12-3-2007

Virtual Radicalisation: Challenges for Police

Simon O'Rourke
Edith Cowan University

DOI: 10.4225/75/57a83c57befab
8th Australian Information Warfare and Security Conference, Edith Cowan University, perth Western Australia, 3rd-4th December, 2007

Virtual Radicalisation: Challenges for Police

Simon O'Rourke
School of Computer and Information Science
Edith Cowan University
sorourke@student.edc.edu.au

Abstract

Recent advances in communications technology are providing a medium for individuals or groups to subscribe to extremist worldviews and form networks, access training and obtain information, whilst remaining virtually undetected in the online world. Whilst the Internet is facilitating global virtual communities like Second Life, MySpace and Facebook it is also providing an anonymous meeting place for disenfranchised individuals to gather, share ideas, post and exchange information regarding their particular ideology. This virtual community provides a sense of belonging to a global cause in which the actions of an individual can be aligned to, and seen to contribute towards something more significant than their own lives. Membership of this virtual community can facilitate the indoctrination of individuals, thereby negating psychological barriers that would normally inhibit particular types of behaviour. Terrorist groups operate as amorphous, fluid networks providing them significant advantages over rigidly structured state and nation based law enforcement agencies. In addition terrorist groups are exploiting the combination of rapidly evolving technology and incommodious legislation to prevent detection.

Keywords

Terrorism, Internet, Training, Radicalisation, Data Mining, Social Networking, NORA, IBM, Police, Intelligence, Las Vegas, Internet Archive, Subject & Pattern Based, Fourth Generation Warfare, Web 2.0.

INTRODUCTION

Recent advances in information and communications technology (ICT) are providing a medium for individuals or groups who subscribe to extremist worldviews to form networks, access training and obtain information, whilst remaining virtually undetected in the online world. The Internet is facilitating global virtual communities like the social networking dot com addresses, Second Life, MySpace and Facebook. However, it is also providing an anonymous meeting place for disenfranchised individuals to gather, share ideas, post and exchange information regarding their particular ideology. The Nielsen Net Ratings 2006 highlights the exponential growth of these social networking sites over a 12 month period. For example MySpace grew by 367% over the survey period (Nielsen, 2007). Such growth is being readily exploited by terrorist groups as they seek to increase recruitment and support, "Without a doubt, the Internet is the single most important venue for radicalisation of Islamic youth" (Custer cited in Pelley, 2007, p.1).

The destruction of terrorist training camps in Afghanistan by US led forces has necessitated the transition from physical training locations, to online training environments. Terrorist groups are now emerging, "as robust online networks, regaining the ability to communicate, recruit, indoctrinate, train and plan attacks" (Katz & Devon, 2007, p.3) . Participation in the resultant extremist sites provides for those involved, a sense of belonging to a global cause where the actions of an individual can be aligned to, and be seen to contribute towards, something which they see as more significant than their own lives. This transition to, "self taught terrorism suggests that personal initiative and decentralisation may soon provide additional elements of chaos to the already difficult task of tracking the web of terror groups and individuals", (Weimann cited in Forest, 2006a, p.110).

Therefore new intelligence-led anticipatory capabilities will need to be developed in order for the police to successfully identify those individuals or groups in cyberspace, who warrant further investigation and the subsequent allocation of finite resources. The operational structures and communications methodologies adopted by contemporary terrorists, "means that in the future a greater number of terrorists and terrorist plots may escape the notice of intelligence services altogether" (Hamm, 2007, p.209). This paper will discuss the significant challenges that these online communities pose for police and intelligence agencies, in their efforts to identify those individuals or groups undergoing virtual radicalisation and training. This identification needs to occur before the transition from virtual ideology to physical acts of terrorism. As Mitchell Waldrop (2003, p.44) states, "it's time to take intelligence gathering and interpretation into the network age".

THE IDEOLOGICAL WEB

The Internet is proving to be crucial to terrorist campaigns because it facilitates the promotion of a particular ideology and allows groups to present events from their perspective. This ability to provide a particular perspective on events is crucial to their efforts because, "publicity is the oxygen of terrorism" (Richardson cited in Walker, 2005, p.3). Membership of a virtual community based around extremist views can allow indoctrination of individuals potentially bypassing psychological barriers that would normally inhibit particular types of behaviour. Terrorist groups operate as amorphous, fluid networks providing them significant advantages over rigidly structured state and nation based law enforcement agencies. "We are currently losing the war on terrorism due to Web 2.0" and the reasons cited for this are the capabilities for "these folks to communicate, share tradecraft, recruit and synchronize at a velocity and resiliency that is unprecedented" (Jonas, 2007). In addition terrorist groups are exploiting the combination of rapidly evolving technology and incommodious legislation to prevent detection. Kirby (2007, p.415) acknowledges that whilst the occurrence of self radicalisation had its roots in social issues it, "is infused with Islamic ideology and rhetoric". Its promotion via the Internet however, makes Western Countries who do not limit access vulnerable. "It's a different type of warfare. It's a battle of perceptions. And Al Qaeda understands it. And America needs to understand it" (Custer cited in Pelley, 2007, p.3). The Internet allows terrorist groups like Al Qaeda, "to guide a worldwide movement without meeting their followers or even knowing who they are" (Richardson cited in Walker, 2005, p.2).

Weimann (cited in Forest, 2006a, p.111) identifies the widespread use of the Internet by various extremist groups to market their causes, keep in touch with their support base and to, "teach and train" their operatives. It is this use of the Internet that poses the greatest challenge for police in identifying 'persons of interest' from the billions of packets of data travelling across the Web. This view is supported by Ronczkowski (2007, p.226) who identifies the sheer volume of electronic communications used by terrorists as disturbing. Terrorists have identified the inherent risks and limitations imposed by traditional structures and not unlike recent changes to corporate business entities they are now evolving towards, "transnational internetted groups" (Arquilla et al. cited in Forest, 2006a, p.117). These groups provide greater resilience in the event of a successful police operation. Their loose, widely dispersed structure ensures that not all operatives and resources are vulnerable to interception to a single law enforcement operation. In addition this model provides increased flexibility and the devolution of authority resulting in decisions being made and actions taken at a local level, in support of a strategic ideological cause like the return of the Islamic Caliphate or the removal of Western influence from a particular geographical region. Weimann (2006, p.116) discusses Al Qaeda's evolving structure following the US led operations in Afghanistan as comprising of a, "rapidly changing multicellular transnational structure spanning the entire globe". This has created a new cadre of terrorists whom Kirby (2007, p.416) classifies as self starters who have attained a level of operational autonomy unmatched by any comparable terrorist or government entity. It is this autonomy, which allows individuals and groups to identify, select and carry out attacks against targets without any further authority or approval from groups with whom they see themselves as being aligned.

Kirby (2007, p.416) details the crucial role that technology has played, "in the emergence of this new brand of terrorism". Unlike previous candidates for Jihad, individuals can now nominate themselves and become involved, whilst still living in their country of residence or birth. There is no longer a compulsion to travel to places like Afghanistan or Iraq unless that is what the individual desires in order to become a Mujahid (holy warrior). Previous logistical and in some cases financial impediments to undertaking Jihad have being largely negated by advances in technology thereby making such activity available to a much wider group that anytime previously. This stance is supported by Weimann (2006, p.111) who cites the online training camp Al Battar as an example of what is provided in cyberspace by Al Qaeda for those unable to travel yet who still wish to undertake training. This provides an online learning environment whereby individuals can attain the requisite skill set necessary to carry out their own attacks

RECRUITMENT, RADICALISATION & TRAINING

Terrorist entities are amplifying their capabilities via the Internet in order to present themselves as a greater tactical threat than they can physically achieve. "It's a war of perceptions. They understand the power of the Internet. They don't have to win in the tactical battlefield. They never will. No platoon has ever been defeated in Afghanistan or Iraq. But, it doesn't matter. It's irrelevant" (Custer cited in Pelley, 2007, p.1). The Web is being used to facilitate the active recruitment of individuals who have grown up in Western societies and are comfortable meeting new people and discussing issues in Cyberspace. Weimann (2006, p.118) details how the full suite of multimedia capabilities facilitated by the Internet are used to, "recruit and mobilise supporters to play a more active role in terrorist activities or causes". A variety of terrorist groups including radical Islamists are marketing themselves in such a manner as to generate support for their causes and identify and radicalise those they identify as potential converts to their interpretation of Islam. This approach is particularly effective given what is now known about the recruitment of potential terrorists. Sageman (2004, p.108) conducted extensive research into terrorist networks and recruitment methods and discovered an absence of "brainwashing" or "top-down recruitment". Instead candidates were self-recruiting and searching for ways to join either via the Internet or by introductions from members of their current social network who may already be members. The only recent deviation from this recruitment methodology was uncovered by the SITE Institute and details the 2003 drive by Al Qaeda, "to recruit fighters to travel to Iraq and attack US and coalition forces there" (Weimann cited in Forest, 2006b, p.61).

The Internet is being used to articulate a particular view often contrasting with mainstream media and it allows terrorists to generate "publicity and propaganda" (Walker, 2005, p.3) for their cause as well as justifying violent acts. When interviewed by the 60 Minutes program the head of US Intelligence at Central Command General John Custer explained that on some of these sites terrorists could, "download scripted talking points that validate you have religious justification for mass murder" (Custer cited in Pelley, 2007, p.1).

Gruen (cited in Forest, 2006b, p.12) identifies the need for Islamist groups to recruit and radicalise their "target audience" whilst minimising any detectable contact. This would allow them to avoid physical police surveillance operations of persons or places of interest. Instead they reach their targets via the Internet where they can broadcast their ideology anonymously from International servers. The websites used to attract potential candidates need to be visually appealing with excellent multimedia and in the native language of the target group. Terrorist entities also have to ensure that these outer sites do not promote extremism to a degree that they warrant additional attention from police and intelligence agencies. However these groups do monitor those who browse their sites and retain information about them including IP and Email addresses if acquired. Should these individuals then be of interest to such groups by virtue of their geographical location or other criteria then they are often contacted (Weimann cited in Forest, 2006b, p.60).

Once contact is established then the candidate can then be drawn further into the extremist world and be granted access to far more radical sites hidden from public view and inconspicuous enough not to warrant further investigation by police if located by commercial search engines. Katz and Devon (2007) support this view listing password protected sites including forums and message boards as the most utilised communications medium. These candidates are likely to be individuals susceptible to indoctrination who are dissatisfied with their current status and position in life regardless of any outward veneer of normality or success. Terrorists then seek to segregate these individuals by supplementing their social structure with a new network of like minded individuals in Cyberspace (Gruen cited in Forest, 2006b, p.14). This ensures that the indoctrination process can proceed unimpeded by contrasting views or arguments from family and former friends and colleagues. Individuals are made to feel highly valued and special by their new friends. This virtual world provides camaraderie, "and enables individuals to see themselves as part of a larger, connected community, despite the vast geographic distances and cultural differences that may exist between them" (Katz & Devon, 2007, p.1). They are often assigned a mentor who keeps in personal contact and advises and guides them on their journey. Whilst this entire process can occur in Cyberspace, Weimann (cited in Forest, 2006b, p.60) is of the opinion that the Internet may only be used to, "profile and select potential candidates for recruitment". This is due to the potential by police and intelligence agencies to introduce cyber operatives to the network in a methodology not dissimilar to that employed against Internet paedophiles.

The potential exists for an individual or group to actively seek out extremist sites, become radicalised, undergo training and prepare for an attack whilst remaining undetected by conventional policing techniques. Following the July 7 attacks in London the British police and intelligence agencies, "faced profound policy challenges" (Kirby, 2007, p.426) even though their structures were well attuned to terrorism from their previous IRA experience. This is due to the paradigm shift required to deal with the new threat posed by, "the emergence of radical autonomous cliques empowered by the Internet" (Kirby, 2007, p.426).

Therefore, new methodologies need to be introduced and where necessary legislation amended to allow police to keep pace with the terrorist groups who are fast surpassing them in terms of expertise and resources (Ronczkowski, 2007, p.227). This will also require a change in mindset for police agencies as they come to terms with the realisation that individuals or very small groups may radicalise in cyberspace and then fund their own attacks all without any contact or discernable instruction from an existing terrorist entity. Accordingly these new terrorists may be home grown and have had no previous dealings with police. This presents the possibility that there are currently individuals in Australia who are in the process of evolving from cyber radicals to active terrorists. Therefore, "new paradigms are needed to understand the process by which individuals are driven to embrace terrorism and execute attacks" (Kirby, 2007, p.423).

Terrorist groups are now providing online training that would rival the offerings of most established universities. The training can encompass a wide variety of topics all designed to slowly indoctrinate and alter the worldview of the student whilst simultaneously equipping them with the skill set necessary to carry out attacks. In an effort to limit the possibility of interception members of terrorist groups may place important messages in draft form in email folders in cybercafes, where they can be accessed by other members but not transmitted into cyberspace (Richardson cited in Walker, 2005, p.3). This practice is not dissimilar to the cold war technique of dead letter drops used by intelligence operatives.

In addition to the techniques learnt online Hamm (2007, p.208) has identified the variety of skills that individuals from a variety of socio-economic backgrounds contribute when forming terrorist cells. These range from academic expertise in fields as diverse as chemistry and computer security to knowledge of police methodologies and criminal contacts gained from the streets. This combination is being well utilised by the terrorists who understand the modern asymmetric battlefield better than those charged with stopping them. Terrorist groups will actively target their enemies on a variety of levels, blurring the traditional distinctions between the battlefield and civilian environments resulting in a new form of conflict, which can be classed as Fourth Generation Warfare (4GW), (Lind et al. cited in McCue, 2007, p.216).

INHERENT CHALLENGES

As with all material on the Internet once a concept for a terrorist attack is committed to digital format it can be utilised by anyone who so choses even if the individual who proposed it is captured or killed (Katz & Devon, 2007). Whilst the Internet can be used to challenge information released by governments via the mainstream media it is now the media themselves who are being seen as legitimate targets in locations like Iraq. Journalists are no longer viewed as impartial in their role as the fourth estate. “Civilians are targets. The press has no credentials here. Kidnap them. Put a gun to their head and put ‘em on the evening news” (Custer cited in Pelley, 2007, p.2). Whilst the evolving terrorist threat of self-starters comes from within a nations own borders comprising members lacking in operational experience from theatres like Iraq and Afghanistan they are no less of a threat (Hamm, 2007, p.208). Whilst most criminal actions are motivated by greed, the crime of terrorism is motivated by an ideology. This presents inherent challenges to investigators, as the normal motivations to cooperate may not be applicable. Established practice allows for charged suspects to provide information, which may assist police investigations in return for consideration by a Judge when determining any subsequent term of imprisonment. Terrorists are highly unlikely to provide such information unless their beliefs can be successfully challenged and altered.

Ronczkowski (2007, p.227) discusses the technical capabilities of many terrorist groups and their ability to learn from previous encounters with police and law enforcement agencies. Full disclosure legislation in Australia can potentially provide these groups with an insight into the methodologies used by police to intercept and track electronic communications, thereby ensuring that terrorist groups learn how to better secure and hide future communications. The vastness of the Internet and the volume of data transmitted would challenge even the resources of specialist interception agencies like the US National Security Agency (NSA) and the Australian Defence Signals Directorate (DSD). There is an identified need to enhance the ability of policing agencies to capture and organise the vast amount of information so it can be subsequently analysed and turned into actionable intelligence (McCue, 2007, p.xix). The resources and expertise required to identify and intercept suspect communications are difficult to sustain in a policing environment where funding is predominately linked to measurable outcomes. Post 9/11 the US commenced evaluating data mining as a means to uncover terrorist plots prior to them being executed (Jonas & Harper, 2006). Whilst it was found to be an attractive option, it was identified that legislation could prevent it from being utilised to its full potential. In the US this situation has in part being rectified by the introduction of Section 215 of The US Patriot Act, which allows broad requests for information holdings from the private sector without specifying any individual, or group as was previously required. This facilitates the cross matching of large data sets to identify individuals, patterns or themes of concern.

This is a causing concern amongst civil liberties groups due to the volume of data that is required and the number of people with no active involvement in criminal behaviour whose private information ends up on government databases as a result. However, this would take the efforts of police and intelligence agencies into the digital age as they try to identify themes and relationships using various computer based applications in an effort to successfully undertake large scale data mining (Markoff & Shane, 2006). These types of data analysis operations are resource intensive. They can also be limited due to the lack of an accepted common protocol that would enable the rapid transfer of data between servers, as well as searches of propriety systems and information held by a variety of public and private organizations (Mitchell Waldrop, 2003, p.45). It is not just the flow of data between servers that is crucial to this effort there needs to be a, “transparent, fluid interface between analytical and operational personnel” (McCue, 2007, p.xix). Analysts need to understand and where possible pre-empt the needs of investigators. Jonas identifies the crucial aim of data analysis to produce actionable intelligence, not just more information or data. He defines this as, “information that puts the analyst in a position to act appropriately in a given context” (Jonas & Harper, 2006, p.5).

IBM recently acquired a company in Nevada called Systems Research and Development. The former head of the company Jeff Jonas, a leading software developer, is now a distinguished engineer with IBM. His original software called Nonobvious Relationship Awareness (NORA) was designed to provide a solution to the identity matching problems being faced by the casinos in Las Vegas. It has now being further enhanced and is marketed by IBM as Identity Resolution and Relationship Resolution. Jonas has generated interest with his view that the potential for data mining as a tool to identify and predict terrorist activity is very limited. Jonas and Harper (2006, p.2) are of the opinion that data mining would be “problematic and generally counterproductive”. Their rationale is that unlike the private sector or established crime types, terrorism has very few events by which to develop a framework to benchmark analysis against. This is in stark contrast to other crimes like fraud or the commercial applications of data mining, where private entities use data mining to profile their customers and identify market trends and shifting consumer demand and spending patterns. What Jonas proposes in its place is a system whereby data pertaining to key individuals is able to “located, accessed and aggregated” (Jonas & Harper, 2006, p.4) requiring the shared access by agencies of various databases both public and private.

Whilst software continues to be developed and refined the legal and moral arguments regarding data mining by police and intelligence agencies will continue. Jonas and IBM are currently developing new technology, which will allow all the analysis to be done whilst the data sets are still in encrypted form thereby ensuring that privacy is retained unless a particular piece of data is identified as of concern and warrants further investigation (Olsen, 2006). The two approaches to data mining relevant to counter terrorism are subject and pattern based (Jonas & Harper, 2006). Once a person of interest is identified then data including electronic communications, bookings and transactions can be scanned to identify linkages with places, individuals or groups. These individuals can then be further investigated allowing the analyst to build up a picture of the network or group and attempt to discern their activities and possible objectives. As previously discussed for such an endeavour to be successful the analyst requires the ability to interrogate and retrieve data from numerous databases. In order to use pattern based data mining successfully the statistical framework needs to be able to recognise critical yet innocuous pieces of information. There are however, opposing views to Jonas regarding the potential of data mining to successfully provide police and intelligence agencies with another capability to add to their investigative portfolio. Some programs like ‘Total Information Awareness’ undertaken by the US Defence Advanced Research Projects Agency (DARPA) are attempting to provide a digital solution to the problem. Such capability is critical given the data that is being transmitted and the difficulties in providing real time monitoring of sites of interest and those accessing them. It is estimated that over 80% of the data held on individuals is held in the private sector, and much of this is available on a commercial basis. Databases such as Choicepoint, Lexusnexus and Axion provide search capacity and electronic profiles beyond that held by police databases. Accordingly, terrorist groups operating in the UK actively recruited members with computer expertise to assist with camouflaging their electronic traffic and availed themselves of services provided by a variety of Internet cafes and pay as you go ISP’s (O'Neill & McGrory, 2006, p.115).

Policing practices will need to evolve from reliance upon informants and traditional reactive intelligence feeds, to a proactive approach in cyberspace. Recently the Australian Federal Communications Minister Helen Coonan tabled a bill in Parliament proposing to give the Commissioner of the Australian Federal Police the power to order Internet Service Providers to block access to terrorism and cyber crime web sites (Dearne, 2007). Proposing restricting access to extremist sites pose technical challenges and are indicative of the frustrations faced by lawmakers regarding some of the ideology that is being actively promoted via the Internet. Restricting access to pornographic sites has proved a difficult challenge, given the recent media coverage regarding the cracking of the Federal Governments new Internet Filter by a teenager still in high school. Other comments placing the responsibility directly at the ISP level are prone to difficulty with regards to enforcement. Many of the service providers that host extremist web sites have no knowledge of their activities and remove them once advised. However, many of these sites are located offshore in countries that actively support such extremist views and their promulgation.

Other difficulties exist as once these sites are removed or taken down they can still be accessed via applications like, ‘The Internet Archive: Way Back Machine’. This means that whilst they aren’t being updated with the latest propaganda, they can still be accessed by anyone with even limited technical knowledge. Rather than drive such sites underground another approach may involve the use of electronic surveillance to monitor those who access their content and subsequently interact with them. This would allow police to build up a profile of persons of interest, their online activities and identify the electronic address of those they come in contact with. It would also provide insight into the more extremist sites including their hosts, users and content.

CONCLUSION

As technology progresses both terrorists and those charged with preventing them from committing atrocities will have to remain abreast of innovative developments. As identified by Hoffman (2006, p.252) there is a need for terrorists to continually take action, and in order to effectively do so they need to be able to evade those measures put in place by the police and intelligence agencies. Terrorist groups and innovative individuals are continually identifying and exploiting potential weakness in order to achieve their objective. Policing agencies need to ensure that future investments in equipment and personnel for counter terrorism are not restricted to a tactical or response capability. Highly skilled analysts and the supporting IT framework should receive equal priority for funding in order to prevent the loss of life and reduced sense of security in the event of an attack. "While authorities play catch up on the Internet, the online terrorist network continues to expand, recruiting others to jihad and growing stronger each day" (Katz & Devon, 2007, p.2). Lessons learnt from cyber paedophile investigations and the methodologies developed could be adapted to meet the requirements of counter terrorist officers. Information sharing and tasking protocols may need to be enhanced between State and Territory police departments and Federal Intelligence agencies. The combination of Federal resources with information provided to the police by the community could prove highly successful in preventing future terrorist attacks.

REFERENCES

Dearne, K. (2007). Coonan seeks to censor the Web. *The Australian IT*.

Forest, J. (2006a). *Teaching Terror: Strategic and Tactical Learning in the Terrorist World*. Lanham: Rowan & Littlefield.

Forest, J. (Ed.). (2006b). *The Making of a Terrorist: Recruitment, Training and Root Causes* (Vol. I). Westport: Praeger Security International.

Hamm, M. (2007). *Terrorism As Crime: From Oklohoma City to Al-Qaeda and Beyond*. New York: New York University Press.

Hoffman, B. (2006). *Inside Terrorism: Revised and expanded edition*. New York: Columbia University Press.

Jonas, J. (2007). Web 2.0 - Al Qaeda's Most Effictive Force Multiplier. Retrieved 14 October, 2007, from http://jeffjonas.typepad.com/jeff_jonas/2007/05web_20_al_qaeda.html

Jonas, J., & Harper, J. (2006). Effective Counterterrorism and the Limited Role of Predictive Data Mining. No.584. Retrieved 10 October 2007, 2007, from http://www.cato.org/pub_display.php?pub_id=6784

Katz, R., & Devon, J. (2007). Web Of Terror [Electronic Version]. *Forbes.com*. Retrieved 15 October 2007 from http://members.forbes.com/forbes/2007/0507/184a_print.html.

Kirby, A. (2007). The London Bombers as "Self-Starters": A Case Study in Indigenous Redicalization and the Emergence of Autonomous Cliques. *Studies in Conflict and Terrorism, 30*(5), 415-428.

Markoff, J., & Shane, S. (2006, 25 February 2006). Agencies Look for More Ways to Mine Data. *The New York Times*.

McCue, C. (2007). *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. Burlington: Butterworth-Heinemann.

Mitchell Waldrop, M. (2003). Can Sense-Making Keep Us Safe [Electronic Version]. *Technology Review*, 43-48. Retrieved 12 October 2007 from http://www.technologyreview.com.

Nielsen. (2007). NetRatings: A global leader in Internet media and market research. Retrieved 10 October, 2007, from http://www.nielsen-netratings.com

O'Neill, S., & McGrory, D. (2006). *The Suicide Factory: Abu Hamza and the Finsbury Park Mosque*. London: Harper Collins.

Olsen, F. (2006). FlipSide: A few minutes with Jeff Jonas [Electronic Version]. *Federal Computer Weekly*. Retrieved 13 October 2007 from http://www.fcw.com/print/12-2/news/92036-1.html.

Pelley, S. (2007). Terrorists Take Recruitment Efforts Online. Retrieved 30 September 2007, 2007, from Http://www.cbsnews.com/stories/2007/03/02/60minutes/printable2531546.shtml

Ronczkowski, M. R. (2007). *Terrorism and Organised Hate Crime: Intelligence Gathering, Analysis, and Investigations* (2nd ed.). Boca Raton: CRC Press, Taylor & Francis Group.

Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press.

Walker, R. (2005). Terror online, and how to countract it. *Harvard University Gazette* Retrieved 14 October, 2007, from http://www.hno.harvard.edu/gazette/2005/03.03/01-cyberterror.html

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

COPYRIGHT