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

The Hizballah Security Apparatus

By Carl Anthony Wege

Abstract: There is little in the open literature concerning the intelligence and security apparatus of the Hizballah organization. Understanding Hizballah's security organ is essential in comprehending its emergence as the most successful liberation and terrorist organizations in the Near East.

Hizballah's Emergence

Political mobilization among Lebanon's Shi'a began in the 1960s with an influx of Shi'a scholars and jurists returning to Lebanon from Najaf (Iraq) after Iraq's 1968 Ba'athist coup. [1] The outbreak of Lebanon's civil war in 1975, followed by the Syrian intervention and Iran's revolution of 1979, saw this Shi'a mobilization become radicalized. Islamic Amal (Amal Al-Islamiyah) was one such radical Shi'a militia created by Hussein Musawi during the July 1982 Israeli-Lebanon war when he and approximately 500 followers from AMAL [2] moved into Nabisheet (Hussein Musawi's home town) in the eastern Lebanese town of Baalbek. They linked up with al-Quds (Jerusalem) elements of Iran's Revolutionary Guard [3] (Iranian Revolutionary Guard Corps, IRGC, or Pasdaran) that had also entered eastern Lebanon's Bekka valley in July 1982 in response to Israel's invasion. Sheikh Subhi Tufayli, and his cadre from Lebanon's al-Dawah (the Islamic Call) movement, had already arrived in the Bekka, creating an environment conducive to the Islamist enterprise.

A coalition developed between the Musawi organization (the followers of Sheikh Subhi al-Tufayli), the Association of Muslim Students, and the Association of Muslim Ulema in Lebanon. [4] The Pasdaran Quds drew from this and sired the creation of Hizballah in Baalbek in coordination with the Iranian Embassies in Beirut and Damascus. [5] Martin Kramer argued that the Pasdaran initially sought out the Shi'a clans of the Bekka, rather than south Lebanon's Shi'a, because for various cultural reasons the group had been excluded from the upper ranks of the AMAL movement. [6] Sequentially, Hizballah would be established first in the Bekka, then in Beirut, and only lastly in Lebanon's south.

The Shi'a clans of southern Lebanon, where kinship is of greater significance than in other areas of the country [7], evidenced greater continuity with the traditional Zi'am (Zu'ma) system. Consequently, they were more oriented toward AMAL's secularists than Hizballah's Islamists. Yet the AMAL militia never developed anything remotely close to the organizational coherence of Hizballah as it matured. Although Hizballah's strength in south Lebanon developed slowly, nonetheless by the time of the 2006 Israeli-Hizballah war, southern Lebanon could militarily be called Hizballahland.

The formal end of the Lebanese civil war with the T'iaf Accords in 1989 saw Hizballah evolve into something greater than a Lebanese confessional militia as it cleaved into a relatively moderate politically oriented and Islamist faction. The Islamist faction itself divided, as Sheikh Tufayli attempted to create a "Movement of the Hungry" with aspirations corresponding to Hizballah's original program for an Islamic Republic of Lebanon. It was stillborn by 1998; as a result the Islamic Resistance (al-Muqawama) became the "mainstream" Hizballah Islamist faction that no longer sought to create an Islamic Republic, but rather to force the Israelis out of southern Lebanon. They achieved that goal in 2000 with the withdrawal of the Israel Defense Forces (IDF).

Hizballah's Security Architecture

In the evolution of Hizballah and its security services, it is important to look at the function of the developing security organs, rather than particular entities or nomenclature, [8] as these differ with different authors. Political authority in Hizballah flows through a clerical-security matrix rooted in lines of kinship influenced by both clan patronage and Iran's Revolutionary Guards. Therefore, formal institutional arrangements are unlikely to reflect functional organization.

Hussein al-Khalil first established Hizballah's security apparatus in Bekka [9] during the summer of 1982, coordinating operations with Islamic AMAL before it was formally subordinated to Hizballah under Hussein Musawi after 1984. [10] The Musawi and Hamadi clans became the core clans of the embryonic Hizballah organization, [11] and this structure magnified the difficulty for hostile services attempting to penetrate Hizballah. It made the exercise akin to penetrating a family. Hizballah's security apparatus reflected the configuration of Shi'a clans and Hizballah's operational emphasis in each of Lebanon's three distinct geographic regions of Shi'a dominance. The geographic regions themselves became subdivided into sectors, creating a compartmentalized operational environment. The Bekka region with the largest IRGC component was characterized by a focus on logistics and training. [12] The southern region of Lebanon had an operational emphasis on the confrontation with Israel, and the organizational focus in the Beirut region was primarily political. In all of the regions, the security apparatus focused initially on internal security, then on covert and military operations.

Hizballah developed multiple and overlapping security organs aimed at maintaining organizational integrity. Hizballah's operational security requires a strict separation between Hizballah's political and military wings. Consequently, the ability of Hizballah's political wing to exercise administrative control over the military wing and its security organs is problematic. Additionally, Hizballah is, at least in part, heavily influenced by Iran, which has created divisions over any external political and administrative control over the military and security components of the organization. Because the impetus for the creation of Hizballah was Iran's Revolutionary Guard, administrative control over the Hizballah's military and security components are divided between both the Hizballah political leadership and the Pasdaran Iran's objectives were to further Shi'a Islamist revolution, while Syrian President Hafez al-

Assad facilitated Pasdaran operations in the Bekka to immunize his troops in Lebanon against Shi'a militants.[13] Al-Assad's support of both AMAL and the Hizballah was important because of the greater affinity of Assad's Alawite tribe for the secularists of AMAL.

A common element across all of Hizballah's security entities is their reliance on fighters drawn from the Shi'a communities throughout Lebanon. The initial model for Hizballah's security services was Fatah's Jihaz al-Razd and the AMAL security entity based loosely on it. [14] Because Hizballah is not a state, a basic intelligence dilemma that faces the organization is the problematic task of establishing and maintaining secure territory and secure facilities. The problem is ameliorated somewhat by using secure facilities in territories of friendly states like Iran. [15] Hizballah's first security concern was necessarily a counterintelligence function [16] to maintain organizational integrity. Hizballah counterintelligence capabilities were influenced by the Pasdaran Quds and applied by Hizballah to local Lebanese circumstances in the context of Syrian occupied Lebanon. Hizballah has successfully executed both defensive and offensive counterintelligence operations. Successful defensive counterintelligence operations are documented as far back as the middle 1980s, when Imad Mugniyah disrupted United States operations involving Lebanese nationals working the Lebanese-Cyprus ferry lines. [17] By 1997, Hizballah counterintelligence could effectively use double agents to mislead the Israelis, successfully executing operations against 13 Israeli Shayetet naval commandos near Sidon, leaving 12 Israelis dead [18] The Hizballah kidnapping of Mossad operative Colonel Elhanan Tannenbaum in 2000 illustrates a more recent successful defensive counterintelligence operation. Tannenbaum had apparently tried to run a "false flag" operation against Hizballah from Europe by claiming to represent a European country. Hizballah lured Col. Tannenbaum to Beirut, where he was taken into custody by Hizballah security personnel. [19]

There are also several known instances of successful Hizballah offensive counterintelligence operations. Hizballah, for example, managed to compromise IDF Lieutenant Colonel Omar al-Heib, who traded surveillance data on IDF military installations for narcotics later distributed by al-Heib's organization. The IDF believes that data compromised by Lt. Col. al-Heib allowed for successful Hizballah targeting of Mt. Meron [20] at the outset of the Israel-Hizballah war of 2006.[21] Recently, Hizballah successfully placed Nadia N. Prouty in the CIA. In a classic operation reminiscent of the U.S-Soviet Cold War, Prouty legally entered the U.S. and then gained citizenship through a sham marriage. She thereafter applied for work and successfully infiltrated the FBI and used that position to leverage a job at the CIA. [22]

Western services have also seen achievement. The defection of Abu al-Kassam Misbahi (Farhad, a co-founder of Iran's VEVAK intelligence organ) in Germany during the middle 1990s [23] was a significant accomplishment. The 2007 defection in Ankara of General Ali Reza Ashgari [24] of Pasdaran Quds, who was instrumental in building Hizballah's organization in Bekka during the early-middle 1980s, was also important. Most recently, the February 2008 assassination of Imad Mugniyah (Hajj Radwan),

presumably by Mossad's Kidon element, was a significant coup for Western intelligence. [25]

Hizballah's intelligence collection abilities have improved over time as well. Israel's occupation of southern Lebanon taught Hizballah the importance of tactical intelligence collection, precipitating Hizballah's careful and ongoing effort to understand how the IDF conducted operations in southern Lebanon. Intelligence collected by Hizballah respecting IDF operational methods prior to the IDF withdrawal in 2000 paid off with the Hizballah victory in the 2006 war.

Hizballah covert operations are carried out using multiple descriptors for its security apparatus. Hizballah followed some early Fatah conventions wherein Fatah's Jihaz al-Razd security entity operated using the Black September Organization moniker during the 1970s. The creation of Hizballah in the summer of 1982 under IRGC guidance necessarily saw preliminary operations limited to the coalescence of Hizballah's constituent entities under multiple names. Hizballah's only opposition at that juncture were small scale actions aimed at controlling territory and organizing personnel with AMAL and other local militias. [26] The security apparatus was then focused on a very narrow core of Hizballah operations, organized with fighters drawn primarily from the Hamadi and Musawi clans. These same fighters conducted operations using different organizational names. The core functions were configured and nurtured by elements of the Bekka's Pasdaran Qud's [27] sustaining Hizballah's Lebanese operations. The attack on the U.S. Embassy in the spring of 1983, and attacks on both the multinational forces and the Israeli intelligence center established in occupied Tyre in the fall of that year, were Hizballah's first major operations against foreigners. These covert operations executed by the security apparatus initiated an operational pattern characterizing subsequent major events. The pattern was direct IRGC support in financing and logistics facilitated by Syrian non-interference [28] in Hizballah operations. During the middle 1980s, this pattern was followed by the security apparatus in its management of kidnapping operations directed against foreigners. [29]

As Lebanon became relatively more stable, the tasks of the security apparatus evolved to include security functions supporting Hizballah's social and political operations as well as military operations. With Hizballah's emergence as a political party representing the bulk of Lebanon's Shi'a, the security apparatus accrued some functions analogous to an Interior Ministry. Police functions became necessary to maintain both the integrity of the party and Lebanon's Shi'a body politic in territories controlled by Hizballah. Within this "domestic" side of the security apparatus was an entity Amad Hamzeh described as an "engagement and coordination unit" under the authority of Hajj Wafic Safa. [30] It eventually turned ordinary criminals threatening Hizballah persons or property over to Lebanon's ostensive authorities. [31] The security apparatus thereby divided functionally between these police functions and functions supporting military and covert operations. Additionally, about two hundred Hizballah fighters operate in a preventive security apparatus under Mahmud Haidar (Abu Ali) in an executive protection role modeled on Fatah's Force 17 that provides security for Hizballah politicians. Elements of the security apparatus also served as an asset for the IRGC Quds. Hizballah's Unit 1800, for example,

was established primarily to serve Iranian foreign policy goals by coordinating Hizballah assistance to multiple Sunni Palestinian Islamists organizations in the West Bank and Gaza. The operational genesis was rooted in the deportation by Israel of four-hundred Hamas militants into southern Lebanon in 1992. Those Sunni Palestinian Islamists were housed and indoctrinated through the good offices of Hizballah. This allowed ties to be forged across the not so insignificant religious division between Shi'a and Sunni Islamists. The Sunni have historically seen the Shi'a as an illegitimate heretical sect, and much blood has been shed between the two main sects of Islam throughout the centuries over these religious disputes. In this instance, however, Israel's role as a common enemy, superseded the two sect's theological differences, and this coordination against Israel facilitated a rarely seen cooperation between the Sunni and Shi'a.

Conclusion

The security architecture created by the Hizballah organization reflects its development in Lebanon's operational environment. The structure of the security apparatus was a function initially of the kinship patterns within the Hamadi and Musawi clans and their associated Islamist groups welded to a security architecture created by the Pasdaran Quds within Syrian and Israeli-occupied Lebanon. Additional Shi'a clans and families were incorporated into Hizballah as the organization expanded. Hizballah's security architecture evolved with the reconstruction of Lebanon in the 1990s and the changing role of the Shi'a in Lebanese society. The emergence of a more developed and assertive Shi'a polity saw the expansion of the Hizballah security apparatus into a more nuanced and sophisticated organization even as relations between Hizballah and Iran strengthened.

The various Hizballah security entities interact today with external services which necessarily shape the configuration of Hizballah's security apparatus at any given point in time. Hizballah's fundamental intelligence challenge is filtering analysis through an Islamist veneer thereby degrading the analytical product. Hizballah has emphasized Hebrew language skills for some of its fighters, yet comprehending Hebrew is not the same thing as grasping Israeli thought. Archie Roosevelt [32] argued long ago that a lust for knowing which seeks understanding unclouded by worldview must animate the intelligence enterprise. Hizballah's security apparatus must lust to know Israel even as it understands Hebrew. In a larger sense, the Hizballah security apparatus must create a raison d'être that goes beyond moribund dreams of a Lebanese Islamic Republic or its utility furthering Iran's imperial ambitions. Hizballah's security apparatus must affirm Shi'a political and social aspirations in Lebanon to survive.

Carl Anthony Wege is a Professor of Political Science at Coastal Georgia Community College.

NOTES

[1] Shapira, Shimon "The Origins of Hizballah" Jerusalem Quarterly 46 (Spring 1988): 116. The secular Ba'athist parties in Iraq and Syria opposed to the Islamist's who later created Lebanon's al-Dawah (the Islamic Call) movement.

[2] These were primarily al-Dawah members who had infiltrated AMAL earlier intending to maneuver the organization in an Isamist direction. AMAL was created by Musa Sadr in 1974 and is generally consider the first Shi'a militia. It's goals were to protect the Shia community and it was a relatively secular organization with an initial focus on Lebanese political and social reform.
[3] Hussein Musawi initiated the split within AMAL during the Fourth Congress in Tyre during March of 1982. See Sankari, Jamal. Fadlallah: The Making of a Radical Shi'ite Leader. London: Saqi Books, 2005. pg. 196.
[4] Shapira, "The Origins of Hizballah." p. 124.
[5] See Aboul-Enein, Youssef and Rudolph Atallah. "Hizballah: A Discussion of Its Early Formation." Infantry, 94 (3) May / June 2005 pg, 24. See also Al-Muharar, Lebanon 28 July 1989.
[6] See Kramer, "Hizbullah: The Calculus of Jihad," Bulletin of the American
Academy of Arts and Sciences, May, 1994, p. 25. These Bekka clans included the Hamiya, Musawi, Aqueel, Shahadehs, and Ezzedeens.
[7] See Al-Itihad 13 September 1988.
[8] This is analogous to Americans still referring to a Directorate of Operations or D.O. rather than a National Clandestine Service irrespective of changing organizational structures.
[9] Al-Khalil (who holds a degree in mathematics oddly enough) is now more of a politician and has less involvement in operations. However, like Imad Mugniyah, he started out as a member of the Palestinian Fatah's Force 17 and commanded Fatah military formations in Tyre during the 1978 Israeli invasion. In the 1982 Israeli invasion he fell back to Beirut with PLO forces and after the Palestinian evacuation to Tunis he migrated to Hizballah where he managed security for Hussein Musawi. Al-Khalil would briefly be in charge of Hizballah foreign operations and then Hizballah counterintelligence. He also maintained a parallel political role with election to Hizballah's Shura (decision making) Council in 1985. See Intelligence Online 22 December 2006.
[10] Ranstorp, Magnus. Hizb'allah in Lebanon: The Politics of the Western Hostage Crisis. New York: St. Martin's Press, 1997.P. 66. Khalil would later become chairman of Hizballah's Politburo.
[11] Some Hamadi clan branches had roots around the southern village of Sawaraneh as tobacco farmers. It claimed between two and three hundred members many of whom migrated to Beirut. There are also Hamadi clan branches based in the Hermel plain between Baalbek and Syria proper. Clan members have been prominent across the social spectrum from Sabry Hamadi, a long serving Speaker of Parliament to Hamadi clan elements prominent in the Hashish industry. Across several decades the Hamadis and Assads acted as Shi'a dynasties with alternating service as Parliament Speaker.
[12] In 1990 the IRGC began rotating Quds trainers after discovering that Mossad had compromised three of them. See al-Sharq al-Awsat 16 July 2006.
[13] This policy was continued by Bashar Assad as President of Syria after the death of his father Hafez al-Assad in 2000.
[14] Prior to the rise of the Shi'a Islamists, Lebanese Shi'a tended to migrate into the Lebanese Communist Party or Fatah (even though the Shi'a and Palestinians would have strained relations in later years). The first exposure many Shi'a had in the 1970s to guerrilla training was under Fatah instructors.
[15] Mustafa Badreddine faced this problem when he assumed command of Hizballah's counterintelligence directorate in the early 1990s and formalized at the seventh Hizballah Congress in 1991. Badreddine is a son-in-law of Imad Mugniyah and one of the Kuwait prisoners Hizballah was trying to free in the middle 1980s. He escaped Kuwait after the Iraqi invasion in 1991 and made his way to Beirut in 1992. Badreddine would later become the mayor of Nabitiyyah.
[16] Counterintelligence is divisible into offensive and defensive activities. Offensive counterintelligence would refer to operations run against rival organizations such as the Prouty penetration of the CIA by Hizballah. Defensive counterintelligence has its focus on internal organizational security.
[17] See "Iran's plans in Lebanon" Foreign Report 12 November 1987, pg. 3. Also in the fall of 1994 Hizballah prevented a CIA kidnap operation aimed at Hassan Ezzeddine who ran Hizballah foreign operations prior to its disbanding in 1995. The operation had been facilitated through a compromised AMAL official who managed to escape to the Cyprus station and from there went to the United States. See Intelligence Online 26 October 1995.
[18] See Jones, Clive. "A Reach Greater than the Grasp: Israeli Intelligence and the Conflict in South Lebanon 1990-2000." Intelligence and National Security Vol. 16, No. 3 (Autumn 2001), pg. 12. Israel had organized an appendage to its South Lebanon Army (SLA) proxy militia called Unit 501. This ethnically mixed unit was intended to gather intelligence on the Islamic Resistance but was used instead by Hizballah to gather information on the South Lebanon operations of the IDF
[19] See The New York Times 17 October 2000.
[20] An Israeli Air Force surveillance center is located there.
[21] See Col. David Eshel. "Hezbollah's Intelligence War" www.defense-update.com Accessed 12/11/2007.
[22] In a response also reminiscent of some cold war penetrations the United States allowed her to plead guilty to some minor charges thus avoiding government embarrassment in open court.
[23] The historic ties between Germany and Persia, dating to the 19th century, also provide an entrée into Hizballah via the German BND.
[24] General Ashgari apparently helped identify Nada Prouty (al-Quar) penetration of CIA in 2007.
[25] It is likely that General Ashgari provided relevant information here as he had a relationship with Mugniyah very early on.
[26] Although formed in response to the Israeli invasion of 1982, the IDF was preoccupied with the Palestinians and aware of little more than the arrival of the IRGC into the Bekka.
[27] The mission of Quds is to export the Shi'a Islamic revolution and it is functionally divided into geographically defined departments. The Lebanon / Palestine Department has been the most successful.
[28] Syria's Alawite regime found it useful to maintain an alliance of sorts with the Twelver Shi'a of Iran. Iran gained access to Lebanon's Shi'a community and a point of confrontation against Israel while Syria gained political and economic support that partially replaced that lost with the collapse of the USSR.
[29] Domestic kidnapping and other criminal activity was a money making enterprise for dozens of Lebanese militias in those years.
[30] Safa was one of the founders of Hizballah and has extensive security experience. During the middle 1990s Safa's deputies included Hassan Ezzeddine, Hamze Zakaria and Abdul Hadi Hamadi. See Intelligence Online 16 March 1995. Abdul Hamadi was himself assisted by Mustafa Chehade, Talal Hussein Hamadi, and Nabil Kaouk (who ran Hizballah security in south Lebanon). See Intelligence Online 14 September 1995.
[31] See Hamzeh In The Path of Hizbullah, pg.65.

[32] Roosevelt, Archie. For Lust of Knowing: Memoirs of an Intelligence Officer. Boston: Little, Brown and company, 1988.

BIBLIOGRAPHY

Aboul-Enein, Youssef and Rudolph Atallah. "Hizballah: A Discussion of Its Early Formation." Infantry. 94 (3) May / June 2005: 21-26.
Early, Bryan "Larger than a Party, yet Smaller than a State' Locating Hezbollah's Place within Lebanon's State and Society World Affairs 168 (Winter 2006): 115-128.
Hamzeh, Ahmad Nizar. In The Path Of Hizbullah. New York: Syracuse University Press, 2004.
Harris, William W. Faces of Lebanon: Sects, Wars, and Global Extensions Princeton: Markus Weiner Publishers, 1997
Jones, Clive. "A Reach Greater than the Grasp: Israeli Intelligence and the Conflict in South Lebanon 1990-2000." Intelligence and National Security Vol. 16, No. 3 (Autumn 2001):1-26
Kennedy, David and Leslie Brunetta. Lebanon and the Intelligence Community. C15-88-859.0 Case Program, John F. Kennedy School of Government, Harvard University, 1988.
Kliot, N. "Lebanon – a geography of hostages." Political Geography Quarterly 5 (July 1986): 199 - 220.
Kramer, Martin. "Hizbullah: The Calculus of Jihad," Bulletin of the American Academy of Arts and Sciences, May, 1994. Pages 20-43
Mallat, Chibli. Shi'i Thought From The South Of Lebanon. Oxford: Centre for Lebanese Studies, 1988.
Ranstorp, Magnus. "Hizbollah's Command Leadership: Its Structure, Decision-Making and Relationship with Iranian Clergy and Institutions." Terrorism and Political Violence 6 (3): 303-339.
Hizb'allah in Lebanon: The Politics of the Western Hostage Crisis. New York: St. Martin's Press, 1997.
Roosevelt, Archie. For Lust of Knowing: Memoirs of an Intelligence Officer. Boston: Little, Brown and Company, 1988.
Sankari, Jamal. Fadlallah: The Making of a Radical Shi'ite Leader. London Saqi Books, 2005.
Shapira, Shimon. "The Origins of Hizballah." Jerusalem Quarterly 46 (Spring 1988): 115 – 130.
Shahahan, Rodger. The Shi'a of Lebanon: Clans, Parties and Clerics. London And New York: Tauris Academic Studies, 2005.

Terrorism Knowledge Base: A Eulogy (2004-2008)

By Brian K. Houghton

On the night of March 31, 2008, the intensely useful Terrorism Knowledge Base® went from an interactive site of tens of thousands of terrorism incidents, group profiles, indictment records, and mapping and graphing tools, to a mere static single page misleading everyone that the site is just down while it is "being refreshed". For those of us who have relied on the TKB for our research, teaching, journalism, analysis, and general reference on terrorism, this knowledge base will be sorely missed.

The TKB emerged out of the RAND Corporation's Terrorism Chronology, which Brian Jenkins likes to say was first started in 1970 on 3" x 5" cards, detailing terrorism incidents which began in the modern era in 1968. From these modest beginnings, RAND's database grew into one of the most comprehensive chronicles of international terrorism, and yet it was solely used within RAND. For decades, critics and scholars longed to peek inside RAND's proprietary data to gain access to the same knowledge that this "think tank" held. For a brief time the Chronology was jointly held by RAND and the University of St Andrews in Scotland, but this ended in 1997, and the database lay dormant until 2001.

At that time, RAND received a grant from the new Memorial Institute for the Prevention of Terrorism (MIPT), a non-profit organization chartered to be a living legacy to those who lost their lives in the tragic bombing of the Murrah Federal Building in Oklahoma City. MIPT knew the significance of the database and wanted it not only preserved, but also made available to the public at large. With new funding, RAND resurrected the dataset and also began collecting information on domestic terrorism incidents around the world. Partnering with DFI International and adding court trial data from the University of Alabama at Birmingham, the concept for a knowledge base was born.

The new Terrorism Knowledge Base was unique in its form and function, taking full advantage of the growth of internet tools. The TKB was not merely a portal or online database, but rather the fusion of data with related information, making it a true knowledge base. The site allowed users to find a wealth of knowledge with minimal effort. Upon searching for an incident, users could find links to the group responsible or other attacks in that country. TKB's group profiles showed researchers all incidents committed by the group, quick "baseball card-like" statistics for the attacks, group leader bios and pictures, official terrorist designations by the State Department, and other governments, related organizations, and sources of analysis for further research. Free analytic tools could be used to compare groups, create dynamic graphs, or dig into certain categories of targets and tactics.

The TKB was literally a dream come true for analysts, researchers, academicians, journalists, and the public at large. From its first online presence in 2004, the site literally exploded with users—and those users kept coming back again and again. What I personally found appealing was that from the beginning users were asked to help improve

the knowledge base by offerings corrections or suggestions. No database has perfect data, but this one strived toward perfecting itself through user input. Certainly, there are other databases available to researchers (e.g. ITERATE, Global Terrorism Database and WITS), each with their inherent strengths and weaknesses, but the TKB made research intuitive and far reaching.

So if the Terrorism Knowledge Base was such a good tool for the counter-terrorism community, why did it "die"? There will be no autopsy on the corpse, and those responsible for the death will most likely fade away into their bureaucratic cubicles to inflict neglect on other projects. The original funding of MIPT's TKB came through Congressional earmarks administered by the Department of Justice. After the creation of the Department of Homeland Security, funding and administrative oversight was shifted to an office in DHS intended to provide equipment to emergency responders. For a time in the short period after 9/11 funding was no issue, but government attention has started to move away from terrorism to a focus on disasters (post-Katrina), war (Iraq and Afghanistan), and other social issues. One might think that there would be a plethora of funding available, but the stark fact is that there is a shrinking in terrorism analysis funding and a concern within government about funding projects, like databases, that are never-ending. With the evaporation of government terrorism research monies it is only a matter of time until more projects terminate. Unfortunately, the contest is not strictly Darwinian; the best ones do not necessarily always survive.

The TKB's demise was simply brought about by the economic "free rider" principle—everyone loved using it, but nobody wanted to pay. Typically in situations like this, the government steps in and creates a method to fund the public good, but in the case of the TKB, the Department of Homeland Security office who provided previous funding did not see how a counter-terrorism knowledge base impacted their narrow focus, and those who utilized the knowledge base the most did not put enough pressure on DHS to continue the funding. After all the funding and effort to create such a useful tool, which truly was a living legacy for those who perished in past acts of terrorism, the TKB died from bureaucratic neglect. What a waste.

Yes, we will still have other terrorism databases, but none of them are true *knowledge bases*. It is hard to gauge who will fill the vacuum left by TKB, and if they can make the same level of commitment to supporting the next generation of terrorism scholars and counterterrorism practitioners. We must ask ourselves if the disappearance of TKB portends the loss of other terrorism databases in the future. Are we closing our eyes to the threat again?

Brian K. Houghton is an Associate Professor of Public Policy & Management at BYU-Hawaii, and the former Director of Research at the Memorial Institute for the Prevention of Terrorism.