Cybercortical Warfare: Hizbollah's Internet Strategy

Maura Conway

School of Law & Government
Dublin City University
Glasnevin, Dublin 9
Ireland

maura.conway@dcu.ie

INTRODUCTION

The acceleration of the historical tempo and the move from hierarchical to networked conceptions of power is disintegrating the mechanisms of control and political representation at the disposal of the state. The upshot of this is that 'resistance confronts domination, empowerment reacts against powerlessness, and alternative projects challenge the logic embedded in the new global order' (Castells 1997, 69). These reactions and mobilizations, often take 'unusual formats and proceed through unexpected ways' (Castells 1997, 69). This chapter deals with one such alternative project. It is a preliminary empirical analysis of the adoption by the Lebanese-based terrorist group Hizbollah (Party of God)[i] of a strategy of cybercortical warfare. In his introduction to the Vintage edition of *Covering Islam* (1997), Edward Said refers to the 'information wars that have gone on since 1948 around the whole question of the Middle East' (p. xxi). He is particularly concerned with the way in which Hizbollah 'who identify themselves and are perceived locally as resistance fighters' are 'commonly referred to in the American media as terrorists' (p. xiii). Hizbollah are one of a number of groups that have utilized the Internet 'to produce and articulate a conscious and forceful self-image' (Said: 66) of themselves not as terrorists, but as resistance fighters and statesmen. The major focus of this chapter is the way in which Hizbollah have wielded the Internet as a weapon in their information war. As will be demonstrated, the group's collection of Web sites is targeted not at Lebanese or Palestinian audiences, but at the Israeli population and global publics. For this reason, the chapter represents a case study of the possibilities of the new technology, discussed and defined by this chapter as 'cybercortical warfare'.

SZAFRANSKI'S NEOCORTICAL WARFARE

Neocortical warfare 'attaches more importance to communicating with other minds than to targeting objects' (Szafranski 1997: 396). It points to the reframing of conflict as warfare against minds and envisions its weapons as any means used to change the

enemy's will (Szafranski 1997: 404). It is founded on the belief that at base politics is the pursuit and eventual exercise of power, and that "power" is 'the ability to influence people who otherwise might not choose to be influenced' (p. 397). The concept of neo-cortical warfare originated with Richard Szafranski in his article entitled 'Neocortical Warfare? The Acme of Skill,' which first appeared in 1994 in the *Military Review*, a publication of the U.S. Army Command and General Staff College. Szafranski quoted Sun Tzu to the effect that 'To subdue the enemy without fighting is the acme of skill' (p. 399).

Neocortical warfare may be conceived of as a species of Perception Management, which is generally held to include the disciplines of Public Affairs, Public Diplomacy, Psychological Operations, Deception and Covert Action (Dearth 2002: 1). Perception Management may be defined as:

> Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives (Dearth 2002: 2).

This chapter is concerned more with the conveyance of information than its denial, and focuses on its effects upon foreign publics rather than intelligence systems and leaders. Its focus is therefore Public Diplomacy, rather than the other disciplines that compose Perception Management. The practice of Public Diplomacy has undergone significant change as a result of the information revolution.

THE NEW PUBLIC DIPLOMACY

Diplomacy has traditionally been thought of as the development and implementation of foreign policy by diplomats. However, states and their representatives are no longer the only actors in diplomatic relations. There is an increasing emphasis on the role of non-state actors and publics in diplomacy, not only as recipients of diplomacy -- the traditional understanding of 'public diplomacy' as a government's process of communicating with the public of another nation in order to influence its opinion -- but also as diplomatic actors. Put simply, the public dimension of diplomacy has been increasing in importance. While there was a time when diplomats were the sole interlocutors between countries, now unmediated dialogue and information exchange between citizens from around the globe occurs 24 hours a day, seven days a week. The theory and conduct of diplomacy is undergoing a radical rethink as a result. There have been repeated calls for diplomacy to be 'reinvented' to take account of the Information Revolution and a welter of analyses published suggesting how this might be accomplished (Vickers 2001). This chapter is concerned with just such a reinvention, albeit a reinvention outside the purview of a majority of the research undertaken to date.

In the past, Public Diplomacy was often seen as irrelevant and unimportant. However, there is a growing movement to give Public Diplomacy a greater prominence in the conduct and study of international relations. This interest follows from an emergent view that the practice of world politics is changing; that things are being done in a

new way, that new actors are important. Rather than a realist world composed purely of states acting militarily to maximize their power positions, this consensus points to a world in which international politics can be thought of in terms of an 'informational pluralism.' On the one hand this is a world with a variety of agents at work, but where the operation of this pluralism is shaped by the impact of the information or communications revolution. These processes can be summarized in the idea that we are seeing the development of a 'new Public Diplomacy.' This idea has a double meaning. Firstly, that we are seeing diplomacy -- understood in the broad sense as the practice of international relations -- taking place in public and the public being involved. Secondly, that the central instrument of this new diplomacy is actually Public Diplomacy: that is communication and communications technologies (Brown 2001a; White 2001: 317-330).

Soft Power

Brown (2001a) suggests that the new public diplomacy entails a change in the nature of power, but it also helps us to understand how power is utilized in international affairs. The most widely discussed alternative conceptualization is the idea of Soft Power developed by Joseph Nye. Nye first put forward his thesis in *Bound to Lead* (1990), but has returned to the idea on several occasions, most notably in two contributions to the journal *Foreign Affairs*. In 1996, in an article with William Owens, Nye defined Soft Power as "the ability to achieve desired outcomes in international affairs through attraction rather than coercion" (Nye and Owens 1996: 21). In a 1998 article with Robert Keohane, Nye returned to this theme to draw a distinction between free information (such as scientific data, advertising, political propaganda), commercial information (information that is sold), and strategic information (information that is useful because it is possessed by one actor, but not others). They argue that:

> Politically…the most important shift has concerned free information. The ability to disseminate free information increases the potential for persuasion in world politics. NGOs [non-governmental organizations] and states can more readily influence the beliefs of people in other jurisdictions…Soft power and free information can, if sufficiently persuasive, change perceptions of self-interest and thereby alter how hard power and strategic information are used (Keohane and Nye 1998: 89-92).

As Brown has pointed out, one major consequence of this new environment is the importance of credibility as a source of power (Brown 2001b: 11)

Although there have been many guerrilla groups fighting as oppressed national minorities, only five groups have had the credibility that allowed them to become significant diplomatic actors in the last two decades. In the mid-1970s, the Palestinian Liberation Organization (PLO) and South West African People's Organization (SWAPO) achieved membership of the Non-Aligned Movement and the Group of 77, along with observer status in the UN General Assembly and at all UN conferences. Three other groups -- the ANC, the Pan-African Congress, and the Patriotic Front of Zimbabwe -- obtained the right to attend UN conferences (Willetts 2001, 368). However, world politics today transcends simple inter-national relations and inter-

governmental organization, and much of the change has taken place as a result of the spread of information infrastructures. Diplomacy is no longer the sole province of states and their representatives. Instead, the Internet offers the opportunity for non-state actors and marginalized groups to engage in what has been called 'virtual diplomacy' (Smith 2000) or 'cyber-diplomacy,' (Potter 2002) essentially the practice of Public Diplomacy via the Internet.

CYBERCORTICAL WARFARE

'Neocortical warfare is warfare that strives to control or shape the behavior of enemy organisms, but without destroying the organisms' (Szafranski: 404), it 'uses language, images and information to assault the mind, hurt morale and change the will' (Szafranski: 407). In other words, neocortical warfare is the conduct of Public Diplomacy in an explicit conflict situation. 'Cybercortical warfare' is therefore an apposite term to describe the conduct of Public Diplomacy *via the Internet* in the same situation. In the broadest sense, cybercortical warfare is about offensively shaping the information environment, particularly the 'conflict space' (Dearth 2002: 8). To do this successfully, one must possess credible political and military power in order to command attention and convincingly project information power. In the realm of Public Diplomacy, for example, all Arab states have launched their own Web sites and many have several such sites. These sites are designed to get information about their countries out to the rest of the world, and to counter or balance information provided on the Web by Israel, Iran, and other states (Franda 2002, 81). States are not the only actors to establish a presence on the Internet, however. Worldwide, recent years have seen more and more groups that are engaged in militancy and political violence -- the representatives of 'uncivil society', if you like -- establish an online presence. A comprehensive list of all such sites, both official and unofficial, is maintained by an individual in the United States and is available online.[ii] An overview of the background to and purpose of these sites is provided below.

TERRORISM AND MASS COMMUNICATION

In their study of terrorism and the media, *Violence as Communication* , Alex Schmid and Janny De Graaf point out that:

> Before technology made possible the amplification and multiplication of speech, the maximum number of people that could be reached simultaneously was determined by the range of the human voice and was around 20,000 people. In the nineteenth century, within one lifetime, the size of an audience was expanded twenty-five to fifty times. In 1839 the *New York Sun* published a record 39,000 copies; in 1896, on the occasion of President McKinley's election, two U.S. papers, belonging to Pulitzer and Hearst, for the first time printed a million copies. William McKinley paid dearly for this publicity. In 1901 he was killed by an anarchist, Leon Czolgosz, who explained his deed with the words: 'For a man should not claim so much attention, while others receive none'" (Schmid and De Graaf 1982: 10).

Historically, access to the communication structure was intimately related to power (Crelinsten 1987: 443). With the growth of the press, and later television, a situation arose that gave unequal chances of expression to different people. This connection between power and free expression was summed-up by A.J. Liebling who observed that 'Freedom of the press is limited to those who own one' (quoted in Schmid and De Graaf 1982: 177).

Terrorism has always been about communication. In fact, scholars argue that 'without communication there can be no terrorism' (Schmid and De Graaf 1982, 9). Each new advancement in communication technology has resulted in new opportunities for terrorists to publicize their positions. From Marxist revolutionaries such as Brazil's Carlos Marighela's advice to his comrades to use photocopying machines to produce large numbers of pamphlets and manifestos to Hizbollah's establishment of its Al Manar television station in the early 1990s. While seeking to convey a message through their 'propaganda of the deed', terrorists also must employ written and spoken language in an effort to legitimize, rationalize and, ultimately, advertise their actions. Now, thanks to the new communications technologies, particularly the Internet, for the first time terrorists are equal communication partners in the electronic agora.

In the space of thirty years, the Internet has metamorphosed from a U.S. Department of Defense command-and-control network consisting of less than one hundred computers to a network that crosses the globe. Today, the Internet is made up of tens of thousands of nodes (i.e. linkage points) with over 105 million hosts spanning more than 200 countries. With a current estimated population of regular users of just under one billion people, the Internet has become a near-ubiquitous presence in many world regions (Clickz Stats 2004). That ubiquity is due in large part to the release in 1991 of the World Wide Web. In 1993 the Web consisted of a mere 130 sites, by 2004 it boasted more than one billion (Dunnigan 2003, 37).

Media have for decades been attributed with considerable significance in processes of cultural and political transformation. The Internet is daily heralded as a new media technology of enormous and increasing significance; it is the first many-to-many communication system and the instrument of a political power shift. The ability to communicate words, images, and sounds, which underlies the power to persuade, inform, witness, debate, and discuss (not to mention the power to slander, propagandize, engage in misinformation and/or disinformation, etc.) is no longer the sole province of those who own or control printing presses, radio stations or television networks. Every machine connected to the Internet, from laptop computers to mobile phones, is potentially a printing press, a broadcasting station, a place of assembly. And in the twenty-first century, terrorists are availing themselves of this opportunity to connect.

It is the unmediated nature of the Internet, in conjunction with high levels of connectivity, which renders it a communications medium unlike any other. There is a tendency in newspapers and on television for the primary sources of political information to be those who represent authority or who are members of the existing power structure. The British scholar Stuart Hall distinguishes between these 'primary definers' (politicians, police spokesmen, government officials), and what he calls 'secondary definers' (political or social activists, 'reformers,' terrorists) who reside

outside of the existing power structure. The latter are used much less frequently by the media than are primary definers, according to Hall (Crelinsten 1987: 420). So while modern terrorists can manipulate the media into devoting newsprint and airtime to their activities, political claims, and demands, the media in turn manipulate the terrorists: "The insurgent terrorist messages are transported to the public mainly by the media and the message is thereby almost invariably abbreviated, distorted or even transformed" (Schmid and De Graaf 1982: 110). Journalists and TV presenters achieve this by playing up the violent spectacle at the expense of analysis, in order to attract consumers, thus undermining the terrorists' claim to legitimacy by depicting them as merely violent, often irrational and even psychotic, and not political (Crelinsten 1987: 421). With the advent of the Internet, however, the same groups can disseminate their information undiluted by the media and untouched by government censors. In 1998 it was reported that 12 of the 30 terrorist organizations identified by the U.S. State Department had their own websites. Today, a majority of the 36 groups on the same list maintain an official online presence (see Conway 2002, Table 1).[iii]

THE STATE OF THE RESEARCH ON THE INTERNET AND TERRORISM

In 1979 Nathan Leites recognized that although much work of a varied nature had been undertaken on what terrorists do and a smaller amount on what makes them do it, very little research considered 'what they thought they were doing,' or more precisely 'what good they thought it would do' (Cordes 1988: 151). Since then, large amounts of research have been devoted to describing and analyzing what terrorists have done in the past and to identifying trends in order to gauge what they might do in the future. However, much less attention has been focused upon terrorist motivations, mindsets or self-perceptions. Leites' analysis is therefore as relevant today as it was more than two decades ago, which is surprising given the easily accessible primary materials provided by modern terrorists (in the form of their Web sites) from which much information can be gleaned. These Web sites, however, have not yet been the subject of any sustained academic investigation. A majority of the research and analysis pertaining to the Internet and Web sites as political tools has focused on the power of transnational advocacy groups, such as Green Peace, Amnesty International and other civil society actors, and their ability to harness the power of international communications technologies to forward their goals (Bennett 2003, Cleaver 1998, Couldry and Curran 2003, Van De Donk et al 2003, Hajnal 2002, Kahney 2003, Leizerov 2000, Lin and Dutton 2003). Much less attention has been paid to those groups that compose 'uncivil society,' particularly terrorist groups. This may be due to a number of factors, including the difficulty associated with fitting groups that employ violence into the various frameworks devised to categorize social movements, and a certain 'feel good factor' that imbues the work of scholars concerned with issues of transnationalism, international advocacy, etc.

An alternative reason why the academic community has essentially ignored Web sites maintained by terrorist organizations may be that scholars doubt the efficacy of the Internet as a political tool. Walter Laqueur, a respected figure in terrorism studies, made the following observation in 1999:

> No amount of e-mail sent from the Baka Valley to Tel Aviv, from Kurdistan
> to Turkey, from the Jaffna peninsula to Colombo, or from India to Pakistan

will have the slightest political effect. Nor can one envisage how in these conditions virtual power will translate into real power (p.262).

This statement is particularly startling when one considers that a few lines previously Laqueur admits that audiocassettes smuggled into Iran played a key role in the Khomeini revolution. In more recent times, numerous civil society actors have conducted successful campaigns via the Internet that have had significant political effects. For example, email was credited with halting a U.S. banking plan aimed at combating money laundering. The Nobel Prize-winning International Campaign to Ban Landmines, which successfully lobbied for a treaty stopping the use, production, stockpiling, and transfer of antipersonnel mines, coordinated its activities via the Net. The website MoveOn.org, best known today for its efforts to mobilize opponents of both George W. Bush and the Iraq war, has attracted over two million subscribers to join its email list and has instituted a U.S. television advertising campaign paid for by online donations. In each case 'virtual' or 'soft' power was translated into 'real' power, whether financial, legal or otherwise. It is the ability of such 'soft' power to bring about 'real' effects that is the subject of the remainder of this chapter, which describes Hizbollah's strategy of cybercortical warfare and analyses its effects.

HIZBOLLAH: SOME BACKGROUND INFORMATION

Hizbollah[iv] has been described as "one of the most significant terrorist organizations operating today" (Whittaker 2001: 41). The U.S. government has maintained a list of foreign terrorist organisations since October 1997 when former U.S. Secretary of State Madeline Albright approved the designation of the first 30 groups under the Immigration and Nationality Act (as amended by the Antiterrorism and Effective Death Penalty Act 1996). Hizbollah appeared on the original list and has remained on it to the present time. Groups officially designated as foreign terrorist organisations by the U.S. Secretary of State (in consultation with the Attorney General and the Secretary of the Treasury) are subject to a number of legal restrictions. It is unlawful, for example, for a person in the United States or subject to the jurisdiction of the United States to provide any kind of financial or material support to such organizations. Both representatives and members of these groups may be denied visas or excluded from the United States, and U.S. financial institutions must block the funds of these groups and report the blockage to the Office of Foreign Assets Control of the U.S. Department of the Treasury.

Hizbollah was established in 1982 in response to the Israeli invasion of Lebanon. The group is composed of radical Shia's and takes its ideological inspiration from the Iranian revolution and the teachings of the Ayatollah Khomeini. The Majlis al-Shura, or Consultative Council, is the group's highest governing body and is presided over by Secretary General Hassan Nasrallah. Hizbollah advocates the establishment of Islamic rule in Lebanon and the liberation of all occupied Arab lands, including Jerusalem. It has expressed as a goal the elimination of Israel (Saad-Ghorayeb 2002: 134-167). The group refused to work within Lebanon's established political system until 1992, when it fielded candidates in parliamentary elections (Palmer Harik 2004: 95-110). Although closely allied with and often directed by Iran, the group is thought to have conducted operations that were not approved by the Iranian leadership. While Hizbollah does not share the Syrian regime's secular orientation, the group has been a

strong tactical ally in helping Syria advance its political objectives in the region (see Palmer Harik 2004: 29-41). In addition to political, diplomatic and organizational aid, Hizbollah receives substantial amounts of money, training, weapons, and explosives from both Iran and Syria (U.S. Department of State 2003).

The group has thousands of supporters, but only a few hundred terrorist operatives. These operate in the Bekaa Valley, the southern suburbs of Beirut, and southern Lebanon. According to U.S. experts, the group also has established cells in Europe, Africa, South America, North America, and Asia, and are suspected to have been involved in numerous anti-U.S. terrorist attacks, including the suicide truck bombings of the U.S. Embassy in Beirut in April 1983, the U.S. Marine barracks in Beirut in October 1983, and the U.S. Embassy annex in Beirut in September 1984. Three members of Hizballah are on the FBI's list of 'Most Wanted Terrorists' for the hijacking in 1985 of TWA Flight 847 during which a U.S. Navy diver was murdered. Elements of the group were responsible for the kidnapping and detention of U.S. and other Western hostages in Lebanon in the 1980s (see Jaber 1997: 97-144; Ranstorp 1997). The group also attacked the Israeli Embassy in Argentina in 1992 and is a suspect in the 1994 bombing of an Israeli cultural centre in Buenos Aires (U.S. Department of State 2003; Saad-Ghorayeb 2002: 88-111).

Hizbollah was among the few groups that President Bush mentioned by name in his January 2002 State of the Union address:

> Our military has put the terror training camps of Afghanistan out of business, yet camps still exist in at least a dozen countries. A terrorist underworld -- including groups like Hamas, Hezbollah, Islamic Jihad, Jaish-i-Mohammed -- operates in remote jungles and deserts, and hides in the centers of large cities (Bush 2002).

Bush also condemned the group as terrorists in his June 2002 speech on the Middle East:

> I've said in the past that nations are either with us or against us in the war on terror. To be counted on the side of peace, nations must act. Every leader actually committed to peace will end incitement to violence in official media and publicly denounce homicide bombings. Every nation actually committed to peace will stop the flow of money, equipment and recruits to terrorist groups seeking the destruction of Israel, including Hamas, Islamic Jihad and Hezbollah (Bush 2002a).

Hizbollah's Cyber Capabilities

The issue of Hizbollah's cyber capabilities was discussed as early as 1996. In that year, John Deutch, former director of the U.S. Central Intelligence Agency, testified before a Senate committee that international terrorist groups had the capability to attack the critical information infrastructure of the United States. Deutch said the methods used could range from such traditional terrorist methods as a vehicle-delivered bomb – such as one directed against a telephone switching center or other communications node -- to electronic attacks relying on paid computer hackers. He

identified Hizbollah as one of a number of terrorist groups who used the Internet for their communications and might therefore have both the inclination and the ability to launch such an attack (Deutch 1996).

More recently, a CIA report to the U.S. Senate Intelligence Committee identified a number of terrorist organizations, Hizbollah among them, that 'have both the intentions and the desire to develop some of the cyberskills necessary to forge an effective cyberattack modus operandi' (McCullagh 2002). There is ample evidence confirming that 'terrorists who fight modernity and its perceived evils in the name of defending traditional values and religious principles do not shy away from enlisting advanced technology for their holy wars or secular fights to enforce their agendas' (Nacos 2002: 108). For example, the leadership of Hizbollah wear traditional dress and adhere to Islamic custom in the way they live their daily lives and in their preaching. But like other similar fundamentalist and anti-modern groups, they rely heavily on the predominantly younger members of their organisation that are trained in modern communication technologies. Members of Hizbollah and other terrorist groups are known to be computer-literate. There is evidence that they compose training manuals on their laptop computers, distribute them on CD-ROMs, or transmit their files via email to trusted operatives (Whine 1999: 236). This chapter is concerned neither with the ability nor the desire of Hizbollah to carry out a cyber attack on the United States, which is a matter for further research. Rather, this chapter seeks to describe and analyse the effect of the group's strategy of cybercortical warfare, carried out via its collection of Web sites, on the citizens of Israel and Western publics more generally.

HIZBOLLAH'S INTERNET STRATEGY

Autonomous communication is a paramount objective for Hizbollah. The group first went on line in early 1996. The Central Press Office site, or Hizbollah.org, is the group's official homepage, and is available in both English and Arabic. Hizbollah maintains at least three other sites of an official character (all of which are available in both English and Arabic versions): http://www.moqawama.tv known as the 'Islamic Resistance Support Association' and which describes the group's attacks on Israeli targets; http://www.manartv.com the news and information site that is essentially the homepage of Hizbollah's Al Manar Television; and http://www.nasrollah.net, the official homepage of the group's leader Sayyed Hassan Nasrallah (and available in French). The sites are said to receive between one and three thousand hits per day.

The Hizbollah Web sites are reasonably well designed. In recent times, both Nasrollah's personal homepage and the Al-Manar TV site have been redesigned to a fairly high standard. Although the Central Press Office and Moqawama sites are the group's flagship sites in their campaign of cybercortical warfare, they are beginning to look slightly dated. Both sites are, however, densely packed with information. The top English-language page of the Central Press Office site provides links to sections entitled 'In the Press,' 'Statements of the Resistance,' 'Political Declarations,' 'Speeches of the Secretary General,' and others. The site contains an extensive photographic archive, sound recordings (in Arabic only), and over one hundred video clips for viewing or download. The latter are divided into four categories: 'Aggressions,' 'Operations,' 'Intifada,' and 'Miscellaneous.' The top English-

language page of the Moqawama site provides links to sections entitled 'Reality,' 'Background,' 'Features,' 'Views in Zionism,' 'Cartoons,' and 'Readers Letters,' amongst others. The sections entitled 'Military Operations,' 'Martyrs,' and 'Israeli Aggressions' are updated on an almost daily basis. The 'Military Operations' section, for example, provides a day-to-day accounting of Hizbollah operations from 1997 to the present, while the section entitled 'Israeli Aggressions' contains hundreds of pages – over 700,000 words – detailing what appears to be every perceived act of Israeli aggression against the Lebanese since 1998. The Moqawama site also contains a gallery of photographs of dead 'martyrs' numbering over one hundred and fifty. The Al-Manar TV site, designed in grey and gold, contains information about the station's programming, and extensive television footage drawn from same. The Secretary General's homepage contains a biography of Nasrollah, updated news, an archive of speeches and interviews, a photographic archive, and more. There is a 'Contributions' button located on the top page of the Moqawama site, but this is not operational. A request for financial contributions was at one time included on the Al-Manar TV site and was accompanied by an account number for a bank in Beirut, Lebanon. However, all such requests for contributions now appear to have been deleted from Hizbollah's English-language Web sites. None of the Hizbollah sites offer items for sale.

A study published in November 1997, over a year after the establishment of the Hizbollah sites, found that the total number of Internet users in the Arab world, (excluding Israel) as of July 1997 was 215,500. Of a population of over 3.5 million people, there were just 35,520 Internet users in Lebanon (Nua 1997).[v] Hizbollah maintained their sites in both Arabic and English from the outset. This despite the low number of Internet users in the whole of the Middle East and the fact that a 1998 study found that Arabic sites with Arabic text received many more visitors from within the Arab world than Arabic sites with English text (Nua 1998). Further, Pippa Norris has shown that in societies where the online population is not large there is minimal incentive for groups to develop Web sites, and the lack of infrastructure hinders their development (Norris 2001). This indicates that Hizbollah were interested in targeting a non-Lebanese and non-Middle Eastern audience from the outset. Their targeted audiences were the citizens of Israel and English-speaking publics more generally.

In March 1997, an article in Beirut's *Al-Safir* newspaper drew attention to the 'psychological warfare' being employed by Hizbollah. The article is devoted to describing Hizbollah's al-Manar television station's Web site, which is depicted as Hizbollah's corrective to the Israeli's mis-education of Western publics:

> Psychological warfare can be used as a weapon of war to be added to the military materiel, not only to repulse the aggression, but also to confront the enemy's deceptive policy toward the world public. Although this war has many faces, it has one head only, namely the media… Hizballah's step is primarily aimed at refuting the fallacies Israel has been spreading abroad concerning the occupation of south Lebanon. (FBIS 1997).[vi]

The report goes on to say that the site managers regularly receive email from Internet surfers 'some of which salute the resistance and others request information on the Lebanese-Israeli conflict' (FBIS 1997). In addition, it is reported that some of the subscribers to the site's email list – 'who began to show sympathy with the resistance

when the Qana massacre occurred' (FBIS 1997) -- transmit the information they receive across other networks and lists thus spreading these messages further than would otherwise be the case. Finally, the article also explains that al-Manar employees view Internet access as a useful educational resource due to the availability of reports and analyses produced by the Israeli Foreign Ministry and other agencies, which allow Hizbollah members to become familiar with the methods by which governments demonize terrorist organizations and thus educate the former as to how to carry out a counter-campaign. A number of employees were also said to be taking training courses via the Net (FBIS 1997).

In a September 2001 interview, Hassan Ezzieddine, the head of Hizbollah's Department of Media Relations, confirmed:

> We feel that the media can be effective in creating a special climate in public opinion on the main issues of interest…We are heading toward a new sensitive security situation (in the region) which means we need to follow events very closely so that we can informatively help shape international and Arab public opinion…We believe that the media has an important role in the conflict, as important as the military wing (Blanford 2001).

To underscore the importance of the media's role in the conflict, Hizbollah's leadership decided in 2001 to place al-Manar TV under the direct supervision of a committee composed of senior figures in the organization and chaired by the group's secretary-general, Sayyed Hassan Nasrallah. The Central Information Office, which had liased with the press and published Hizbollah's weekly newspaper *Al-Ahed*, was abolished and replaced by the new Department of Media Relations. Ezzieddine, a member of Hizbollah's political council, was put in charge. Ezzieddine and his staff reportedly examine newspaper articles dealing with Hizbollah and follow television and radio broadcasts. The new department is also responsible for maintaining the group's official Web sites, which are currently in the process of a major overhaul.

Tsfati and Weimann (2002) have pointed out that almost all terrorist groups that maintain an online presence avoid presenting and detailing their violent activities: 'Although the organizations behind these sites have a record of bloodshed, they hardly ever record these activities on their sites' (p.321). The exceptions, they point out, are Hizbollah and Hamas. Hizbollah's site contains a section ('Daily Operations') that provides updated statistical reports of its actions that 'display in minute detail all of the organization's operational successes' (p.321). A separate page enumerates the number of dead 'martyrs' along with the number of 'Israeli enemies' and 'collaborators' killed. This is part of Hizbollah's campaign of cybercortical warfare:

> Hizbollah differs somewhat from other organizations in that it highlights its military achievements, gloating over enemy victims (showing pictures of funerals of murdered Israelis), and publishing detailed statistics about its military successes. The motive for this unique approach has been Hizbollah's attempt to influence the public debate in Israel about withdrawal from Lebanon. The organization has stated explicitly that its aim has been to exert pressure in Israel in favor of withdrawal. The organization knows that many Israelis visit the site, whose address is published in Israeli media. Hizbollah publishes its records of murdered Israelis, maintains electronic connections

with Israelis, and appeals to Israeli parents whose sons serve in the Israeli army, all with the aim of causing demoralization (Tsfati and Weimann 2002: 325).

CYBERCORTICAL WARFARE: THE EFFECTS

Josef Goebbels, Hitler's Minister of Propaganda, once said: 'We do not talk to say something, but to obtain a certain effect' (Schmid and De Graaf 1982: 14). Terrorism entails the use of violence for effect, 'speaking with action' rather than words. The meaning of terrorist acts is not always clear, however. An integral part of most terrorist activity, therefore, is the explanation later provided in written and oral forms (Cordes 1998: 164). There is an added dimension to cybercortical warfare, however. The object of the strategy adopted by Hizbollah was to understand the adversary well enough to condition or determine the choices they made: 'Using the adversary's lexicon, syntax and representational systems allows the neocortical warrior to lead the adversary through the cycle of observation, orientation, decision and action. Mastery is the result' (Szafranski: 408).

Hizbollah has succeeded in entering the homes of Israelis via the Internet, thus creating an important psychological breakthrough (see Tsfati and Weimann 1999: 317). The group accomplished this goal in 1999 when it provided details on its website about the return of the bodies of Israeli marine commandoes who had fallen in Lebanon. Hizbollah stated that the single coffin returned contained not just a single body, but the body parts of a number of the marines. The statement caused uproar among the families of the deceased and resulted in a bitter confrontation between the latter and the Israeli Defense Force (IDF) authorities. Hizbollah also has published appeals to the parents of Israeli soldiers stationed in Lebanon on their sites. A prominent example was the publication of an interview, originally aired in Israel, with four mothers of IDF soldiers entitled 'I Don't Want My Son to Die in Lebanon.' Many Israelis, particularly parents of soldiers serving in Lebanon, admit visiting the Hizbollah site to get news updates. 'I regard these sites as a legitimate source of information,' one Israeli father is reported to have said. According to Tsfati and Weimann (1999: 327), 'the Hizbollah site even offers to answer anyone who sends questions by email, and does indeed reply to Israeli questioners, sending information and news to their email addresses.'

There is no doubt that Hizbollah's leadership would also like to gain access to Western, particularly American, audiences via the Internet. It is difficult to gauge how successful they have been in this respect. They appear to have met with relatively little success in targeting the American public, despite the fact that 'given the absence of censorship and the private ownership of most public media and the fact that "violence is as American as apple pie," the United States seems to be the country most open to terrorist uses of the media (Schmid and De Graaf 1982: 33).A Hizbollah spokesman was recently quoted as saying: 'The service is very important for the morale of our resistance fighters. They are always happy to know that people around the world are backing them' (Whine 1999: 233). Considerably more evidence than this is required, however, before the group's campaign of cybercortical warfare is deemed successful outside of their immediate region.

CONCLUSION

Terrorists are not limiting themselves to the traditional means of communication; they increasingly employ the new media to pursue their goals. The terrorists of today, like those of yesteryear, are keen to exploit the traditional mass media while also recognizing the value of more direct communication channels. As has been pointed out, 'if what matters is openness in the marketplace of ideas…then the Web delivers an equal opportunity soapbox' (Norris 2001: 172). As far back as 1982, Schmid and De Graaf acceded that:

> If terrorists want to send a message, they should be offered the opportunity to do so without them having to bomb and kill. Words are cheaper than lives. The public will not be instilled with terror if they see a terrorist speak; they are afraid if they see his victims and not himself…If the terrorists believe that they have a case, they will be eager to present it to the public. Democratic societies should not be afraid of this (Schmid and De Graaf 1982: 170).

Keen to exploit the Internet, by 2004 a majority of the 36 organizations that appear on the U.S. list of Designated Foreign Terrorist Organizations had established an online presence. These include not only Hizbollah, but Aum Shinrikyo, the Tamil Tigers, Basque Fatherland and Liberty (ETA), Lashkar-e-Tayyiba, the Kurdistan Workers Party (PKK), and others.

The leadership of Hizbollah realized early on that establishing a meaningful virtual power-base was reliant on a functioning and effective Web presence. In a recent report for the United States Institute of Peace entitled *WWW.terror.net: How Modern Terrorism Uses the Internet* (2004), Gabriel Weimann highlights the advantages offered by the Internet to terrorists: ease of access; the ability to evade regulation, censorship, and other forms of government control; potentially huge audiences with a global spread; anonymous intra-group communication; rapid transfer of information; inexpensive development and maintenance of Web sites; a multimedia environment; and the ability to shape coverage in the traditional mass media, which increasingly use the Web as a source for reporting (p.3). For terrorists, therefore, Web-based communication offers the potential to be a more immediate, dynamic, in-depth, interactive, and unedited process than was ever possible in conventional media. It was this realisation, along with the institution of an extremely skilful and effective information strategy, which has ensured that Hizbollah has been able to use the Web as an additional tool for their political aims. However, it remains to be seen whether they will be able to parlay their 'local' success into the ability to influence international opinion in a meaningful way with the tools of the Web.

REFERENCES

Bennett, W.L. (2003) 'Communicating Global Activism: Strengths and Vulnerabilities of Networked Politics.' *Information, Communication and Society* 6(2).

Blanford, N. (2001) 'Hizbullah Steps up Psychological Warfare: Party believes that the Media Plays Critical Role in Palestinian Uprising.' *Daily Star* (Beirut) 8

September. Available online
<http://www.hizbollah.org/english/press/p2001/p20010908a.htm>.

Brown, R. (2001a) 'The New Public Diplomacy: Power in the Age of Mixed Media.'
Paper presented at 4th Pan-European International Relations Conference, Canterbury,
UK.

Brown, R. (2001b) 'Power and the New Public Diplomacy.' Paper presented at the
British International Studies Association Annual Conference, University of
Edinburgh, Scotland, 2001.

Bush, G.W. (2002) *State of the Union Address*. Washington DC: White House.
Available online <http://www.law.ou.edu/hist/state2002.shtml>.

Bush, G.W. (2002a) 'Text of President Bush's Address on the Middle East.'
Washington Post 25 June.

Castells, M. (1997) *The Power of Identity*, Oxford: Blackwell.

Cleaver, H.M. (1998) 'The Zapatista Effect: The Internet and the Rise of an
Alternative Political Fabric.' *Journal of International Affairs* 51(2).

Clickz Stats Staff. (2004) 'Population Explosion!.' *Clickz.com* 10 May. Available
online
<http://www.clickz.com/stats/big_picture/geographics/article.php/5911_151151>.

Conway, M. (2002) 'Reality Bytes: Cyberterrorism and Terrorist "Use" of the
Internet', *First Monday* 7(11). Available online
<http://www.firstmonday.org/issues/issue7_11/conway/index.html>.

Cordes, B. (1988) 'When Terrorists Do the Talking: Reflections on Terrorist
Literature.' In D.C. Rapoport (ed) *Inside Terrorist Organizations*. London: Frank
Cass.

Couldry, N. and Curran, J. (2003) Contesting Media Power, New York: Rowman.

Crelinsten, R.D. (1987) 'Power and Meaning: Terrorism as a Struggle Over Access to
the Communication Structure.' In P. Wilkinson and A.M. Stewart (eds)
Contemporary Research on Terrorism, Aberdeen: Aberdeen University Press.

Dunnigan, James. 2003. *The Next War Zone,* New York: Citadel Press.

Dearth, Douglas H. (2002) 'Shaping the "Information Space."' *Journal of Information
Warfare* 1(3).

Deutch, J. (1996) *Statement Before the U.S. Senate Governmental Affairs Committee*
(Permanent Subcommittee on Investigations), June 25. Available online
<http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html>.

Foreign Broadcast Information Service (FBIS) (1997) 'Hizballah's al-Manar TV on Internet.' FBIS-NES-97-043, 3 March.

Franda, M. (2002) *Launching into Cyberspace: Internet Development and Politics in Five World Regions,* Boulder and London: Lynne Rienner.

Hajnal, P.I. (ed) (2002) *Civil Society in the Information Age,* Aldershot: Ashgate.

Jaber, H. (1997) *Hezbollah: Born With a Vengeance,* New York: Columbia University Press.

Jorisch, A. (2004) *Beacon of Hatred: Inside Hizballah's Al-Manar Television* (Washington DC: The Washington Institute for Near East Policy).

Kahney, L. (2003) 'Internet Stokes Anti-War Movement.' *Wired*, January 21. Available online <http://www.wired.com/news/culture/0,1284,57310,00.html?tw=wn_story_related>

Keohane, R.O. and J. S. Nye, Jr. (1998) 'Power and Interdependence in the Information Age.' *Foreign Affairs* 77(5).

Laqueur, W. (1999) *The New Terrorism: Fanaticism and the Arms of Mass Destruction,* Oxford: Oxford University Press.

Leizerov, S. (2000) 'Privacy Advocacy Groups Versus Intel: A Case Study of How Social Movements are Tactically Using the Internet to Fight Corporations.' *Social Science Computer Review* 18(4).

Lin, W. and W.H. Dutton (2003) 'The 'Net' Effect in Politics: The 'Stop the Overlay' Campaign in Los Angeles.' *Party Politics* 9(1).

McCullagh, D. (2002) 'CIA Warns of Net Terror Threat.' *C|Net* 29 October. Available online <http://news.com.com/2100-1023-963771.html?tag=cd_mh>.

Norris, P. (2001) *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide,* Cambridge: Cambridge University Press.

Nua Internet Surveys (1998) 'Internet Usage in the Arab World.' Available online <http://www.nua.com/surveys/index.cgi?f=VSandart_id=888945819andrel=true>.

Nua Internet Surveys (1997) 'Middle East Internet Usage.' Available online <http://www.nua.com/surveys/index.cgi?f=VSandart_id=878906966andrel=true>

Nye, J.S. (1990) *Bound to Lead: The Changing Nature of American Power,* New York: Basic Books.

Nye, J.S. and W.A. Owens (1996) 'America's Information Edge.' *Foreign Affairs* 75(2).

Palmer Harik, J. (2004) *Hezbollah: The Changing Face of Terrorism,* London: I.B. Tauris.

Potter, E. H. (ed) (2002) *Cyber-Diplomacy*. Canada: McGill-Queens University Press.

Ranstorp, M. (1997) *Hizb'Allah in Lebanon: The Politics of the Western Hostage Crisis*, London: Macmillan.

Rapoport, D. (1988) 'The International World As Some Terrorists Have Seen It: A Look at a Century of Memoirs.' In D.C. Rapoport (ed.) *Inside Terrorist Organizations*, London: Frank Cass.

Saad-Ghorayeb, A. (2002) *Hizbu'llah: Politics and Religion*, London: Pluto Press.

Said, E. (1997 [1981]). *Covering Islam*, London: Vintage.

Schmid, A. P. and J. De Graaf (1982) *Violence as Communication,* Minneapolis: University of Minnesota Press.

Smith, G. S. (2000) 'Reinventing Diplomacy: A Virtual Necessity.' *United States Institute of Peace: Virtual Diplomacy Report* (VDS6), February. Available online <http://www.usip.org/vdi/vdr/gsmithISA99.html>.

Swartz, J. (2001) 'Experts: Cyberspace Could Be Next Target', *USA Today*, October 16.

Szafranski, R. (1997 [1994]) 'Neocortical Warfare: The Acme of Skill?' In J. Arquilla and D. Ronfeldt (eds) *In Athena's Camp: Preparing for Conflict in the Information Age*, California: Rand. Available online at http://www.rand.org/publications/MR/MR880.

Tsfati, Y. and G. Weimann (2002). 'www.terrorism.com: Terror on the Internet.' *Studies in Conflict and Terrorism* 25(5).

United States Department of State (2003). *Patterns of Global Terrorism 2001*. Washington DC: Department of State. Available online at: http://www.state.gov/s/ct/rls/pgtrpt/2003/.

Vickers, R. (2001). 'The New Public Diplomacy in Britain and Canada.' Paper presented at the British International Studies Association (BISA) Annual Conference, Edinburgh, UK.

Van De Donk, W., B. Loader, P. Dixon, and D. Rucht (Ed.s) (2003). Cyberprotest: New Media, Citizens, and Social Movements. London: Routledge.

Weimann, G. (2004). *WWW.Terror.Net: How Terrorism Use the Internet*. Washington DC: United States Institute of Peace. Available online at http://www.usip.org/pubs/specialreports/sr116.html.

Whine, M. (1999). 'Cyberspace: A New Medium for Communication, Command, and Control by Extremists.' *Studies in Conflict and Terrorism* Vol. 22.

White, B. (2001). 'Diplomacy.' In John Baylis and Steve Smith (Eds.), *The Globalisation of World Politics* (2nd Ed.). Oxford: Oxford University Press.

Whittaker, D.J. (2001). 'Lebanon.' In D.J. Whittaker (ed.), *The Terrorism Reader*. London: Routledge.

Willetts, P. (2001). 'Transnational Actors and International Organizations in Global Politics.' In John Baylis and Steve Smith (Eds.), *The Globalization of World Politics* (2nd Ed.). Oxford: Oxford University Press.

---

[i] The 'correct' English spelling of the group's Arabic appendage is Hizb'Allah or Hizbu'llah, however it is more usually spelled 'Hizbollah,' 'Hizballah,' or 'Hezbollah.' I have chosen 'Hizbollah' because that is the spelling employed in the URL designating the group's official homepage. However, where I have employed quotation I have retained the original spelling used by the author.

[ii] Bob Cromwell's 'Separatist, Para-Military, Military, and Political Organisations' is available online at http://www.cromwell-intl.com/security/netusers.html.

[iii] The European Union (EU) has recently updated its list of prohibited organizations (see http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_099/l_09920040403en00280029.pdf). Hizbollah has never made an appearance on the EU list, which contains twenty-five organisations.

[iv] According to the U.S. Department of State, the group is also known as Islamic Jihad, Revolutionary Justice Organization, Organization of the Oppressed on Earth, and Islamic Jihad for the Liberation of Palestine. They are also known to refer to themselves as the Islamic Resistance Movement.

[v] The study's findings were based on actual subscription numbers to ISPs. It has since been shown that the average number of users per Internet account in most Arab counties is three, see Nua Internet Surveys, 'Arab Net Population Passes 3.5 Million' (2001). The latter is available online at http://www.nua.com/surveys/index.cgi?f=VSandart_id=905356603andrel=true.

[vi] For an alternative position on Al-Manar TV, see Jorisch 2004.