LEGALFOXES LAW TIMES

CYBER TERRORISM 'AN EMERGING THREAT

By Vaishnavi Roy and Abhimanyu Singh

INTRODUCTION

"Just as a modern thief can steal more with a computer than with a bag, tomorrow's terrorist may be able to cause more damage with a computer mouse than with a bullet or a bomb." – National Research Council

1. Statements and Problems

With the help of digital technology, everyone has a space. Cyberspace, which offers a separate area for their activities, is this area. Almost all aspects of everyday life, including communication, business, advertising, banking, education, research, and entertainment, include the usage of the internet. Virtually no activity is unaffected by the internet. Since decades, the majority of computer users have been misusing the technology for either their own or others' gain.[1] In 1995, Sussman and Heuston initially suggested the phrase "cyber crime." Cybercrime is best understood as a group of activities or conducts; there is no one term that adequately captures it. These actions are based on the tangible offence item that has an impact on computer systems or data. It cannot be denied that internet technology has given a new speed to the development. At the same time law enforcement agencies started their task but failed and frustrated because of the peculiarity or the nature of the cyber terrorism. They found themselves unable to adhere with the fast growing technology. On the other hand, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world's public and private networks. Additionally, law enforcement

[1] Dewangan, M. (2020, October 1). A review on Cyber Crime and Cyber Law's. *International Journal of Technology*. https://ijtonline.com/HTML_Papers/International%20Journal%20of%20Technology__PID__2020-10-1-8.html

officers and investigative organisations use the same methods for gathering, scrutinising, and assessing the evidence in cases of traditional crimes as they do when looking into cybercrimes.[2]

Cyberterrorism is the act of spreading fear online. It entails manipulating people's minds in order to advance violence or cause harm to the public or property. Typically, it is done to advance a group's political or social goals. It is the act of introducing terror into cyberspace. It entails influencing people's thoughts in order to advance violence or cause harm to the public or property. In general, it is carried out to further a group's political or social goal.

Since cyber terrorism is not just an issue for India. The nations have also established own laws and statues. Different nations have their own internal cyber laws, however the issue is that the majority of books only discuss the rules of certain countries. The goal of this research is to provide a comprehensive overview of cyber terrorism, including its scope and character, as well as provide insight into those who are behind it. This research project will also take a wide picture of the efforts being made by governments in India and other countries to halt these crimes and will thoroughly examine their successes and failures. Additionally, a concerted effort will be made to carefully examine all of the aspects of the IT Act of 2000, including its flaws and potential solutions.

On the subject of cyber terrorism, the majority of publications on cyber law are mute. In this study, the researcher examined cases of cyberterrorism, essential infrastructure that is at risk of assault, and the laws and policies of several nations regarding cyberterrorism.

"*Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation*."

Section 66 f of the IT act 2000, According to the law, "Whoever commits or conspires to commit cyber terrorism shall be penalized with imprisonment which may amount to imprisonment for life." Cyberterrorism is the act of spreading fear online. It entails manipulating people's minds in order to advance violence or cause harm to the public or property. Typically, it is done to advance a group's political or social goals. It is the act of introducing terror into cyberspace. It

[2] "Cyber Thieves are Caught, But Conviction is Wobbly", Hindustan Times, August 9, 2006, p. 18.

entails influencing people's thoughts in order to advance violence or cause harm to the public or property. In general, it is carried out to further a group's political or social goal.

Phishing, the use of malware, DoS attacks, and the dissemination of viruses are all examples of cyber terrorism that are used to get information that is not permitted to be used to encourage violence or cause harm to people or property. Typically, it is done to further a group's political or social goals.

Examples of cyber terrorism include:

1. The cyber conflict between Israel and Palestine: Israel and Palestine have both launched websites and email accounts that have been utilised by rival parties to further their political objectives. They allegedly spied on ordinary citizens. Israel and Iran have both been notably more outspoken about these assaults. For instance, the Israel National Cyber Directorate acknowledged a "cyber-breach attempt" of water command and control systems in April 2020.

2. ISIS: Recent ISIS activities include images and videos of terrorist acts. It encourages the spread of fear and belligerent rhetoric. Young minds are influenced to join the extremists and propagate terror.

2. Research Objective

- To comprehend the true scope and nature of the cybercrime problem and how it affects every aspect of prevention and correction.
- To research the judicial tendencies surrounding cyber terrorism both before and after the Information Technology Act of 2000 was passed.

3. Research Mythodology

It might be difficult to get the most recent and pertinent information on this recently established artificial world because the subject is still growing and new trends are appearing every day. As a result, this study uses document-based and analytical methodologies. The majority of the material was compiled from research journals, newspapers, magazines, weeklies, and fortnightly publications. Primary sources also included government studies, reports on different agreements or treaties, legislation, and case law, Information Technology Act 2000[3], Information Technology Act 2008[4], reports published by Cyber security authorities[5], etc.

CYBER TERRORISM

"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."

"Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."

- Defense analyst Dorothy Denning

1. DEFINING CYBER TERRORISM

Even while cyber criminologists, cyber law experts, and social science researchers have given the topic of cyber terrorism a great deal of attention, very few studies have been conducted to examine the legal difficulties associated with cyber terrorism in India. The four primary perspectives from which the subject of cyber terrorism has been examined globally are as follows: the missions associated with cyber terrorism; [6], the methods that are followed for

[3] https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2

[4] https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf

[5] https://www.meity.gov.in/cyber-security-division

[6] Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing.

achieving the ultimate purpose of cyber terrorism[7,8], the results of cyber terrorism[9] and the role of laws in combating cyber terrorism[10].

The majority of these studies have demonstrated that terrorist groups use cyberspace for three distinct purposes: to publicise the danger, to learn as much as possible about the target government and its property, and in certain cases to "recruit" new forces.[11] It would be incorrect to think that cyber terrorism is a new form of cybercrime because several studies have shown that the activity encompasses two primary sorts of activities: cybercrime and misuse of information technology.[12] It may be important to emphasise that cyber terrorism involves a variety of cybercrimes, including denial-of-service attacks and identity theft.[13] In addition, when actual terrorist conduct has occurred, radicals may leave a digital trace.[14] The challenge is how the police, the legal system, and the justice system battle this widespread misuse of technology in the cause of jihad. This obviously includes visiting websites and sending emails. Security professionals and law enforcement may not be able to find the troublemaker due to a lack of adequate infrastructure and simple ways to destroy evidence.[15]

Additionally, several research have revealed that prior to 9/11, requests from extremist organisations to the government were more commonly connected with cyber terrorism than with jihad.[16] Since 9/11, the phrase "cyber terrorism" has mostly been used to refer to the cyberwar that has broken out between Muslim extremists and the government, particularly the US and

[7] Ibid.

[8] Wykes, M. & Harcus, D. (2010). Cyber-terror: construction, criminalisation and control. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 214 - 229). Cullumpton: Willan Publishing.

[9] Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing.

[10] Trachtman, J. P. (2009). Global Cyberterrorism, Jurisdiction, and International Organization. In M. F. Grady & F. Parisi (Eds.), The Law and Economics of Cybersecurity (pp. 259 - 296). New York: Cambridge.

[11] Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing.

[12] Schjolberg, S. (2007) Terrorism in Cyberspace - Myth or reality? Available At : http://www.cybercrimelaw.net/documents/Cyberterrorism.pdf

[13] Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing.

[14] Wykes, M. & Harcus, D. (2010). Cyber-terror: construction, criminalisation and control. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 214 - 229). Cullumpton: Willan Publishing.

[15] Jewkes, Y. (2010). Public Policing and Internet crime. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 525 - 545). Cullumpton: Willan Publishing.

[16] Denning, D. E. (2010). Terror's Web: How the Internet is transforming Terrorism. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 194 - 213). Cullumpton: Willan Publishing.

those countries that support US policies, laws, and regulations.[17] There have been several attempts to define the word "cyber terrorism."

The US National Infrastructure Protection Center (2001) defined cyber terrorism as a criminal act committed through the use of computers and telecommunications that results in violence, destruction, and/or disruption of services with the intention of instilling fear among a target population and causing them to act in accordance with a specific political, social, or ideological agenda.[18]

The term has also been defined by the International Handbook on Critical Information Infrastructure Protection (CIIP) 2006 Vol. II, as “attacks or series of attacks on critical information carried out by terrorists and instills fear by effects that are disruptive or destructive and has a political , religious and ideological motivation”[19].

Because of this, the EU convention on cybercrimes, which was established in 2001, established strategic roles for the member states to play in situations of illegal exploitation of cyberspace.[20] It has been noted that domestic courts play a significant role in countering cyber terrorism since cyber terrorism comprises criminal misbehaviour and trespass in the internet realm.[21]

The National Infrastructure Protection Center (NIPC)[22] defines cyber terrorism as “a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.”

The National Conference of State Legislatures[23], a group of lawmakers established to assist decision-makers with matters including the economy and homeland security Cyberterrorism is

[17] Wykes, M. & Harcus, D. (2010). Cyber-terror: construction, criminalisation and control. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 214 - 229). Cullumpton: Willan Publishing.

[18] Denning, D. E. (2010). Terror’s Web: How the Internet is transforming Terrorism. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (p. 198). Cullumpton: Willan Publishing.

[19] Schjolberg, S. (2007) Terrorism in Cyberspace - Myth or reality? (p.2) Available at: http://www.cybercrimelaw.net/documents/Cyberterrorism.pdf

[20] See chapter III, Article 23-35 of the EU Convention on Cyber Crimes, 2001.

[21] Schjolberg, S. (2007) Terrorism in Cyberspace - Myth or reality? Retrieved on 12.08.2011 from http://www.cybercrimelaw.net/documents/Cyberterrorism.pdf

[22] Formerly a unit of the Federal Bureau of Investigation, the National Infrastructure Protection Center (NIPC) moved to the Department of Homeland Security (DHS) when the latter began its functions in March 2003. NIPC is charged with assessing threats to critical infrastructure—particularly computer systems—and providing warnings concerning threats and vulnerabilities. It also conducts investigations and provides a response to computer attacks.

defined as: The use of information technology by terrorist groups and individuals to further their agenda, including the organisation and carrying out of attacks against networks, computer systems, and telecommunications infrastructures, as well as the electronic exchange of information and threat-making. Examples include gaining access to computer systems by hacking, infecting weak networks with viruses, defacing websites, engaging in Denial-of-Service assaults, or making terrorist threats via electronic communication.

In law, the closest definition is found in the U.S. Patriot Act 18 U.S.C. 2332b's definition of "acts of terrorism transcending national boundaries" and reference to activities and damages defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. Interestingly, the CFA's discussion of the "punishment for an offense" entails fines or imprisonment and suggests that it is a criminal act as opposed to an act of terrorism.[24]

2. CONCEPT OF CYBER TERRORISM

Various security organizations view cyberterrorism and the parties involved differently. The U.S. Federal Bureau of Investigation (FBI) defines cyberterrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs and data, which results in violence against noncombatant targets by subnational groups or clandestine agents."[25]

When Internet usage was quickly rising and discussions about the "information society" were in full force in the early 1990s, the concept of cyber-terrorism first emerged. Numerous studies were done at the time on potential risks to the United States, which was largely relied on high tech at the time and becoming more and more networked. Cyberterrorism may not pose a

[23] The National Conference of State Legislatures (NCSL) is a bipartisan non-governmental organisation (NGO) established in 1975 to serve the members and staff of state legislatures of the United States (states, commonwealths, and territories). NCSL has three objectives: to improve the quality and effectiveness of state legislatures; to promote policy innovation and communication among state legislatures; and to ensure state legislatures a strong, cohesive voice in the federal system. All state legislators and staff members are automatically members of NCSL. Available at: https://en.wikipedia.org/wiki/National_Conference_of_State_Legislatures.

[24] Cybersecurity and Cyber Terrorism | Fairleigh Dickinson University Online. (n.d.). In *Fairleigh Dickinson University Online*. https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/

[25] What is cyberterrorism? (2022, January 1). In *Security*. https://www.techtarget.com/searchsecurity/definition/cyberterrorism

physical threat, but its psychological effects on weaker societies can be just as harmful as terrorist bombs.[26] According to former US President Barack Obama, the cyber threat is one of the most significant economic and national security concerns that a nation currently faces.[27]

Midway through the 1980s, Barry C. Collin, a senior research fellow of the California-based Institute for Security and Intelligence [28], first coined the term "cyber terrorism". Collin's definition of cyber terrorism at the time was simply "the intersection of cybernetics and terrorism"[29]. It is without a doubt a wide phrase. There are many challenges that must be overcome in order to define "cyberterrorism" precisely and consistently. The majority of the conversation about cyberterrorism has taken place in the mainstream media, where writers are more interested in the drama and controversy than in giving the recently coined phrases a consistent and useful meaning. Additionally, adding "cyber," "computer," or "information" to existing words has become a frequent practise among those who utilise computers. In order to describe what some political strategists refer to as the "new terrorism" of our times, a variety of terms, such as cyberterrorism, cybercrime, cyber-tactics, cyberattack, and cyber-break-ins, are employed.[30]

There are difficulties in categorizing attacks, according to the CRS(Cyber Range Solution), For instance, Sony experienced a cyberattack in 2014 that disabled systems, destroyed data and released internal materials. Later that same year, warnings surfaced of terrorist attacks on theaters scheduled to show the film "The Interview," a fictional account of an interview with North Korea's Kim Jong Un. The threats caused theaters to cancel screenings, and Sony canceled its widespread release. The FBI and the Director of National Intelligence attributed the Sony

[26] Weimann, G. (2004). Cyberterrorism: How real is the threat? (Vol. 119). United States Institute of Peace.
[27] Obama, B. (2009, May 29). Remarks by the President on Securing Our Nation's Cyber Infrastructure | whitehouse.gov. Whitehouse.Gov; obamawhitehouse.archives.gov. https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

[28] Akhgar, B., Staniforth, A., & Bosco, F. (2014, July 14). Cyber Crime and Cyber Terrorism Investigator's Handbook - 1st Edition. Cyber Crime and Cyber Terrorism Investigator's Handbook - 1st Edition; www.elsevier.com.https://www.elsevier.com/books/cyber-crime-and-cyber-terrorism-investigators-handbook/akhgar/978-0-12-800743-3

[29] Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. Computers & Security, 102, 102145.
[30] Alık, N. A. H. A. (2022). Emerging Cyber Security Threats: India's Concerns and Options. International Journal of Politics and Security, 4(1), 170-200.

attacks to the North Korean government, and then-President Barack Obama promised to respond to North Korea’s alleged cyber assault, “in a place, time and manner of our choosing.”

These events raised plenty of questions. Was the cyberattack on Sony, though it is a private corporation with headquarters in Japan, an attack on the United States? Was it a terrorist act, a use of force or a cybercrime? Some questioned the extent of the response to which Obama eluded and who would be on its receiving end. Another potential policy question is under what circumstance the United States would commit troops in response to a cyberattack.

The National Cybersecurity and Communications Integration Center (NCCIC), which is under the Department of Homeland Security (DHS), developed the NCCIC Cyber Incident Scoring System (NCISS) to estimate the risk opens in new window of an incident. The NCISS looks at the risk severity and incident priority from a nationwide perspective, which can help with various cyber threats and cyber terrorism.[31]

Methods used for cyberterrorism

The intention of cyberterrorist groups is to cause mass chaos, disrupt critical infrastructure, support political activism or hacktivism, or inflict physical damage and even loss of life. Cyberterrorism actors use various methods. These include the following types of attacks:

- Advanced persistent threat (APT) attacks use sophisticated and concentrated penetration methods to gain network access. Once inside the network, the attackers stay undetected for a period of time with the intention of stealing data. Organizations with high-value information, such as national defense, manufacturing and the financial industry, are typical targets for APT attacks.
- Computer viruses, worms and malware target IT control systems. They are used to attack utilities, transportation systems, power grids, critical infrastructure and military systems.
- DoS (Denial-of-Service) attacks attempt to prevent legitimate users from accessing targeted computer systems, devices or other computer network These attackers often go after critical infrastructure and governments.

[31] Cybersecurity and Cyber Terrorism | Fairleigh Dickinson University Online. (n.d.). In *Fairleigh Dickinson University Online*. https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/

- Hacking, or gaining unauthorized access, seeks to steal critical data from institutions, governments and businesses.
- Ransomware, a type of malware, holds data or information systems hostage until the victim pays the ransom. Some ransomware attacks also exfiltrate data.
- Phishing attacks attempt to collect information through a target's email, using that information to access systems or steal the victim's identity.[32]

Involvement of cyber terrorism in 9/11 attack: Al Qaeda tracked and planned actions through cyberspace to carry out their objective. Terrorists exploited the internet as a planning tool for their online activities. Cyber planning is the digital coordination of a plan across geographic borders. There are several locations that have supposedly had ties to Al Qaeda. Cyber planning components were included on several websites. Utilizing the gaps in the nation's cyber legislation is a part of cyber strategy.

3. DISTINCTION BETWEEN CYBERCRIME, CYBER TERRORISM AND CYBER WARFARE

Cyberterrorism essentially consists of using computer technology to engage in terrorism. Since “crime” and “terrorism” are similar in certain respects, and since both target societies’ ability to maintain internal order, we must begin by differentiating the two.

Basically, crime is “personal” while terrorism is “political.” Crimes are committed for individual, personal reasons, the most important of which are personal gain and the desire (need) to harm others psychologically and/or physically.

Terrorism often results in the infliction of “harms” indistinguishable from those caused by crime (e.g., death, personal injury, property destruction), but the “harms” are inflicted for very different reasons. A U.S. statute, for example, defines “terrorism” as (i) committing acts constituting “crimes” under the law of any country (ii) to intimidate or coerce a civilian population, to

[32] What is cyberterrorism? (2022, January 1). In *Security*. https://www.techtarget.com/searchsecurity/definition/cyberterrorism

influence government policy by intimidation or coercion or to affect the conduct of government by mass destruction, assassination or kidnapping[33].[34]

In the fall of 2006, the U.S. Air Force announced a new mission statement in which it pledges to "fight in Air, Space and Cyberspace." [35]The new mission statement recognizes what has been apparent for some time : warfare can and will migrate into cyberspace. "Cyberwarfare" constitutes the conduct of military operations by virtual means. [36]It consists of nation-states' using cyberspace to achieve the same general ends they pursue through the use of conventional military force, i.e., to achieve certain advantages over a competing nation-state or to prevent a competing nation-state from achieving advantages over them. [37][38]

However, the approach does not wholly disregard laws controlling battle. They are, at the very least, pertinent to the requirement to separate cyberwarfare from cybercrime and cyberterrorism inasmuch as they have an influence on it. In the part after this one, we'll return to this subject and examine how and why it might be challenging to distinguish between the three.

Both cyberterrorism and cybercrime are illegal activities carried out online. But there is a distinction between the two. The distinction relates to the reasons why cyberattacks are conducted. Cybercrime is an illegal or criminal conduct when a computer is either a tool or the victim (133)[39] or a target (or both)(134).[40] It is a relatively recent topic of criminological research that originates in the field of criminal justice and it includes computer-related crime and

[33] 18 United States Code § 2331(1).

[34] Cybercrime, cyberterrorism and cyberwarfare. (n.d.). In *https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm*.

[35] *Cyberspace as a Domain In which the Air Force Flies and Fights. (2006, November 2). In Air Force. https://https%3A%2F%2Fwww.af.mil%2FAbout-Us%2FSpeeches-Archive%2FDisplay%2FArticle%2F143968%2Fcyberspace-as-a-domain-in-which-the-air-force-flies-and-fights%2F*

[36] Steven A. Hildreth, *Cyberwarfare*, Congressional Research Service (June 19,2001), http :// www. fas. org/ irp/ crs/ RL30735. pdf.

[37] war. (n.d.). In *https://en.wikipedia.org/wiki/War*.

[38] Cybercrime, cyberterrorism and cyberwarfare. (n.d.). In *https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm#no32*.

[39] Some of the basic weapons of cyber terrorists include Viruses, Trojan Horses, Logic Bombs, Worms, DoS Attack, Zombie, Vampire.

[40] P. Britt, Ethical hackers: Testing the security waters. Information Today, 22(8), 2005, pp. 1-28. BADLO

cybercrimes (135).[41] However, cyberterrorism refers to the intentional deployment of disruptive cyberweapons or the threat of such use in cyberspace. Every act of cyberterrorism is motivated by one or more social, intellectual, religious, political, or other comparable purposes. In order to achieve their goals, cyberterrorists may also want to intimidate individuals or groups (136).[42] It is essential to remember the definition of "premeditation" in this context. An act of cyberterrorism is always planned beforehand. However, a criminal conduct might be classified as cybercrime even if it is not planned ahead of time. In layman's terms, cybercrime and cyberterrorism are two different species. Cyberwarfare is what is used when a State declares cyberwar on another political sovereign. Here, state apparatuses are utilised to carry out unauthorised entry or malware distribution into the computer networks and computer systems of the adversary nation. In contrast to cybercrimes and cyberterrorism, which involve individuals and terrorist groups, respectively, cyberwarfare involves the State apparatus of two or more governments.

EMERGING TRENDS AND CASES

1. ***Mumbai terrorist attacks of 2008,*** [43]

“Multiple terrorist attacks that occurred on November 26–29, 2008, in Mumbai (Bombay), Maharashtra, India.”

Regarding cyberterrorism, India is no longer naive.[44] On April 2, 2002, the Pakistani Anti India Crew (AIC) broke into 88 Indian websites and made an effort to delete and destroy all the data on the computer systems and computer networks of those websites.[45] such as the websites maintained by the Indian Government.[46]

[41] D.Wall, Crime and the Internet. Routledge, London, 2001. BADLO

[42] J.F. Dunnigan, The Next War Zone: Confronting the Global Threat of Cyberterrorism, Citadel Press, New York, 2003. BADLO

[43] MOHAMMED AJMAL MOHAMMAD AMIR KASAB @ ABU MUJAHID v. STATE OF MAHARASHTRA [2012] 8 S.C.R. 295

[44] India Risk Survey - 2018.pdf. (n.d.). In *https://ficci.in/SEDocument/20450/India%20Risk%20Survey%20-%202018.pdf*.

[45] Saxena, A. (2011) 117 Indian Government Websites Defaced Till July, Medianama [Online] Available from: https://www.medianama.com/2011/08/223-indiangovernment-websites-hacked/

The horrific 26/11 Mumbai attack serves as a vivid example of how terrorists' use of ICT (information and communication technology) made it difficult for Indian security forces to locate and capture these offenders. In the July 13, 2010, Zaveri blast, the ICT was utilized improperly. The 2010 Varanasi bombing also involved the use of ICT for communication; the Indian Mujahidin claimed responsibility for the explosion via email, which was connected to WIFI in Vashi, Navi Mumbai. The 2010 bombing in the holy city of Varanasi also featured cyberterrorism remnants, as did the 2008 attack on the Mumbai Taj Hotel, which is now infamously known as 26/11. (NDTV Correspondent, 2010). Ironically, Muslim jihadists like the Indian Mujahiddin were engaged in the majority of these incidents. However, a review of news articles on the excessive use of cyberspace would reveal that non-Muslim adolescents had also been involved in disseminating terror messages that targeted state leaders or claimed responsibility for terrorist actions. All of these incidents point to two fundamental characteristics of cyber terrorism, namely the collecting of intelligence and the dissemination of fear through cyberspace in order to undermine peace and security on a national level. The Information Technology Act 2000, which has particular rules for combatting cyber terrorism, had a series of suggested revisions that the Indian government had put into force following the 26/11 incident. The section 66F clause addresses cyberterrorism in the broadest possible sense.[47]

This clause specifies the punishment that will be meted out to cyberterrorism perpetrators. The aforementioned law clause conspicuously lacks a definition of the word "cyber terrorism." The Indian government has furthermore suggested a series of Rules in 2011 to reinforce the legislation against cyberterrorism,[48] this should make the slack loops tighter.

[46] Bhansali, S. (2012) Commentary on Information Technology Act, 1st Ed., New Delhi: Universal Publication.
[47] The definition can be found in Section 69F of the Information Technology Act, 2000 (amended in 2008). The definition will be analyzed in later parts of this chapter.
[48] These rules could be found at http://www.mit.gov.in/sites/upload_files/dit/files/RNUS_CyberLaw_15 411.pdf

2. 2019 Pulwama attack

“The 2019 Pulwama incident took place on February 14, 2019, when a vehicle-borne suicide bomber struck a convoy of cars transporting Indian security personnel on the Jammu-Srinagar National Highway near Lethapora in the Pulwama district of the former state of Jammu and Kashmir.”

The Jaish E Mohammad suicide bomber in the Pulwama tragedy on February 14, 2019, used virtual SIM cards.[49] In the end, cyberspace served as a terrorists' base of operations and a battleground. The terrorist organisation sees cyberattacks as a powerful Islamist weapon for fighting their enemies. Terrorist organisations have gotten good at taking use of the internet.[50]

Videos of talks, pamphlets, and social media posts made using Pakistani phone numbers on Facebook, WhatsApp, and Telegram are all part of the evidence gathered by India. At a 2018 address, Mufti Asghar promises to transform Pulwama into Talhawama by exacting bloody retribution for the murder of his family members in Balakot, the Jaish terror hub attacked by Indian Air Force planes on February 26.

The material also contains an audio message from Masood Azhar on February 5 in which he urged Kashmiri Muslims to come together and promised success within a month if they did.

The evidence also demonstrates that Pakistani intelligence agents called CRPF offices, hospitals, police control centres, and villagers using fictitious names in order to learn about fatalities and the movement of Indian soldiers following the attack. The idea that the strike was carried out by a disgruntled local Kashmiri and was a result of widespread discontent in the Valley was spread using these specifics. The attack on the Pathankot airfield on January 2, 2016, and the one on the Indian embassy in Mazar-e-Sharif, Afghanistan, are two more well-known and earlier JeM incidents that India has also released brief details about. All four terrorists involved in the Pathankot assault were in contact with Pakistani phone lines, with one of those numbers, +92321312786, actually being connected to the JeM's Bahawalpur, Pakistani Punjab,

[49] Press Trust of India, 2019

[50] Dhar, P. (2017) Changing dimensions of criminal jurispudence in virtual reality: a critical evaluation of information technology laws, ‘cybercrimes and crimes per se’ in India, Bharati Law Review, 6(2), pp: 117–130

headquarters. Shahid Latif and Kashif Shahid Latif were the two JeM handlers of the Pathankot airbase terrorists; both were freed by India in 2010 after serving 16 years in prison on terrorism-related charges.[51]

LEGAL MEASURSES

Here are the current cybersecurity laws in operation in India right now:

1. **The Information Technology Act, 2000**[52]

The Information Technology Act of 2000 was India's first significant cybersecurity law. The Indian Computer Emergency Response Team (CERT-In) is responsible for enforcing the IT Act of 2000, which was passed by the Indian Parliament to direct cybersecurity laws, establish data protection standards, and control cybercrime. Along with many other things, it defends online banking, online shopping, and the private sector.

India employs the IT Act and several other sector-specific rules to promote cybersecurity standards, despite the lack of a single, exclusive cybersecurity law in the country. Additionally, it offers India's crucial information infrastructure a legal foundation. For instance, Section 43A of the IT Act mandates that Indian firms and organisations have "reasonable security processes and procedures" to guard against the compromise, damage, or exposure of sensitive information. Any intermediaries or individuals who release personal data without the owner's authorization (with

[51] Gupta. (2019, March 13). *Speeches, cyber trail in India’s Pulwama proof establish role of Jaish*. Hindustan Times. Retrieved February 8, 2023, from https://www.hindustantimes.com/india-news/speeches-cyber-trail-in-india-s-pulwama-proof/story-n1mmAHPrvHiSoj0n1mmM1I.html

[52] THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000). (n.d.). In *https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C*.

malicious intent and inflicting harm) are subject to up to a three-year jail sentence, a fine of up to Rs500,000, or both under Section 72A of the IT Act.[53]

The Act was created in order to address e-commerce and all the complexities associated with digital signatures, as well as to achieve the following goals :

- The purpose of the Act is to safeguard all electronic transactions.
- Paperwork utilised for communication has decreased as a result of e- commerce. Additionally, it provides legal protection for information sharing and communication conducted electronically.
- It safeguards the electronic signatures needed for any kind of legal authentication.
- It controls the authority of intermediaries to govern their operations.
- By defining numerous offences connected to citizen data privacy, it protects citizen data.
- It also controls and safeguards private information kept by social media and other online intermediaries.
- It recognises electronic books of accounts maintained in accordance with the 1934 Reserve Bank of India Act. [54]

2. **Information Technology (Amendment) Act 2008**[55]

The IT Act of 2000 was significantly expanded by the Information Technology Amendment Act of 2008 (IT Act 2008), which was approved in October 2008 and went into force the following year. The original measure, which initially failed to open the door for more IT-related growth,

[53] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

[54] Information Technology Act, 2000 - iPleaders. (2022, August 24). In *iPleaders*. https://blog.ipleaders.in/information-technology-act-2000/

[55] The Information Technology ACT, 2008. (n.d.). *Https://Police.Py.Gov.in/Information%20Technology%20Act%202000%20-%202008%20(Amendment).Pdf*.

was improved by these modifications. It was praised as a ground-breaking and eagerly anticipated move towards an enhanced cybersecurity framework in India. The IT Act of 2008 expanded the definition of cybercrime and the verification of electronic signatures by adding new phrases that were updated and reinterpreted for modern usage. Additionally, it holds businesses accountable for data breaches and actively pushes them to establish better data security measures. Any person, business, or organisation (intermediaries) using computer resources, computer networks, or other information technology in India is subject to the IT Act of 2008. Internet, network, and telecom service companies are also included. It also covers firms from outside the nation that operate in India as well as international institutions with a presence there.[56]

The IT Amendment Act, 2008 was approved by Parliament with the goal of containing the worsening condition affecting the IT sector. In order to guarantee that the IT Act remains dynamic, the current article summarises a few of the new or updated laws pertaining to Data Protection, Privacy, and Cyber Crime. It also attempts to analyse how successful these revisions will be. The Information Technology (Amendments) Act, 20081 ("ITA, 2008") clearly focuses on cyber terrorism and, to a significant extent, cybercrime, in contrast to the Information Technology Act, 2000 ("IT Act," which had a clear focus on the recognition of electronic records and the facilitation of E-Commerce. First, some background information: In 2005, the Ministry of Information Technology published a draught of proposed changes to the IT Act. After that, in 2006, the IT Bill was introduced with significant modifications as a result of widespread and unanimous objections to the 2005 amendment proposals. Many of the reforms outlined in the IT Bill of 2006 were included in the ITA, which was swiftly enacted by the parliament in December 2008. However, significant additions and revisions were made as a result of the recent wave of terrorist incidents.

This article's goal is to draw attention to a few of the new or updated regulations regarding data protection, privacy, and cybercrime. In addition to these clauses, the definition sections have undergone significant changes. These are only briefly mentioned here. In general, these changes

[56] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

seem to be made to guarantee that the IT Act is dynamic and to keep the requirements technologically agnostic.[57]

3. Information Technology Rules, 2011[58]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 are a key component of the cybersecurity laws under the IT Act (Privacy Rules).

The most notable changes include intermediary regulation, revised fines and punishments for cheating, defamation, and posting private photographs without consent, as well as speech censorship/restriction and cybercrime.

For the purpose of regulating how Indian companies and organisations process sensitive information, data protection, data retention, and gathering of personal data and other sensitive information, it is crucial to follow both the Information Technology Act (ITA) and the IT Rules. The laws governing other Indian industries, such as banking, insurance, telecommunications, and healthcare, also have regulations pertaining to data privacy.[59]

[57] M. (n.d.). Articles – Manupatra. In *Articles – Manupatra*. https://articles.manupatra.com/article-details/Information-Technology-amendment-Act-2008-An-Overview

[58] MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY. (n.d.). In *https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf*.

[59] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

4. Indian SPDI Rules, 2011 for Reasonable Security Practices[60]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (hence, "The SPDI Rules") were adopted by the Central Government to comply with the IT Act's data protection obligations. There are provisions to regulate in the SPDI Rules:

a. Processing of Sensitive Personal Data/Information or Personal Data/Information that is Personal

b. Establishing security standards and guidelines for the management of sensitive personal data and/or personal data with regard to individuals.

Personal information, according to the SPDI Rules, is “any information relating to a natural person, which, either directly or indirectly, in conjunction with other information accessible or expected to be available with a body corporate, is capable of identifying such person.”[61]

“Further, Sensitive Personal Data or Information has been defined as personal information which consists of information relating to[62]:

a. Password

b. Financial information

c. Physical, physiological and mental health conditions

d. Sexual orientation

e. Medical records and history

f. Biometric information”

[60] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. (n.d.). In *https://cis-india.org/internet-governance/files/it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.pdf*.

[61] Rule 2(1)(i), SPDI Rules, 2011.

[62] Rule 3, SPDI Rules, 2011

It is pertinent to mention that although the SPDI Rules define “Personal Information”, the rules are majorly focused on protecting “Sensitive Personal Data or Information”.[63]

The Indian SPDI Rules, 2011, designate the IS/ISO/IEC 27001 norms as international standards. Since a result, Indian businesses are not required to follow these guidelines, but they are strongly encouraged to do so as they can assist them in adhering to the "reasonable security measures" required by Indian law.

Additionally, the regulations may grant people the ability to rectify their information and establish limitations on information dissemination, data transfer, and security measures. The authenticity of sensitive personal data (SPD) such as sexual orientation, medical records and history, biometric data, and passwords is not their responsibility because they only apply to corporate organizations.[64]

5. National Cyber Security Policy, 2013[65]

The National Cyber Security Policy 2013 was published in 2013 by the Department of Electronics and Information Technology (DeitY) as a security framework for public and commercial entities to better defend themselves against cyberattacks.

The National Cyber Security Policy's objective is to build more flexible rules that would better safeguard India's online environment. Through skill development and training, the strategy seeks to produce a workforce of more than 500,000 knowledgeable IT workers over the next five years.[66]

The National Cyber Security Policy briefly addresses the following topics:

[63] IT Act & SPDI Rules: Data Protection Regime of India. (2021, September 2). In *Tsaaro*. https://tsaaro.com/blogs/it-act-spdi-rules-data-protection-regime-of-india/

[64] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

[65] National Cyber Security Policy -2013. (n.d.). In *https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf*.

[66] Ibid.

- A vision and purpose statement that aims to create a resilient and secure cyberspace for individuals, organisations, and the government.
- Setting goals that will make the nation less vulnerable to cyberattacks, prevent cyberattacks and cybercrimes, reduce reaction and recovery times, and improve the investigation and prosecution of cybercrimes.
- Targeted government initiatives, public-private partnerships, technological measures connected to cyber security, protection of vital information infrastructure, national alerts and advise systems, awareness- and capacity-building initiatives, and promotion of information exchange and collaboration.
- Increasing coordination and collaboration between all domestic stakeholders.
- Plans and objectives that support the national cybersecurity mission and vision.
- A framework and projects that may be pursued by the government, sectors, and via public-private partnerships.
- Facilitating the tracking of significant national trends, such as those relating to the expansion of cyberinfrastructure, cyberattacks, and compliance with cyber security regulations.[67]

The NSCP's other goals include:

- Building a robust and secure online environment for people, businesses, and the government.
- Monitoring, protecting information and cyber infrastructure, minimising vulnerabilities, and bolstering defences against cyberattacks.
- Developing frameworks, capabilities, and vulnerability management techniques to lessen, prevent cyber events and threats more quickly, or to respond to them.
- Encourages businesses to create cybersecurity policies that are in line with their strategic objectives, operational procedures, and industry best practises.

[67] George, A. A. (2013, December 4). National Cyber Security Policy 2013 - In a nutshell. In *ClearIAS*. https://www.clearias.com/national-cyber-security-policy-2013/

- Establish institutional frameworks, personnel, workflows, technological advancements, and cooperative efforts simultaneously to lessen the harm caused by cybercrime.[68]

6. **IT Rules, 2021[69]**

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 were established by the Ministry of Electronics and Information Technology on February 25, 2021, to replace the IT Rules, 2011. A little over a year later, on June 6, 2022, the Indian MeitY (Ministry of Electronics and IT) announced the freshly revised proposed modifications to the IT Act in an effort to make it more effective and keep up with the difficulties of the rapidly evolving digital ecosystem.

The proposed revisions seek to provide regular users of digital platforms the option to file complaints, demand responsibility when their rights are violated, and impose greater due diligence on businesses. Additionally, IT Rules, 2021 establishes a distinction between less significant and more major social media intermediaries based on user counts and imposes significantly greater obligations on bigger social media intermediaries with regard to the security of personal data.[70]

Governments throughout the world are debating how to control social media intermediaries (SMIs). It is crucial for governments to update their regulatory framework to deal with new challenges given the complexity of the issue, the significance of SMIs in influencing public discourse, the impact of their governance on the freedom of speech and expression, the volume of information they host, and the ongoing technological advancements that affect it. India revised its ten-year-old SMI legislation in 2021 with the IT Rules, 2021, which were largely designed to impose requirements on SMIs to promote an open, safe, and trusted internet.

[68] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

[69] MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY. (n.d.). In *https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf*.

[70] Ibid.

Why did the IT Rules, 2021 need to be modified?

The declared goals of the revisions were threefold, according to the press release that came with the draught amendments in June 2022. The interests and constitutional rights of netizens needed to be protected, the Rules' grievance procedure needed to be strengthened, and early-stage Indian start-ups shouldn't be negatively impacted by compliance with these requirements. This resulted in a series of changes that may be generally divided into two groups. The first category comprised giving SMIs more responsibilities to ensure greater user interest protection, while the second type required establishing an appeals procedure for grievance redressal.[71]

7. **National Cyber Security Strategy, 2020**[72]

The Indian government's long-awaited follow-up plan to strengthen cybersecurity efforts was the National Cyber Security Strategy of 2020. The major objective of the strategy, which is currently in the drafting stage and is awaiting approval by the National Security Council Secretariat, is to act as official advice for stakeholders, policymakers, and business leaders in order to stop cyber incidents, cyberterrorism, and cyberespionage. In order for enterprises to perform better evaluations of their cybersecurity architecture and understanding, the plan strives to increase the quality of cybersecurity audits. Once the regulation is in place, it is hoped that cyber auditors would raise their security requirements, pushing businesses to strengthen their security initiatives.[73]

8. **KYC (Know Your Customer)**[74]

Businesses reported fraud-related losses resulting from account opening and account takeover in 57% of cases. It indicates that cyber dangers are gaining access to KYC procedures and that

[71] Explained | The amendments to the IT Rules, 2021. (2022, October 31). In *Explained | The amendments to the IT Rules, 2021 - The Hindu*. https://www.thehindu.com/sci-tech/technology/explained-the-amendments-to-the-it-rules-2021/article66079214.ece

[72] Data Security Council of India. (n.d.). In *https://www.dsci.in*.

[73] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

[74] Know your customer - Wikipedia. (2022, October 21). In *Know your customer - Wikipedia*. https://en.wikipedia.org/wiki/Know_your_customer

further security measures are necessary. Businesses currently provide safe KYC solutions for increased cybersecurity. Facial liveness solutions that employ artificial intelligence and machine learning technology to provide a failsafe verification procedure are assisting in preventing fraud. Prior until now, it was difficult to conduct face liveness tests without physical confirmation, but today, the same may be accomplished with a selfie or a brief video chat. Such technologies can be used by social media networks to stop cybersecurity scams.[75]

The RBI has required the usage of KYC (Know Your Customer) protocols as norms and practises worldwide (Reserve Bank of India). When it comes to better protecting against fraud and the theft of payment credentials, KYC refers to the tracking and monitoring of client data security. Every customer of banks, insurance firms, and other digital payment providers that conduct financial transactions must be verified and identified.

Businesses must implement the following cybersecurity measures for good KYC compliance and to satisfy financial regulatory requirements:

- Utilizing a knowledge-based quiz exam to confirm the identity of customers
- Using pre-screening KYC verification techniques, such as phone verification, reputational data, device ID intelligence, and others
- Using machine learning and AI to check papers and government-issued identification.
- Verifying a user's identification using biometrics such as fingerprinting and face recognition.

• Keeping track of clients in a database for verification reasons.

Businesses that have KYC policies reassure their consumers that their digital identities and financial transaction data are protected by the necessary compliance management and anti-fraud solutions. With the help of KYC Compliance, Indian businesses can handle payments safely and securely, abide by SEBI rules, and build client confidence.

[75] Kukatlapalli, S. (2022, May 13). Role of KYC in cybersecurity. In *Times of India Blog*. https://timesofindia.indiatimes.com/blogs/voices/role-of-kyc-in-cybersecurity/

Failure to follow the KYC guidelines might result in financial penalties of 2 lakh (200,000) rupees for banks, companies, and organisations.[76]

9. **Reserve Bank of India Act 2018**[77]

The RBI Act, which outlines cybersecurity policies and regulations for UCBs (urban cooperative banks) and payment operators, was implemented by the Reserve Bank of India in 2018.

The 2018 RBI Act seeks to:

- Establish guidelines to ensure that banks and payment providers' security frameworks are equalised in accordance with how they adopt new technologies and digitalization.
- Require banks to develop and submit their plans for handling cyber crises.
- Order banks to adopt corporate information security policies that successfully define cybersecurity readiness.
- Make it essential for banks to adopt breach notifications, whereby UCBs must swiftly identify and notify RBI of cybersecurity breaches within 2–6 hours of discovery in order to better defend against assaults.
- Encourage banks to arrange threat assessment audits on a regular basis.
- Assist banks with DMARC security measures and the implementation of their own email domains with anti-phishing and anti-malware technologies.

These rules must be adhered to by all Indian banks in order to standardise cybersecurity standards for payment processing and address the ever-growing business challenges in a digital world. In situations of non-compliance with their cybersecurity standards, banks and

[76] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

[77] RESERVE BANK OF INDIA ACT, 1934. (n.d.). In *https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RBIA1934170510.PDF*.

the financial industry are subject to fines under the RBI Act of 2018. The fines might reach 10 lakh rupees ($1,000,000).[78] The three main focuses of the RBI cyber security framework are: (1) Create a baseline for and build resilience in cyber security (2) Run a Cyber Security Operations Center (C-SOC) (3) Reporting Cybersecurity Incidents (CSIR).[79]

CONCLUSION

“The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.” Ban Ki-moon – Secretary General of the United Nations.

Section 66f of the IT act 2000, According to the law, "Whoever commits or conspires to commit cyber terrorism shall be penalized with imprisonment which may amount to imprisonment for life." Cyberterrorism is the act of spreading fear online. It entails manipulating people's minds in order to advance violence or cause harm to the public or property. Typically, it is done to advance a group's political or social goals. It is the act of introducing terror into cyberspace. It entails influencing people's thoughts in order to advance violence or cause harm to the public or property. In general, it is carried out to further a group's political or social goal.

Phishing, the use of malware, DoS attacks, and the dissemination of viruses are all examples of cyber terrorism that are used to get information that is not permitted to be used to encourage violence or cause harm to people or property. Typically, it is done to further a group's political or social goals.

It is tragic to note that despite the significant provisions and changes made by the government to combat cybercrime, India still lacks the effective cyber-security measures needed to combat the growing threat posed by cyberterrorism. As a result, India stands to be one of the major targets of cyberattacks and cyberterrorism. One of the biggest dangers facing all countries in the current

[78] chin. (2023, January 5). *Top Cybersecurity Regulations in India [Updated 2023] | UpGuard*. Top Cybersecurity Regulations in India [Updated 2023] | UpGuard. Retrieved February 9, 2023, from https://www.upguard.com/blog/cybersecurity-regulations-india

[79] D. (2023, January 2). RBI Cyber Security Framework in India - Cyber Security Services & Payment Security Services Company. In *Cyber Security Services & Payment Security Services Company*. https://valuementor.com/en-in/rbi-cyber-security-framework/

period is cyberterrorism. The terrorists' original intention of terrorising hundreds of people while murdering one person has altered over time, and they are progressively using more lethal weaponry. They think that by murdering an increasing number of people, they will win the pointless war. Their nature has changed to become more deadly, and they gain from the advancement of technology in civilization. They are promoting fear and anarchy by utilising contemporary technology. However, the State must proceed with great prudence. Care must be taken to guarantee that innocent people are not punished and their fundamental rights are not abused because all laws are reinforced by both the consent of the governed and the power of the State. Security issues and human rights considerations should coexist peacefully. Regulations and monitoring procedures must be in place in order to deter, identify, and track terrorists, but they must not infringe upon the rights and liberties of residents.