and intelligence.