A CRITICAL REVIEW ON CYBER TERRORISM

Dr. Rajeev Nain Singh

Assistant Professor, Faculty of Law,
Nehru Gram Bharati (N.G.B.D.U),
Prayagraj

Shishir Kesarwani

Research Scholar
Nehru Gram Bharati (Deemed to be University),
Prayagraj

INTRODUCTION

Terrorism has presented a significant challenge in our daily lives. Terrorist attacks in major metropolitan areas, towns, and tourist destinations around the world have displayed the ineptitude of the state's response to the threat. Many major counter-strategies are being developed by nations in order to deal with the challenges. However, the majority of the endeavours are designed in a conventional manner that may be efficacious in customary terror attacks. Nevertheless, there are difficulties when it comes to an unconventional terror attack, which has displayed the ineptness of the state system to solve the problem.(1)

Many major counter-strategies are being developed by nations in order to deal with the challenges. However, the majority of the endeavours are designed in a conventional manner that may be efficacious in customary terror attacks. However, there are constraints when it comes to an unconventional terror attack. I.T. has provided users with access to a massive data bank of information on everything and anything. However, it has given terrorism a new dimension. According to recent reports, terrorists are also preparing to use cyberspace to undertake terror attacks. Such attacks in the future cannot be ruled out.(2)

Cyber terrorism is a term that refers to terrorism that occurs in cyberspace. India has carved out a niche in information technology over the last few decades. The

majority of the Indian financial sector, postal offices, other agencies, and financial institutions have replaced manual processes with IT. Cyber terrorist attacks are primarily carried out in these institutions via IT, such as hacking, fraudulent e-mails, ATM spoofing, mobile phones, satellite phone hacking, and so on. The article envisions an awareness of the nature and effectiveness of cyber threats, as well as studying and analysing India's efforts to address the challenge and highlighting what more could be done.(3)

As a fast expanding postcolonial nation, India's internal political and social environment has profoundly influenced its approach to cyberspace and cyber security. India's potential for cyber defense was generally restricted due to a lack of awareness combined with a lack of technology to develop adequate cyber security structures, that latter of which was secured by global technology guidelines recommended such as the Wassenaar Framework. Furthermore, India's cyber security policy has traditionally been positioned with sovereign equality considerations, particularly state-sponsored terrorism and national defence. Integrating stated objectives with sovereign rights and security reasons, cyber security has thus been approached primarily from a state-centric perspective, with the discourse focusing on national security rather than a broader multi-stakeholder perception focusing on social or economic aspects.

The increasing prevalence of I.T. and the web in India occurred only in the last decade, despite its roots in the early 1990s liberalisation of the Indian economy. As a result, the evolution of cyberspace regulation was delayed. Because computers and the internet were not widely used until late 1990s, there was limited pressure for the development of laws to govern computers and cyberspace. The Information Technology Act, India's overriding regulations for governing information technology, was imposed in the year 2000, even then, it didn't sufficiently address these issues of cyber defense, only introducing and penalising the incidence of hacking.

Following that, in 2004, the Indian Computer Emergency Response Team (CERT-in) was formed, and it has since dominated cyber security in India. The Cert-in annual reports, that provide annual statistics on cyber attacks, paint a picture of cyber threats' exponential growth over the last decade.(4)

Statistics published by the government adds context to the growing importance of cyber security policymaking. According to NCRB data for the years 2010-2020, a

total of 1791, 2876, and 4356 Cyber Crime complaints were registered under the Information Technology Act, respectively. Moreover, during the same years, 422, 601 and 1337 cases were brought under Cyber Crime related Sections of IPC.

Furthermore, from 22060 in 2010 to 96383 in 2020, the number of incidents reported to the CERT-In increased exponentially. These incidents included phishers, scanning, spam, malicious code, website intrusions, and so on. According to the CERTin report 2020, there were 8,311 security breach crimes reported in the nation in January 2019 alone, up from 5,967 the previous year. An upsurge in cybersecurity incidents, both domestically and internationally near the close of the decade heightened the need for cyber security mechanisms to be established.

Following that, in 2008, the IT Act was amended to define the role of CERT-In and to introduce penal behaviour against cyber-threats such as cyber-terrorism, identity theft, and data protection. The 2008 reform also included a system for identifying "Critical Infrastructure" and mechanisms for protecting it. However, the IT Act's development of a successful cyber security infrastructure has been delayed. The National Cyber Security Policy, that also outlines the government's policy objectives, was introduced in 2013, years after cyber security was ostensibly recognised as a concern, and has not been updated since. Similarly, the NCIIPC, the central team responsible for CII protection, was only informed in 2014, after a 6 year gap from its conception under the IT Act.

DEFINITION OF CYBER TERRORISM AND CYBER CRIME

Cybercrime is a type of crime that involves computers and computer technology. The computer could have been used to commit a crime or it could be a target. Cybercrime can have an impact on a country's national financial and security situation. Hacking, copyright infringement, child pornography, and child grooming are examples of crimes.(5) Individuals may be harmed in this regard if they disclose confidential information such as ATM pins, bank details, and so on in public. When terrorist groups send out emails about women's security, cross-border crimes, financial theft, and so on, a nation-state will be attacked... Cybercrime was defined by Prof. Halder and Prof. Jaishankar as

"offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of victim or cause physical or

mental harm or loss to the victim directily or indirectly using modern telecommunication networks such as Internet and Mobile Phones(SMS/MMS)". (6)

This two anthers also commented on the focus gender and defined cyber crime against women as "crimes directed at women with the intent to purposefully harm the victim both psychologically and physically through the use of modern telecommunication networks such as the Internet and mobile phones."(7)

Cyber terrorism is the use of the internet in terrorist activities. Cyber terrorism is a contentious concept. Some authors selected a very specific meaning. They believe that this terrorism is connected to the deployment of known terrorist organisations or disruption threats against information systems with the primary goal of instilling fear and panic. Other authors chose a much broader definition, which tends to include cyber crime when, in reality, they believe cyber crime and cyber terrorism are two distinct issues.(8) Cyber terrorism is also defined as the deliberate use of computers, networks, and the public internet to harm innocent people and damage for personal gain.(9)

Because this is a form of terrorism, the terrorists' goal could be political or ideological. Because this is a form of terrorism, the terrorists' goal could be political or ideological. These terrorist organisations include Alqaeda, ISIS, Mujahideen, and others. These organisations communicate with their members via the internet. Eugene Kaspersky now believes that cyber terrorism, rather than cyber war, is a more accurate term.(10) "Without attacks, they have no idea who did it or when they'll strike again, so it's not a cyber war, but cyber terrorism," he said. According to some authors, cyber terrorism does not exist and is simply a matter of hacking or cyber warfare.(11)

In a broad way cyber terrorism is classified as "The preplanned use of activities or the threat of same, against networks and computers with the goal of causing harm or further social, philosophical, religious, diplomatic or similar objectives " religious, political or similar aims " . The term first appears in defence literature, in reports by the US Army War College as early as 1998.

The national conference of state representative and organisation of legislator established to assist policy makers with problems such as economic system and homeland security described cyber terrorism as "The use of I.T. by terrorist individuals and organizations to further their agenda. This can include using IT to

plan and carry out attacks on networks, computer systems, and telecommunications infrastructures, as well as exchanging information and making threats electronically."(12)

METHOD OF ATTACKS

Computer viruses and warms are the most commonly used weapons in cyber terrorism. As a result, this type of terrorism is also known as computer terrorism. The computer infrastructure attacks or methods can be divided into three categories.

a. Physical Attack: The computer infrastructure is effected using traditional methods such as bombs, fire, and so on.

b. Syntactic Attack: The computer infrastructure is harmed by altering the system's logic in order to produce delay or make the system unpredictable. In this type of attack, computer viruses and trojans are used. In this type of attack, computer viruses and trojans are used.

c. Semantic Attack: This is more damaging because it exploits the user's trust in the system. During this attack, the information entered into the system while entering and using it is modified without the user's knowledge.

Tripwire, a research community, published an article titled "Where are your cyber attacks coming from?" in Verizon's DBIR 2015. They explain the five most common cyber attack attack patterns in 2014. The year of the attacks was 2015. They explain the five most common cyber attack attack patterns in 2014. The attack types were as follows:

- Web Application: According to the authors of DBIR 2015, organised crime has become the most commonly seen actor behind web application attacks.
- Privilege Misuse: These attacks are carried out for monetary gain.
- Cyber espionage: This had the greatest impact on the manufacturing, public, and professional sectors.
- Crimeware
- POS (Point of Sale)

TOOLS OF ATTACK

Cyber terrorists employ specific tools and methods to usher in this new era of terrorism. The attack tools are hacking is the most common method used by terrorists. It is a catch-all term for any type of unauthorised computer access. Hacking is associated with packet snipping, tempest attacks, password cracking, and so on.

Trozans: Programs that pretend to do one thing but are actually designed to do something else, such as the wooden trozan horse from the 12th century BC.
Emails: Viruses and warms attach themselves to a host programme in order to be injected. Emails are used to disseminate misinformation, threats, and defamatory material.

A computer virus is a type of malicious software programme ("malware") that, when executed, replicates itself (by copying its own source code) or infects other computer programmes by modifying them. The computer warm is a computer term that refers to a self-contained programming or a set of programmes that are capable of spreading functional copies of themselves.

HOW INDIAN NATIONAL SECURITY IS AFFECTED BY CYBER TERRORISM AND CYBER ATTACKS

In terms of e-governance, India began to use I.T. in many government entities such as I. Tax, Passport Service, Bank, Visa, and so on. Police and the judiciary are next in line. This is also heavily used in the travel industry. This sector's complete computerization has also introduced the concept of e-commerce. These are highly lucrative targets for wreaking havoc on the country and paralysing the financial and economic institutions. In terms of e-governance, information technology is used in many public sectors such as Income Tax, Passport Service, Bank, Visa, and so on. Police and the judiciary are next in line.

This is also heavily used in the travel industry. This sector's complete computerization has also introduced the concept of ecommerce. These are highly lucrative targets for wreaking havoc on the country and paralysing the financial and economic institutions.

The DRDO suspected Chinese hackers of breaching the computer system of India's top military organisations in March 2013. Following that, India's defence minister at the time, A.K. Antony, demanded proof of the incident, despite an official statement denying any sensitive files had been compromised.

While the threat of cyber attacks remains "imminent," as according to Supreme Court lawyer and renowned cyber law expert Pavan Duggal, the nation needs an institutionalist framework of the cyber army to handle the threat. He also stated that cyber warfare is not covered by Indian cyber laws.

Over the last few years, India has seen an increase in the number of cyber attacks on government departments. The DRDO also validated that some Algerian hackers attacked the websites of the DRDO, the PMO, and other government agencies. According to CERT-in, a government mandated information technology security organisation, 14392 websites in the nation were hacked in 2012. A report stated that 14232 websites were hacked in 2011, while 9180 websites were hacked in 2009 and 16126 in 2010.

According to Rikshit Tandon, consultant for the IAMAI and consultant to the UP police's cyber crime unit, cyber terrorism is a serious threat not only for India but also to the rest of the world. According to the report, approximately 90119369 Indian websites were hacked between 2012 and 2021. The majority of them were government offices, the defence sector, diplomatic missions, railways, BSNL, TRAI, CBI, and so on.

According to the EC Council report, there is a talent crisis in Indian information security, which has revealed major gaps in the current skill situation concerning IT security, which can impact the handling of cyber threats in industries such as banking, defence, healthcare, information technology, energy, and so on. The EC also revealed that approximately 75% of the participants demonstrated a low level or a lack of skill in error checking, displaying a vulnerability known to lead to the disclosure of confidential data and denial of service attacks. Along with cyber crime, Indian home minister Rajnath Singh described cyber terrorism as one of the most serious threats to society. Addressing the 2019 batch of IPS officers trainees who had come to meet him. At the time, Singh stated that cyber crime has become a challenge that the police are currently dealing with. In his language, cybercrime in the cyber world can be multifaceted, multi-locational, multilingual, multicultural, and multi-legal, making it difficult to scrutinise and apprehend the criminal. He also stated that the officers must also work hard to solve the people's problems. The home minister also urged officers to achieve higher levels of excellence and professionalism by process of consolidation aspects of intelligence, surveillance, communications, and modern policing.

In Indian Express, it was stated that "currency banned effect" between December 9-16, 2016 at least 80000 cyber attacks aimed to Indian networks, showing that "why the current regime attempt to switch over to a digital economy". According

to top intelligence sources, they observed an average of 2 lacs threats and vulnerabilities per day until November 28, 2016, these grew to five lacs following the note ban.

Banking sector threats are increasing, so a 360-degree security audit of information infrastructure, including financial networks, was ordered. An intelligence note on mobile phone vulnerabilities was once reviewed by Indian Express. Banking sector threats are increasing, so a 360-degree security audit of information infrastructure, including financial networks, was ordered. An intelligence note on mobile phone vulnerabilities was once reviewed by Indian Express.(17) According to sources, between November 22 and November 26, 2019, we observed 335000 attacks on Indian networks by hackers from China, Pakistan, Singapore, the USA, Russia, Romania, Ukraine, Dubai, and Sweden. In the largest cyber attack on the Indian banking system to date, 3200000 debit cards authorised by SBI, HDFC bank, ICICI bank, AXIS bank, and Yes bank were compromised in October 2019.

EXISTING CYBER SECURITY INITIATIVE

India used its security programme to combat cybercrime and cyberterrorism. Some organisations affiliated with the Police, I.B. DEPARTMENT, began to collect information from all over the world. Here are a few examples:

NIC (National Information Centre): It is a non-profit organisation that provides network backbone and e-governance assistance to the Central Government, State Governments, Indian territories, districts, and governmental bodies.

CERT-IN (Indian Computer Emergency Response Team): It is the most important organisation among the cyber community initiative groups in India. Its mandate states that it is responsible for ensuring the security of a country's cyberspace by improving security communication and information infrastructure.

The National Information Security Assurance Program (NISAP) is designed for the government and critical infrastructures. This government organisation implemented security policies and established a point of contact for the government and critical infrastructure. CERT-IN established this governmental organisation.

NASSCOM (National Association Of Software And Services Companies): The NASSCOM is a trade association for the Indian IT and business process outsourcing (BPO) industries. NASSCOM is a non-profit organisation that was founded in 1988. NASSCOM's role has primarily been related to software services or

BPO services; it is an organisation that ensures service quality and intellectual property rights enforcement are properly implemented in the Indian software and BPO industries.

REFERENCES

1. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
2. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
3. Hower, Sara; Uradnik, Kathleen (2011). Cyberterrorism (1st ed.). Santa Barbara, CA: Greenwood. pp. 140–149 2016.
4. Saikat Datta, Internet Democracy Project, Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents, (January 2016) available at https://internetdemocracy.in/reports/
5. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
6. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
7. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
8. Hower, Sara; Uradnik, Kathleen (2011). Cyberterrorism (1st ed.). Santa Barbara, CA: Greenwood. pp. 140–149 2016.
9. Matusitz, Jonathan (April 2005). "Cyberterrorism:". American Foreign Policy Interests. 2: 137–147.
10. "Latest viruses could mean „end of world as we know it,“ says man who discovered Flame", The Times of Israel, June 6, 2012
11. Harper, Jim. "There's no such thing as cyber terrorism". RT. Retrieved 5 November 2012.
12. Cyber terrorism National Conference of State Legislatures. https://cyberterrorism, as accessed on 08th November, 2019