

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

### *The Internet and terrorism: pathways towards terrorism & counter-terrorism*

#### **Introduction**

The speed at which terrorist and extremist groups have embraced the possibilities offered by the Internet has been reflected in the sheer number of websites espousing support for terrorists, white supremacists and radical Islamic militants, among many others. Levin (2002) partially explains the growth of internet use by extremists and terrorists with reference to its economical and 'far reaching' nature. The speed of Internet acquisition may also be attributed to its inherent nature; it is easy to access with a chaotic structure that facilitates anonymity, and an international character that affords an easy and effective arena for action (Tsafti & Weimann 2002). While violence remains essential to the terrorist movement for the psychological impact of terrorism, the Internet provides a safe, easy and cheap means of communicating, disseminating propaganda, gathering intelligence, promoting support, demonising the enemy and raising funds.

Historically the Internet has been associated with military, scientific and academic institutions and communities, providing a particular historical and cultural context for online communication and membership. An important implication of this is that the internet can be used to explore "*political action and affiliation online*" (Kendall 1999, p. 63). 'Terrorist use of the Internet' provides a new solution to the old problem of communication. Where once terrorist movements were reliant on 'traditional' forms of media to bring their 'cause' to the public, the Internet now facilitates a broad spectrum of communication possibilities, ranging from websites to virtual communities. While websites serve the important function of providing a link between movement and supporter, it is the virtual community that allows for the construction and maintenance of political and ideological discourses in support of that movement, providing the 'public space' supporters crave (Arendt 1990). Virtual communities can be likened to 'communities of practice' (Lave 1988; Wenger 1998), informal social learning environments which facilitate increasing commitment of group members to movements, including those movements that justify the use of terrorism and political violence to achieve their goals (Hundeide 2003). Virtual communities of practice are virtual spaces used effectively by members who interact in a meaningful community driven way. Regular community members pride themselves on their commitment to the community and the activities they pursue, for example communicating with others, disseminating their truth, creating a place where others can come to learn, offering validation to others on their ideological beliefs. Discourses created within these communities provide validation, justifying and legitimising the use of terrorism. These discourses are central to the ways that the Internet can contribute to the facilitation of involvement either online (within the virtual community) or offline (in a potentially more active capacity). Involvement within a virtual community and potential involvement in offline activities thus presents itself as a potential pathway toward individual radicalisation. For the purpose of this chapter, 'radicalisation' is defined as an end stage on a continuum that spans from lower level support to the involvement or willingness to be directly involved in violent terrorist activities.

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

A crucial issue here is whether the Internet can be considered a catalyst for action by terrorists and their supporters. To try to understand this issue it is useful to begin by asking some key questions relevant to this; why do terrorist movements and their supporters use the Internet, i.e. what functions does it serve and what pathways toward involvement are facilitated?

### ***Why do terrorist movements and their supporters use the Internet?***

Much has been written on terrorist use the Internet in relation to the function of websites (see for example Whine 1998, 1999, 2000; Tsafiti & Weimann 2002; Conway 2003 & Weimann 2006a&b). It is widely agreed that terrorist use of the Internet incorporates, but is not limited to, resource acquisition, intelligence gathering, propaganda (including auto-propaganda), support and recruitment. While the physical membership of core activists of most terrorist movements is kept to a minimum both because of the psychological premium associated with restricted membership and for security reasons, there is no practical limit to the numbers of supporters sought by any terrorist movement. The Internet can be used as a catalyst for fostering support and recruitment, the different levels of involvement that websites and online communities make available to the supporter facilitate involvement at various levels; a supporter can send a donation, buy merchandise, support prisoners, chat online, become more active and distribute propaganda/fliers, or attend marches/demonstrations. Both online research and a consideration of relevant psychological literature and theory can further inform us about this process of potential radicalisation.

### **Resource Acquisition**

Many websites that support a terrorist movement, link directly to online shopping facilities. Rather than serving as an income-generator that is of any real significance to the movement, in reality the symbolic nature of the products represent the true value of the commodities being offered. For example, via a right wing extremist online shop, browsers can purchase any of the following: music CDs (including entire collections of the music of famous Right Wing extremist music groups, such as Hammerskins), DVDs, flags, badges, pins, baseball caps, calendars, key rings, shirts, posters, and an extensive range of movement literature, including Hitler's 'Mein Kampf', MacDonald's 'Turner Diaries' and Duke's 'My Awakening' (see for example websites <http://www.resistance.com/catalog> & <http://www.aryanwear.com/>). The selling of such materials via websites is not limited to Right Wing Extremist sites, although these may be some of the most prolific.

Many websites also provide visitors with an option to directly donate funds, for example on opening the [www.Kahane.org](http://www.Kahane.org) website,<sup>i</sup> a pop up invites you to donate funds directly to the movement. Others provide addresses where donations can be sent, for example National Alliance at [www.natvan.com](http://www.natvan.com). One of the more interesting examples of resource acquisition can be found on the Ulster Loyalist Information Services website,<sup>ii</sup> the virtual home of the Loyalist Volunteer Force an extreme Loyalist faction based in Protestant areas of Belfast. This movement quickly realised that not all its supporters "*feel comfortable in giving monetary donations*", but encourages donations of unwanted items:

*"Want to help out LVPW, but don't feel comfortable (sic) with making monetary donations? You can also help by donating various items. Some of these items will be*

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

*used for obvious uses, others will be packaged as Christmas gifts for less fortunate families of imprisoned volunteers or widows. Please review the list below, if you have any of the items and would like to donate them, please contact us at Projects.*

- **Bullet Proof Vests** - Any size, new or used. These can be found used at reasonable prices on eBay
- **Computers** (Pentium II or newer), software of use, computer games
- Items that would make nice **Christmas gifts** for children of all ages.
- You may also make a monetary donation, via **PayPal** by following the link below.”

The purchase of items, often culturally significant to the movement, is important to a supporter providing a link to the organisation and its history, functioning not only as a means of donating some small amount to the organisation, but also serving to forge a tangible link between the supporter and the organisation. Donating money or goods to a movement may be seen as indicative of a belief that the goals of the movement are legitimate and that their means of achieving these goals, even through the use of violence and terrorism, are acceptable. This may be a first step on the pathway toward involvement. As one Right Wing extremist within the virtual community of Stormfront ([www.stormfront.com](http://www.stormfront.com)) comments:

*“I was on the internet one night looking for a song on some file sharing program. I came across one called "White Power" by a band called Skrewdriver. I hated negroes, spics, gays, etc. and decided to download it. The second Ian Stuart shouted out "White Power 1,2,3,4" I was HOOKED.”*

### **Intelligence Gathering**

The Internet is also an unsurpassable tool for information gathering. This does not automatically bring us into the realm of how the Internet can be used to gather information, using tools such as Google Earth or The Anarchists Cookbook, to cause destruction to critical infrastructures (although this is of course possible), but can also be considered from another perspective. The Internet is by now well known as being a fast and efficient way to gather information on people, places and groups all over the world. As such, terrorist organisations can avail of the opportunity to keep well informed on up to minute news on how they are perceived by the mass media, as well as providing the group with information on their perceived enemies and allies. The Internet may also be a way for ideologically similar groups to forge alliances across international borders which are inconsequential online. ‘Webrings’ are an important feature that supports this, facilitating the networking of websites that are used to express similar views, perspectives and ideologies. They allow the user to work more efficiently through related sites and can serve to mark implicit affiliations between groups. Evidence for this can be found through an examination of the links between websites, for example current online links between the Ulster Volunteer Force and the Neo-Nazi group Combat 18, and online links between Aryan Unity and the British People’s Party. Indeed, cyber-space is one place that serves as an ideal ground for contagion effects. Terrorist movements use websites to catalogue their successful operations. This is useful to boost member morale and can also serve as an effective tool to advertise successful violent campaigns. The Hizbollah websites for example, ([www.hizbollah.org](http://www.hizbollah.org) & [www.almashriq.hiof.no/lebanon](http://www.almashriq.hiof.no/lebanon)) provide coverage of successful para-military operations as feature items.

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

### **Propaganda**

*“Propaganda is an art requiring special talent. It is not mechanical, scientific work. Influencing attitudes requires experience, area knowledge, and instinctive judgement of what is the best argument for the audience”.* Bogart (1976, p. 195-196)

A visit to any website proclaiming support for the actions of a terrorist movement will at once reveal its most immediate purpose, propaganda. Terrorist website homepages demonstrates that the Internet can serve as a valuable tool to disseminate information about the objectives, strategies, tactics and other features of the group to influence the publics' perception of them, their ideology and goals. The instrumental nature of terrorist violence serves to perform a variety of functions that go some way towards explaining the attractiveness of the strategy of terrorism for isolated, marginalised political groups, and an important primary function is that of communication. For most sub-state terror groups, their tactics are predicated on attempting to overthrow or effectively destabilise a political influence. Winning hearts and minds is central to this, and terrorists must justify and legitimate their activity with facts. Alerting the world to the grievances of a particular movement, as well as documenting the history of injustices suffered (real or imagined) by a particular minority (depending on the kind of terror group) is of primary importance and is central to any attempt to gain support. The message of the terrorist organisation must be credible and believed by the user if it is ever to progress to some sort of support that may be measurable and tangible.

A pertinent example of this comes from the Hizbullah website ([www.almasqriq.hiof.no/lebanon](http://www.almasqriq.hiof.no/lebanon)) which includes this detailed statement outlining the ideology of the group and dealing with the perception of Hizbullah in the west as a terrorist organisation. It relates the progression of the movement from 'turbulent' times of violence to its re-emergence as a 'pivotal force' in the Middle Eastern political arena. While recognising that the violent activities against Israel have been perceived as terrorism and thus condemned, it is defended as a 'natural human reaction' to the violence perpetrated by the Israeli occupying forces. This statement highlights the importance of justifications bound in rhetoric of righteousness and rationality. Such justifications facilitate the call for violence and promote the legitimacy of the movement and the goals they seek to achieve.

*“The prevalent perception of Hizbullah in the "west" is of a militant, armed terrorist organization bent on abduction and murder. While the initial years of its emergence as a political movement in Lebanon were turbulent and controvertial (sic), The Party of God has matured to become an important and pivotal force in Middle East politics in general and Lebanese society in particular. Hizbullah does not believe it is right for some people in the world to view the Zionist Jewish occupation as accepted violence and terrorism, while they condemn the counter-violence, which is a natural human reaction to the Zionist violence and terrorism.”*

On a related note, propaganda on websites can be used to actively promote violent activity against specific targets. For example, a website affiliated with The Animal Liberation Front, No Compromise ([www.nocompromise.org](http://www.nocompromise.org)), which defines itself as

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

*“The militant, direct action news source of animal liberationists and their supporters.”* includes within its gallery archive, photographs of Federal Agents. The images included in this part of the site *“are photos of federal government officials who have nothing better to do with their time than harass activists”*. This website also provides access to a “Directory of Abusers”, which lists labs conducting animal testing including their addresses and the home addresses and telephone numbers of the directors and managers of these labs. Finding this type of listing on a website is especially interesting, particularly in terms of its similarity to what are known as the ‘Nuremberg Files’, a listing of abortion doctors in the U.S. which was distributed online by Anti-abortion extremists. Although the ‘Nuremberg Files’ were claimed not to be a death list, following its presence online a number of assassination attempts were made on abortion doctors, successful in the case of Dr. Selpian. Whilst court proceedings followed to ensure the removal of this list from the Internet alternate versions of it can still be found on particularly extremist anti-abortion websites.

Websites are undoubtedly useful to terrorist movements in the orchestration of their propaganda campaigns. However, once a website of interest has been found by a supporter its role is limited and the role of the supporter remains relatively passive, limited to downloading information, perhaps donating funds. This is where virtual communities in support of terrorist movements constitute a significant change in the role of the online supporter. Through involvement in a virtual community the online supporter can move from the passive onlooker toward a potentially more active role. This progression is certainly interesting from a psychological perspective, particularly in terms of how online activities might inform our understanding of processes of involvement and pathways toward radicalisation in the offline world.

### ***Facilitating Involvement: Considering Virtual Communities of Terrorist Support***

The term virtual community is used here as an ‘anchor’, an already formulated notion of shared online space and communicative interaction between users. Community in cyberspace can be perceived in the same ways as communities in the physical world; they can be characterised by regular user interaction, most often with a sense of status associated with long-term membership, the construction of ‘relevant’ discourses with interactions adhering to community ‘norms’, with these often developed through a process of in-group monitoring.

Virtual communities vary in their levels of technological sophistication and of course in terms of the content of the discourses created within them, particularly in terms of ideology, current affairs and so forth. Similarities lay primarily in how these communities function in particular ways, both for the individual and the group, in terms of communication, information dissemination, propaganda, ideological development, the development of a negotiated political identity (individual and group), and increasing involvement in support activities over time. Furthermore, these functions are important in relation to the social and psychological processes to which they relate, such as how social interaction within the community can be viewed in terms of processes themselves; processes of communication (including propaganda), processes of identity negotiation and processes of involvement and increased support and activity over time.

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

Research in this area (Bowman-Grieve 2006) indicates that the discourses created within virtual communities are fundamentally similar; community members use their virtual community to discuss and debate, to praise and to criticise, creating discourses related to issues of importance to the movement. Such discourses often consider how the movement might move forward to achieve their goals and aims and it is often from this perspective that the decision to use violence or terrorism is discussed, with the choice to use terrorism often justified as the only viable course of action.<sup>iii</sup>

### **Identity Negotiation, Recruitment & Radicalisation**

*“Everyone, Republican or otherwise has their own particular part to play. No part is too great or too small, no one is too old or too young to do something.”* (Bobby Sands 1954- 1981)

#### *Identity Negotiation*

The negotiation of self-identity is an important function of the virtual communities and an important process for members, many of whom join the community with little sense of their position on various issues and who therefore negotiate their views over time and through interaction with other, often more experienced, community members. This process is also important in relation to the status of members, with older members (those who have negotiated their political identity) interacting with newer (or less sure) members and facilitating their identity negotiation and development. Similarly this process of negotiation allow for the justifications and legitimations of support to be verbalised and reiterated providing validation for members. In-group validation serves an important psychological function for group members contributing to their sense of community and of the validity of their views and opinions, which are often in the minority in everyday life outside of this virtual community. In these communities supportive views for extremist and terrorist movements are acknowledged and accepted, thus normalising these ideologies for the individual, and contributing to the creation and sustenance of strongly held views that are more resistant to change in the long term. The processes involved in community justifications and validations can also contribute to increased ideological control. Whilst community members are encouraged to negotiate their political affiliations and ideologies through on-going interaction, other community members also encourage them in blatant and subtle ways to demonstrate their commitment and support through action and involvement. Thus, the ideology of the group and group processes within the virtual community can contribute to increased ideological control in in-group members, particularly those who seek to ‘prove’ their commitment to the group.

Identity negotiation and ideological control occur over time, input from the individual community member and interaction with other community members. As such political identity is open to radicalisation within the online community. Wenger (1998) suggests that we experience identity in practice; that it is a lived experience within a specific community. Similarly the construction of identity can be viewed as a central part of learning (Lave and Wenger 1991; Packer and Goicoechea 2000). According to this argument, learning is viewed as social participation with the onus upon each individual to construct their own identity within the social space of the group. This occurs through processes of participation and interaction (Packer et al. 2000). Additionally, Wenger (1998) argues that we develop identity by assessing who we are in relation to the community in which we are practising members so that in a practical

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

sense, identity development occurs through participation and interaction within the community. This negotiation of identity is a reflexive process, where individuals must be capable of considering and reflecting on the meaning of their own identity throughout the process of negotiation. In this sense identity construction is a careful negotiation between the individual and the community.

### *Recruitment & Radicalisation*

The discourses created and sustained within the virtual communities are used to disseminate information, to communicate ideologies, to promote and propagandise, to encourage involvement and throughout all of these to potentially facilitate the radicalisation of individuals and groups. These discourses seek to dehumanise the enemy, to delegitimise the enemy and to justify and legitimise the ideology of the movement. Their sustenance contributes to the community of validation that exists for members of the movement and their content contributes to the justifications of the use of the terrorism (often despite in-group differences of opinion). These discourses in particular promote the notion of a 'right' to act in whatever way necessary in the face of an 'imminent' threat, always identified as some 'other' that is wholly 'evil'. Such ideals can contribute to the radicalisation process, making the decision to use violence or terrorism unavoidable and therefore the responsibility of the enemy.

Committed virtual community members exist in a pre- or semi-radicalized state. In this state individuals are aware of the 'conflict' and the goals of the movement. They are open to movement propaganda that espouses the movement's ideology. Through online interaction they have negotiated a position, perhaps even a role for themselves as a supporter. They may have become involved in support activities, on and offline. In this sense virtual community involvement can be viewed as a potential pathway toward radicalisation. Increased involvement over time may parallel increased ideological development and control (as a justification for actions a priori or post hoc). Processes of support and involvement, facilitated by online interaction, can contribute to ideological control and individual radicalisation, particularly when these are viewed as incremental processes, with each stage linked with the previous and demonstrating increased involvement in increasingly illegal or violent activities and behaviours over time. If involvement is considered in this way, as a process increasing over time, then particular interventions at any of the various stages might be open to development. Individual radicalisation (i.e. individuals becoming involved in the support of or the carrying out of violent activities) while not facilitated by online interaction alone, may be related to earlier stages of the support and involvement process and the formation of interpersonal bonds and relationships, an important factor in the recruitment process (della Porta 1988, 1992; Sageman 2004). Arguably, the most potent combination to facilitate radicalisation that incorporates use of the Internet will be exposure to radical ideology online, in addition to exposure to radical ideology and behaviour in the physical world.

## **Countering Terrorist use of the Internet**

### *Internet Regulation & the Role of Civil Society*

*"It is essential to appreciate the very strong collective ethos of the Internet. From its inception Internet users have always been passionately in favour of internal control*

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

*and against outside influence. In effect, for many years the Internet has operated as a fully functioning anarchy.”* (Langford 1998, p. 98)

Regulating, governing and possibly censoring the Internet is met with complex arguments both for and against any such moves, primarily because it is not a simple thing to apply the traditional laws of a state or international community to the Internet which, as a vast network, recognises no international borders. Unfortunately, because of the nature of the beast and the lack of international legislation regulating it, websites and virtual communities in support of terrorism proliferate online. It is important to note that while some websites can be easily found (because those who construct and maintain them want them found by potential supporters), others are more difficult to track, particularly those which seek to remain hidden to all but a select membership. Take for example the website “Alneda.com”, this is the name of the website believed to be the primary means of communication initially used by Al Qaeda (currently over fifty websites in support of Al Qaeda exist online (Weimann 2006a)). Legitimate service providers originally hosted Alneda.com and removed the site having been alerted to its contents. Although ownership of the domain name was lost, Alneda.com, continues to exist online according to Delio (2003). The website now appears to function as an Internet parasite, embedding itself within other websites without the owner’s knowledge, for example by burying itself in sub-directory files. Although the site is not updated regularly it appears to be updated upon relocation, and its location is indeed difficult to ascertain at any given time and without the relevant knowledge. Generally, followers of the website are alerted to its newest location through posts on radical Bulletin Boards and particular mailing lists. As complicated as it may appear to regularly relocate a website and bury it within an already established (and apparently legal and unassociated) website, it is in reality a relatively uncomplicated manoeuvre manageable with ‘cracking’ tools that are currently available online (Delio 2003).

Internet regulation and legislation are important issues; however the question of who does the regulating remains pertinent. As the Internet is a public domain, many Internet watchdogs, human rights groups and other concerned citizens argue that any decisions made with regard to the issue of regulation and/or censorship must seriously consider the wider implications of such issues and the importance of the role of civil society in making these decisions.

Civil society refers to the arena of un-coerced collective action around shared interests, purposes and values. Civil society can be meaningful in contributing to the development of respect for diversity and tolerance and may be useful in bridging cultural divides (Shulman 2004). The institutional forms of civil society can be distinguished from those of the state and may include foundations, think tanks and other non-governmental organisations. Civil society as a concept has modernised over time and in relation to modernisation in our world. As such, the forms of civil society we see today offer new, alternative and innovative forms of solidarity, connectedness and civic and political engagement, in particular as these are now facilitated by the Internet (Ester & Vinken 2003). According to Shulman (2004) active civil society can enhance the vitality of democracy and may function as a means of easing interaction between the state and the individual. The Internet can facilitate a degree of organisational cohesion and coherence to groups outside of the political establishment



Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

who seek to orchestrate campaigns of political protest without relying on the traditional mass media (Reilly 2003). While civil society currently has positive connotations it is important to note that not all civil society is good, for example the Ku Klux Klan was a civil society organisation. In fact terrorist movements, according to Reilly (2003, p. 1), “*use the Internet like marginalised elements of “civil society” to communicate with sympathetic diasporas, disseminate propaganda and issue statements unfettered by the ideological refractions of the mass media*”.

Given the nature of terrorism, in particular the psychological element of this strategy with its aims of undermining public morale and creating an atmosphere of fear (which may incidentally lead to the acceptance of policy and legislation that effects public civil liberties over time, as has been seen post 9/11), it is important to recognise the role the public can play in counter- and anti- terrorism strategies, in particular the role of civil society. Because the Internet is a public domain offering almost unlimited access to the user, it is important that the public who use this technology are afforded the opportunity of monitoring this domain themselves. The appropriate role of civil society in addressing terrorist use of the Internet has not yet been clearly addressed. However, arguably its primary online role is in self-regulation; civil society can take the role of in-group monitors. However, as Jewkes (2002) points out, self regulation can too be problematic, in some cases giving rise to online vigilantism. Nevertheless, civil interest groups have the potential to act in a real and useful way in attempting to limit the use of the Internet by deviant, extremist or terrorist movements.

Internet Haganah (Internet Defence) is a website dedicated to this purpose - researching, reporting and shutting down Internet websites currently being used to support terrorist organisations and their activities. Their focus is primarily on Islamist terrorist websites and the site itself is run on a voluntary basis. They argue that because the sites they target are usually in violation of their hosts' terms of service action can be taken to have them removed. According to the website, volunteers have succeeded in shutting down more than 700 terrorist support sites. All of the sites removed represented organisations designated terrorist by the US State or Treasury Departments. Of course due to the very nature of the Internet it is not unusual to see many of these sites back online in a short period of time. However, this group of volunteers remains vigilant in their fight against terrorist use of the Internet. This group of volunteers represents a form of self-regulation and self-governance online; a group of concerned individuals working to remove terrorist support sites making them less accessible.

### **The Internet and Possible Counter-Terrorism Initiatives**

Apart from Internet watchdogs and the role they might play, both civil society organisations and the government can also play an active role in using the Internet to counter terrorism in other ways, for example by attempting to counter the propaganda campaigns of such movements. In fact, the UN has historically used this approach particularly in relation to combating racism. The Internet offers no greater medium to launch such campaigns. Effective counter-propaganda campaigns can be conducted online, as terrorist and extremist movements have demonstrated through their own Internet use. Such propaganda campaigns must consider the importance of both the credibility of the communicator and the audience being targeted.

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

In considering this further it may be useful to use former terrorists or former supporters of terrorism in the dissemination of anti-terrorist material and propaganda. The experiences and perceptions of former terrorists or supporters can lend credibility to the anti-terrorist argument and may be particularly useful in reaching those who have become more entrenched in the ideology and the group they support. Similarly, propaganda campaigns must recognise the various audiences being targeted and their levels of commitment to the movement or ideology, which range from those who are 'on the fence' to those who are supportive but not active in their support, to those who are actively involved in support related activities. The effectiveness of counter-propaganda is dependent on various factors, such as the credibility of the communicator, the organisation of persuasive arguments, the use of fear arousing appeals, group and individual factors (Hovland et al. 1953). These factors warrant serious consideration in preparing and presenting such campaigns to public audiences.

Crelinsten and Schmid (1992), also suggest that particular communication strategies and psychological operations (PsyOps) can contribute to the fight against terrorism. Arguably such strategies can also be effectively promoted online. These communication strategies can be divided into those that are considered offensive or defensive operations, in other words those directed at one's own community or those directed at the constituency of the terrorists. In essence, any anti-terrorism propaganda campaign must be well structured, coordinated and integrated considering both the importance of the communicator and the importance of the particular audience being targeted.

Likewise, the Internet can be used by governmental and non-governmental organisations in positive ways to combat terrorism through educational campaigns, particularly those that promote non-violent forms of debate and dissent, such as those that encourage non-violent conflict resolution and promote negotiation and compromise (Weimann 2006a). Educational web campaigns can also actively challenge the "*morally disengaged rhetoric*" of terrorist movements and "*can provide potential recruits with logical analysis of a groups' purported grievances and activities*" (Weimann 2006a, p. 240).

Finally, Internet use by terrorist and extremist movements can be used to gather Intelligence necessary for counter- and anti- terrorism strategies. Such 'Intell' relating in particular to perceptions of successful attacks and acceptable targeting for example, may be useful in preparing for counter- and anti- terrorism initiatives and in the planning of intervention strategies.

In conclusion, given the difficulty in tracking & tracing cyber communications, the lack of globally accepted processes & procedures for investigation and inadequate and ineffective information sharing between public & private sectors (Weimann & Von Knopp 2008), it is apparent that in order to attempt in any real way to combat terrorist use of the Internet at the very least there must be an international recognition and agreed definition of the problem area. Such definition and recognition of an international issue is essential for the evaluation of the problem from an international perspective in order to develop 'International Strategies' to attempt to combat it effectively.

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

---

<sup>i</sup> [www.Kahane.org](http://www.Kahane.org) is an Israeli Extremism website and the first website to be designated a terrorist organisation by the US Dept. of State, 2003.

<sup>ii</sup> This website no longer exists but it was previously located at <http://www.ulisnet.com> which now appears to be an general information website made up of external links.

<sup>iii</sup> This relates to supporting literature that sees terrorism as a strategic choice, see Crenshaw 1990.

### **References**

- Arendt, H. (1990) *On Revolution*. London: Penguin Books.
- Bogart, L. (1976) *Premises for Propaganda: The United States Information Agency's Operating Assumptions in the Cold War*. New York: Free Press.
- Bowman-Grieve, L. (2006) *Terrorist supporters and the Internet: An exploration of online 'virtual' communities*. PhD Thesis, Department of Applied Psychology, National University of Ireland, Cork.
- Conway, M. (2003) *Cybercortical warfare: The case of Hizbollah.org*. Paper presented at the European Consortium for Political Research (ECPR) Joint Sessions of Workshops, Edinburgh, UK.
- Crelinsten, R.D. & Schmid, A.P. (1992) Western responses to terrorism: A twenty-five year balance sheet. In A.P. Schmid (Ed.) *Western Responses to Terrorism*. Special issue of *Terrorism and Political Violence*, 4(4), pp. 322-323.
- Crenshaw, M. (1990) The logic of terrorism: Terrorist behaviour as a product of strategic choice. In W. Reich (Ed.), *Origins of terrorism: Psychologies, ideologies, theologies, states of mind*, Cambridge: Cambridge University Press, pp. 7-24.
- Delio, M. (2003) Al Qaeda website refuses to die. Available from <http://www.wired.com/techbiz/it/news/2003/04/58356?currentPage=2> [Accessed March 10, 2009].
- della Porta, D. (1988) Recruitment processes in clandestine political organizations: Italian left-wing terrorism. *International Social Movement Research*, 1, pp. 155-169.
- della Porta, D. (1992) Political socialization in left-wing underground organizations: Biographies of Italian and German militants. In D. della Porta (Ed.), *Social movements and violence: Participation in underground organizations*, Greenwich, CT: JAI Press, pp. 259-290.
- Ester, P., & Vinken, H. (2003) Debating Civil Society: On the fear for civic decline and hope for the Internet alternative. *International Sociology*, 18, 659-680.
- Jewkes, Y. (2002) Policing the Net: crime, regulation and surveillance in cyberspace. In Y. Jewkes (Ed.) *Dot.cons: crime deviance and identity on the Internet*, Devon UK: Willan Publishing, pp 15-35.
- Hovland, C.I., Janis, I.L., & Kelley, H.H. (1953) *Communication and persuasion: Psychological studies of opinion change*. New Haven: Yale University Press.
- Hundeide, K. (2003) Becoming a committed insider: Acquiring skills through participation as an apprentice in a community of practice. *Culture and Psychology*, 9(2), 107-127.
- Kendall, L. (1999) Recontextualising "cyberspace": Methodological considerations for online research. In S. Jones (Ed.), *Doing Internet Research: Critical issues and methods for examining the Net*, London: Sage Publications, pp. 57-74.
- Langford, D. (1998). Ethics @ the Internet: bilateral procedures in electronic communication. In B. Loader (Ed.) *Cyberspace Divide: Equality, Agency and Policy in the Information Society*. London: Routledge, pp. 98-112.
- Lave, J. (1988) *Cognition in Practice*. New York: Cambridge University Press.
- Lave, J. & Wenger, E. (1991) *Situated learning: Legitimate peripheral participation*. Cambridge: Cambridge University Press

Bowman-Grieve, L. (2011). The Internet & terrorism: Pathways toward terrorism & counter-terrorism. In A. Silke (Ed.), *Psychology, Terrorism and Counterterrorism*. Oxon: Routledge, pp76-88.

---

- Levin, B. (2002) Cyberhate: A legal and historical analysis of extremists' use of computer networks in America. *American Behavioural Scientist*, 45 (6), 958-989.
- Packer, M. & Goicoechea, J. (2000) Sociocultural and constructivist theories of learning: Ontology, not just epistemology. *Educational Psychologist*, 35, (4), 227-241.
- Reilly, P. (2003) 'Civil Society, the Internet and Terrorism: Two case studies from Northern Ireland', Presented at the European Consortium for Political Research Joint Sessions of Workshops, Edinburgh. Available from <http://www.essex.ac.uk/ecpr/events/jointsessions/paperarchive/edinburgh/ws20/Reilly.pdf> [Accessed January 16, 2009].
- Sageman, M. (2004) *Understanding terrorist networks*. Philadelphia: University of Pennsylvania Press.
- Shulman, M. R. (2004). *Civil Society's response to the challenges of terrorism: A conference Report*. From a meeting held at headquarters of the Luso-American Foundation, Lisbon, Portugal, June 7-8.
- Tsafti, Y., & Weimann, G. (2002) [www.terrorism.com](http://www.terrorism.com): Terror on the Internet. *Studies in Conflict and Terrorism*, 25, 317-332.
- Weimann, G. (2006a) *Terror on the Internet: The new arena, the new challenges*. Washington D.C.: The United States Institute of Peace Press.
- Weimann, G. (2006b) Virtual Disputes: The use of the Internet for terrorist debates. *Studies in Conflict and Terrorism*, 29, 623-639.
- Weimann G. & von Knopp, K. (2008) Applying the Notion of Noise to Countering Online Terrorism. *Studies in Conflict & Terrorism*, 31, 883-902.
- Wenger, E. (1998) Communities of practice: Learning as a social system. *Systems Thinker*, June.
- Whine, M. (1998) Islamist organisations on the Internet. Available from <http://www.ict.org.il/Articles/tabid/66/Articlsid/716/currentpage/32/Default.aspx> [Accessed November 2, 2008].
- Whine, M. (1999) Cyberspace: a new medium for communication, command and control by extremists. *Studies in Conflict and Terrorism*, 22 (3), 231-245.
- Whine, M. (2000) The use of the Internet by far right extremists. In B. Loader & D. Thomas (Eds.), *Cybercrime: Law, security and privacy in the information age*. London: Routledge, pp. 234-250.