Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1082 – 1090

RESEARCH ARTICLE

CYBER TERRORISM ATTACK OF THE CONTEMPORARY INFORMATION TECHNOLOGY AGE: ISSUES, CONSEQUENCES AND PANACEA

Kuboye Oluwafemi Samuel[1],
koluwafemisam@yahoo.com
Yazan Al-Khasawneh[3],
yazankhasawneh689@yahoo.com

Wan Rozaini Sheik Osman[2],
rozai174@uum.edu.my
Saif Duhaim[4]
saifmtter@yahoo.com

School of Computing, Universiti Utara Malaysia, Sintok, Kedah

ABSTRACT: It is crystal clear that there has been systematic transformation of human activities and societies since the advent of information's technologies (IT). However, this information Technology that ought to be of enormous advantage without any fear in its usage by people has been hijacked by the world terrorists to lunch many attacks via cyberspace (internet).Cyber terrorism has been one of the social ideological menaces that have great challenges to the contemporary society all over the world. However, the emergence of this cyber terrorism has the potentials to vitiate the positive uses of information technology if not properly and promptly addressed. It is in the light of this that this study critically explores contemporary literatures of this topical issue of information technology aided terrorism (cyber terrorism). The study presents the semantic interpretations of cyber terrorism, the components of cyber terrorism, the motivating factors of cyber terrorism, the various cyber terrorism techniques usually adopted by the perpetrators (terrorists), and the consequences of such a prevalence cyber attack. The study equally suggests the possible panaceas to tackle the problem of cyber terrorism so as to maximize the benefits attached to information technology (IT) and minimize the evil posed by the terrorists.

Keywords: *Information Technology (IT), Cyber terrorism, Cyber attack, Cyberspace*

I. INTRODUCTION

Information Technology is a computer based tools used by people in other to work with information, support the information as well as processing the information for the need of an organizations, nations and individual needs (Haag & Cummings, 2010). However, this information Technology that ought to be of enormous advantage without any fear in its usage by people has been hijacked by the world terrorist to commit many crimes via cyber cyberspace (internet) which had wrecked much havoc on some of the organisations, individuals as well as the nation in general that are in dire need of it. Terrorism has been one of the social ideological menaces that have great challenges to the contemporary society all over the world. Effort has been made by those concerned to reduce the activities of perpetrators of traditional terrorism so that the world can be a safe place for all and sundry to live but it is so disheartening that as steps were taken to reduce the activities of the traditional terrorism, terrorism is becoming hard-headed especially with the development of terrorism aided by IT called cyber terrorism which has wrecked many havoc to organisations and nations of the world (Weimann, 2004). This so called cyber terrorism is caused as a result of quest for wealth, unemployment and the strong destructive motive (Hassan, Funmi & Makinde, 2012).

However, Weimann, (2004) stated that the tremendous growth experience in the information technology era has also created a new form of vulnerability which is cyber terrorism been experienced today in many of the developed countries of the world which gives terrorists the chance to launch any attack into to the national defence systems and the air traffic control systems. Weimann said that the more a country developed in the area of technology, the more it becomes vulnerable for cyber attacks against its infrastructure.

II. THE CONCEPT OF CYBER TERRORISM

The term terrorism can be refer to the unlawful use of force or violence against persons or property so as to intimidate a government or its citizens and organizations which may be to achieve a political or a fraudulent objectives (Bogdanoski & Petreski, 2013). Terrorism has metamorphosed from the traditional form to the cyber form of technology aided terrorism known as cyber terrorism. The term cyber-terrorism was coined in 1982 by Barry Collin who conceived the term to be the combination of the physical and cyber world. The cyber world is an online computer interaction environment where many users can exchange information in a real time which usually has influence on the physical environment (Klastrup & Tosca 2004). Different researchers and scholars in the information technology community and also in other fields of study had been able to give different definitions to the term cyber Terrorism base on their own perspective. This form of Cyber attack/threats refers to an action that is been taken deliberately against any critical infrastructures which may be the data, software, or the hardware in computer systems in other to degrade, disrupt, destroy, or even deny access (Denning & Denning, 2010). Also, Cyber terrorism is the use of computer networks for the purpose of posing harm to human life or to destroy most of the important and national critical infrastructure in a way that will paralyze the nation and also its citizens, that cyber terrorism emerge as a result of the convergence of the physical terrorism and the development of ICT (Ahmad, Yunos, & Sahib, 2012). It is because of the ease, low cost, speed and anonymity of the Internet, in addition to the current lack of an international convention on cyber-crime, that the number of cyber-attacks as well as the degree of destruction increases very rapidly (Dang, 2011). Three main factors have been identified to have been supporting the increasing number of such a hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks (Gercke, 2012). It can be deduced base on the different definitions from the different scholars and researcher that Cyber terrorism is the use of cyber word to launch an attack to the valuable infrastructures that the existence of organisations and nations totally relied upon which can lead to its closed down. Bogdanoski and Petreski (2013) stated that if drastic steps and actions are not taken to tackle the prevalence and the increasing of such a cyber attack (cyber terrorism) that the terrorist of the future to come will emerge in any of their wars/attack without making an attempt in firing a single shot just by destroying infrastructure that significantly relies on information technology.

III. COMPONENTS OF CYBER TERRORISM

Several attacks in the form of cyber terrorism are having some components which has been identified by many empirical scholars in the research community**.**

According to Ahmad, Yunos, and Sahib (2012) in their conceptual model identify the five components that a cyber terrorism is made up which are; the target of the attack, motivation and mission to be achieved when such attack is been launch, impact, tools been used to launch such attack, domain which is the environment as well as the method of action, the study further stretched that Cyber terrorism can be well understood by identifying the profile of actions or motivations that drive the action of the perpetrators.

Similarly, MacKinnon, et al .(2013) in the study on Cyber security counter measures to combat cyber terrorism emphasized that most contemporary definitions of cyber terrorism focuses on the following three aspects, the motivation of the perpetrator(terrorist), the targeted cyber system and at the same time the impact on an identified population, that the key issue in cyber terrorism is the motivation to carry out such an activity in cyberspace that results in violence/harm to an individuals and their property. This is in line with some of the components identified by Ahmad, Yunos, and Sahib (2012).The terrorists of the world take the advantage of the cyber world with strong motivation as a platform with which they can use to launch greater attack.

Yunos, Ahmad, Suid and Ismail, (2010) said that with the use of Information and communication technology, terrorist can pose greater damages or inflict the nation with difficult conditions as a result of the disruption of critical services that the cyberspace terrorist causes more harm and havoc through the cyberspace than through the traditional method of terrorism.

IV. MOTIVATING FACTOR OF CYBER TERRORISM

Anonymity Nature of the internet

Anonymity is one of the crucial factors that every evil perpetrator prefers so that their identity could not be traceable after performing their devilish act. Awan, (2014) said that the Internet is a safe environment as well as hiding platform for the terrorist as they can remain anonymous in such a way that their identity cannot be known and that they do not need to travel for long distance before they could lunch any attack. The terrorist of the world uses fake name that could not be traceable when performing any cyber attack. Younis Tsouli who make use of the fake name Inhabit (terrorist) 007 to perform many attack so that he will be difficult to trace is a typical example of cyber terrorist (Awan, 2014) .

Supportive Nature of the Websites

The internet has been seen as a medium that is very vast and that can at the same time attract the interest of many people to join any group of interest. The cyber terrorist prefer the use of the website because of its supportive nature in that it can send message to millions of people within a twinkle of an eye, they see it as a platform that is easy to recruit interested people (Awan,2014).

V. TECHNIQUES ADOPTED BY THE CYBER TERRORIST

The cyber terrorists of nowadays uses various forms of techniques and methods in ensuring that they unleash their terrorist attack to critical infrastructures. Bogdanoski and Petreski, (2013) affirmed that Cyber terrorism as a new form of security threat (Neo cyber attack) can sometimes manifest itself in different ways, which includes the hacking of a computer based systems, programming of a virus and worms, the Web pages attack, conducting a denial of service attacks, or the act of conducting a terrorist attacks through the electronic communications.

Hacking

The general term of all forms of unauthorised access to any computer system network is hacking which can occur in any form as such as "**cyber murder**" (Nagpal, 2002). The 1994 British hacker who hacked into the Liverpool hospital that changes the medical prescription that has been made by the nurse to the patient is a typical example of cyber murder (Nagpal, 2002). Many of these hackers make use of a 'brute force' which is the combinations of all possible letters as well as numbers and symbols till they get the password that they can use to lunch their evil attack.

Password Sniffing

The Cyber terrorist may at times make use of password sniff as techniques to carry out their cyber attack on any organizations and nation's critical infrastructure. The password Sniffer is software used to monitor network and at the same time capture password that passes through the network adaptor. This techniques are normally employed to monitor all the traffic of an area network which the terrorist do installed on many of the network system that they plan to penetrate such as the telephone system and the network providers (Hassan, Funmi, & Makinde, 2012).The sniffer software will automatically collect the information that users type such as username and a password when using internet access such as FTP or telnet. The example of this form of cyber attack was the one experience in 1994 which affects thousands of website (David et al, 1995)

Spam messages

The cyber terrorist at times makes use of spam messages as a strategy to launch their attack**.** "Spam" is the release of unwanted bulk messages. Though the attackers uses various form of spam messages but the commonly used one is the e-mail spam which at times may be in form of advertisement for products and services in disguise that if been open by receivers will automatically generate such a receiver password and username which they can later used to penetrate into his/her mail and perform their attack (Gercke, (2012).

Computer Viruses

Computer viruses are sometimes dispersed on a system to in other to perform harmful activities which may be to serve as a spy, generate information or even crack down the system. MacKinnon, et al, (2013) in his study identified that cyber weapons are mainly the software tools that is usually used by the cyber terrorists to pose havoc to any organisations and even the nations in other for them to achieve their missions and goals, that these software tools used can manipulate the computers, make intrusions into the systems, and at the same time perform espionage by sending spying which can be inform of viruses into a system.

VI. CONSEQUENCES OF CYBER TERRORISM

Cyber terrorism is new form of cyber threat and attack which has many consequences attached to it when launched against any nations and organisations.

Data Intrusion

The need for data in performing many functions in an organization cannot be over emphasized since it is the main instrument converted into information when been processed by organisations and nations. Koltuksuz, (2013) stated that cyber terrorism can destroy data integrity so that the data could no longer be trusted, destroying its confidentiality as well as interrupt its availability. The increasing rate of this cyber terrorism in intruding organizations and nations data has caused a lot of challenges which has resulted into the lost of vitals and crucial data that is usually hard to recovered.

Attacks on Critical Infrastructures

The heartbeat of any organizations are the critical infrastructure through which many of the organizations work is been carried out and also contain vital information. It is crystal clear that any attacks wrecked on the critical infrastructures of a nation could paralyze its economy. According to Thuraisingham (2004),an attack can be lunched on any of the following Infrastructure which includes telecommunication lines, the electronic, power, gas, reservoirs and water supplies, food supplies and as well as other critical entities that are essentials for the nation operations, that the attack on the software been used by the telecommunications industry could leads to the close down of all the telecommunications lines and the software used by the power and gas supplied could be attacked by the Cyber-terrorism.

Attack on Businesses

Many industries oriented businesses has been closed down and paralyzed as a result of the attack lunched by the cyber terrorist which in one way or the other affects the economy growth of the nations in the world. Thuraisingham (2004) estimated that cyber-terrorism could cause an organisations to lose billions of dollars in the area of businesses, that the information system of a bank can be attack or hack by the terrorists which will definitely leads to an unauthorised access to such bank account and make them to lose huge millions or billions of dollars which can make such bank to run into bankruptcy and finally make them to closed down. Thuraisingham also said that the computer system that is been destroyed and hacked is a great lose that took several time and effort to produce which in terms of monetary aspect may be equate to several millions of dollars.

Loss of Life

Cyber terrorism has claimed many innocent life's and at the same time render many homes to a state of dilemma that sometimes resulting to psychological trauma to the affected families. Awan, (2014) stated that cyber-terrorism can in one way or the other leads to the loss of life as well as causing serious damages, that this has manifested in attack on the computers usage, networks' and attacks that has resulted to the various forms of 'explosions of several plane crashes issues all over the world which that has claimed many life. It so disheartening that cyber terrorism are claiming life at an exponential rate which if urgent efforts are not taken to combat will keep claiming innocent life that ought to contribute their quota to the world economy growth. Terrorist might even break into the air traffic control and try to do manipulation on it which can leads to plane crashes or even causing a collision that can claim many life (Igbal, 2004). Igbal stretched further that the pharmaceuticals computer system of a company can also be hacked by the terrorist which can cause changes in the real formula of some of the essential medications that might have been prepared by the pharmacist.

Consumer Trust in Doubt

It is an established fact that the growth of any businesses and its patronage depends on the trust that its consumer have on such organisation as trust can be seen a tools that strengthens relationship and confidence between organisations and customers. Saini, Rao, and Panda, (2012) stated that cyber- attackers can in any way intrude into others'cyberspace in ensuring that they discourage and at the same time frustrate end users and customers that are normally visiting the concerned page for business dealings, this site when been intruded and attacked affects businesses and make end users to be a victim of the of the cyber terrorist which will definitely make customers to lose confidence in the said internet site. The power and the efficacy of trust in the information technology era are just too significant as without it organizations and businesses will not be able to withstand and even succeed a competitive environment.

VII. PREVENTIVE MEASURES OF CYBER TERRORISM

Regular System Maintenance/ Cyber system Auditing

The maintenance of organizations and nations system (technology) is very essential most especially in this era where there are daily occurrences of cyber terrorism attacked all over the world. Best practices for maintaining systems should be regularly followed as organizations standard procedures; the operating systems and the software should be regularly updated; policies on strong password should be fully implemented, systems should be 'locked down for the period of inactive; antivirus software to prevent intrusion should be installed and regularly updated; high intrusion detection systems and firewalls should be employed (Beggs & Butler, 2004). Regular cyber system auditing should also go along with system maintenance .Winterfeld and Rosenthal (2011) suggested that there should be regular and structured evaluation of every cyber system, the processes and even the personnel that is been used by an enterprise or organizations.

Co-operation of Various Organization/Nations

Co-operation is a vital tool in every organizations and nations that have goals and mission to be achieved as it will be difficult for goals to be achieved without it. Two are better than one as they can join forces and hands together in getting things done has been an age long adage. More organizations within the private sector need to co-operate with government bodies and also with the anti cyber-terrorism organizations to help prevent cyber related threats and attacks occurrences (Beggs & Butler, 2004).

Similarly, military co-operation against cyber terrorism will also help to fight against cyber terrorism and the enforcement of cyber deterrence which is a proactive measure that are taken to counter the activities of cyber terrorism (Czosseck, Tyugu, and Wingfield, 2011).

Enlightenment /Education of all and sundry

Enlightenment and education in every works of life is so essential that it can go a long way to address the menaces of cyber terrorism that affect the nation's critical infrastructure. Winterfeld and Rosenthal,(2011) posited that reformation of the education system in the religious world is one the crucial method that can help in fighting against cyber terrorism act in this information age since it is believed that extremist do come from the society where there is a high level of extremist teachings. The managers, employees and individuals needs to be educated on the security mechanisms and strategies being used within the organizations so as lead to a better understanding of the security mechanisms in place which will in protecting their information asset(Beggs & Butler, 2004). Thus, it is imperative that the general public should be well enlightens and informed about cyber terrorism so as to be able to take precautions in the usage of any system and to also identify the steps that can be taken in order to handle the concern better.

Implementation of Cyber law /Enactment of Cyber Law

The implementation of cyber law in totality without any fair or favour will reduce cyber terrorism to the minimal. Governments should ensure that their laws apply to cybercrimes and to be fully implemented and adhere to, it is important that the nation's of the world take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes (Hassan, Funmi & Makinde, 2012). The Government must ensure laws are formulated and strictly adhered to. Organisations that are totally dependent on network for their operations must ensure that the Network, Information and computer systems used are very secure (Hassan, Funmi, & Makinde, 2012).

Data Protection/Intrusion Detection

The confidentiality, availability and the integrity of data in any organizations are very important which efforts must be put in place to ensure that they are highly secure because it is the valuable cyber asset that makes every organizations to stand and at the same time relied upon. The data been penetrated by the cyber terrorist are more than just documents which may includes emails, web pages, web applications and as well as some vital operating systems (Winterfeld & Rosenthal ,2011). It is Therefore of high importance to give priority to a detailed cyber strategy that emphasis on data protection in other to safeguards the organizations and nation's vital information's. Monitoring any form of intrusion in an organizations and nation's critical infrastructure should also be encouraged as it will help to take immediate actions to avert threat before it happens. Organizations and nation's infrastructure systems will to some large extent have a high degree of protection if only the authorized people are the one that have access to the system but the insider as well as the authorized individuals can be used and influenced by the perpetrators (Winterfeld & Rosenthal 2011).

CONCLUSION

The importance of information technology around the globe cannot be over emphasised only that the havoc posed by terrorist who has taken its advantages to shut down many organisations and even destroyed nations relied and critical infrastructure are just too alarming. This study has been able to delve much on the semantic interpretations of cyber terrorism, the techniques adopted by the perpetrators (terrorist), the influencing factors, the consequences of such a prevalence new form of cyber attack (cyber terrorism) as well suggesting possible panacea to tackle the increasing rate of such a cyber attack so as to maximised the benefits attached to information technology (IT) and minimise the evil posed by the terrorist. Effort to secure the cyber space should be given the ultimate priority else the information technology will not be effectively utilized by users. The terrorist of the future will win the wars without firing a shot just by destroying nation's critical infrastructure if steps are not taken to tackle the prevalence of the increase in such a cyber attack (Bogdanoski & Petreski, 2013).

REFERENCES

Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in Nigeria. Electronic Library, The, 26(5), 716-725.

Ahmad, R., Yunos, Z., & Sahib, S. (2012, June). Understanding cyber terrorism: The grounded theory method applied. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on (pp. 323-328). IEEE.

Awan, I. (2014) Debating The Term Cyber-Terrorism: Issues And Problems. Internet Journal of Criminology .ISSN 2045 6743 (Online).

Beggs, C & Butler, M (2004). Developing New Strategies to Combat Cyber-Terrorism, 2004 IRMA International Conference.

Bogdanoski, M., & Petreski, D. (2013). Cyber Terrorism–Global Security Threat.Contemporary Macedonian Defense-International Scientific Defense, Security and Peace Journal, 13(24), 59-73.

Czosseck, C. Tyugu, T. Wingfield, T (2011), International Conference on Cyber Conflict

Dang, T.S. (2011) The Prevention of Cyberterrorism and Cyberwar; GA First Committee: Disarmament and International Security (DISEC) ODUMUNC 2011 Issue Brief for the

Denning, P. J., & Denning, D. E. (2010). Discussing cyber attack.Communications of the ACM, 53(9), 29-31.

Dembek, Z. F. (2014). Terrorism 101. In Conflict and Catastrophe Medicine (pp. 147-158). Springer London.

Iqbal, M (2004). Defining Cyberterrorism; journals of Computer and Information. L. 397.

Klastrup, L., & Tosca, S. P. (2004, November). Transmedial Worlds-Rethinking Cyberworld Design. In CW (pp. 409-416).

Gercke, M (2012).Understanding cybercrime: Phenomena, challenges and legal response. The ITU publication

Hassan, A. B., Funmi, D. L., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology,2(7).

Haag, S., & Cummings, M. (2010) Management Information Systems for the Information Age, 8th Edition.

Koltuksuz, A. (2013). Use of Cyberspace and Technology by Terrorists.Technological Dimensions of Defence Against Terrorism, 115, 106.

Kuznetcov, V.A & Kuznetcov, M.A (2013). The Legal Definition of Terrorism in the United States and Russia, World Applied Sciences Journal 28 (1): 130-134.

Lewis, J. A. (2002). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic & International Studies.

Linden, E. V. (Ed.). (2007). Focus on terrorism (Vol. 9). Nova Publishers.

MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). Cyber security countermeasures to combat cyber terrorism. Akhgar B and Yates S. Strategic Intelligence Management. Butterworth-Heinemann, London, 234-257.

Nagpal, R. (2002), Cyber terrorism in the context of globalization, II World Congress on Informatics and Law.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research & Applications (IJERA), 2(2), 202-209.

Thuraisingham, B. (2004). Data mining for counter-terrorism. Data Mining: Next Generation Challenges and Future Directions, 157-183.

Weimann, G. (2004). Cyberterrorism: How real is the threat?

Winterfeld, S., & Rosenthal, R. (2011). Understanding Today's Cyber Challenges. Policy, no. May, 28.