2010

"Make A Bomb In Your Mums Kitchen": Cyber Recruiting And Socialisation of 'White Moors' and Home Grown Jihadists

Robyn Torok
Macquarie University

Originally published in the Proceedings of the 1st Australian Counter Terrorism Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

"Make A Bomb In Your Mums Kitchen": Cyber Recruiting And Socialisation of 'White Moors' and Home Grown Jihadists

Robyn Torok
Centre for Policing, Intelligence and Counter Terrorism
Macquarie University
Sydney, Australia
robyn.torok@mq.edu.au

The times have changed, and we must design a method of confrontation, which is in accordance with the standards of the present time.

Al- Suri, Inspire Magazine 2010, p. 53

If you have the right to slander the Messenger of Allāh, we have the right to defend him. If it is part of your freedom of speech to defame Muḥammad, it is part of our religion to fight you.

Shaykh Anwar Al-Awlaki, Inspire Magazine 2010, p. 26

Abstract

As a consequence of the war on terror, al-Qaeda and associated jihad groups have evolved and made increasing use of internet technologies for cyber recruitment. Recently, there has been an increasing focus on recruiting home grown terrorists who can more easily escape the scrutiny of cross border entries. Case study analysis indicates that links do exist between cyber tools, radicalisation and terrorism, however, the strength and nature of these relationships is generally unclear. Evidence does seem to support that cyber tools are most significant in the initial phases of recruitment and radicalisation. Coupled with this is the strong evolution of the use of cyber tools from hosted jihad websites to the use of social networking sites such as Facebook and MySpace as well as forums such as Yahoo groups. Additionally, al-Qaeda's latest development is an online magazine that contains a wide range of material from inspirational narratives to practical bomb making techniques. It is argued that these links between evolving cyber tools and cyber recruitment/radicalisation must be taken as a serious threat with possible responses outlined.

Keywords

al-Qaeda, terrorist recruitment, cyber recruiting, internet terrorism, radicalisation, social networking

INTRODUCTION

Since 9/11 and the subsequent war on terror, al-Qaeda and other Islamic jihad groups(1) have been very adept at evolving to the changing shifts caused by continual attacks to its base of operations resulting in restrictions in their ability to operate openly. One of the primary areas of adaptation is in the use of internet technology to support a number of its strategic and operational objectives that include recruiting, fundraising, strategic direction and research (McNeal, 2007). In addition, internet technology also opens up a worldwide audience able to access extremist views and form networks, all in a ubiquitous and virtually untraceable environment (O'Rourke, 2007). Importantly, the internet provides an essential media battlefield as part of their terrorism strategy as al-Qaeda's Dr. al-Zawahiri states: 'We are in a battle, and more than half of this battle is taking place in the battlefield of the media. We are in a media battle for the hearts and minds of our *umma*' (Michael, 2009, p. 142). Therefore, it is this battle for hearts and minds that will be addressed.

As the title of this paper suggests, the focus of this paper is on how al-Qaeda attempts to use cyber technologies to recruit and engage home grown terrorists and also create converts to radical Islam, known as 'White Moors' (Michael, 2009). Initially, the focus will be on why this specific target group is so important as part of al-Qaeda's strategy to target the West. Subsequently, it is imperative to examine how the internet is an important part of that strategy, a strategy that complements the cultural notion of terrorism as theatre (Cowen, 2006). A number of case studies will then be presented followed by proposed responses.

TARGETS: WHY "WHITE MOORS" AND HOME GROWN JIHADISTS?

Research by Weimann (2008) on the target audiences of terrorist websites indicates that their intended audience is actually very broad and includes potential recruits, the international community and its enemies. However, the focus on potential recruits is an important aspect and often involves more culturally sophisticated planning coupled with

more tech savvy skills in its implementation. Key aspects include the use of colour, latest multimedia technologies, professional finish and interactivity (McNeal, 2007). Many of these sites are targeted at younger males, with reports in the United Kingdom (UK) indicating terrorist groups specifically targeting male university undergraduates and even secondary students (Mendez, 2008). Furthermore, it is the disaffected and the alienated that are especially vulnerable to the 'seductive' efforts of recruiters (Murphy, 2007). These groups include diasporic communities (Awan, 2007) as well as first and second generation Muslims who are 'citizens in name but not culturally or socially.' (Leiken, 2005, p. 123). Nevertheless, it is this 'citizen in name' aspect that is important, just like the ring of Roman citizenship gave freedom to travel throughout the Roman Empire, likewise a 'Western' passport gives greater freedom to travel throughout the Western world. This is especially important given that some of those travelling on Middle-Eastern, North African or Asian passports are coming under increasing scrutiny given their regional reputations for terrorist activity, radicalism and training activities (Michael, 2009).

However, now it is this freedom to travel throughout Europe and the West that is causing concern for both European and US officials (Leiken, 2005; Michael, 2009). For this reason 'White Moors' and home grown jihadists can be considered prized recruits. Coupled with this, there is the increasing individualisation of the concept of *jihad* as part of a global resistance (Michael, 2009). One of al-Qaeda's most notable strategists, al-Suri, has articulated the power of the internet as a key tool in promoting individual terrorism (Michael, 2009). It is therefore critical to look at the dynamics of how the internet is used as such an important strategic tool in promoting home grown terrorism.

STRATEGY: INTER(N)ETWORKS

Strategically, al-Qaeda is forming a vast series of internet networks (inter(N)etworks). They provide a platform to reach a worldwide audience while giving leaders much greater control over their message compared to other more traditional media (print, television) (Anderson, 2003; Conway, 2006). Moreover, the internet platform allows terrorists groups to release large unlimited, uncensored amounts of propaganda, inspire supporters, target recruits and undermine Western media credibility (Conway, 2006; Lachow & Richardson, 2007; Maher, 2007). Lachow and Richardson (2007) argue that terrorist groups have become experts at manipulating public opinion and undermining media credibility by providing well presented 'news' services that are on par with the those of much larger and well established organisations. In terms of recruiting, the danger lies in the ability to expose potential recruits to large amounts of information quickly, and in an interesting multimedia format (Conway, 2006). What is most striking about the strategic use of internet technologies is the 'paradigm shift' they create by redirecting power from the state to individual members and society as a collective (Weimann, 2008, p. 83). In conceptualising how and why these new forms of terrorism are so internet dependent (Anderson, 2003), we can borrow some insights from social network research.

Insights from Social Network Research

As a consequence, at least in part, of using internet technology, terrorist groups have become more network oriented in their structures which allows actors to communicate free from space or organisational constraints at a very low cost (Conway, 2006). Social network theory is concerned with connections between actors rather than actors in isolation (Brass, Galaskiewicz, Greve, & Tsai, 2004; Matusitz, 2008). One of the foundational tenets of network research is that actors are part of an interconnected social network that has the potential to both constrain and create new behaviours (Brass, et al., 2004). Matusitz (2008) argues that there are many similarities between terrorist networks in antiquity (Jewish resistance to the Roman Empire) and modern day cyber networks. In particular is the 'Chain of trust', where individuals are introduced and then required to display certain attitudes and behaviours (Matusitz, 2008, p. 189). This is particularly the case with more interactive internet media such as chat rooms and social networking sites. Table 1 below summaries some important insights from interpersonal networks which are also relevant to cyber networks.

Table 1: Antecedents and Consequences of Interpersonal Networks (Based on Brass, et al., 2004, p. 796-798)

Antecedents	Consequences
Actor similarity – interactions tend to be among similar people (aims, interests).	**Attitude similarity** – interaction among similar actors creates similar attitudes
Personality – personality does affect social network patterns.	**Power** – central network positions are associated with power and influence

Social network research indicates that similar people tend to find each other (Table 1). Al-Qaeda and other groups endeavour to make that process as easy as possible. Consider also the impact of personality, with a disaffected youth networking with a strong radical terrorist recruiter. Most importantly, as a consequence of such interactions (whether

cyber or personal) is a change in attitude which in turn can impact on behaviour, especially when being directed by more central network actors. The question we turn to is, how have terrorist groups made the ability for similar actors to connect much easier?

Explosive Growth of Online Jihad

From an insignificant cyber presence pre-9/11, al-Qaeda now has a very strong cyber network that uses cutting edge technology (Murphy, 2007). This exponential growth in websites (Awan, 2007) has led to a matching growth in potential recruitment opportunities (McNeal, 2007). In one of the most comprehensive research studies on online terrorist websites, Weimann (2008, p. 75) reported that the number of terrorist websites grew from about 12 in 1998 to over 5300 at the end of 2006. What is perhaps even more disconcerting is the rapid rise of English speaking websites (over 100 reported in late 2007) (Michael, 2009, p. 143). Such a shift reflects attempts to create 'White Moors' from disaffected youth who can now easily access hundreds of English language sites, interact and be targeted by jihad recruiters (Jenkins, 2010). This new threat is perhaps one of the most pervasive cyber threats we face.

Which Is The Greater Threat: Cyber Terrorism Or Cyber Recruitment And Socialisation?

While acknowledging that the risk of cyber terrorism and hacking is very real, many scholars argue that the risk of cyber terrorism is overemphasised (Kohlmann, 2006; Lachow & Richardson, 2007; Lewis, 2005). While we should certainly not play down the threat of cyber terrorism into 'cyber graffiti' as Lewis (2005, p. 113) does, we need to avoid the other extreme of overstating 'science-fiction scenarios' (Kohlmann, 2006, p. 116). Kohlmann (2006) argues that the Unites States (US) online war on terror has been defensive and technology focussed, concentrating on protecting critical infrastructure. While the importance of cyber security should never be understated nor taken for granted, neither should be the dangers of unabated propaganda and cyber recruitment strategies (Lachow & Richardson, 2007). In answer to the question of which is the greater threat, in absolute terms, this is difficult to answer. However, in relative terms, cyber recruitment and socialisation is perhaps a greater threat, simply for the reason that we take cyber terrorism seriously and seek to constantly prevent attacks, while some Western nations are lagging behind in response to cyber recruitment and socialisation.

Recruitment Cyber Tools

In this section, cyber tools will be divided into three sections: Hosted sites, which include sites created and hosted by terrorist groups; Non-hosted sites, which look at exploiting free network sites such as social networking and message boards, and thirdly the focus will be on al-Qaeda's latest strategy – the online *Inspire* magazine.

Hosted sites

Terrorist created web sites convey their cause as defenders of the Islamic faith against the 'crusades' of the West (Lewis, 2005). These web sites are primarily an information tool used to challenge hegemonic Western views with those of their minority cause (Awan, 2007; Lewis, 2005). One of the key strategies for forwarding their propaganda goals is through the creation of 'alternative' news sources (Awan, 2007, p. 397). An impression of legitimacy is created through media savvy and high quality presentation (Awan, 2007). McNeal (2007) gives several examples of these 'news' services that include jehad.net (al-Qaeda's perspective on the war in Afghanistan), and azzam.com which features jihad biographies and encourages others to join the cause. Although these web sites are a tool for cyber recruitment, they are disadvantageous in that they rely on potential recruits seeking out and finding these sites. A better strategy for al-Qaeda and other jihad groups is to use well established Western sites (non-hosted sites) that already have a much larger online audience.

Non-hosted sites

Based on an in depth longitudinal study, Weimann (2008) argues that Yahoo has now become one of al-Qaeda's key recruiting and operational tools. Key features used include the use of email and related chat functions as well as Yahoo groups based on common interests (Weimann, 2008). It is these e-groups that have become a focal point of al-Qaeda's strategy. Not only are they present on Yahoo, but also on major social networking sites that include MySpace and Facebook(2). These groups pose an increased risk because they are legal, easy to create and manipulate, allow for discussion, interaction and transfers of data files. Furthermore, in congruence with social network research it provides an easy avenue for those with similar interests to connect (Weimann, 2008).

These e-groups can range from hate groups to sophisticated recruiting forums. Radical hate groups can quickly expand with Oboler (2008) giving the example of an anti-Israeli hate group growing to over 48000 members in just 18 months. More disturbingly, some e-groups are run and managed by leading al-Qaeda recruiters. Kohlmann (2008) provides an example of the now disbanded Muntada al-Ansar (The Supporters Forum) which featured high level recruiters from a number of Islamic Terrorist organisations. In fact, this forum was considered a 'virtual matchmaking service for budding Islamic militants searching for a path to jihad' (Kohlmann, 2008, p 8). Other affiliated terrorist groups have also clearly stated their intention to use social networking sites like Facebook as a media tool for the cause of jihad (Shaidle, 2009). As a further illustration, Anwar al-Awlaki, who was raised as an 'all American boy' and has since fled to Yemen, held an account on Facebook with a large following of disaffected youth before his account was finally shut down (Hamill, 2010). Additionally, Anwar was also an avid user of the multimedia site YouTube where he had posted over 5000 videos (Hamill, 2010).

New strategies: *Inspire* magazine

Al-Qaeda's latest cyber tool is a colourful, professionally produced online magazine called *Inspire* which was released in 2010. The first part of the title of this paper is a paraphrase of an *Inspire* article "Make a bomb in the kitchen of your mom" which gives detailed written instructions and illustrations on how to make a bomb using simple materials as part of open source jihad. Overall, the magazine has varied content that includes messages, words of encouragement, strategic advice, news, exhortations on giving to the poor (challenging Western capitalism), campaigns, and articles from prominent leaders such as Usama Bin Laden and al-Suri. Although the web site has been shut down, the magazine was not difficult to find and could easily be circulated as a simple portable document file (PDF) through chat rooms and social groups. This magazine would no doubt find appeal among disaffected youth.

(COUNTER) CULTURE: TERRORISM AS THEATRE

The internet is more than simply a propaganda tool, it is an essential mechanism for imparting and transferring the culture and ideology of the journey that terrorists take toward jihad (Awan, 2007).

Perhaps one of most fundamental aspects of this cultural identity is that of 'terrorism as theatre' (Awan, 2007; Cowen, 2006). Reflecting on the tragic events of 9/11, London and Bali, the media coverage presented a 'spectacle' designed to strike fear into the heart of Western civilisation. These events are critical to al-Qaeda's strategy because 'The act of political violence itself is still the best way to obtain publicity, not simply the circulation of information via the Internet.' (Anderson, 2003, p. 30). Terrorism as theatre is well suited to the internet where uncensored videos can be posted which contain events of graphic violence. These events include: IED (improvised explosive device) attacks and beheadings of Western hostages (Awan, 2007). Additional spectacles are provided by the testimonials of suicide bombers that exploit the use of overt graphic imagery (McNeal, 2007). Thus, internet technology allows for maximum psychological impact on the enemy, current supporters and potential recruits (Weimann, 2008).

A further distinction also needs to be made in terms of the culture of terrorism as theatre. Equally important, terrorists conceptualise themselves as a counter-culture, a resistance movement, seeking freedom from 'Western Crusaders'. Terrorists gain support for this concept by exploiting Western spectacles of violence (Awan, 2007). These include graphic images and videos of civilian casualties, violent videos posted by US marines and images of prisoner abuse. In addition, al-Qaeda is also keen to exploit controversies that support a Western/Muslim split such as the New York Mosque controversy and the associated threats from a Pastor to burn the Qur'an (Thomas, 2010). What raises concern here is that the disaffected youth being targeted also feel that they are a minority counter culture. Consequently, jihad recruiters seek to build a common interest and affinity with these youth in congruence with the antecedents of social network research.

CASE STUDIES

How successful have these aforementioned strategies for al-Qaeda's jihad? It is important to examine briefly a number of key case studies that involved the internet for recruitment or socialisation. Firstly, there are some important caveats to our understanding of the effectiveness of cyber recruitment strategies. The ability to study the effect of cyber tools on potential and new converts is exceedingly difficult. There is also the possibility that cyber recruitment tools are simply 'preaching to the converted' rather than causing any significant change (Awan, 2007, p. 400). More research is needed in this area including better methods of inquiry coupled with new conceptual models. Data, in the vast majority of cases, can only be gathered 'post fact', as a result of police investigations and court action.

In terms of statistics on home grown terrorism, the best evidence to date is a recent RAND corporation report on US domestic radicalisation. Upon investigating cases of domestic radicalisation between 9/11 and the end of 2009, Jenkins (2010) reported 46 cases totalling 125 persons. However, only 81 of these were indicted (Jenkins, 2010). Although these figures are relatively small, Jenkins (2010) did report a rising trend in the number of cases and individuals, particularly in 2009. These statistics do give some support for the effectiveness of al-Qaeda's cyber recruitment tools, especially given that Jenkins (2010) report cites that many jihadists actually began their journey on the internet as a place to connect with other disaffected and discontented individuals. To gain further insights, the role of the internet in four home grown terrorist case studies from around the world will be explored.

Case Study 1: Madrid Train Bombings 2004 and London Bombings 2005

A brief account of these cases presented by Awan (2007) illustrates that the Madrid bombers were inspired by online Iraqi jihad texts in an attempt to cause Spain's withdraw from Iraq. Hussein Oman (Defendant – London Bomb Trial) admitted to investigators that while having no direct al-Qaeda contacts, regularly visited their web sites, viewed their videos and read their propaganda (Awan, 2007). Both these case studies lend support for cyber tools in inspiring and sustaining home grown terrorists.

Case Study 2: Foiled Plot of 17 Canadian Muslims 2004

Surveillance of an online chat room and subsequent investigation led to the arrest of 17 Canadian Muslims (Awan, 2007). Contact through internet chat and a common anti-Western discourse seemed to be an important antecedent to the plot which then took on more conventional means including face-to-face contact (Awan, 2007). This case supports the internet as an important recruitment/contact point for disaffected youth to begin a path of radicalisation.

Case Study 3: Five Young British –Muslims Charged Under the 2000 UK terrorism Act 2004

Five young British-Muslims had not yet committed an act of terrorism, yet they were charged in relation to the large amount of material downloaded from extremist websites (Livingstone, 2007). Furthermore, surveillance of the groups internet chat logs indicated that they were well and truly on the path to radicalisation (Livingstone, 2007). Maher (2007, p. 144) cites the judge's decision on their path to radicalisation:

> You were intoxicated by the extremist nature of the material that each of you collected, shared and discussed – the songs, the images and language of violent jihad. So carried away by that material were you that each of you crossed the line.

What is interesting about this case is that the youths had no specific plans of a terrorist threat, and it was still unclear how they planned to carry out their jihad; all that was clear was that these youths had made a deliberate decision to take the path of jihad (Livingstone, 2007). This case clearly links cyber recruitment tools to radicalisation, but is (fortunately) unable to provide further details to links with actual terrorist acts.

Case Study 4: Adam Gadahn 1995 Onwards

Michael's (2009) fascinating case study of Adam Gadahn gives perhaps one of the best insights into the power of the aforementioned cyber tools to begin the disaffected on their path to radicalisation and ultimately jihad. Gadahn is a prime example of a 'White Moor' convert. Raised in the US, Gadahn eventually moved to the Middle East and rose to the highest ranks of al-Qaeda, becoming a vital part of their media strategy (Michael, 2009). Gadahn was not raised as a Muslim but as an agnostic with a non-practicing Jewish Father and Fundamentalist Christian grandparents. Interestingly, it was when a disaffected Gadahn moved in with his Christian grandparents that he had access to the internet and started down a new path. It was here that he was attracted to Islam, and finding their online discussions intriguing finally converted. Having been attracted to more radical online discussion sites, Gadahn continued his journey with fellow radicals at a local mosque. From here he began his epic rise to the al-Qaeda leadership ranks.

Evidence from these case studies combined with Jenkins (2010) study lends potent support for the effectiveness of cyber tools for recruitment as a starting point on the path to jihad for home grown terrorists and 'White Moors'. Studies also support the use of cyber tools to socialise and sustain radicalisation. Nevertheless, it is also important to point out that these cases also involved human contact at some later stage. The level of overall internet influence from recruitment to terrorist action still remains unclear. Nonetheless, we must ask how we can respond to the threat of cyber recruitment in attracting youths on the path to jihad terrorism.

WHERE TO FROM HERE?

Given the spate of terrorist attacks on Western soil using home grown terrorists, McNeal (2007) argues that one thing is certain; we can no longer do nothing. In tackling cyber recruitment, there are a number of serious challenges faced by governments and law enforcement. With terrorist hosted sites, it is easy for groups to simply change Internet Service Providers (ISP's) if they are shut down. This then becomes problematic to track down again (Awan, 2007). Compounding this challenge is the fact that some (US) companies provide domain names and host these sites while often ignoring the nature of the content (McNeal, 2007). As an alternative McNeal (2007) suggests bypassing the ISP's and shutting down the domain name (such as jihad.net) which has often been purchased from a US company. This step could only be taken once a site was identified as a terrorist affiliated site.

Even if it was possible to shut down terrorist hosted sites, groups could and already have shifted to legal sites such as Yahoo groups, Facebook and MySpace. Such discussion groups often waiver their rights from liability indicating that the material on the site does not reflect the views of administrators (Awan, 2007). Moreover, users can have multiple identities, fraudulent identities and shifting identities making them very hard to trace. This quandary was demonstrated in a case where an Australian Jewish woman was threatened by a Hezbollah terrorist on Facebook leaving police to admit the near impossible nature of tracking down the perpetrator (Kerbaj, 2008). A further problem is that administrators of the site are often slow to act. A prime illustration is the eventual banning of Abu Izzadeen's (jihadist) Facebook profile only after amassing a significant following (Mendez, 2008).

Frustrated with Facebook's (and others) lack of action on this issue, there has been the emerging phenomena of private 'activist' groups, most notably the Jewish Internet Defence Force (JIDF). This group became prominent after legally conducting a takeover(3) and then subsequently shutting down an Israeli hate group (Oboler, 2008). This move was orchestrated after 18 months of inaction by Facebook and a rapid growth in the size of the group.

Overall, responses can be categorised into two broad areas. First, there are attempts to challenge the socialisation process. A case in point is Livingstone's (2007, p. 151) proposed 'web-engagement strategy' which relies on countering terrorist truth claims in attempting to reduce the support and evidence to follow along a radicalised path. Second, there is the traditional approach of intelligence gathering and intervention. As a recommendation of his report on domestic terrorism, Jenkins (2010) supports the continual and judicial use of cyber monitoring and surveillance in order to disrupt and uncover terrorist recruitment and operations. Perhaps a combination of both strategies would be useful, nonetheless, what is clearly evident is that internet intelligence operations need to continue and develop in their counter terrorist sophistication.

CONCLUSION

This paper has examined the evolving threat of cyber recruitment targeting home grown terrorists. Cyber tools and strategies continue to develop and evolve in an attempt to better hone in and attract disaffected Western youth. What is particularly concerning about this trend is that evidence from case studies does provide tentative support to the dangers of these cyber tools at least in initiating, and in other cases sustaining, the path of jihad. Al-Qaeda and other jihad groups are increasingly making use of legal social networking sites that also allow users high levels of control and interactivity making targeting these sites more difficult. The latest al-Qaeda online magazine, *Inspire*, demonstrates just how adept they have become at continually trying to develop better cyber recruitment strategies by producing high quality, media savvy and seductive propaganda that specifically target potential 'White Moors'. These emerging threats need to be the subject of intelligent action responses that continue to monitor and intervene as early as possible before individuals travel too far down the path of radicalisation, hatred and terrorism.

NOTE

(1) There are other spelling variations for al-Qaeda such as al-Qa'ida and al-Qi'idah. Although al-Qaeda is the primary focus of this paper, the principles apply to related and affiliated Islamic jihad groups.

(2) Facebook has a membership of over 500 million users world-wide with 50% logging on in any one day (http://www.facebook.com/press/info.php?statistics). This equates to approximately 1 in every 14 of the world's population.

(3) This manoeuvre was conducted by emptying the group of its members. Once all the members were removed, the group could be shut down (Oboler, 2008).

REFERENCES

Anderson, A. (2003). Risk, Terrorism, and the Internet. *Knowledge, Technology & Policy, 16*(2), 24-33.

Awan, A. N. (2007). Virtual jihadist media. *European Journal of Cultural Studies, 10*(3), 389-408.

Brass, D. J., Galaskiewicz, J., Greve, H. R., & Tsai, W. (2004). Taking Stock of Networks and Organizations: A Multilevel Perspective. *The Academy of Management Journal, 47*(6), 795-817.

Conway, M. (2006). Terrorism and the Internet: New Media—New Threat? *Parliamentary Affairs, 59*(2), 283-298.

Cowen, T. (2006). Terrorism as Theater: Analysis and Policy Implications. *Public Choice, 128*(1/2), 233-244.

Hamill, J. (2010, 26 September). Web Watch: How the internet cultivated the new Bin Laden, *Herald Scotland.* Retrieved October 10, 2010, from http://www.heraldscotland.com/comment/guest-commentary/web-watch-how-the-internet-cultivated-the-new-bin-laden-1.1057480

Jenkins, B. M. (2010). Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States since September 11, 2001. Santa Monica: RAND Corporation.

Kerbaj, R. (2008, April 5). Jewish woman threatened through Facebook. *News.com.au,* (April 5, 2008). Retrieved October 10, 2010, from http://www.news.com.au/technology/would-be-friend-a-facebook-terrorist/story-e6frfrnr-1111115980877

Kohlmann, E. F. (2006). The Real Online Terrorist Threat. *Foreign Affairs, 85*(5), 115-124.

Kohlmann, E. F. (2008). Al-Qa`ida's "MySpace": Terrorist Recruitment on the Internet. CTC Sentinel, 1(2), 8-9.

Lachow, I., & Richardson, C. (2007). Terrorist Use of the Internet: The Real Story. *JFQ: Joint Force Quarterly*(45), 100-103.

Leiken, R. S. (2005). Europe's Angry Muslims. *Foreign Affairs, 84*(4), 120-135.

Lewis, J. A. (2005). The Internet and Terrorism. *Proceedings of the Annual Meeting (American Society of International Law), 99 (*March 30-April 2), American Society of International Law, 112-115.

Livingstone, D. (2007). Taking on the Radicals. *Index on Censorship, 36*(4), 148-153.

Maher, S. (2007). Road to Jihad. *Index on Censorship, 36*(4), 144-147.

Matusitz, J. (2008). Similarities between terrorist networks in antiquity and present-day cyberterrorist networks. *Trends in Organized Crime, 11*(2), 183-199.

McNeal, G. S. (2007). Cyber Embargo: Countering the Internet Jihad. (German). [Conference Paper]. *Case Western Reserve University School of Law, 39*(3), 789-826.

Mendez, D. (2008, February 15). Facebook and Terrorism: a love hate relationship, *Tech.Blorge [Technology News]*. Retrieved October 10, 2010, from http://tech.blorge.com/Structure:%20/2008/02/15/facebook-and-terrorism-a-love-hate-relationship-2/

Michael, G. (2009). Adam Gadahn and Al-Qaeda's Internet Strategy. *Middle East Policy, 16*(3), 135-152.

Murphy, C. (2007). The Internet: Midwife of Global Radicalism?: High-Tech Savvy Mushrooms from First Primitive Web Site. *Science & Spirit, 18*(1), 36-39.

O'Rourke, S. (2007). *Virtual Radicalisation: Challenges for Police.* Paper presented at the Proceedings of the 8th Australian Information Warfare and Security Conference, Perth.

Oboler, A. (2008). The rise and fall of a Facebook hate group. *First Monday, 13*(11).

Shaidle, K. (2009, January 7). Facebook Jihad *Right Side News*. Retrieved October 10, 2010, from http://www.rightsidenews.com/200901073240/world/terrorism/facebook-jihad.html

Thomas, G. (2010, August 26). Radical Islamists Try to Exploit Islamophobia, *Voice of America*. Retrieved October 10, 2010, from http://www.voanews.com/english/news/Radical-Islamists-Try-to-Exploit-Islamophobia-101592048.html

Weimann, G. (2008). The Psychology of Mass-Mediated Terrorism. *American Behavioral Scientist, 52*(1), 69-86.