IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 1, January 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001047

Study of Cyber-Terrorism

Amit Singh, Prof. Rama S.Bansode

P.G. Student, Department of Computer Application, P.E.S. Modern College of Engineering College, Pune, Maharashtra, India

Research Scholar, TMV Pune, Asst. Professor, P.E.S. Modern College of Engineering, Pune, Maharashtra, India

ABSTRACT:Thanks to the web, the distances between the countries are easily overcome and therefore the communication network rapidly expands. This situation also affects the cybersecurity of the countries to an excellent extent. Attacks on critical infrastructures, companies, and public institutions can be a magnitude that makes great harm. These developments in cyberspace bring new problems. One of them is cyber terror. Cyberterror doesn't have a particular and well-known definition. Cyberterror is that the realization of terrorist acts within the field of cyberwar. In addition, cyberspace may be a place of display for terrorist acts. This effect of cyberterror attacks has reached A level to scare all countries. There is not enough information about the definition, characteristics, methods utilized in cyber terror attacks, and cyber terror groups. In this chapter, information is going to be presented, endeavors on awareness-creation are going to be made, and a task of guiding the longer-term studies is going to be taken.

I. INTRODUCTION

The term “Cyber-Terrorism” is complex and combines two concepts: “Cyber”, pertaining to cyberspace, and “Terrorism”, whose meaning and scope are going to be nalyzed later on this basis, we can assume that cyber-terrorism is a special type of terrorism, where the “Place” or “Medium” it is carried out in is cyberspace. Cyberspace is taken into account “A globally interconnected network of digital information and communication infrastructures”, normally understood to mean the web and, more broadly, computer networks.

The concept of cyberterrorism usually refers to a variety of very different actions, from the straightforward spread of propaganda online, to the alteration or destruction of data , and even to the design and completing of terrorist attacks via the utilization of computer networks. as such, so as to raised understand what cyberterrorism is, this text will begin by analyzing the concept of “terrorism” –including its structure, harm principle, and elements– as a broad category to which the species “cyberterrorism” belongs; later, it'll delimit the thought of cyberterrorism and distinguish it from others with which it's a particular similarity; finally, it'll raise a number of the foremost important challenges that cyberterrorism implies during a global and technologically interconnected world.

In that sense, “the better thanks to considering terrorismin that sense, “the better thanks to considering terrorism . . . isn't as a criminal offense but as a special dimension of crime, a higher, more dangerous version of crime, a sort of super-crime incorporating a number of the characteristics of warfare”

II. LITERATURE REVIEW

Despite the inherent advantages, the dependence on information technology has left nations and society much more vulnerable to cyber-attacks like computer intrusions, scrambling software programs, undetected insider threats within the network firewalls, or cyber terrorists. the web was designed as a benign venture of data exchange, making it inherently insecure and ill-equipped to trace attackers or to prevent them from abusing the intrinsic openness of cyberspace.
during a survey completed by 118 researchers working in 24 countries across six continents Jarvis & Macdonald, (2015) have found that a majority of researchers agree that a specific definition of cyberterrorism is vital for academics and policymakers. the talk about how they lie around what this exact definition is, further highlighting the necessity for a universal definition of this multijurisdictional problem for policymakers and researchers alike. The definition should pin down the core characteristics or principal of the concept; and, the range of actual or potential scenarios to which the term cyber terrorism is usually applied. Defining

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001047

cyberterrorism is made even harder by the abstract nature associated with understanding how certain incidents occur in cyberspace.

III. WHAT IS CYBER-TERRORISM

The expression of "Cyber Terrorism" includes the intentional attack on the computer for the knowledge to producing destructive effects to property of the government.
Hacking of a computing system then deleting the useful and valuable business information of the rival competitor may be a part and parcel of cyber terrorism.

IV. CYBER-ATTACKS

A computer attack could also be defined as actions directed against the rival competitor's computer systems to disrupt equipment operations, change processing control, or corrupting the stored data. Different attack methods target different vulnerabilities and involve differing types of weapons, and a number of other could also be within the present capabilities of some terrorist groups. Three different methods of attack are identified during this report, supported the consequences of the weapons used

1. Physical Attack
2. Electronic Attack (EA)
3. Network Attack (CNA)

1. **Physical Attack:** A physical attack disrupts the reliability of computer equipment and the availability of knowledge. Physical attack implements through the use of compact weapons, creating heat, blast, and dividing into a different part, or through direct control of wiring or equipment, usually after detecting unauthorized physical access.
   A physical attack involves compact weapons directed against a rival or government computer facility or its transmission lines. The temporary loss of communications links and important data added to the consequences of the physical attack by closing financial markets for up to every week.

2. **Electronic Attack (EA):** Electronic attack, most ordinarily mentioned as an Electromagnetic Pulse (EMP), disrupts the reliability of equipment through generating instantaneous high energy that overloads circuit boards, transistors, and other electronics. EMP effects can penetrate computer facility walls where they will erase electronic memory, upset software, or permanently disable all electronic components.
   An electronic attack (EA) involves the profitable and effective use of the facility of electromagnetic energy as a weapon, more commonly used as an electromagnetic pulse (EMP) to overload the computer circuit, but also during a non-violent form, to insert a stream of pretty and spiteful digital codes directly into an enemy microwave radio transmission.

3. **Network Attack (NA):** A network attack (NA), usually involves unfamiliar codes used as a weapon to infect enemy or rival computers to take advantage of a weakness in software or network, within the system configuration, or the computer security practices of a corporation or person. Other sorts of NA are enabled when an attacker uses stolen information to enter restricted computer systems.
   A network attack (NA), or "cyberattack," disrupts the integrity or authenticity of knowledge, usually through malicious code that alters program logic that controls data, resulting in errors in the output. Computer hackers opportunistically scan the web trying to find computer systems that are misconfigured or lacking necessary security software. Once infected with malicious code, a computer is often remotely

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001047

controlled by a hacker who may, via the web, send commands to spy on the contents of that computer or attack and disrupt other computers.

V. FORMS OF CYBER-TERRORISM

1. Privacy Violation

The law of privacy means recognizing of the individual's right to be includes and to possess his personal space inviolate. Individual's privacy is being violated with various Cyber-Attacks in world.
The right to privacy as an independent and distinctive concept originated within the field of tort law, under which replacement explanation for action for damages resulting from unlawful invasion of privacy was recognized.

2. Secret Information Appropriation and Data Theft

The information technology is often misused or leaked by breaching the precious government secrets and confidential data of personal individuals and therefore the government nd its agencies.
A network owned by the government may contain valuable information concerning defense and other top secrets.
These top secrets are targeted by the terrorsits to facilitate their activities, including destruction property.

3. Demolition of E-Governance Base

The aim of E-Governance is to from the interaction of the citizens with the government offices hassle free and to share information during a free and transparent manner.
Cyber-Terrorism targets the E-Governance database to wreck the connection between the people and government.
In result Cyber-Terrorism can reveal the secret of government including the trading secret.

4. Distributed Denial Of Services Attack

The Cyber Terrorists can also use the tactic of Distributed Denial Of Service (DDOS) to overburden the government and its agencies electronics bases. This is made possible by first infecting several unprotected unprotected computes by way of virus attacks the taking control of them.
Once control is obtained, they will be manipulated from any locality by the terrorists. These infected computers are the made to send information or demand in such an outsized number that the server of the victim collapses.

5. Network Damage and Distribution

The main aim of cyber-terrorist activities is to cause network damage and disruptions.This process may involve a mixture of unauthorized computer access, virus attacks, hacking, etc.
After an attack, the network gets collapsed and results in the network system failure due to this network sector suffers a major loss and system crash problem.

Network damage causes an entire list of problems, and every one of them are often very costly. you'll even face fines for each minute of the network outage. If the network is down for extended then a couple of minutes you'll be facing tons of cash in penalties or Service Level Agreement for Services (SLA) refunds.

VII. CONCLUSION

With over 200 countries connected to the web, cybercrime has become a worldwide issue that needs the complete participation and cooperation of the general public and personal sectors altogether countries, including the 150 plus developing countries around the globe.
Avoiding "Cyber Havens" (like concealment havens).
We will sink or swim together coordinating and cooperation are success key.
Safeguards are needed to make sure that laws that place restrictions on Internet access and content aren't abused and are following the rule of law and human rights.
The clarity within the law is additionally needed to make sure that laws aren't wont to prohibit access to content during a manner that violates human rights law. A danger exists for "organization" or "function creep"

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001047

(i.e., a piece of personal information that is collected for terms wont to describe the expansion of law and/or other measures in areas beyond their original scope), where laws and investigatory powers introduced to focus on one sort of cybercrime are then wont to target other, less serious sorts of cybercrime. Overall, existing many-sides and regional legal instruments, and national laws, vary in terms of communicated material and extent of coverage of criminalization, investigative measures and powers, digital evidence, regulation, risk, and jurisdiction, and international cooperation.

REFERENCES

1. Australian Cyber Security Centre. (2016). Threat Report. Retreived from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf
2. Chen, Thomas M. (2014). Cyber terrorism after STUXNET. Strategic Studies Institute & US Army War College Press: Pennsylvania. Retrieved from http://strategicstudiesinstitute.army.mil/pdffiles/PUB1211.pdf
3. Goodman, S. E., Kirk, J. C., & Kirk, M. H. (2007). Cyber space as a medium for terrorists. Technological Forecasting and Social Change, 74(2), 193-210. Retrieved from http://www.sciencedirect.com.virtual.anu.edu.au/science/article/pii/S004016250600148X
4. Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). Cyber terror: Prospects and Implications. [White Paper] Center for the Study of Terrorism and Irregular Warfare: Los Angeles, CA. Retrieved from http://www.au.af.mil/au/awc/awcgate/nps/cyberterror_prospects.pdf
5. United States Department of Defence. (2015). The DoD Cyber Strategy. Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details