# Cyber Terrorism: Causes, Challenges and Solutions

Muhammad Shuaib Qureshi[*,1], Muhammad Bilal Qureshi[2] and Vijey Thayananthan[1]

[1]Computer Science Department, Faculty of Computing & Information Technology,
King Abdulaziz University, Jeddah, 21589, Saudi Arabia.
[2]Department of Computer Sciences, COMSATS Institute of Information Technology,
Islamabad, Pakistan.
[*]msqureshi@kau.edu.sa

**Abstract:** Cyber terrorism is a kind of cyber crime that is ever growing challenging threat enfolding the whole world under its attacks in one shape or another. The rate at which cyber terrorists commonly known as hackers are being generated induce extensive challenges of security, economy, and prevention mechanisms. Cyber terrorism demands massive power and economy to execute safety procedures for its prevention. Cyber security procedures provide an abstraction of protection and safety to the users and national infrastructure. However, underlying this abstraction, there are stringent requirements and challenges to facilitate safe and secure service through effective infrastructure, efficient and well designed solutions, intelligent mechanisms, and powerful approaches. This paper shortly describes and analyzes different cyber attacks, their origins, various challenges related to the cyber paradigm and asses possible protection solutions.
[Qureshi M.S, Qureshi M.B, Thayananthan V. **Cyber Terrorism: Causes, Challenges and Solutions.** *Rep Opinion* 2015;7(11):63-67]. (ISSN: 1553-9873). http://www.sciencepub.net/report. 8. doi:10.7537/marsroj071115.08.

**Keywords:** Cyber security, Cyber crime, Cyber terrorism, Hacking, Cyber war

## 1. Introduction

The internet is the fastest growing phenomenon in the world encompassing every walk of life. More than 5 billion internet users were estimated in mid 2013, and by the end of 2020 many expect this ratio more than 10 billion. The survey reports show that about 60% of the users use dark side of the internet generating substantial threats and vulnerabilities targeting a common internet user to a multinational billion dollars company or even the vital government information resources. It is a big challenge for the developing as well as developed countries because cyber terrorism worstly affects the technological progress in the area of E-commerce which in turn slows down the economic progress of a country. Being a global village today, absence of strong legislations and punitive actions encourages the cyber terrorists globally to further their objectives in or through a particular country resulting in bad reputation on international level. Cyber terrorists are always trying to use internet resources to change the mindset of the people so that they can actively commit different types of cyber crimes against persons (like pornography, harassment, etc), property (like unauthorized access and use of digital information), financial infrastructure (like stock exchange, trading floor etc), and communication infrastructure of a country (like satellite/cellular/network, air traffic control system etc). Almost all of the sectors including government, private, banking, economic, education, judiciary, etc are facing cyber security problems and fighting cyber war today. Cyber attacks are the biggest national security threat in 21st century. What an individual can do, if for example he/she cannot access his/her bank account or credit/debit card? Everything he/she has worked for could be lost in a click of mouse. Computers can play 2T's role in a crime; tool in a crime, target in a crime. Both uses have the same ratio and mostly innocent people are targeted. The main components of cyber crime are: (i) initiator: attacker that initiates crime (ii) event: attack (iii) platform: source or target infrastructure.

In this paper we are shortly describing cyber terrorism, its causes, challenges facing by the affectees, and possible solutions. This paper is organized as follows. Section 2 describes cyber terrorism, Section 3 gives classification of cyber terrorism, Section 4 shows profile of cyber terrorists, Section 5 enlist cyber terrorism victims, Section 6 analysis cyber terrorism, Section 7 accumulates cyber terrorism techniques, Section 8 details technical challenges, Section 9 explains possible solutions, and Section 10 concludes the paper.

## 2. Cyber Terrorism

Cyber terrorism is a harmful act of creating terror and loss of critical infrastructure. Cyber terrorism is usually not intended for physical harm, rather its intension is to attack a network computer to gain access to confidential data or financial information [1][2][3]. This act is carried out through the computer because it is cheap, difficult to track and can be operated from anywhere throughout the world.

### *A. Components of Cyber Terrorism*

(i) Initiator or attacker that initiates the crime,

(ii) event or attack, (iii) platform which is source or target infrastructure.

*B. Components of Cyber Terrorism*

(i) Initiator or attacker that initiates the crime, (ii) event or attack, (iii) platform which is source or target infrastructure.

*C. Characteristics of Cyber Terrorism*

Some of the characteristics of cyber terrorism are:

(i) Silent in nature

(ii) Global in character

(iii) No existence of physical evidence

(iv)Creates high impact

(v) High potential and easy to perpetrate

*D. Preferences of Cyber Terrorists*

What cyber terrorists want? What are their objectives and targets? Figure 1 groups some of the major preferences of cyber attackers, but these objectives are not limited to the below mentioned ones.

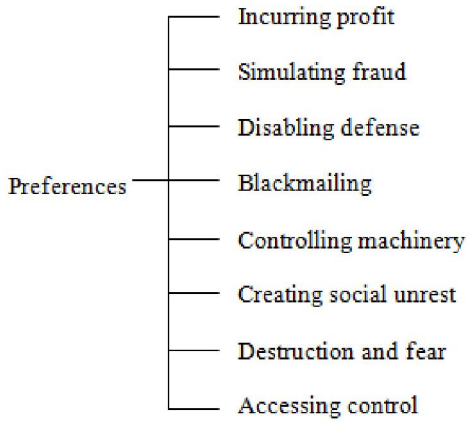


Fig 1: Taxonomy of cyber terrorist's preferences

## 3. Classification of Cyber Terrorism

Cyber terrorism can be classified into following four major categories.

A. Cyber terrorism against individuals

B. Cyber terrorism against property

C. Cyber terrorism against organizations

D. Cyber terrorism against society

*A. Cyber terrorism against individuals*

*(i) Email Spoofing:* In this type of attack a forged email is sent from fake source but appears to originate from the original source. In spoofed email the email header is forged.

*(ii) Spamming:* Multiple copies of spontaneous mails are sent continuously such as chain letters.

*(iii) Cyber Defamation:* In cyber defamation, computer and/or internet is used against someone by publishing defamatory material on website or sending defamatory information.

*(iv) Cyber Stalking & Harassment:* Cyber Stalking is tracking of someone's activities over internet. For this purpose e-mail, chat rooms, forms, net groups are used.

*B. Cyber terrorism against property*

*(i) Credit Card Fraud:* Theft of credit card details, passwords and using it for own benefit.

*(ii) Intellectual Property crimes:* These include; a) Software piracy: illegal distribution of copies of software. b) Copyright violation. c) Trademarks infringement d) Theft of computer source code

*(iii) Internet point larceny:* It means using internet hours illegally which is paid by other individual.

*C. Cyber terrorism against organizations*

*(i) Illegal access of computer system:* Illegal access of a system means accessing a computer system or network without prior permission from the owner of the system. It can be done in two ways;

*a) Altering of data:* It is illicit changing or deleting of data of an organization.

*b) Computer voyeur:* It is the illegal reading or copying of confidential information of an organization without changing or deleting of the actual data.

*(ii) Denial of Service:* In this type of cyber attack, incessant spurious requests are sent to the server so that the server becomes flooded and denying legitimate users to access the server. The server is crashed in this type of attack.

*(iii) Computer contamination:* A computer contamination is due to virus attack. Virus is a computer program that contaminates other programs. Viruses affect files and boot sector of computer.

*(iv) E-mail Bombing:* E-mail Bombing is a type of cyber attack in which huge number of mails are sent to the individual or company or mail servers that resulting into crashing.

*(v) Salami Attack:* Salami attack is when small attacks are adjoining to a major attack that cannot be detected due to its nature. These types of attacks are used for the commission of financial crimes.

*(vi) Logic Bomb:* Logic Bomb is an event reliant program. The computer system crashes as soon as the designated event occurs.

*(vii) Trojan Horse:* Trojan Horse is an illicit program which function from inside what looks to be an authorized program, thereby obscuring what it is actually doing.

*(viii) Data Diddling:* Data Diddling attack is a form of active attack that involves alteration of existing data just before it is processed by a computer and then changing it back after the processing is completed. This type of attack is exceedingly common.

*D. Cyber terrorism against society*

*(i) Forgery:* This type of attack is called fictitious attacks. Currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers.

*(ii) Cyber Terrorism:* Cyber Terrorism is acts of sabotage to create terror and loss of critical infrastructure. Cyber Terrorism is usually intended for physically harm rather it intension is to attack a network computer to gain access to confidential data or financial information.

*(iii) Web Jacking:* in these attacks generally attackers/hackers get access and control over the website of another organization or personnel and then modify the content of website for fulfilling political or financial objectives.

## 4. Profile of Cyber Terrorists

It is reported that almost all of the cyber terrorists are not the professional ones, but miserable people who only want to achieve their target objective and then ban their activities.

Below we list some of the cyber criminals who commit crimes.

(i) Disgruntled employees
(ii) Teenagers
(iii) Political activists
(iv) Professional hackers
(v) Business rival
(vi) Terrorists
(vii) Greedy people

## 5. Cyber Terrorism Victims

Almost every sector of our life is affected by cyber terrorism but mostly the following sectors are the main targets of cyber terrorists.

(i) Industry
(ii) Government
(iii) Law Enforcement
(iv) ISP
(v) E-Health
(vi) E-Commerce
(vii) Entertainment
(viii) Military
(ix) Telecommunication
(x) Education
(xi) Online Services
(xii) Political Organizations
(xiii) News
(xiv) Finance
(xv) Social Networks
(xvi) Sports
(xvii) Forums
(xviii) Other Organizations

## 6. Analysis of Cyber Terrorism

**Table 1:** Last three years ratio of cyber terrorism victims

| Target Sectors | 2012 (%) | 2013 (%) | 2014 (%) |
|---|---|---|---|
| Industry | 21 | 27 | 33 |
| Government | 18 | 22 | 29 |
| Law Enforcement | 2 | 5 | 11 |
| ISP | 4 | 6 | 12 |
| E-Health | 3 | 7 | 9 |
| E-Commerce | 2 | 11 | 18 |
| Entertainment | 2 | 4 | 5 |
| Military | 4 | 13 | 19 |
| Telecommunication | 4 | 8 | 15 |
| Education | 8 | 9 | 11 |
| Online Services | 5 | 14 | 22 |
| Political Organizations | 5 | 7 | 8 |
| News | 5 | 9 | 13 |
| Finance | 4 | 13 | 28 |
| Social Networks | 6 | 17 | 26 |
| Sports | 3 | 5 | 6 |
| Forums | 2 | 3 | 7 |
| Other Organizations | 5 | 12 | 18 |

The values of Table 1 are pictorially presented in Fig.2 [1][10].

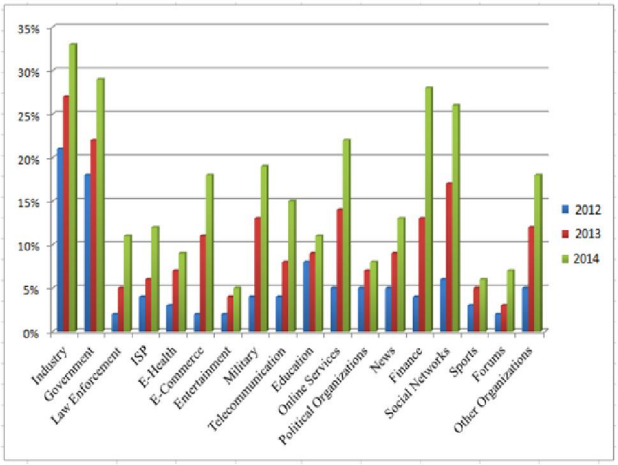


Fig 2: Last three years ratio of cyber terrorism victims

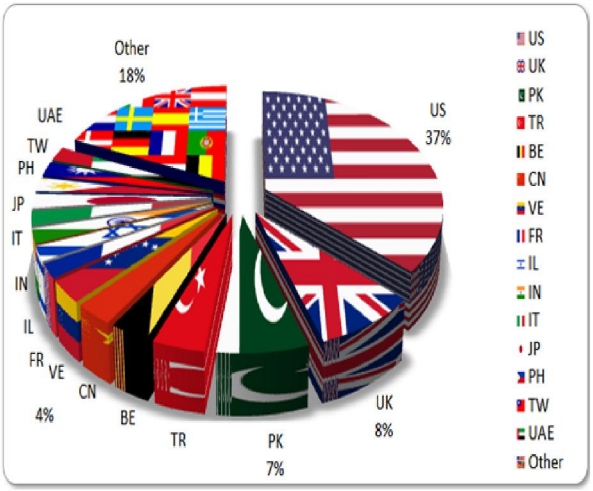


Fig 3: Countries affected by cyber terrorism [1][2][5]

Table 1 indicates that cyber terrorism affectees have been increased in the recent year 2014. It shows that till now countries have not got any successful control over cyber crimes and terrorism.

## 7. Cyber Terrorism Techniques

Cyber terrorists are using multiple advanced techniques for cyber attacks. During 2013, the techniques used by the cyber terrorists for cyber terrorism and the frequency distributions of these techniques are mentioned in Table 2 [7][8][11].

**Table 2:** Distribution of cyber terrorism techniques

| Technique | Frequency (%) |
|---|---|
| Defacements | 21 |
| Account Hijacking | 20 |
| Unknown | 19 |
| SQLi | 15 |
| DDoS | 9 |
| Unspecified Malware | 5 |
| Targeted Attacks | 4 |
| Exploited Vulns | 2 |
| iFrame Injection | 2 |
| Brute Force | 1 |
| DNS Poisoning | 1 |
| XSS | 1 |

Values of Table 2 are pictorially presented in Fig 4.

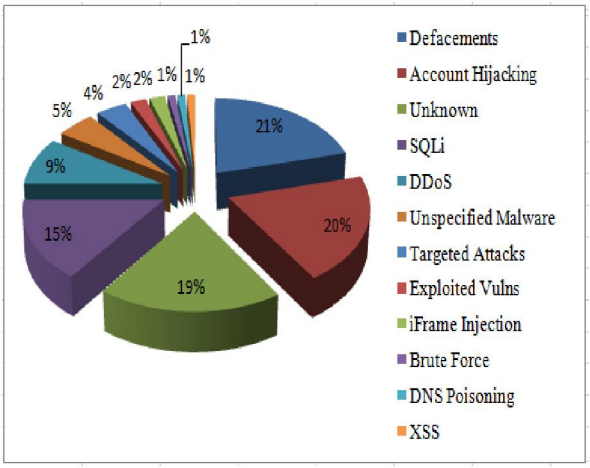


Fig 4: Cyber terrorism techniques used by cyber terrorists

## 8. Technical Challenges

(i) Acute shortage of Information security professional specially in government organizations,
(ii) No information security policy,
(iii) Breaches are not being reported,
(iv) Information outflow to un-authorized channels without any due care,
(v) In most of the organizations, there is no concept of security audit.

## 9. How to Combat Cyber Terrorism

There are no 100% ideal solutions to stop cyber terrorism. But some precautions and measures can be taken that can be used to secure ourselves from cyber terrorism [4][6][7][8][9]. We can make difficulties for cyber attackers to attack on our systems. Some of the suggested procedures are described below.

(i) Security and defense should take actions to stop using our systems against us. It also needs collective response and efforts from public.
(ii) Google, Microsoft, Yahoo etc should work to give secure services to the customers who are affected by the attackers.
(iii) Collective efforts should be voluntarily, stakeholder driven and should take advantage of the experts of the civil society.
(iv) We cannot solve all of the cyber attacks but should be less and minimum. We can make much more difficulties for attacker to attack our system.
(v) Federal code of conduct and laws should be implemented against cyber criminals and it is one of the most powerful ways to stop cyber attacks.
(vi) Workshops should be arranged to make awareness and educate public from different types of cyber attacks.
(vii) Cyber security working groups should be made in government as well as private sectors to overcome cyber attacks. They should deliver practical solutions to such kind of problems.
(viii) Proper campaign should be circulated through paper-based and paper-less media to make awareness among general public how cyber terrorists can damage or miss use their intellectual properties.
(ix) The government should make proper arrangements to train internet users of government and private bodies to identify vulnerabilities and how to tackle such attempts.
(x) Access control policies must be implemented by the organization to control unauthorized access to the information systems.
(xi) Business organizations should train their employees how to use systems efficiently and securely.
(xii) Organizations should improve the risks associated with their system intervention.
(xiii) Strong legislations and punitive actions should be taken on government level to discourage the cyber terrorists globally not to further their objectives.

*A. Suggestions for Individual User:*

(i) Use a window firewall.
(ii) Use registered and updated antivirus.
(iii) Use long, complicated and complex passwords.
(iv) Be careful what you download.
(v) Be careful and safe browsing.
(vi) Don't share your personal confidential information on internet.

(vii) Chat rooms are the most dangerous areas on the internet. Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each others. Criminals use it for meetings; hackers use it for discussing their exploits / sharing the techniques.
(viii) Don't install or open unknown mail attachment and software.
(ix) Electronic transactions are not secured. The credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

## 10. Conclusion

In this paper we have briefly described cyber terrorism, its classification, victims, facing challenges, profile of cyber terrorists, and possible solutions and measurements that should be taken on national and international level to combat this curse, because about 70% of the national economy is spent on avoiding cyber terrorist activities. But till now, no country of the world has got full command over this issue which needs full attention and possible techniques to combat it.

## References


1. Cyber Attacks Distribution 2012 Reports, http://hackmageddon.com /2012-cyber-attacks-statistics-master-index/ accessed on Nov 25, 2014.
2. Poole, Bernard John, and Elizabeth Sky-McIlvain. "Education for an information age." (2014).
3. R. Anderson and B. Schneier, "Economics of Information Security," IEEE Security & Privacy, vol. 3, no. 1, 2005, pp. 12–13.
4. Sinrod, Eric J., and William P. Reilly. "Cyber-crimes: A practical approach to the application of federal computer crime laws." *Santa Clara Computer & High Tech. LJ* 16 (2000): 177.
5. Kshetri, Nir. "The simple economics of cybercrimes." *Security & Privacy, IEEE* 4, no. 1 (2006): 33-39.
6. Choo, Kim-Kwang Raymond. "The cyber threat landscape: Challenges and future research directions." *Computers & Security* 30, no. 8 (2011): 719-731.
7. Willison, Robert, and James Backhouse. "Opportunities for computer crime: considering systems risk from a criminological perspective." *European journal of information systems* 15, no. 4 (2006): 403-414.
8. Boateng, Richard, Olumide Longe, Victor Mbarika, Innocent Avevor, and Stephen Robert Isabalija. "Cyber crime and criminality in Ghana: Its forms and implications." *AMCIS 2010 Proceedings* (2010).
9. Douglas, John, Ann W. Burgess, Allen G. Burgess, and Robert K. Ressler. *Crime classification manual: A standard system for investigating and classifying violent crime*. John Wiley & Sons, 2013.
10. Giunipero, Larry C., and Reham Aly Eltantawy. "Securing the upstream supply chain: a risk management approach." *International Journal of Physical Distribution & Logistics Management* 34, no. 9 (2004): 698-713.
11. http://hackmageddon.com, accessed on Nov 10, 2014.


11/10/2015