Terrorist Use of the Internet: Exploitation and Support through ICT infrastructure

Namosha Veerasamy, Marthie Grobler
Council for Scientific and Industrial Research, Pretoria, South Africa
nveerasamy@csir.co.za
mgrobler1@csir.co.za

Abstract: The growth of technology has provided a wealth of functionality. One area in which Information Communication Technology (ICT), especially the Internet, has grown to play a supporting role is terrorism. The Internet provides an enormous amount of information, and enables relatively cheap and instant communication across the globe. As a result, the conventional view of many traditional terrorist groups shifted to embrace the use of technology within their functions. The goal of this paper is to represent the functions and methods that terrorists have come to rely on through the ICT infrastructure. The discussion sheds light on the technical and practical role that ICT infrastructure plays in the assistance of terrorism.

The use of the Internet by terrorist groups has expanded from traditional Internet usage to more innovative usage of both traditional and new Internet functions. Global terrorist groups can now electronically target an enormous amount of potential recipients, recruitees and enemies. The aim of the paper is to show how the Internet can be used to enable terrorism, as well as provide technical examples of the support functionality and exploitation. This paper summarises the high-level functions, methods and examples for which terrorists utilise the Internet. This paper looks at the use of the Internet as both a uni-directional and bi-directional tool to support functionality like recruitment, propaganda, training, funding and operations. It also discusses specific methods like the dissemination of web literature, social-networking tools, anti-forensics and fund-raising schemes. Additional examples, such as cloaking and coding techniques, are also provided. In order to analyse how ICT infrastructure can be used in the support of terrorism, a mapping is given of communication direction to the traditional Internet use functions and methods, as well as to innovative Internet functions and methods.

Keywords: anti-forensics, Internet, terrorism, ICT, propaganda, social-networking

1. Introduction

According to the Internet World Stats webpage, the latest number of world Internet users (calculated 30 June 2010) are 1 966 541 816 representing a 28.7% penetration of the world population (2010). Although this does not reflect a majority of the world population, it presents an enormous amount of potential recipients, recruitees and enemies that global terrorist groups can target electronically. However, terrorist groups' embracing of technology used to be an uncommon phenomenon.

In the book, *The secret history of al Qaeda,* an eye witness to the al Qaeda men fleeing United States bombardments of their training camps in November 2001 are quoted: *"Every second al Qaeda member [was] carrying a laptop computer along with his Kalashnikov"* (Atwan 2006). This scenario is highly paradoxical where an organisation utterly against the modern world (such as al Qaeda), are increasingly relying on hi-tech electronic facilities offered by the Internet to operate, expand, develop and survive. Especially in the early 1980s, some groups in Afghanistan were opposed to using any kind of technology that is of largely Western origin or innovation (Atwan 2006).

However, the world has changed. Technology has been introduced in most aspects of daily lives and the Internet has become a prominent component of business and private life. It provides an enormous amount of information and enables relatively cheap and instant communication across the globe. As a result, the traditional view of many traditional terrorist groups shifted to embrace the use of technology within their functions. In 2003, a document titled *'al Qaeda: The 39 principles of Jihad'* was published on the al-Farouq website. Principle 34 states that 'performing electronic jihad' is a 'sacred duty'. The author of the principle document calls upon the group's members to participate actively in Internet forums. He explains that the Internet offers the opportunity to respond instantly and to reach millions of people in seconds. Members who have Internet skills are urged to use them to support the jihad by hacking into and destroying enemy websites (Atwan 2006).

Keeping this principle in mind, the use of the Internet by terrorist groups has expanded from only traditional Internet usage to more innovative usage of both traditional and new Internet functions. This

paper will summarise the high-level functions, methods and examples for which terrorists utilise the Internet. The examples and methods often provide for various functions and thus a strict one-to-one mapping cannot be provided. Rather, the examples given shed light on the technical and practical role that ICT infrastructure plays in the support of terrorism.

2. Functionality of the Internet

Terrorists use the Internet because it is easy and inexpensive to disseminate information instantaneously worldwide (Piper 2008). By its very nature, the Internet is in many ways an ideal arena for activity by terrorist groups. The Internet offers little or no regulation, is an anonymous multimedia environment, and has the ability to shape coverage in the traditional mass media (Weimann 2005).

Whilst the Internet was originally created to facilitate communication between two computers, its functionality now extends to information repository as well. Figure 1 shows the general functions that terrorists may use the Internet for, with an indication of which type of methods are used for each functionality type.

- **Recruitment** – the process of attracting, screening and selecting individuals to become members of the terrorist groups; both web literature and social networking tools can be applied for this purpose.
- **Training** – the process of disseminating knowledge, skills and competency to new recruits with regard to specific topics of knowledge that may be needed during terrorist operations; social networking tools and anti-forensics methods are employed for this purpose.
- **Communication** – the process of conveying information to members of the terrorist group; social networking tools and anti-forensics methods are employed for this purpose.
- **Operations** – the direction and control of a specific terrorist attack; web literature, anti-forensics and fundraising methods are employed for this purpose.
- **Propaganda** – a form of communication aimed at influencing the terrorist community toward a specific cause; both web literature and social networking tools can be applied for this purpose.
- **Funding** – financial support provided to make a specific terrorist operation possible; fundraising methods are used for this purpose.
- **Psychological warfare** – the process of spreading disinformation in an attempt to deliver threats intended to distil fear and helplessness within the enemy ranks; both web literature and social networking tools can be applied for this purpose.

The Internet is the perfect tool to exploit in order to support terrorist activities. Not only does it provide location independence, speed, anonymity and internationality, but is also provides a relatively low cost-benefit ratio (Brunst 2010), making it a desirable tool. Figure 1 shows the complexity of terrorist groups' use of the Internet (as both traditional communication and information gathering tool) in innovative new ways. The Internet is also used as both uni-directional and bi-directional communication tool.

Although this list of functionalities is not exhaustive, it provides a better understanding of the need for specific methods to exploit the ICT infrastructure to support terrorist activities. The next section discusses the methods in more detail, and explains these with actual examples.

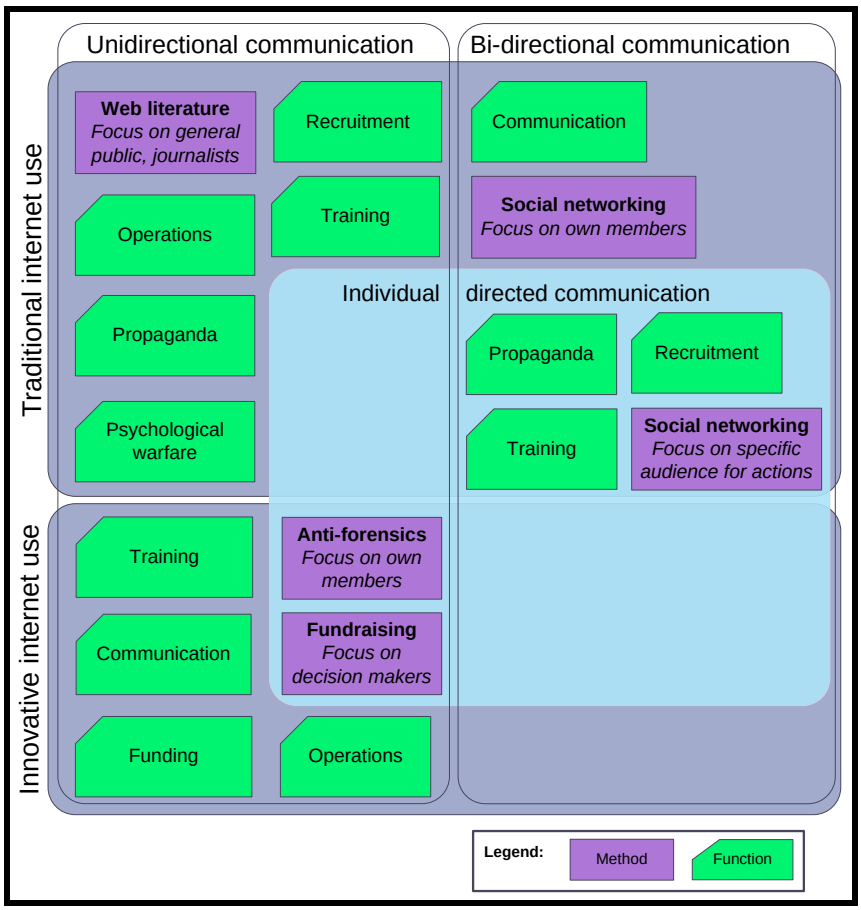

Figure 1: The Internet as terrorist supporting mechanism

3. Exploiting the ICT infrastructure to support terrorist activities

For the purpose of this article, Internet exploitation methods are divided into four distinct groups: web literature, social networking tools, anti-forensics and fundraising. Figure 2 shows these groups with some examples of how the methods may be employed.

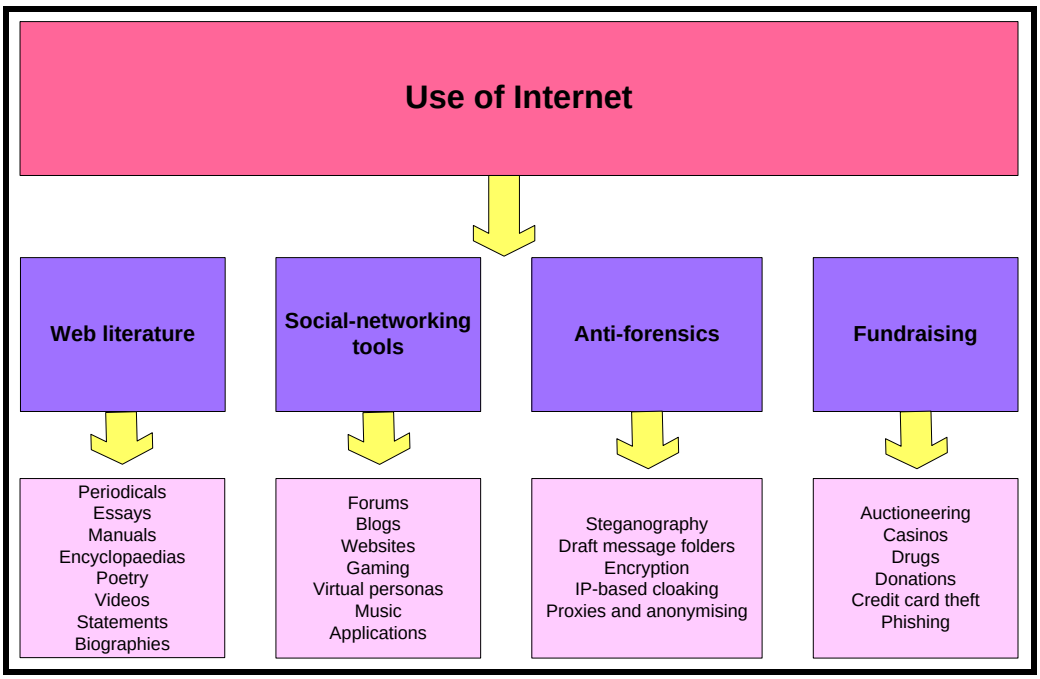

Figure 2: Examples of how terrorists may use the Internet

3.1 Web literature

Web literature refers to all writings published on the web in a particular style on a particular subject. Some of the types of web literature facilitated by terrorist groups include published periodicals and essays, manuals, encyclopaedias, poetry, videos, statements and biographies. Since web literature often takes on the form of mass uni-directional communication, this media is ideal for terrorist use in recruitment, operations, training and propaganda.

Radio Free Europe/Radio Liberty compiled a special report on the use of media by Sunni Insurgents in Iraq and their supporters worldwide. This report discusses the products produced by terrorist media campaigns, including text, audiovisual and websites (Kimmage, Ridolfo 2007). The distribution of text and audiovisual media is a traditional use of the Internet, with little innovative application. Text media include press releases, operational statements, inspirational texts and martyr biographies. Audiovisual media include recordings of al Qaeda operations in Iraq (Atwan 2006). Online training material can provide detailed instructions on how to make letter bombs; use poison and chemicals; detonate car bombs; shoot US soldiers; navigate by the stars (Coll, Glasser 2005) and assemble a suicide bomb vest (Lachow, Richardson 2007).

The use of *dedicated websites* within terrorist circles is prominent. By the end of 1999, most of the 30 organisations designated as Foreign Terrorist Organisations had a maintained web presence (Weimann 2009). In 2006, this number has grown to over 5000 active websites (Nordeste, Carment 2006). These websites generally provide current activity reports and vision and mission statements of the terrorist group. *Sympathetic websites* focus largely on propaganda. These websites have postings of entire downloadable books and pamphlet libraries aimed at indoctrinating jihadi sympathizers and reassuring already indoctrinated jihadists (Jamestown Foundation 2006). *Pro-surgent websites* focus on providing detailed tutorials to group members, e.g. showing how to add news crawls that provide the latest, fraudulent death toll for US forces in Iraq.

According to an al Qaeda training manual, it is possible to gather at least 80% of all information required about the enemy, by using public Internet sources openly and without resorting to illegal means (Weimann 2005). More than 1 million pages of historical government documents have been removed from public view since the 9/11 terror attacks. This record of concern program aims to *"reduce the risk of providing access to materials that might support terrorists"*. Among the removed documents is a database from the Federal Emergency Management Agency with information about all federal facilities, and 200 000 pages of naval facility plans and blueprints. The data is removed from

public domain, but individuals can still request to see parts of the withdrawn documents under the Freedom of Information Act (Bass, Ho 2007).

Other examples of web literature and information collected through the Internet include maps, satellite photos of potential attack sites, transportation routes, power and communication grids, infrastructure details, pipelines systems, dams and water supplies, information on natural resources and email distribution lists. Although this type of information may not necessarily be useful in cyberterrorism activities, it can be used to plan traditional terrorism activities without actually going to the geographical location of the target. Some terrorist groups have recently been distributing flight simulation software. Web literature can thus be used in the initial recruitment campaigns by glorifying terrorism through inspirational media, as well as the training of members, propaganda and the operations of the terrorist group.

3.2 Social networking tools

Social networking tools focus on building and reflecting social networks or social relations among people who share a common interest. Some types of social networking tools facilitated by terrorist groups include online forums and blogs, websites, games, virtual personas, music and specialised applications. Social networking tools offer both uni-directional and bi-directional communications, and can be used for recruitment, training, propaganda and communication within terrorist groups.

Social networking and gaming sites often require new members to create accounts by specifying their names, skills and interests. Through the creation of these virtual personas, terrorist groups are able to gather information on potential recruits. Individuals with strong technical skills in the fields of chemistry, engineering or weapons development can be identified and encouraged to join the group. This type of information can be derived from interactions in social networking sites, forums and blogs where users share information about their interests, beliefs, skills and careers. Online gaming sites also provide a source of potential members. For example, terrorist groups identify online players with a strong shooting ability that might be indicative of violent tendencies. In some terrorist groups, this type of temperament would be ideal for operational missions.

In addition to traditional social networking sites like Facebook and MySpace, Web 2.0 technologies evolved to customisable social networking sites. West and Latham (2010) state that social networking creation sites are an online extremist's dream - it is inexpensive, easy-to-use, highly customisable and conducive to online extremism. Ning users, for example, can create an individualised site where users have the ability to upload audio and video files, post and receive messages and blog entries, create events and receive RSS feeds. If a terrorist group sets up a customised social site, they would have the ability to control access to members, post propaganda videos and even use the site for fundraising.

Another way of promoting a cause is with music (Whelpton 2009). Islamic and white supremist groups perform captivating songs with pop and hip-hop beats that often attract young influential teenagers. The lyrics of the music promote the cause and the catchy beats keep the youth captivated.

Other examples of social networking include chat rooms, bulletin boards, discussion groups and micro blogging (such as Twitter). The type of social networking used by terrorist groups depends on the group's infrastructure, ability and personal preference. For example, al Qaeda operatives use the Internet in public places and communicate by using free web based email accounts. For these public types of communication, instructions are often delivered electronically through code, usually in difficult-to-decipher dialects for which Western intelligence and security services have few or no trained linguists (Nordeste, Carment 2006).

3.3 Anti-forensics

Anti-forensics is a set of tools or methods used to counter the use of forensic tools and methods. Some of the identified types of anti-forensic measures include steganography, dead dropping, encryption, IP-based cloaking, proxies and anonymising. Since anti-forensic measures mostly offer targeted uni-directional communication, it is ideal for training, operations and communication within terrorist groups.

Steganography is a method of covertly hiding messages within another. This is done by embedding the true message within a seemingly innocuous communication, such as text, image or audio. Only

individuals that know of the hidden message and have the relevant key will be able to extract the original message from the carrier message. The password or passphrase is delivered to the intended recipient by secure alternative means (Lau 2003). Although it is difficult to detect the modified carrier media visually, it is possible to use statistical analysis. The February 2007 edition of Technical Mujahid contains an article that encourages extremists to download a copy of the encryption program *"Secrets of the Mujahideen"* from the Internet (2007). The program hid data in the pixels of the image and compressed the file to defeat steganalysis attempts.

Another technique that would bypass messaging interception techniques is the use of virtual dead dropping, or draft message folders. Bruce Hoffman from Rand Corp. (in (Noguchi, Goo 2006)) states that terrorists create free web based email accounts and allow others to log into the accounts and read the drafts without the messages ever been sent. The email account name and password is transmitted in code in a chat forum or secure message board to the intended recipients. This technique is used especially for highly sensitive information (Nordeste, Carment 2006) and if electronic interception legislation may come into play.

Redirecting of traffic through IP-based cloaking is another anti-forensic technique. At a seminar in FOSE 2006, Cottrell (in ((Carr 2007))) stated that: *"When the Web server receives a page request, a script checks the IP address of the user against a list of known government IP addresses. If a match is found, the server delivers a Web page with fake information. If no match is found, the requesting user is sent to a Web page with real information"*. From this, the expression cloaking as the authentic site is masked. This also leads to a similar technique called IP-based blocking that prevents users' access to a site instead of redirecting the traffic.

Other techniques include the use of a proxy and secure channel to hide Internet activity. The Search for International Terrorist Entities Institute (SITE) detected a posting that encouraged the use of a proxy as it erases digital footsteps such as web addresses and other identifiable information (Noguchi, Goo 2006). The premise of this approach is that the user connects to a proxy that requests an anonymising site to redirect the user to the target site. The connection to the proxy is via a secure encrypted channel that hides the originating user's details. The well-known cyber user Irhabi 007 (Terrorist 007) also provided security tips by distributing anonymising software that masks an IP address (Labi 2006).

Another innovative use of the Internet is provided by spammimic.com. Spam (unsolicited distribution of mass email communication) has become a nuisance for the average netizen. Most people automatically delete these messages or send it to the spam folder. Spammimic.com provides an interesting analogue of encryption software that hides messages within the text of ordinary mail. It does not provide true encryption, but hides the text of a short message into what appears to be an average spam mail. Not only will the messages be disguised, but few people will take the chance to open the email in fear of attached malware. Thus, only the intended recipients will know about the disguised messages and decode it through the web interface (Tibbetts 2002).

3.4 Fundraising

Fundraising is the process of soliciting and gathering contributions by requesting donations, often in the form of money. Some of the identified types of fundraising methods include donations, auctioneering, casinos, credit card theft, drug trafficking and phishing. Since fundraising methods mostly offer targeted communication, it can be used for operations and funding activities.

Since the 9/11 terrorist attack, terrorist groups have increasingly relied on the Internet for finance related activities. Popular terrorist organisation websites often have links such as *"What You Can Do"* or *"How Can I Help".* Terrorist websites publish requests for funds by appealing to sympathetic users to make donations and contribute to the funding of activities. Visitors to such websites are monitored and researched. Repeat visitors or individuals spending extended periods on the websites are contacted (Piper 2008). These individuals are guided to secret chat rooms or instructed to download specific software that enables users to communicate on the Internet without being monitored (Nordeste, Carment 2006).

However, malicious or disguised methods of fundraising are also possible. Electronic money transfer, laundering and generating support through front organisations are all fundraising methods used by terrorists (Goodman, Kirk & Kirk 2007). According to the Financial Action Task Force, *"the misuse of*

nonprofit organizations for the financing of terrorism is coming to be recognized as a crucial weak point in the global struggle to stop such funding at its source" (Jacobson 2009). Examples of such undertakings include Mercy International, Rabita Trust, Global Relief Fund, and Help the Needy (Conway 2006). Some charities are founded with the express purpose of financing terror, while others are existing entities that are infiltrated by terrorist supporters from within (Jacobson 2009).

Other methods related to fundraising include online auctioneering to move money around. This involves two partners, known as smurfs, to arrange a fake transaction. One partner bids on an item and pays the auction amount to the auction house. The other partner receives payment for the fake auction item. There are also scams where users bid on their own items in an effort to store money and prevent detection (Whelpton 2009). In one specific auction, a set of second-hand video games were offered for $200, whilst the same set could be purchased brand new from the publisher for $39.99 (Tibbetts 2002). Although the ludicrously high selling price is not illegal, this item will only attract selected attention from a trusted agent. This allows terrorist groups to move money around without actually delivering the auctioned goods or services.

Online casinos can be used for both laundering and storing money. When dealing with large sums of money, terrorists can place it in an online gambling site. Small bids are made to ensure activity, while the rest of the money is safely stored and hidden (Whelpton 2009). Alternatively, any winnings can be cashed in and transferred electronically to bank accounts specifically created for this purpose (Jacobson 2009).

Stolen credit cards can help to fund many terrorist activities. For example, Irhabi 007 and his accomplice accumulated 37 000 stolen credit card numbers, making more than $3.5 million in charges (Jacobson 2009). In 2005, stolen credit card details were used to purchase domain space with a request stemming from Paris. When a similar request for nearby domain space was requested, shortly after the initial request, through another name in Britain, it was detected as fraud and the backup files of the initial site was investigated. Although the files were mostly Arabic, video footage includes insurgent forces clashing with American forces, depicting Iraqi conflict from the attacker's point of view (Labi 2006).

Drug trafficking is considered a large income source for terrorist groups. Fake Internet drugs are trafficked, containing harmful ingredients such as arsenic, boric acid, leaded road paint, polish, talcum powder, chalk and brick dust. In an elaborate scheme, Americans were tricked in believing they are buying Viagra, but instead they received fake drugs. The money paid for these drugs is used to fund Middle Eastern terrorism. The UK Medicine and Healthcare Regulatory Agency reports that up to 62% of the prescription medicine on sale on the Internet, without requiring a prescription, are fake (Whelpton 2009).

3.5 Other examples of the exploitation of the ICT infrastructure

Kovner (in (Lachow, Richardson 2007)) discusses one of al Qaeda's goals of using the Internet to create resistance blockades to prevent Western ideas from corrupting Islamic institutions. In some instances, Internet browsers designed to filter out content from undesirable Western sources were distributed without users being aware of it. Brachman also discusses jihadi computer programmers launching browsing software, similar to Internet Explorer that searches only particular sites and thus restricts the freedom to navigate to certain online destinations (2006).

Another technique from the infamous terrorist Irhabi 007 was to exploit vulnerabilities in FTP servers, reducing risk from exposure and saving money. Irabhi dumped files (with videos of Bin Laden and 9/11 hijackers) onto an FTP server at the Arkansan State Highway and Transport Department and then posted links warning users of the limited window of opportunity to download (Labi 2006).

SITE (in (Brachman 2006)) discovered a guide for jihadis to use the Internet safely and anonymously. This guide explains how governments identify users, penetrate their usage of software chat programs (including Microsoft Messenger and Paltalk), and advise readers not to use Saudi Arabian based email addresses (ending with .sa) due to its insecure nature. Readers are advised to rather register from anonymous accounts from commercial providers like Hotmail or Yahoo!.

Cottrell in 2006 (in (Dizard 2006)) discusses the following emerging cloaking trends:

- Terrorist organisations host bogus websites that mask their covert information or provide misleading information to users they identify as federal employees or agents;
- Criminal and terrorist organisations are increasingly blocking all traffic from North America or from IP addresses that point back to users who rely on the English language;
- Another cloaking practice is the provision of fake passwords at covert meetings. When one of the fake passwords are detected, the user is flagged as a potential federal intelligence agent who has attended the meetings, which in turn makes them vulnerable to being kidnapped or becoming the unwitting carriers of false information; and
- Another method was used in a case in which hackers set a number of criteria that they all shared using the Linux operating system and the Netscape browser, among other factors. When federal investigators using computers running Windows and using Internet Explorer visited the hackers' shared site, the hackers' system immediately mounted a distributed denial-of-service attack against the federal system.

Sometimes communication between terrorists occurs through a special code developed by the group itself. By using inconspicuous word and phrases, it is possible to deliver these messages in a public forum without attracting untoward attention. For example, Mohammed Atta's final message to the other eighteen terrorists who carried out the attacks of 9/11 is reported to have 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."* The reference to the various faculties is code for the buildings targeted in the attacks (Weimann 2005).

Defacing websites are a popular way for terrorist groups to demonstrate its technical capability and create fear. These defacements often take the form of public alterations of a website that are visible to a large audience. An example of such an attack took place in 2001, when a group known as the Pentaguard defaced a multitude of government and military websites in the UK, Australia, and the United States. *"This attack was later evaluated as one of the largest, most systematic defacements of worldwide government servers on the Web"*. Another example is pro-Palestinian hackers using a coordinated attack to break into 80 Israel-related sites and deface them, and when al Qaeda deposited images of the murdered Paul Marshall Johnson, Jr. on the hacked website of the Silicon Valley Landsurveying, Inc (Brunst 2010).

5. Conclusion

The use of the Internet by terrorist groups has expanded to both traditional Internet usage and the more innovative usage of both traditional and new Internet functions. Global terrorist groups can now electronically target an enormous amount of potential recipients, recruitees and enemies. Terrorist groups often embrace the opportunities that technology innovation brings about in order to advance their own terrorist workings.

This paper is informative in nature, aiming to make the public aware of the potential that ICT infrastructure has in assisting terrorist groups in their operations and normal functions. These functions include all the processes from recruitment and training of new members, communicating with existing members, planning and executing operations, distributing propaganda, fund raising and carrying out psychological warfare. Due to the unique nature of the Internet, many of these traditional and innovative Internet uses can be carried out in either a uni-directional or bi-directional fashion, depending on the nature of the communication required.

Based on this research, in can be seen that international terrorist groups can use the Internet in most of its daily functions to facilitate the growth and operation of the groups. In a sense, terrorist groups can actively exploit the existing ICT infrastructure to advance their groups. This paper discussed specific instances and provided examples of this exploitation through web literature use, social-networking tools, anti-forensic techniques and novel fundraising methods. In conclusion, further research may be done to identify ways on how these innovative uses of the Internet can be used to counter terrorism attacks, and not only support their activities.

References

Atwan, A. (2006), *The secret history of al Qaeda,* 1st edn, University of California Press, California.

Bass, R. & Ho, S.M. 2007, *AP: 1M archived pages removed post-9/11*.

Brachman, J.M. (2006), "High-tech terror: Al-Qaeda's use of new technology", *Fletcher Forum of World Affairs,* vol. 30, pp. 149.

Brunst, P.W. (2010), "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet" in , ed. P.W. Brunst, Springer, A war on terror?, pp. 51-78.

Carr, J. (2007), *Anti-Forensic Methods Used by Jihadist Web Sites*.

Coll, S. & Glasser, S.B. (2005), "Terrorists turn to the Web as base of operations", *The Washington Post,* vol. 7, pp. 77–87.

Conway, M. (2006), "Terrorist Use' of the Internet and Fighting Back", *Information and Security,* vol. 19, pp. 9.

Dizard, W.P. (2006), *Internet "cloaking" emerges as new Web security threat*, Government Computer News.

Goodman, S.E., Kirk, J.C. & Kirk, M.H. (2007), "Cyberspace as a medium for terrorists", *Technological Forecasting and Social Change,* vol. 74, no. 2, pp. 193-210.

Internet World Stats 2010, May 27, 2010-last update*, Internet usage statistics - The internet big picture: World internet users and population stats*. Available: http://www.internetworldstats.com/stats.htm [2010, 06/08] .

Jacobson, M. (2009), "Terrorist financing on the internet", *CTC Sentinel,* vol. 2, no. 6, pp. 17-20.

Jamestown Foundation, (2006), *Next Stage in Counter-Terrorism: Jihadi Radicalization on the We*b.

Kimmage, D. & Ridolfo, K. (2007), "Iraqi Insurgent Media. The War of Images and Ideas. How Sunni Insurgents in Iraq and Their Supporters Worldwide are Using the Media", *Washington, Radio Free Europe/Radio Liberty*.

Labi, N. (2006), "Jihad 2.0", *The Atlantic Monthly,* vol. 102.

Lachow, I. & Richardson, C. (2007), "Terrorist use of the Internet: The real story", *Joint Force Quarterly,* vol. 45, pp. 100.

Lau, S. (2003), " An analysis of terrorist groups' potential use of electronic steganography ", *Bethesda, Md.: SANS Institute, February,* , pp. 1-13.

Noguchi, Y. & Goo, S. (2006), *Terrorists' Web Chatter Shows Concern About Internet Privac*y, Wash.

Nordeste, B. & Carment, D. (2006), " Trends in terrorism series: A framework for understanding terrorist use of the internet ", *ITAC,* vol. 2006-2, pp. 1-21.

Piper, P. (2008), *Nets of terror: Terrorist activity on the interne*t. Searcher, vol.16, issue 10.

Tibbetts, P.S. (2002), "Terrorist Use of the Internet and Related Information Technologies", *Army Command And General Staff Coll Fort Leavenworth Ks School Of Advanced Military Studies,* pp. 1-67.

Weimann, G. (2009), "Virtual Terrorism: How Modern Terrorists Use the Internet", Annual Meeting of the International Communciation Association, Dresden International Congress Centre, Dresden.

Weimann, G. (2005), "How modern terrorism uses the internet", *The Journal of International Security Affairs,* vol. Spring 2005, no. 8.

West, D. & Latham, C.(2010), "The extremist Edition of Social Networking: The Inevitable Marriage of Cyber Jihad and Web 2.0", *Proceedings of the 5th International Conference on Information Warfare and Securit*y, ed. L. Armistead, Academic Conferences, .

Whelpton, J. (2009), "Psychology of Cyber Terrorism" in *Cyberterrorism 2009 Semina*r Ekwinox, South Africa.