CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

CSC 32 / CCEM 32

MASTER OF DEFENCE STUDIES

THE INTERNET: AN EVOLUTIONARY OR REVOLUTIONARY INFLUENCE ON TERRORIST COMMUNICATIONS, STRUCTURES AND ACTIVITIES?

By / par Major P de Rouffignac

24 April 2006 / 24 Avril 2006

TABLE OF CONTENTS

List of Tables

List of Figures

ABSTRACT

This paper examines the use of the Internet by terrorist groups as a means of communication. Whilst noting that others have put forward the idea of cyber terrorism as a weapon of mass effect, this paper concentrates on the evolutionary and revolutionary aspects of the Internet as a communications medium. Terrorist events before and during the "Information Age", such as Oklahoma, and 9/11 will be studied. Provisional Irish Republican Army and Al-Qaeda activities and structures will be compared and contrasted to show the effect of Internet use for communications by terrorist groups. In addition, examples of the use of the Internet by Right-wing terrorist groups will also be given. The use of the Internet by organised crime and the rise of cell phone technology will be used as comparators for terrorist use. The uses, usefulness and limitations of the Internet for terrorist groups will also be assessed. By doing so, it will be shown that the use of the Internet for communications by terrorists is merely an evolutionary rather than revolutionary process.

INTRODUCTION

"We also call on Muslim *ulema*, leaders, youths and soldiers to launch the raid on Satan's US troops and the devil's supporters allying with them.[1]"

On 7 July 2005, four men wearing backpacks boarded London Underground trains on the Victoria and Circle lines between 08:42 and 08:49. The London rush hour was at its height, with commuters travelling to work aboard packed trains. At 08:50, three of the men detonated the bombs they had carried on their backpacks. The final bomb failed to explode. The fourth man, diverted from the temporarily suspended Northern Line, then caught a bus in the direction of King's Cross, but was diverted via Tavistock Square. Seconds later, an explosion ripped off the roof of the number 30 bus on which he was travelling. The picture of the devastated red London Bus provided the world with one of the most graphic images of terrorism since the attacks on New York and Washington almost four years earlier. Two groups swiftly claimed responsibility for the attacks[2]: the hitherto unknown Secret Group of Al-Qaeda of Jihad Organisation in Europe and the Abu Hafs al-Masri Brigade. These claims appeared on the website of Muhammad al-Massari's Islamic Renewal Organisation: as a result of these claims being published on the Web, the website was severely disrupted as a consequence. Tacit endorsement of the attacks quickly came from Hani al-Siba'I, Director of the Al-Maqrizi Centre for Historical Studies in an interview with al-Jazeera television. Equally quickly came a strongly worded statement for the G8 countries that were holding their summit in Gleneagles, Scotland, at the time of the attacks. As well as condemning the attacks, they emphasised the importance of preventing people from turning to terrorism:

---

[1] Osama Bin Laden's "Jihad against Jews and Crusaders", February 1998, cited by M Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), 19.

[2] P Tumelty, "An In-Depth Look at the London Bombers", *TerrorismMonitor*, Volume 3, Issue 15, July 28, 2005, www.jamestown.org, accessed 11 November 2005.

> Knowledge of the terrorists and their networks helps us to understand how and why individuals join these networks. Together, we are analysing why individuals have chosen the path of violence and how, for example, terrorists use the Internet to promote radicalisation and pursue recruitment.[3]

Whilst the motivation for these attacks and the history of the terrorists who executed them is outwith the scope of this paper, the text above reveals the use of communications as an important weapon in both the terrorist and counter-terrorist arsenal. It can be seen that the Internet played a significant role in the planning, execution of and subsequent claiming of responsibility for these attacks; however, so does the use of television, either through al-Jazeera's interviews with terrorist sympathisers, or through the subsequent release of video footage by one of the men[4] responsible for Western Europe's first home-grown suicide attack. Equally important were the use of cell phones for command, control and coordination of the attacks[5]; perhaps unintended by the terrorists, but equally forceful, were the harrowing effects of broadcasts of video images[6] captured on cell phones by survivors of the attack as they made their way to safety through dark, dusty and smoke-filled Underground tunnels.

As the link to Islamic terrorist networks and the London attacks became clearer[7], numerous reports heralded these attacks as an example of terrorism in the "Information Age", of

---

[3] G8 Statement on Counter-Terrorism, issued 8 July 2005, at http://www.fco.gov.uk/Files/kfile/PostG8_Gleneagles_CounterTerrorism.pdf accessed 22 November 2005.

[4] Video of Mohammad Sidique Khan, broadcast by al-Jazeera, at http://news.bbc.co.uk/1/hi/uk/4208250.stm accessed 26 February 2006.

[5] Use of Hasib Hussain's cell phone given at http://news.bbc.co.uk/1/hi/uk/4181454.stm accessed 26 February 2006.

[6] Footage at http://news.bbc.co.uk/1/hi/in_depth/uk/2005/london_explosions/default.stm# accessed 26 February 2006.

[7] M Evans, "New clues support al-Qaeda link for London Bombing", *Sunday Times*, 30 January 2006, http://www.timesonline.co.uk/article/0,,22989-2016192,00.html accessed 26 February 2006.

the type described by Arquilla, Ronfeldt and Zanini using the term "NetWar"[8]. On a wider basis, the same authors would argue that the information age has led to a radical, indeed *revolutionary* shift in terrorist group structures and activities as a result of information technology[9]. For example, the "flattening" of groups, from a rigid, chain of command model, to a less hierarchical structure, without a recognised figurehead, is one such effect. However, there are remarkable similarities in the planning and execution of these attacks and the numerous attacks carried out on the United Kingdom (UK) mainland by terrorists of the Provisional Irish Republican Army (PIRA) during the 1980s and 1990s. These include: the recruitment methods used to attract the bombers; the use of a small independent cell; the targeting of an economic centre; and the immediate claim of responsibility. In addition, the lack of an established hierarchy is not a new idea. For example, Bushart[10] describes the concept of "small, armed militant groups, independent of each other, autonomous, but fighting for the same cause" in 1998. Beam, the most well known theoretician within the ranks of the extreme right wing in the US and an ex-Grand Dragon of Texas White Knights, traces back this concept of a networked, non-hierarchical structure– which he terms "leaderless resistance" - back through Amoss in the 1960s to as far back as the Committees of Correspondence organised to fight the British prior to American Independence in 1776. One could reasonably ask, therefore, if the impact of information technology and the Internet on shaping terrorist communications, and, as a second order effect, their activities and structures, is as great as is suggested.

---

[8] Arquilla et al, "Information Age Terrorism" *Current History*, (April 2000): 179-185.

[9] Arquilla et al, "Networks, Netwar and Information Age Terrorism", in *Strategic Appraisal* ed Khalizad and White, (Santa Monica California: RAND, 1999)

[10] Bushart et al, *Soldiers of God: White Supremacists and their Holy War for America*, (New York: Kensington Pub Corp,1998) 234-57.

This paper will examine the role of the Internet by terrorists and argue that, for their purposes, it is an evolutionary, not revolutionary method of communication, with a corresponding evolutionary effect on structures and activities. In order to do so, first the distinction between revolution and evolution will be made. This will be done by studying communication methods and assessing their impact, not just for terrorists but also for all users. Second, I will limit my focus to non-state actors who use violence to further their cause and the civil and military authorities facing them. Third, the terrorist situation before the spread of the Internet will be described, using a case study of PIRA pre-1990, in order to demonstrate the subtle differences and compelling similarities in terrorist activity prior to the spread of the Internet. Fourth, terrorism in the contemporary era will be examined in order to look at how technology has changed terrorism as well as how terrorists use technology for their purposes. Examples used will include the Oklahoma bombing in 1995, the Omagh bombing in 1998 and the attacks on New York and the Pentagon in 2001. In addition, a detailed examination will be made of terrorist purposes for the Internet, such as recruiting, financing and networking. Fifth, after contrasting portraits of pre- and post-Information Age terrorism have been established, the effect of different communication methods in each of these will be compared and contrasted to show that the effects of the Internet on structures and activities is evolutionary, not revolutionary. As comparators, the effects of the Internet on organised crime and the rise of cell phone technology will be assessed in order to demonstrate similar evolutionary trends. Finally, the arguments will be summarised, concluding that the use of the Internet by terrorist groups has had an evolutionary effect on communication methods, structures and activities.

EVOLUTION OR REVOLUTION?

INTRODUCTION

In order to determine if the Internet is indeed an "evolutionary" or "revolutionary" method of communication for terrorist purposes, we must first begin by what we mean by the distinction between both of these terms. How will we know when we see a revolution as opposed to an evolution?

Table 2.1 – Evolution and Revolution

Word	Meaning	Synonym	
Evolution	The gradual development of something into a better more or complex form.	development fruition growth progress advancement	
Revolution	A dramatic change in ideas or practice.	transformation upheaval conversion development	change reform innovation modernisation

Source: Oxford English Dictionary

Historical Examples

Whilst the table above gives dictionary definitions and synonyms as a basic framework, it may be useful to look at historical examples to give substance to these. For example, the Industrial Revolution that occurred in Great Britain during the 19th Century saw great changes in manufacturing industry and transport as a result of advances in technology. Mass production transformed the way the societies made their living and became the core principle of industrial economies[11]. The French Revolution saw the end of feudalism, the creation of a Constitution and is widely seen as a major turning point in continental European history, from the age of absolutism to that of the citizenry, and even of the masses, as the dominant political force.

[11] C Sloan, *The Revolution in Military Affairs*, (Montreal: McGill-Queens University Press, 2002), 19.

Incidentally, the French Revolution also gave us the first use of "terrorist" in the English language in 1795, in the writings of Edmund Burke commenting on Robespierre's regime of terror[12]. The so-called Revolution in Military Affairs (RMA) takes its basis from "…a paradigm shift in the nature and conduct of military operations"[13], where a significant advance in technology has dramatically and rapidly altered the way a military force does its core business in a way that ultimately renders previous forms obsolete.

Evolution

Evolution, however, implies straightforward, linear, progressive change. Biologists would use the term to demonstrate how organisms have developed from simple single cell creatures into those we see today. However, there is no guarantee that any particular organism existing today will become more intelligent, more complex, bigger, or stronger in the future. Evolution can favour lower intelligence and reduced complexity if those traits lead to an advantage in the organism's environment.[14] This issue of reduced complexity actually being advantageous is, for example, a question mark against whether or not there has been an RMA; modern sensor to shooter technology may be effective against an adversary with similar equipment, but of limited use against an asymmetric opponent[15]. Similarly, many technologies hailed as revolutionary have their origins decades ago, with stepped evolutionary changes being responsible for their development[16].

---

[12] Gearson, J, *The Nature of Modern Terrorism*, (London: Political Quarterly Publishing Co, 2002) 14.

[13] Ibid, 3.

[14] Encyclopaedia Britannica, https://www.britannica.com accessed 10 April 2006.

[15] Sloan, *The Revolution in Military Affairs*, 30.

[16] Ibid, 34.

How, then, does one distinguish between an evolution and a revolution? A revolution occurs when the change is rapid, profound and in such a fashion that previous evolutionary change is rendered almost obsolescent or ineffective.

COMMUNICATION METHODS AND THEORY

INTRODUCTION

In order to establish exactly when a revolution – or, indeed, if one has taken place – in the field of communications, it is essential to study both a basic level of communication theory and a more detailed study of mediated (formerly mass media) methods of communication. In doing so, it will be determined which methods of communications that information technology has most greatly affected and begin to establish why the impact of this has become important for the structure and activities of terrorist organisations.

COMMUNICATION THEORY

The Oxford English Dictionary[17] describes "communications" as:

> the technology and systems used for sending and receiving messages, for example, postal and telephone networks; the effective use of words to convey ideas or information …the study of the different means people use to communicate with each other,

Essentially, therefore, communication is a transactional, symbolic process, which allows people to establish contact, exchange information, and both reinforce and change attitudes and behaviours. Various models of communication theory have been proposed, which are shown below:

Table 3.1 - Communication Models

Model	Shannon	Lasswell	Matlezke	de Rouffignac
Elements	Information source Transmitter Signal + Received signal Receiver Destination	Communicator Message Channel Receiver Effect	Communicator Message Medium Receiver	Creation Transmission Reception Interpretation Action

Source: Adapted from McQuail, *Mass Communication Theory*

[17] Oxford English Dictionary, http://www.oed.com/, accessed 10 April 2006.

The core communication model has five elements, adapted from the other three models using terminology relating to actions and effects as opposed to physical entities and systems:

Creation. This is the act of composition of the message by the individual or group wishing to pass on the information, via cognitive process, then verbally or physically via electronic or written media.

Transmission. This is the act or process of passing the information through media. This could be as simple as through the air in a voice conversation or as complicated as a fibre-optic or satellite-based network.

Reception. This is the process whereby an individual or group for whom the message is intended receives the information, either through direct aural methods or through an electronic device producing aural or visual output, such as a radio, a TV screen or a computer monitor.

Interpretation. The information must be assigned a particular meaning or significance by the individual or group that it is received by. Issues of language, culture and expectations can affect interpretation.

Action. The important issue to note is the effect the message has on the receiver after interpretation, remembering that one of the purposes of communication is to change or reinforce attitudes and behaviours.

Scales of Communication

This basic model can be adapted to suit all scales of communication, four key magnitudes of which are commonly identified:

Interpersonal. This is communication between two individuals. The reaction of the individual to the message is termed a *psychological* one.

Small group. Small group communication takes place in settings of between more than two individuals. Small groups are influenced differently from individuals upon receiving a message and their interactions relate to common perceptions and interpretations of a message. This is termed a *sociological* reaction and becomes important when considered in the context of the small independent cell structure of modern "networked" terrorist groups.

Organisational. This occurs in large groups, such as organisations or businesses. Organisational communication aims largely to coordinate separate elements into a structure or a coherent whole. This too has implications for the context in which terrorist group structures are considered, given the bureaucracy and latitude of interpretation that tends to be associated with disseminating messages within large hierarchical organisations.

Mediated, or mass communication. This describes communication to huge numbers of individuals. It is this method of communication that has, arguably, been affected to the

greatest extent by information technology. It is also this method that terrorist groups have sought to communicate for the majority of their purposes in a sociological context.

Accordingly, mediated communication will be studied in further detail to demonstrate why the Internet in particular is perceived to offer advantages to the terrorist.

MEDIATED COMMUNICATION

McQuail[18] identifies five forms of mediated communication: book, newspaper, film, broadcasting – including television and radio – and finally the Internet. The characteristics of each are listed below, by technology and material type, typical formats and genres, perceived uses and institutional setting:

[18] D McQuail, *Mass Communication Theory*, (London: Sage, 1983), 24-45.

Table 3.2 – Characteristics of Mediated Communication

Mediated communication form	Characteristics	
Book	Technology of moveable type Bound pages Multiple copies Multiple content Individual in use Individual authorship Claim to freedom of publication	
Newspaper	Regular and frequent appearance Reference to current events Urban, secular audience Relative freedom	
Film	Audiovisual technology Extensive appeal Predominantly narrative fiction More international than national in character Subjection to social control From mass to multiple markets	
Broadcasting	<u>Radio</u> Flexible and economic production Flexible in use Multiple contents Relative freedom Individualised use Participant potential	Television Large output, reach and content Audiovisual content Complex technology and organisation Public character Extensive regulation National and international character Very diverse content forms
Internet	Computer based technologies Hybrid, non-dedicated, flexible character Interactive potential Private and public functions Low degree of regulation Interconnectedness Ubiquity and delocatedness Accessible to individuals as communicators	

Source: Condensed from McQuail, "Mass Communication Theory"

It can be seen from the table above that there are differences between mediated forms. These differences can be categorised in terms of physical content, trust and credibility, freedom from regulation and the usefulness of a particular medium from the point of view of the creator and receiver. Whilst the first three of these can be assessed in a quantitative terms, it is the qualitative effect of the fourth that is the issue at question in this paper.

Differences in Mediated Forms

The differences between mediated forms are becoming less divergent. This can be seen in the fact that many of the differences between mediated forms are lessened due to the rise of information technology. Many media forms are distributed across different transmission channels, reducing uniqueness and experience in use. Secondly, digitisation has mean that many forms now diverge: newspapers, books and now even television broadcasts are available over broadband Internet. Thirdly, globalisation of national and international media have led broadcasters to disseminate information over many forms, whose content does not vary from national to international versions. For example, the British Broadcasting Corporation (BBC) website offers television and radio streams, access to BBC books and periodicals and even news alerts to cell phones and mobile personal data assistants (PDAs). All this is available in thirty-three languages.[19] Finally, the lack of regulation regarding information technology makes it useful for broadcasting material that could not be disseminated through any other form. Its networked structure and global reach make it impossible to police. Attempts to shut down a website are normally met with the site re-appearing a few days later, based on a different server in a different country[20].

The Internet: History, Growth and the Future

Having seen how mediated communication has been influenced by information technology as a result of its characteristics, it is worth examining the history and growth of the Internet as a specific form of information technology, and examine some issues facing it in its

[19] http://www.bbc.co.uk/home/i/ accessed 01 Mar 06.

[20] G Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report no 116, March 2004, 1.

future. By doing so, it will be shown that the Internet has had arguably greater effects than any other mediated form of communication in the areas of access and content. The drawbacks faced by the Internet in terms of trust, credibility and usefulness will be examined in detail later.

History of the Internet

The first use of the Internet is generally acknowledged as July 1977, when computers of the US Advanced Projects Research Agency (ARPA) transmitted a message over a total of 94000 miles of satellite, radio and land-line telephone networks.[21] This technology was adapted by the *Conseil Europeen pour la Recherché Nucleaire* (CERN) in order to link laboratories in the United Kingdom, France and Italy. In 1989, Tim Berners-Lee created the programming language necessary to link servers to common protocols which allowed access to shared data from multiple sites. By 1993, the World Wide Web, as it was then termed, had a total of 50 websites, but was still heavily in the world of academia.[22] It was not until the web was presented to the National Centre for Supercomputing Applications (NCSA) that growth took off. By January 1994, the Internet had some 2 million users and grew at 11% per week. The arrival of Microsoft's Internet Explorer in 1995 fuelled this exponential boom. Additionally, the birth of AOL and CompuServe in 1995-96 led to a 100-fold increase in Internet traffic, largely in conjunction with the introduction of graphical content on the Web.[23] By 1999, Internet traffic was doubling every 100 days, with some 65000 new websites per hour and a predicted 1 billion users by 2005.[24] In fact, by 2006, the total number of Internet users was over 1.1 billion.[25]

---

[21] No author cited, Oxford Brookes University, *History of the Web*, Oxford Brookes University, 2002, 11.

[22] Ibid, 28.

[23] K Coffman and A Odlyzko, *Growth of the Internet*, report for AT&T Labs – Research, July 2001, 27.

[24] Ibid, 29.

It is therefore no surprise that McQuail cites the "…harnessing power of the computer"[26] as one of the main drivers for what he terms "The Communications Revolution: 'New' Media versus Old"[27]. The rise of information technology has led to greater interactivity; the ability to "create" media, especially with the rise of digital imaging has blurred the boundaries and encouraged freedom of personal expression to a hitherto unseen degree. Also of note are the social networks that form around the "new" media. Internet chat rooms allow anonymous communication instantly, globally and in a secure fashion: a simple Google search revealed over forty-nine million chat rooms currently in operation. However, improvements in electronics may well shift the balance away from the home computer onto the cell phone. Its ability to mix voice, text messaging, Wireless Application Protocols (WAP) Internet services, digital imaging and now television broadcast receipt may well lead to a even more mobile social network as these services are no longer tied to the home or indeed to the mobile computer. However, whilst cell phone technology will be covered in more detail later, it is important here to focus on the Internet as one of McQuail's "New" media in order to further determine why it is has become so important.

Uses of the Internet

One has only to look at our own use of the Internet to realise its usefulness. Banking; keeping in touch with friends, family and co-workers; reading the daily news or sports results and researching a new purchase are just a few examples. Four main areas for Internet use have

---

[25] Internet Usage Statistics, http://www.internetworldstats.com/stats.htm accessed 6 March 2006.

[26] McQuail, *Mass Communication Theory*, 38.

[27] Ibid.

been adapted from McQuail's four uses for mediated communications, using as basis what McQuail terms "gratification theory."[28]

The first is "information", where the Internet is used to educate us in certain areas, such as learning more about the world, seeking advice on practical matters, or fulfilling our curiosity. The second factor is "personal identity". From watching television we may come to associate an actor character with our own. For example, in a comedy, all the actors have different personalities, the audience imagines or desires that resembling them. This has developed in a similar fashion with the rise of "online gaming" over the Internet, whereby users come to associate themselves with game characters in fantasy or combat games: the use of pseudonyms by online gamers is evidence of this. The danger here is that this depersonalization makes it increasingly difficult to separate fantasy from reality. One chilling example can be found in the so-called " Suicide Bomber Game"[29], where "players" cast themselves in the role of a suicide bomber in order to kill and injure men, women and children. The third usage of the Internet is "integration and social interaction", and refers to gaining insight into the situations of other people, in order to achieve a sense of belonging. For example, when watching a film, we may get very emotional because we experience a sense of connection to the plot, and experience symptoms like crying, or covering our eyes. A similar phenomenon can be seen in the rise of the Internet chat room described earlier, or by growth in the number of web-based logs, or "blogs". These online diaries and billboards allow freedom of expression and interaction in a more open forum than a chat room: a simple Google search for "blogs" on terrorism revealed some 536,000

[28]Internet Audiences - Key Theorists: Denis McQuail http://wiki.media-culture.org.au/index.php/Internet_Audiences_-_Key_Theorists:_Denis_McQuail accessed 02 March 2006.

[29] http://www.newgrounds.com/portal/view.php?id=50323 accessed 12 March 2006.

hits. The Internet also facilitates us in our personal relationship with friends as we are able to relate and discuss details of media texts that we like in common with our friends: a recent example of this is the rise of the "Podcast", an internet broadcast designed to be recorded and viewed, or listened to a digital music player. The effect of sharing music and images in this fashion has been the subject of research by the Georgia Institute of Technology[30]. The fourth usage of the Internet is "entertainment", that is, using it for purposes of obtaining pleasure and enjoyment, or escapism. For example the Internet allows access to many nefarious sites where we end up going into a new world of fantasy, diverting attention from our problems when we are free and even sometimes acquiring emotional release. These could be through viewing pornographic, violent or subversive sites, accessible to any age group, whose content would be unthinkable on any other form of mediated communication.

This freedom of access is aided by the lack of legislation regarding content on the Internet. There is a degree of self-regulation on the part of large Internet service providers (ISPs), search engines and so called "hacktivists", anonymous users who hack for political cause using the Internet as a forum for electronic civil disobedience. An example of direct action by the latter is given by Conway[31], who describes the actions of Internet protestors against the Institute for Global Communications (IGC). IGC hosted the Web version of the journal *Euskal Herria*, run by the Basque separatist group ETA. Following the assassination of a popular councilor in Northern Spain, protestors bombarded IGC with thousands of spurious or "spam" e-mails, filed

[30] Voida et al, *Listening In: Practices Surrounding iTunes Music Sharing*, University of Gerogia, presented at CHI 2005, April 2-7 2005, www-static.cc.gatech.edu/~amyvoida/listeningIn-chi05.pdf accessed 05 March 2006.

[31] M Conway, *Reality Bytes: Cyberterrorism and Terrorist Use of the Internet*, paper presented at Annual Meeting of the American Political Science Association, 2002, www.firstmonday.org/issues/issue7_11/conway/index.html accessed 22 November 2005.

hundreds of bogus credit card orders and threatened to employ similar tactics against any other company hosted by IGC. The site was withdrawn, but, acting in the interests of freedom of speech, IGC allowed the site to be copied by other ISPs and the journal reappeared the next day hosted by servers on three different continents.

Legislative Restrictions on Internet Use

More recently, however, following the terrorist attacks against the US on September 11, 2001, the US Congress passed the USA PATROIT Act, which allowed law enforcement agencies to monitor an individual's Internet and e-mail usage, subject to the granting of a court order.[32] This allowed ISPs to divulge records or other information pertaining to a subscriber if they reasonably believe there is danger of death or serious physical injury. This threshold of "reasonably believe" was subsequently lowered by the Cyber Security Amendment Act of 2002, to that of a "good faith" belief, which could be reported to any Federal, state or local government entity, as opposed to a law enforcement agency[33]. Lawmakers were also given greater authority to gain access to electronic financial transactions, largely to target those who illegally launder money[34]. However, it is important to note that even with this legislation, action by ISPs is still voluntary; in addition, privacy campaigners and civil liberties organisations have vowed to closely monitor these legislative acts to ensure that the rights of the individual are not at risk[35].

---

[32] Smith et al, *Internet: An Overview of Key technology Policy Issues Affecting Its Use and Growth*, CRS Report for Congress, (Washington: US Library of Congress, 2004), 5.

[33] Ibid, 5

[34] Ibid, 17.

[35] Ibid.

Summary of Internet Characteristics and Uses

Thus, so far, it has been demonstrated that the Internet offers an interactive mediated communication form, which is individually accessible, has almost unrestricted content, almost no regulation and offers the opportunity to project a psychological and sociological reaction across an expansive delocated network. It offers unparalleled rapid, global and almost unregulated access to information, which requires little or no technical skill to do so when compared with other forms of mediated communication:

Table 3.3 – Accessibility Determinants for Mediated Forms

Form/ characteristic	Book	Newspaper	Film	Broadcast		Internet
				Radio	Television	
Speed	Slow	Slow	Slow	Instantaneous	Instantaneous	Instantaneous
Reach	Global	National	Global	Global	National	Global
Regulation	High	High	High	Medium	High	Low
Availability	Good	Good	Good	Excellent	Excellent	Good
Skill	Low	Low	Low	None	None	Low

Source: Adapted from McQuail, *Mass Communication Theory*, by author

Thus, it can be argued that the Internet may well be a "revolutionary" form of general communication when compared with other mediated forms given its characteristics and subsuming of other media. However, for the purposes of this paper, it is being argued that, for terrorist purposes, it is an "evolutionary" form of communication with subsequent evolutionary, rather than revolutionary effects. Thus, having looked at the background and "revolution" in communications, it is now necessary to examine terrorism using the same construct in order to begin to build the framework to support this argument.

TERRORISM

INTRODUCTION

This section will attempt to define terrorism and use a short case study of Irish Terrorism in the period 1969-1990 in order to establish a historical baseline as to how terrorist groups communicated and the effect on their structures and activities. Terrorism in the contemporary era will then be examined, using the acts of terrorism of the bombing of the Alfred P. Murrah Federal Building in Oklahoma in 1995, the Omagh bomb in 1998, and finally the attacks against the World Trade Center and the Pentagon in 2001. Using these attacks will ensure that use of the Internet by both far-Right and Irish as well as Islamic fundamentalist terrorism are compared and contrasted. In doing so, the issues of how technology changes terrorists as well as how terrorists use the technology for their purposes will begin to be examined.

DEFINING TERRORISM

One of the major obstacles in any work on terrorism is defining "terrorism" itself. Howard and Sawyer propose that the change from political to ideological terrorism has made defining the act of terrorism more critical than ever[36]; Hoffman states his concern that "terrorism" has come to cover everything from narcotics to organised crime, from smuggling to physical attacks such as those on September 11, 2001[37]. His earliest available report for the RAND Corporation highlights this as a difficulty over two decades ago[38]. O'Neill concurs[39],

---

[36] R Howard and R Sawyer, *Terrorism and Counter-terrorism: Understanding the New Security Environment*, (Connecticut: McGraw-Hill/Dushkin, 2002), XV.

[37] Ibid, 3.

[38] Hoffman et al, *Trends in International Terrorism, 1982-1983*, report for RAND Corporation, http://www.rand.org/pubs/reports/2005/R3183.pdf accessed 9 March 2006.

highlighting the confusion that can occur when terms such as terrorism, guerrilla warfare, insurgency and revolutionary are used interchangeably, especially when their tactics are often indistinguishable: "…assassinations, bombings, arson, torture, mutilation, hijacking and kidnapping."[40]

Indeed, there is no universally accepted definition of terrorism. Lee and Perl point to the failure of international organisations to agree on a definition since "one man's terrorist is another man's freedom fighter."[41] Whilst they attempt to broadly adopt a definition of terrorism as "…politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents"[42], they do so recognising that this fails to take account of ideologically motivated violence, acts by individuals as opposed to groups, and attacks against combatant targets such as that carried out against the USS *Cole* in October 2000. O'Neill and Hoffman encounter similar difficulties again in attempting to define terrorism. The former defines terrorism as "…a form of warfare in which violence is directed primarily against non-combatants rather than operational military and police forces and economic assets."[43] This would rule out acts by the Provisional Irish Republican Army (PIRA) who systematically targeted British soldiers, the Royal Ulster Constabulary and the City of London, and, in a similar fashion, the 1983 PLO attack on a US Marine Corps barracks in Beirut. O'Neill defines terrorist attacks

---

[39] B O'Neill, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare*, (Virginia: Brassey's, 1990), 11.

[40] Ibid, 24.

[41] R Lee and R Perl, *Terrorism, the Future and US Foreign Policy*, (Washington: Congressional Research Service, 2002), 4.

[42] Ibid, 41.

[43] Ibid.

executed by non-state actors outside the borders of their own country as *transnational* terrorism, with state-sponsored acts being *international* terrorism[44]. In contrast, however, Hoffman originally defined international terrorism as "…incidents in which terrorists [state or non-state] go abroad to strike their targets, select victims or targets that have connections with a foreign state or create international incidents by attacking airline passengers, personnel or equipment."[45]

Common Definitions of Terrorism

Where, then, does one turn to for a definition? Schmidt[46] devoted more than a hundred pages to examining more than a hundred different definitions of terrorism in order to find a broadly acceptable, reasonably comprehensive explanation of the word. The following table brings together some of the common definitions in order to select the most suitable for the purposes of this paper:

[44] O'Neill, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare*, 11.

[45] Hoffman et al, *Trends in International Terrorism, 1982-1983*.

[46] Schmidt et al, *Political terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, (New Brunswick: Transaction, 1988).

Table 4.1 – Common Definitions of Terrorism

Author	Definition
Bruguiere	A form of war, a low intensity and circumventing strategy, [which] thrives outside the realm of the state to fight it in the name of an ideology, of a political reasoning or within the frame of a geopolitical claim[47].
Arquilla	Ways to spread fear and alarm by means of surreptitious, surgical and asymmetric strikes[48].
US State Department	Premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience[49].
US Federal Bureau of Investigation	The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives[50].
US Department of Defence	The unlawful use of – or threatened use of – force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious or ideological objectives[51].
Hoffman (1983)	Violence or the threat of violence calculated to cause an atmosphere of fear or alarm[52].
Hoffman (2002)	The deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change[53].

Source: Adapted from Hoffman, *Defining Terrorism*, by author

For the purposes of this paper, Hoffman's 2002 definition of terrorism will be used as the standard; although it could be classed as incomplete as it does not mention religious, ideological or social aims, it is the issue of *exploitation* that makes it important for studying the effects of

[47] JL Bruguiere, *Terrorism: Threats and Responses*, Occasional Paper prepared for The Geneva Centre for Security Policy, Geneva, May 2001, http://www.gcsp.ch/e/publications/Other-pubs/Occ-papers/2001/31-Bruguiere.pdf accessed 28 November 2005.

[48] Arquilla et al, *Information Age Terrorism*, 185.

[49] Hoffman, "Defining Terrorism" in *Terrorism and Counter-terrorism: Understanding the New Security Environment*, 20.

[50] Ibid.

[51] Ibid, 21.

[52] Hoffman et al, *Trends in International Terrorism*, 1982-1983.

[53] Hoffman, "Defining Terrorism" in *Terrorism and Counter-terrorism: Understanding the New Security Environment*, 21.

communication on terrorists, their structures and activities. As Jenkins states, "Terrorists do not want a lot of people dead, just a lot of people watching."[54]

[54] R Howard and R Sawyer, *Terrorism and Counter-terrorism: Understanding the New Security Environment*, xxii.

IRISH REPUBLICAN TERRORISM 1969-1991

INTRODUCTION

In order to establish a historical baseline in the pre-Internet era to demonstrate how terrorists communicated, and arguably were structured and carried out their activities as a result of this, the Provisional Irish Republican Army (PIRA) will be used as a case study. Equally important is the second order question that will begin to be answered: not just *how* terrorists communicated, but *why* they communicated. Defining the reasons why terrorists communicate and the effects of this – and these effects being denied - will then lead into an examination of why the Internet appears to offer an advantage for their purposes.

From the Easter Uprising in 1916 in Dublin, where PIRA members did nothing more than occupy the main Post Office, the issue of terrorism in Ireland has been a vexing one for the British Government until the signing of the IRA "ceasefire" in 2005. Although PIRA's history dates back from 1916, through the Irish Civil War of 1922, it is the situation from 1969 onwards that is most relevant for the purposes of this paper.

Since the deployment of British troops to Northern Ireland in 1969 to prevent sectarian attacks on the Catholic minority, the division between Catholics and Protestants in Northern Ireland has been demarked by the existence of paramilitary groups on each side. PIRA was formed as the armed wing of Sinn Fein, the legal political entity dedicated to the removal of British Forces from Northern Ireland and unifying the country. PIRA drew its ideological strength from the Catholic church's emphasis on community, solidarity, and the unquestioning acceptance of hierarchy. This resulted in PIRA being viewed as a "…highly disciplined and

structured "secret army" whose campaign design involved "…random murder and selective targeting, state-sponsored terror…psychopathic murder and torture."[55] Despite ceasefires in the late 1970's, high profile bombings in both Northern Ireland, the British mainland and British bases in Germany have been a trademark of PIRA's campaign. These so-called "spectaculars" included the assassination of Lord Louis Mountbatten on board his yacht in 1979; the Brighton Hotel bombing during the Conservative Party Conference in 1984, which claimed the lives of five people; city centre bombings in Guildford, Birmingham and Manchester, and the Baltic Exchange attack in the City of London in 1992. As an organisation, it has been involved with the Soviet Union for training, Libya for supplies of arms – demonstrated by the seizure of massive quantities of arms and ammunition aboard the freighter *Eksund* in 1987 - and the Palestinian Liberation Organisation (PLO) as a provider of training. It also enjoyed significant financial support from Irish-American communities in the US.

However, despite almost three thousand deaths at the hands of PIRA over this period, the largest death toll in a single attack was no more than twenty-nine. Indeed, Gearson[56] believes it was only the attacks on economic centres in the City of London at the culmination of the mainland bombing campaign that began to effect strategic change, although this was stalled somewhat by the attempt on the life of the then British Prime Minister John Major and his War Cabinet by a PIRA mortar attack in February 1991.

Organisation and Structure

[55] C Crawford, *Inside the UDA: Volunteers and Violence*, (London: Pluto Press, 2003), 5.

[56] Gearson, *The Nature of Modern Terrorism*, 14.

How, then, were PIRA organised during the period 1969-1991? Boyne[57] estimated the strength of the IRA at about 400 hard-core activists, with perhaps a similar number of "auxiliary" or "second-line" activists who could be called on in a crisis. Most of these members, known as "volunteers" were concentrated in Northern Ireland, although a smaller number were based in the Republic of Ireland and there were also small cells in the UK. IRA cells may have also operated from time to time in the USA and other overseas locations. Many of these volunteers were not necessarily full-time but also worked at other occupations.

Boyne also believed there to be a hard core of about 40 middle-ranking members of the PIRA who made operational decisions, who were spread amongst the upper hierarchy. The seven-person Army Council conducted the day-to-day running of PIRA. Members of the council always include the chief of staff, the adjutant general and the quartermaster general.
The General Army Convention (GAC) was the supreme authority of PIRA and met rarely, around once every two years. Delegates to the GAC included PIRA members selected by various units within the organisation as well as the members of the Army Council. When the GAC was not in session, the Army Council was the supreme authority of the IRA. The planning and implementation of Army Council decisions was carried out by the General Headquarters (GHQ) Staff, which acted as the link between the Council and Northern and Southern commands. The Northern Command covered Northern Ireland as well as the Republic's border counties. The Northern Command had at least five brigades - Belfast, Derry, Donegal, Armagh and Tyrone-Monaghan. The Southern Command, which covered 21 counties, had a much smaller number of personnel spread around the Republic: a Dublin brigade and a number of smaller units in the provinces. Each command had its own commanding officer, director of operations and

[57] S Boyne, "Uncovering the Irish Republican Army", *Janes Intelligence Review*, August 1996.

quartermaster. In the late 1970s, the IRA reorganised into "cells" who, theoretically, could not compromise the whole movement if caught. These cells within the operational arm were known as Active Service Units (ASUs) each with usually five to eight members. It was estimated by Boyne[58] that there were some thirty-five to forty ASUs capable of carrying out operations.

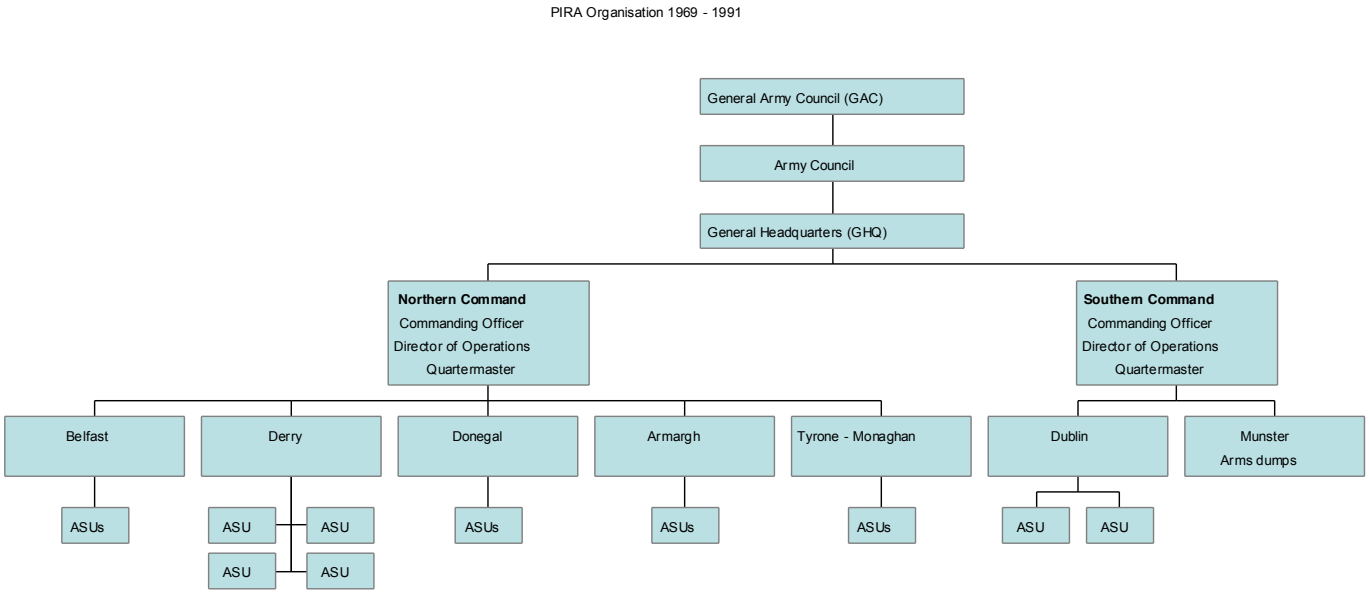


Figure 4.1 – PIRA Organisation 1969 – 1991, condensed from Boyne[59]

This hierarchical organisational structure shown above served a useful purpose, in that comparatively few members knew what other members were up to, especially so at the ASU level. This, and the relatively low numbers of personnel involved, made the organisation difficult to infiltrate, although British security forces did have some success. The structure had been in place long before communications technology such as television or telephones became commonplace: there is no issue of cause or effect of communications upon the structure.

[58] Ibid.

[59] Note that only the Derry Brigade has the cell structure of the ASUs shown for clarity.

PIRA Communications

Turning now to study how PIRA communicated, care must be taken to state exactly what we are looking at. For PIRA, *internal* communication was relatively straightforward, with face-to-face meetings being the norm, given the significant electronic communications monitoring infrastructure set in place throughout Northern Ireland by British security forces. Cell phones were uncommon, the Internet was not in place and the public telephone network was subject to extensive wiretapping. Meetings between terrorist players often took place in broad daylight at political rallies or marches. In order to prevent compromise, ASUs had no knowledge of the movements or activities of other cells and communication between ASUs – indeed, if necessary – was carried out via the Brigade commander. It is in PIRA's *external* communications that we begin to see an interlinking of communication and activities: for terrorists, a successful act of violence *is* communication. As Arthur[60] stated:

> … simply put, violence is used as a communicative dimension. It is saying to the state or to government, "We are here. You have to talk to us. If we have to bomb our way to a negotiating table, we will." … the violence was a classic example of armed propaganda. There always was the belief that the death of one British soldier was worth at least, in propaganda terms, ten policemen from Northern Ireland, because in Britain itself, the British mainland, the demand to get out would grow.

Rubenstein concurs, citing his belief that acts of terror by protest groups can be considered indirect efforts at communication that use the news media to inform the public about the motives of the group in an effort to "give violent voice to the voiceless, and to awaken their sleeping brethren to the necessity of mass action."[61]

---

[60] P Arthur, *The Conflict*, transcript of interview for "Behind the Mask", http://www.pbs.org/wgbh/pages/frontline/shows/ira/conflict/ accessed 9 March 2006.

[61] R Rubenstein, "Rebellion in America: The fire next time", in *Violence in America: Protest, Rebellion and Reform*, ed T Gurr, (Newbury Park: Sage, 1989), 323.

Taking examples from Wright[62] and Cohen[63], it can be seen that PIRA's external communication, whether involving violent acts or not, had six main purposes:

Publicity. Curtis noted that terrorism was "theatre" and that it depended for survival on "the oxygen of publicity"[64]. This view is echoed by Damphousse[65], who cites Schmid's view that "terrorism cannot exist without communication." One of the features to note about PIRA's publicity campaign is it's claiming of responsibility for terrorist attacks. One such example of this is PIRA's immediate statement after the Brighton bombing in 1984, with the words "Today we were unlucky, but remember we only have to be lucky once. You have to be lucky always."[66] In doing so, the perpetrators of this incident exploited the publicity generated by a successful attack on the complete Cabinet of the Conservative Government.

Propaganda. Propaganda is used by terrorist groups to inform the general public or other specific groups in order to make them understand the necessity or urgency of the terrorist's actions. This could include leaflets, fliers, posters and newspapers, as described by Damphousse, but she also cites the concern that propaganda distributed to the general public in this way may well become discarded. However, PIRA's targeting of youths

---

[62] J Wright, *Terrorist Propaganda: The Red Army Faction and the Provisional IRA 1968-1986*, (New York: St Martin's, 1990).

[63] F Cohen, "Terrorism and Cyberspace", *Network Security*, Vol 5, 2002.

[64] L Curtis, *Ireland: The Propaganda War* (London: Pluto Press, 1984), 142-144.

[65] K Damphousse and B Smith "The Internet: A Terrorist Medium for the 21st Century", in *The Future of Terrorism: Violence in the New Millenium*, ed H Kushner, (California: Sage, 1998), 209.

[66] http://news.bbc.co.uk/1/hi/uk/1201738.stm accessed 9 March 2006.

during emotive events in Northern Ireland, such as Loyalist marches, ensured that their target audience was reached.

Recruitment. Propaganda in turn provides the incentive for others to engage in violence through joining the organisation responsible.

Fundraising. Aside from the proceeds of organised crime, such as extortion, protection rackets and smuggling, one of PIRAs most important sources of fundraising were American donations. Arthur[67] describes the 1973 FBI report acknowledging what he terms the "grass roots" of New York and Southern Boston funding PIRA activities. This was recognised as a concern in a meeting in 1975 described by the Irish Independent, in which officials of the British Governments Northern Ireland Office recognised "there is a unique emotive element to be considered in America: the strong, active Irish strain which is recognised at the highest level as a formidable pressure group and is deeply entrenched in Congress."[68] McKinley[69] estimated that NORAID, the American fundraising group, donated up to $800,000 annually to Sinn Fein.

Political Action. Sinn Fein, the political wing of PIRA, developed its twin track strategy of politics and violence in 1981 following the death of hunger strike

---

[67] P Arthur, *The Conflict*.

[68] http://www.unison.ie/irish_independent/stories.php3?ca=9&si=1534497&issue_id=13482 accessed 9 March 2005.

[69] M McKinley, "The Irish Republican Army and Terror International: An Inquiry into the Material Aspects of the First Fifteen Years" in P Wilkinson and A.M Stewart, eds. *Contemporary Research on Terrorism* (Aberdeen: Aberdeen University Press, 1987), 203-218.

protestor and PIRA member Bobby Sands. Morrison, at a speech in Belfast, asked the now infamous rhetorical question "Who here really believes we can win the war through the ballot box? But will anyone here object if, with a ballot paper in one hand and the Armalite in the other, we take power in Ireland?"[70] Thus, by separating PIRA and Sinn Fein, Morrison opened the door for legitimate political action by Sinn Fein Councillors and, from 1983, Sinn Fein Members of Parliament in Westminster, to have legitimate cause to communicate PIRA's message. However, despite the success of the "good cop/bad cop" strategy of Sinn Fein and PIRA, tension between those keen to continue armed struggle and those more willing to put their faith in the political process eventually led to a split in PIRA.

Warning. PIRA consistently gave telephone calls issuing coded warnings to journalists, local authorities or security forces prior to attacks against civilian infrastructure or economic targets. No warnings were given before attacking military targets.

The Media Ban

The effect of limiting external communication and the impact on these six purposes can be illustrated in the British Government's response to PIRA attacks in 1987-88 by the media ban imposed on coverage of PIRA and Sinn Fein activities. 1987 saw the deaths of 11 Protestants at a Remembrance Day service in Eniskillen, a small Northern Irish border town; 1988 saw the televised murder of two British soldiers who had accidentally driven into the route of a funeral march for a PIRA member killed by Loyalist gunman Michael Stone. Emotions were high:

[70] D Morrison, cited in *The Irish Post*, http://archives.tcm.ie/businesspost/2001/11/04/story390373828.asp accessed 9 March 2005.

Stone's attack was carried out at the funeral of three PIRA members who had been shot by British Special Forces in Gibraltar. The two soldiers were dragged from their car, stripped, beaten by a mob, and subsequently handed over to PIRA members at the march, who then shot them with their own weapons. Both these attacks caused furore around the world, with the then Prime Minister Margaret Thatcher banning media interviews with Sinn Fein members, television coverage of PIRA funerals and reporting of court proceedings involving PIRA members. As the then Home Secretary, Douglas Hurd stated in the House of Commons:

> The terrorists themselves draw support and sustenance from having access to radio and television, and from addressing their views more directly to the population at large than is possible through the press. The Government has decided that the time has now come to deny this easy platform to those who use it to propagate terrorism[71].

The short-term effect of the media ban was dramatic. Denied the "oxygen of publicity", PIRAs contact with the media declined sharply[72] and donations from NORAID dropped substantially. However, the long-term effect was less certain. Although programmes were not made and certain others cancelled, this is difficult to measure, partly due to the refusal of the broadcasters to monitor it[73]. The ban was lifted temporarily for local elections in Northern Ireland in 1989 and national broadcasters began to use actors for voiceovers during interviews with Sinn Fein officials. Indeed, the ban may have forced PIRA to resort back to violence as a means of communication to get its message across. High profile bombings of the Royal Marines School of Music at Deal, Kent; the murder of a wife of a British soldier in Dortmund and the car bomb attack on a British soldier in Hanover all took pace without any coded warning. These

---

[71] The Rt Hon Douglas Hurd, MP, cited by E Moloney, "Closing down the airwaves: the story of the Broadcasting Ban" in *The Media and Northern Ireland* ed by B Rolston, (McMillan, Basingstoke: 1991), Appendix.

[72] Ibid, 20.

[73] Ibid, 21.

attacks, and the release of the "Guildford Four" wrongly convicted during the 1970s for a PIRA bombing of a pub, all occurred in 1989. Without a single interview of a Sinn Fein member or any coverage of PIRA funerals, high profile media coverage of these attacks gave the Irish Republican cause all the publicity and propaganda it needed, proving the earlier comments of Arthur and Rubenstein.

TERRORIST USE OF THE INTERNET

INTRODUCTION

Having established a historical baseline for terrorist communications in the pre-Internet era, methods of internal communication and the six main purposes of external communications by PIRA, it is essential to examine how terrorists use the Internet in order to exploit this utility when compared with other communications means. Following this, two terrorist incidents in the contemporary era will be compared and contrasted to show how each used the Internet or other mediated forms of communication.

TERRORIST USES

Conway[74] has examined the work of numerous authors who propose categories for terrorist use of the Internet; an adapted version of her research is given below, along with the six purposes of communication for PIRA during the pre-Internet era as a means of comparison:

[74] M Conway, *Terrorist 'Use' of the Internet and Fighting Back*, prepared for Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Oxford Internet Institute (OII), Oxford University, 8-10 September, 2005.

Table 5.1 – Terrorist Uses of the Internet

Author	PIRA	Furnell and Warren[75]	Damphousse[76]	Thomas[77]	Weinmann[78]
Use	• Publicity • Propaganda • Fundraising • Political action • Recruitment • Warning	• Propaganda and publicity • Fundraising • Information dissemination • Secure communications	• Propaganda machines • Communication devices • Virtual graffiti • Support activities	• Profiling • Propaganda • Anonymous/ covert communication • Generating "cyberfear" • Finance • Command and control • Mobilisation and recruitment • Information gathering • Mitigation of risk • Theft or manipulation of data	• Psychological warfare • Publicity and propaganda • Data mining • Fundraising • Recruitment and mobilisation • Networking • Sharing information • Planning and coordination

Source: Adapted From Conway, *Terrorist "Use" of the Internet and Fighting Back*

From this, Conway surmised five main functions. These are:

Information Provision. Efforts by terrorists to engage in publicity, propaganda and psychological warfare.

Recruitment. Efforts to recruit and mobilise sympathisers to actively support terrorist cases or activities.

Financing. Direct solicitation via terrorist websites, exploitation of e-commerce tools and entities and exploitation of charities and fronts.

[75] S Furnell and M Warren, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium", *Computers and Security*, no 18, 1999.

[76] K Damphousse and B Smith *The Internet…* 214-220

[77] TL Thomas, "Al-Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, Spring 2003.

[78] Weinmann, *www.terror.net*. *How Modern Terrorism Uses the Internet*, 5-11.

Information Gathering. Data mining, sharing information and exploitation of open sources.

Networking. Transforming organisational structures, planning and coordination, and mitigation of risk.

By describing each of these uses in more detail, the foundations will be laid to develop understanding of how far-right and Islamic terrorists have structured their organisation and conducted their activities in order to maximise benefits from using the Internet in these five areas.

Information Provision

This function relates to terrorist activities in support of publicity, propaganda and psychological warfare. Conway[79] describes how terrorists use the Internet to carry information such as profiles of leaders, manifestos and historical details in order to draw attention to and romanticise their cause. Weinmann[80] also points out that the lack of what he terms a "selection threshold", which was outlined in Table 3.2, results in content being available on terrorist websites which mainstream media would not countenance. One example of this is cited by Thomas[81], namely the use of the Internet to replay the images of the beheading of Daniel Perl by his Pakistani captors. These functions, as Conway suggests, clearly benefit from the instantaneous speed and global reach outlined in Table 3.3. The advent of broadband Internet

[79] M Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

[80] G Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, 5-11.

[81] Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*.

has made the transmission of video images increasingly simple, with almost television-like quality. A media ban of the type imposed on PIRA and Sinn Fein described in the earlier section would have little effect, as the Internet allows terrorists an unprecedented degree of control over their own message: the creation function in the communication model can be performed with as little as a video camera and a laptop computer, yet still reach millions. One example of this is given by Arquilla[82], who describes the activities of the anti-Israeli group Hezbollah. The group manages three websites: one for its central press office, one dedicated to describing its attacks on Israeli targets and a third for general news and information. The site dedicated to descriptions of attacks on Israel[83] offers extensive video footage of recent attacks, articles describing the activities of Jewish and Israeli terrorists and extensive writings from Sayyed Hassan Nasrollah, Hezbollah's Secretary General. The latter in particular describe his role as a statesman, scholar, and man of peace: his organisation is armed only for "peace, stability and national unity."[84] Desoite this, Hezbollah is thought to have been responsible for the bombing of a US Marine Corps barracks in Beirut and the 1985 TWA airliner hijacking.

One intriguing aspect of websites seeking publicity for terrorist activities is the use of semantics as a persuasive tool. The differing terms used by terrorist groups, and, subsequently, the media to describe their activities and members has been explored by Lockyer[85]. He notes that mediated communication forms may adopt the language of the terrorist inadvertently or

---

[82] Arquilla et al, *Information Age Terrorism*, 179-185.

[83] http://www.moqawama.org/english/index.php accessed 12 March 2006.

[84] http://www.moqawama.org/english/_amenspeeches.php?filename=2005111214381211 accessed 12 March 2006.

[85] A Lockyer, *The Relationship between the Media and Terrorism*, (Canberra: Australian National University Press, 2003), 2.

deliberately as a result of editorial bias. The BBC courted recent controversy following the London July 7 2005 bombings, where the terrorists responsible for the attack were described as "bombers" in accordance with their guidelines on terror reporting[86]:

> Our credibility is undermined by the careless use of words which carry emotional or value judgements. The word "terrorist" itself can be a barrier rather than an aid to understanding. We should try to avoid the term, without attribution. We should let other people characterise while we report the facts as we know them. We should use words which specifically describe the perpetrator such as "bomber", "attacker", "gunman", "kidnapper", "insurgent", and "militant".

Terrorist websites do not have the limitation of editorial guidelines in order to ensure integrity, and therefore can gain an advantage over other mediated forms by using semantics or synonyms to ensure that their members are portrayed in Internet messages in the best possible light. One such website, the Palestinian Information Centre, a suspected front for Hamas, describes the results of an Israeli air strike in which two suspected terrorists were killed as: "Two Islamic Jihad activists and an eight-year-old child were killed in an Israeli air strike in Gaza on Monday, Palestinian medics and witnesses said."[87] In one sentence, this portrays Islamic Jihad members as "activists" and clearly implicates Israel in the killing of children.

Recruitment

This is the next step after getting the attention of potential followers and relates to efforts to recruit and mobilise sympathisers to actively support terrorist cases or activities, drawing them into hands-on work for the group. It is the interactivity that allows a clear advantage for the

[86] Cited by N Cohen, *The Observer*, 17 July 2005, http://observer.guardian.co.uk/comment/story/0,6903,1530248,00.html accessed 12 March 2006.

[87] http://www.palestine-info.co.uk/am/publish/ accessed 12 March 2006.

Internet over other forms of mediated communication for recruiting purposes. Conway[88] gives examples of this where Internet chat rooms are used for vetting potential applicants. Weinmann[89] gives further examples, citing an exchange between two users: a potential Al-Qaeda member, seeking to go to Iraq for jihad, and using the pseudonym "Redemption is Close" and his "groomer", "Merciless Terrorist", who gives him instructions on how to join the mujahideen. Propaganda videos, terrorist manuals and software are exchanged: the latter involves downloading PalTalk, which allows anonymous communication without fear of being monitored in chat rooms. The Dartmouth-based Institute for Security Technology Studies (ISTS) have conducted extensive research into the contents of video footage of terrorist training camps designed to recruit would be followers[90]. They found several remarkable similarities between these and, ironically, the then-current US Army recruiting video.

Just as important as *how* individuals are recruited is the issue of *which* individuals are recruited. As early as 1995, Al-Qaeda was recruiting students in American universities undergoing training in computer science. One such case is cited by Weinmann[91], where Ziyad Khalil, largely through his operation of a Muslim website, came to the attention of Osama Bin Landen and was subsequently recruited as Al-Qaeda's US technical procurement officer. ISTS state clearly that, in 1999, Osama Bin Laden was clearly recruiting "…highly skilled professionals in the fields of engineering, medicine, chemistry, physics, computer programming,

---

[88] Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

[89] Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, 8.

[90] Technical Analysis Group, ISTS, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, (Dartmouth: Dartmouth College, 2004), 18.

[91] Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, 8.

communications and so forth…"[92] More recently, Kohlmann[93] describes the case of Intel engineer Maher Mofeid Hawash, who pled guilty in August 2003 to charges of conspiring to join a group of individuals who sought to join the Taliban in fighting against the U.S. military. Hawash and the others conspirators in the "Portland 7" jihad cell were "prepared to take up arms and die as martyrs if necessary to defend the Taliban government in Afghanistan." Prior to his days as a would-be soldier for the Taliban, Mike Hawash worked as an engineer on Intel's MMX technology software team. This emphasises both the continuing recruitment of highly skilled professionals, but also the clear intent to continue to use the Internet for recruiting purposes.

Financing

This function relates to direct solicitation via terrorist websites, exploitation of e-commerce tools and entities and exploitation of charities and fronts. Direct solicitation can occur through general statements requesting donations, or a more targeted form which requests immediate Internet payments, often giving bank details: Weinmann[94] cites an example where PIRA's home page allowed credit card donations: this is still the case on the *Solar General* right-wing site[95]. Online sales of books, t-shirts and so forth are described by Conway as another means of fundraising: Aryan Wear, a far-Right website run in support of American "white power" groups sells DVDs, t-shirts, CDs, Nazi symbols, flags and badges[96]. Another far-Right radio station site run by

---

[92]ISTS, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, 19.

[93] E Kohlmann, *Legal and Investigative Loopholes in Modern Cyberterrorism Cases*, (master's thesis, University of Pennsylvania Law School, 2003), 22.

[94]Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, 7.

[95] http://www.solargeneral.com/ accessed 12 March 2006.

[96] http://aryanwear.com/product_info.php?products_id=469&osCsid=cdc3ee131abe674c8a4dc08ab95d9b87 accessed 12 Mar 2006.

Turner even sells advertising space at $35 per advertisement and cigars "in support of freedom."[97] Exploitation of e-commerce tools involves mainly credit card fraud and the establishment of Internet-related front businesses to provide communications, funds and support to terrorist groups. For example, Thomas[98] notes that Ricard, one of France's top anti-terrorism investigators, believed that many Islamic terrorist activities in North America and Europe were financed in this way. Additionally, Conway[99] cites the example of Infocom, a Texas based ISP whose capital was provided by the wife of a Hamas leader. Finally, exploitation of charities and fronts involves the creation of charitable websites whose contents may not immediately point to their true purpose. The Anti-Defamation League's report[100] into the use of the Internet by Islamic terrorists gives three such charities: Al-Shahid, Al-Emdad and Al-Jarha. Noting that it is a duty of observant Muslims to make charitable donations regularly, each website requests "sponsorship" either of a wounded Hezbollah "soldier", or the orphan or widow of a suicide bomber or "martyr". Donations requested range from $25 to $360 dollars per month. However, Conway clearly states that as well as advertising on websites, these charities also advertised in "sympathetic communities" press."[101] What advantage does the Internet offer over printed media? Several are proposed. The first has already been mentioned in the study of PIRA, that of being able to target more effectively those likely to donate: rather than printed material simply being discarded, websites offer permanence. This can be achieved through surreptitious means, such as a "cookie" or software implant leading Internet surfers back to the same site, or through

---

[97] http://www.halturnershow.com/index.html accessed 12 March 2006.

[98] Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*, 116.

[99] Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

[100] ADL, *Jihad Online: Islamic Terrorists and the Internet*, 2002.

[101] Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

"pop-ups", adverts for the charity which appear when surfing other websites. Since private access to the Internet requires significant financial investment through ownership of a computer, the chances of influencing those with disposable income is higher. Additionally, costs of maintaining a website are minimal compared to that of printed media. The audio-visual impact of a full colour website, often with accompanying speeches and poems, is far greater than that of a simple black-and-white printed advert. The Internet can be used with complete anonymity and freedom, allowing the legitimate charitable front to deny all knowledge of the terrorist's activities and without fear of printing presses being shut down.

Information Gathering

This function relates to the use of the Internet for Data mining, sharing information and exploitation of open sources. Thomas cites US Secretary of Defense Donald Rumsfeld's observation in January 2003 that an Al-Qaeda training manual stated "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information about the enemy."102 He went onto say that "…at more than 700 Gb, the DoD web-based data makes a vast readily available source of information on our DoD plans, programs and activities. One must conclude our enemies access DoD websites on a regular basis"[103] However, this is not a recent phenomenon: as early as 1998, Hamre wrote about the idea that the Web is a "potent instrument to obtain, correlate and evaluate an unprecedented volume of aggregated information regarding DOD capabilities."[104] The exponential growth of the Internet and the information available has made this problem even more acute. Google Earth, for example,

---

[102] Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*, 118.

[103] Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

[104] Hamre, cited at http://www.fas.org/sgp/news/2001/10/dier102601.html accessed 12 March 2006.

provided highly detailed three-dimensional satellite imagery of Olympic venues for the 2006 Winter Games in Turin, Italy. Whilst undoubtedly useful for tourists, such imagery can easily be of use to potential terrorists; proposed Olympic venues for the 2010 Winter Games in Vancouver, Canada can already be studied. As the satellite images are updated during construction of future venues, there is no need for a terrorist to run the risk of obtaining blueprints. Sweetman, a technological warfare expert with Jane's, the military and intelligence specialist publisher, said the images could enable terrorists in Iraq to pinpoint targets inside military bases, stating "Information gleaned from Google Earth can be of use to these people. They can use overhead images to get co-ordinates for a mortar attack or for a suicide bomber to try to figure out where a building is in the base so they don't get lost on their way in."[105] The growth of search engines, including Google, Lycos and Yahoo, has made it far easier to trawl for information. The Intelligence and Terrorism Information Centre at the Centre for Special Studies revealed in March 2005 how a search including any combination of Hamas, Gaza and Palestine immediately led to a website sponsored by and linked to the "al Qassam Battalions, the resistance website and the legend of jihad"[106]. However, given that the ITIC is in fact the "unofficial" website of the Israeli Intelligence community, the highlighting of this issue is unsurprising. ISTS describe[107] how, in 2001, laptops belonging to Al-Qaeda operatives were seized in Afghanistan. Intelligence officials found strings of "hits" on websites dealing with pipelines, emergency services dispatch control systems, and digital switches for water, power,

---

[105] B Sweetman, cited in *The Daily Telegraph*, "Insurgents Using Google Earth", *The Daily Telegraph*, 12 December 2005, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/12/18/ngoog18.xml accessed 13 March 2006.

[106] ITIC CSS Special Information Bulletin of 27 March 2005, http://www.terrorism-info.org.il/engsite/home/default.asp accessed 22 November 2005.

[107] ISTS, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, 43.

transport and communications grids. Ironically, the work of those attempting to combat terrorism has often made it easier. A Google search for *The Turner Dairies* the so-called "Bible of the Far Right", led to the discovery of the "Hate Directory"[108]: in an attempt to draw attention to the influence of the far-Right, this lists over 140 pages on websites, newsgroups and chat rooms, the majority of which can be accessed with a single mouse click. This allows inter-group communication and eases the task of any disaffected person searching for like-minded individuals.

As well as background information, the Internet offers the opportunity to search for information relating to more direct methods of action. A simple Google search revealed over 134,000 hits for "home-grown chemical warfare", and over a million for "simple biological warfare". As well as sharing information on how to create one's own simple chemical weapons and delivery systems, Web pages also give detailed plans used in response to use of such agents, allowing terrorists to maximise their effect by circumventing these plans. In addition, the Internet offers what Spafford termed "…a virtual worldwide training camp."[109] The website of the Search for International Terrorist Entities (SITE) Institute lists how jihad message boards have directed forum members to a manual covering subjects including explosives, unarmed combat, kidnapping and how to build-your-own devices, including remote control circuits and pistol silencers[110]. Again, this information can be downloaded with almost complete anonymity unless an ISP choose to monitor traffic on a home machine; the use of a public machine in a

---

[108] R Franklin, *The Hate Directory*, http://www.bcpl.net/~rfrankli/hatedir.pdf accessed 12 March 2006.

[109] E Spafford, cited by Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

[110] SITE Institute, *Jihadist Message Boards Link to Website Offering Advanced Military Training Manuals*, 25 February 2006, http://www.siteinstitute.org/bin/articles.cgi?ID=publications21805&Category=publications&Subcategory=0 accessed 12 March 2006.

library or Internet café reduces this risk. Most recently, despite the increased security measures applied to information technology, the BBC reported[111] how The Chicago Tribune compiled a list of 2,653 CIA employees, just by searching the Internet. The newspaper said it gathered the information from online services that compile public data that any fee-paying subscriber can access. Many of the agents are believed to be covert. The paper also located over two dozen "secret" facilities.

Networking

This is perhaps the most controversial purpose put forward for terrorist use of the Internet. Whilst networking will be described now, the issue of networked structures will be returned to later: there is considerable debate about what "networking" really means, whether it is completely attributable to information technology and whether it is such a revolution in terrorist means and methods as is being proposed.

Conway describes networking as relating to "…group's efforts to flatten their organisational structure and act in a more decentralised manner through use of the Internet, which allows dispersed actors to communicate quickly and at low cost."[112], and divides the idea of networking into transforming organisational structures and mitigation of risk. Thomas[113] uses networking as a basis for command and control, putting distance between those planning the

[111] BBC "Internet Blows CIA Agents Cover", http://news.bbc.co.uk/1/hi/world/americas/4799174.stm accessed 12 March 2006.

[112]Conway, *Terrorist 'Use' of the Internet and Fighting Back*.

[113] Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*, 118.

attack and their targets, and mobilising groups or diasporas. Weinmann[114] gives uses of networking as facilitating decentralisation and horizontal communication.

The main advocates of networking are Arquilla, Rondfelt and Zanini[115]. They propose that terrorists will continue to move away from hierarchical toward information-age network designs. Within groups, "great man" leadership will give way to flatter decentralised designs. Stand-alone groups will transition to transnational Internet-linked groups. This is encapsulated in a phenomenon they term "Netwar", where transnational terror networks develop "swarming" strategies to allow attacks from multiple directions on a single target, in "pulses" rather than "waves". They propose this is largely possible due to the development of network forms, doctrine and strategy attuned to the information age.

Networks essentially consist of "nodes". Each node could be a person, a cell, or an organisation. In order to show the difference between pre-information age and information age groups, two main types of structure are proposed: hierarchical and networked, with the latter further subdivided into chain, hub-and-spoke and all channel networks:

[114] Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, 9.

[115] Arquilla et al, *Information Age Terrorism* and "Networks, Netwar and Information Age Terrorism" in *Terrorism and Counter-terrorism: Understanding the New Security Environment*.

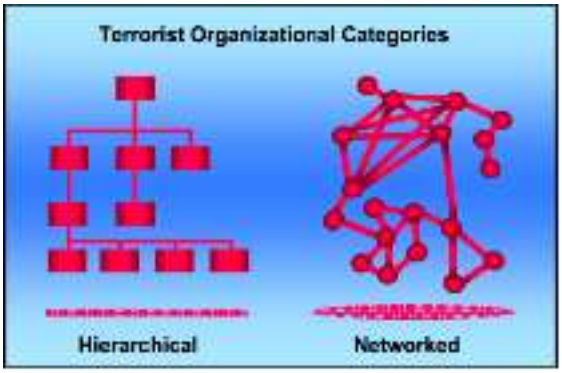


Figure 5.1 – Terrorist Organisational Categories

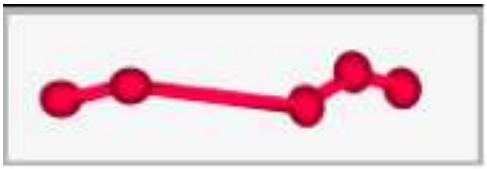


Figure 5.2 – Chain network

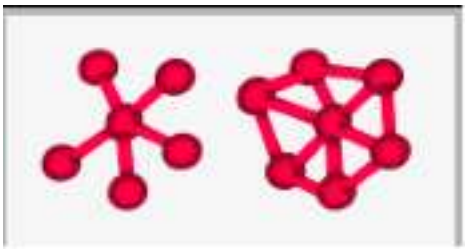


Figure 5.3 – Hub And Spoke Network

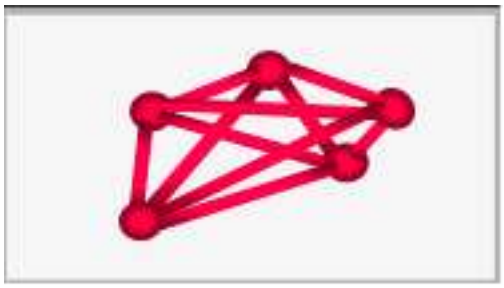


Figure 5.4 – All Channel Network

Source: *A Military Guide To Terrorism in the 21st Century*

In figure 5.2, the chain network, each node links to the next sequentially, with communication between nodes achieved by passing information down the line. In figure 5.3, the hub-and-wheel network, nodes communicate with one central node, or with one or two other nodes around the rim of the wheel. Finally, in figure 5.4, the all-channel network, all nodes are

interconnected, and the organisation is "flattened", with no recognisable hierarchy. Command, control and communications are distributed across the network. This all-channel network has been proposed as the one adopted by Islamic organisations by, for example, Dauderstadt, Weinmann and Gearson, in addition to Arquilla, Rondfelt and Zanini[116].

[116] M Dauderstadt, "Negotiating with Terrorists – an Option Not to be Forgotten", *Internationale Politik und Gesellschaft*, No. 3, 2004, 9-13, www.sre.gob.mx/imred/biblioteca/bol57/polinter.htm accessed 28 November 2005. See also Weinmann, *www.terror.net. How Modern Terrorism Uses the Internet*, 9, Gearson, *The Nature of Modern Terrorism*, 17 and Arquilla et al, *Information Age Terrorism*, 179-185.

TERRORISM IN THE CONTEMPORARY ERA

INTRODUCTION

Having briefly examined structure, communication and activities of PIRA in the pre-Internet era, it is now necessary to do the same for terrorist activities in the post Internet era, or the Information Age. Two main events will be briefly described, in order to compare and contrast the effects of the Internet on each. These are the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma, US and the attacks on New York and the Pentagon in 2001. The attacks chosen represent far-Right and Islamic terrorist activities respectively. By doing so, the evolution in terrorist communications, and the subsequent impact on structures and activities will begin to be demonstrated.

OKLAHOMA, 1995

On 19 April 1995, far-Right terrorists Timothy McVeigh and Terry Nichols destroyed the Alfred P. Murrah Federal Building in Oklahoma City with a massive truck bomb based on fertiliser explosive. 166 people were killed and hundreds more injured in what was, at the time, the largest terrorist attack ever on American soil. Two theories attempt to account for McVeighs actions[117]. The first proposes McVeigh blew up the building in pre-emptive retaliation for the execution of Richard Wayne Snell, a convicted member of the far-Right white supremacist group The Covenant, The Sword and the Arm of the Lord (CSA). The second proposes that McVeigh carried out the attack in response to the US Bureau of Alcohol, Tobacco and Firearms (ATF) siege at Waco, Texas, home of the Branch Davidians religious cult exactly two years earlier.

---

[117] M Hamm, "Terrorism, Hate Crime and Antigovernment Violence: A Review of the Research", in *The Future of Terrorism: Violence in the New Millennium*, 80-81.

McVeigh's and Nichol's attack raises a number of interesting issues with regard to terrorist communications and the impact of information technology on communications, structure and activities. The first is that, despite spending two years in College and scoring high marks on computers – including his use of the Internet - there is little evidence that information technology was used in the planning, coordination or execution of the attack. The majority of his communications were by public telephone, letter, or pamphlet. Secondly, the idea of networked cells without an established hierarchy, proposed as a direct result of the Information Age by Arquilla, Rondfelt and Zanini is clearly evident in influencing McVeigh's actions, but in this case has evolved without the influence of the Information Age.

The Role of Communication in the Oklahoma Attack

Turning to the first issue, that of McVeigh's use of communication, it can best be described as rudimentary. In late 1994, McVeigh sent a series of letters to his fellow conspirators: Terry Nichols and Michael Fortier. These crudely written letters describe McVeigh's plan to destroy a Federal building. McVeigh's sister, Jennifer, also received upwards of twenty letters from him, detailing his hatred of the Federal Government. In addition, Federal investigators traced records of over six hundred calls from a pre-paid calling card, which was used for communication between McVeigh, Nichols, and a host of Kansas distributors of fuel, fertiliser, chemicals and plastic barrels[118]. Given his skills with the Internet, which were reflected in his performance at business college, why did McVeigh choose not to use it? Firstly, this is to do with his purported belief that the Internet was tool of the Federal Government, and was therefore not to be trusted: reports that McVeigh had profiled himself as "Mad Bomber" on an

[118] L Romano, "Fortier Says He Was Asked To Join In McVeigh, Nichols Plan Of Action", *Washington Post*, 13 November 1997, http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/nichols1113.htm accessed 13 March 2006.

AOL account were later proven to be a hoax by Rosenberg[119]. Secondly, much of the information that McVeigh needed could be easily accessed from his local public library. Finally, McVeigh's appetitive for anti-Government propaganda was sated by his ownership of militia produced videotapes alleging conspiracy theories for a Government plot to kill the Branch Davidians during the 1993 Waco siege[120] and various far-Right talk radio shows. In addition, one intriguing aspect is the impact of other forms of mediated communication on McVeigh: his most-rented VCR films included *Red Dawn*, *Rambo II*, *Planet of the Apes* and *The Omega Man*[121]. All feature a single lone warrior battling against foreign culture. Thus, the credibility of the Internet and the accessibility and impact of other media made the use of the Internet irrelevant in this attack.

More intriguing is the idea that McVeigh's cell was acting in accordance with an overarching ideology, but without central direction from a centrally established hierarchy. This is clearly in accordance with Arquilla's theory of Netwar described earlier. However, Arquilla clearly states that part of the underlying pattern of the Netwar phenomenon is "…technology attuned to the information age."[122] This is clearly not evident in McVeigh's case. Indeed, the idea of Arquilla's statement that Netwar "…can set boundaries and provide guidelines for decisions

---

[119] S Rosenberg, "*The Net After the Oklahoma Bomb*" 28 April 1995, http://www.wordyard.com/dmz/digicult/okbomb-4-28-95.html accessed 13 March 2005.

[120] ADL, "A Decade After Oklahoma City Bombing, Domestic Terrorism Threat Still Looms", 6 April 2005, http://www.adl.org/learn/extremism_in_the_news/Anti_Government/okc_10years_40805.htm?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_the_News accessed 13 Mar 05.

[121] Ibid.

[122] Arquilla et al, *Information Age Terrorism*, 180.

and actions so that the members need not resort to a hierarchy – "they know what they have to do"[123] itself draws the last phrase from a much older concept, that of Leaderless Resistance.

Leaderless Resistance

Leaderless Resistance has its roots in the writings of Louis Beam, a noted far-Right thinker who first described the concept in far-Right magazine *The Seditionist*[124]. Leaderless Resistance has its roots in the Committees of Correspondence formed during the American Revolution, groups which rose up to fight against British rule. These groups, with a common ideology, carried out many successful attacks, yet did so without knowledge of the intentions or actions of other groups. As Beam describes it:

> Yet even in these bygone days of poor communication, of weeks to months for a letter to be delivered, the committees without any central direction whatsoever, were remarkable similar in tactics employed to resist government tyranny. It was, as the first American patriots knew, totally unnecessary for anyone to give an order for anything. Information was made available to each committee, and each committee acted as it saw fit[125].

This idea was taken up by the American far-Right, given that it neatly encapsulates the idea of a lack of hierarchy that epitomises those groups with anti-Federal intentions. Beam points out the advantages of Leaderless Resistance : it is resistant to infiltration, not easily susceptible to electronic surveillance (albeit that available at the time) and thus difficult for a pyramidal, hierarchical structure - such as a Government Agency - to bring down. Beam recognises that this

---

[123] Ibid, p181.

[124] L Beam, "Leaderless Resistance", *The Seditionist*, February 1992, http://www.louisbeam.com/leaderless.htm accessed 13 March 2006.

[125] Ibid.

type of organisation – or, indeed, non-organisation - may at first appear unrealistic, yet provides an answer which points to the evolutionary influence of information technology :

> The natural question thus arises as to how are the "Phantom cells" and individuals to cooperate with each other when there is no intercommunication or central direction? The answer to this question is that participants in a program of Leaderless Resistance through phantom cell or individual action must know exactly what they are doing, and how to do it. It becomes the responsibility of the individual to acquire the necessary skills and information as to what is to be done. Organs of information distribution such as newspapers, leaflets, computers, etc., which are widely available to all, keep each person informed of events, allowing for a planned response that will take many variations. No one need issue an order to anyone.

Thus it appears that a decentralised network can survive *without* information technology, instead relying on other mediated forms and a common ideology. Since there is no communication between cells, any mediated form of communication can be used to spread the ideology: all the Internet has done is to increase the speed of ideology distribution, not influence communications between cells. Thus proposed advantages of the use of the Internet for Information Sharing, Networking and, given the limited resources used in McVeigh's attack, Fundraising, are rendered neutral.

The Turner Diaries

The best example of use of a non-Internet form of mediated communication to promote ideology this in the case of the American far-Right is *The Turner Dairies*[126]. Authored by Dr William Pierce in 1978, it tells the story of Earl Turner, a white male who joins an underground

[126] Although available from bookshops, the Turner Diaries (Barricade Books, New Jersey: 2nd ed 1996) was accessed at http://www.solargeneral.com/library/TurnerDiaries.pdf accessed 13 March 2006. This does not intend to imply in any way that the Internet in fact superseded the printed form as an influence on McVeigh.

resistance movement to fight against an oppressive government formed from a "Jew-Negro conspiracy." One of Turner's first missions as part of this movement is to blow up the FBI's primary computer installation in Washington DC. A copy of *The Turner Diaries*, along with a second racist novel, *Hunter*, also by Pierce, were recovered from McVeigh's home by the FBI. As it transpires, there are remarkable similarities between the fictional bomb used by Turner and McVeigh's bomb in Oklahoma:

Table 6.1 - Oklahoma and "Turner's Fictional Washington Bomb" Similarities.

	Timothy McVeigh	**Earl Turner**
target	Alfred P. Murrah Federal Building Oklahoma City	FBI Federal Building Washington, D.C.
date	Wednesday, April 19, 1995 9:02 A.M.	Saturday, October 12, 1991 9:15 A.M.
payload	5,400 lbs. ammonium nitrate mixed with nitro racing fuel and diesel	4,400 lbs. ammonium nitrate mixed with heating oil
delivery	rented Ryder panel truck parked curbside, out front	hijacked panel truck parked in sub-basement loading dock

Source: Adapted from Pierce and Rosenberg

In summary, whilst McVeigh's attack was one of the first major terrorist attacks to occur in the time of the Information Age, it relied on little or no information technology, limited passage of information and a networked structure designed to operate without any information. Despite McVeigh's skill with the Internet, it was of no use nor benefit in the planning, coordination or execution of his attack. Does the Internet, therefore, really represent a revolution in terrorist communications, structures and activities?

NEW YORK AND WASHINGTON, 2001

Given the question raised above, it is necessary to undertake a second case study in order to determine if the Internet has had an effect on terrorist activities in the Information Age. On

September 11, 2001 (9/11), nineteen men boarded four separate aircraft flying to destinations across the United States. Shortly after take-off, and armed with only rudimentary weapons, they seized control of the aircraft. Shortly after, two of the hijacked airliners crashed into the twin towers of the World Trade Center. Less than an hour later, a third hijacked plane struck the Pentagon. A fourth hijacked plane, suspected to be bound for a high-profile target in Washington – either the Capitol Building or the White House - crashed into a field in southern Pennsylvania. Almost three thousand citizens of the US and 78 other countries perished in the attacks, which were quickly linked to Osama bin Laden and Al-Qaeda[127].

Al-Qaeda and the 9/11 Attacks

Al-Qaeda is the leading transnational Islamist terrorist network. It was founded and is still led by Osama bin Laden, a multimillionaire Saudi who became an active Islamist in 1979, when he went to Afghanistan to fight the Soviet Union. In 1996 and1998, his organisation issued two *fatwa* (edicts). The first was a "Declaration of War against the Americans Occupying the Land of the Two Holy Places"[128]. The second was under the banner of the "World Islamic Front for Jihad Against the Jews and Crusaders"[129], urging Muslims to do their duty and kill Americans everywhere. Al-Qaeda bombed U.S. embassies in Kenya and Tanzania that same year and attacked the U.S.S. *Cole* in 2000 before carrying out the 9/11 attacks. There is considerable evidence to suggest that al-Qaeda operatives relied heavily on the Internet for help in planning and coordinating the September 11 attacks[130]. Encrypted messages that had been posted in a

---

[127] Lee and Perl, *Terrorism, the Future and US Foreign Policy*, 1.

[128] http://www.pbs.org/newshour/terrorism/international/fatwa_1996.html accessed 19 April 2006.

[129] http://www.fas.org/irp/world/para/docs/980223-fatwa.htm accessed 19 April 2006.

[130] ADL, *Jihad Online: Islamic Terrorists and the Internet*, 2002

password-protected area of a Web site were found by federal officials on the computer of arrested Al-Qaeda operative Abu Zubaydah, who reportedly masterminded the September 11 attacks. The first messages ran from May 2001 until September 9, 2001, two days before the attacks. The frequency of the messages was highest in August 2001, the month immediately preceding the attacks. Three weeks before the attack, one such message read from Mohammed Atta, later broadcast on Al-Jazeera television read: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering."[131] The identities of the various buildings targeted in the attack were concealed by the faculty references.

Both online and off, Al-Qaeda members operated clandestinely. To preserve their anonymity, they used the Internet in public places and send messages via e-mail accounts that were likely registered using fabricated information. In addition, these radicals used the Internet to research their targets and weapons of choice. Most significantly, they used computer programs to stop anyone but their compatriots from reading or finding the messages they transmit online. Some of the September 11 hijackers accessed the Internet in public libraries. It is often simple to use the Internet in such facilities without being traced or identified; at many public libraries, nearly anyone can walk up to a terminal and access the Internet without presenting identification. Another place Al- Qaeda members accessed the Internet is in *hawalas*, storefront money exchanges that have been used to funnel money to bin Laden and Al-Qaeda.

Certain September 11 hijackers communicated using free, Web-based e-mail accounts provided by a popular Internet company. Al-Qaeda operatives used the Internet to search for, and

[131] Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*, 119.

find, logistical information to use in planning attacks. Some of the September 11 hijackers used the Internet to research the chemical dispersal capabilities of crop dusters, and their ringleader, Mohammed Atta, made his plane reservations online. Information about manufacturing a nuclear bomb and files describing American utilities, downloaded from the Internet, were found in Al-Qaeda safe houses by U.S. officials in Afghanistan.

Despite the many uses of the Internet described above, it is worth examining how many of the five terrorist purposes of the Internet are covered: in reality, only Networking and Information Gathering fall into the activities described above. Financing is suspect, given Osama bin Laden's considerable personal financial resources, estimated at somewhere between $280-$300 million[132]. Weinmann points out one key fact about the 9/11 attacks, namely that "…there is a reason why the 9/11 hijackers used box-cutters instead of keyboards: it is impossible to hijack a plane remotely."[133] Therefore, despite the "cyberposturing", the need for direct action is paramount in order to maintain credibility. As Barber stated: "…the Internet is a place where it's hard to tell the difference between gossip and truth, between lies and truth, between knowledge and wisdom, between mere aggregation and facts and realistic judgements about the world we live in"[134] Thus, whilst the Internet may assist in planning and coordination of attacks, it has yet to be involved in the *execution* of a major attack. The "digital Pearl Harbour"[135] described by Weinmann has yet to transpire.

---

[132] Lee and Perl, *Terrorism, the Future and US Foreign Policy*, 6.

[133] G Weinmann, *Cyberterrorism: How Real Is the Threat?*, United States Institute of Peace Special Report no 119, May 2004, 10.

[134] B Barber, speaker on "*Democracy, Terrorism and The Internet*", International Summit on Democracy, Terrorism and Security, 8-11 March 2005.

[135] Weinmann, *Cyberterrorism: How Real Is the Threat?*, 11.

COMPARISONS WITH ORGANISED CRIME AND CELL PHONE TECHNOLOGY

INTRODUCTION

In order to determine if terrorist use of the Internet for communication, and its second order effect on structure and activities is evolutionary or revolutionary, other comparators are needed. The first of these, use of the Internet by organised crime will be described here. The second, the rise in cell phone use and technology will be described later.

ORGANISED CRIME

What does organised crime use the Internet for? The following table lists the uses of the Internet by perpetrators of organised crime suggested by a variety of authors:

Table 7.1 – Uses of the Internet for Organised Crime

Author	Williams[136]	McAfee[137]	Matai[138]	Tupman[139]
Use	Fraud Theft White collar crime Cyber extortion Nuisance tools Jurisdictional arbitrage Money laundering Networking Communications	Fraud Phishing Political crime Money laundering Hacking Corporate espionage	Criminal profiteering Information gathering Information monitoring Financial transactions Fraud Business interruption	Fundraising Fraud Counterfeiting Money laundering Online legitimate business

Source: Adapted from Williams, McAfee, Matai and Tupman

[136] P Williams, *Organised Crime and Cyber Crime: Implications for Legitimate Business*, Carnegie Mellon University, 2002, 1-7.

[137] McAfee Inc, *McAfee Virtual Criminology Report: North American Study into Organised Crime and the Internet*, (Santa Clara: McAfee, 2005), 2-3.

[138] D Matai, *Cyberland Security: Organised Crime, Terrorism and the Internet*, speech given at Oxford Internet Institute, Oxford University, 10 February 2005, p1-13.

[139] W Tupman, "Where Has All the Money Gone: The IRA as a profit-making concern", *Journal of Money Laundering Control*, Vol 1, No 4, p303-311, April 1998.

Of these, fraud, money laundering and information activities appear to be common. Three of the terrorist uses of the Internet proposed earlier by Conway appear in the list: Networking, Financing and Information Gathering. Does this suggest a degree of commonality between the two?

Real Crime and Cybercrime

McAfee suggest that three comparisons can be made between real-life crime and cybercrime[140]:

> Criminals do not need to be physically present at the scene to commit the crime.
>
> These crimes can be committed across geographies, ie, someone in Russia could commit a crime in the US/Canada/France/UK/Germany/Italy, etc.
>
> Using computers, the crime is carried out automatically, at high speed and attacks a vast number of victims at the same time, making it harder to track and prosecute.

There appears to be a degree of correlation between these functions and terrorist uses of the Internet. Lack of physical presence and geographical separation correlate to the Mitigation of Risk subset of Networking; multiple synchronised attacks correlates to the "swarming" theory proposed by Arquilla. Additionally, Curtis and Karacan propose that there is a clear connection between terrorism and organised crime, especially in respect of weapons trafficking, narcotics and smuggling. However, their research does not specifically point to the Internet as a significant factor in this. They do, however, give indications that a "chain" type network is most suitable for the smuggling and trafficking aspects of organised crime, and that it the idea of a "fighter turned

[140] McAfee Inc, *McAfee Virtual Criminology Report*, 8.

felon" is far less likely with a large, multinational organisation with an active charismatic leader – such as Osama bin Laden[141].

PIRA plc

It is perhaps more interesting to study Tupman's proposals in more detail. He draws from his own spoof prospectus for "PIRA PLC" in which he breaks down the income and expenditure of PIRA in the same manner as a small international company. Thus, his uses of the Internet actually relate to the terrorist organisation as a going concern in the field of organised crime. All his uses could be simply grouped under that of Financing: none of the other proposed terrorist uses, such as Recruitment, Networking and Information Provision appear in the list, suggesting that there is a clear differentiation between terrorism and organised crime.

Differences Between Internet Use for Organised Crime and Terrorism

This difference becomes more clear when one determines the *effects* that need to be achieved through use of the Internet by organised crime. Extortion, hacking and interruption are all *direct* – in military terms, *kinetic* - effects, involving attack in some form. Terrorist uses of the Internet relate to *indirect* or *non-kinetic* effects, termed "soft power"[142] by Arquilla. Additionally, whilst anonymity is desired by both organised crime and terrorists, the latter have a distinct disadvantage in this respect. In order to achieve infamy and credibility, they must lose their group anonymity when undertaking direct action. To leave responsibility for an attack unclaimed does not assist with furthering the political cause: using Hoffman's definition adopted

[141] G Curtis and T Karacan, *The Nexus Among Terrorists, Narcotics Traffickers, Weapon Proliferators And Organised Crime Networks In Western Europe*, (Washington: Federal Research Division, Library of Congress, December 2002), 21-24.

[142] Arquilla et al, *Information Age Terrorism*, 179-180.

earlier, there is no *exploitation* if anonymity is maintained. This ties in with the first of Hoffman's five sequential objectives of terrorism, namely that of *attention*: where terrorists, "…through dramatic, attention-rivetting acts of violence, seek to focus attention on themselves and their causes through the publicity they receive, most often from news media coverage."[143]

CELL PHONE TECHNOLOGY

The second comparator to be used to determine whether the Internet has had an evolutionary or revolutionary effect on terrorist communications, structures and activities is the rise in cell phone technology and use.

The Rise of the Cell Phone

The prominence of the Internet has, according to Odlyzko[144], tended to overshadow the rise of another great high-tech success, namely that of the wireless industry. Wireless communications or cellular phone - cell phone – technology has seen an upsurge in use. The earliest wireless transatlantic link between the US and Europe in 1927 was a single radio circuit; by 1995, this had grown to 23,000 voice circuits by 1995[145]. A study of the US domestic cell phone network showed growth from 200,000 subscribers to 97 million subscribers in 2001[146]; by 2003, this had increased further still to 120 million[147]. It should be noted that the situation in the

---

[143] Hoffman, "The Modern Terrorist Mindset: Tactics, Targets and Technologies", in *Terrorism and Counter-terrorism: Understanding the New Security Environment*, 92.

[144] A Odlyzko, *The history of communications and its implications for the Internet*, AT&T Labs – Research, June 2000, 112.

[145] Coffman and Odlyzko, *Growth of the Internet*, 7-8.

[146] Ibid, 7.

US, where Internet use is greater than cell phone use, is not mirrored in other countries. China, for example, has five times as many cell phone users (300 million) as Internet connections (60 million)[148]. Indeed, a report from Portio Research suggests that the US still remains a potential growth market; that the Asia-Pacific region will see a 50% rise in cell phone use, with China and India sharing over one billion subscribers and that over half the world's population will own a cell phone by 2011[149]. Cell phones offer a number of clear advantages over landline telephone networks: they are mobile; they offer rapid point-to-point communications; they do so over a high quality and robust network. Its ability to mix voice, text messaging, Wireless Application Protocols (WAP) Internet services, digital imaging and now television broadcast receipt may well lead to a even more mobile social network as these services are no longer tied to the home or indeed to the mobile computer. Compared with other forms – albeit mediated ones - of communication, cell phones offer the characteristics of high speed, global reach, high availability with little requirement for any skill in their use.

Terrorist Uses of Cell Phones

Given that terrorists have exploited Internet technology to seek an advantage, how have they done the same with cell phone technology? Bedi[150] describes how terrorists use mobile phones to detonate explosives, such as in Jakarta and Bali. This is due to their digital technology

---

[147] A Ratner, "Cell Phones and Internet Convey Vivid Human Stories", *Baltimore Sun*, September 13, 2001, http://www.baltimoresun.com/news/custom/attack/bal-te.cell13sep13,0,6276724.story?coll=bal-attack-utility accessed 14 March 2006.

[148] Hong Kong China Mobile figures, http://www.cellular.co.za/news_2004/may/050404-china-record_sign.htm accessed 14 March 2006.

[149] Portio Research, "Half the World Will Own a Cell Phone by 2009", http://www.mobiledia.com/news/43104.html accessed 14 March 2006.

[150] R Bedi, *Telecom – the Terrorism Risk*, International Centre for Political Violence and Terrorism Research, IDSS Singapore, September 2005, 1.

and the quality of the network. He goes on to describe how governments often suspend cellular networks to prevent such attacks, or to avoid the risk of a secondary device being detonated when emergency services rush to the scene of an attack. The same report also states that "Government agents have recently uncovered numerous calls from difficult to track prepaid cell phones…prepaid phone cards and public payphones in the US to known Al-Qaeda locations overseas."[151] Terrorists can also encrypt cell phone transmissions, steal cell phone numbers and program them into a single phone, or use prepaid cell phone cards purchased anonymously to keep their communications secure. Mohammed Atta used prepaid wireless and telephone cards whilst planning the 9/11 attacks; similar methods for communicating back to terrorist bases were used in the Madrid train attacks in March 2004. The so-called "Belmarsh Ten", suspected terrorists released into the community under British Government "control orders" were subjected to a ban on the use of cell phones as part of their restrictions[152]. Thomas[153] also describes the use of cell phone technology as a misinformation tool. Terrorists, aware that they may be under surveillance, can introduce false information, gauge the reaction from the security services and then attempt to pinpoint the technology being used against them. For example, describing a fake operation against a well known landmark during a cell phone call may lead to a Government warning about this, allowing the terrorists to know their communications are being monitored.

Cell phones do have some disadvantages for terrorist users. Call tracing can establish the approximate location of an individual. In November 2002, the US used cell phone data to

---

[151] Ibid, 1.

[152] R Ford, "More Suicide Bombs on the Way, says Terrorism Watchdog", *Sunday Times*, 3 February 2006, http://search.thetimes.co.uk/cgi-bin/ezk2srch?-aSTART accessed 14 March 2006.

[153] Thomas, *Al-Qaeda and the Internet: The Danger of 'Cyberplanning'*, 122.

establish the position of "Abu Ali" a Yemeni with links to Al-Qaeda. Minutes later, a missile strike form an orbiting Predator drone struck the vehicle in which he was travelling, killing him and several other suspected terrorists[154]. This is one reason that Osama bin Laden's satellite phone always travels separately from him[155]. In addition, phone records can be kept as evidence. For example, Italian police used cell phone records to track down one the London suicide bombers whose attacks failed on 21 July 2005[156]. Proposals from the EU include one that unregistered pre-paid cell phones and calling cards should be banned to allow the possibility of phone communications being monitored[157].

Despite these disadvantages, cell phones may be a growth area for terrorists. Odlyzko's research points out that there have only ever been two "killer app[lication]s" on the Internet: the Web and e-mail[158]. Both of these are now available on cell phones. Indeed, the same research points out to an eventual convergence between point to point and mediated communication: could one of these be the cell phone as a broadcast system? Inadvertently, this may already have been achieved. Amongst the first pictures transmitted following the London July 7 bombings were video images captured on the cell phones of the surviving passengers, such as that by Chadwick[159]. By doing so, the full horror of what it was like to be involved in the aftermath of a

---

[154] P Smucker, "The intrigue behind the drone strike", *Christian Science Monitor*, November 12, 2002, http://www.csmonitor.com/2002/1112/p01s-2-wome.html accessed 25 October 2005.

[155] Sageman, *Understanding Terror Networks*, 160.

[156] Bedi, *Telecom – the Terrorism Risk*, 5.

[157] Ibid, p4.

[158] Odlyzko, , *The history of communications and its implications for the Internet*, 19.

[159] BBC News, "London Blasts in Pictures", http://news.bbc.co.uk/1/hi/in_depth/uk/2005/london_explosions/default.stm accessed 14 March 2006.

terrorist attack was brought home to millions of television viewers: the terrorists had been given "the oxygen of publicity".

EVOLUTIONARY OR REVOLUTIONARY?

INTRODUCTION

The aim of this paper was to argue that the Internet represented an evolutionary, not revolutionary, method of communications for terrorists and that this had a corresponding evolutionary second order effect on the structures and activities of these groups. Now that the evidence has been presented, it is necessary to compare and contrast the evolutionary and revolutionary aspects in order to determine if, indeed, this is true.

COMMUNICATIONS

From the point of view of communications, the Internet was assessed as "revolutionary": however, this was only when compared with other mediated forms. When compared with point-to-point systems, its revolutionary status seems less assured. Odlyzko states that "…the Internet is not unique. Most likely it will continue to *evolve* [emphasis added] as other communication services did."[160] He goes on to state that "No broadcast medium has ever been replaced by another; despite predictions to the contrary at various times in the past, newspapers were not killed by radio, nor radio by television."[161] This is recognised for point-to-point forms as well; "After all, why hasn't the Internet eliminated the fax yet?"[162] Indeed, the only truly revolutionary form of communication recognised by Odlyzko is the telegraph: "In many ways, the telegraph was a greater innovation than the Internet. It was the first technology that separated communication from transportation. It had a dramatic effect on science and technology, and it

---

[160] Odlyzko, *The history of communications and its implications for the Internet*, 10.

[161] Ibid, 25.

[162] Ibid, 37.

facilitated huge economic changes"[163] For all the rise in Internet use, the use of other methods of internal communications used by terrorists in the Information Age have been remarkably varied: letter, landline, cell phone, satellite phone, fax, printed media, such as pamphlets and newspapers, and voice. This is echoed in the civilian world: Yourdon[164] states that an organisation which controls Internet resources - for example, by restricting access or to maximise productivity - will be unable to do so for all forms of communication: cell phone, landline phone and wireless pager. Even Arquilla[165], the strongest proponent of information technology's effect on Netwar and terrorist communications, recognises that even old technologies, such as human couriers may suffice. Despite the plethora of terrorist training material and communication capability on the Internet, the role of simple voice communication is still vital. The impact of loss of satellite phone technology is, according to Sageman[166], one of the reasons for the amateurish nature of the failed Casablanca bombing in May 2003. The bombers, stripped of their communication technology due to surveillance, were separated from the guidance of the Al-Qaeda central staff and got lost *en route* to the target.

Social Interaction and the Internet

Additionally, the lack of social interaction – as opposed to electronic interaction – is one of the limits of communication by information technology. Borum's study into the psychology of terrorism emphasises clearly the key role of interpersonal relationships or cliques of friends in

---

[163] Ibid, 39.

[164] E Yourdon, *Byte Wars: The Impact of September 11 on Information Technology*, (Prentice Hall: Upper Saddle River, NJ: 2002), 271.

[165] Arquilla et al, *Information Age Terrorism*,181.

[166] Sageman, *Understanding Terror Networks*, 160.

terrorist recruiting[167]. This is echoed by Sageman, who points out that the Internet does not offer a means for direct contact with jihad. Neither does it offer a friend or kin to vouch for a potential recruit. Indeed, he believes that the Internet alone is not persuasive enough for the type of allegiance demanded by jihad. In his study of Islamic terrorism, he found no evidence that any individual – despite Internet exposure to Muslim issues and the virtual *umma*, or community, that it offered – went straight from the Internet into an Afghan training camp. The demands of jihad requires an intensive period of interaction and grooming by a committed member in order to fully prepare the would-be terrorist for the cause. This is seen in the examples of those terrorists responsible for the 7 July London bombings: Mohammed Sidique Khan acted as a mentor for the others, who formed part of a clique at his gym[168]. All, however, were required to travel to Pakistan to prepare for their task, despite the abundance of terrorist training material on the Internet.

Vulnerabilities of Terrorist Groups

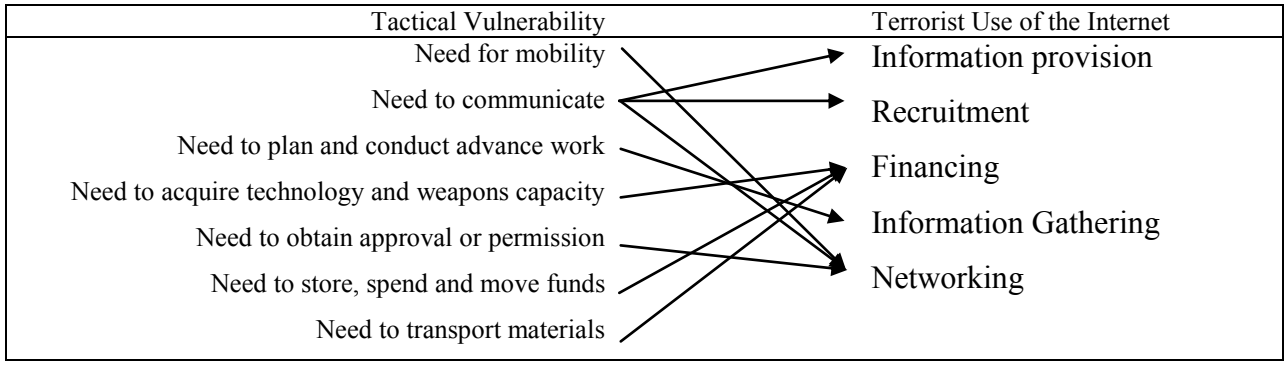
Finally, the functions that make the Internet useful for internal terrorist communications also make it vulnerable. Borum[169] offers a number of tactical vulnerabilities for terrorist group disruption from a psychological perspective. These provide an interesting comparison with the terrorist uses of the Internet in Table 5.1:

[167] R Borum, *Psychology of Terrorism*, (Tampa: University of South Florida, 2004), p58.

[168] Tumelty, *An In-Depth Look at the London Bombers*.

[169] Borum, *Psychology of Terrorism*, 55.

Table 8.1 – Terrorist group vulnerabilities compared with terrorist uses of the Internet



Source: Adapted from Borum and Conway

It can be seen from the table above that there is considerable mapping between the strengths of the internet and the weaknesses inherent in terrorist groups. It is therefore argued that use of the Internet makes a group vulnerable: if this is the case, can the Internet really be as revolutionary as is claimed?

External Communication

Turning to external communication: has the Internet had a revolutionary effect on how a terrorist group gets its message across? Certainly, it has allowed faster dissemination of information: however, as Handler states, "The Internet provides the ability for organisations to access information quickly, yet this aspect is a *function* of the Internet and not a *prerequisite* for its use as a medium."[170] Therefore we must be clear that speed of dissemination is not enough for a revolution on its own; indeed, Table 3.3 proposed that the speed of dissemination for the Internet, TV and radio were the same. This can be seen in the so-called "CNN effect" where global media organisations can report news before those in the official chain of command are aware is well known. This fact - that violent acts will be covered by other forms of mediated

[170] L Handler, "Rhetorical Terrorism: Online News Visual Representation of Suicide Bombing", (Masters Thesis, University of Florida, August 2004), 51.

communications well before the event makes it onto the Internet – reduces the "shock and awe" potential for the Internet as a publicity tool.

For terrorists, there may a similar "al-Jazeera effect". The Qatar based television station *al-Jazeera* (the island) has demonstrated a willingness to broadcast statements from Al-Qaeda terrorists. For example, on no less than three occasions, videotapes of Osama bin Laden have been broadcast by the station; these were *subsequently* posted on the Internet. In fact, in bin Laden's October 2004 speech[171], he cites the mediums by which his words have been disseminated: *Time* magazine and CNN. Sageman builds on this, stating a further limitation of the Internet as a mediated form: that the poorest social classes in the world could simply not be connected to the global jihad through the Internet. This lack of access due to social deprivation rules out the majority of sub-Saharan Africa, much of the Persian Gulf region, and even those around the Afghan-Pakistan border where Al-Qaeda maintains its headquarters, as areas of online recruiting and support. It is interesting to note that Al-Qaeda's next recruiting drive is expected to be into Moslem Indonesia[172]. Given that there are only half a million Internet users, as opposed to twenty million cell phone users, and with over 60% of households owning televisions, it will be interesting to see which medium Al-Qaeda chooses to use to forward its message. Finally, as Al-Qaeda itself evolves, the Internet itself, being perceived as a Western tool, may become part of the jihad. Al-Zawahiri, Al-Qaeda's second-in-command, declared that

[171] Text of Osama bin Laden's October 2004 speech, http://en.wikisource.org/wiki/Text_of_2004_Osama_bin_Laden_videotape accessed 15 March 2006.

[172] R Lee and R Perl, *Terrorism the Future and US Foreign Policy*, 6.

the new jihad involved a struggle between Islam and hostile forces, including "…(4) The international communications and data exchange systems."[173]

Al-Zawahiri's warning of the Internet as a Western tool leads into the next limitation of the Internet: that Western security services have the technological "upper hand". The more that terrorists use the Internet, the more opportunity there is to monitor them. Conway cites those such as Aftergood and Lasker who glean the majority of their intelligence on Al-Qaeda from their websites: "They are greater value as an intelligence source than if they were to disappear."[174] The use of fake websites to attract would-be terrorists has been used by British security services; the USA Patriot Act described earlier also allows Government agencies an unprecedented degree of access to electronic information. Advances in software allow decryption of e-mails and electronic files. Government websites can be sanitised to deny information to terrorists. The hardware itself also provides a valuable source of information. In Iraq, the near-capture of Abu Musab Zarqawi, Al-Qaeda's leader in the country, led to the seizure of a laptop computer with his entire online support network intact on the hard drive[175]. The days when an old-fashioned terrorist would resist interrogation are gone: now, the computer can compliantly give up the required information. Has new technology made previous practices obsolescent, or has it made organisations less secure?

---

[173] Sageman, *Understanding Terror Networks*, 20.

[174] Conway, *Reality Bytes*, 24.

[175] B Glasser and S Coll, "The Web as a Weapon", *Washington Post*, 7 August 2005, http://pqasb.pqarchiver.com/washingtonpost/access/878566671.html?dids=878566671:878566671&FMT=ABS&FMTS=ABS:FT&fmac=&date=Aug+7%2C+2005&author=Steve+Coll+and+Susan+B.+Glasser&desc=Terrorists+Turn+to+the+Web+as+Base+of+Operations accessed 22 August 2005.

STRUCTURES

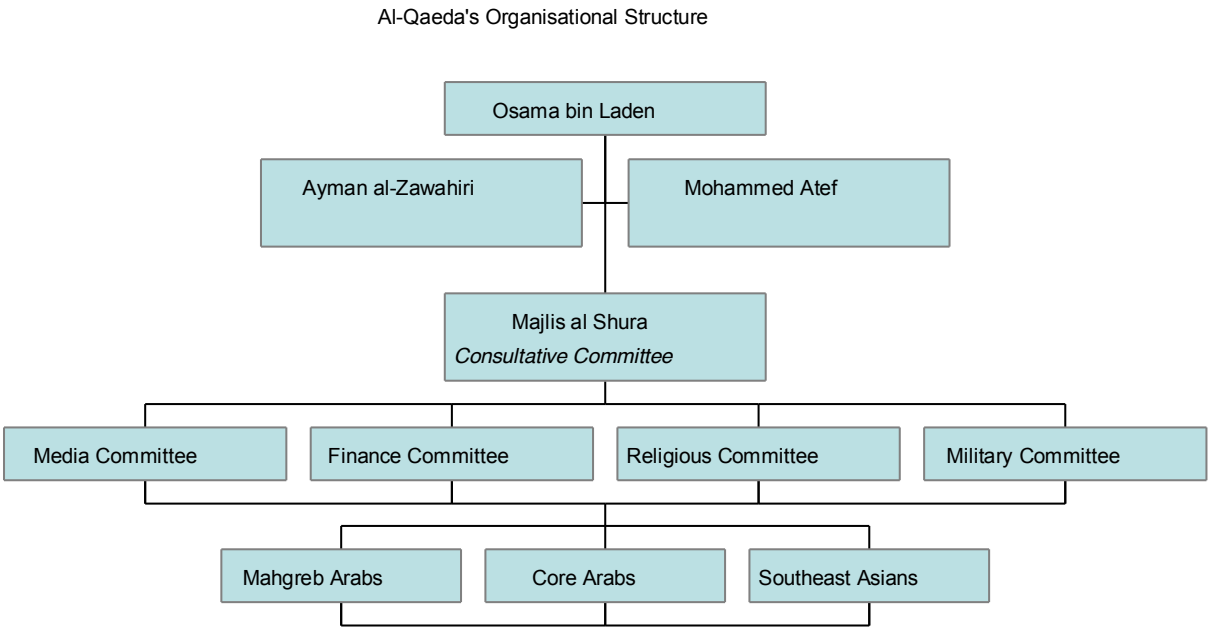
Hierarchy, Network or Hybrid?

Turning now to the second order effects of Internet communication upon terrorist group structures and activities, there is still considerable debate on how the Internet has altered the structure of terrorist groups. It was described earlier how Arquilla and others believed that the all-channel network was the structure used by Al-Qaeda, largely as a result of the influence of the Internet. This is disputed by Simon, Smith and most notably Mayntz. Simon[176] proposes Al-Qaeda's structure as a "spoke and wheel" system, which combines robustness with command and control. Smith[177] proposes a more hierarchical structure, which is shown below with the final layer of Sageman's global jihad structure added. This structure is remarkably different from the all-channel network proposed earlier:

[176] S Simon, *The New Terrorism and the Peace process*, Madeleine Feher European Scholar Lecture, Bar-Ilan University, 2000, http://72.14.207.104/search?q=cache:8Wwa0rBuatQJ:www.biu.ac.il/SOC/besa/publications/simon/new-terror.pdf+new-terror.pdf&hl=en&ct=clnk&cd=1&client=safari accessed 28 November 2005.

[177] P Smith, Transnational Terrorism and the Al-Qaeda Model: Confronting New Realities, *Parameters*, Summer 2002, 33-46.

Figure 8.1 – Al Qaeda's Organisational Structure



Source: Adapted from Smith and Sageman

Mayntz[178] proposes that in fact Al Qaeda may indeed be a mix of hierarchical and networked structures, with some networks being used for specific purposes. For example, the hierarchy may direct certain nodes to form a chain network for smuggling, others to form a hub network for money laundering and so forth. However, he clearly compares the structure of Al-Qaeda to be analogous to that of PIRA in that:

> They have a clearly defined leadership.
>
> They are differentiated both vertically and functionally, with a third layer of operatives organised into cells.
>
> Vertical communication dominates.

[178] R Mayntz, *Organisational Forms of Terrorism: Hierarchy, Network or a Type sui generis?*, Max Planck Institute for the Study of Societies, May 2004, 11.

Thus, again, it is argued that the impact of the Internet on group structures is clearly not revolutionary, given the remarkable similarities between Al Qaeda's structure and that of PIRA in the pre-Information Age.

Similarities Between Pre- and Post-Information Age Terrorism

Mayntz also provides another argument against the network structure of Information Age group: he cites those who state that, since networks are leaderless by definition, they do not take orders[179]. Yet, however, he demonstrates above that all terrorist groups have a clearly defined leadership. The critical role of leadership in terrorist organisations has been examined by Borum[180], and found to include tasks such as controlling the flow of communication, maintaining collective belief and to keep action going. Already, Curtis and Karacan identified Osama bin Laden as an example of a charismatic leader: Thomas[181] concurs, recognising the inspirational leadership of bin Laden and Zawahiri. Without such leadership, an all-channel network lacks the credibility it needs for survival, as it has no central spokesman to draw attention to its cause. Borum suggests that the only group that has survived without leadership are the ethno-nationalist groups such as the American far-Right. This is partly because of the far-Right movement's repeated failure to achieve its objectives and thus avoid scrutiny by law enforcement, but more likely due to its philosophy of Leaderless Resistance – a concept described earlier which clearly predates the Information Age and the Internet. Indeed, since evolution can favour lower complexity in order to survive, it is argued that the use of the Internet been a retrograde step

[179] Ibid, p8.

[180] Borum, *Psychology of Terrorism*, 61-62.

[181] Thomas, *Al Qaeda and the Dangers of 'Cyberplanning'* 122-123

which creates vulnerability. Thus, such a step could not be described as revolutionary since it has not rendered previous evolutionary change almost obsolescent or ineffective.

CONCLUSION

This paper proposed that terrorist use of the Internet had an evolutionary, not revolutionary effect on terrorist communications, and a similar corresponding second order effect on their structures and activities. This argument began by defining evolution and revolution in order to make it clear when we see a revolution take place: when rapid and profound change rendered previous practices almost obsolescent or ineffective.

Following this, I provided a brief survey of communication theory, mediated forms of communication and examined the rise in growth and uses of the Internet in order to establish a comparative baseline between forms. It was argued at this stage that, given its characteristics, the Internet may indeed have been a revolutionary step in mediated forms of communication, but that for terrorist purposes, it was an evolutionary step.

This argument was carried forward by setting a historical baseline for terrorism. One definition of terrorism from many was chosen, to emphasise the fact that any terrorist act had to be exploited through communication of the act and the intent behind it. PIRA was used as an example of terrorism in the pre-Information Age in order to allow comparison of communication purposes and methods, structures and the effect of denial of communications on a terrorist group. Comparisons could be drawn at this stage regarding the use of autonomous cells in terrorist organisations then with those of today.

Terrorist use of the Internet was examined in some detail, with the purposes of its use and the advantages terrorists seek to draw from it were described. Comparisons were drawn between

these and pre-Information age purposes of communication: one of the main differences is the theory of Netwar, where information technology was proposed to have a "revolutionary" effect on terrorist communications and structures. In order to show the differences between pre- and post-Information Age terrorism, two examples were used from the far-Right and Islamic terrorist groups respectively: the 1995 Oklahoma bombing and the 9/11 attacks on New York and Washington in 2001. In the former, despite knowledge and experience with the Internet, the individuals involved eschewed its use in favour of more traditional methods of communication. In the latter, despite the Internet being used extensively, its use was concurrent with other forms of communications, such as cell phones and land lines. Thus, the idea that, for terrorist purposes, the Internet had not completely replaced other forms of communication began to be proven.

As comparators, the use of the Internet by organised crime and cell phone technology were used. There were some comparisons between the former and terrorism, although it was argued that the effects to be achieved were different: organised crime required direct action against Internet services in anonymity, whereas terrorist groups seeking the oxygen of publicity sought to forgo their anonymity in order to achieve credibility. Other news media were more effective in allowing them to do this. The second comparator of cell phone technology demonstrated that his may well be a more important area than the Internet for terrorist exploitation. Their use and advantages were explained, and, whilst noting their disadvantages, it was noted that the rise in cell phone technology and ubiquity of their use perhaps offered more potential than the Internet.

Finally, the argument that the Internet was not a revolutionary step was proven by examining its effect on internal and external terrorist communications and structures. The vulnerabilities posed by use of the Internet for internal communications and the limitations of its use for external communications, such as accessibility, were stated. Comparisons were drawn between the structure of PIRA and Al-Qaeda in the pre- and post-Information Age and found to be little different despite the growth of the Internet and its supposed revolutionary effect. The idea that groups linked through the Internet could exist without hierarchy, such as in an all-channel network, was dismissed through demonstrating the key role played by charismatic leadership in providing command, reinforcing ideology and maintaining action. Only one group, the extreme far right, has survived without charismatic leadership, and does so by eschewing direct contact between cells altogether, instead relying on a mix of mediated communication forms to reinforce its ideology.

Many of the authors cited in this paper have argued that the growth of the Internet has occurred in parallel with the advent of terrorism based on ideology, rather than politics. By contrast, however, this paper has argued that there is little correlation between cause and effect. The fact that both mediated and point-to-point forms of communication have evolved to take advantage of, or compete directly with, the Internet proves that it has not rendered these almost obsolescent or ineffective and is thus not revolutionary. This is proven when terrorists continue to use more traditional means of communication to for their purposes.

It is hoped that this paper serves to divert attention away from the universal panacea that is the Internet, and concentrate on the other facets of terrorist communication and structures that can be exploited and contribute toward their eventual demise.

BIBLIOGRAPHY

ADL, "A Decade After Oklahoma City Bombing, Domestic Terrorism Threat Still Looms", 6 April 2005, http://www.adl.org/learn/extremism_in_the_news/Anti_Government/okc_10years_40805.htm?LEARN_Cat=Extremism&LEARN_SubCat=Extremism_in_the_News accessed 13 Mar 05.

ADL, "Jihad Online: Islamic Terrorists and the Internet", 2002.

Arquilla et al, "Information Age Terrorism" *Current History*, April 2000.

Arquilla et al, "Networks, Netwar and Information Age Terrorism", in *Strategic Appraisal* ed Khalizad and White, RAND: Santa Monica California, 1999.

Arthur P, "The Conflict", transcript of interview for "Behind the Mask", http://www.pbs.org/wgbh/pages/frontline/shows/ira/conflict/ accessed 9 March 2006.

Barber B, speaker on "Democracy, Terrorism and The Internet", International Summit on Democracy, Terrorism and Security, 8-11 March 2005.

BBC News "Internet Blows CIA Agents Cover", http://news.bbc.co.uk/1/hi/world/americas/4799174.stm accessed 12 March 2006.

BBC News, "London Blasts in Pictures", http://news.bbc.co.uk/1/hi/in_depth/uk/2005/london_explosions/default.stm accessed 14 March 2006.

Beam, L "Leaderless Resistance", *The Seditionist*, February 1992, http://www.louisbeam.com/leaderless.htm accessed 13 March 2006.

Bedi R, *Telecom – the Terrorism Risk*, International Centre for Political Violence and Terrorism Research, IDSS Singapore, September 2005.

Borum, R, *Psychology of Terrorism*, Tampa: University of South Florida, 2004.

Boyne S, "Uncovering the Irish Republican Army", *Janes Intelligence Review*, August 1996.

Bruguiere, JL *Terrorism: Threats and Responses*, Occasional Paper prepared for The Geneva Centre for Security Policy, Geneva, May 2001, http://www.gcsp.ch/e/publications/Other-pubs/Occ-papers/2001/31-Bruguiere.pdf accessed 28 November 2005.

Bushart *et al*, *Soldiers of God: White Supremacists and their Holy War for America*, New York: Kensington Pub Corp, 1998.

Coffman, K and Odlyzko, A, *Growth of the Internet*, report for AT&T Labs – Research, July 2001.

Cohen F, "Terrorism and Cyberspace", *Network Security*, Vol 5, 2002.

Cohen N, *The Observer*, 17 July 2005, http://observer.guardian.co.uk/comment/story/0,6903,1530248,00.html accessed 12 March 2006.

Conway, M, *Reality Bytes: Cyberterrorism and Terrorist Use of the Internet*, paper presented at Annual Meeting of the American Political Science Association, 2002, accessed at www.firstmonday.org/issues/issue7_11/conway/index.html 22 November 2005.

Conway, M, *Terrorist 'Use' of the Internet and Fighting Back,* paper prepared for Cybersafety: Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Oxford Internet Institute (OII), Oxford University, 8-10 September, 2005.

Crawford C, *Inside the UDA: Volunteers and Violence*, London: Pluto Press, 2003.

Curtis G and Karacan T, *The Nexus Among Terrorists, Narcotics Traffickers, Weapon Proliferators And Organised Crime Networks In Western Europe*, Washington: Federal Research Division, Library of Congress, December 2002.

Curtis L, *Ireland: The Propaganda War* London: Pluto Press, 1984.

Dauderstadt M, "Negotiating with Terrorists – an Option Not to be Forgotten", *Internationale Politik und Gesellschaft*, No. 3, 2004, 9-13.

Evans M, "New clues support al-Qaeda link for London Bombing", *Sunday Times*, 30 January 2006, http://www.timesonline.co.uk/article/0,,22989-2016192,00.html accessed 26 February 2006.

Footage at http://news.bbc.co.uk/1/hi/in_depth/uk/2005/london_explosions/default.stm# accessed 26 February 2006.

Ford R, "More Suicide Bombs on the Way, says Terrorism Watchdog", *Sunday Times*, 3 February 2006, http://search.thetimes.co.uk/cgi-bin/ezk2srch?-aSTART accessed 14 March 2006.

Franklin R, *The Hate Directory*, http://www.bcpl.net/~rfrankli/hatedir.pdf accessed 12 March 2006.

Furnell S and Warren M, "Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium", *Computers and Security*, no 18, 1999.

G8 Statement on Counter-Terrorism, issued 8 July 2005, at http://www.fco.gov.uk/Files/kfile/PostG8_Gleneagles_CounterTerrorism.pdf accessed 22 November 2005.

Gearson, J, *The Nature of Modern Terrorism*, London: Political Quarterly Publishing Co, 2002 .

Glasser B and Coll S, "The Web as a Weapon", *Washington Post*, 7 August 2005, http://pqasb.pqarchiver.com/washingtonpost/access/878566671.html?dids=878566671:878566671&FMT=ABS&FMTS=ABS:FT&fmac=&date=Aug+7%2C+2005&author=Steve+Coll+and+Susan+B.+Glasser&desc=Terrorists+Turn+to+the+Web+as+Base+of+Operations accessed 22 August 2005.

Hamre, cited at http://www.fas.org/sgp/news/2001/10/dier102601.html accessed 12 March 2006.

Handler L, "Rhetorical Terrorism: Online News Visual Representation of Suicide Bombing", Masters Thesis, University of Florida, August 2004.

Hoffman et al, *Trends in International Terrorism, 1982-1983*, RAND Corporation, http://www.rand.org/pubs/reports/2005/R3183.pdf accessed 9 March 2006.

Hong Kong China Mobile figures, http://www.cellular.co.za/news_2004/may/050404-china-record_sign.htm accessed 14 March 2006.

Howard, R and Sawyer, R *Terrorism and Counter-terrorism: Understanding the New Security Environment*, Connecticut: McGraw-Hill/Dushkin, 2002.

http://72.14.207.104/search?q=cache:8Wwa0rBuatQJ:www.biu.ac.il/SOC/besa/publications/simon/new-terror.pdf+new-terror.pdf&hl=en&ct=clnk&cd=1&client=safari accessed 28 November 2005.

http://aryanwear.com/product_info.php?products_id=469&osCsid=cdc3ee131abe674c8a4dc08ab95d9b87 accessed 12 Mar 2006.

http://news.bbc.co.uk/1/hi/uk/1201738.stm accessed 9 March 2006.

http://www.bbc.co.uk/home/i/ accessed 01 Mar 06.

http://www.fas.org/irp/world/para/docs/980223-fatwa.htm accessed 19 April 2006.

http://www.halturnershow.com/index.html accessed 12 March 2006.

http://www.moqawama.org/english/index.php accessed 12 March 2006.

http://www.newgrounds.com/portal/view.php?id=50323

http://www.palestine-info.co.uk/am/publish/ accessed 12 March 2006.

http://www.pbs.org/newshour/terrorism/international/fatwa_1996.html accessed 19 April 2006.

http://www.solargeneral.com/ accessed 12 March 2006.

http://www.unison.ie/irish_independent/stories.php3?ca=9&si=1534497&issue_id=13482 accessed 9 March 2005.

Internet Audiences - Key Theorists: Denis McQuail http://wiki.media-culture.org.au/index.php/Internet_Audiences_-_Key_Theorists:_Denis_McQuail accessed 02 March 2006.

Internet Usage Statistics, http://www.internetworldstats.com/stats.htm accessed 6 March 2006.

ITIC CSS Special Information Bulletin of 27 March 2005, http://www.terrorism-info.org.il/engsite/home/default.asp accessed 22 November 2005.

Kohlmann, E, *Legal and Investigative Loopholes in Modern Cyberterrorism Cases*, University of Pennsylvania Law School, 2003.

Kushner, H, ed *The Future of Terrorism: Violence in the New Millenium*, Thousand Oaks: Sage, 2002.

Lee, R and Perl, R, *Terrorism, the Future and US Foreign Policy*, Washington: Congressional Research Service, 2002.

Lockyer A, *The Relationship between the Media and Terrorism*, Canberra: Australian National University Press, 2003.

Matai D, "*Cyberland Security: Organised Crime, Terrorism and the Internet*", speech given at Oxford Internet Institute, Oxford University, 10 February 2005.

Mayntz, R, *Organisational Forms of Terrorism: Hierarchy, Network or a Type sui generis?*, Max Planck Institute for the Study of Societies, May 2004.

McAfee Inc, *McAfee Virtual Criminology Report: North American Study into Organised Crime and the Internet*, McAfee: Santa Clara, 2005.

McQuail D, *Mass Communication Theory*, London: Sage,1983.

Morrison D, cited in The Irish Post, http://archives.tcm.ie/businesspost/2001/11/04/story390373828.asp accessed 9 March 2005.

O'Neill, B, *Insurgency and Terrorism: Inside Modern Revolutionary Warfare*, Virginia: Brassey's, 1990.

Odlyzko A, *The history of communications and its implications for the Internet*, report for AT&T Labs – Research, June 2000.

Oxford Brookes University, *History of the Web*, Oxford Brookes University, 2002.

Pierce, W, *The Turner Diaries*, New Jersey: Barricade Books, 1996.

Portio Research, "Half the World Will Own a Cell Phone by 2009", http://www.mobiledia.com/news/43104.html accessed 14 March 2006.

Ratner A, "Cell Phones and Internet Convey Vivid Human Stories", *Baltimore Sun*, September 13, 2001, http://www.baltimoresun.com/news/custom/attack/bal-te.cell13sep13,0,6276724.story?coll=bal-attack-utility accessed 14 March 2006.

Rolston, B ed *The Media and Northern Ireland*, Basingstoke: McMillan, 1991.

Romano L, "Fortier Says He Was Asked To Join In McVeigh, Nichols Plan Of Action", *Washington Post*, 13 November 1997, http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/nichols1113.htm accessed 13 March 2006.

Rosenberg S, "*The Net After the Oklahoma Bomb*" 28 April 1995, http://www.wordyard.com/dmz/digicult/okbomb-4-28-95.html accessed 13 March 2005.

Rubenstein R, "Rebellion in America: The fire next time", in *Violence in America: Protest, Rebellion and Reform*, ed T Gurr, Newbury Park: Sage, 1989.

Sageman M, *Understanding Terror Networks*, Philadelphia: University of Pennsylvania Press 2004.

Schmidt et al, *Political terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, New Brunswick: Transaction, 1988.

Simon S, "The New Terrorism and the Peace process", Madeleine Feher European Scholar Lecture, Bar-Ilan University, 2000.

SITE Institute, Jihadist Message Boards Link to Website Offering Advanced Military Training Manuals, 25 February 2006, http://www.siteinstitute.org/bin/articles.cgi?ID=publications21805&Category=publications&Subcategory=0 accessed 12 March 2006.

Sloan C, *The Revolution in Military Affairs*, Montreal: McGill-Queens University Press, 2002.

Smith et al, *Internet: An Overview of Key technology Policy Issues Affecting Its Use and Growth*, CRS Report for Congress, Washington: Library of Congress, 2004.

Smith P, "Transnational Terrorism and the Al-Qaeda Model: Confronting New Realities", *Parameters*, Summer 2002.

Smucker P, "The intrigue behind the drone strike", *Christian Science Monitor*, November 12, 2002, http://www.csmonitor.com/2002/1112/p01s-2-wome.html accessed 25 October 2005.

Sweetman B, "Insurgents Using Google Earth", *The Daily Telegraph*, 12 December 2005, http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/12/18/ngoog18.xml accessed 13 March 2006.

Technical Analysis Group, ISTS, "*Examining the Cyber Capabilities of Islamic Terrorist Groups*", Dartmouth College, Dartmouth, 2004.

Text of Osama bin Laden's October 2004 speech, http://en.wikisource.org/wiki/Text_of_2004_Osama_bin_Laden_videotape accessed 15 March 2006.

Thomas TL, "Al-Qaeda and the Internet: The Danger of 'Cyberplanning' ", *Parameters*, Spring 2003.

Tumelty P, "An In-Depth Look at the London Bombers", *TerrorismMonitor*, Volume 3, Issue 15, July 28, 2005, www.jamestown.org, accessed 11 November 2005.

Tupman W, "Where Has All the Money Gone: The IRA as a profit-making concern", *Journal of Money Laundering Control*, Vol 1, No 4, April 1998.

Use of Hasib Hussain's cell phone given at http://news.bbc.co.uk/1/hi/uk/4181454.stm accessed 26 February 2006.

United States Army Deputy Chief of Staff for Intelligence, A Military Guide to Terrorism in the Twenty-First Century, Handbook No.1, Version 3.0, 15 August 2005, http://www.fas.org/irp/threat/terrorism/guide.pdf accessed 23 April 2006.

Video of Mohammad Sidique Khan, broadcast by al-Jazeera, at http://news.bbc.co.uk/1/hi/uk/4208250.stm accessed 26 February 2006.

Voida et al, "Listening In: Practices Surrounding iTunes Music Sharing", University of Gerogia, presented at CHI 2005, April 2-7 2005, accessed at www-static.cc.gatech.edu/~amyvoida/listeningIn-chi05.pdf accessed 05 March 2006.

Weinmann G, *Cyberterrorism: How Real Is the Threat?*, United States Institute of Peace Special Report no 119, May 2004.

Weinmann G, *www.terror.net. How Modern Terrorism Uses the Internet*, United States Institute of Peace Special Report no 116, March 2004.

Wilkinson P and Stewart A.M. eds. *Contemporary Research on Terrorism* Aberdeen: Aberdeen University Press 1987.

Williams P, *Organised Crime and Cyber Crime: Implications for Legitimate Business*, Carnegie Mellon University, 2002.

Wright J, *Terrorist Propaganda: The Red Army Faction and the Provisional IRA 1968-1986*, New York: St Martin's, 1990.

www.sre.gob.mx/imred/biblioteca/bol57/polinter.htm accessed 28 November 2005.

Yourdon E, *Byte Wars: The Impact of September 11 on Information Technology*, Upper Saddle River: Prentice Hall, 2002.