An Analysis of Online Terrorist Recruiting and Propaganda Strategies

https://www.e-ir.info/2017/07/19/an-analysis-of-online-terrorist-recruiting-and-propaganda-strategies/

MARK TAYLOR, JUL 19 2017

Through a critical examination of the online recruitment and propaganda strategies of terrorist organisations, their evolution, reasons for their appeal and governmental responses aimed at countering them, this paper proposes to advance a strategic response methodology which may augment current strategies aimed at circumventing online extremism. It will be argued that terrorist organisations have increasingly seized upon the opportunity, afforded by the rapid emergence of new Internet technologies, to exploit anti-western sentiments among Muslims *en masse*, and consequently, to ramp-up both their online recruitment strategies and the mass dissemination of their ideological propaganda. Additionally, that government programs, to date, have not been adept at combating this rising phenomenon. By examining the current scholarly literature regarding online terrorist propaganda and recruitment, its evolution, motivational attraction and how governments have sought to deal with it, a clearer picture can be discerned regarding why it has increased and what can be done to attenuate against it. Upon examination, technological advances and web-based innovation were seen to be driving the growth in online terrorist propaganda and recruitment, fueled by long-unresolved grievances existing in segments of the Islamic community. The ease of access and anonymity afforded by online technologies may be seen to have enabled terrorist groups to more easily, and without fear of capture, exploit these feelings of injustice utilising the online environment. Lastly, that government programs aimed towards countering this online threat have shown nominal efficacy and that a more proactive approach utilising intelligence-led interventions may be of additional benefit.

The Evolutionary Reshaping of Online Terrorist Recruitment and Propaganda Strategies

The evolution of online terrorist organisation recruitment and propaganda strategies, necessitated in response to heightened securitisation, has occurred in parallel with technological change,. Historically, the reach of terrorist recruitment/propaganda strategies was technologically and geographically constrained. Audiovisual and print media attention provided limited exposure to subjective media representations of their cause. The 1990s saw the rise of Al Qaeda who extended the terrorist's reach beyond the mainstream Western media, capitalising on sympathetic Middle Eastern journalistic sources.[1]

Terrorist use of Web 1.0 – The World Wide Web

The late 1990s saw terrorist organisations beginning to harness the new Internet technologies for fundraising and publicity purposes. This media afforded greater autonomy regarding their message content and audience targeting.[2] By 1999, the Internet became the principal arena for the disseminating jihadist propaganda.[3] Post 9/11, Al Qaeda diversified, providing multilingual translations of their online propaganda.[4] After the US invasion of Afghanistan, a demoralised Al Qaeda altered their message. Foreign adherents were now called to wage jihad within their home countries with the methodological training provided through online terrorist channels. By 2005, 40 terrorist organisations maintained an online presence involving over 4500 websites and YouTube's advent enabled the worldwide dissemination of professional looking audiovisual propaganda and tradecraft videos.

Terrorist use of Web 2.0 – Social Networking

The 2000s saw a new medium for the distribution of terrorist propaganda through the advent of social media. Unlike web 1.0 technologies, social media enabled back and forth between terrorists and their audience and the ability to target recruitees demographically.[5] This professionalisation increased their ability to mass recruit and disseminate propaganda in a way previously only available to nation states. [6] [7] Radicalization becoming more of a pull than a push game resulting in an explosion in the number of new adherents flocking to online terrorist causes.[8] The rise of the Islamic State (IS) in the 2010s continued this media professionalisation push, further extending the reach of the terrorist message and increasing recruitment in the Middle East and worldwide. [9]

Reasons for The Appeal of Online Strategies for Recruiting and Propaganda

Firstly, taking the terrorist organisation's point of view, there is great appeal in the utilisation of online media for the dissemination of propaganda messages and for recruiting purposes. New media technology has resulted in professional looking online cause offerings falling within the capacity of organisations with minimal skill sets and budgetary resources. Additionally, high levels of anonymity and site relocation/transportability are afforded by online publication thereby allowing a lower risk of circumvention or apprehension by law enforcement. [10]

Secondly, the simplicity of accessing online resources and groups makes the online world an appealing and nurturing environment through which to participate in a terrorist cause or explore terrorist ideologies minus the harsh ramifications of actual physical involvement. [11] [12] The terrorist's strategy involves the provision of self-paced participation that may incrementally lead into later full-scale radicalisation. [13] [14] Through the exploitation of some widely held sentiments (the sense of religious discrimination and victimisation by Western powers that exists amongst some Islamic peoples), potential recruits are progressively exposed to indoctrination and organisational involvement.[15] An increasing sense of interconnectedness with other recruits and organisation members is cultivated in a perceptibly safe online experience.[16]

Today's most prominent terrorist group, IS, currently utilises online media strategies as their primary tool for propaganda and recruitment. They seek to disseminate emotionally charged media propaganda that appeals to a wide cross-section of people groups, personality types, sectarian affiliations and political motivations.[17] Gone are the days of simple ideological appeals based on a consistent unipolar message. The IS approach is not a complex one to discern; attract recruits into the fold using motivational messages and then indoctrinate them into the cause of forcefully establishing of an Islamic caliphate. [18] [19]

Governmental Response to Addressing Online Terrorist Recruitment and Propaganda

Given the significant power of attraction that modern terrorist organisations have acquired through their slick use of online media, it is clear that a great and necessary effort is required to stem the growth of their radicalising online presence. It must also be realised that this effort to combat online terrorist propaganda may result in the curtailment of some of the freedoms civilised society now takes for granted in exchange for greater security and the protection from terrorism that it affords.[20] However, other scholars are unconvinced that the terrorists' online presence is a significant factor in radicalisation.[21] Some assert that these online dialogues allow individuals to cathartically vent their frustrations without actually resorting to physical violence. [22] There are no guarantees that an individual who engages in violent online rhetoric will automatically follow through with acts of terrorism,[23] and there is a dearth of hard evidence showing that such a causal relationship exists beyond speculation.[24] Considered together, both outlooks carry some weight of truth and it would be an error to approach an analysis of online terrorist propaganda and recruitment without considering them both. Consequently, laissez-faire and/or highly reactive approaches to online extremism may equally be of assistance in curtailing the spread of terrorism.

Governments worldwide have enlisted a combination of three broad strategies which deal with online extremist narratives. A hard line strategy which seeks to suppress online extremist activity; a soft diplomacy strategy involving counter narratives, detente and the promotion of social pluralism aimed at counter radicalisation; and lastly, an intelligence-led strategy that utilises online extremist activity and the information that it provides to identify and physically prosecute those involved in terrorism.[25] Although all three are aimed at combating the spread of violent extremism, they interact with the online terrorist narrative in very different ways.[26] A number of significant real-

world applications of each follows, examining the practical merits and shortcomings of each approach.

Hard Line Censorship, Securitisation and Deterrence Strategy

The majority of governments display some elements of zero tolerance 'deny access and/or delete' policies in their approach to dealing with online spaces that are engaged in terrorist propaganda or recruiting. The denial of access to an unfiltered version of the Internet or the assertive deletion of terrorist content are a significant tool in the online counter-terrorism fight. China for example, has been quite successful in countering dissenting online voices (including terrorist ones), by using authoritarian deny and delete policies that seek to control the information being made available to its citizens. The strategy has successfully prevented outside propaganda from reaching the vast majority of the populace even though some Internet users have been able to circumvent these policies and gain some degree of unfettered Internet access.[27] However, China's successful application has been the exception rather than the rule. In most international applications of this strategy, technological innovation and the inattention to detail on the part of those performing the blocking/deleting has allowed this online counter-radicalisation method to be undermined. For example, the government of Syria in 2012 sought, but failed, to limit the dissemination of online propaganda regarding a popular uprising through denying 90% of the population access to Internet. Again in 2014, the Turkish government sought to delete online anti-government rhetoric, again unsuccessfully. The dissenting voices found an alternate route using cellphone instant messaging to communicate their propaganda. Lastly, in 2014 during the growing conflict in Iraq, citizens were denied access to social media but still found ways to communicate using alternate unblocked web-based platforms.[28]

No doubt, Western governments and intelligence agencies, utilising superior technologies and personnel, have had greater success blocking/deleting terrorist propaganda sites. However, despite this technological superiority, they still fall victim to the same problems encountered in the previous examples. Technological advances and the dynamic nature of the Internet have similarly thwarted their efforts to effectively control content. As fast as one site/group/application is dealt with, another one arises to fill the void.[29] There appears to be no long term solution in this strategy, rather, it seems a decidedly stop-gap measure. It also bears consideration how these strategies are effected by the differing political environments that may exist at the time of their deployment. These hard line strategies are more in tune with realist-oriented political parties who would be more inclined to enact the legislation necessary for their efficient conduct. Conversely, liberal political approaches may encounter greater levels of philosophical and moral resistance within their ranks and may have qualms regarding the implementation of the enabling legislation. Furthermore, attempts to enact this type of strategy within Australia may be impeded by the guaranteed civic freedoms that the nation embraces. The strategy may impinge upon the common law right to personal privacy and represent a stifling of the civil liberties of freedom of expression and association. Additionally, the open Internet access that exists in Australia may also pose significant barriers to the strategy's enactment. Any move toward a more hard line approach would likely provoke a public backlash and would provide a staunch political headwind for any political party seeking to bring them into being. Such strategies may additionally work to push illegal terrorist communications further below the radar and negate any benefit being provided.

Soft Line Diplomacy Strategy – Countering Violent Extremism (CVE)

An alternate strategy involves using soft power diplomatic methods in order to disarm the terrorists' extremist message. The strategy utilises community based programs promoting social cohesion and the demarginalisation of groups at risk of becoming radicalised.[30] Additionally, it enlists both government departments and local moderate Islamic groups to disseminate counter narratives which challenges those espoused by online terrorists.[31] However, this has been purported to have had at most, a limited degree of success,[32] being hamstrung by the lack of credibility afforded to government instituted programs by the broader Islamic community.[33]

Both the UK 2011 counter-terrorism strategy (in particular, the 'Prevent' section),[34] and the 2014 report on Counter-Terrorism[35] incorporate formal approaches of this type within their framework for dealing with online radicalisation. These approaches have been enacted with what may be regarded as a questionable degree of success.[36] [37] Money was spent and the instigators of programs were lauded for their novel approaches, however little was provided by way of concrete empirical evidence which pointed to any specific program's efficacy at reducing

radicalisation. The UK's approach, involving the co-opting of Islamic community leaders in its counter-radicalisation programs, has drawn additional criticism. It has been argued that it has bordered on the promotion of Islamic belief systems, and unintentionally, IS extremist standpoints as well.[38] Similarly, Australia has mimicked the UK approach as delineated within the 2012 'National Counter-Terrorism Plan' (in particular, the 'resilience' section).[39] [40] The Australian policy also involves the shoring up of collective harmony and the challenging of terrorist dogma with alternative viewpoints.[41] As with the UK example, the Australian approach has suffered similar criticisms owing to the lack of empirical evidence regarding its efficacy[42] and by its general lack of acceptance in the Islamic community whose help it was aiming to co-opt.[43]

Most recently, the current round of grants for the countering violent extremism program were retrospectively assessed by the Australian National Audit Office (ANAO). Gross deficiencies were revealed regarding the Attorney-General's department's (AGD) assessment of the eligibility and merit of grant applications. The audit also revealed communication failures between funding recipients and the AGD regarding referral of at risk individuals to appropriate programs.[44] In their defence, these soft power programs are poorly funded compared to securitisation programs and it is unsurprising that they are mismanaged and poorly conceived. Many programs, do however, provide a sense of community co-option[45] with which the government can attempt to placate critics of the its predominantly securitised approach to CVE. Ultimately there is little incontrovertible proof of their effectiveness, leaving one to wonder if they ever represented more than a cheaply funded propaganda ruse?

Despite the poor performance of these programs, some other successes have presented a glimmer of hope. Indonesian and Singaporean de-radicalisation programs have focused on the disparity between the terrorist message and the characteristic desires of today's youth, successfully helping to dampen the appeal of the radicalising message to the terrorists' target audience. [46]

Another contemporary approach has emerged in the mass posting of humorous Internet 'memes' that attempt to ridicule, subvert and diminish the impact of the online messages distributed by terrorist groups, especially those that portray acts of terrorist violence. This is an approach mirroring the 1970's counter-culture movement of political jamming that utilises satire to highlight and reinforce counter-ideological thought. This approach has shown some anecdotal effectiveness in undermining the impact of online videos depicting terror acts such as beheadings. Rather than the terrorist perpetrators seeming to be heroes (so called Jihadi-cool), they are ridiculed as being fools, hence detracting from their mass appeal to young Muslim audiences.[47]

Intelligence-Led Collection Strategy (The Laissez-Faire Approach)

The last of the three presented strategies involves the use of intelligence services to monitor jihadist internet postings, utilising them to provide information with which to understand the terrorist groups who authored them and to formulate operations against them. This strategy involves predominantly covert collection and does not directly seek to interfere with the propaganda content that is posted online. Instead, the content is left as an in-vivo asset thorough which to garner valuable informational leverage against terrorist operations rather than as a risk which needs to be removed or counteracted against. [48] The downside is that this approach has little direct effect on curtailing the radicalising effect of online terrorist content on its target audience.

All three presented strategies are generally operationalised by attacking the message and/or physically removing the terrorist from the equation. As mentioned, their efficacy has been questionable. A new, alternate, intelligence-led approach may be required which serves to augment these three approaches, hence, providing a more encompassing counter-propaganda strategy. One such strategy may involve extending on the current intelligence-led approach, going beyond its use of covert surveillance and prosecution towards a remit which is more action oriented and useful for undermining terrorist narratives. Such a strategy would likely take the form of covertly obtaining intelligence about those individuals who are authoring terrorist propaganda online, the type of information that could be used to discredit them in the eyes of the Islamic community, i.e. alcohol or drug use, sexual leanings or theft of the cause's money. Rather than using this information to apprehend the author or shut down the site, it could be mass disseminated through the news media and back channels. Consequently, the person's credibility would be compromised and their audience triggered to question the believability of their online discourse. The 'perseverance of

belief' phenomenon dictates that attacking a belief system (terrorist discourse) is ineffective, as the discourse, at face value, may adhere to Islamic theology thereby making it difficult to debunk. It is much easier to turn a group against an individual than it is to turn them against a belief or an ideology, as people lack the same sense of unquestioning trust toward an individual.[49] The psychology behind this approach revolves around rumour theory. Rumour theory asserts that an ideological representation is difficult to debunk,[50] especially if it is disseminated by a trusted source.[51] However, if you undermine the credibility of the source, the propaganda message they are disseminating becomes easily challenged, and historically, once a terrorist organisation's ideological support is compromised, their ongoing viability is jeopardised.[52] Furthermore, once a believable accusation/slur is made against a trusted terrorist source of online propaganda, despite any attempts to rebut it, the accusation remains intact (mud sticks). [53] In fact, attempts to dislodge the slur actually add to the believability of the accusation.[54] [55] Going one step further, intelligence services may even fabricate credible evidence to undermine the legitimacy of terrorist voices. However, this may require a shift in ethical boundaries similar to the shift that occurs in times of war. Obtaining or fabricating embarrassing personal information about a terrorist that can be used to undermine their legitimacy in the eyes of other Islamic believers may represent an indirect but powerful tool with which to combat terrorist propaganda and recruiting strategies.[56]

The war against online extremism has recently taken on new importance in light of the Islamic State movement's transformation into a pseudo-state, led by a pseudo-conventional army.[57] Moving beyond the existing tripartite arsenal of approaches involving CVE, online securitisation and intelligence-led collection strategies, this more aggressively assertive intelligence-led approach may provide additional strength and effectiveness in the online war of information. Intelligence about a terrorist could be garnered utilising social media analysis tools to identify possible informational sources. Private communications (phone/Internet usage, GPS data) could also be monitored with a court order, as well as financial records in order to identify exploitable intelligence. Phishing the target may also provide valuable insight into their private dealings. [58] Once useful intelligence is obtained and a suitable derogatory rumour concocted, it could then be quickly transmitted through social media and its effect shaped by an online army of seemingly credible pseudo-peers. A possible logistical approach would be for the Australian government to stand up a dedicated section akin to that employed by the Chinese intelligence services ('wǔmáo dǎng' or '50 Cent Party'). Their sole task involves the monitoring of web based social media content and inserting regime propaganda utilising fictitious online personas.[59] The advent of digital media has meant that this rumour based propaganda approach can precisely deliver dis-information to an audience with a high degree of targeting specificity. Furthermore, the effects can be easily measured using social media metrics in order to evaluate the efficacy of the approach.[60] The potential negative consequences of this approach would be minimal beyond the possibility that some terrorists may be marginalised from their support base and may become increasingly desperate for approval resulting in increasingly belligerent online rhetoric and behaviour. However, this escalation may further serve to discredit the terrorist cause in the eyes of a rational audience. Great care would need to be taken to ensure that terrorists who are increasingly marginalised are contained before they can resort to physical expressions of violent extremism. The strategy also demands the maintenance of a covert status to ensure its operational functionality.

Conclusion

The rise to prominence of online terrorist recruitment and propaganda strategies has become a major concern of national security services worldwide. Terrorist organisations, afforded an increased opportunity to spread their ideological stance and to recruit new membership, have seized upon technological advances in Internet media distribution and online anonymity. The goal being to exploit anti-Western sentiment resident in the Islamic community for their own ideological ends. This represents a significant but highly effective departure from the conventional mass media dissemination channels that terrorists utilised in the past and has resulted in the greatly increased efficacy of their operations. Government responses formulated to combat this rising threat have been characterised by three distinct strategies: securitisation, diplomacy and intelligence-led collection/prosecution. However, the strategies have had limited success owing to their inability to cope with the dynamic and resilient nature of online propaganda and difficulties in co-opting an already marginalised Islamic population who maintain a broad distrust of Western government authority. A possible solution has been proposed that when used in conjunction with existing government strategies and extending on the existing intelligence-led collection approach, may provide more effective disruption of terrorist radicalisation strategies. This extension aims at exploiting covertly acquired personal information about a

terrorist that can be utilised to discredit their standing in the Islamic community, hence, undermining the radicalising message that they disseminate online. Future research may seek to examine how the proposed logistical methodology derived from the Chinese 'wǔmáo dǎng' strategy may be successfully operationalised in Australia and how it may work to heighten the efficacy of the existing counter radicalisation strategies.

References

Agarwal, S., Applying Social Media Intelligence for Predicting and Identifying On-line Radicalization and Civil Unrest Oriented Threats, PhD Thesis, Indraprastha Institute of Information Technology, 2015.

Aly, A., Macdonald, S., Jarvis, L. and Chen, T., 'Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization', *Studies in Conflict & Terrorism*, vol. 0, no. 0, 2016, pp. 1–9.

Alzona, R., 'Israeli Embassy says understanding social media can prevent terrorism', *Philippine Business Daily Mirror*, 21 February 2016.

Attorney General's Department: Countering Violent Extremism Unit, 'Living Safe Together: Building Community Resilience to Violent Extremism', [web site], http://www.livingsafetogether.gov.au/partners/Pages/communities.aspx, (accessed 13 June 2016).

Attorney General's Department, *National Counter-Terrorism Plan*, 2012, p. 13, https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-counter-terrorism-plan-2012.pdf, (accessed 17 June 2016).

Bergin, A., 'Debunking extremism needs more than a lame website, it needs strategic, bold changes', *Sydney Morning Herald*, 15 January 2015, http://www.smh.com.au/comment/debunking-extremism-needs-more-than-a-lame-website-it-needs-strategic-bold-changes-20150114-12nq5f.html, (accessed 02 June 2016).

Conway, M., 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism*, 2016, pp. 1-22.

Cronin, A., 'ISIS is not a terrorist group; Why Counterterrorism Won't Stop the Latest Jihadist Threat', *Foreign Affairs*, vol. 94, no. 2, 2015, http://go.galegroup.com/ps/i.do?id=GALE|A412275541&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=, (accessed 13 June 2016).

Dean, G., Bell, P. and Newman, J., 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

DiFonzo, N. and Bordia, P., *Rumor Psychology: Social and Organizational Approaches*, Washington, DC, American Psychological Association, 2007.

European Policy Planners' Network, *The Role of Civil Society in Counter-Radicalisation and De-Radicalisation*, London, Institute for Strategic Dialogue, 2010, http://www.strategicdialogue.org/PPN%20Paper%20%20Community%20Engagement_FORWEBSITE.pdf, (accessed 1 June 2016).

House of Commons Home Affairs Committee, *Counter-terrorism: Seventeenth Report of Session 2013– 14,* London, The Stationery Office, 9 May 2014.

Huey, L., 'This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming', *Journal of Terrorism Research*, vol. 6, no. 2, 2015, pp. 1-16.

Ivan, A., Iov, C., Lutai, R. and Grad, M., 'Social Media Intelligence: Opportunities and Limitations',*CES Working Papers*, vol. 7, no. 2a, 2015, pp. 505-510.

King, G., Pan, J., and Roberts, M., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*, Working Paper, Harvard University, 2016.

Lambert, R., 'Competing Counter-radicalisation Models in the UK', in R. Coolsaet (ed.),*Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences,* Farnham, Ashgate Publishing, 2011.

Lee, N., *Facebook Nation: Total Information Awareness*, New York, Springer, 2014.

Poe, M. and Cronin, A., 'How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns',*New Books in History Blog*, [podcast], 28 May 2010, http://ir.uiowa.edu/context/history_nbih/article/1108/type/native/viewcontent, (accessed 10 June 2016).

Rabasa, A., 'Where Are We in The "War of Ideas"?', in B. Jenkins and J. Godges (eds.),*The Long Shadow of 9/11: America's Response to Terrorism*, Santa Monica, RAND Corporation, 2011.

Rawnsley, G., 'Old Wine in New Bottles: China–Taiwan Computer-Based 'Information Warfare' and Propaganda', *International Affairs*, vol. 81, no. 5, 2005, pp. 1061–1078.

Sadler, D., 'How refugees are finding their feet at a drop-in football clinic', *ABC news*, 16 Sep 2016, http://www.abc.net.au/news/2016-09-15/refugees-finding-their-feet-at-drop-in-football-clinic/7842998, (accessed 13 October 2016).

Secretary of State for the Home Department, *Contest: The United Kingdom's Strategy for Countering Terrorism* , Norwich, The Stationery Office, 2011.

Shanahan, R., 'Sectarian Violence: The Threat to Australia', *National Security College Occasional Paper*, no. 7, 2014.

Smith, A., 'Countering violent extremism – the 'soft power' approach', *The Strategist: Australian Strategic Policy Institute Blog,* [web blog], 31 January 2013, http://www.aspistrategist.org.au/countering-violent-extremism-the-soft-power-approach/, (accessed 20 June 2016).

The Auditor-General ANAO, *The Design of, and Award of Funding Under, the Living Safe Together Grants Programme: Report No.12 2016-17 Performance Audit*, Canberra, Australian National Audit Office, 2016, https://www.anao.gov.au/sites/g/files/net1661/f/ANAO_Report_2016-2017_12.pdf, (accessed 13 October 2016).

Werbin, K., 'Spookipedia: Intelligence, Social Media and Biopolitics', *Media, Culture & Society*, vol. 33, no. 8, 2011, pp. 1254–1265.

[1] A. Aly, S. Macdonald, L. Jarvis and T. Chen, 'Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization', *Studies in Conflict & Terrorism*, vol. 0, no. 0, 2016, pp. 2-3.

[2] Dec. 17, 1996, The Tupac Amaru communist rebels launched a web site which represented a groundbreaking moment for terrorist organisations in that this was the first time a terrorist group could reach a worldwide audience utilising its own distribution channels free from outside censorship or the reshaping of its message.

[3] A. Awan, *The Virtual Jihad: An Increasingly Legitimate Form of Warfare* , 2010, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[4] Aly et al., *op. cit.*, p. 3.

[5] J. Woolley, A. Limperos and M. Beth, 'The 2008 Presidential Election, 2.0: A Content Analysis of User- Generated Political Facebook Groups', *Mass Communication and Society*, vol. 13, no. 5, 2010, pp. 631-652, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[6] S. Agarwal, Applying Social Media Intelligence for Predicting and Identifying On-line Radicalization and Civil Unrest Oriented Threats, PhD Thesis, Indraprastha Institute of Information Technology, 2015, p. 1.

[7] J. Earl and K. Kimport, *Digitally Enabled Social Change: Activism in the Internet Age* , Boston, Massachusetts Institute of Technology Publishing, 2011, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[8] Department of Homeland Security, *Terrorist use of Social Networking Sites: Facebook Case Study* , 2010, http://publicintelligence.net/ufouoles-dhs-terrorist-use-of-social-networking-Facebook-case-study, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[9] L. Huey, 'This is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming', *Journal of Terrorism Research*, vol. 6, no. 2, 2015, p. 2.

[10] Agarwal, *op. cit.*, p. 2.

[11] *ibid.*, p. 1.

[12] A. Ivan, C. Iov, R. Lutai and M. Grad, 'Social Media Intelligence: Opportunities and Limitations',*CES Working Papers*, vol. 7, no. 2a, 2015, p. 505.

[13] Huey, *op. cit.*, p. 2.

[14] J. White, 'Virtual Indoctrination and the Digihad: The Evolution of Al-Qaeda's Media Strategy',*Small Wars Journal*, 19 November 2012, cited in A. Aly, S. Macdonald, L. Jarvis and T. Chen, 'Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization', *Studies in Conflict & Terrorism*, vol. 0, no. 0, 2016, p. 4.

[15] Aly et al., *op. cit.*, p. 4.

[16] D. Gray and A. Head, 'The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven', *European Journal of Scientific Research*, vol. 25, no. 3, 2009, pp. 396-404, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[17] A. Cronin, 'ISIS is not a terrorist group; Why Counterterrorism Won't Stop the Latest Jihadist Threat',*Foreign Affairs*, vol. 94, no. 2, 2015, http://go.galegroup.com/ps/i.do?id=GALE|A412275541&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=, (accessed 13 June 2016).

[18] Aly et al., *loc. cit.*

[19] Aly et al., *op. cit*., p. 5.

[20] R. Alzona, 'Israeli Embassy says understanding social media can prevent terrorism',*Philippine Business Daily Mirror*, 21 February 2016.

[21] M. Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism*, 2016, p. 1.

[22] G. Ramsay, 'Relocating the Virtual War', *Defence Against Terrorism Review*, vol. 2, no. 1, 2009, p. 35, cited in M. Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism*, 2016, p. 4.

[23] Intelligence and Security Committee of Parliament, *Report on the Intelligence Relating to the Murder of Fusilier Lee Rigby*, London, Her Majesty's Stationery Office, 2014, p. 131, cited in M. Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research', *Studies in Conflict & Terrorism*, 2016, p. 4.

[24] C. Leuprecht and D. Skillicorn, 'Radicalisation: What (If Anything) is to be Done? When Facts Get in the Way of a Good Story', *Home Team Journal*, vol. 3, 2011, pp. 38-46, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[25] *loc. cit.*

[26] A. Bergin, S. Osman, C. Ungerer and N. Yasin, *Countering Internet Radicalisation in Southeast Asia*, Canberra, Australian Strategic Policy Institute, 2009, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[27] N. Lee, *Facebook Nation: Total Information Awareness*, New York, Springer, 2014, p. 228.

[28] *ibid.*, p. 230.

[29] G. Weimann, 'Terror on Facebook, Twitter, and YouTube', *The Brown Journal of World Affairs*, vol. 16, no. 2, 2010, pp. 45-54, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[30] I. Caldwell, 'Terror on YouTube', *Forensic Examiner*, vol. 17, no. 3, 2008, pp. 80-83, cited in G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[31] . G. Dean, P. Bell and J. Newman, 'The Dark Side of Social Media: Review of Online Terrorism', *Pakistan Journal of Criminology*, vol. 4, no. 2, 2012, http://go.galegroup.com/ps/i.do?id=GALE%7CA313840278&v=2.1&u=macquarie&it=r&p=EAIM&sw=w&asid=0c5d2400e5ffe21de5ed44f219358017, (accessed 15 June 2016).

[32] European Policy Planners' Network, *The Role of Civil Society in Counter-Radicalisation and De-Radicalisation* , London, Institute for Strategic Dialogue, 2010, p. 25, http://www.strategicdialogue.org/PPN%20Paper%20%20Community%20Engagement_FORWEBSITE.pdf,

(accessed 1 June 2016).

[33] Huey, *op. cit.*, p. 9.

[34] Secretary of State for the Home Department, *Contest: The United Kingdom's Strategy for Countering Terrorism* , Norwich, The Stationery Office, 2011, p. 1.

[35] House of Commons Home Affairs Committee, *Counter-terrorism: Seventeenth Report of Session 2013–14,* London, The Stationery Office, 9 May 2014, pp. 33-34.

[36] *ibid.*, pp. 41-42.

[37] R. Lambert, 'Competing Counter-radicalisation Models in the UK', in R. Coolsaet (ed.),*Jihadi Terrorism and the Radicalisation Challenge: European and American Experiences,* Farnham, Ashgate Publishing, 2011, pp. 215-216.

[38] A. Rabasa, 'Where Are We in The "War of Ideas"?', in B. Jenkins and J. Godges (eds.),*The Long Shadow of 9/11: America's Response to Terrorism*, Santa Monica, RAND Corporation, 2011, p. 64.

[39] Attorney General's Department, *National Counter-Terrorism Plan*, 2012, p. 13, https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-counter-terrorism-plan-2012.pdf, (accessed 17 June 2016).

[40] A. Smith, 'Countering violent extremism – the 'soft power' approach', *The Strategist: Australian Strategic Policy Institute Blog,* [web blog], 31 January 2013, http://www.aspistrategist.org.au/countering-violent-extremism-the-soft-power-approach/, (accessed 20 June 2016).

[41] Attorney General's Department: Countering Violent Extremism Unit, 'Living Safe Together: Building Community Resilience to Violent Extremism', [web site], http://www.livingsafetogether.gov.au/partners/Pages/communities.aspx, (accessed 13 June 2016).

[42] R. Shanahan, 'Sectarian Violence: The Threat to Australia', *National Security College Occasional Paper*, no. 7, 2014, p. 10.

[43] A. Bergin, 'Debunking extremism needs more than a lame website, it needs strategic, bold changes',*Sydney Morning Herald*, 15 January 2015, http://www.smh.com.au/comment/debunking-extremism-needs-more-than-a-lame-website-it-needs-strategic-bold-changes-20150114-12nq5f.html, (accessed 02 June 2016).

[44] The Auditor-General ANAO, *The Design of, and Award of Funding Under, the Living Safe Together Grants Programme: Report No.12 2016-17 Performance Audit*, Canberra, Australian National Audit Office, 2016, p. 8, https://www.anao.gov.au/sites/g/files/net1661/f/ANAO_Report_2016-2017_12.pdf, (accessed 13 October 2016).

[45] D. Sadler, 'How refugees are finding their feet at a drop-in football clinic', *ABC news*, 16 Sep 2016, http://www.abc.net.au/news/2016-09-15/refugees-finding-their-feet-at-drop-in-football-clinic/7842998, (accessed 13 October 2016).

[46] Cronin, *loc. cit.*

[47] Huey, *op. cit.*, p. 3.

[48] K. Werbin, 'Spookipedia: Intelligence, Social Media and Biopolitics', *Media, Culture & Society*, vol. 33, no. 8, 2011, p. 1255.

[49] N. DiFonzo and P. Bordia, *Rumor Psychology: Social and Organizational Approaches*, Washington, DC,

American Psychological Association, 2007, p. 243.

[50] *ibid.,* p. 216.

[51] *ibid.,* p. 234.

[52] M. Poe and A. Cronin, 'How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns', *New Books in History Blog*, [podcast], 28 May 2010, http://ir.uiowa.edu/context/history_nbih/article/1108/type/native/viewcontent, (accessed 10 June 2016).

[53] *ibid.,* p. 222.

[54] *ibid.,* p. 212.

[55] *ibid.,* p. 224.

[56] Cronin, *loc. cit.*

[57] Cronin, *loc. cit.*

[58] Phishing is the practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords, credit card numbers or any manner of personal details or beliefs online.

[59] G. King, J. Pan, and M. Roberts, *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*, Working Paper, Harvard University, 2016, pp. 33-34.

[60] G. Rawnsley, 'Old Wine in New Bottles: China–Taiwan Computer-Based 'Information Warfare' and Propaganda', *International Affairs*, vol. 81, no. 5, 2005, pp. 1067-1068.

Written by: Mark Taylor
Written at: Macquarie University Department of Security Studies and Criminology
Written for: Professor Benjamin Schreer
Date written: October 2016