Towards a Conceptual Framework for Cyberterrorism

N Veerasamy

Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
nveerasamy@csir.co.za

Abstract: Terrorism has entered a new wave in that the latest battleground to emerge is cyberspace. Cyberterrorism reflects a current concern in the way terrorists will seek to strike the innocent and wreak havoc. Since explosives are no longer the only means to bring a system down, many are uneasy about random cyber attacks that could leave us with difficult conditions due to the disruption of critical services. As a result of our increased dependency on networked communications, the outcomes of such interruptions could be quite disastrous. Cyberterrorism is an aspect of cybercrime that has thus become a growing interest in this the Digital Age. Various hacking and computer intrusion scenarios could possibly play a critical role in cyberterrorism. In the global battle of information and network warfare, cyberterrorism has become a more dominant force. However, much misconception exists over what exactly cyberterrorism entails. Media has sensationalised the possibility of cyberterrorism attacks causing great havoc. Images of eccentric activists taking down critical infrastructures like power stations or railway lines bombard us. Many live in fear of the possibility of vital resources being taken down.

The role of security violations and hacking techniques also need to be better investigated to better understand the reality of such threats. Various theories surround cyberterrorism. However, there is a need for a more structured approach to understanding the various components of cyberterrorism.

A conceptual framework outlining the core aspects of cyberterrorism is therefore proposed. This paper focuses on clarifying the field of cyberterrorism through a conceptual framework that addresses the techniques, objectives, target, types, effects, characteristics and capabilities required. The framework strives to provide a more descriptive synopsis of the field of cyberterrorism. It therefore aims to form a good baseline to contextually place the area of cyberterorism against the backdrop of other computer and network related crime.

Keywords: Cyberterrorism**,** cybercrime, warfare, hacking, framework

1. Introduction

Shock and panic often face society with the strike of terrorist activities. The randomness and scale of attacks, causes great disbelief and outrage. The anxiousness raised in anticipation of an attack, and the fear that is generated after the execution of an act of deliberate violence, weighs heavily in the hearts of all nations.

The events of September 11 2001 clearly showed the global impact that an organised terrorist attack could have on various sectors. It also raised an awareness of the possibility of future attacks and the various repercussions. Although the attack was mainly a physical onslaught, the notion that computers and networks were used to orchestrate such an attack is raised.

Terrorism used to be synonymous with kidnappings, hijackings and bombings. However, in this the digital age, the concept of cyberterrorism or the use of cyberspace to carry out terrorist activities has emerged. Cyberterrorism draws up images of eccentric extremists using computers to unleash a wave of disasters by shutting down emergency systems or causing malfunctions at nuclear plants.

Embar-Seddon talks of the difficulty of understanding terrorist attacks as well as the fear created from the senseless and randomness of becoming a target (2002). The use of technology to facilitate attacks increases people’s fear due to the conceptual and connected nature of the channel. This brings the possibility of the impact of an attack being far wider. Across borders and timelines, attacks could be planned and orchestrated through this abstract medium of global networks.

An issue that arises is whether computers, networks and cyberspace are instruments in cyberterrorism. Computers may be referred to as “weapons” as they act indirectly (Pollitt 1998). Just as guns cannot shoot themselves, and are considered weapons, should the same analogy not be applied to computers/networks? In the hands of an assailant, both guns and computers could cause irrevocable damage. Guns don't kill people; rather it is the people that use the guns. The consideration in cyberterrorism should be the intention of the actor, not their choice of weapon or method of conveyance (Desouza, Hensgen 2003). Therefore, the aim of the perpetrator plays a key role in determining the classification as cyberterrorism.

The outlook towards cyberterrorism generally falls into two groups. One camp asserts that cyberterrorism cannot hurt you while the other claims the threat is real and points to financial damage caused by well-publicised virus attacks delivered over the Internet (Desouza, Hensgen 2003). The argument that cyberterrorism is not really a huge threat stems from the notion that no has actually died from a cyber attack. Inconvenience, annoyance and monetary loss are the examples of negative outcomes. The Internet can be used a tool for spreading propaganda or gather information but not to cause considerable harm. Schneier says that the network is excellent for propaganda purposes (whatever that might entail) or to gather information, whereas die-hard terrorists are still generally "more concerned with causing harms than gathering information (Giacomello 2004). The other argument addresses the possibility that control of critical systems (air traffic, power plants, hospitals), could cause loss of life. The question that is raised once again is the extent of control that can be gained. This will largely lie in the environmental conditions, as well as the amount of built-in safety mechanisms. For example, keeping critical systems on separate networks could prevent attempted penetrations from the Internet. Redundancy measures and manual overriding of systems are all tactics used to operate in times of crisis.

How real is the threat of cyberterrorism? The lines of cybercrime, cyberwar, and hackervism are all blurred. A closer investigation is needed to describe the various contributing forces in the field of cyberterrorism. This paper addresses the core components in the cyberterrorism field and will look at the techniques, objectives, characteristics, targets, and capabilities. The framework strives to provide a descriptive synopsis and form a good baseline to place the area of cyberterorism in context against the backdrop of other computer and network related crime and terrorism in general.

The remainder of this paper is structured as follows: Section 2 provides a background to cyberterrorism. Thereafter, Section 3 introduces the framework which is then is further explored in Sections 4-6. Section 7 concludes the paper.

2. Background

This section provides a background to the field of cyberterrorism in relation to other terroristic activities as well as computer and network crime. The background serves to provide a context to cyber terrorism and thus, elaborate on the initial purpose of this paper. Other literature can be consulted for more detailed overviews (Weimann 2004)(Gordon, Ford 2002)(Green 2002)

Cyber terrorism brings together two concepts – ie: The use of cyberspace and bringing about a reign of terror. Cyberterrorism thus encapsulates the use of computer and network technologies to promote extremist or aggressive tendencies, usually politically or socially motivated which leave a forceful or even brutal impact.

The most cited definition of cyberterrorism is Denning's testimony before the Special Oversight Panel on Terrorism. It states (Gordon, Ford 2002):

"*Cyberterrorism is the convergence of terrorism and cyberspace. .. unlawful attacks and threats of attack against computers, networks, and the information… done to intimidate or coerce a government or its people in furtherance of political or social objectives..to qualify a cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear.*

Cyberterorism refers to two basic ideas: cyberspace and terrorism. Cyberspace is an abstract realm and depicts the virtual world in which computers and networks operate in. Cyberterrorism can be seen as the unlawful use of force or violence against information, computer systems and networks to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. Whilst this definition provides a good introduction to the topic, it does address ordinary activities of computer abuse and the supportive role that computers and networks can have in facilitating terrorism in general. Thus, a discussion of cybercrime follows in order to clarify the field and place it in perspective with regards to assumptions and associated ideas. In addition, the proposed framework will discuss support functions that technology provides as well categorisation of cyberterrorist methods and practices in order to better argue the scope of cyberterrorism.

The lines between cybercrime and cyberterrorism cross over. A contributing factor is the role of computers and networks to facilitate their terrorist objectives and using them as the target/weapon. One argument is that in order to be considered cyberterror, some form of fear and/or political or social objective needs to be attained. This would mean that only activities having computers and networks as their target would be deemed cyberterroristic in nature. Various computer and network related practices can be used to support terrorist activities but their exact use alone is not considered an act of cyberterrorism. For example, the unleashing of a virus to cause the malfunctioning of a power plant differs from an email virus that sends out spam mail to a user's address book members. A critical component of distinguishing between cyberterrorism and traditional activities of cybercrime is the motivation of the perpetrator and as well as a consideration of the nature of the activities. The goal of causing large-scale terror and ulterior political/social motive needs to be an inherent part of a cyberterrorist attack. Therefore, various computer and network related activities support cyberterrorism at an implementation level but the high-level objectives may differ from normal computer and crime (for example causing annoyance, economic loss, fraud, espionage, etc.) Actions taken in response to an attack are not considered criminal if they are carried out in a defensive (and not malicious) capacity only. For example, police officers sometimes have to take offensive action to bring down a violent criminal. So too the defence industry has to take retaliatory action in order to prevent further damage to systems.

Cyberterrorism can be viewed as acts of terrorism carried out through computer, networks and cyberspace. In a similar manner, cyber crime can be considered criminal acts that are committed by using computer resources, tools and environments. Cyberterrorism acts form part of cybercrime- when the action crosses legal boundaries. Both cyberterrorists and cybercriminals will use knowledge of security and hacking to electronically leave an impact, but the underlying goal might differ. Whilst cyberterror tries to cause a political change and targets innocent victims through computer-based violence or destruction, cybercrimal activities aims have an economic gain from individuals and companies by carrying out fraud, id theft, blackmail, and other computer attacks and exploits (Lachow 2008). A cyberattack or crime needs to have an element of “”terrorism” (threats, disturbances or infliction of violence) in order to be considered cyberterrorism. Athough, cyberterrorism may seem as a more indirect approach to launching an attack, a critical consideration is the terror that is generated from a potential attack. The intent of the attack will be the typical terrorist objective to cause/threaten violence or promote a social/political viewpoint. For example, consumers are petrified at the idea of a critical system like the rail lines or power station going down. Fear is a critical aspect of terrorism and though it may not seem as cyberterrorist acts are as violent as their physical counterparts, the implication of consumed fear and terror should be undermined. Thus, the psychological edge that is to be gained by keeping a nation in constant doubt and anxiety is a huge payoff for terrorists.

Possible Cyberterrorist situations envisaged by Collin (1997) include :

- Altering the iron supplement level in a cereal manufacturing plant such that it poisons and kills all that consume the unsafe levels
- Modifying the formulas of medication at pharmaceutical companies. This could result in an enormous loss of life
- Gaining control of air traffic control systems and cause aircraft to crash into each other. The same could be applied to rail services
- Disrupting the services of financial institutions thus causing citizens to lose confidence in the economic systems

Pollitt points out the discrepancies that could prevent the first two scenarios from materialising (1998). He argues that since such minimal quantities of supplement level is added to cereal; the necessary quantity to poison a person would be incredibly substantial. Furthermore, such increased consumption would be noticeable, when the supplement supplies ran low unnecessarily. Also routine product testing would detect such an abnormal quantity of an active ingredient. A similar argument could also be applied to the second scenario of modifying the formulas of medication. Pollitt also disputes that the entire human element and structuring of air traffic control rules would be overlooked were a terrorist to gain control (1998). Pollitt explains that computers in air traffic control provide information and do not actually control the aircraft (1998). Pilots are trained to use their situational awareness and thus taught to be aware of position as well as approaching aircraft. Rules are also meant to ensure smooth operation should no air traffic control be available.

However, in April 2007, a series of cyber attacks was launched against the Estonian state. The targets included the Estonian parliament, banks, ministries, newspapers and broadcasters (Von Solms 2008). The execution of such an onslaught left a state without the availability of critical services including the presidency and parliament, government ministries, news resources, banks and communications. The incident is indicative of the probability of such attack and the inconvenienced conditions that was left in its wake. The case is often carefully studied to understand the circumstances that led to its materialisation and furthermore how the situation can be prevented.

Cyberterrorism can thus be seen as a relevant threat due its strong relation to computer and network crime. However, a closer inspection of the role that is plays will provide a better understanding of the pertinent forces and domains of operation. The application and significance will be better revealed through a more detailed study of the field. The rest of the paper will therefore look at placing the area of cyberterrorism in context. More specifically, the paper will aim to describe the influential considerations and the role that technology plays.

3. Framework

This section introduces the framework, which will be further explored in the rest of the paper. Later sections will provide for discussions of individual issues.

The framework is given in Figure 1. It consists of three main sections: operating forces, techniques and objectives.

Five operating forces are considered: characteristics, target/focus, types, capabilities and social factors. Each operating force in turn has a number of related sub-items. The operating forces provide the context in which cyberterrorism is functioning. Various high-level techniques are given. These high-level techniques are supported though various information gathering and invasive/offensive computer and network security practices. The objectives are similar to the motivation behind standard terrorist activities, though some distinction is given to show the more pronounced intentions.

The contribution of the framework lies in the organisation of the field of cyberterrorism and the provision of an overview to place the area into context. The operating forces describe the various advantages of utilising cyber terror, the intended systems to be attacked and the mindset of the terrorist. The techniques section addresses the classification of attack tactics. The objective section looks at the immediate aims of the attacker and also distinguishes between cyber terror activities and the supportive functionality that computers and networks can play (often confused as cyberterror). This discussion helps clarify important details concerning the functional mindset of a cyberterrorist as well as elucidating which aspects of cybercrime and hacking will be utilised. A discussion dealing with the various components in the framework follows.

4. Operating Forces

When discussing the field of cyberterrorism a number of operating forces need to be considered. A discussion of these forces will delve into the underlying features affecting cyberterrorism. The findings are drawn from related literature as well as practical insight from studying the area of interest. The operating forces depict qualities of a cyberterrorist as well as the properties of cyterrorism in general.

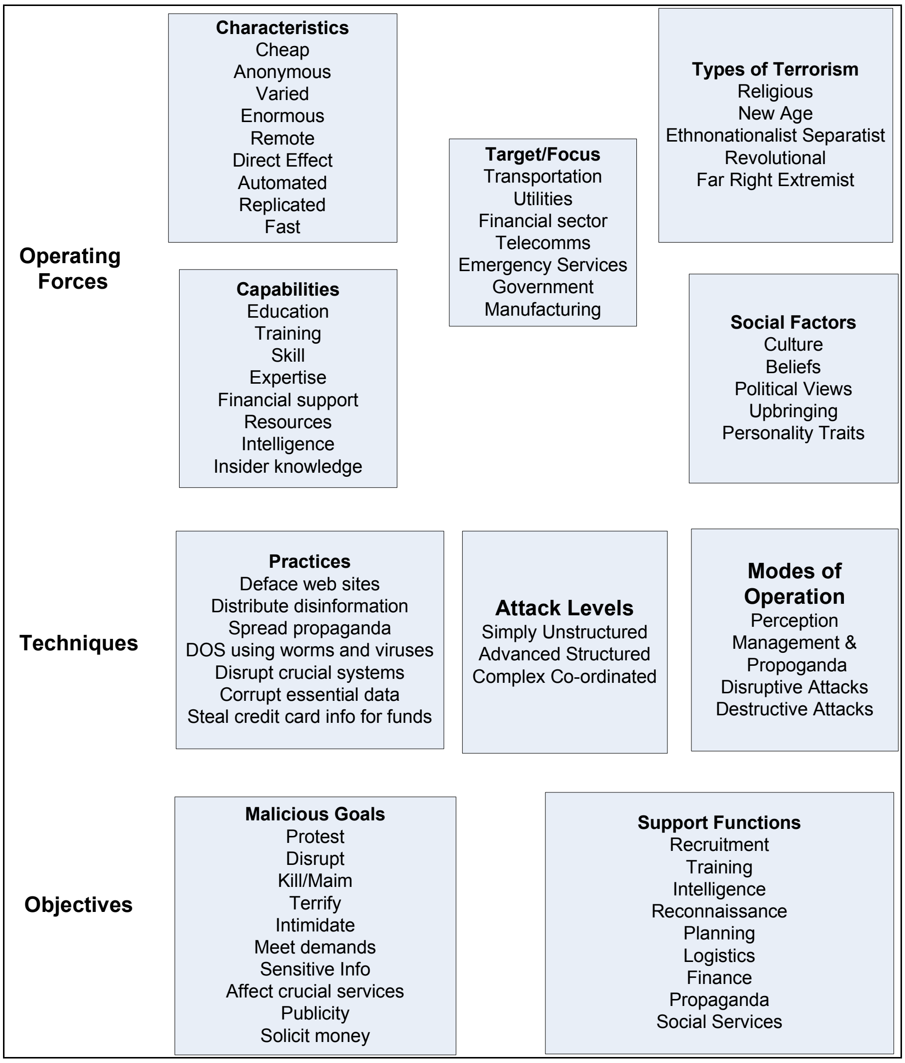

Figure 1: Framework of Cyberterrorism

4.1 Characteristics

Denning talks of cyberterrorism having the advantage of being able to be conducted remotely and anonymously, as well as being cheaper as it does not require the purchase of explosives or a suicide mission (2000). In comparison to buying explosives, a laptop and Internet connection is by far less expensive. Weimann also talks of cyberterrorists having the ability to immediately reach a bigger number of targets directly (2004). Other advantages afforded by cyberterrorism are the ease and speed at which attacks can be launched. With the use of digital technology, attacks can be automated and repeated quickly and thus less effort is often required.

4.2 Target/Focus

Cyber-terrorism is “the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population (Lewis 2002) ”. Water, like energy is an example of critical utilities that could be attacked. Desouza & Hengsen discuss the dependence of business on electronics and how cyberterroristss will seek to expose vulnerabilities in banking, brokering, e-commerce, transportation, fuel supply, power grid and governmental systems (2003) . Other targets include emergency services like the police, ambulance and fire department. “”The 911 emergency response system, a specialised communications network that relies on local telephone service, is also a favourite target for theorists of cyberterrorism (Lewis 2002)”

Furthermore Collin discusses potential cyberterrorism scenarios and proposes attacks in a cereal manufacturing plant, disruptions to banks, stock exchange, air traffic control, pharmaceutical manufacturers or gas liners (1997). In addition, Folt talks of cyberterrorism threats include interfering or disrupting information and communications networks, infrastructure systems, banking and finance systems, transportation systems, emergency services, and government services (2004). Six high level groups of potential targets thus emerge. Targets include transportation, utilities, financial sector, manufacturing, telecoms, emergency and government. Thus, by looking at the target section, it is evident that critical systems providing services to the general population will generally be focussed on. This will aim to leave the most influential impact if a larger section of the nation is affected.

4.3 Capabilities

This section addresses key underlying qualities, traits and qualifications in the mindset of a cyberterrorist. Upbringing and educational background will play a critical role. With experience, grows expertise and skill. Training will seek to develop the aptitude of the individual. Financial support is a vital requirement to support ongoing terrorist activities. Funds are needed to co-ordinate, plan and execute attacks. Resources like equipment and tools will be required to sustain operations. An advantageous position would be gained through the collection of insider information. In addition, intelligence to provide background and guidance will also be helpful. The capability section aims to show that several physiological issues play a role in the development of a cyber terrorist. In addition, other resources will also be required to facilitate the malicious activity.

4.4 Types of Terrorism

Whilst the motivation for terrorism ranges from religion principles to political agendas, various types of terrorists can be classified. However, the distinctions between the types often blur and thus the ideological views often cross over. Weimann draws attention to a report, “Cyberterror: Prospects and Implications,” published in August 1999 by the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California (2004). The report is said to have studied five groups of terrorists: religious, New Age, ethnonationalist separatist, revolutionary and far-right extremist. This finding is the basis of classification of the types of terrorists in the framework. Post discusses the etho- nationalsist terrorism groups that are fighting to establish a new political order based on ethnic dominance/homogeneity as well as the social-revolutionary terrorists (terrorism of the left) who seek to overthrow the capitalist economic and social order (2005). In addition, Gearson addresses the New Age of Terrorism which looks at the vulnerability of modern societies to unconventional attacks (2002). Furthermore, Laqueur 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 (1996). According to the Israeli political scientist, Ehud Sprinzak, right wing terrorism is characterised by the process of “split-deligitimation” in which not only the “outsider” (eg. 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 (Michael 2003). In addition, revolutionary terrorism consists of a strategy to seize political power (Targ 1988). This section is indicative of the various underlying motivating factors that influence terrorism. It is by far merely a brief introduction into some of the primary reasons driving terrorism today.

4.5 Social Factors

A core underlying factor impacting the acts of terrorists in general stems from various social issues. Jenkins states that terrorism is generally derived from out concepts of morality, law and the rules of war, whereas actual terrorists are shaped by culture, ideology and politics (2006). This introduces a few influential considerations, namely culture, belief system, political views, upbringing and personality traits. These intangible social issues will impact the line of action that a terrorist follows and thus lays the foundation for terrorist activity in general.

5. Techniques

This Section looks at various practical methods and classification descriptions of carrying out cyberterrorism. It commences with a description of technical practices, before looking at differing levels and modes of operation. The classification of techniques explains those aspects of cybercrime and hacking that will be utilised to carry out cybercrime. Thus, this section provides details of specific attack methods and absolves concerns that all computer and network crime is cyberterroristic in nature.

5.1 Practices

A discussion of high-level technical attack practices takes place in this section. Overall practices covered include:

- Web site defacement to distribute disinformation and spread propaganda using hacking and other vulnerability exploitation techniques
- Denial-of-service attacks on valid machines to cause loss of availability using worms, viruses and bots
- Gaining unauthorised access to crucial systems and networks to cause disruptions in vital services or to corrupt essential data through espionage, penetration and modification practices
- Try to raise funds for operations through credit card theft and other fraudulent financial activities

5.2 Attack Levels

From the discussion on practices, it is evident that a variation occurs depending on the complexity and motivation of the attack. Thus, the various attack techniques can be classified according to the level of organisation. According to a report “Cyberterror: Prospects and Implications” compiled by the Naval Postgraduate School there are three levels of cyber acts (Desouza, Hensgen 2003). They are:

1) “Simply Unstructured”: basic attacks against individual systems with easily available tools. Many terrorist organizations (eg. Hozbollah) have their own web sites in which they vision and activities are promoted. Attacks in this category include the deployment of worms and viruses
2) “Advanced Structured: more elaborate attacks against numerous systems. This attack requires the hacker to adapt tools/applications
3) “Complex co-ordinated”: capacity to cause serious interruptions to many targets at the same time or in succession. This type of attack includes striking from various sources. An attack of this nature requires sophisticated planning and orchestration (usually many years and large groups)

5.3. Modes of Operation

Another framework that can be used to categorise attacks is their broad-spectrum modes of operation which will be closely linked to high-level cyberterrorist objectives. Arquilla and Rondfeldt discuss the development of terrorist organization and their changing modes of operation (2001). More effort will be placed in forming organized networked parties rather than cultivating isolated groups. It has been realized that the effectiveness of networked based approached far exceed the restricted hierarchical arrangements. The authors further propose that the information-age technology can assist terrorists in three broad offensive categories (Arquilla, Ronfeldt 2001). They are:

- Perception Management and Propoganda: Getting a message across to potential supporters in extremely important and thus technology serves as the ideal communication medium to attract more followers/members, generate funding and influencing people’s views. Recruiters comb though chat rooms and bulletin boards to find ideally suited candidates to further group activities. Web sites provide a forum for marketing and exposing groups’ activities. For example, the militant group Hizbollah, together with its web site has its own broadcasting television station,. Reports include dramatic footage of physical attacks. Most terrorist groups have a web presence in the form of a web site (Al-Jama’ah Al-Islamiyyah, Hamas, etc)
- Disruptive Attacks: This type of attacks seeks to temporarily immobilize a site/service/system. Examples include e-bombs, fax spamming and hacking to deface web sites. Interruption in service and the economic repercussions are the outcomes of this mode of attacking. For example: The Tamil Tigers carried out an email bomb attack against the Sri Lankian diplomatic mission in 1996. Automated tools were used to send thousands of messages to the Sri Lankian embassy. Blackmail and fund extortion are other examples.
- Destructive attacks: The use if IT-driven operations can actually lead to the ruin of physical or virtual systems/networks. Malware can destroy data or modify it such the information is corrupted. Systems could then possibly fail due to the loss of data/service/

6. Objectives

Objectives are broken down into cyberterrorism malicious goals and those relating to support functions that computer and networks provide in enabling terrorism. Thus the distinction is drawn between those intentions to cause direct damage/difficulties (cyberterorrism) versus practices that facilitate the grander scheme.

6.1 Malicious Goals

Weimann touches on various objectives of terrorists. Firstly, he mentions at a generalised level they seek to protest, disrupt, kill/maim and terrify people (Weimann 2004). “Historical experience has taught terrorists that to spread terror and thus expand their political capital the most effective way is to break things and kill people (BTKP) (Giacomello 2004)”. Desouza and Hensgen discuss the intention of terrorists as trying to intimidate a population/government into meeting their demands (2003). Release of political prisoners, money and changing of laws are examples of demands from terrorists. More specific to cyberterrorism, Weimann discusses the goal of gaining access to sensitive information and to the operation of critical services (2004). This will serve to cripple or disable these critical services. Those concerned with terrorism and the media frequently find the staging of incidents, the publicity sought and the manipulation of the audience primary themes in their analyses (Gordon, Ford 2002). This highlights another two objectives- the need to stage incidents to draw attention and thus gain publicity from the incident. Groups many also need to raise funds for operations and therefore seek to solicit money to gain support. This discussion addresses the short-term goals of attackers. The classification of types of terrorism (in Section 4.4) briefly looks at more long-term objectives and underlying plans of cyberterrorists.

6.2 Support Functions

Whilst, terrorist goals mainly serve to threaten or cause violence, the role of cyberspace and networked technology can provide various support functions that may not be directly linked to mass damage, but rather lay the foundation of terrorist activities as well as provide the maintenance of operations. Thus, by looking at the various techniques, networks and electronic devices may not always be used in a direct attack, but can still provide assistance in terms of communication, guidance, information gathering, preparation and financial backing. Jenkins talks of functionally specialisation tasks like recruiting, training, intelligence, reconnaissance, planning, logistics, finance, propaganda, and social services (support for families of suicide attackers) (2006). Thus, it can be seen that the various technologies can play an enabling role in terrorism in general as well as directly achieve cyberterrorism attacks. Computers and networks can 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). In this case, the technological components provide a supportive role as computers, networks and controlled infrastructure does not form part of the target but instead were used as tools to facilitate the terrorist activity.

7. Conclusions

Cyberterrorism is the latest catchphrase in the domain of cyberattacks, cybercrime and network warfare. However, most fail to realise that many cyberattacks are usually ordinary recreational hackers testing out their skills or trying to commit some fraudulent activity. However, hacking skills and security violations are used as part of cyberterror attacks. Whilst the targets and motivation of ordinary hackers thus differs from military and terrorism threats, the technical mode of operation of a cyberterrorist relies heavily on security knowledge and skills. Cyberterrorism has become a realistic threat in that those seeking to damage/disrupt computer systems, programs, infrastructure and data, could leave a meaningful impact on the civilian sector.

Cyberterrorism thus raises a new wave of concern in the form of political or social activists interrupting or destroying critical system infrastructure. The goals of causing disruptions, protestations, intimidation and demands are being facilitated through the electronic medium of computers and networks. Moreover, various computer security violations (web defacement and data corruption/loss and service loss through the unleashing of worms and viruses) are being used to surge this new form of terror.

This paper considered the various features of cyberterrorism to present a structured account of the field. The framework serves a basis of the underlying influential considerations in the domain of cyberterrorism. Cyberterrorism has been compared to cybercrime and cyber attack. However, the discussion explained the use of these various security violation techniques to aid the higher level objectives of propaganda, disturbance or destruction. As technological developments progress and new vulnerabilities and weaknesses are developed, terrorists might find novel ways of interfering with critical data and systems.

Computer security thus plays a huge role in the way that systems and networks can be exploited as well as the way better protection can be provided.

The framework should provide a good overview of the area of cyberterrorism and placing it in context against the backdrop of other current concerns like cybercrime and cyber attacks. The paper addresses the operating forces acting on cyberterrorism. These include aspects like the target/focus area, and the characteristics, types and capabilities of cyberterrorists. An analysis of attack types, levels and techniques was also carried to clarify the role of security hacking and violation practices. An outline of the objectives of cyberterrorists was also given to indicate their high-level motivation of carrying out these destructive and hurtful practices.

The framework allows for continued research into the area of cyberterrorism and thus allows for an extension of ideas. Various other influential considerations could be identified and more insight into the mindset of a cyberterrorist can be gained. However, it is firmly believed that the framework provides a good summary and can be utilised for further insight.

References

Arquilla, J. & Ronfeldt, D.F. 2001, *Networks and Netwars: The future of terror, crime, and militancy,* Rand Corporation.

Collin, B.,C (1997), "The Future of Cberterrorism: The Physical and Virtual Worlds Converge", *Crime and Justice International,* pp. 14-18.

Denning, D. (2000), *Cyberterrorism*, Georgetown University.

Desouza, K.C. & Hensgen, T. (2003), "Semiotic Emergent Framework to Address the Reality of Cyberterrorism", *Technological Forecasting and Social Change,* Vol. 70, No. 4, pp. 385-396.

Embar-Seddon, A. (2002), "Cyberterrorism: Are We Under Siege?", *American Behavioral Scientist,* Vol. 45, No. 6, pp. 1033.

Foltz, C.,Bryan. (2004), "Cyberterrorism, Computer Crime, and Reality", *Information Management & Computer Security,* Vol. 12, No. 2, pp. 154-166.

Gearson, J. (2002), "The Nature of Modern Terrorism", *The Political Quarterly,* Vol. 73, No. s1, pp. 7-24.

Giacomello, G. (2004), "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", *Studies in Conflict and Terrorism,* Vol. 27, No. 5, pp. 387-408.

Gordon, S. & Ford, R. (2002), "Cyberterrorism?", *Computers & Security,* Vol. 21, No. 7, pp. 636-647.

Green, J. (2002), *The Myth of Cyberterrorism*.

Jenkins, B.M. (2006), "The New Age of Terrorism", *The McGraw-Hill Homeland Security Handbook (New York: McGraw-Hill, 2006),* pp. 118–119.

Lachow, I. (2008), *Cyber security : A few observations*, National Defense University, Washington.

Laqueur, W. (1996), "Postmodern Terrorism", *Foreign Affairs,* Vol. 75, pp. 24.

Lewis, J.A. (2002), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", *Center for Strategic and International Studies,* pp. 1-12.

Michael, G. 2003, *Confronting Right Wing Extremism and Terrorism in the USA,* Routledge.

Pollitt, M.M. (1998), "Cyberterrorism - fact or fancy?", *Computer Fraud & Security,* Vol. 1998, No. 2, pp. 8-10.

Post, J.M. (2005), "The New Face of Terrorism: Socio-Cultural Foundations of Contemporary Terrorism", *Behavioral Sciences & the Law,* Vol. 23, No. 4, pp. 451-465.

Targ, H.R. (1988), "Societal Structure and Revolutionary Terrorism: A Preliminary Investigation", *The Politics of Terrorism,* pp. 127-152.

Von Solms, B. (2008), "Critical Information Infrastructure Protection- Essential During War Times, or Peace Times or both?", *IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace*, eds. J. Phahlamohlaka, N. Veerasamy, L. Leenen & M. Modise, Council for Scientific and Industrial Research , pp. 36.

Weimann, G. (2004), *Cyberterrorism: How real is the threat?*, United States Institute of Peace, Washington, United States.