Countermeasures to Consider in the Combat against Cyberterrorism

N Veerasamy and M Grobler
CSIR, Pretoria, South Africa
nveerasamy@csir.co.za
mgrobler1@csir.co.za

Abstract: Cyberterrorism addresses the convergence of the fear-causing world of terrorism with the abstract realm of cyberspace, computers and networks. While cyberterrorism can be executed using various technical security exploits, it inherently stems various social, political or religious views. This paper presents an overview of the motivating forces behind cyberterrorism which can provide the baseline to develop a countermeasure strategy. In this paper, countermeasures that can be used to deter cyberterrorism from both these psychological and technical perspectives are covered. It provides a high-level overview of the fight against terrorism and discusses countermeasures that can be used to combat cyber terrorism to create awareness.

Keywords: cyberterrorism, countermeasures, terrorism

1. Introduction

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 [16]. Cyberterrorism looks at the convergence of cyberspace and terrorism. It addresses the malicious use of Information, Communication and Technology (ICT) infrastructure with the aim of causing distress and disturbance. Linked to terrorism are the associated political, social and religious motivations.

This shows that in many cases innocent members of the community can be targeted to protest a certain issue. The definition from Pollitt also refers to premeditation, indicating that responses are planned and directed in order to inflict damage and cause terror.

One of the most cited definitions of cyberterrorism as presented by Denning before the Special Oversight Panel on Terrorism, 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 [8]. Terrorism in general is indicative of offensive techniques that are used to promote political, social and religious issues. Cyberterrorism therefore spans both technical and psychological issues. It differs from traditional cyber crime that mainly stems from financial or economic purposes.

This paper cover countermeasures that can be used to deter cyberterrorism. It provides a high-level overview of the fight against terrorism and discusses countermeasures that can be used to combat cyber terrorism to create awareness. In this section, a brief introduction to cyberterrorism was given. This paper will continue with a further discussion covering a concise overview of cyberterrorism. Thereafter, the authors will classify terrorism into types. This will be followed by a more detailed explanation of countermeasures from both a psychological and technical perspective.

2. Cyberterrorism background

The origin of cyberterrorism can be traced back to the early 1990s, when the rapid growth in and dependence on the internet became obvious. Already in 1990, the potential of cyberterrorism has been visualised: *"… Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."* Not only is cyberterrorism ranked amongst other weapons of mass destruction, but it is also likened to an electronic Pearl Harbour [21].

Figure 1 shows a conceptual framework that summarises the influential considerations in the field of cyberterrorism in [19, 20]. This framework provides an apt summary of significant issues that need to be considered when discussing cyberterrorism. High-level issues that are addressed in the framework include:

- Characteristics
- Target/focus

- Social factors
- Types of terrorism
- Capabilities
- Practices
- Attack levels
- Modes of operations
- Malicious goals
- Support functions

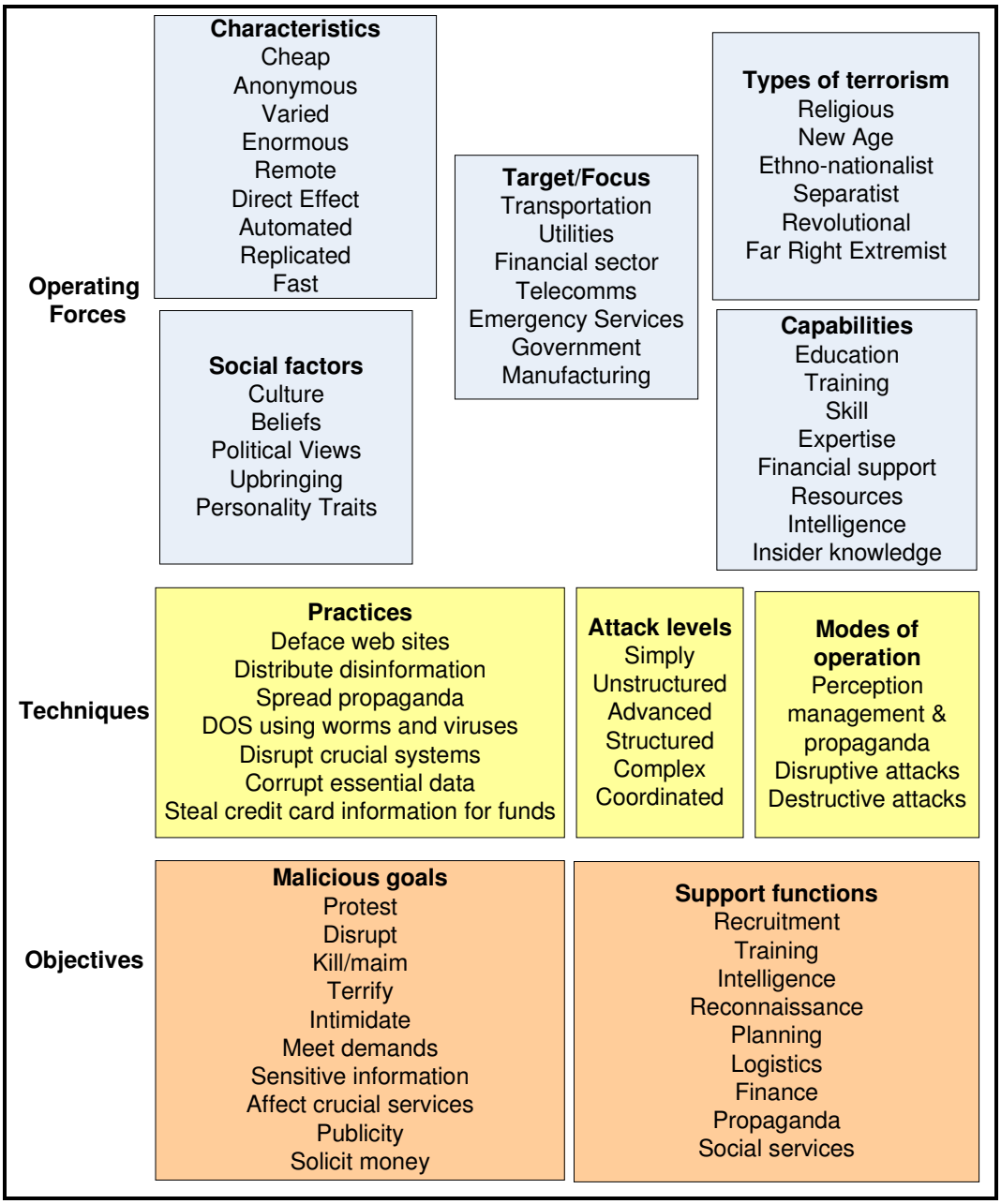

Figure 1: Framework for cyberterrorism

This framework discusses the technical and psychological considerations in the field of cyberterrorism. The ability to quickly send an attack directly, anonymously and remotely offers significant advantage over the financial and planning overhead of detonating a bomb. However, the types of attacks and practices stems from the motivating force driving the higher cause.

ICT infrastructure can also be seen as either the tool or the target of cyberterrorism attacks. When critical computers, networks or systems are maliciously targeted, the goal can be to cause wide-

spread damage, interference to services and panic amongst users. However, ICT can also be used to assist with terrorism in general. For example, the Internet can be used to do research and gather information on bomb-building; email, discussion forums and social networking sites can be used for recruitment and communications; and phishing scams and credit card fraud can be used to fund terrorist activities. Thus, ICT infrastructure can also facilitate and support terrorism in general by serving as an aid and not the intentional target of attacks. As shown in Figure 1, ICT can provide a supportive role by aiding recruitment, training, intelligence, reconnaissance, planning, logistics, finance, propaganda and social services.

3. Types of cyberterrorism

Critical to cyberterrorism is the motivation driving these activities. The reasoning behind cyberterrorism will influence the intervention methods and thus a discussion of motivation behind terrorism in general follows. Weimann proposes the following types of terrorists: religious, New Age, ethno-nationalist separatist, revolutionary and far-right extremist [22].

Figure 2 shows a summary of terrorist types and example targets. Laqueur states that many terrorist groups traditionally contain strong quasi-religious fanatical elements for only total certainty of belief (or total moral relativism) provide justification for taking lives [11]. Religious terrorism thus includes the promotion of strong religious beliefs that can include the justification of lives.

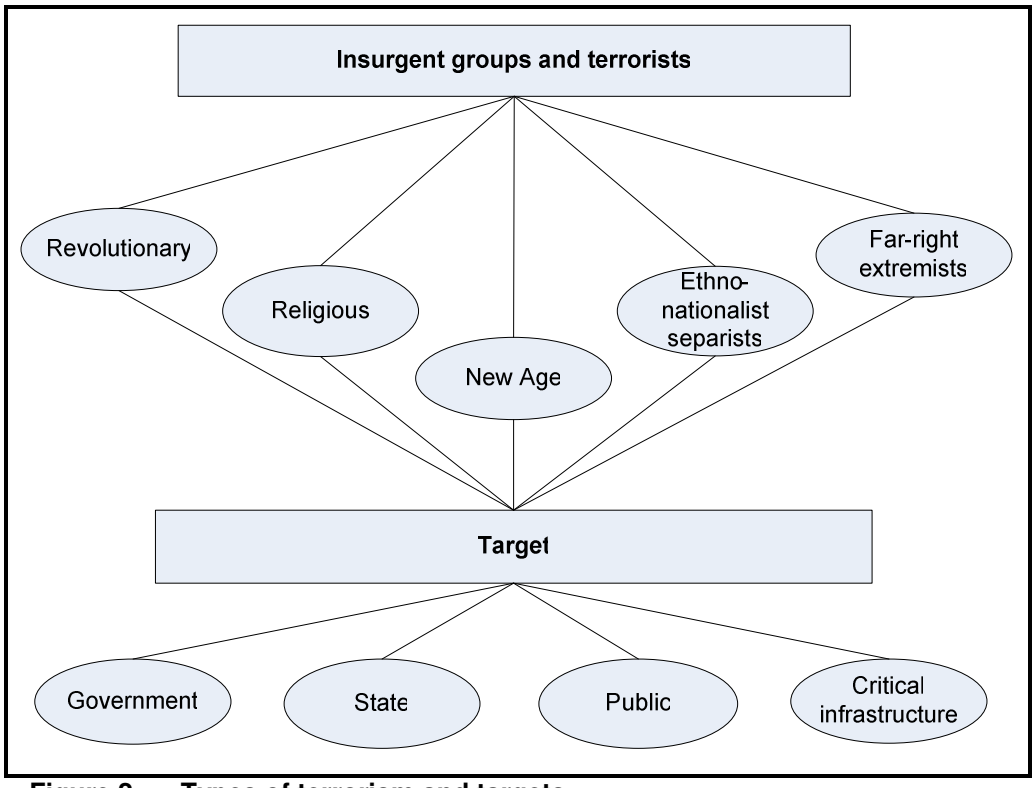

Figure 2: Types of terrorism and targets

Gearson discusses New Age Terrorism which looks at the vulnerability of modern societies to unconventional attacks [7]. New Age thinking can involve manipulation techniques and attacks that are planned using unconventional methods (the use of ICT).

Post discusses ethno-national separatists who are fighting for the establishment of a new political order based on ethnicity, as well as social-revolutionary terrorists who are trying to overthrow the capitalist economic and social order [17].

According to the Israeli political scientist, Ehud Sprinzak, right wing terrorism or far right extremism is characterised by the targeting of not only the “outsider” (e.g. foreigners, ethnic and religious minorities) but contemporaneously the state itself, as they are seen as ineffective or worse under the sway of the outsiders [12]. Far-right extremists thus justify the seizing of power based on the belief

system of superiority. In order to intervene, consideration needs to be given to the cause being promoted and how the mindset of the terrorist can be influenced.

Core to cyberterrorist intervention methods is the understanding of where cyberterrorism stems from and the development of a strategy to influence or change the thinking patterns that are inherent to certain cultures and tribal groups. As shown in Figure 1, consideration must be given to the social factors that influence the development of terrorism. This will include the environments that individuals are brought up in, culture, beliefs, political views, as well as the personality traits that may lead to conformity or defiance of expected behaviour.

This section provided an introduction to the field of cyberterrorism as well as a discussion of some of the core issues that will influence the development of countermeasures to combat cyberterrorism. In the next section, some of the countermeasures will be further elaborated on.

4. Introduction to countermeasures

Weiman [22] talks of the growing dependence of society on information technology that has created a new form of vulnerability and if terrorists follow the lead of hackers, theoretically they could access and even cripple critical sectors like the military or financial services. Unconventional war techniques require the influencing of the local population opinion rather than resorting to firepower. The emerging threat has social, political, economical and religious roots and therefore consideration should not only be given to the technical method of intrusion prevention, detection and reaction. Power lies in the hands of gangs, tribes, religious and ethnic groups. The lines between civilian and military are blurred when considering the domain of terrorism. Therefore, it is necessary to consider at a high-level how the opinions of people can be shaped as well as how to detect the growth of insurgency in groups.
Cyberterrorism merges two spheres, terrorism and technology. As a result, countermeasures for both spheres need to be addressed. Unfortunately, few of the issues can be strictly qualified as according to type, and is rather considered as cross boundary. For example, cultural centres can impact influence both religious and social opinions. In addition, treaties and policies have both legal and political implications.

In many instances, responses to terrorism are reactive. For example, handling medical emergencies after a bombing or carrying out investigation that traces the events that lead up to a malicious gas dispersal. To understand the threat, consideration needs to be given to the overall legal, religious, social, economic, political and technical considerations. A more detailed discussion follows in the next sub sections.

4.1 Cyberterrorism countermeasures from a psychological perspective

Cyberterrorism countermeasures specific to terrorism can be categorised as five types: legal, political, economic, social and religious. Figure 3 shows a summary of these countermeasures.

Cronin states that the major focus areas in response to terrorism are the use of law enforcement and the effectiveness of military responses [3]. The South African Information Warfare Course promotes the establishment of treaties, protocols, regulations and acts of law to ensure the just and fair conduct of relations between nations [23]. Laws can indicate that violence are an unacceptable form of protest and tries to provide a consistent means to deal with political and religious fanaticism. The public needs to be assured that the government is consistently handling factors that could affect their security and through policies and laws these foundational blocks can be set. International presence like that of Interpol and the Council of European Convention on Cyber Crime (first international treaty against cybercrime) are playing a huge role in the combat against cyberterrorism [6].

Military force can be used to retaliate against attacks, but the outcome of such action can result in various groups going into hiding and conducting underground operations. Therefore, while military force can be effective in disrupting plots, terrorist groups are evolving through the use of ICT infrastructure. Targeting hierarchical groups is no longer a simple task as members are geographically dispersed and can remotely target critical services like the water or transport sector. Cronin argues that military force is only effective as part of a multi-faceted campaign along with social, economic, legal and political elements.

Wilson discusses the establishment of fusion centres that will have intelligence, cultural specialists, security personnel, linguists, political military specialists, engineers, psychological operations (PSYOPS), media relations and economic advisors to collect, analyse, process and define courses of action depending on the specific region [25]. Wilson also states that humanitarian aid and peace-keeping can assist with battle needs [25].

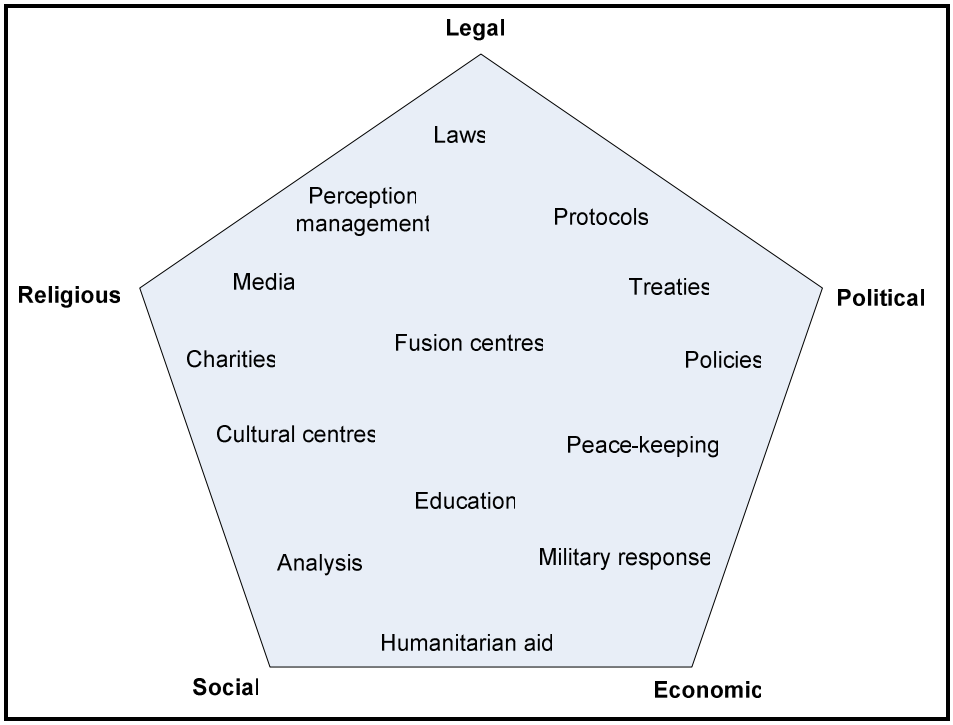

Figure 3: Counterterrorism measures from a psychological perspective

Williers concurs that assistance should be given to people who suffer from famine, political repression, natural disasters and violence as such steps can help with conflict resolution [23]. Favourable responses can be created by the supply of money, food, medicine, education, fuel and employment and this contributes to the perception management in a region. Providing charity and education to members of the community shows the effort to uplift those that are less fortunate. Education at cultural centres and perception management through the media can also try to discourage some fanatical religious and political views that promote violence. Studies have shown that extremists are active in recruitment through charity and cultural centres while also listening to inspirational preachers [5]. Thus, operatives at such centres will be beneficial in identifying potential extremist recruiters.

In order to increase intelligence, analysis at various levels is required. This can include the study of patterns, links, forensics, cultural, tribal, religious and communications-linguistics [24]. Overall, intelligence gathering though fusion and culture centres will provide insight into the unpredictable human aspect of terrorism.

In a report by the Centre for Strategic and International Studies the following comments by Jensen, Gordon and Spalding were recorded with regard to international collaboration [5]:

- Agencies need to co-operate more to ensure that information from highly specialised intelligence agents are actually communicated to members on the ground.
- Lack of information leads to speculation. Therefore, the media and the public need to share more informed analysis data.
- Greater international collaboration is needed, especially through the European Union.
- Like the US, interaction needs to take place between the community and academia
- Notice should be taken of the location of terrorism. In many cases, political and general instability provides the environment whereby support can easily be raised.

- Reading the mail of convicted terrorists can help detect potential crimes. The three prisoners involved in the 1993 World Trade bombing, whilst placed at the federals highest security prison were able to exchange around 900 letters with extremists between 2002 and 2005 including terrorists in Spain.

Overall, affecting people and their ideas are the means though which the war on terror can be fought. However, at a technical level prevention, detection and reactive methods can also be deployed. The next section addresses some technical methods in the fight against terrorism.

4.2 Cyberterrorism countermeasures from a technical perspective

Cyberterrorism countermeasures specific to terrorism can be categorised as six types: CSIRTs, intrusion prevention, network monitoring, interception and blockage, disaster recovery and forensics. Figure 4 shows a summary of these countermeasures.

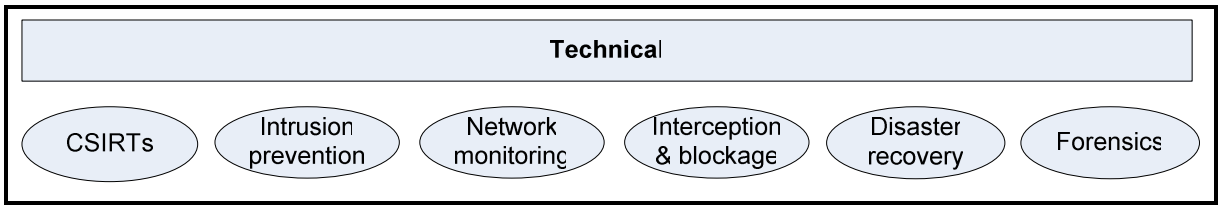

Figure 4: Counterterrorism measures from a technical perspective

The use of the Internet and web-based software applications by extremist groups is a growing phenomenon [1]. *"Terrorists have shown a clear interest in hacking skills and combining real attacks with cyber attacks* [14]*"*. To counter a scenario where sophisticated cyber-terrorists electronically break into computers that control dams or air traffic control systems, wreaking havoc and endangering not only millions of lives but National Security itself, it becomes essential to use technical countermeasures. "*The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure"* [21].

As a result of the unique circumstances of a cyberterrorism attack, countermeasures take the form of proactive, detective and reactive measures. For example, cyber attackers generally follow a strategy similar to traditional warfare: they first spy on the target site and find its vulnerabilities. Then, they identify and target the most vulnerable points of a site and probe their accessibility. The vulnerability and accessibility can be based on one or more of the security elements of technology, security policies and procedures or information use behaviours of individuals. The actual attack is launched to intrude and destroy the infrastructure and systems [10]. *Proactive countermeasures* will put specific measures in place to prevent a cyberterrorism attack. *Detective countermeasures* will put specific measures in place to detect a cyberterrorism attack or a potential cyberterrorism attack. *Reactive countermeasures* will put specific measures in place to address a cyberterrorism attack after it happened and to get the victim system up and running as soon as possible after the attack.

Intrusion prevention can be regarded as a proactive technical countermeasure to combat cyberterrorism. An intrusion can be classified as *"… any intentional event where an intruder gains access that compromises the confidentiality, integrity, or availability of computers, networks, or the data residing on them"* [9]. Intrusion prevention proactively protects computer assets from illegal or potentially threatening calls to the operating system, and it prevents potential infection with malicious code. Intrusion prevention differs from intrusion detection in that security mechanisms are put in place to prevent any intrusions before the system is violated, and without affecting the system's functionality [18]. It also protects a computer asset from being the target of automated intrusion scripts that can either attack the computer as part of a terrorist attack, or use it as a pawn in an attack. Based on the general attack strategy of cyberterrorism, intrusion prevention averts terrorists from spying on the target site, and accordingly prevents them from finding vulnerabilities. Both intrusion prevention and intrusion detection is indispensable because standard security control techniques are known to be fallible [9].

Computer Security Incident Response Teams (CSIRTs) have a number of proactive and reactive services that can be used against cyberterrorism. The proactive services provide assistance and information to help prepare, protect and secure constituent systems in anticipation of attacks,

problems or events. Performance of these services will directly reduce the number of incidents in the future. Some services include announcements (e.g. intrusion alerts raised by other constituents, vulnerability warnings and security advisories), technology watch (e.g. new technical developments, intruder activities and related tends), security audits, development of security tools and security-related information dissemination. Reactive services include alerts and warning, incident handling, vulnerability handling and artefact handling [2]. The range of services offered by a specific CSIRT depends on the hosting organisation/country, available funding and constituency requirements.

Network monitoring can be classified as a detective countermeasure. In January 2008, former US president Bush signed a directive that expanded the intelligence community's role in monitoring internet traffic to protect against a rising number of attacks on federal agencies' computer systems. This authorised the National Security Agency to monitor the computer networks of all federal agencies. This directive is in response to a string of attacks on networks at the State, Commerce, Defense and Homeland Security departments [15]. One of the benefits of both network monitoring and interception is that entities can be informed on how often they are mentioned or referred to in electronic communications. If any suspicious behaviour are uncovered through either network monitoring or interception, blocking that specific website, IP address or port can serve as effective countermeasure.

Cyberterrorism should definitely be addressed in a country/organisation's disaster recovery/business continuity plan. At a minimum, contact information for the appropriate people at technology service providers should be listed to assist a country/organisation in recovering from a cyber disaster [13].

Closely linked to forensic investigations, is the cyberterrorism first responder (CFR). CFRs are trained to effectively and efficiently counter any type of cyber-based terror attack against the internet, communications and network-based infrastructure [4]. Any response, either forensic first responder or CFR, are reactive in nature and investigates the actual cyberterrorism attack.

5. Conclusion

Cyberspace has emerged as a potential means in which terrorists can cause chaos and thus affect the psyche of communities. Underlying terrorism is political, social or religious reasoning that can justify violent and extremist behaviour. Carrying out cyberterrorism can involve using various information security exploits.

In this paper, the motivating forces behind cyberterrorism are covered. This provided a baseline on which potential countermeasures were proposed. This paper provides a summary of political, religious, legal, economic, social and technical issues that can be used in the combat of cyberterrorism. Suggested countermeasures range from laws to fusions centres, education, treaties, policies, the use of the media and perception management. From a technical perspective, countermeasures include activities like CSIRTS, network monitoring, interception and blockage.

References

[1] J. Carr, "Anti-Forensic Methods Used by Jihadist Web Sites," ESecurity Planet, 2010.

[2] CERT, "CSIRT services," 2002.

[3] A.K. Cronin, "The diplomacy of counterterrorism lessons learned, ignored and disputed," International Research Group on Political Violence (IRGPV), pp. 1-8, 2002.

[4] Cyberterrorism Defense Initiative , "CDI: Cyberterrorism First Responder (CFR)", Available online at http://cyberterrorismcenter.org/cfr.html.

[5] A. de Borchgrave, T. Sanderson and J. Harned, "Force multiplier for intelligence," Centre for Strategic and International Studies, 2007.

[6] M. M. Elmusharaf , "Cyber Terrorism:The new kind of terrorism", Computer Crime Research Center, Accessed 20086 October, Available online at http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism.

[7] J. Gearson, "The Nature of Modern Terrorism", The Political Quarterly, vol. 73, pp. 7-24, 2002.

[8] S. Gordon and R. Ford, "Cyberterrorism?", Computers & Security, vol. 21, pp. 636-647, 2002.

[9] J.V. Hansen, P.B. Lowry, R.D. Meservy and D.M. McDonald, "Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection", Decision Support Systems, vol. 43, pp. 1362-1374, 8 2007.

[10] S.M. Ho, "A Framework of Coordinated Defense", 2008.

[11] W. Laqueur, "Postmodern Terrorism", Foreign Affairs, vol. 75, pp. 24, 1996.

[12] G. Michael, Confronting Right Wing Extremism and Terrorism in the USA, New York and London: Routledge, 2003.

[13] D. Mortman, "Disaster recovery risk assessment for cyberterrorism attacks," 06 November 2009. 2009.

[14] MyBroadband.co.za, "Cyber terrorism on the rise," MyBroadband.Co.Za, 05 March, 2010. 2010.

[15] E. Nakashima, "Bush Order Expands Network Monitoring," The Washington Post, vol. Technology - Special Reports, Saturday, January 26, 2008. 2008.

[16] M.M. Pollitt, "Cyberterrorism - fact or fancy?", Computer Fraud & Security, vol. 1998, pp. 8-10, 1998.

[17] J.M. Post, "The New Face of Terrorism: Socio-Cultural Foundations of Contemporary Terrorism", Behavioral Sciences & the Law, vol. 23, pp. 451-465, 2005.

[18] J. Rrushi, "SCADA Intrusion Prevention System", 2006.

[19] N. Veerasamy, "A high-level conceptual framework of cyberterrorism", Journal of Information Warfare, vol. 8, pp. 42-54, 2009.

[20] N. Veerasamy, "Towards a conceptual framework for cyberterrorism", in Proceedings of the 4th International Conference on Information Warfare and Security, pp. 129-137, 2009.

[21] G. Weimann, "Cyberterrorism: The Sum of All Fears?", Studies in Conflict & Terrorism, vol. 28, pp. 129-149, 2005.

[22] G. Weimann, "Cyberterrorism: How real is the threat?" United States Institute of Peace, Tech. Rep. 119, pp. 1-12, 2004.

[23] C.J. Williers, C.J. Voster, A. van 't Wout, J.P. Venter, S.J. Naude and R. van Buuren, "IW Basic Course," Council for Scientific and Industrial Research, Tech. Rep. DEFT-IW-00200, 2005/06.

[24] G. I. Wilson, G. Wilcox and C. Richards, "Fourth Generation Warfare and the OODA Loop Implications of The Iraqi Insurgency", Smartpei.typepad.com, Accessed 20100507, Available online at http://smartpei.typepad.com/robert_patersons_weblog/files/4gw_ooda_iraq.ppt.

[25] G.I. Wilson, G. Wilcox and C. Richards, "4GW and OODA Loop Implications of The Iraqi Insurgency", in 16th Annual AWC Strategy Conference, 2005.