



Relocating the Virtual War

Gilbert RAMSAY

Centre for the Study of Political Terrorism and Violence, University of St. Andrews, Scotland

Abstract: *Countering Al Qaeda and other terrorist groups' use of the Internet for both organizational purposes and the dissemination of radical propaganda has frequently been conceptualized in terms of a war in a virtual space. This assumption has led to a distorted understanding of how the Internet is relevant to terrorism, and what methods are appropriate for addressing this. In particular, it has led to an overemphasis on action by governments 'on' the Internet. This entails moving the 'fight' into a terrain in which it cannot easily be won. Better strategies for countering the benefits terrorists draw from the Internet might proceed from instead drawing on governments' overwhelmingly greater power over matter and physical space, and their ability to shape agendas across the complete spectrum of media.*

Keywords: *Terrorism, Al-Qaeda, internet, media, virtual war, counter-terrorism.*

Introduction

The issue of countering the use of the Internet for terrorist purposes has become an increasing policy concern in recent years. While the 'Electronic Pearl Harbour' foretold by writer and consultant Winn Schwartau¹ has not yet materialized (if 'materialized' is quite the right word for such a phenomenon), there is now a significant literature devoted to the various ways in which the Internet can be used to further the purposes of terrorist groups. Terrorists, it has been proposed, use the Internet for a wide variety of purposes, such as fundraising, training, recruitment, networking, secret communication, propaganda, intelligence gathering, psychological warfare and so on – depending on which particular list of such uses is consulted.

Given the exploitation of the 'new arena' of the Internet by terrorists, who are supposed to find therein a 'safe haven' for organizational activities which are no longer so easy to conduct in more traditional ways, the argument has tended to run that ways must be found of bringing the Internet

¹ Winn Schwartau, *Terminal Compromise*, Interpact Press, New York, 1991.

more thoroughly under control. As one scholar puts it, 'the war against Al Qaida has been fought on a virtual as well as a physical battlefield'.² The Internet, a British cabinet minister has said, is not a 'no-go area' for government.³ Indeed, more apocalyptically, a US senator has pronounced that 'we cannot afford to cede cyberspace to the Islamist extremists, for if we do they will attack us in our normal environment'.⁴

Given the apparently unquestioning reliance on the spatial metaphor of cyberspace as a way of conceptualizing the relationship between terrorism and the Internet, it is perhaps not surprising that proposals to counter this threat have also tended to emphasize activity by governments and others 'on' the Internet. In this vein, Davis (2006) has emphasized a dramatic strengthening of the Internet 'governance' exercised by ICANN (the Internet Corporation for Assigned Names and Numbers – a non-profit corporation responsible for administering the Internet's underlying address system) and the United Nations. Weimann and Von Knop,⁵ by contrast, have called for a more unilateral approach in which individual actors would use the principle of 'noise' in order to disrupt terrorist dissemination of content on the Internet. This could vary from counter-narratives, aimed at challenging terrorist discourses, through to more unconventional (some might say underhanded) tactics such as the use of cyberattacks or malware to disrupt terrorist communications. The principle of 'counter-narrative' on the Internet has also been endorsed by recent think tank reports, including the Institute for European and International Affairs' Countering Militant Islamist Radicalisation on the Internet and the Centre for the Study of Radicalisation and Political Violence's Countering Online Radicalisation: A Strategy for Action. The latter advocates the use of small start up seed funds for community based initiatives aiming to use, in particular 'web 2.0' as a means for promoting alternatives to radical (Islamic) agendas.

The purpose of this paper will be threefold: to challenge (or at least query) some of the assumptions that are generally made about the relationship between terrorism and the Internet; to point out some of the flaws in approaches which depend on addressing the notion of 'terror on the Internet' and, finally, to suggest how many of the actual terrorist threats arising from use of the Internet may be better addressed by focusing not on the 'virtual' arena, but rather on the very substantial powers which governments retain over the physical world in which, thus far, terrorism has continued to actually take place. Many of these proposals are, as we shall see, normal actions which governments are already taking. Recognizing their significance, however, against terrorist use of the Internet offers a potentially useful way to reframe action against this particular issue.

² Akil Awan, "Al Qa'ida's Virtual Crisis," *The RUSI Journal*, Vol 154, 1, 2009, p. 1.

³ Jacqui Smith, reported in Tim Stevens and Peter Neumann, *Countering Online Radicalisation, A Strategy for Action* International Centre for the Study of Radicalisation and Political Violence, London, 2009, p. 7.

⁴ Senator Joseph Lieberman, quoted in Anne Broach, 'Terrorists voice alarm over terrorist Net presence' CNET News May, 3, 2007 available at http://news.cnet.com/Senators-voice-alarm-over-terrorist-Net-presence/2100-1028_3-6181269.html.

⁵ Gabriel Weimann and Katherina Von Knop 'Applying the Notion of Noise to Countering Online Terrorism', *Studies in Conflict and Terrorism* Vol 31, No 10, pp. 883-902.

Terrorism and the Internet

What's in a name? A remarkable feature of discussion on terrorism and the Internet has been the number of different formulations used to describe the phenomenon (if, indeed, it is a single phenomenon that is being described). Cyberterrorism is still, particularly in policy circles, used in a broad sense to refer to the full gamut of uses to which terrorists might put the Internet, from cyberattacks through to social networking. Generally speaking, academics have tended to favor somewhat more precise language: cyberterrorism, it is insisted, eg Denning,⁶ is to be understood strictly as the serious disruption of computer systems resulting in real, frightening damage for ideological purposes. It is not equivalent to just any use of the Internet by terrorists – for example, for purposes of fundraising, recruitment, internal communication, dissemination of training and so on.

Uses of the Internet which are in some way 'terrorist', but which are not 'cyberterrorism' are, in turn, described by a number of different formulations. Lt Col Timothy Thomas⁷ proposed the term 'cyberplanning' to describe this set of situations. Others have preferred less snappy, but arguably more descriptive phrases. Conway⁸ favors 'terrorist "use" of the Internet' – the quote marks perhaps implying the term 'misuse' or even 'abuse' often favored by governments, rather as if sending someone a letter calling for bloodthirsty revolution were an illegitimate abuse of the good will of the postal service. Weimann has used formulas such as 'how ...terrorism uses the Internet',⁹ 'terror on the Internet'¹⁰ and simply 'online terrorism'.¹¹ A more cautious phrase adopted by the Council of Europe¹² and the United Nations¹³ has been 'use of the Internet for terrorist purposes'. Hovering around the edges of the subject area have been related concerns such as 'radicalisation on the Internet',¹⁴ 'cyberwar'¹⁵ and 'information war'.

⁶ Dorothy Denning, 'Is Cyber Terror Next?' SSRC essays, 2001 <http://www.ssrc.org/sept11/essays/denning.htm>, also Dorothy Denning 'Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Arquilla and Ronfeldt (eds) *Networks and Netwars: The Future of War, Crime and Militancy* RAND, Santa Monica, 2001 pp. 239-288.

⁷ Lt Col. Timothy Thomas, 'Al Qaeda and the Internet: The Danger of "Cyberplanning"', *Parameters*, Spring 2003, pp. 112-123.

⁸ Maura Conway 'Terrorist "Use of the Internet, and Fighting Back' International Relations and Security Network, 2006 <http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=20642>.

⁹ Gabriel Weimann, 'www.terror.net: how modern terrorism uses the Internet' Special Report, United States Institute of Peace, 2006 <http://www.usip.org/pubs/specialreports/sr116.html>.

¹⁰ Gabriel Weimann *Terror on the Internet: The New Arena, The New Challenges*.

¹¹ Op cit. p. 2.

¹² Ulrich Sieber, *Cyberterrorism: The Use of the Internet for Terrorist Purposes*, Council of Europe Report, 2007.

¹³ See 'Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes' <http://un.org/terrorism/workgroup6.shtml>.

¹⁴ Akil Awan, 'Radicalization on the Internet?' *The RUSI Journal* Vol 152, No 3, 2007 pp. 76-81.

This lack of a precise terminology matters. It indicates a continued uncertainty as to what we are actually talking about. Is the problem with ‘terrorists’ on the Internet, for example, or is it with ‘radicals’? If the former, then are we talking about actual ‘terrorists’, or about some sort of new category of ‘terrorists on the Internet’. If the latter, then what assurance is there that radicalism is, in itself, something to worry about? Is it cause for concern simply that terrorists use the Internet (of course they do!), or is the point that the unique capabilities of the Internet give rise to a new and unique type of terrorist phenomenon requiring special remedies?

To make the point concrete, there is the issue of ‘terrorist websites’. Various estimates of the number of these exist: a lower estimate being around 5,300¹⁶, an upper estimate being as many as 50,000.¹⁷ None of these estimates, however, provide an accurate definition of what a ‘terrorist website’ actually is. If it is the site of a ‘supporter’ of terrorism, then that is categorically different (though not necessarily recognizably different) from a website actually maintained by a terrorist organization. Are individuals behind ‘terrorist’ websites (of whatever definition) contributing to ‘terrorism’ on that account? Are ideological supporters of terrorism guilty of a terrorist offense on that account? The problem is that, uncomfortable as it may sound, support for terrorist groups is often more widespread than the small number of actual participants in the violence. As Gupta points out, ‘while an entire community may be sympathetic to the cause, a miniscule minority carries out the acts of violence.’¹⁸ Acting, therefore, on the assumption that sympathy for terrorism is a kind of terrorist offense may be a classic example of the counterproductive counterterrorist excess criticized by Silke.¹⁹

At the same time, there are certainly ways in which the Internet’s unique convergence of capabilities does appear to present some genuine conundrums in this regard. The Internet, as has often been observed, helps to collapse the distinction between consumer and producer. As Conway points out, an implication of this is that it also collapses the distinction between the terrorist propagandist and the consumer of this propaganda.²⁰ This in turn invites, so it seems, ideas of ‘networked’, ‘leaderless’, ‘home grown’ types of terrorism, in which individual consumers-producers-interacters of terrorist propaganda go on to think of themselves as participants in a wider militant movement and, from there, move on either to more concrete forms of support activity (e.g. fundraising and recruitment) or actually progress to violence themselves.

¹⁵ John Arquilla and David Ronfeldt, ‘Cyberwar is coming!’ in John Arquilla and David Ronfeldt (eds) *In Athena’s Camp: Preparing for Conflict in the Information Age* RAND, Santa Monica, p. 23.

¹⁶ Gabriel Weimann ‘The Psychology of Mass-Mediated Terrorism’ *American Behavioural Scientist* Vol 52, No 1, 2008 pp. 69-86.

¹⁷ Eric Swedlund, ‘UA effort sifting web for terror threat data’ *Arizona Daily Star* 24/09/2007.

¹⁸ Dipak K. Gupta ‘Towards an Integrated Behavioural Framework for Analysing Terrorism: Individual Motivations to Group Dynamics’ Paper presented at the annual meeting of the International Studies Association, San Diego, California 22/03/06.

¹⁹ Andrew Silke ‘The Fire of Iolous: The Role of State Counter-Measures in Causing Terrorism, and What Needs to be Done’ in Tore Bjorgo (ed) *Root Causes of Terrorism: Myths, Reality and Ways Forward* Routledge, London, 2005, pp. 524-621.

²⁰ Maura Conway, ‘Mass Communication - from Nitro to the Net’ *The World Today* Vol 60 No 8/9 pp. 19-22.

Even taken at fact value, there is the paradox that the most obviously objectionable materials on the Internet in terms of flagrant attempts at incitement to violence are often not the 'official' websites of terrorist organizations, but rather the sites of their supporters.²¹

But it is worth stressing that this narrative of the role of the Internet in terrorism is only one possible interpretation of the story. Indeed, there are some (Kimmage: 2008 for example) who contend that the anarchic nature of the net is a thorn in the flesh to terrorist groups as much as it is to governments. Al Qaeda, embarrassed by the postings of enthusiastic but ignorant fans was forced to make moves to rein in what it called 'media exuberance'. Indeed, the posting guidelines for Al-Faloja²² – currently one of the primary outlets on the Internet of Al Qaeda affiliate propaganda – primly exhort posters to avoid material likely to give offense or create *fitna* (division) in the community, as well as, interestingly, information on subjects such as how to make bombs. According to the author's discussion with a member of the Belgian special police unit dealing with terrorism and the Internet, observers here have concluded that forums are rigidly controlled, and that posting even of official videos in advance of their specified issue date is cause for a serious reprimand.

Indeed, one fundamental problem of looking for 'terrorism' on the Internet is that it is so easy to find. With radical forums boasting memberships in the tens of thousands and a proliferation of radical materials of one sort or another, looking for actually dangerous individuals is, arguably, like looking for a needle in a stack of needles. Denning (and others) has rightly poured cold water on the idea of a threat posed by 'virtual terrorism' as practiced by groups such as the 'Second Life Liberation Army'.²³ However, statistical odds alone speak for the fact that hordes of avid 'jihobbyists' (to use the term proposed by Brachman)²⁴ are living out a not dissimilar fantasy – reveling in the sense of agency given them by practicing 'jihad of the tongue', but still a very long way from crossing over to the more demanding path of 'jihad of the sword'. Presumably, no one would be obtuse enough to mistake the irony intended in Syrian poet Ahmed Matar's popular poem 'Yes, I am a terrorist'; but, a not dissimilar discourse appears to stand behind the declarations of the popular jihadi nasheed 'Irhabyun Ana' (I am a terrorist), the handle of the 'cyberjihadi' irhabi007, and even the declaration made in the Al Qaeda document dating from 2007 entitled 'the dictionary' in which it is baldly declared that the word 'terrorism' is to be translated simply as 'jihad'. Where then, does this leave a case such as that of Muhammad Atef Siddique, who reportedly declared 'Osama bin Laden is my God' – a statement hardly likely to flatter the strictly literalist Wahhabi sentiments of the 'sheikh', - and was alleged to have 'caused a breach of the peace by claiming to be a member of the terror network, Al Qaeda'.²⁵ Reportedly, there were better reasons (inadmissible in court, because they derived from surveillance by intelligence) for why this individual, was prosecuted under the UK 2006 Terrorism Act, essentially

²¹ Gabriel Weimann and Yariv Tsfati 'www.terrorism.com: terror on the Internet' *Studies in Conflict and Terrorism* Vol 25, 317-332, 2002, 317-332.

²² <http://www.al-faloja.info/vb/announcement.php?f=10>

²³ Dorothy Denning 'The Jihadi Cyberterror Threat', powerpoint presentation from SUMIT 07, 2007.

²⁴ Jarret M. Brachman *Global Jihadism: Theory and Practice* Routledge, Abingdon (Oxon) 2009 p. 19.

²⁵ Aberdeen Press and Journal, 17/09/07.

for the possession of documents on explosive materials and the establishment of pro-Al Qaeda websites. As well, it has been alleged, Atef Siddique's online social network included individuals who were more deeply involved in activities preparatory to actual violence than he (apparently) was.²⁶ Nonetheless, the controversies surrounding this case provide an elegant illustration of the difficulties and ambiguities inherent in distinguishing between real terrorists and self-styled terrorists.

Another difficulty in approaching the issue of terrorism on the Internet is distinguishing between causation and mere co-occurrence. This is not just an issue in questions of Internet radicalization (does a large collection of terrorist propaganda material turn one into a terrorist, or is it simply a side-effect of another process which turns one into a terrorist?). It is also an issue of much more concrete uses of the Internet by terrorists. So, for example, Weimann (2006) asserts that the 9/11 hijackers 'used the Internet, and used it well'. According to Weimann's account, the 9/11 hijackers were heavy users of email, which they accessed through Internet cafés, even receiving orders in this way, by means of a very primitive word substitution cipher. They may indeed have 'used the Internet well' – but did they, in most respects a normal group of Western educated middle class Arabs, use the Internet any better, or any differently than their peers? If not, then the implication is that terrorist use of the Internet is, to this extent, an unremarkable correlate of the age, education and socioeconomic status of the individuals concerned. Of course, this may be the point. Indeed, it is perhaps ironic (given the frequent suspicion in which terrorism researchers are held, of being, as Wilkinson puts it, 'more right wing than Genghis Khan'), that much of the background to the assertion that the Internet is a powerful new medium for terrorism rests on a wide-eyed techno-optimism more characteristic of the new-age tinged liberalism of the likes of Howard Rheingold.²⁷

In fact, determining whether or not the Internet has really given terrorists a new edge is immensely difficult to prove either way – particularly where the issue is not with terrorists benefiting from 'abnormal' uses of the Internet (such as hacking or identity theft) but with 'normal' uses of the Internet. Globally speaking, there is no good evidence that terrorism, as a whole, has become more common or more lethal since the beginning of the 1990. Indeed, the period of the exponential rise of the Internet between the mid 1990s and the mid 2000s has seen an overall decline in the incidence and (9/11 excepted) a generally stable lethality of terrorist violence.²⁸

Reflecting on this fact does not negate the idea that the Internet is valuable to terrorists, but it does force us to reflect on what the usefulness of the Internet to terrorists actually means. Does the Internet give terrorists a special edge over counterterrorists (counterterrorists being understood in the broadest possible sense – not just as military and law enforcement personnel, but as anyone whose actions, intentional or otherwise, might ultimately result in terrorism not occurring)? Does

²⁶ Network diagram in Steve Swann, 'Aabid Khan and his Global Jihad' 18th August 2008 available at <http://news.bbc.co.uk/1/hi/uk/7549447.stm>.

²⁷ Howard Rheingold *The Virtual Community: Homesteading on the Electronic Frontier*, Addison Wesley Publishing, Reading (Massachusetts), 1993.

²⁸ See Rik Coolsaet and Teun Ven De Voorde 'The Evolution of Terrorism in 2005: A Statistical Assessment' Special Report, University of Ghent, 2006.

the Internet merely provide a different way for things to happen that would happen anyway, or does the Internet create new terrorist phenomena which are not so much better or worse, but simply different?

For example, just as it has been argued that many types of terrorist incidents in the past (for example barricade and hostage situations) have been deliberately orchestrated for maximum televisual impact²⁹, so too it might be argued that certain types of recent terrorist activity have been carefully scripted for the different properties of the Internet. Hence, it could be argued that hostage beheadings are ideally suited to the Internet's lack of censorship, super-abundance of choice (meaning that material needs to have a certain shock value to compete for attention) constraints on bandwidth (which rewards conciseness), temporal ambiguity (meaning that an image must contain its own narrative within itself), celebration of montage³⁰ and craving for physical authenticity³¹ (Gies 2008). This would relate to another well-known Internet video series: the 'Baghdad Sniper' of the Islamic Army of Iraq. Here, a particular series of violent acts have been elaborately assembled into a sophisticated new-media narrative. The Baghdad sniper videos are essentially compilations of sniper attacks on US personnel in Iraq. However, they have been stitched together around the (probably fictional) character 'Juba,' the sniper of Baghdad, who is portrayed as a paragon of Islamic and chivalric virtue – scrupulously discriminate in his use of violence, patriotic and pious. This character has been surrounded by a carefully constructed online personality cult. Anasheed (Islamic hymns) have been composed in his honor, and his website offers a variety of resources for fans – including posters. Paradoxically, however, despite the apparent artifice of the character of Juba, in the introduction to 'Juba, the Baghdad Sniper 2' a blurred out figure claimed to be the 'commander of the sniper brigade in Baghdad' explains the popularity of the videos in terms of bodily authenticity: 'filming the operations is very important, because the scene that shows the falling soldier when hit has more impact on the enemy than any other weapon'. This is in contrast to other types of attack commonly filmed by the IAI such as roadside IEDs or rocket attacks, where casualties are not normally visually apparent.

This illustrates elegantly the difficulty of distinguishing issues of terrorism 'on the Internet' from the Internet actually leading to terrorism on the ground. Creating a montage of sniper assassinations makes for compelling propaganda, but did the 'Juba' project actually inspire the Islamic Army in Iraq to carry out assassinations purely for the sake of the video? If it did, did this displace other kinds of more lethal or more reprehensible attacks? Are hostage beheadings worrying because of their inherently repulsive qualities (like a sort of violent equivalent to obscene pornography); are they worrying because they may encourage others to go and do likewise? Are they worrying (to make a subtle, but important distinction) because their success as propaganda may lead terrorist groups to carry out more of them? Certainly, hostage beheadings are upsetting and effective at achieving 'terror', but they are no more lethal than any other situation in which terrorists kill a hostage.

²⁹ For examples of this see, eg Alex Schmid and Janny de Graaf *Violence as Communication: Insurgent Terrorism and the Western News Media*, London, Sage 1982.

³⁰ See Lev Manovich, *The Language of New Media* MIT Press, Cambridge, Massachusetts, 2002.

³¹ Lieve Gies, 'How Material are Cyberbodies? Broadband Internet and Embodied Subjectivity' *Crime, Media, Culture* Vol 4, No 3, 2008 pp. 311-330.

Terrorism is not just about lethality. By this metric, it is well known that terrorism has always been insignificant by comparison with other types of cause of death. The impact of terrorism has always been psychological as well as physical. Its sensationalism is an inseparable part of its reality. Nonetheless, the idea that terrorism 'on' the Internet must be countered 'in' cyberspace implies a worrying shift away from the centrality of concern over the actual damage that terrorism does to human lives and towards a much more nebulous concern over the presumed danger presented by certain combinations of words and ideas. But the objection to attempting to fight terrorism 'on' the Internet is not just an objection to a project which could risk becoming a creeping de-legitimization of the right to dissent. It is also an objection to engaging in a misconceived and potentially expensive attempt to shift the 'battle' against terrorism to a place where it cannot be won.

Combating Terrorism on the 'Virtual Battlefield'

While determining what 'terrorism on the Internet' could actually mean is difficult, determining, in the abstract, what sort of online actions might be taken against it is relatively straightforward. This is because, ultimately, the Internet is not a parallel dimension, but rather a means for the transmission of electronic data between computers. This means that, in any activity taking place by means of the Internet, there are two basic issues at stake: the fact of communication taking place, and the dissemination, in the course of this communication, of an item of digitally expressed information. It is a central peculiarity of the Internet and other forms of digital communication that the properties of digital content (as discussed by Negroponte: 1993), that digital information of any kind, once created, can be copied infinitely at virtually zero cost, and this fact creates an important duality between person to person communication and the mass dissemination of content. Nonetheless, it is possible for the sake of simplicity to distinguish between two basic issues: *interpersonal communication* by electronic means, and social activities occurring in an online public space through the medium of *digital content*.

Interpersonal communication, as a counterterrorist issue, is in essence the same problem regardless of medium (though concern, specifically, over electronic communication by terrorists has played its part in justifying laws such as the USA PATRIOT act, and in the UK the Regulation of Investigative Powers Act). In principle, the question 'should we monitor communications on the Internet?' is identical to the question 'should we tap phone lines?' or 'should we steam open envelopes?' This is not to say that there are not Internet specific concerns. Far from it; the basic architecture of the Internet as a packet switched 'best effort' system means that any attempt to intercept communications, in contrast to a directly routed telephone conversation, is liable both to unwarranted intrusion into the private communications of non-suspects and to being thwarted by evasive means. Moreover, the economic organization of Internet Service Provision provides a further policy dilemma regarding what level of customer data governments can legitimately require.

However, such concerns have not tended to lend themselves well to discussions on the issue of 'countering' terrorism on the Internet (though they take a prominent place in Weimann's: 2006 chapter on the subject). They are at once too generalized (they impinge on all sorts of illegal activity that may be conducted by means of the Internet, not only terrorism); and too specific (they

tend to relate to concretely criminal actions, such as conspiracies to commit actual crimes). Finally, they give rise to no obviously new terrorist phenomenon. A technology which enables X and Y (who must already have successfully established each other's bona fides – perhaps through face to face contact) to communicate with each other secretly implies no dramatic change in the underlying way in which terrorism happens – just a new evolution of ancient practice to keep up with new technology.

In so far as it has produced genuinely new social phenomena, the Internet has not done so simply by being a text and graphic based version of the phone system. Rather, the revolutionary potential of the Internet has derived from the potential of multi-way exchanges of digital data to create the possibility of 'public space'. This is no less true for assertions about terrorism on the Internet as it is for anything else. Claims about terrorists providing 'training' on the Internet, 'recruiting' on the Internet, 'networking' on the Internet and even, in some instances, raising funds on the Internet are founded on the notion of there being online public spaces of multi-way communication in which such things can occur. While the World Wide Web is by no means the only Internet application which creates this possibility, any multi-way communication by any means (for example, instant messenger) ultimately entails the existence of a quasi-physical 'space' created by the existence of digital items viewable by several people at once. In other words, online community relies on the notion of several people looking at the same thing at once. This means that, ultimately, it boils down to a question of what to do about digital content.

What to do About Digital Content?

Given the notion that digital content of a given type is pernicious in its effects, there are two obvious courses of action that might be taken. Either attempt to eliminate the content in question (or at least make it more difficult to get hold of), or, somehow, attempt to eliminate the pernicious effects of the content. Mark Potok, senior intelligence agent at the Southern Poverty Law Centre, a civil rights practice specializing in countering hate groups (especially of the extreme right) in the USA puts this choice in a elegant public health based metaphor: either quarantine, or inoculate.

Quarantining

The idea that material judged to be terrorism related or radical can be effectively removed from the Internet is not dead. In the European Union, a new proposal is calling for further examination of the extent to which the hotline model, currently used for reporting child pornographic and sometimes extreme right material to ISPs for removal, can be usefully extended to this area. In Australia, a national filtering system is being tested that lists, among other things, terrorism related material.³² In the US, Senator Joseph Lieberman was responsible for successfully lobbying for an alteration of the acceptable use terms of the video sharing site YouTube.³³ Others have called for more radical solutions still, involving an international level treaty that would regulate content on the Internet, or for action at the level of the global domain name system to similar effect. Yet

³² Joshua Keating, 'The List: Look Who's Censoring the Internet Now.' *Foreign Policy* March, 2009.

³³ 'Lieberman to YouTube: 'Remove Al Qaeda Videos' CNN, 20/05/08.

others have suggested a more devious approach, involving, amongst other things, the use of 'cyberwar' techniques against terrorist material such as denial of service attacks or the disruptive use of malware.³⁴

In spite of this, there is a growing expert consensus that censorship of whichever variety is unlikely to be effective against terrorism related content. In particular, Ryan (2007) has pointed out that even the best filtering systems are both inaccurate and vulnerable to malicious subversion, while a recent United Nations report has cast doubt on the viability of a new instrument for the regulation of terrorist or radical content on the Internet. However, existing critiques of the viability of combating radical content through a strategy based on limiting access to it have tended to focus on the technical limitations to such a strategy, failing to emphasize that there are also reasons inherent to the way that terrorist propaganda content is actually disseminated which argue against the likely success of repressive tactics – at least within the limitations imposed by liberal-democratic frameworks.

Indeed, the discussion on the problems of countering radical/terrorist content on the Internet has tended to focus on what might be called the *international* problem of Internet governance. That is to say, the difficulty created by the fact that content which is illegal within a particular locality may well be perfectly legal elsewhere. This has stimulated a focus either on solutions based on local filtering systems, or on international agreements.

The tacit assumption behind such an approach is that terrorist propaganda content survives because it is hosted in places where it cannot be taken down; but this is, in fact, substantially not the case. It is true that much radical and terrorist content is hosted in the US (as is the majority of all material on the Internet). However, unlike extreme right wing content, which is now increasingly hosted on private servers where it shelters at the furthest extremity of the cover offered by the First Amendment to the US Constitution, this content is generally to be found on mainstream, commercial hosting companies. Such companies have a history of voluntarily removing such content when they are informed about it, as demonstrated by the work of Aaron Weisburd, a private researcher into Islamic radicalism on the Internet, who for a time specialized in doing just this, removing over a thousand sites in the process.³⁵ Indeed, radical material is frequently encountered in locations such as blog hosting, file hosting or video hosting sites where it is explicitly in contravention of publicly available acceptable use agreements. Getting such material removed is simply a matter of clicking on the appropriate button and informing the host. Indeed the proliferation of defunct sites and materials encountered by any researcher of radical and terrorist propaganda materials is eloquent testimony to the fact that such facilities are actually used.

The continued survival and proliferation of radical material on the World Wide Web is, then, not the result of an absence of will or ability to remove such content. Rather, it is due to the singularly robust qualities of digital material disseminated through the Internet. A useful example of this is presented by the radical Islamist forum 'Medad al-Suyuf'. According to 'Al Mihdar' a senior member, the 'companions' of the forum back the entire site up every day in anticipation of

³⁴ Weimann and Von Knop, op cit. p. 2.

³⁵ Correspondence with the author.

its being attacked or removed. Moreover, they maintain an email list of every member, which serves a dual purpose: on the one hand, it is used on a day to day basis as a means of sending fresh releases direct to interested parties. On the other, it serves as a means for keeping the community alive and informing it of any future change of venue for the main site. Indeed, this appears to reflect a strategy discussed during the last days of another radical forum, Al Hisbah, where, faced with attacks which had taken down the other major Al Qaeda forums, it was proposed that members network by email list, with a view to taking over any useful-looking Islamist forums they might encounter, without being entirely reliant for the survival of the community on any one forum's permanent existence.

A further interesting point raised by 'Al Mihdar' in response to ongoing concerns about intelligence infiltration of radical Islamist forums is his eminently realistic and sensible assessment that it happens, but it doesn't matter. Al Mihdar argues that creating closed forums as an attempt to prevent intelligence infiltration is ineffective and a recipe for petty factionalism. Rather, he advocates an open policy in which the community will focus on disseminating information freely regardless of whether some of those reading it are doing so for ulterior motives.

The evolution of this robust system (which in fact parallels still more sophisticated measures taken by still more heavily persecuted communities devoted to child pornography and Neo-Nazism) is a useful demonstration of why measures aimed at restricting the dissemination of content is probably a non-starter. The material survives not because it is not adequately policed, but simply because the demands, of the Internet, both technical and commercial make for a system in which gatekeeping always takes place after the event: in other words, after the horse has bolted.

Inoculating

Given widespread acceptance that restriction of radical material is not likely to be an effective strategy (at least on its own), another strategy that has been much promoted recently is that of 'counter-narrative': that is to say, using the Internet as a means of promoting alternative, positive messages. In contrast to censorship of the Internet, which is inevitably distasteful to analysts coming from a liberal perspective, the idea of 'harnessing the power of the Internet' to provide 'positive messages' has been trumpeted with almost uniform enthusiasm from policy-makers and experts alike. In this vein, Ryan³⁶ talks of the importance of empowering end users to engage extremists in dialogue; Stevens and Neumann (2009) advocate 'promoting positive messages' through 'an independent start up fund to provide seed money for online initiatives'; and Weimann and Knop discuss the usefulness of counter-narrative as a means of creating cultural and psychological 'noise'.

Unfortunately, such an approach is more attractive as a principle than as a practice. 'If you build it they will come' type approaches, in which governments help to finance websites devoted to views they would like to see put forward are likely to be costly failures – as is demonstrated by the failure of the UK Home Office backed 'Radical Middle Way' site to generate more than a few thousand hits a week. Worse, as the scholar of modern Islamic politics Olivier Roy points out,

³⁶ Johnny Ryan, *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* Institute of European and International Affairs, Dublin, 2007.

government backing for such views can be a kiss of death for any credibility that their proponents might have with the disaffected individuals at whom such campaigns are (rightly or wrongly) targeted.³⁷ Direct engagement in conversations on radical sites is most likely to result simply in ejection from these sites, as is elegantly illustrated by a conversation on the forum 'Islamic Awakening' in which a member laments having been promptly ejected from the Al Qaeda affiliate forum 'Al Ikhlas' after questioning Al Qaeda in Iraq's tendency to kill Muslim civilians. Another member informs him that it serves him right, and that the mujahidin must be sick of such questions.

Moreover, attempting to engage in Islamic dialogue may be a red herring in any case if, as scholars such as Roy suggest, Al Qaeda is actually better understood as a youth movement than as a religious grouping. As Roy points out:

To my knowledge, none of the arrested [al Qaeda] terrorists or suspects had Zawahiri or other books in their house, while they often have handbooks on how to make bombs or videos about 'atrocities' perpetrated against Muslims. Contrary for instance to the Hizb ut-Tahrir members, who always formulate their positions in elaborate ideological terms, Al Qaeda's members do not articulate before or after having been caught a political or an ideological stand (most of AQ suspects keep silent or deny any involvement during their trial, a very unusual attitude for political militants, who traditionally transform their trial into a political tribunal). We should certainly not discard entirely the fact that some quarters in Al Qaeda are writing or thinking in terms of ideology, but this does not seem to be the main motivation for joining Al Qaeda.³⁸

Indeed, many of the most militant of 'jihadi' cultural items available from the Internet are highly ideologically promiscuous, referencing in turns a heady mix of half understood Islamism, Arab nationalism, Salafism, the Nation of Islam, conspiracy theories of the left and the right and so on. The logic expressed is not that of a well-worked out theological justification for jihad as a *fardh 'ayn*, but rather a loose, but emotive sense that Muslims (as an imagined community more than as adherents to a highly specific creed) are under attack and must be defended. While there may be a narrative behind such beliefs, it is emotive rather than intellectual and therefore not necessarily accessible to argumentation.

An Offline Strategy Against Online 'Terrorist' Activity

The failure to build a coherent policy on terrorism on the Internet is based, arguably, on the fact that it has been built on two important fallacies. The first is the assumption that terrorism on the Internet is a problem in and of itself. The second is that because it is 'on' the Internet, the response to it must be as well. In fact, terrorist use of the Internet (however, defined) is a *terrorist* problem only when it leads to terrorism in real life. And in so far as material on the Internet might be a problem in its own right, it could be that there are other *offline* actions which would do more to counter it than anything governments could do online. Indeed, offline actions to counter online

³⁷ Olivier Roy, *Al Qaeda in the West as a Youth Movement: The Power of a Narrative*, Microcon Policy Working Paper, November 2008.

³⁸ Op cit. previous page.

problems may often hold more promise for the simple reason that they enable government to act where its power is strongest – namely, over matter and physical space rather than where it is most open to being contested, that is to say, in the domain of ideas.

To begin with one very specific example of what this might mean, consider the alleged role of Google Earth in the November 2008 attacks in Mumbai. Whether Google Earth was in fact used is not known – the dossier of evidence produced by the Indian government³⁹ concerning the attacks confirms the use of GPS devices (which might be seen as related, in a wider sense to ‘cyberspace’). For the sake of argument, however, let us assume that Google Earth was used.

This example is a useful test case, since the Internet material in question, though beneficial to terrorists, is clearly innocent. Admittedly, according to an article in the (London) *Times*⁴⁰ an Indian court did actually consider outlawing the service in India (another story from around the same time claimed that an Indian company was planning a more detailed and up to date version of the same service specifically for India). However, how such a measure would have prevented terrorists, who started their journey in *Pakistan*, from using it in their planning is difficult to understand. Nor would a more limited service be possible. Google Earth has, at request, removed sensitive military locations from the images it provides. Although, the terrorists in this instance did not (as terrorists customarily do not) attack such a location. Terrorist targets are precisely the same type of civilian locations which a service such as Google Earth can hardly avoid covering.

Therefore, in this instance, removing material from the Internet is clearly not a solution. Nor, indeed, is any type of activity that might realistically be carried out on the Internet. What, then, is? According to Google’s geo-location services manager, Rob Painter, the satellite images used by Google are a year old (which incidentally makes them, as he points out, 364 times more compliant with US law than they need to be, since government mandates exclusive access to the data only for its first 24 hours after capture). Consequently, one obvious counterstrategy is simply to move potential targets often enough to ensure that the information is out of date. While this advice is clearly more applicable to, for example, military formations than it is to city centers, it is not necessarily completely irrelevant to the case at issue. Newman and Clark,⁴¹ for example, advocate regular changes to physical space, such as changing the names and signs of popular cafés, as one way of rendering them less vulnerable to suicide bombers who may be unfamiliar with the terrain and dependent on a set route.

A related approach might be to plan counter-terrorist responses around the assumption of an opponent well supplied with certain types of general geographical data, but without other types of more specific topographical information. Targets could be hardened, for example, or traps sprung in places identified as likely to look tempting to an attacker with a bird’s eye view.

These are not comprehensive suggestions. The idea is, rather, to suggest an alternative state of mind that might be brought to thinking about threats emanating from the Internet. The key point

³⁹ Dossier available from <http://www.nefafoundation.org/documents>.

⁴⁰ Rhys Blakely ‘Indian court asked to ban Google Earth’ *The Times* (London) 10/12/08 http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5314085.ece.

⁴¹ Ronald V. Clarke and Graeme R. Newman, *Outsmarting the Terrorists* Praeger Security International, Westport, Connecticut, p. 93.

being made in the example above is this: while a government may be almost powerless to affect a certain activity happening online, it may well retain an overwhelming advantage in another area which, if denied to terrorists, would render their online advantage irrelevant. By choosing to have the confrontation on the Internet, governments are denying themselves the right to take the initiative and confront the enemy on territory where they enjoy an advantage.

This approach is not new. In fact, it corresponds closely with historical experiences of confrontations between heavy, hierarchical, industrialized forces and lighter, more maneuverable opponents. To take one example, in *Making Sense of War: Strategy for 21st Century* Alan Stephens and Nicola Baker⁴² point to the example of how General Ulysses S. Grant was able to win the American Civil War for the Union, following a series of disastrous defeats at the hands of a Confederacy inferior in men and material, but superior in the tactical abilities of its leadership. Grant's strategy was to 'never maneuver'. Rather than try to defeat the enemy at their own game, he simply concentrated on grinding them down. This is not, of course, to suggest that a brutal emphasis on physical force is in any way appropriate for a 'virtual' or 'information' war on a sometimes almost metaphysical adversary. Rather, the point is that, like the Northern Union in the civil war, governments' greatest comparative advantage *viz à viz* amorphous ideational networks lies precisely in their superior *weight*.

From the point of view of Western democracies, the most important issue in terms of terrorism and the Internet appears to be its role in supporting the type of leaderless political violence which Raffaello Pantucci identifies as that advocated by the jihadi strategic thinker Abu Mus'ab al-Suri.⁴³ This suggests a model of terrorist activity in which individually inspired groups of activists, unknown to each other but sharing a common agenda spontaneously engage in acts of violence against a commonly agreed on enemy.

One obvious weakness of this model is that, while it may create plenty of enthusiastic volunteers, it is less good at providing people with the necessary tradecraft and military skills necessary to translate this fervor into effective terrorist action. This is amply evidenced by the number of botched operations carried out by 'leaderless jihadis' and their equivalents from different ideological spectra.⁴⁴ These could include the failed bombing attempts in London on 21 July (which Kohlmann observes differed to the 7/7 bombings, which benefited from some formal training camp experience) 'only in the quality of their explosives'; the equally unsuccessful attempts by Bilal Abdullah and Kafeel Ahmed on Glasgow Airport, and the failed nail bombing on 'The Giraffe' restaurant in Exeter.

⁴² Alan Stephens and Nicola Baker, *Making Sense of War: Strategy for the 21st Century* Cambridge University Press: Cambridge; New York, 2006, pp. 71-72.

⁴³ Raffaello Pantucci, 'Operation Praline: The Realisation of Al-Suri's Nizam, la Tanzim?' *Perspectives on Terrorism* Vol 2, No 12.

⁴⁴ Marc Sageman, *Leaderless Jihad: Terror Networks in the 21st Century* Pennsylvania State University Press, Philadelphia, 2008.

In explanation of this, Sageman observes, following the work of Michael Kenney⁴⁵ on organizational learning by criminal and terrorist networks, that there are certain skills (such as bomb making) which cannot be learned simply through acquiring theoretical technical knowledge (which Kenney calls *techne*). There must also be a more abstract type of know-how gained by practical experience (*metis* in Kenney's terminology).

While governments may, then, have limited powers to prevent individuals from acquiring the necessary *techne* for bomb making (and indeed other types of operation), there may be a great deal that can be done to prevent the acquisition of *metis*. Indeed, at least in a UK context, it is fair to say that significant measures in this regard have already been taken. For example, the 2006 Terrorism Act contains explicit provisions against training for terrorism and attendance at a place used for terrorist training. At the same time, the establishment of a hotline to report terrorist activity has led, at times, to useful information on the construction of explosives.

It is also possible, however, that other, relatively subtle measures might be useful in denying would-be-terrorists the opportunity to hone their skills. For example, in the UK context, it is interesting that the one relatively successful example of 'leaderless' terrorism based on information downloaded from the Internet was carried out not by a 'jihadi', but rather by David Copeland, an individual with neo-Nazi sympathies. Copeland reportedly practiced his bomb making skills late at night on his local Hampshire common. Hence, his success in contrast to jihadi terrorists is conceivably related to the generally urban background of proponents of this ideological tendency, which may limit the opportunities of the latter to hone their skills. It would follow that measures which would deny empty rural spaces to would-be terrorists – even through means as innocuous as promoting greater recreational use of such areas could, potentially, have knock-on effects in terms of preventing terrorism. At the same time, this observation emphasizes the relevance of attempts, whether political or military, to reduce the physical availability of training facilities in other parts of the world.

The 'War of Ideas'

Measures to reduce access of would-be terrorists to physical opportunities for developing necessary skills are sensible enough, but may be seen as a complacent retreat from the wider issue of countering the (in a broad sense) ideological narratives that are seen as sustaining continued involvement in terrorist violence. In fact, conspicuous and humiliating failures (and, in the case of Kafeel Ahmed, agonizing and protracted death) may well be more effective in discouraging involvement than any amount of government counterpropaganda. However, there may also be ways in which a de-emphasising of the importance of Internet 'space' may provide potentially interesting avenues for countering the rise of radical ideas as well.

Firstly, a concept of there being an Internet space dominated by terrorists invites a distorted perspective on the actual state of play in what is sometimes termed the 'war of ideas'. Comparing Al Qaeda with, say, NATO on the Internet and then asking who is winning is simply a meaningless comparison if we accept that by 'Al Qaeda' we mean something like 'any sort of

⁴⁵ Michael Kenney *From Pablo to Osama Trafficking and Terrorist Networks, Government Bureaucracies and Competitive Adaptation*, Pennsylvania State University Press, Philadelphia, 2007.

concept relating to jihad as a violent activity and the applicability of this interpretation to contemporary contexts and the lives of individuals'. Even if we take a narrower understanding of 'Al Qaeda' – say, only the official 'Islamic Media Foundations' charged with dissemination the productions of the organization and its affiliates, then the best comparison, given its all-embracing anti-Western, anti-secular state agenda would not be with any given military or political entity, but with media giants such as Al-Jazeera or even Reuters.

Moreover, despite the growing difficulties of monetizing traditional news sources, the Internet is ironically making such traditional, corporate sources of news more important than ever. This is because, while the Internet does much to transmit news, it does not generally supplant its original sources. So, paradoxically, while fewer people than ever may buy newspapers or watch television news, they remain at least as dependent as ever on conventional sources at second or third remove. In fact, as Paterson has demonstrated, far from providing a cornucopia of media diversity, the overwhelming majority of Internet use actually derives from either the Associated Press, or Reuters. The Internet offers almost unlimited possibilities for collation, discussion and analysis of news material, but physical limits on the actual creation of news still remain, providing an effective potential lever for governments seeking to influence agendas.

All of this suggests that the traditional agenda-setting power of governments has not been removed by the Internet. Indeed, if anything, discussion of government actions on the Internet, as reported by traditional news sources, has the potential to greatly amplify their apparent import. In media terms, government, as Nacos⁴⁶ has demonstrated, *is* the story. Government achieves this informational superiority, like terrorists, through propaganda of the deed. But as theorists such as Chomsky⁴⁷ have wryly observed, this state power over media agenda is, paradoxically, reliant on the perception of media independence. By trying to write the story as well it undermines its credibility. This, in fact, is a principle which appears to have been tacitly accepted by RICU – a trilateral UK initiative which aims to counter Al Qaeda and global jihadism by means of press releases submitted to independent media. The premise is, so it seems, that by means of this sort of filter, a measure of credibility can be retained: the stories must in the first place be good enough to report. Ultimately, mass media management may be as effective a tool for governments on the Internet as anywhere else.

Indeed, jihadist media is frequently reactive in tone. This is particularly true in relation to English language content, where sites such as jihadunspun are premised on the familiarity of their audience with an 'official' account produced by mainstream media.⁴⁸ On English language forums with a militant bent, such as the politics, jihad and current affairs section of 'Islamic Awakening', official productions of Al Qaeda are much less common than conspiracy theories cobbled together from English language books and media sources. By directly intervening in these discussions, the

⁴⁶ Brigitte Nacos, *Terrorism and the Media: From the Iran Hostage Crisis to the World Trade Center Bombing* Columbia University Press, New York, 1994.

⁴⁷ Noam Chomsky, *Necessary Illusions: Thought Control in Democratic Societies* South End Press, Boston MA, 1989.

⁴⁸ See Akil Awan 'Virtual Jihadist Media: Function, Legitimacy and Radicalizing Effectiveness' *European Journal of Cultural Studies* Vol 10, No 3 pp. 389-408, 2007, also Akil Awan 'Radicalisation on the Internet?' in the RUSI Journal Vol 152 No 3, pp. 76-81, 2007.

risk is that government, far from taking the initiative, actually hands it to the very extremists it hopes to counter. Moreover, it is worth remembering that a core fact underlying the compelling nature of jihadist media is the very physical limit on the production of digital content just observed. Terrorists and militants have, over their counterparts, the crucial edge that they are actually doing, and through their documentation of this fact have, ipso facto mastery at source of compelling new material. Rather than seeking to counter this through rational or ideological argumentation further down the line, one approach might be for governments to provide the local victims of groups such as the Taliban with the physical means to document their own suffering.

The Physicality of ‘Cyberterrorists’

A final point to bear in mind may be that people do not leave their bodies behind when they go online. This simple observation is emphasized by Stevens and Neumann⁴⁹ in their recommendation that physical arrests are probably a more powerful tool in countering online incitement to violence than are attempts to remove content from the Internet. However, there may be subtler ramifications to the point as well. According to Keith Verrells, an investigator in the case of the ‘cyberjihadi’ and propagandist Younis Tsouli, this individual demonstrated behavior which, while not clinically diagnosed, appears to be a plausible case of Internet addiction. On his arrest, Tsouli’s parents expressed incredulity at their son’s activities, not believing that it was possible to commit the crimes he was accused of while sitting at a computer. Regardless of any political views concerning the appropriateness or otherwise of certain types of Internet activity, it might be suggested that a more proactive approach to the physical problem of computer dependence may be relevant to disrupting this sort of activity in the early stages of its development. In an opposite case, Tsouli’s co-conspirator Tariq al-Daour was, apparently, responsible for a number of physical assaults on Orthodox Jews. Again, a focus on physical activity in this instance might have served to disrupt the development of an individual who was later convicted for what was considered to be a significant role in terrorist activity.

Conclusion

Misunderstandings and misconceptualizations of the relationship between terrorism and the Internet, and of the way the Internet works, have the potential to draw governments into a ‘conflict’ which they cannot possibly win, and in which they have a significant amount of credibility to lose. By recognizing the limitations of the Internet as a tool for terrorism, and by a nuanced appreciation of what it does offer, governments stand a much better chance of countering threats which do emerge from it. In practice, much that is relevant to countering the worst implications of the Internet for terrorism is already being done. However, it is not being recognized and appreciated as such. Better appreciation of how offline measures may impact on a threat considered ‘online’ may lead to the evolution of further measures that may be effectively applied by governments.

⁴⁹ Op cit. p.1

BIBLIOGRAPHY

- Arquilla, John and David Ronfeldt, 'Cyberwar is coming!' in John Arquilla and David Ronfeldt (eds) *In Athena's Camp: Preparing for Conflict in the Information Age* RAND, Santa Monica.
- Awan, Akil, "Al Qa'ida's Virtual Crisis," *The RUSI Journal*, Vol 154, 1, 2009.
- 'Radicalization on the Internet?' *The RUSI Journal* Vol 152, No 3, 2007 pp. 76-81.
- 'Virtual Jihadist Media: Function, Legitimacy and Radicalizing Effectiveness' *European Journal of Cultural Studies* Vol 10, No 3 pp. 389-408, 2007.
- 'Radicalisation on the Internet?' *The RUSI Journal* Vol 152 No 3, pp. 76-81, 2007.
- Blakely, Rhys, 'Indian court asked to ban Google Earth' *The Times* (London) 10/12/08 http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article5314085.ece.
- Brachman, Jarret M., *Global Jihadism: Theory and Practice* Routledge, Abingdon (Oxon) 2009.
- Broach, Anne, 'Terrorists voice alarm over terrorist Net presence' CNET News May, 3, 2007 available at http://news.cnet.com/Senators-voice-alarm-over-terrorist-Net-presence/2100-1028_3-6181269.html.
- Chomsky, Noam, *Necessary Illusions: Thought Control in Democratic Societies* South End Press, Boston MA, 1989.
- Clarke, Ronald V. and Graeme R. Newman, *Outsmarting the Terrorists* Praeger Security International, Westport, Connecticut.
- Coolsaet, Rik and Teun Ven De Voorde, 'The Evolution of Terrorism in 2005: A Statistical Assessment' *Special Report*, University of Ghent, 2006.
- Conway, Maura 'Terrorist "Use of the Internet, and Fighting Back' International Relations and Security Network, 2006 available at <http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=20642>.
- 'Mass Communicaton - from Nitro to the Net,' *The World Today* Vol 60 No 8/9 pp. 19-22.
- Denning, Dorothy, 'The Jihadi Cyberterror Threat', powerpoint presentation from SUMIT 07, 2007.
- 'Is Cyber Terror Next?' SSRC essays, 2001 available at <http://www.ssrc.org/sept11/essays/denning.htm>.
- 'Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' in Arquilla and Ronfeldt (eds) *Networks and Netwars: The Future of War, Crime and Militancy* RAND, Santa Monica, 2001 pp. 239-288.
- Gies, Lieve, 'How Material are Cyberbodies? Broadband Internet and Embodied Subjectivity' *Crime, Media, Culture* Vol 4, No 3, 2008 pp. 311-330.

- Gupta, Dipak K., 'Towards an Integrated Behavioural Framework for Analysing Terrorism: Individual Motivations to Group Dynamics' Paper presented at the annual meeting of the International Studies Association, San Diego, California 22/03/06.
- Keating, Joshua, 'The List: Look Who's Censoring the Internet Now.' *Foreign Policy*, March, 2009.
- Kenney, Michael, *From Pablo to Osama Trafficking and Terrorist Networks, Government Bureaucracies and Competitive Adaptation*, Pennsylvania State University Press, Philadelphia, 2007.
- Manovich, Lev, *The Language of New Media* MIT Press, Cambridge, Massachusetts, 2002.
- Nacos, Brigitte, *Terrorism and the Media: From the Iran Hostage Crisis to the World Trade Center Bombing*, Columbia University Press, New York, 1994.
- Pantucci, Raffaello, 'Operation Praline: The Realisation of Al-Suri's Nizam, la Tanzim?' *Perspectives on Terrorism* Vol 2, No 12.
- Rheingold, Howard, *The Virtual Community: Homesteading on the Electronic Frontier*, Addison Wesley Publishing, Reading (Massachusetts), 1993.
- Roy, Olivier, *Al Qaeda in the West as a Youth Movement: The Power of a Narrative*, Microcon Policy Working Paper, November 2008.
- Ryan, Johnny, *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* Institute of European and International Affairs, Dublin, 2007.
- Sageman, Marc, *Leaderless Jihad: Terror Networks in the 21st Century* Pennsylvania State University Press, Philadelphia, 2008.
- Schmid, Alex and Janny de Graaf, *Violence as Communication: Insurgent Terrorism and the Western News Media*, London, Sage 1982.
- Schwartz, Winn, *Terminal Compromise*, Interfact Press, New York, 1991.
- Sieber, Ulrich, *Cyberterrorism: The Use of the Internet for Terrorist Purposes*, Council of Europe Report, 2007.
- Silke, Andrew, 'The Fire of Iolus: The Role of State Counter-Measures in Causing Terrorism, and What Needs to be Done' in Tore Bjorgo (ed) *Root Causes of Terrorism: Myths, Reality and Ways Forward* Routledge, London, 2005, pp. 524-621.
- Stephens, Alan and Nicola Baker, *Making Sense of War: Strategy for the 21st Century* Cambridge University Press: Cambridge; New York, 2006, pp. 71-72.
- Stevens, Tim and Peter Neumann, *Countering Online Radicalisation, A Strategy for Action* International Centre for the Study of Radicalisation and Political Violence, London, 2009.
- Swann, Steve, 'Aabid Khan and his Global Jihad' 18th August 2008 available at <http://news.bbc.co.uk/1/hi/uk/7549447.stm>.
- Swedlund, Eric, 'UA effort sifting web for terror threat data' *Arizona Daily Star* 24/09/2007.

Thomas, Timothy, Lt Col., 'Al Qaeda and the Internet: The Danger of "Cyberplanning"', *Parameters*, Spring 2003, pp. 112-123.

Weimann, Gabriel, 'www.terror.net: how modern terrorism uses the Internet' Special Report, United States Institute of Peace, 2006 <http://www.usip.org/pubs/specialreports/sr116.html>.

— 'The Psychology of Mass-Mediated Terrorism' *American Behavioural Scientist* Vol 52, No 1, 2008 pp. 69-86.

Weimann, Gabriel and Katherina Von Knop 'Applying the Notion of Noise to Countering Online Terrorism', *Studies in Conflict and Terrorism* Vol 31, No 10, pp. 883-902.

Weimann, Gabriel and Yariv Tsfati 'www.terrorism.com: terror on the Internet' *Studies in Conflict and Terrorism* Vol 25, 317-332, 2002, 317-332.