pISSN: 2454-7107, eISSN: 2455-4189

Indian Journal of Law and Human Behavior
Volume 5 Number 2 (Special Issue), May - August 2019
DOI: http://dx.doi.org/10.21088/ijlhb.2454.7107.5219.5

Original Article

Cyber Terrorism in India: A Physical Reality Orvirtual Myth

Shiv Raman[1], Nidhi Sharma[2]

Author Affiliation

[1,2]Assistant Professor, Amity University, Gurugram, Haryana 122413, India.

Corresponding Author

Nidhi Sharma, Assistant Professor, Amity University, Gurugram, Haryana 122413, India

E-mail: advocateshivraman2007@gmail.com

Abstract

Cyber terrorism is a global issue which is one of the most ignored & underestimated issue considered in India. India has the maximum internet users, called as 'Netizens' after USA and China. The over dependency over the internet increase the vulnerabilities & transformed their aggressions into feeling of revenge, which turned them criminals, Cyber warriors and hostility to the country. Most of the Indian citizens are insensitive towards cyber threats of being victimized of virtual world. The information technology has opened the ocean of opportunities to the world for development of their financial infrastructures. The Cyber crimes are increasing every moment. The netizens are ignorant and of state of mind that their activities are unnoticed. We generally share our significant & super sensitive data & information unintentionally on social media. The momentous growth of Cyber world posed the threats of Cyber terrorism. The Cyber attacks has tendency of depiction of lethal, non-lethal psychological well being, public confidence & political attitudes. Generally, it is to consider as Cyber terrorism affects only the national security system. But infect- it also affects their psyche & cognition. The Cyber terrorist expanded growth of Cyber attacks, which is dramatically increased in past few years. It has caused mass destruction & damage to nuclear facilities & critical command & control system. The Cyber experts are working to strengthen more and more capacity to restrain Cyber attacks over Govt. system, defence websites, financial and banking system and most important nuclear facilities.

Keywords: Cyber terrorism; Cyber crimes; Netizens.

How to cite this article:

Shiv Raman, Nidhi Sharma. Cyber Terrorism in India: A Physical Reality Orvirtual Myth. Indian J Law Hum Behav. 2019;5(2): 133–140.

Introduction

Cyber terrorism is a global issue which is one of the most ignored and underestimated issue considered in India. India has the maximum internet users, called as *'Netizens'* after USA and China. The over dependency over the internet increase the vulnerabilities and transformed their aggressions into feeling of revenge, which turned them criminals, Cyber warriors and hostility to the country. Most of the Indian citizens are insensitive towards cyber threats of being victimized of virtual world. The information technology has opened the ocean of opportunities to the world for development of their financial infrastructures. The Cyber crimes are increasing every moment. The netizens are ignorant and of state of mind that their activities are unnoticed. We generally share our significant and super sensitive data and information unintentionally on social media.

The momentous growth of Cyber world posed the threats of Cyber terrorism. The Cyber attacks

has tendency of depiction of lethal, non-lethal psychological well being, public confidence and political attitudes. Generally, it is to consider as Cyber terrorism affects only the national security system. But infect it also affects their psyche and cognition. The Cyber terrorist expanded growth of Cyber attacks, which is dramatically increased in past few years. It has caused mass destruction and damage to nuclear facilities and critical command and control system. The Cyber experts are working to strengthen more and more capacity to restrain Cyber attacks over Govt. system, defence websites, financial and banking system and most important nuclear facilities.

Cyber space is running in veins of modern digital system, business and other essential services. The Cyber security is one of important aspect, the failure of which turned in to battle field for Cyber attacks and Cyber terrorism. The Cyber crime or E- crimes are now become the reality of life which includes the various kinds and modes of Cyber crimes like website hacking, ID or password hacking, data theft or service denial to various systems. The industrial Cyber espionage is also factor responsible for the growth of 'Cyberattack' over others information system for the acquisition of *'higher sensitive data'*. The 'hostile actor' (Cyber terrorist) in order to control, manipulations and command to Cyber infrastructure, they using hacking, malware or ransomware programs and softwares to corrupt and destroy the digital information system that might be inclusive of strategic data, intellectual property rights and future development projects etc.

Meaning of Cyber Terrorism

The term Cyber terrorism- is composition of cyber terms *Cyber and terror*. The Cyber terrorism is needed to be understood with term 'terrorist'. Cyber terrorism was coined by Banny C. Collin of *Institute for Security and Intelligence (ISI)* in late 1980's. This concept originates only to resonate with general public, because countdown begun from year 2000 and the millennium buys associated with the big date switch, which gained wide scale recognitions. The terror attacks on September 11, 2001. Further thrust the concept of Cyber terror into public discourse, which threat of giant disruptions to economy, infrastructure and national security were often discussed in depth by the media.

Cyber terrorism is also named as- *electronic terrorism, electronic jihad, information warfare or Cyber warfare.* The basic objective of Cyber attack is hacking, generally to satisfy the ego of hackers of creating terror.

Sometimes it seems too similar or over lapping with each other like cyber attack and cyber terrorism. The objective of Cyber terrorism is to generate the feeling of terror in the mind of the Cyber victims. Cyber terrorism is also causing threat to most vulnerable point, which cover physical and virtual world. It includes commission of acts of destruction, alteration, acquisition and acts of transmission against the following:

- Defence forces
- Financial Infrastructure
- Civilians
- Destructions of supervisory control and data acquisition system of smart cities
- Exploration of smart army etc

Historical Flashback of Cyber Terrorism

The first quoted case of Cyber terrorist attack was of 1996. The Cyber terrorist was suspected as co-accused of 'White Supremacist Movement', He was alleged for temporary disablement of part of the ISP's (Internet service provider) record keeping system and 'Massachusetts Internet service provider'. The ISP had made efforts to restrain the hackers from spreading and sending racist massage worldwide. Finally, the attacker fleshes the message "*You have yet to see electric terrorism. This is a promise*", at signing-off the system. This was the first Cyber attack, which opened the doors of probabilities and possibilities of Cyber terrorism worldwide.

Cyber Terrorism, Myth or Reality

Cyber terrorism is a very terrifying term ever used for traditional crimes. If we consider the gravity of the terrorism and tools of cyber terror it seems to be similar in their sphere but not in reality. Cyber terror tools seem to be similar with cyber attacks. An 'e-bomb' is really terrorism or is it just hacking? It might be matter of debate. Computer system's hacking in not a new phenomenon, which has been happening since the early 1980s. The hacker of email account can't be tagged as terrorist. Terrorists use various means to spread fear and terror, to accomplish their objectives. Now it is pertinent to explore probable outcomes of a terrorist actions initiated with cyber domain. The main feature of cyber attack is lack of jurisdictional

restrictions. The citizen or non- citizen can operate secretly in any cyber domain against any person, Govt., group, infrastructure or organization.

The public attention is most important for terrorist organizations then technical hurdles. The present world terrorist organizations (for e.g. IS and Al Qaeda) adept themselves in Cyber world and use it to spread their propaganda, recruitmentand for arrangement of funds. Some terrorist groups use social media for recruitments, dissemination of propaganda and aiding in the radicalization process. But attack on cyber network is a completely different aspect. The world terrorist organizations have intent to wage warfare by using cyber domain. The most appropriate example is of-Inspire online magazine, published by Al Qaeda, and included articles on bomb making process and instructions for how to contact with group. It's not pertinent to exclude large Cyber attacks in future while considering future security threats to the nation. It would be horrible if the cyber-attacks-targeting basic infrastructure or financial systems, conducted in collaboration with a traditional attack with other capabilities. This is a deadly combination of Cyber techniques with traditional resources.[1]

The Cyber security is not a choice but a national responsibility. The Indian Govt. has made satisfactory steps for the development and implementation of *national cyber security strategy,* but we must be more cautious about the future complications. The Govt. Intelligence agency states that World terrorist organizations have keen interest in developing destructive cyber technologies and capabilities, but they have financial constraints, organizational limitations and competing priorities. Demarking line between Cyber attack and Cyber terrorism is not clear and confusing. Our critical infrastructure is dependent (directly and indirectly) over the internet.

Cyber threats to India

The Central Bureau of Investigation (CBI), India and Cyber experts continuously warned about the Cyber attack threat to India. Even CBI website is hacked by hackers in 2010 by *'Pakistani Cyber Army'*. The Ex-President of India, Dr. Abdul Kalam raise alarm in his lecture on Cyber terrorism, 2005. Instead of that our India has not yet expertise in 'Cyber security system'. It is to consider a great damage for India. In India, Companies, Govt. and Private Infrastructure and Institutions including financial and insurance sector, spent less and least concerned for cyber security".

In August 2013 Indira Gandhi International Airport (IGI) faced Cyber attack. A destructive virus program called as 'technical snag' hit the operations of terminal no. 03. This malicious code was spread remotely for the trespassing- 'the security system of Airport'. The cyber attackers tried to take advantage of weakness of security system. Their *modus of oprendi* was to transfer of virus program through 'check-in centers' of boarding gates and finally to the operation of CUPPS (Common use Passengers Processing System), which materially affects airlines online reservation system and expected time of departure and capacity of waiting lounge.

Furthermore, Pakistani Cyber Criminals deface nearly 60 Indian websites every day. Pakistani hackers conveniently hacked our websites and writing derogatory information against India for spreading political, religious, social or financial cause. The latest Cyber weapon of Cyber terrorist is *VoIP (Voice over Internet Protocol)* for e.g. What's app voice and video calls, Skype, Video calls through Google talk etc., Coded chats, Secret message inside images, e-mail drafting and encrypted pen drive to propagate their agenda. According to NASSCOM-IDC surveys *"The demand for ethical hackers is estimated at 77,000, in India and 188,000 worldwide currently"*.[2]

The investigation of 26/11 Mumbai attack revealed the- evidence of Cyber telecommunication of terriost, with the help of which they acquainted with map, population infrastructure, place etc. They use the "Google earth" to execute their plan, mobile network for command and control, social media to track the movement of Indian Rescue and defence forces. Furthermore, they use the technology for "conversion of audio signals into data", which made it impossible to track the source of Information by "Indian defence forces[3]. This conversation is decoded by ethical hacker Ankit Wadia.

Another Cyber attack was in year 2011, bomb explosion in market Jhaveri Bazaar, Mumbai. In Varanasi bomb blast case of 2010, which was also executed with the help of E-Communication. Ultimately Govt. of India was compelled to develop a strong mechanism to deal with issue of Cyber terrorism. As a result, the Information Technology Act, 2000, was amended in 2008 and includes Sec. 66F to deal with Cyber terrorism and other related issue, though that was not in detail. It also made also to amend Indian Penal Code, 1860 and Indian Evidence Act, 1872. Instead of this we Indian has spend less for Cyber security.

Legal Provisions for Cyber Terrorism other relevant provisions

India has no specific legislation to deal with Cyber Terrorism. The amendment act of 2008 in Information Technology Act, 2000 inserted Sec. 66F to deal with Cyber terrorism. Those provisions and rules are complimentary with other legal provision in legislations and special legislations relating to terrorism. Section 66F is the only provision which deal with and covers any act committed with intent to threaten unity, integrity, security or sovereignty of India or promoting terror with DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty or integrity of India, the security, friendly relations with other states, public order, decency, morality or relating with contempt of court, defamation or incitement to an offence or to advantage of any foreign nation or group of individuals.

For other offences mentioned in Sec. 66, punishment prescribed is three years and fine of five lakhs has been prescribed and these offences are cognizable and bailable. Sec. 66A provides punishment for sending offences messages through communication service etc. Further Sec. 84B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new Sec. 84C makes attempt to commit an offence also a punishable offence with imprisonment for a term which may extend to one-half of the longest term of imprisonment provided for that offence. In certain offences, such as hacking (Sec. 66) punishment is enhanced from three years of imprisonment and fine of two lakhs to five lakhs. In brief following are the provisions and complimentary rules to deal with Cyber terrorism:

- Sec. 66: Computer related offences including Hacking.
- Sec. 66A: Punishment for sending offensive messages through communication service etc.
- Sec. 66C: Punishment for Identity theft.
- Sec. 66D: Punishment for cheating by personation by using computer resource.
- Sec. 66F: Punishment of Cyber Terrorism.
- Sec. 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- Sec. 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
- Sec. 70B: Indian Computer Emergency Response Team to serve as national agency for incident response.
- Sec. 84B: Punishment for abetment of offences.
- Sec. 84C: Punishment for attempt to commit offences.
- Implementation of Information Technology (IT) Security Guidelines, 2000.
- The Information Technology (Procedure and Safeguard for Interception Monitoring and Decryption of Information) Rules, 2009.
- The Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.
- The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.
- The Information Technology (Electronic Service Delivery) Rules, 2011.
- The Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties Rules, 2013.

Matrixes' of Cyber Terrorism

The are the basic elements of cyber terrorism. Those are as follows:

1. Perpetrator or group of people i.e. Cyber Criminal
2. Place-Cyber Space
3. Action/Method or mode of action-Any Cyber techniques
4. Tools-Cyber Arsenal or Armory
5. Targets-e.g. Govt. Company, Place, individuals, administration or digital infrastructure
6. Affiliations-actual or claimed
7. Motivations-social, religious, communal or revenge.[4]

Most Prominent targets of Cyber terrorism

The aim and objectives of every terrorist organization and every terror attack is different in their own sphere. Here below is the list of possible Cyber attack or terrorism target but these are not exhaustive:

- Communication Infrastructure: News Agencies, Media and Tele communications companies
- Corporations: Component suppliers, Civilian consulting companies
- Financial Institutions: Banks, public or private, Insurance and Government Funding Agencies or Institutions
- Health care Industry: Drugs manufacturing Companies (Vaccines, antibiotics), Pharmacies, Hospital and Clinics
- Power Grids
- Transportation Systems
- Water Authorities
- Nuclear power plants
- Railways
- Information technology Systems etc

Cyber Terror Armory

There is long list of cyber weapons used to create terror. Every weapon is unique in their own aspect and effects according to the objective of terrorist organizations, terrorist or Cyber attacker. Following are most commonly weapons used from Cyber armory to spreadterror:

- Hacking
- Virtual sit-ins and blockades
- Automated email bombs
- Computer viruses and worms
- Denial of services (DoS)
- Cryptography

Cyber Terrorism: Social Media and Terrorist Groups

Cyber terrorism has gravity to influence directly the victims of cyber attacks. The basic objectives of terrorism is to draw attention by causing or with acts of violence globally. In 1990, the National Security Council envisaged that 'Computer could in the future to be used to not only facilitate crime but also as the main too for criminal act. The modern thief can steal more with a computer then with a gun. Tomorrow terrorist may be able to do more damage with a keyboard then with a bomb'.

What Internet offer to Terrorists

The internet offers the following advantages to the terrorist:

- Easy Access
- Minimum Regulation, Censorship, or any type of Govt. control
- Potentially high audience spread throughout the world
- Anonymity
- Fast circulation of information
- Low cost maintenance of web page
- A multimedia effect- ability to combine text, graphics, audio-visual and to allow user to download movies, songs, books, posters very fast
- The ability to shape coverare in the traditional may media, which increasingly use internet as a source of stories

Conventional Terrorism to Cyber Terrorism

The subject of 'terrorism' is always controversial. The origin of word terrorist is from French word *'terrorisme'* that derives from Latin verb *'terroeo'*, meaning thereby *'I frighten'*. Cyber terrorism is an extended form of conventional terrorism where the nature of weapons is in electronic form or devices instead of arms and ammunitions. The objective of both is same i.e., creation of terror. Followings are the qualification of an act to be address as Cyber terrorism:

- Place of occurrence must be cyber space
- Use of Computer system or like device to use as tool
- The aim to act is to create fear, harm or violence
- Motive-religious, ideological, or political objectives

*The **'Electronic Jihad'**, Use of Social Media and Internet by Terrorists:* The "*Electronic Jihad*" by terrorist organizations improvises their terror

technique from traditional to technological. The International terrorist group *Al-Qaeda*, used internet technology to spread their wings of terror in like manner. Similarly, ISIS completely revolutionized "terrorism world" with the use of "*social media*". The reason for this obvious:

- To spread propaganda with electricity speed then, the speed of traditional cart.
- Internet Communication like net calling, video calls etc.
- Lowest cost than other method.
- More complicated to trace.
- Cab ne commit without jurisdictional hurdles.
- Can affect public at large.

Cyber terrorism is worldwide phenomenon. About forty terrorist groups all over the world maintain their websites and use of different languages, which provide the information about them. Generally, their basis objective is to change public ideology, weaken public support to the govt.

ISIS's (Islamic State of Iraq and Syria) presence in India

The *ISIS (Islamic State of Iraq and Syria)* or '*Daesh*', also trying to spread their network in India. This fact is revealed when US Army killed Indian *'IS fighter'* in Afghanistan. It was revealed and confirmed after investigation that Indian citizens confirmed their affiliations with IS. Some of made successful or attemptedto travel to Syria, Afghanistan or Iraq for recruitment, propagandists, financers, conspirators and other synthesis. About 142 Indian citizens (132 named) have confirmed their affiliation with ISIS. The numbers of recruits are increasing year by year as illustrated in Figure 1. Furthermore, the figure 2 shown the ISIS statics in India.

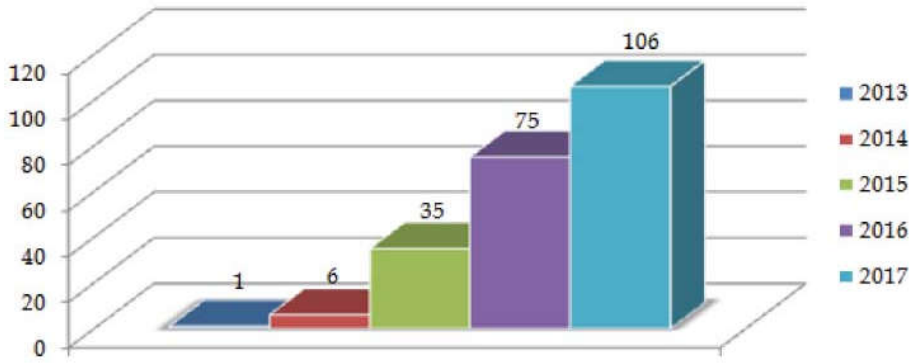
The South and Northern part of India seems to be inclined towards ISIS. National Agencies identified the following numbers of recruits States:

1. Andhra Pradesh- 1
2. Delhi- 1
3. Gujarat- 4
4. Jammu & Kashmir- 2
5. Karnataka- 16
6. Kerala- 35
7. Madhya Pradesh- 6
8. Maharashtra- 19
9. Rajasthan- 1
10. Tamil Nadu- 5
11. Telangana- 21
12. Uttar Pradesh- 16
13. Uttarakhand- 3
14. West Bengal- 3[5]

India Successful Counter ISIS. About 85 of 142 IS sympathies were arrested and interrogated, some returned to and intercepted their homes, some were arrested from Airport and some deported back to India before or during their transit.

Digital Promotion of terror propaganda

Terrorist spread their propaganda by various means including internet and social media platform like facebook, twitter, whatapp etc. Actually, there is not any web source of *www.isis.com or www.alqueda.org*, but their propaganda can still be found. ISIS used twitter for the propaganda of their message, video and recruiting material online. In 2016 twitter



Increasing Recruitment in is from India

Fig. 1: Increasing Recruitment in ISIS from India

freeze about 1,25,000 accounts linked with ISIS. It was contended by *Abu Abdullah al Malghribi*, ISIS detector that "The media people are more imported then solders", he said. "Their monthly income is higher. They have better cars. They have the power to encourage those inside to fight and the power to bring more recruits to the Islamic State".[6] The ISIS Cyber campaign is differ from terrorist group in social media such as *Al Qaeda* in context of their content in vey brutal in posting video massages, beheading of with Social media and internet there terrorist group trying to glorify their acts especially in the eyes of the youth.

Cyber Terrorism and Cyber warfare

In Cyber warfare there is use of information and information systems as weapons, projecting two potentially contradictory policy issues. At one end there is obligation to restrain and guard against information attack, on other side, the requirement to protect the right to use a non-lethal instrument in obtaining national or international requirement. At a time apparently ripe to mobilize international sentiment against all forms of terrorism, it could be particularly worthwhile to canvas the relevant international treaties, agreements and resolutions in search of principles that might be helpful in formulating new norms to help states to distinguish between legal and illegal uses of information warfare techniques.According to Denning "*Information warfare consist of these actions intended to protect, exploit, corrupt, deny or destroy information or information resources in order to achieve a significant advantages, objective, or victory over an adversary*".[7]

The Information technology boon opened new horizons for criminals. The Cyber warfare involves 'attack and defense of 'information and information system' both in time of armed conflict and in operations short of war. The information technology provides the promise of a new class of less lethal military instruments. These vulnerabilities, when exploited by those who would target civilians to inspire widespread fear in hopes of accomplishing a political agenda.[8] The Indian govt. also sent a notice to Mark Zukerberg, facebook for the information regarding possible data breaches and manipulation in about 241 million active members. Indian Govt. also seek the information "whether personal data of votes has compromised by Cambridge Analytica, world's leading data mining firm, or other downstream entity. It was alleged that Cambridge Analytica misused data of millions of social media user and attempted to influence elections.

Conclusion

From the above dissection we can conclude that We could not deny apprehension of cyber terrorism activities in future. We should be act on preventive mode rather then remedial mode of this virtual and physical realities. Today digital India needs response readiness for cyber attacks which is moving ahead for digitized economic system. Which required a quick response and preparedness against cyber attacks. India should be more aggressive in responding to cyber threats and attacks. The cases of ransom demand cases have been reported in private companies for protections of their data secrets and information infrastructures.

Despite of digital awareness among netizens, another aspect of preventive actions is regulating the role of software developers and IT product companies. We should ensure the accountability and liability of software developers and companies launching such exploitable softwares for accessing. Further mishandling of software tools should have more severe punitive consequences, which require regulation of making and leaking of such tools. Such regulatory controls should be on similar pattern of manufacturing or mishandling of firearms or ammunitions.[9] Recently the Daily Excelsior, a leading news paper of Jammu, published an article on June 25, 2019 which says 'Govt to act tough on top militants, cyber terrorism' through major amendments to the anti-terrorism. The Indian Govt. would soon present a Parliament, which would prove another milestone to curbterrorist activities and prevention of cyber terrorism. Some of the amendments proposed in the Law included curbing activities through cyber terrorism by registering cases undervarious provisions of law. These proposed amendments not only help the Government to keep strict vigil and surveillance on militants operating in Jammu and Kashmir but also in various parts of India.[10] The Govt. accepted the proposal for amendment of NIA Act, which equipped the agency to register and investigation terrorist acts on foreign countries if any Indian Citizens or interests are harmed. This draft bill seeks to extend the scope of cases, which an agency is empowered to investigate. New offences being added to the schedule of NIA Act including cyber terrorism cases under IT Act as well as crimes under Sec. 370-371 of Indian Penal Code relating to human trafficking those often have international connections.[11]

Further former National Security Adviser M.K. Narayananat a seminar on 'Cyber-terrorism and

the economy' organized by Centre for Eastern and North Eastern Regional Studies (CENERS-K), also focused on strengthening cyber warfare capacities for peace and security. He asserted that "India is on the threshold of a digital age and the use of IT technologies, which now turned ubiquitous. The danger is that not only it is becoming easier to mask an identity online, but also once the malware codes come into the open market, it can be bought and repurposed by hackers anywhere in the world".[12]

References

1. Cyber terrorism and the reality of threat, Available at https://www.aspistrategist.org.au (Visited on June 12, 2019)
2. Ibid
3. Cyber terrorism: The Fifth Domain, available at: http://www.indiabloom.com (Visited on March 13, 2019)
4. Symantec Cyber terrorism?, Available at: https://www.symantec.com (Visited on June 18, 2019)
5. Assessing the Islamic State threat to India: It is a serious but manageable challenge: http://www.brookings.edu (Visited on July 02, 2019)
6. The Washington Post; Inside the surreal world of the Islamic states' propaganda machine, Available at: https://www.google.co.in/search (Visited on May 21, 2019)
7. Cyber Terrorism and information warfare, Available at: http://www.open.edu.ao (Visited on May 21, 2019)
8. Available at: https://www.hsdl.org (Visited on May 7, 2019)
9. Digital India's response readiness against cyber attacks is frail, lack of online security awareness biggest weakness – Firstpost https://www.firstpost.com (Visited on June 21, 2019)
10. Govt to act tough on top militants, cyber terrorism, https://www.dailyexcelsior.com (Visited on May 26, 2019)
11. Union Cabinet moves to strengthen anti-terrorism law, India News - Times of India https://timesofindia.indiatimes.com (Visited on 05 July, 2019)
12. Govt to act tough on top militants, cyber terrorism, https://www.dailyexcelsior.com (Visited on 05, 2019)