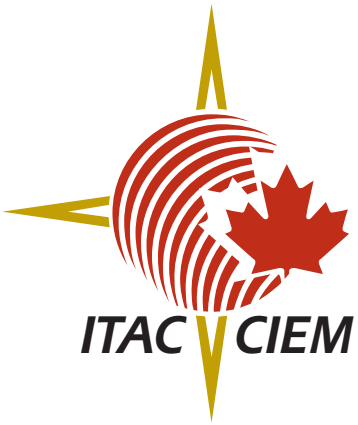
Volume 2006-2



ITAC Presents

Trends in Terrorism Series

A Framework for Understanding Terrorist Use of the Internet

This article is written by the Canadian Centre for Intelligence and Security Studies, The Norman Paterson School of International Affairs, Carleton University.

This brief outlines how the internet is being used by terrorists to more effectively recruit and fund and plan their activities. The brief outlines key concepts, current modes of activity and emerging issues. An annotated bibliography is included as an appendix.

Introduction

According to a majority of experts in the field of terrorism and counterterrorism, the presence of subversive groups and organizations on the internet has grown, and continues to grow at an alarming pace. Estimates on the number of active terrorist websites currently on the net vary. However, there is a consensus that the total number of websites has grown from under one hundred in 1996, to well over 5,000 today. In 2006, all active terrorist groups (including those organizations listed under the US *Antiterrorism and Effective Death Penalty Act* of 1996) have established their presence, in some form, on the internet. Indeed, the internet was a central tool used in the planning and coordination of the September 11th, 2001 attacks on New York and Washington. As officials and experts now know, internet traffic use by terrorists and their associates spiked noticeably prior to the attacks, indicating the need to more effectively monitor and interpret the use of the internet by subversive groups such as Al Qaeda. This finding begs the question: *What is the relationship between subversive groups and individuals (and more importantly terrorists) and the internet?*

From Denning's perspective, there are three broad methods of activity by non-state actors: "activism", "hacktivism", and "cyberterrorism"

To begin, one must identify what the internet offers to all individuals and organizations. According to the United States Institute of Peace's special report *www.terror.net: How Modern Terrorism Uses the Internet*, the internet "was hailed as an integrator of cultures and a medium for business, consumers, and governments to communicate with one another" offering "unparalleled opportunities for the creation of a forum in which the 'global village' could meet and exchange ideas, stimulating and sustaining democracy throughout the world". Some go as far as to label the internet the foundation of democratic society in the 21st century, highlighting the close alignment in the core values of the internet and democracy: openness, participation, and freedom of expression for all.

More specifically the internet possesses a number of key virtues: easy access; little or no regulation, censorship, or other forms of government control; potentially huge audiences spread throughout the world; anonymity of communication; a rapid flow of information; the inexpensive development and maintenance of a web presence; a multimedia environment; and the ability to shape coverage of the traditional mass media, which increasingly uses the internet as a source for its news coverage. While a majority of users worldwide respect these virtues, in an open and participatory environment such as the internet, where freedom of expression is arguably embodied, there are individuals and groups who view it as an ideal arena for subversive activities.

Concepts and Terms

Dorothy E. Denning's analysis of the internet as a tool for influencing foreign policy provides a framework for understanding how subversive groups and individuals (including terrorists) use the internet. From Denning's perspective, there are three broad methods of activity by non-state actors: "activism", "hacktivism", and "cyberterrorism". Acknowledging that the boundaries between the three are often fuzzy and prone to interpretation, the majority of activity carried out by non-state actors (and for the purposes of this paper, that term is used to describe subversive and terrorist groups) falls within one of these methods.

Activism refers to the normal, non-disruptive use of the internet in support of an agenda or cause; for example browsing the web for information, constructing websites and posting materials on them, transmitting electronic publications and letters through e-mail, and using the internet to discuss issues, form coalitions, and plan and coordinate activities.

Hacktivism is the union of hacking and activism; for example, operations that use hacking techniques against a target's internet site with the intent of disrupting normal operations but not causing serious damage. 'Web sit-ins' and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms are all examples of hacktivism.

Cyberterrorism is the convergence of cyberspace and terrorist activity; for example, politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. Concerns that terrorist groups or individuals may penetrate a nation's electronic energy, transportation, financial or security grid or system and cause catastrophic damage (nuclear reactor or dam failure, multiple mid-air collisions or downed airliners, disrupting national economies through stock market interference, etc.) are all related to the phenomenon known as cyberterrorism.

Analysts and experts refer to this threat (cyberterrorism) as "exaggerated"

Of the three methods of activity, it is fear of the consequences and the damage of a successful cyberattack that animates the focus of authorities, policymakers, and mass media on the danger of cyberterrorism. In fact, analysts and experts refer to this threat as 'exaggerated', and demonstrate concern that it shifts the spotlight of attention away from the more routine uses of the internet (activism) that prove to be invaluable to subversive and terrorist groups and individuals.

A December 7th, 2005 article by the Associated Press cites US FBI assistant director, Louis Reigel, as stating that Al Qaeda and related terrorist networks are presently incapable of mounting cyber-attacks that could damage US critical infrastructure. While Reigel acknowledges the increasing sophistication and technical mastery demonstrated by terror groups, FBI experts believe that they presently lack the capability to mount a significant cyber-terrorism campaign.

Engaging in cyberterrorism may in fact be counter-productive to the current strategy of terrorist groups, such as Al Qaeda, who place much more importance on exploiting the internet for its aforementioned virtues in the pursuit of their agenda. Mounting a campaign of cyberterrorism could have the effect of mainly encouraging the strengthening of cyberdefense policies, both nationally and internationally, leading to tighter regulation, control, and monitoring of activities on the internet, possibly denying the vital freedom that these groups currently enjoy and require in cyberspace.

Hacktivism occurs at a greater frequency. However, the potential for causing great harm on its own is limited. Of greater concern is its use in conjunction with the activist use of the internet by subversive groups and individuals. With relation to terrorists, hacktivism may be used to post propaganda on target sites, such as the posting of successful insurgent attacks in Iraq on US forces on the web pages of vulnerable government websites and other popular Western web forums. The same technique can be used to leave encrypted messages on public sites, and transmitting a number of communications, from manuals, to execution orders, to coordination strategies for an attack.

In addition, hacktivism may be used in coordination with a planned attack; for example, using an email bomb or 'bot attack' (the hack-in and subversion of the computers of thousands of online users to target a specific site) in order to slow down the communication networks of particular government emergency or law enforcement agencies in order to increase the likelihood of a successful attack by delaying early warning detection and response time.

Nevertheless, hacktivism remains a preferred method by individuals with the specific knowledge and skills to conduct such activities, and is more frequently used by non-violent subversive groups as a form of political activism than by terrorist groups. Undoubtedly, activism is where the majority of terrorist groups focus their activities. It is the innovative and expanding use of this method that analysts and experts believe to be the greater long-term threat to national and international security. These activities include: psychological warfare; publicity and propaganda; data mining; fundraising; recruitment and mobilization; networking; information sharing; and planning and coordination.

Terrorism and the Internet: Building Support

Before moving on to describe specifically the operation of terrorist groups in these activities, it is important to first note why the internet has become the medium through which terrorism carries on into the 21st century. Essentially, the roots of the modern internet are found in the desire of US Department of Defense (DOD) to reduce the vulnerabilities of its communication infrastructure to a Soviet nuclear attack. By designing and creating an interconnected web of computer networks, DOD achieved two important goals

for the maintenance and perpetuation of its security and defense communications infrastructure: decentralization and redundancy. Ironically, these two features now play an important strategic role in the re-organization, maintenance and perpetuation of the proclaimed 'greatest foe' of Western security services in the 21st century: international terror.

Having been denied, for the most part, geographical space in which to operate effectively, terrorist groups and networks have undergone a reorganization of sorts in cyber-space, using the aforementioned virtues that the internet provides to de-centralize their operations, all the while allowing for the information revolution to supply a redundancy in the system that ensures its survival and perpetuation.

The modern terrorist network, particularly in its 'global jihad movement' incarnation, is no longer hierarchical. A more accurate portrayal is a loose association of nodes and hubs, at some point in time directly connected into the network, and at other times operating independently. Hence, there is no option of decapitating the administrative head of the network as it no longer exists, increasing the ability of the organization to persist.

Moreover, while several nodes and hubs may be taken out at times, the organization continues to operate, and because of the built-in redundancy in the system, the activities of any given node or hub can be relocated and replaced in time, allowing for a regenerative quality to the organization that it did not possess prior. Accordingly, an understanding of the relationship between terrorist groups and the internet must recognize the centrality of the communications and technological revolution. As non-state actors, denied or lacking a physical territory from which to operate, today's terrorist groups seek to carve out a virtual territory (or virtual sanctuary) from which they can base, plan, coordinate, and carry out their agenda. The reconstitution of the internet as a type of central nervous system for organizations such as Al Qaeda is critical to their viability as an organization and as a movement.

Al Qaeda was described as the first "guerrilla movement in history to migrate from physical space to cyber space"

The Al Qaeda network and associated terrorist groups are perhaps the prototypical example of this current phenomenon. In an August 7th, 2005 *Washington Post* article by Steve Coll and Susan B. Glasser, Al Qaeda was described as the first "guerrilla movement in history to migrate from physical space to cyber space", using modern communications and information technologies to (re)create online the operational bases they once possessed in the physical world in sanctuaries such as post-2001 Afghanistan. The authors contend that the 'global jihad movement', sometimes led by Al Qaeda but increasingly made up of diverse groups and ad hoc cells with less direct links, has become a 'web-directed' phenomenon, allowing for a virtual community, guided indirectly through association of belief, to come alive. Ultimately, the activities of groups like Al Qaeda on the internet serve not only to promote their ideological and theological tenets, but to convert large portions of cyberspace into "an open university for jihad".

The activism of terrorist groups, the most prominent being Al Qaeda and its affiliates, demonstrates this trend. The use of the internet to spread disinformation, to deliver threats intended to instill fear and helplessness, and to disseminate horrific images of recent actions and attacks (videotaped executions of foreign nationals and aid worker hostages; attacks on US armed forces etc.) are all part of a deliberate campaign of psychological warfare, conducted openly and widely in cyber-space. As Gabriel Weiman of the United States Institute of Peace contends, "the internet – an uncensored medium that carries stories, pictures, threats, or messages regardless of their validity or potential impact – is peculiarly well suited to allowing even a small group to amplify its message and exaggerate its importance and the threat it poses". The internet is a medium through which non-state actors can assume to play an international role, influence public opinion, and conceivably foreign policy decisions.

Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy

Closely related to the activity of psychological warfare is that of publicity and propaganda. Before the internet, a terrorist's thirst for publicity was tempered by the 'selection threshold' of the media, who decided what stories and events were newsworthy, and most importantly how the story would be communicated to the public. Today, terrorists have direct control over the content of their messages by constructing and operating their own websites and online forums, effectively eliminating the 'selection threshold'. Terrorists have no difficulty in shaping how they are perceived by different target audiences by manipulating their own images and those of their enemies.

The Internet as a "How-to" Manual

A November 23rd, 2005 article in the *New York Times*, by Scott Shane, reports on recent moves by the US intelligence community to fuse open-source analysis into the US intelligence system. The article praises the abundance and uniqueness of information that can be garnered from endless online surfing and searching. This fact is not new to terrorists. The ability to actively use the internet for data-mining purposes is perhaps one of the most valuable services that the internet can provide. Cyber-space is an endless repository of knowledge and instruction that terrorist networks actively use.

Through data-mining, terrorists are able to gain valuable information about transportation facilities, nuclear power plants, public buildings, ports and even the counter-terrorism activities and strategies of Western security services. Moreover, they are able to collate this data in manuals, instructions, and volumes of material ranging from creating terrorist cells to evading Western authorities. From acquiring arms and material to constructing explosives (and most recently a detailed manual on how to construct chemical, radiological and nuclear devices).

Modern but inexpensive imaging software means that interactive diagrams and maps can be produced and made available for easy access. Refined search engines such as Google mean that streams of information are easily available. Sensitive information and questions that terrorists may want to keep from public online fora may be accessed through email distribution lists, chat rooms, and discussion groups.

Experts believe that sophisticated terrorist cells now operate with the assistance of large databases, set up and maintained by numerous cells working cooperatively, where intelligence on specific targets is aggregated and analyzed to assist in planning and coordinating attacks. "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of all information required about the enemy" – these are not the words of security and intelligence analysts in the West, but those of an Al Qaeda training manual recovered in January 2003 in Afghanistan.

Funding and Recruitment

An essential part of operating a terrorist network is to locate and obtain the necessary funding for their activities. The internet provides the cloak of secrecy and global reach necessary for the fundraising activities of numerous subversive groups. Al Qaeda and its affiliates, for instance, depend heavily on donations which are obtained through a global fundraising network of charities, non-governmental organizations, and other financial institutions that actively canvass on the internet through websites, chat rooms, and forums. Groups make bank account numbers and banking information publicly available on their websites and those of their associates where sympathizers may anonymously show their support through monetary contributions.

An August 8th, 2005 *Washington Post* article by Craig Whitlock discusses the case of a 31-year-old computer expert and mechanical engineer, Babar Ahmad, who was arrested on charges of running a network of websites that served as propaganda and fundraising for Islamic extremists, including Chechen rebels, the Taliban militia and Al Qaeda affiliates. On his websites, Ahmad provided account numbers where supporters could make donations. In a more proactive approach, terrorists use modern software to capture internet user demographics (and those of their affiliates and front organizations) to identify those who may be sympathetic to a related cause or issue. These people are then individually contacted by email and asked to make a donation to an organization with no direct ties to the terrorist organization.

This process of capturing information and profiles of the users who browse their websites is also used for the related activities of recruitment and mobilization. Users who seem most interested or well-suited to carrying out an organization's cause are contacted much in the same manner as those solicited for donations. The increasing ability to interact personally online has offered terrorist groups and recruiters the option of being more proactive in their recruitment drive. Recruiters roam online chat rooms and cybercafés, post messages on online bulletin boards, looking for receptive individuals, and particularly vulnerable youth, who, through grooming and encouragement in a private online setting, can encouraged to join the ranks of a terrorist group. The Dutch General Intelligence and Security Service's Annual Report for 2004 notes the importance of the internet, specifically in the radicalization of parts of the Muslim communities in the Netherlands, through 'virtual' dawa (online radical sermons) and increasingly through unmonitored chat rooms, where intensive exchange of Islamic ideas is taking place more and more along the electronic highway (a self-directed method) as opposed to personal indoctrination by preachers.

This phenomenon is not limited to the Netherlands. Once identified, potential recruits are bombarded with religious decrees, propaganda, and training manuals on how to become a part of the 'global jihad movement'. Those who become ensnared either by rhetoric or curiosity are then guided through an online maze of secret chat rooms or instructed to download software called *Paltalk*, which enables users to speak to each other on the internet without fear of being monitored, at which point the personal online indoctrination begins.

Many terrorist groups have undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of semi-independent cells with no single commanding hierarchy

Networking

According to Weiman, many terrorist groups have "undergone a transformation from strictly hierarchical organizations with designated leaders to affiliations of semi-independent cells with no single commanding hierarchy". The communications and technology revolution embodied in the internet has greatly reduced the time and cost of communication, while increasing the variety and complexity of information that can be shared online. Networking facilitates the reorganization of modern terrorist organizations into decentralized arrays of transnational groups, linked to others with similar agendas or beliefs, communicating and coordinating horizontally rather than vertically, with speed and complexity.

The ability to network more easily with cells and other groups worldwide allows for the more effective use of the internet in the planning and coordination of actions and attacks. The events of September 11th, 2001 are perhaps to date the most illustrative example of the medium the internet provides for those individuals and organizations who desire to plan, coordinate and carry out attacks in Western democracies. The

Al Qaeda operatives used the internet in public places and communicated using free web-based email accounts to preserve anonymity. Similarly, other groups like Hamas use chat rooms to discuss and plan operations, while operatives use email to coordinate actions across Gaza, the West Bank, Lebanon and Israel. Instructions are delivered electronically through code, usually in difficult-to-decipher dialects for which Western intelligence and security services have few or no trained linguists.

Terrorist groups also use a method known as a 'virtual dead drop' to relay some of their most sensitive information with regard to planning and coordination. This involves the opening of an account on a free, public email service (i.e. Hotmail), where the a message is written and saved in draft form, at which point the email account name and password are transmitted in code or in chatter on a secure message board. The recipient can then access the account and read the draft message. Instructions in the form of interactive maps, detailed photographs, directions and technical details are known to be disguised by means of stenography (which involves the careful concealment of files or messages in graphic files).

Conclusion: The Near Future

Recently a dispatch from the Criminal Intelligence Service of Canada described the activities of an internet forum member, who goes by the name 'Ayaf' and is a prolific contributor to the Islamic Renewal Organization (IRO) website. In an October 3, 2005 statement on the website, 'Ayaf' announced that he had direct contact with an Al Qaeda affiliated person and was instructed to convey orders to the Al Qaeda division in the US, led by Abu-Azzam al-Amriki, to destroy a nuclear reactor.

A November 10, 2005 *Washington Post* article by Molly Moore and Daniel Williams reports on the influence of online French blogs and mobile phone text messaging in the organization, mobilization, and inciting of mobs of young French Muslims to violence in the suburbs of Paris and some 300 other cities across France.

These two events clearly show that during a crisis, the internet is a valuable tool for distorting the debate and disseminating misleading images of reality, as well as fueling emotions with messages of hatred and promotion of violence. They also highlight the importance of such forums as conduits for operational information to be passed on, and the coordination of activities between terrorist cells operating in different geographical spaces. Perhaps foreshadowing events to come, they also demonstrate the difficulty authorities face when monitoring and controlling such behaviour. ◆

Bruno Nordeste
David Carment

Carleton University,
Ottawa

APPENDIX: SOURCES

NEWS ARTICLES AND DISPATCHES (by date)

***Washington Post:* "Terrorists Turn to Web as Base of Operations"** – by Steve Coll and Susan B. Glasser, Sunday, August 7, 2005 (available at http://www.washingtonpost.com/wpdyn/ content/article/2005/08/05/ AR2005080501138.html)

- Intelligent article, part of series by the *Washington Post*, examining the relationship between the global jihad movement (as represented by Al Qaeda) and the Internet.
- Argues that Al Qaeda has become the first "guerrilla movement in history to migrate from physical space to cyber space", using modern communications and information technologies to (re)create online the operational bases they once possessed in the physical world in sanctuaries such as post-2001 Afghanistan.
- The 'global jihad movement', sometimes led by Al Qaeda but increasingly made up of diverse groups and ad hoc cells with less direct links, has become a 'web-directed' phenomenon, allowing for a virtual community, guided indirectly through association of belief, to come alive.
- The article describes the growing library and archives of material made available and circulated widely online among members of this virtual community, from online sermons, theoretical, theological, scientific papers, to maps and manuals, all serving to indoctrinate, recruit, communicate, train, f fund, mobilize, and organize the 'global jihad movement'.
- Ultimately, the activities of groups like Al Qaeda on the internet serve not only to promote their ideological and theological tenets, but also to convert large portions of cyberspace into "an open university for jihad".
- The article also describes the emerging trend of the creation of 'virtual cells', where like-minded individuals meet and anonymity is preserved until mutual bonds of trust are created, and training is complete, at which point the group is prepared to meet and conduct an operation in the field.

***Washington Post:* "Briton Used Internet as His Bully Pulpit"** – by Craig Whitlock, Monday August 8, 2005 (available at http://www.washingtonpost.com/wpdyn/ content/article/2005/08/07/AR2005080700890.html)

- Intelligent article, part of series by the *Washington Post*, examining the relationship between the global jihad movement and the internet.
- Examines the case of 31-year-old computer expert and mechanical engineer Babar Ahmad, who was arrested on charges of running a network of websites that served as propaganda and fundraising for Islamic extremists, including Chechen rebels, the Taliban militia and Al Qaeda affiliates.
- Demonstrates the belief that the global jihad movement is not limited to a military engagement, but is also an information war, and that the most effective military jihad is to use the internet to spread ideas; to harness the power of words.

***Washington Post*: "The Web as Weapon"** – by Susan B. Glasser and Steve Coll, Tuesday, August 9, 2005 (available at http://www.washingtonpost.com/wpdyn/ content/article/2005/08/08/AR2005080801018.html)

- Intelligent article, part of series by the *Washington Post*, examining the relationship between the global jihad movement and the Internet.
- Examines the astounding success that Abu Musab al-Zarqawi, and his Al Qaeda militants in Iraq, have had in intertwining their real-time guerrilla conflict with the online electronic jihad.
- Remarkable not only for the volume of content Zarqawi's 'information wing' is able to release for a world audience, but also for the level of sophistication in setup and presentation, as well as how astonishingly fast his 'online empire' has developed; non-existent little more than a year ago.
- Zarqawi is an example of the new generation of mujaheddin, adept and willing to use the conveniences and advances of modern communications and information technology to level the playing field where possible, and overcome the handicap of the overwhelming military superiority of the US.

DEBKA File Special Report: "New Surge in Al Qaeda's Internal Electronic and Human Traffic" – August 13, 2005 (available at http://www.debka.com/article.php?aid=1070)

- Reports on a heightened volume of Al Qaeda's internal communications, signals, publications and websites, mostly in code, the likes seen in the months leading up to the September 11th, 2001 attacks.
- According to the article's interpretation, the coded communications passing around internal sites indicate a movement and shifting of personnel and new recruits, and indicate a renewed capability for the network to carry out multiple attacks in several target arenas.
- Authors believe that surge of activity, electronic and human, seems to signpost an Al Qaeda offensive in the works, and despite its uncorroborated nature, given the quality of intelligence on the Al Qaeda network possessed by Western intelligence agencies (which has not improved in the opinion of the authors), internal electronic traffic must be treated as a serious guide to the organization's intentions.
- Probably the article's most important contribution is highlighting the importance that should be given to the volume and tone of electronic traffic (most which is coded and inaccessible to outsiders) among terrorist networks.

Glenmore Trenear-Harvey – Intelligence Digest: " Al Qaeda Embarks on Internet Media Campaign to Terrorize US" – by Habib Trabelsi, News24.com, August 19, 2005

- Reports that an Al Qaeda linked "Brigade of Media Jihad" is embarking on an internet-based campaign to terrorize the United States by disseminating images of killings and casualties among Americans in Iraq.
- Recognizing the importance of the media battle to the success of the war on the ground, the group has called on militants to post gruesome and terrifying images of death and destruction in order to terrorize and demoralize the enemy.
- Such a tactic is not limited to US-led forces, but extended though to their families and relatives in the US through a mass emailing and hacking strategy to convey these images internationally.

- A technical document advising on best practices for use of cameras and other image-capturing devices was published along with the call for postings.
- This article demonstrates the centrality the internet plays in attempts by Al Qaeda related groups to convey their message, and more importantly to engage in information warfare.

Globe and Mail: **"Ottawa to give police more power to snoop"** - by Bill Curry, Friday, August 19, 2005

- The article discusses the Canadian government's intention to introduce legislation in the fall of 2005 that would give police and national security agencies new powers to eavesdrop on cell phone calls and monitor internet activities of Canadians.
- The bill is set to update what the Minister of Justice has called "outdated surveillance laws" written before the telecommunications revolution (1974).
- The legislation would require internet service providers to retain records on the internet use of their clients, including surfing habits of individuals and online pseudonyms, and store them in a manner that is easily retrievable by authorities.
- Concern has been voiced that these new measures are creating far-reaching and intrusive new surveillance powers that may be abused and reveal sensitive information about unaware Canadians.
- This new legislation can be seen as an attempt by government to place law enforcement individuals on the same level playing field as criminals and terrorists in the matter of using technology and accessing technology.

Toronto Star: **"Terrorism/Internet – A Virtual Sanctuary for Al Qaeda networks"** – by Shawn Brimley and Aidan Kirby, August 23, 2005 (www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/layout/Article_PrinterFriendly&c=Article&cid=1124747413259&call_pageid=968256290204)

- The article is an intelligent analysis of the way the internet is being used as a "virtual sanctuary" by Al Qaeda terrorist networks.
- Al Qaeda appears to be winning the war in cyberspace as the web has become the organization's communications network, recruiting vehicle, fundraising mechanism and training camp, with every dimension of the global jihad, at least in some measure, taking place online.
- The migration of Al Qaeda into cyberspace, with terrorist-related websites exploding from under 20 in 1998 to more than 4,500 presently, has outpaced the ability of Western intelligence agencies to monitor their activities online and formulate responses.
- The internet is not simply a tool for terrorists; it constitutes a type of central nervous system for organizations such as Al Qaeda, and remains critical to its viability as an organization and a movement, as well as contributing to its regeneration.
- Any strategy that seeks to undermine global terrorist networks must recognize the internet as a vital component to their ability to communicate, organize and persist.

***BBC News:* "Saudi dissident shuts down site"** – August 28, 2005 (http:news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/4191396.stm)

- News story about Dr. Muhammed al-Massari's controversial website, which has allowed postings of images of suicide bombings in Israel and Iraq as well as allowing messages from Al Qaeda supporters to be viewed.
- The article brings forth the issue of free speech and the boundaries of decency and security in the realm of cyberspace.
- Efforts to shut down the site were successful, and government officials have called for Dr. al-Massari's deportation, which is being contested by civil liberties groups including Amnesty International.

FBIS Feature *(FEA20051004010077)*: "Analysis: Increasing Prolific Contributor Posts Threat to US Nuclear Reactor" – October 5, 2005 (Article obtained from Greg OHayon, CISC)

- The article discusses the activities of internet forum member who goes by the name 'Ayaf' and is a prolific contributor to the Islamic Renewal Organization (IRO) website (www.tajdeed.com.uk/forums).
- While previous postings by 'Ayaf' were limited to reposts of jihadists' statements and news articles, as well as personal information about himself, an October 3, 2005 statement was the first of its kind to announce a direct contact with an Al Qaeda affiliated person and convey orders to the Al Qaeda division in the US led by Abu-Azzam al-Amriki to destroy a nuclear reactor in the US, as well as outlining the geographic areas of responsibility for the Al Qaeda leadership.
- This article highlights the importance of such forums as conduits for operational information to be passed on, and the coordination of activities between terrorist cells operating in different geographical spaces.
- It also points out the increased traffic in communication (in this instance a flurry of postings and involvement in forum discussions) as an indication of the possible coordination of a terrorist action.
- Also of importance was the remarkable ability of the website to change server locations rapidly as law enforcement and government authorities repeatedly attempt to shut it down; changing server location three times in a span of less than two months after the July 7th London bombings, from London, to Hong Kong, and finally in Germany.

The Middle East Media Research Institute: Special Dispatch Series, No. 1004 "On Islamic Websites: A Guide for Preparing Nuclear Weapons" – October 12, 2005 (http://memri.org/bin/latestnews.cgi?ID=SD100405)

- Dispatch produced by the Middle East Media Research Institute reporting on the Islamic websites providing guidance for the preparation of nuclear weapons.
- On October 6, 2005, on the Islamist forum http://alfirdaws.org/forums/showthread.php?t=5268&page=1&pp=10, a document labeled "An Encyclopedia for the Preparation of Nuclear Weapons" was posted for open circulation among forum members.
- The document is approximately 80 pages in length and divided into nine lessons prepared as a 'scientific research by Jihad Fighter No.1' who claims to have been studying nuclear physics and missile technology through various scientific and jihadist forums.

- Included in the nine lessons are a historical survey of the development of nuclear science, explanations about natural radioactivity, the nuclear qualities of certain 13 materials, critical mass, the construction of nuclear weapons, and the extraction of radium.
- While the document does not speak to the actual capability of terrorist cells to put together such a device, it conveys the belief that the strategic balance of jihad fighters from a military point of view cannot change without proper scientific progress, and more importantly demonstrates the usefulness of such internet forums as basic information-sharing and networking tools, allowing for combined expertise to advance the knowledge base of terrorist networks.

The Straits Times: **"Countering militant Islam in cyberspace"** – by Mafoot Simon, Tuesday, October 18, 2005 (http://www.asiamedia.ucla.edu/article.asp?parentid=31719)

- Reports that the Internet is no longer a simple tool for terrorists, it is central to their operations; recruiting members, soliciting funds, promoting ideology, and increasingly coordinating tactical operations and training recruits.
- Internet is an ideal medium for today's terrorism, providing anonymity while ultimately allowing an immense degree of pervasiveness.
- More recent and disturbing trend is the ability of the numerous jihadi forums to cater and capture those young internet-savvy Muslims simply interested in understanding their religion better, particularly through online sermons; the battle for the hearts and minds of Muslims has gone onto cyberspace, where alternate and moderate views are dangerously under-represented.
- The author suggests that the efforts to educate and promote internet awareness among the larger Muslim community, and local Muslim lay leaders in particular (making them cyber-comfortable) is the most effective way to combat the terrorist appeal online; by taking 'their' fight to the net, posting the contents of their talks and forums on their own websites, they could provide alternatives and dialogue in a medium that is increasingly dominated by extremist views.

The Times: **"Deported Jihadists resume UK activity by Internet"** – by Sean O'Neill and Yaakov Lappin, October 23, 2005 (http://www.timesonline.co.uk/article/0,,22989-1835824,00.html)

- Article reports on the activities of exiled radical Islamist cleric Omar Bakri Mohammad, particularly his ability to continue to reach his followers through websites and internet chat rooms.
- This is indicative of Al Qaeda and its affiliates' attempt to use the internet to lure a less-visible generation of recruits in Western countries like the UK.
- Using the popular Paltalk internet network, run by a New-York-based company, extremist clerics like Bakri are able to continue reach large audiences.

The Sunday Times: **" Al Qaeda woos recruits with nuclear bomb website"** – by Uzi Mahnaimi and Tom Walker, November 6, 2005 (http://www.timesonline.co.uk/article/0,,2089-1859222,00.html)

- Reports on the posting, in Arabic, on an Al Qaeda website of detailed instructions on how to make nuclear, 'dirty' and biological bombs.
- The website has attracted more than 57,000 hits and hundreds of readers and inquiries, which creates concern that the site could be boosting Al Qaeda's appeal to would-be recruits.

- Document is 80 pages long and divided into 9 lessons, and has alarmed nuclear physicists because of its detail and proper instruction going well beyond generic principles.
- Indicates that the Al Qaeda organization is serious about obtaining and deploying weapons of mass destruction.
- Greater concern is given to the impact such postings may have on vulnerable young Muslims, who may interpret the site's popularity as an indication of the strength and allure of the Al Qaeda organization.

Washington Post: **"France's Youth Battles Also Waged on the Web"** – by Molly Moore and Daniel Williams, November 10, 2005 (http://www.washingtonpost.com/wpdyn/ content/article/2005/11/09/AR2005110902134.html)

- Reports on the influence of French internet blogs and text messages in organizing, mobilizing, and inciting mobs of young French Muslims to violence in the suburbs of Paris and some 300 other cities across France.
- Demonstrates how internet can increase the momentum of the crisis, by distorting the debate and disseminating misleading images of reality, as well as fueling emotions with messages of hatred and promotion of violence.
- The difficulty with monitoring and controlling the content of blogs and online forums was also noted.

Weekend Australian: **"Militant website shows attack tactics"** – by correspondents in Jakarta, November 19, 2005 (http://www.theaustralian.news.com.au/common/story_page/0,5744,17294708%255E170 2,00.html)

- Reports on the use of websites by Jemaah Islamiyah to give guidance to militants on terror tactics, targets and attacks.
- Website instructs militants how to attack foreigners in Jakarta, providing charts of several public locations with details on their value as targets with viable escape routes.

New York Times: **"A T-Shirt-and-Dagger Operation"** – by Scott Shane, November 23, 2005 (http:// www.globalsecurity.org/org/news/2005/051113-osint.htm)

- Reports on moves by US intelligence community to fuse open-source analysis into the US intelligence system.
- Open source intelligence, or OSINT for short, is a low-cost way to try to understand the Islamic militancy that fuels Al Qaeda, by gathering insights not only from foreign newspapers and television, but also from the abundance of sources provided through the internet, as well as other unique sources (i.e music, t-shirt slogans etc.)
- The article reports on this new trend in intelligence-gathering, which provides context through endless online surfing and searching.

Associated Press: **"FBI: Internet-Based Attacks Unlikely"**- Mark Sherman, December 7, 2005 (http:// www.usatoday.com/tech/news/computersecurity/2005-12-07- fbi-terrorism-web_x.htm?csp=34)

- Article cites US FBI assistant director, Louis Reigel, saying that Al Qaeda and related terrorist networks are incapable of mounting cyber-attacks that could damage US critical infrastructure.

- While acknowledging the increasing sophistication and technical mastery demonstrated by terror groups, FBI experts believe that they presently lack the capability to mount a significant cyber-terrorism campaign.
- Also notes that terrorists have made only infrequent use of stenography (hiding a text message in another kind of file, typically a picture).

EMIC ARTICLES, JOURNALS, REPORTS, WEB FORUMS AND CONFERENCE PAPERS (by date)

***AIVD Annual Report 2004*: Dutch General Intelligence and Security Service** – 2004 (http://www.fas.org/irp/world/netherlands/aivd2004-eng.pdf)

- Lengthy report produced by the Dutch General Intelligence and Security Service, covering a broad range of issues and developments relating to security and intelligence.
- Includes a specific section devoted to the topic of terrorism, highlighting not only the latest issues and development but also the activities of various specific and identifiable groups believed to be operating in the Netherlands or Europe.
- Notes the importance of the internet, specifically in the radicalization of parts of the Muslim communities in the Netherlands, through 'virtual' dawa (online radical sermons) and increasingly through unmonitored chat rooms; intensive exchange of Islamic ideas is taking place more and more along the electronic highway (a self-directed method), as opposed to personal indoctrination by preachers.
- Report also briefly highlights efforts by AIVD to monitor, collect and collate data and reports of incidents of electronic or cyber-attacks.

United States Institute of Peace: "Special Report: www.terror.net - How Modern Terrorism Uses the Internet" – by Gabriel Weimann, Special Report 116, March 2004 (www.usip.org)

- The most useful and direct source in understanding how modern terrorist organizations use the Internet.
- Report provides an explanation of the phenomenon of modern terrorism and the Internet, including an overview of the Internet's creation and original purpose, evolution, and allure to terrorist organization.
- A useful overview of some of the current terrorist websites in existence, divided by geographical location, with explanation of content and target audiences, is provided.
- The bulk of the report is devoted to the differing uses of the Internet by terrorists, divided into several categories with detailed analysis: psychological warfare; publicity and propaganda; data-mining; fundraising; recruitment and mobilization; networking; sharing information; and planning and coordination.

International Summit on Democracy, Security and Terrorism: "Madrid – Terrorism, the Internet and Democracy" – March 8-11, 2005 (http://english.safe-democracy.org/index.html)

- Excellent website devoted to the International Summit on Democracy, Security and Terrorism held in Madrid in March of 2005.

- Explores multiple dimensions of terrorism and their effects on the security postures and responses of Western democracies.
- Special working group devoted to the analysis of the relationship between terrorism and the internet, and the effect of security strategies on democratic institutions.
- Claims that the internet is a foundation of democratic society in the 21st century, because of their closely aligned core values of openness and freedom, warns that over regulation and restriction of the internet in democratic societies may undermine the same values that democracies seek to protect.
- Provides conclusions and recommendations, including: embracing the open internet as a foundation of 21st-century democracy and adopting it as a tool in the fight against terrorism; recognize the importance of and strengthen the internet infrastructure against attacks; work to increase the availability of access worldwide (address the 'digital divide'); protect the right to free speech in any forum; resist attempts at international governance of the internet.
- The entire site is an excellent source of material on global trends of terrorism, and provides the foundation for open and educated dialogue on the subject.

***International Journal of Intelligence and Counter-Intelligence:* "The Intelligence Services' Struggle Against Al Qaeda Propaganda"** – by Javier Jordan, Manuel R. Torres, and Nicola Harsburgh, Volume 18, Issue 1, Spring 2005

- The article highlights the importance and attention that anti-terrorist campaigns must pay to the complementary strategies that accompany terrorist action, and consequently prove crucial for the continuity or disappearance of the terrorist network; namely aspects of propaganda and perception management which presently find amplification and wide audiences through the use of modern telecommunication and information technologies.
- Authorities and experts must begin to pay close attention to the battle that is raging on the internet; the 'Netwar' paradigm.
- The authors contend that although the radical ideology that animates the group originates from an extremist and primitive form of intolerance, the organization and modus operandi reflect an advanced adaptation towards the new environment of globalization and the information revolution.
- While funding, training, and acquisition of weapons and explosives remain crucial, in the authors' opinion, it is the information and propaganda battle that constitutes and essential pillar under which organizational architecture resides and continuity is assured; hence the vital importance of a modern medium like the internet.
- Once the message of the global jihad movement, which permits universal understanding, is elaborated and distributed, the likelihood of forging transnational alliances and interaction between dispersed points is increased, all the while supported by the information revolution; meaning the movement becomes organized into nebulous networks (with no clear hierarchy and thus incapable of being decapitated) allowing for the realization of 'franchise terrorism', maintenance and increase of social base of support, potential for amateur terrorism, and perpetuation of the narrative of modern jihad.

NATO Joint STS-CNAD Advanced Research Workshop April 8-11, 2005: "Terrorism and the Use of Communications – Countering the Terrorist Information Cycle" – from Bruce Jones, Chairman, May 3, 2005

- Excellent source discussing the current dimension and nature of terrorist communications, with interrelated cultural, technical and operational components, as well as the perceptions and responses of Western governments and possible countermeasures, interdiction, pre-emption and disruption strategies.
- Lists findings of joint research workshop including the use of the internet in grooming, conditioning and recruitment, communicating 'orders of battle', sharing of technical, tactical and targeting information, shortcomings of armed forces and law enforcement, lack of suitable linguists and forensic information technology specialists (more importantly, individuals with both professional skill sets).
- Outlines conclusions and recommendations including: the need for internationally agreed judicial approaches; international co-operation and co-ordination of law enforcement and intelligence agencies; development and harnessing of linguistic and forensic information technology skills among Western professionals; direct and relevant approaches and strategies of engagement with Islamic populations worldwide; technical hacking of undesirable sites; analysis of existing groups using the internet for criminal purposes to identify applicable patterns and synergies; and effective security education to encourage more informed media coverage of issues and events, and stimulate public awareness.

Terrorism Research Centre: "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" - by Dorothy E. Denning, Sponsored by the Nautilus Institute, June 6, 2005 (http://www.terrorism.com/modules.php?op=modload&name=News&file=article&sid=1211 0)

- Very useful academic article analyzing the strategic use of the Internet and its relationship to accomplishing foreign policy objectives.
- Author divides and examines the use of the internet into three broad and overlapping categories: activism, hacktivism and cyberterrorism, concluding that those groups using the strategies based on the first category are more likely to accomplish their foreign policy goals than the other two.
- This article provides a very important framework through which to understand the differing methods and tactics through which a group or individual can use the internet, and can be applied to gain an understanding of the relationship between terrorism and the internet.

Terrorism Focus: **" Al Qaeda's Next Generation: Less Visible and More Lethal"** – by Michael Scheuer, Volume 2, Issue 18, October 4, 2005 (http://jamestown.org/terrorism/news/article.php?issue_id=3481)

- Examines the emerging generation of Al Qaeda operatives and their ability to embrace and be educated and more adept at using the tools of modernity, particularly communications and weapons, to accomplish their goals, than their predecessors.
- Their intense piety will come from having grown up in a world where the internet and satellite television have given a major outlet to the struggles of the Muslim people around the world, allowing for a greater comfort in a shared and common Muslim identity, and certainty of the role of the West (led by the US) in oppressing the Muslim cause.
- Their professionalism will come from being drawn primarily from the middle and upper middle classes, providing them with comfort and know-how on most of the current communications and information technologies.

- The author believes that the West fails to understand Al Qaeda in the manner it understood the Soviet Union as an adversary, and that it must overcome this institutional malaise in order to meet the challenges presented by the new generation of mujahideen.

Jamestown Foundation: "Technology and Security Discussions of the Jihadist Forums: Producing a More Savvy Next Generation" – October 11, 2005

- Report produced by the Jamestown Foundation on the technology and security discussions on jihadist internet fora, and their utilization to train a more proficient next generation of jihadists.
- Discusses the importance of emerging online forums as a grassroots medium through which individuals without any particular affiliation can post a document or manual of their own creation, subsequently usable as standard procedure for terrorist cells.
- Of particular importance is the emphasis on "know-how", the dissemination of basic security guidelines for hacking and for mobile phone use greatly enhaces the effectiveness of aspiring jihadists, as they make fewer security errors and leave behind a lesser number of leads for authorities and intelligence services.
- Uses example of two recent manuals posted on two internet forums (www.minbarislam. com/forum and www.al-farouq/vb) where basic user-friendly documents are widely and quickly circulated among users, adding to the value of the manual.
- The overall effect is the possibility of creating a new generation of aspiring jihadists with increasing levels of technical and tactical prowess, and the confidence and eagerness to test and use their newly learned skills.

Organization for Security and Co-operation in Europe: "Expert Workshop on Combating the Use of the Internet for Terrorist Purposes" – presented by The Office of the Representative on Freedom of the Media and The Office for Democratic Institutions and Human Rights, October13-14, 2005 (http://www.osce.org/documents/odihr/2005/10/16705_en.pdf)

- Workshop recognizes the threat posed by the increasing terrorist presence and use of the internet to disseminate materials designed to encourage acts of terrorism and the transfer of funds, and to communicate, plan, and co-ordinate activities and attacks.
- However, the purpose of the workshop, and the paper presented, is to try to address these issues while also highlighting the inherent danger to certain important rights relating to private life, freedom of the media and freedom of expression, when governments or authorities begin to interfere with and monitor materials published on the web, banking transfers, or private correspondence conducted over the Internet.

Jamestown Foundation: "An Online 'University' for Jihad" – by Stephen Ulph, *Terrorism Focus*, Volume 2, Issue 19, October 18, 2005 (http://jamestown.org/terrorism/news/article.php?articleid=2369807)

- Claims that AlQaeda's presence on the Internet has developed to the point of presenting itself as a permanent cultural, as well as military, phenomenon.
- An October 7 posting on a jihadi forum (www.al-farouq.com) by the 'deputy general emir' of the Global Islamic Media Front announced the creation of an "Al Qaeda University of Jihad Studies", proclaiming that Al Qaeda is an organization, a state and a university.

- The goal, the author claims, is to use the worldwide internet infrastructure to create a decentralized university without geographical borders, present in every place; providing not only military training, but also rigorous ideological and moral education.
- The so-called 'graduates' of this virtual university pass through each of its 'faculties' making them specialists in 'electronic jihad', 'media jihad', 'spiritual and financial jihad'.

Council on Foreign Relations: "Terrorism: Questions & Answers – How do terrorist organizations use the internet?" – Accessed November 26, 2005 (http://cfrterrorism.org/home/)

- Useful brief overview of the manner in which terrorist networks may and do use the internet to support and conduct their operations.
- Acknowledges an explosion in terrorist-related websites over the last ten years (from less than 100 to more than 4,000).
- Terrorists use the internet to give orders, plan attacks, transfer funds, all within the safety of numerous online message boards and chat rooms.
- Terrorist sites also serve as virtual training grounds, offering tutorials and manuals on diverse subject matter, broadcast propaganda, raise funds, and recruit new members.
- Internet can also provide a theatre through which critical energy, transportation, and security infrastructure could be attacked via cyber-terrorism.
- Terrorist websites also provide an opportunity for intelligence agencies to monitor activities, ommunications and trends, as well as gather valuable information that may allow for early warning of pending attacks.

Intelligence and Terrorism Information Center at the Center for Special Studies: "The Palestinian Islam Jihad Internet infrastructure and its Internet Webhosts" – December 28, 2005 (http://www.intelligence.org.il/eng/eng_n/internet_e1205.htm)

- Interesting case evaluation of the internet presence of a specific terrorist organization.
- Lists and details 5 websites that post, host, and disseminate material promoting the cause and ideology of the Palestinian Islamic Jihad, including analysis of the content, names of individuals who support or contribute to the site, web addresses, internet protocol addresses, names and adresses of the webhosts and, where available, names and addresses of contacts who manage the site.

The Jamestown Foundation: "Internet Mujahideen Intensify Research on US Economic Targets" – by Stephen Ulf, January 18, 2006 (http://www.jamestown.org/news_details.php?news_id=155)

- Reports on the continued interest of terrorist networks to target US economic targets, most specifically energy infrastructure both within and outside the United States, as part of a greater strategy termed 'bleed-until-bankruptcy'.
- This strategy was underlined in a posting last October on the forum Minbar Suriya al- Islami of Abu Musab al-Najdi's Al Qaeda's Battle is an Economic Battle, Not a Military One, in which the targeting was extended to Kuwait, Saudi Arabia and Venezuela (www.nnuu.org.vb); it is accompanied by URLs providing information, maps, and images of distribution networks, transportation hubs and military fuel supply depots.

- Experts are concerned with the level of research traffic that such forums are creating as they solicit greater participation from forum readers who are experts in petrochemical engineering, distribution networks and pumps, specifying the need for PDF documents of books relevant to the subject.
- This article highlights two important facets of the value of the internet for global jihad movement: first, it points to the speed of communication and the potential power that dispersed jihadi sympathizers across the globe can focus on a single project; second, it demonstrates the extent to which the web has become a facility for data-mining purposes allowing instant access not only to academic research data but also sensitive infrastructure details of utilities, distribution and transport networks, as well as threat and vulnerability perceptions of these facilities.