Motivation for Cyberterrorism

Namosha Veerasamy
Defence, Peace, Safety and Security
CSIR
Pretoria, South Africa
nveerasamy@csir.co.za

***Abstract*—Cyberterrorism represents the convergence of the virtual world of cyberspace and the intimidation techniques of terrorism. To better understand why cyber terrorist acts are committed, this paper investigates the motivation behind terrorism by looking at traditional terrorist groups and how their objectives can be met by Information and Communication Technology (ICT). This paper addresses the reasoning behind cyberterror by discussing a few incidents and elaborating on known terrorist groups before providing a classification of terrorist types and an explanation of some support terrorist functions with regard to ICT infrastructure. In this way, insight can be gained into the objectives that are trying to be achieved by terrorist organizations, as well as shedding light into real-life groups and their operations.**

Keywords—terrorism, cybertertorism, Information and Communication Technology (ICT)

I. INTRODUCTION

The potential of terrorism spreading into the virtual world of cyberspace and computers is an area of concern to many. Information and Communication Technology (ICT) is often used as useful tool for communication, recruitment and planning terrorist missions, but malicious targeting of this critical infrastructure could cause widespread damage.

Already in 1998, Pollitt explained that cyberterrorism is the premeditated, politically motivated attack against information, computer systems and data which results in violence against non-combatant targets by sub national groups and clandestine agents [1]. This definitions shows, that terrorist groups may target innocent members of the community to protest a certain issue or promote a cause.

Furthermore, one of the most cited definitions of cyberterrorism as presented by Denning before the Special Oversight Panel on Terrorism [2], refers to cyberterrorism as unlawful attacks and threats of attack against computers, networks and the information stored therein, to intimidate or coerce a government or its people in furtherance of political and social objectives. As an aspect of terrorism, cyberterrorism addresses the methods and motivations driving the exploitation of Information Communication Technology (ICT). In summary, cyberterrorism refers to the:

- Promotion of political/social motives
- Infliction of harm with the aim of creating fear and shock
- Targeting critical ICT infrastructure and resources as the impact is more severe

Cyberterrorism can be examined from two perspectives: the technological attack and the psychological motivation driving the threat. In this paper, the latter is examined by discussing various motivating forces that drive terrorism. In this way, insight can be gained into the objectives that are to be achieved, as well as shedding light into real-life groups and their operations.

This paper investigates the motivation behind cyberterrorism by firstly discussing a few incidents and elaborating on known terrorist groups, before providing a classification of terrorist types and an explanation of some support terrorist functions.

II. INCIDENTS

A few incidents will initially be discussed to show how attacks have been executed in the past. Often, perpetrators are trying to cripple critical targets. Attacks are based on political, social or religious objectives and through these attacks, they are able to gain publicity for their organization or demonstrate their cause. Examples from Denning [3], the Thinkquest organisation [4] and Nagpal [5] are discussed next:

A. White Supremacist

In 1996, a computer hacker associated with a White Supremacist group, brought down a Massachusetts Internet Service Provider (ISP) and damaged part of the ISP's record keeping system. The ISP tried to stop the hacker from sending out racist messages under the ISP's name. In retaliation, the hacker published a message that stated "You have yet seen true electronic terrorism", but the hacker did not surface again. This attack used web page defacement, data corruption and a Denial of Service (DoS) attack to promote the racist intentions.

B. Spanish Protests

In 1998, the citizens of Spain flooded the Institute for Global Communications (IGC) with thousands of email messages. The email bombardment blocked the delivery of mail to San Francisco based ISP users, and people could not get access to their mail. The protest stemmed from the dissatisfaction that IGC hosted websites for the Euskal Herria Journal, which was a New York-based publication supporting Basque independence.

Acknowledgement must be given to the Council for Scientific and Industrial Research (CSIR) for their financial support.

The protestors felt that the IGC supported terrorism because the website contained material on the terrorist group Fatherland and Liberation or ETA, who were believed to be responsible for the assassinations of Spanish political and security officials, as well as military installation attacks. Pressure mounted through the distribution of spam to top IGC staff and member accounts, flooding their web pages with fake credit card orders and threatening to target organizations using IGC services. Due to the dissatisfaction and outrage expressed, IGC were forced to close the site due to the onslaught of mail bombings.

C. Tamil guerrillas

In 1998, ethnic Tamil guerrillas bombarded Sri Lankan email accounts with 800 mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we are doing this to disrupt your communications". Terrorist activity on the web is difficult to control. For example, the Sri Lankan government banned the separatist Liberation Tigers of Tamil Eelam, but could not take down their London-based website.

D. Anti-abortion

Another incident involved an anti-abortionist group, who put up a website terrorizing doctors performing abortions. The names of doctors performing abortions was published and the public was invited to contribute to the material by submitting doctors' home addresses, license plate numbers and even names of their children. As a result, doctors were attacked and some even killed. The murdered doctors had their names scratched out on the website.

This resulted in doctors having to live with constant fear and even resort to disguises, bodyguards and bullet-proof vests. The case went to court with the judge eventually ruling that site was equivalent to death sentences for doctors and thus ordered the removal of the site as well as $100 million in damages to the affected parties

III. KNOWN TERRORIST GROUPS

Now that a few examples of cyberterror have been provided, the discussion turns to known terrorist groups and their practices. The different terrorist groups were chosen to demonstrate the range of different motivating forces behind terrorism, as well as to indicate how different groups operate and behave.

A. Al Qaeeda

The international terrorist group Al Qaeeda regularly draws attention in the media. Their main goal has been to re-establish the Muslim state throughout the Persian Gulf. Al Qaeeda has widely adapted ICT infrastructure and uses electronic forums like bulletin boards and emails to communicate and prevent detection by counter terrorism agencies. In addition, a report in 2004 already shows that Al Qaeeda committed e-frauds and organized assaults on French financial institutions [6].

B. Aum Shinrikyo

The Aum Shinrikyo cult that operated mainly out of Japan has carried out various biological terrorist activities. They are most famously remembered for the 1995 saris gas attack on the Tokyo subway [7]. The extent of their cyberterrorism activities was discovered by Japanese police department in 2000, when it was uncovered that one of the computerized vehicle tracking programs was created by Aum Shinrikyo. Prior to the discovery, Aum Shinrikyo had been using the program to compile classified data with regard to the locations of marked and unmarked police vehicles [8].

The Japanese police also discovered that Aum Shinrikyo were sub contractors for computer programming firms and had developed software for at least 80 Japanese businesses and 10 government agencies. As they carried out the software development, the identification of their Aum Shinrikyo links was difficult to detect.

C. Hizbullah

Hizbullah has a presence in the United States and Lebanon. Hizbullah aims to establish an Islamic theocracy in Lebanon and to eradicate non-Islamic influences in the Middle East [8]. They have claimed responsibility for bombings of the United States Embassy and marine barracks in 1983 and the United States Embassy Annex in Beirut in 1984.

Already in February 1998, Hizbullah were operating three websites: one for the central press office (www.hizbullah.org), another to describe its attack on Israeli targets (www.moqawama.org) and the third for news and information (www.almana.com.lb) [3]. Hizbullah is known to deface websites, but the extent of their more sophisticated cyber attack capability is unknown.

D. Hamas

Hamas mainly operates in Israel and Jordon and their stance is against the Israeli state and in favor of creating an Islamic Palestinian state. In the past, they have used large-scale suicide bombers. Like other terrorist groups, Hamas uses the Internet for emailing plans and promulgation of philosophy and recruitment. Hamas has also reportedly used encrypted communications to transmit maps, pictures and other details relating to terrorist attacks [3].

E. Hammerskin Nation

Hammerskin Nation is a group of white power extremists with members in the United States, Canada, Australia, Germany and England. Their computer sophistication is indicated by the use of the Internet to transmit information to members, recruit members and supply links to white power music vendors [8].

F. StormFront

StormFront is a white power extremist group that has supporters in South Africa. They began as an online bulletin board system in the early 1990s and had a website established in 1995 by a former Ku Klux Clan leader and white nationalist activist Don Black. The group received attention in the United States in a CBS/HBO documentary special called Hate.com that dealt with the white supremacist organizations on the internet. They were controversially involved in targeting an online Fox News poll on racial segregation.

One of its members was a candidate for political office from a major political party. Computer sophistication is also shown by StormFront through use of the internet. Their website has numerous boards covering topics like ideology, science, home schooling and self-defense. It also hosts news stories, content aimed at children and links to various racist organizations. StormFront has an internet virtual community for white extremist families and white extremist singles.

G. Boeremag

The Boeremag is believed to use the internet to generate support in South Africa. The group communicates via newsgroups, email and Small Message Service (SMS). Supporters use Global Positioning Systems (GPS) to plan and execute activities. GPS co-ordinates and recently visited locations become evidence in trials [8].

H. G-Force Pakistan

In 2001 and 2002, this hacking group was considered the most active hacking organization on the internet. Their objective is to liberate Kashmir. As part of hacking activities, members have defaced websites and left profane and insulting messages [9]. The target was the Indian community.

IV. Types of Terrorism

After having introduced various examples and types of groups, the types of terrorists can be classified. To explain traditional terrorism, some psychological theory will be given. This helps to explain the motivation of a terrorist in response to emotional, political and social factors. Armistead [10], Nelson et al. [11] and Weimann [12] discuss the following types of terrorism and counter-terrorism :

- Religious: have strong theological beliefs.
- Ethno-national separatist: establish new political order, based on ethnic dominance.
- Revolutionary (Terrorism to the left): aim to seize political power.
- Far-right extremist (Right wing): believe certain people are inferior.
- New Age: usually focus on one issue (for example animals).
- Hackers: technically competent group with various motivations including activism, financial or challenge-seeking.

Another type of terrorism, discussed by Whelpton [13], is Retributional. The next few sections discuss each of the types of terrorism in more detail.

A. Religious

Laqueur [14] states that many terrorist groups traditionally contain strong quasi-religious fanatical elements, for only total certainty of belief (or total moral relativism) provides justification for taking lives. Al Qaeeda is a typical example.

Theological beliefs often justify the use of violence and can include the sacrifice of one's own life. According to Nelson [11], in contrast to revolutionary terrorism, religious violence may be unfocused and target the wider masses through advanced structured attacks that offer rewards and comply with ideology and goals of religious terrorism.

B. Ethno-nationalist

Ethno-nationalist groups are fighting to establish a new political order based on ethnic dominance/homogeneity [15]. Examples of groups seeking political autonomy include Provisional Irish Publican Army (PIRA), various Sikh movements in India, Palestinian Liberation Army, Kurdish Workers Party (PKK) in Turkey, Basque ETA in Spain and the Liberation Tamil Tigers of Eelam (LTTE) in Sri Lanka. Ethno-nationalists want to achieve publicity and international recognition for their cause and have been shown to demonstrate violent tendencies. In contrast to religious extremists, ethno-nationalists tend to have specific targets and would typically include symbols of the state like public officials, public facilities or utilities, and members of other ethnic groups.

If the terrorist is in close proximity of the target (with a local operating base), conventional physical attacks are more likely as they are simpler to execute. If the target has a different geographical location, cyberterror attacks could be advantageous, as networked resources can be used to achieve the objectives.

Ethno-national separatists rely on the support of local members, as well as the sympathy of the international community. Thus, it is imperative that any violent action is portrayed as purposeful and deliberate. Cyberterror attacks that cause a disruption in service can be beneficial in promoting a cause. This also eliminates casualties and injuries that occur as a result of violent or biological protests.

Accordingly, cyberterror attacks that interrupt services are an attractive option as damages are limited and such activity can generate support and interest in a cause. However, basic attacks can have the opposite effect than its original intention. For example, a planned DoS attack could show up as increased levels of spam or as an unusual amount of requests and go unreported. Like other terrorist groups, ethno-nationalists can use ICT to promote their cause through propaganda and gathering international support.

C. Social revolutionary (Terrorist of the Left)

Social revolutionists seek to overthrow the capitalist economic and social order [13, 15]. Targ [16] also states that revolutionary terrorism consists of a strategy to seize political power. Such a movement would form part of a radical social and political transformation characteristic of a terrorist group. Examples of left-wing terrorist groups include the Red Army Faction (who have kidnapped and assassinated people they blamed for economic and political repression) and the Italian Brigades (who have carried out computer attacks).

Social revolutionists do not wish to maintain current structure and rules. Part of the social revolt is a plan to build a

new and just society [13]. The usefulness of cyberterror attacks is dependant on the information infrastructure of the region (whether it is more rural or urban). Previously, ICT was mainly used by the government and state purposes. However, due to the advent of globalization and technological advancement, ICT is accessible to the wider population. ICT therefore provides a useful medium through which communications can be distributed to the public. Unfocused disturbances of this medium may therefore be counter-productive. Focused attacks on the government and corporations may be useful in protesting against commercial and capitalist regimes and demonstrating an opposed standpoint to state.

D. Far-right extremism (Right-wing)

According to the Israeli political scientist, Ehud Sprinzak, right-wing terrorism is characterized by the process of "split-deligitimation" in which not only the "outsider" (e.g. foreigners, ethnic and religious minorities) is targeted, but contemporaneously the state itself, as they are seen as ineffective or worse under the sway of the outsiders [17]. Far-right extremists can be racist organizations that are willing to use terrorism to repress other racial and ethnic groups who are perceived as the enemy [13]. Examples include Nazis and Italian neo-fascists. Cyberterror is an unattractive option as unfocused attacks could cause harm to the group's own members.

Group members could mainly use ICT infrastructure for propaganda, selling of survivalist gear and distribution of hate material. Far-right extremism is characterized by the strong belief in superiority that justifies the cleansing of the inferior that may include violence. Far-right extremists mainly use ICT for communication, as disruptive attacks interfere with operations and do not meet psychological goals.

E. New Age

Gearson [18] discusses the vulnerability of modern societies to unconventional attacks. New Age terrorism has developed from the shift towards violence, as a form of protestation when traditional method of campaigning do not yield results sufficiently fast enough. Examples are animal rights groups like the Animal Liberation Front (ALF) who have targeted research on animals by pharmaceutical companies. Attacks may include arson and sabotage.

Other examples are anti-abortion or environmental groups. New Age groups mainly have one targeted goal and not a broad range spectrum of issues like social-revolutionary activists. Cyberterror activities can be used to disrupt e-commerce and web-based advertising (dependant of ICT vulnerabilities). Unstructured attacks on low-level targets could also yield benefits.

F. Hacking

Hackers possess advanced technical skills and are thus able to attack systems. Hackers can operate in isolation or as part of a group (typically not a hierarchical structure). Hackers prefer to remain anonymous and build reputation in the underground hacking world where they gain notoriety for their successes (use pseudonyms). Targets can include web and mail servers, financial systems, banks, e-commerce and various other critical infrastructures.

Hackers are technical experts that can use infrastructure to make political statements and exploit vulnerabilities. Hackers demonstrate their own technological prowess and the target's technological weakness. Their activities can be linked to criminal acts. Criminal implications include:

- Financial: theft of funds, credit card numbers, pharming.
- Loss of availability: take down critical servers, crash websites.
- Loss of integrity: malicious data modification, corruption or loss of data.

Hacking skills to a large extent can be used to carry out terrorism stemming from the other types. Political, social or religious reasoning needs to be a core motivating factor. When Janczewski & Colarik [19] talk of the distinction between cyber terror and cyber crime, they say the answer does not lie in the mechanics of the event, but rather in the intent that drove the person's actions.

G. Retributional

The Retributional terrorist has a strong belief that a penalty needs to be inflicted in order to rectify a past wrongdoing. Thus, the act of revenge is justified. According to Whelpton [13], the mental status of such individuals might appear normal, without any sign of psychosis, but when discussing the incident, signs of anger and resentment may surface. Behavior could also be attributed to Post Traumatic Stress Disorder.

V. SUPPORT FUNCTIONS

The previous sections discussed various types of terrorist groups and indicate that cyberterrorism can have the same motives as traditional terrorist, but use computer and network mediums for attacks. In this way, cyberterrorism may span aspects of traditional terrorism and computer crime.

Cyberterrorism acts can form part of cybercrime with the use of security and hacking knowledge to electronically leave an impact through a threat, disturbance or infliction of violence [20]. This seeks to cause fear and influence the opinion of the government and public. ICT infrastructure can also provide many supportive functions. Jenkins [21] talks of functionally specialization tasks like recruiting, propaganda planning, logistics, finance. Whelpton [13] also discusses the hype that is created through media attention and the potential moral disengagement from society. These issues are elaborated on next.

A. Media attention

Terrorism is often referred to as theatrical in nature. Acts are comparable to the staging of a performance that seeks to have a wide-spread response. By using the media, attacks can be widely publicized. A spotlight is placed on the group and their message is more widely distributed. Brutal images from

suicide bombings and explosions bombard news reports. Accordingly, the virtual battle space has introduced various implications for Psychological Warfare.

B. Moral disengagement

Members may feel that their actions are justified as they need retribution. Since there is no governing body that controls the Internet, disgruntled individuals are able to voice their opinions and even establish hate/racist websites. False information can also be published. Terrorist websites are able to promote their causes by rationalizing and justifying their actions.

C. Planning

The internet can be used to collect background information in preparation for an attack, e.g. websites showing detailed instructions on making bombs, rocker flamethrowers, other lethal weapons and poisons. Examples include the "Anarchist Cookbook " from David Copland (recipes and instructions for various weapons) as well as works by Volker van der Graaf. Computers and networks can thus serve as useful tools to facilitate other terrorist attacks – for example the co-ordination of a kinetic attack by using email, web sites and discussion forums to provide instructions (location and guidance to construct explosive materials)) [22].

D. Recruitment

Due to the wide and diverse spectrum of the internet, terrorist groups have been able to reach a number of users identified as potential members. The skills and personality of ICT users may suit the terrorist organization (young, middle-class and technologically competent).

ICT can be used in the following ways:

- Direct communication with potential members
- Propaganda and promotion of cause
- Music - examples include white power music from supremacy and hip-hop Islamic music
- Honeypots - linked to other websites and message boards
- Gaming - encouragement of violent tendencies with shooting games.

E. Financing

Terrorist use various practices to generate funds to support their activities. These include [13]:

- Online auctioneering - two partners, also known as smurfs, arrange a fake transaction to move money. 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. Scams also involve bidding on own items to move money around.
- Online casinos - when dealing with large sums of money, a helpful technique is to place it in on an online gambling site. Thereafter, small bids are made to ensure activity and the rest of the money is safely stored and hidden.
- Wire transfers,
- scams, phishing
- Fake internet drugs - harmful ingredients are used. These include arsenic, boric acid, leaded road paint, floor and shoe polish, talcum powder, chalk and brick dust, and nickel. In one elaborate scheme, Americans believed they were buying Viagra but the drugs are fake and the money paid is actually 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.
- Stealing money and money laundering, keep to low amounts to prevent detection.

VI. FUTURE WORK

This work provides a high-level summary of the types of terrorist groups and motivating forces. Future work entails investigating the technical means that groups use ICT infrastructure to support terrorist activities. This involves examining topics like anti-forensics techniques, social networking tools and electronic propaganda. In addition, countermeasure strategies in the combat of cyberterrorism will also be studied.

VII. CONCLUSION

This paper addressed the motivation behind cyberterror by initially discussing a few incidents of cyberterror, as well as activities of known terrorism groups. The paper also presents a classification of various terrorist groups, as well as a description of ICT support functions of terrorism in general. Thus, insight can be gained into the psychological forces driving cyberterrorism today.

REFERENCES

1] M. M. Pollitt. "Cyberterrorism - fact or fancy ?", Computer Fraud & Security, vol 1998 (2), pp. 8-10, 1998.

[2] S. Gordon and R. Ford.," Cyberterrorism? Comput. Secur.", vol 21(7), pp. 636-647, 2002.

[3] D. Denning, "Cyberterrorism", Testimony before Special Oversight Panel on Cyberterrorism, Georgetown University, 2000.

[4] Thinkquest.org October 2004 web site contest. "Cyberterrorism", Accessed 20091126, Available online http://library.thinkquest.org/04oct/00460/cyberterrorism.html

[5] R. Nagpal, Defining cyber terrorism. WebmasterDigest, 2005 .

[6] D. Kramarenko, "Terrorism and high technologies,"Computer Crime Research Cenrre, Accessed 20040414, Available online at http://www.crime-research.org/news/04.14.2004/211.

[7] K. B. Olson, Aum shinrikyo: Once and future threat? Emerging Infectious Diseases, vol 5(4), pp. 513, 1999.

[8] B. Grobler, "What is cyber terrorism and what is at risk?" in Cyber Terrorism 2009 Seminar, South Africa: Ekwinox, 2009, .

[9] M. M. Elmusharaf, Cyber terrorism:The new kind of terrorism. Accessed 20081108, Available online http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism .

[10] L. Armistead, Information Operations: Warfare and the Hard Reality of Soft Power, Pontomac Books, Dulles VA United States, 2004 .
[11] B. Nelson, R. Choi, M. Iacobucci, M. Mitchell and F. Gagnon.. Cyberterror prospects and implications. Centre for the Study of Terrorism and Irregular Warfare. Monterey, CA, 1999.
[12] G. Weimann, Cyberterrorism: How real is the threat? United States Institute of Peace. Washington, United States, 2004.
[13] J. Whelpton, "Psychology of cyber terrorism," in Cyberterrorism 2009 Seminar,Ekwinox, South Africa, 2009 .
[14] W. Laqueur, "Postmodern terrorism", Foreign Affairs 75, pp. 24, 1996.
[15] J. M. Post, "The New Face of Terrorism: Socio-Cultural Foundations of Contemporary Terrorism," Behav. Sci. Law, vol. 23, pp. 451-465, 2005.
[16] H. R. Targ, Societal structure and revolutionary terrorism: A preliminary investigation. The Politics of Terrorism pp. 127-152, 1988.
[17] G. Michael, Confronting Right Wing Extremism and Terrorism in the USA, Routledge, New York and London, 2003 .
[18] J. Gearson, "The nature of modern terrorism. The Political Quarterly", vol. 73(1), pp. 7-24, 2002.
[19] L. Janczewski and A. M. Colarik., Cyber Warfare and Cyber Terrorism, Information Science Reference, 2007 .
[20] N. Veerasamy, "Towards a conceptual framework for cyberterrorism," in Proceedings of the 4th International Conference on Information Warfare and Security, Cape Town, South Africa, 2009, pp. 129-137.
[21] B. M. Jenkins. 2006, The new age of terrorism , Mcgraw-Hill, New York United States, pp. 118-119.
[22] N. Veerasamy, "A high-level conceptual framework of cyberterrorism," Journal of Information Warfare, vol. 8, pp. 42-54, 2009.