Conceptualising Online Terrorism

By Gilbert Ramsay

Recent years have seen a rapid growth in interest in the relationship between terrorism and the Internet. But despite—or perhaps because of—the perceived immediacy and urgency of the problem, research into 'terrorist use of the Internet' or 'terror on the Internet' has tended to take a 'hands-on approach', dealing only quite peremptorily with conceptual and definitional issues. This is, perhaps, understandable because terrorism and the Internet are renowned for being two of the most slippery subjects in social science. While the inability of scholars to adequately define terrorism is well-known and doubtless more than familiar to most readers, it is also worth quoting James T. Costigan, who said, 'I am not sure I know what the Internet is. I am not sure that anyone does.' [1] Nonetheless, without useful definitions of what is meant by 'terrorist use of the Internet' or 'terror on the Internet', there is a danger of studies treating 'terrorism' in such a loose sense as to devalue the meaning of the word.

In this paper, I will explore how the relationship between terrorism and the Internet has been understood to date. I will try to show that if 'terrorism' is to remain a useful concept in Internet research, careful thought is needed about where exactly it can and cannot apply. To some extent, the very looseness of both terms is the fundamental problem I will address. However, in practice, I will make things easier for myself in two ways. First, I will make no attempt to reopen the interminable search for a satisfactory definition of the word terrorism. Wherever I use the term, I will try to use it in a sense which is sufficiently open to incorporate a wide range of existing scholarly definitions. I make only one real assumption, which is that terrorism entails the use of force of some kind, or at least a strategy based around applying it. Second, I will not define what I mean by 'the Internet' beyond saying this: although I use the term 'Internet', most of what follows will not strictly concern the Internet as a whole so much as the World Wide Web, a term which can be defined quite satisfactorily as 'all the resources and users on the Internet that are using the Hypertext Transfer Protocol'. [2]

The earliest interest in a connection between terrorism and the Internet centered around the feared possibility of cyber-terrorism, with technology writers such as Winn Schwartau popularising the idea of hackers launching a devastating 'electronic Pearl Harbour.' [3] Throughout the mid-nineties (and beyond) a substantial amount of literature emerged which discussed this possibility and ultimately began to be taken seriously by heavyweight terrorism writers—notably Walter Laqueur, who included a chapter on cyber-terrorism at the end of his book, *The New Terrorism*. [4]

Despite the near apocalyptic pronouncements of some writers, and the dedicated efforts of some terrorist organisations (notably the Tamil Tigers), no single unambiguous case of cyber-terrorism has yet occurred. Indeed, with the events of Sept. 11, it began to appear that expectations of a super-high-tech attack on the United States (or anywhere else) were misplaced because Al Qaeda had not used advanced or futuristic methods. Rather, it had

made innovative use of tried and tested tactics in the terrorist arsenal. 9/11 was not a technological coup, but an organisational one. [5]

Partly for this reason, there was a significant growth after 2001 in articles that looked at how terrorists might use the Internet not as a medium for a cyber-attack, but rather, as former White House cyber security Chief Richard Clarke put it, 'just like everybody else.' [6] Although conventional use of the Internet by terrorists may appear to be something only tenuously connected to cyber-terrorism, an examination of the literature reveals that in fact, to a great extent, the one grew out of the other. The earliest academic (and semi-academic) literature on terrorist use of the Internet is by experts on online security, and indeed comes in the context of articles on that subject, e.g., Hayward, Furnell and Warren, Cohen and Denning. [7], [8], [9], [10]. Only later did scholars begin to treat the issue from a non-technical perspective, and even these felt the need to address the cyber-terrorism issue apologetically. (E.g. Thomas, Weimann, Conway). [11], [12], [13].

The bridging concept between cyber-terrorism and terrorist use of the Internet was that of information war. This umbrella doctrine covers a highly heterogeneous range of possible strategies, and it has been said by one expert that 'the concept has as much analytic coherence as that of, say, "information worker". [14] The approach of researchers into terrorist use of the Internet has therefore been a broad one, though focused in the one instance on the creation of a wide variety of possible typologies for terrorist uses of the medium.

These typologies, as early attempts to get to grips with the subject, are understandable. But without genuinely coherent higher order concepts to group them together or establish appropriate methodologies for studying them, they verged on the trivial. Terms such as 'data mining' and 'information sharing' sound important, but when they are reduced to 'looking at pages on the Web' and 'sending e-mails', they are revealed to be not only theoretically obvious, but for all practical purposes, completely disparate activities. Perhaps reference to offline analogues of these activities will make the point obvious. Terrorists can potentially 'mine' valuable information from public libraries and can 'share information' using the phone system. The solution to the first problem (if it is sufficiently severe) is to remove sensitive information from the public domain. The solution to the second may be to tap the calls of suspected terrorists. Both of these have fairly precise online equivalents, but one hardly needs to incorporate the two into an integrated strategy for dealing with, as one article is titled, 'terrorist use of information operations'. [15]

Attempts to analyse 'terrorist use of the Internet', therefore, have the potential to hinder rather than clarify the analysis, particularly when they advocate the reification of the medium and try to transform what are really only problems of degree into dramatically new issues. They are potentially useful, however, when they deal with outcomes of the Internet which are both genuinely new and sufficiently interconnected to suggest that they merit examination from single perspective. A particularly good example of this is the terrorist Web site. Although terrorist groups have been attempting to produce and

disseminate their own propaganda at least since the late nineteenth century, they have generally not been very successful at it. Indeed, the need to coerce free publicity from the institutional mass media has widely been understood as central to the very nature of modern terrorism. With the invention of the World Wide Web, however, terrorists have heightened their ability to engage in self-publicity.

Terrorist Web sites, therefore, represent a valuable area of study, and indeed much of the best work on terrorist use of the Internet has been devoted to analysing their content. Both Weimann and Tsfati, Conway, and Chen (et al) [16], [17], [18] have written important contributions based on a similar premise, first using a list of terrorist organisations (Weimann and Tsfati and Conway use the U.S State Department's official list of foreign terrorist organisations. Chen's Web-crawling project, the Dark Web Portal, uses a list based on the recommendations of a variety of different bodies) to identify a sample of 'terrorist' web sites, and then employing systematic content analysis techniques to examine them.

Despite the value of this approach, it has, however, one major drawback. It is only really methodologically coherent when it is applied to study of the 'official' Web sites of terrorist groups. It is useful for analysing conventional terrorist organisations, whose online propaganda tends to focus on a relatively small number of carefully maintained, closely controlled websites, e.g., FARC, the PKK, the LTTE, Hezbollah, Hamas, Mujahedin-e-Khalq. Unfortunately, it is less successful as a method for analysing the main growth area in terrorist use of the Internet—that is to say, the sprawling mass of ideological material relating to Al Qaeda or, to give it its less snappy title, 'the global salafi jihad'.

The reason for this relates to the fact, touched on by Marc Sageman in his latest book, *Leaderless Jihad*, that as far as Al Qaeda is concerned, Web sites as a unit of analysis are relatively unimportant. [19] Al Qaeda's sites, as Weimann has observed, tend to appear and disappear with remarkable frequency. [20] In fact, this understates the case. Al Qaeda's sites are, in the great majority of cases, small, amateurish affairs. Frequently, they are no more than readymade commercial sitelets, hosted by larger commercial u-site operations such as Angelfire, freewebs, or their Arabic equivalents egysite and jeeran.com. Often these sites are, in turn, little more than collections of links to other sites. Finally, of course, there are the jihadist forums, which remove the issue still further from the deliberately constructed propaganda Web site by providing a venue for individual postings, often accompanied by a standardised disclaimer by the administrators of the site, denying responsibility for content posted by individual forum members.

Methodologies for analysing terrorism on the Internet, originally devised with the official terrorist propaganda site in mind, are stretched to a conceptual breaking point in this online environment. This much is revealed by a careful examination of the methodological passages in Weimann's *Terror on the Internet: The New Arena, The New Challenges.* Weimann describes how most of the material for his book derives from a 'thorough and extensive scan' of the Internet. In fact, he describes two studies: 'eight

years of monitoring and archiving terrorists' websites (1998-2005)' and how 'for the purposes of this book, the Internet was scanned again in 2003-05. The target population for the current study was defined as "the Internet sites of terrorist movements as they appeared in the period between January 1998 and May 2005"'. This scan, so Weimann claims, succeeded in locating 4,300 sites 'serving terrorists and their supporters'. And this is contrasted with the fact that in 1998 fewer than half of the thirty organizations designated as foreign terrorist organizations by the U.S department of state maintained websites'. [21, 22, 23, 24, 25]

Despite the apparent thoroughness of this approach, a number of ambiguities emerge under closer examination. First, why is it that, for his second scan, and for the purposes of his book, Weimann seemingly shifted his definition from simply Web sites of groups appearing on the U.S Department of State list to the much wider categories of terrorist 'movements' and sites 'serving terrorists and their supporters'? These categories, in contrast to those used for his earlier published work on the subject, are loose and left undefined. What is a 'terrorist movement', for example? And where does one draw the line on a site 'serving terrorists and their supporters?'

This whole, subtle shift of approach makes sense when one considers Weimann's claim that 'our findings reveal a proliferation of radical Islamic web sites'. [26] But even though Weimann is at pains to assert that 'this is not a methodological bias, but rather a significant trend highlighted in our study', it is hard not to wonder if he protests too much. Despite this claim, Weimann never says where he draws the line. There are innumerable Islamic Web sites which in some sense 'serve terrorists and their supporters'. Even Islamist organizations, which are not in themselves violent, are highly likely to consider the terrorism of Hamas or Hezbollah to be legitimate. And there are plenty of Web sites broadly dedicated to Islamic theology which, nonetheless, provide material viewed favourably by jihadists. And what is to be made of the fact that large amounts of jihadist material is available on sites which are not intentionally 'terrorist' at all. For example, large amounts of material has actually been found on the hard drive of at least one suspected terrorist from YouTube, archive.org, and even, ironically, counterterrorist sites such as siteinstitute.org. [27]

But while Weimann's predicament is understandable, his solution is inadequate. Expanding the definition from the Web sites of 'terrorists' to include those of 'supporters' is more than just an expansion of his definition, but a complete undermining of it. For while 'terrorist' is at least in principle an objective category, based on a particular category of behaviour, 'sympathisers' are self-defined. This means that, if only for cataloguing purposes, examples of 'terrorist' and 'sympathetic' material are fundamentally different. As Weimann himself has observed, the official Web sites of terrorist organizations are often far from open about the violent activities of their sponsors. Such content is 'terrorist' to the extent that it can be determined to originate with known terrorists. By contrast, sympathetic material must be identified through characteristics intrinsic to the material itself.

This suggests that actor-centered, Web site-based approaches to identifying terrorist content online as exemplified by the work of Weimann, Conway and (to some extent) Chen cannot on their own serve as a conceptual framework for talking about the phenomenon of Al Qaeda or jihadist use of the Internet. Such material, so it would seem, to the extent that it is 'terrorist', must be identified as such, and not through assumptions about the organization behind a particular Web site, but through intrinsic characteristics of the material itself. This presents an apparent paradox. Terrorism is necessarily a form of action—even if it is action in order to send a message. The Internet, by contrast, is almost its perfect opposite: a textually constructed world in which speech acts are the only deeds. As Rheingold has observed, one great advantage of the Internet for the frank exchange of ideas is the very fact that, online, no one can punch you in the nose. [28]

Nonetheless, a great deal of online content can be identified as 'terrorist use of the Internet' more easily than might be supposed. Indeed, it is arguably the case that as Al Qaeda has shifted away from the Web site as basic unit for its online propaganda, its material has become more distinctively labeled. Interestingly, this is, in essence, a fairly precise social network equivalent of the technological approach that lies behind the Internet itself. In order to create a communications system robust enough to survive a nuclear attack, the U.S. Department of Defense's Defense Advanced Research Projects Agency (DARPA) adopted a 'packet switched' approach. This entailed moving from a system reliant on particular lines of communication and instead using 'packets', with each 'packet' containing its own built-in information about its intended destination. These packets could then move freely through any available channel in the network.

Through contrasting Al Qaeda's use of the Internet with other terrorist organizations, an official Web site can be regarded as a single channel of communication with an audience. It has the advantage of being direct, but is also extremely vulnerable because, if compromised, it would be difficult to restore communication with its audience. On the other hand, when a message is encoded as standalone communications, e.g. videos, lectures, etc., it has much greater resilience. Even if any number of Web sites are infiltrated, the message itself will almost certainly survive. This means that to serve as effective propaganda, the message must contain within itself information about its origin. This helps account for the existence of branded jihadist news agencies such as Al-Sahab, Al-Fajr, and the Global Islamic Media Front, whose propaganda videos, though they crop up in all sorts of locations, are immediately recognizable because of the use of distinctive logos and house styles.

While this may be true for material deriving from 'core' Al Qaeda and from its more functional affiliates (e.g., in Iraq or the Islamic Maghreb), for other types of content, in particular ideological material and material related to 'jihadist preparation', subtler justifications are required. These may be supplied to some extent, however, through the concept of radicalization. Indeed, it is on this basis that several jurisdictions have begun to construct legal frameworks aimed at outlawing certain kinds of 'terrorist' content. A good example of this approach can be seen in the UK's Terrorism Act 2006, which defines an item as a 'terrorist publication' if matter contained in it is likely:

> (a) to be understood, by some or all of the persons to whom it is or may become

> available as a consequence of that conduct, as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism; or
>
> (b) to be useful in the commission or preparation of such acts and to be understood, by some or all of those persons, as contained in the publication, or made available to them, wholly or mainly for the purpose of being so useful to them. [29]

While this approach may or may not have legal and political value, it exhibits some important weaknesses from an academic point of view. First, it relies heavily on access to contextual information that is, in fact, extrinsic to the material. Assessing whether a document is 'understood by some or all people' to have a certain function requires knowledge of more than just the document itself. Indeed, it might be argued that the clauses above are actually even more sweeping with regard to the issue of context than it perhaps prudent. After all, a book such as Sayyid Qutb's *Milestones*, despite having unambiguously pro-jihad and takfiri content, is only a direct incitement to violence if it is given to someone on the understanding that it be understood and used in that light. In fact, the text is available not only in secular libraries but also online from apparently quite moderate Islamic sites. The same can even be said of 'preparation' material.

To take a mild example, it is not unusual for jihadist sites to link to martial arts or fitness training material in Arabic which has nothing to do with jihad in its own right. Even with regard to harder-core material, like information on how to make bombs or poisons, the Internet is awash with anarchists' cookbooks of no particular ideological stance other than perhaps a certain colourless libertarianism. It might be argued that such material is usually of dubious value, but the same could be said of many of the explosive recipes circulating on jihadist forums, some of which appear to have been translated from English and perhaps derive from exactly these sources. This all relates, in turn, to another, perhaps deeper reason for why content-based approaches to defining terrorism on the Internet are problematic, in that if content-based criteria are used as the basis on which to select material in the first place, this fact is likely to bias any subsequent content analysis that might be performed on the material.

To make sense of terrorist content online then, it is necessary to anchor it in some sort of context. Because online material cannot often be associated with any specific author, it is necessary that this context also be found online. In theory, this sounds implausible, but in fact almost exactly such a context exists in the 'online communities' that base themselves around what can be regarded as the new central focus of 'al Qaeda' on the Internet: the jihadist forum. This observation is scarcely original. In fact, 'jihadism' and 'terrorism' have, in point of fact, increasingly become virtually interchangeable terms, particularly with relation to online material. Recent reports such as the one written by Johnny Ryan for the Institute of European Affairs [30] eschews the word 'terrorist' altogether. On its current Web site, Chen's Dark Web Portal at the University of Arizona, which has gone to great lengths to find a scientific way of identifying a 'terrorist' Web site, now describes itself in the following way:

> 'The AI Lab Dark Web project is a long-term scientific research program that aims

> to study and understand the international terrorism (Jihadist) phenomena via a computational, data-centric approach.' [31]

In fact, the focus on jihadism as an ideology with its attendant online community as opposed to terrorism as a course of action reflects the effective rout of 'terrorism' as a useful concept in ordering understanding a category of online material. The security focused literature on 'terrorist use of the Internet' which as I have suggested, traces its roots back to grand concepts of cyber war and information war has been quietly routed almost at the very instance of its fullest flourishing. In its place, an approach has been adopted which, because it seeks to understand the phenomenon in terms of online communities of interest, is far closer to the mainstream of Internet studies.

Can the concept of 'terrorism' be rehabilitated as a guiding concept for studies of online material? If there is any place for it, it will be necessary to demonstrate that there exist 'communities' or 'cultures' online for which the inspiration of terroristic violence is so central to their purpose that they are, to all intents and purposes, directly linked to the carrying out of terrorist acts. This is, interestingly, actually quite a good description of 'jihadism', an Arabic neologism which is dedicated to the elevation of a particular militant component of certain political Islamic ideologies into virtually a means to an end. Indeed, my own studies in jihadism online appear to suggest the possibility that inbuilt characteristics of the online environment previously theorised by 'cyber-sceptics' such as Beniger, [32] Jones [33] and Stoll [34] are helping to create a truncated online community in which Internet users who may, in their own lives, subscribe to more complete and diverse versions of Islamic fundamentalism congregate online around a common interest in, specifically, violence. If so, then perhaps looking for terrorism on the Internet may not be so paradoxical after all.

Mr. Ramsay is completing his PhD in terrorist uses of the Internet and the Centre for the Study of Terrorism and Political Violence, University of St Andrews, Scotland.

Notes

[1] James Costigan 'Introduction: Forests, Trees and Internet Research' in Steve Jones ed. *Doing Internet Research: Critical Issues and Methods for Examining the Net* (Thousand Oaks: Sage) 1999
[2] http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci213391,00.html
[3] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth) 1996
[4] Walter Laqueur *The New Terrorism: Fanaticism and Arms of Mass Destruction* (New York: Oxford University Press) 2000
[5] This point is made very succinctly in Alan Stephens and Nicola Baker *Making Sense of War: Strategy for the 21st Century* (Melbourne: Cambridge University Press), 2006
[6] Quoted in Maura Conway 'Terrorist "Use" of the Internet, and Fighting Back' paper presented at the conference *Cybersafety: Safety and Security in a Networked World: Balancing Cyber Rights and Responsibilities* Oxford Internet Institute, Oxford University 2005
[7] Douglas Hayward, 'Net-Based Terrorism a Myth' TechWeb, November 19
[8] Steve Furnell and Matthew Warren 'Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?' *Computers and Security* 18 (1): 28-34
[9] Fred Cohen 'Terrorism and Cyberspace' *Network Security* vol. 5, 2002
[10[Dorothy Denning, 'Information Operations and Terrorism', in *Innovative Terrorism in the Information Age: Understanding the Threat of Cyber-Warfare* 2005 http://www.nps.navy.mil/da/faculty/DorothyDenning/publications/IO%20and%20Terrorism.pdf
[11] Timothy Thomas 'Al Qaeda and the Internet: The Danger of Cyberplanning' *Parameters*, Spring 2003, pp. 112-23
[12] Weimann devotes a whole chapter to cyber-terrorism in *Terror on the Internet: The New Arena, The New Challenges* (Washington: United States Institute of Peace Press) 2006
[13] See Maura Conway 'Hackers as Terrorists? Why it Doesn't Compute' *Computer Fraud and Security* 12, pp10-13, 2004
[14] Martin C. Libicki *What is Information Warfare?* (Washington: National Defence University) 1995
[15] Dorothy Denning – see above.

[16] Gabriel Weimann and Yariv Tsfati, 'Terrorism.com: terror on the Internet' *Studies in Conflict and Terrorism* 25: 317-332 2002
[17] Maura Conway 'Terrorist Web Sites: 'Their Contents, Functioning and Effectiveness' in Philip Seib (ed) *Media and Conflict in the 21st Century* (New York: Palgrave Macmillan) 2005
[18] For example, Hsinchun Chen et al. 'The Dark Web Portal: Collecting and Analyzing the Presence of Domestic and International Terrorist Groups on the Web' Lecture Notes in Computer Science vol. 3495/2005; 2006. 'Collecting and Analysing the Presence of Terrorists on the Web: A Case Study of Jihad Websites' ai.arizona.edu/research/terror/ publications/ISI_AILab_submission_final.pdf
[19] Marc Sageman *Leaderless Jihad: Terror Networks in the Twenty-First Century* Philadelphia: University of Pennsylvania Press 2008
[20] Gabriel Weimann *Terror on the Internet*
[21 – 26] ibid pp 4-15
[27] conversation with Professor Max Taylor
[28] Howard Rheingold *The Virtual Community: Homesteading on the Electronic Frontier* New York: Harper Collins 1994
[29] Terrorism Act 2006 http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060011_en.pdf
[30] Johnny Ryan *Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web* Dublin: Institute of European Affairs 2007
[31] http://ai.arizona.edu/research/terror/index.htm
[32] James Beniger Personalization of the Mass Media and the Growth of Pseudo Community *Communication Research* 14:3, 352-371 1987
[33] Steve Jones. *Cybersociety. Computer-Mediated Communication and Community*.
London: Sage. 1995
[34] Cliff Stoll Silicon Snake Oil: Second Thoughts on the Information Highway. New York: Doubleday 1995