CYBER TERRORISM: A POTENTIAL THREAT TO NATIONAL SECURITY IN INDIA

Jobin Sebastian[1], P. Sakthivel[2]
[1]PhD Research Scholar, Department of Political Science and Public Administration, Annamalai University,Annamalai University, Chidambaram
[2]Professor, Department of Political Science and Public Administration, Annamalai University,Annamalai University, Chidambaram
Gmail: frkuriakosev@gmail.com

Received: 14 March 2020 Revised and Accepted: 8 July 2020

ABSTRACT: The cyber space is one of the most significant real factors of present-day world. Administration, communication, business and practically all the essentials of day by day life are firmly engaged with the internet. The reality of cyber space is a gift to the general public. And yet when it is utilized with a wrong intention it gets one of the most exceedingly awful advancements on the planet. Today terrorists are using the advancement of cyber space to disturb the peaceful existence of the nation states. Cyber terrorism can destroy the entire administrative and economic system of a country. It affects developing countries like India. But the common people are not well aware of the threat of it. The democratically elected governments are facing difficulties in handling the situation. Vital data kept in the computer servers were stolen, confidential data were manipulated or fabricated, malicious software programs infected our computers, the cyber criminals hacked the government websites including defence website (the R&D), income tax dept. Employment office websites, important temple websites, Ministry of external affairs etc. As it is a threat to national security almost all the nations are investing more and more money for cyber security. India too takes many efforts to prevent cyber terrorism. This paper aims to understand the level of cyber terrorism in India and understand the preventive actions taken by India against it. Besides it tries to suggest some initiatives that can be taken to make awareness to common people and other stakeholders about the menace of cyber terrorism.

KEYWORDS: cybercrime, cyber space, cyber terrorism, national security

I. INTRODUCTION

Cyber Space is an unavoidable reality in the advanced world. No one is free from the impact of the cyberspace. Everyday existence of every human being is some way or another related to the cyberspace. This is very clear from social life, communication, government-related programmes etc. The quick development of the cyberspace significantly expanded the cyber security threats in the globe. This is obvious from the various cyber assaults today. Cyber-attacks against the sovereignty and the security of a nation lead to cyber terrorism. The main aim of terrorism is to upset the government and the citizens. This aim is same in the case of cyber terrorism and traditional terrorism.

Cyber terrorism is always related to cybercrimes. In cyber terrorism, terrorists do the crimes against the nations through the technology to redirect or crush framework and foundation which causes injury or death and undermine economies and organizations. In order to accomplish their objectives, they focus the computer systems that control air traffic, electric power grids, telecommunications networks, military command systems and financial transactions (Nehla Hani & Rajan, 2018). Cyber terrorism is a criminal act executed by the use of computers and telecommunication capabilities bringing about viciousness, destruction and/or disruption of services to create fear within a given population to influence a government or population to conform to a specific political, social or ideological agenda (Pujari, 2016).

The wide use of the internet in India for administration and communication made cyber terrorism possible without much expense. At present Cyber attackers are highly motivated, well-funded and technically advanced. Their attacks posed a threat to initiatives of nations like India such as Smart Cities, E-Governance etc. Government and military organisations and other businesses use cyberspace to store and process significant volumes of confidential data. This helps the cyber-terrorist to put national security in danger. By cyber terrorism, the terrorists mainly aim the administrative, economic and security system of India. The use of technology and weapons in terrorism made the terrorist more powerful than ever. By various measures, India is trying to prevent this advanced version of terrorism.

II. OBJECTIVES

1. To unearth the cyber terrorism unleashed against India by cyber terrorists.
2. To elicit the preventive measures taken by both Centre and States in India to combat the menace of cyber terrorism.
3. To understand the lacuna, if any, and suggest some corrective measures to combat cyber terrorism.
4. To understand the correlation between cyber terrorism and national security.

III. METHODOLOGY

This paper adopts the document and analytical method. A major chunk of the literature was collected from articles published in research journals and newspapers, weeklies, fortnightly magazines, government reports, Information Technology Act 2000 and IT Act 2008, study reports by the Cyber security agencies etc.

IV. CYBER TERRORISM IN INDIA

According to the National Association of Software and Services Companies (NASSCOM), India is one of the most susceptible nations in the world when it comes to cyber-attacks (*Cyber Security in India. Opportunities for Dutch Companies,* 2018). The reason behind this vulnerability is the wide use of cyberspace for daily life. In India, telecommunication, business, administration, banking etc are already highly network-dependent and at the same time, they are not protected by proper measures. Hence it is easy to do cyber terrorism in India. While dealing with cyber terrorism in India we can see both national and international level of terrorism. By different cybercrimes, the terrorists both internal and external attack the cyberspace of India. The main categories of cybercrimes in India are the hate propaganda, virus attack and hacking, False Propaganda and Brainwashing the young people, data manipulation and identity theft and undermining the right to privacy. Cyber terrorist commits these crimes to disturb the nation and the individual as in the case of traditional terrorism.

1. Hate Propaganda

Hate propaganda is one of the most popular cybercrimes in India which threats to internal and external security. Even though the false or hate propaganda is prohibited by the sections 153(A) & 295(A) of Indian Penal Code and 66(a) of IT Act many people are circulating wrong matter by using the loophole of the right to expression. In India, the crime of hate propaganda is very much used by the religious fanatic groups to disturb other religious community. Most of the propaganda is circulating on the platform of social media. Sometimes this leads to communal violence. Some terrorist groups also use the same strategy to make a disturbance in secular India.

Online hate propaganda may hostile to certain groups and individual and it affects the values of dignity, liberty and equality. By the wide use of the internet, the hate propaganda through social media increased and as a result government is trying to control it by regulating the use of the internet at the time of communal issues. Hate speech, disinformation and frightening rumours on the platform of social media are already responsible for violence and deaths in India. For example, WhatsApp is being used to disseminate rumours and disinformation to spark dread among the citizen, particularly about people who are perceived as outsiders. The danger is real. In India, the misuse of WhatsApp has already resulted in 30 deaths (Chopra, 2019). Recently in relation to Delhi communal violence, there are 13 cases were registered already for spreading hate matters through social media (*Three more dead bodies found at Delhi*, 2020). Thus hate propaganda through online is a threat to national security.

2. Virus Attack and Hacking

India is one of the most susceptible nations in the cases of virus attack and hacking. According to the business standard reports, 76% of business in India was affected by the cyber attack. (Behera, 2019) There were more than 230,000 ransom ware attack submissions discovered in 2019 between April 1st and September 30th (Dutta, 2020). These show the vulnerability of the issue. Earlier the virus attacks were to destroy the system but now there are attacks of ransom ware by which the hackers are demanding a ransom to restore the system.

The hackers try to disturb the nation and individual by attacking the virtual world around them but it affects the real world. They attack government and private websites to miss guide the people or to demand ransom or to steal data. The hackers are able to attack the whole government-related websites, especially which are related to national security. For example, recently the hackers attacked the Koodamkulam nuclear project. This shows the seriousness of the problem.

3. False Propaganda and Brainwashing Young People

False Motivation and recruitment are usually happening through social media. Many terrorist groups motivate people through social media by spreading their strategies and policies. They are aiming at recruitment too. "Social media has been integral to the terrorist organisation's rise. It enables militants to raise its prestige among terror groups, overtake older jihadist competitors, coordinate with troops, and - most importantly - recruit fresh, young blood" "The ISIS has a full-fledged online recruitment team - which perhaps plays the biggest role in its war strategy - operating from different parts of the world. This team keep an eye out for youngsters who supporting taking up arms to protect Islam or show an interest in the ISIS' ideology" (Ojha, 2017). It was reported that many of the youth were recruited to ISIS from Kerala by using false motivation on Jihad and Caliphate (Mary Koshi & Biswas, 2017; Sharma & Mary Koshy, 2019). There are more than forty-five cases of pro-ISIS activities, ranging from online propaganda to travelling abroad with the intention of joining the Islamic State, recorded in Kerala (Taneja, 2019).

4. Data Manipulation and Identity Theft

Data and Identity theft are very much in India. Online identity theft is a serious crime, often planned for obtaining the personal or financial data of another person. The obtained data is then used for personal gain. Identity theft is referred to as the offence of the new millennium. Identity theft is the theft and use of someone's personal information primarily for monetary gain. In 2017 about 3.24 million records were stolen, missing or uncovered in India. This number has increased by an enormous 783% over the previous year (Khetarpal, 2018). According to the report of the National Crime Records Bureau, there is more than 6500 identity theft cases were reported in India in 2018 (*Crime in India 2018*, 2019).

Most of the Data and Identity theft cases are related to financial information, credentials, credit report information etc. The financial information includes credit card data, bank account numbers etc. Credential means usernames, passwords, account login information, email addresses etc. Credit report information includes addresses, dates of birth, social security numbers, driver's license information etc. All these data are used to cheat the victim.

5. Undermining Right to Privacy

This online crime is usually happening against women and children. Online sexual harassment, cyber stalking, cyber pornography, child pornography (uploading sexual content videos and images and watching it), cyber defamation, morphing etc. come under this crime. According to the report of NCRB, there are more than 3000 cases were reported in 2018 (*Crime in India 2018*, 2019). Most of the cases are happening due to the obsession for love, hate and revenge, ego etc. Most of the sexual harassment issues happen against women who are actively participating in society. Nearly 100 Indian female politicians faced abuse, including rape and death threats, on social media during elections last year. Women are facing online violence and abuse for participating in public life and sharing their opinions on social media platforms. They want to face racist and sexist attacks to rape and death threats (*Indian Female Politicians Face Online Abuse*, 2020).

V. GOVERNMENT INITIATIVES TO PREVENT CYBER TERRORISM IN INDIA

1. IT Act 2000 and its Amendment in 2008

The first step in India to deal with cyber-terrorism was the IT Act 2000. It clearly explains the regulations in the use of cyberspace. Later it was amended in 2008 according to the need of the time. The amendment deals with the issues which were missed by the original act. IT act 2000, Chapters IX and XI, especially sections 64 to 67C of Chapter XI deal with the different cyber offences and its punishment. Sections 68 to 78 deal with the different agencies and their powers to regulate and investigate the cyberspace. Chapter X deals with the Cyber Appellate Tribunal that deals with the cyberspace. In the IT Act amendment of 2008, we can see some modification and amendments in the area of crimes and punishment. Most of the punishment sections were added through the amendment act. Besides, the amendment act gave power to states to monitor and regulate the cyberspace. Now, according to the newspaper report centre government is planning to revamp the IT Act. The aim of this revamping is to bring the IT Act in tune with the hi-tech advancements with a focus on a stronger structure to compact with cybercrimes. ("Centre to revamp IT Act," 2020)

2. Central Monitoring System

Central Monitoring System (CMS) is the centralized telephone interception provisioning system in India. It was installed by the central government for the advance of telematics and it is operated by the telecom enforcement resource and monitoring cells. This is aiming to monitor and intercept the telecommunication such as mobile phones, landlines and internet ("Government Setting up Centralised Monitoring System for Lawful Interception," 2016). The first spark to start CMS was the Mumbai terrorist attack in 2008. The main vision behind the CMS is the public emergency and public safety. The aims of CMS are following the safety of the sovereignty and integrity of India. It works for the defence of the State, friendly relations with foreign states, public order and preventing incitement to the commission of an offence. The agencies like CBI, RAW, IB, NIA, etc. are using the CMS System for their investigation (Xynou, 2014).

3. National Cyber Coordination Centre

National cyber coordination centre (NCCC) is an e-surveillance and cyber security project of Government of India which incorporates cybercrime counteraction strategy, cybercrime investigation training, review of obsolete laws, etc. The aim of this is to assist the nation in dealing with problematic cyber-activities by acting as an Internet traffic monitoring entity that can forestall local or worldwide cyber violations. It is to handle cyber-threats and national security issues in coordination with the country's intelligence agencies.

The centre is to monitor online threats and synchronize with intelligence agencies to deal with national security issues. NCCC will take accountability of investigating any pernicious information that may flow into the networks with the help of service providers. It will be engaged with incorporating information and its examination and make it actionable in real-time by sharing it with various intelligence agencies and law enforcement groups. The centre is expected to coordinate between intelligence agencies, specifically during network intrusions and cyber-attacks (Nandikotkur, 2015).

4. Online Cyber Crime Reporting Portal

Online cybercrime reporting portal is an initiative of the Ministry of Home Affairs. It helps the victims/complainants to report cybercrime complaints online. This portal takes into account the complaints related to cybercrimes and with special reference to cybercrimes against women and children. The complaints reported on this portal are dealt with by law enforcement agencies/ police based on the information available in the complaints (*National Cyber Crime Reporting Portal*, 2020).

In this portal, the victims can report the crime with or without revealing their identity. At present government gives awareness about this portal to the citizen through the SMS.

5. Indian Cyber Crime Coordination Centre (I4C)

Indian Cyber Crime Coordination Centre (I4C) is the initiative of the Ministry for Home Affairs. It has seven components - a national cybercrime threat analytics unit, a national cybercrime reporting portal, a national cybercrime training centre, a cybercrime ecosystem management unit, a national cybercrime research and innovation centre, a national cybercrime forensic laboratory ecosystem and platform for the joint cybercrime investigation team. The main objectives of this initiatives are to fight against cybercrime, to prevent misuse of cyberspace for furthering the cause of extremist and terrorist groups, Suggest amendments, if required, in cyber laws to keep pace with fast-changing technologies and International cooperation and To coordinate all activities related to the implementation of Mutual Legal Assistance Treaties (MLAT) with other countries related to cybercrimes in consultation with the concerned nodal authority in Ministry of Home Affairs (*Details about Indian Cyber Crime Coordination Centre (I4C) Scheme | Ministry of Home Affairs | GoI*, 2020).

6. National Crime Records Bureau

National Crime Records Bureau (NCRB) provides the statistical data of the crime happening in India every year. This is known as 'Crime in India'. This is very much helpful to the investigation agency and policymakers. This data is collected from the different cases reported in the different states and union territories. This data helps to understand the growth of the crime and helps the related agency to concentrate on a special area. In this report, NCRB provides a special chapter for crimes related to cyberspace. 'Crime in India' has become the principal reference document for accurate and reliable information on crimes and criminals, for researchers, criminologists and officials of the criminal justice delivery system in the country. This data is widely used in

India and abroad for academic purposes, and also by MHA/State Governments in framing Public policies (*Crime in India 2018*, 2019).

7. Indian Computer Emergency Response Team and Cyber Swachhta Kendra

Indian computer emergency response Team is a functional organization of the Ministry of Electronics and Information Technology in India which aims to secure the cyberspace. It provides incident prevention and response services as well as security quality management services. Its mission is to enhance the security of India's communications and infrastructure through proactive activity and powerful coordinated effort. It tries to prevent the cyber-attack and respond to the attacks to minimize the damage. Besides, it gives proper awareness to the citizen about cybersecurity and provides technical assistance and advice to them to recover from the computer security incidents (*Indian - Computer Emergency Response Team*, 2020).

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) is the initiative of a digital India project. It is operated by the Indian computer emergency response team. The main aim of this is to identify the attacks in cyberspace and clean the cyberspace in India. It also helps the users to prevent further infections. The centre will also enhance awareness of common users regarding botnet, malware infections and measures to be taken to forestall malware contaminations and secure their computers/systems/devices (*Cyber Swachhta Kendra: Home*, 2019).

8. National Intelligence Grid Project of India

National Intelligence Grid Project of India (NATGRID) is an attached office of Ministry of Home Affairs, has been created as an IT platform to assist the intelligence and law enforcement agencies in ensuring national and international security, with the ultimate aim to counter-terror (*Explained*, 2019). Even though the preliminary thoughts about this project started in 2008 it is going to be fulfilled in this year.

The work of the National Intelligence Grid (NATGRID) is to track any terror suspect and prevent terrorist attacks with real-time data. The NATGRID will have data related to all immigration entry and exit, banking and financial transactions, credit card purchases, telecom, individual taxpayers, air flyers, train travellers besides others to generate intelligence inputs. The NATGRID is the integrated intelligence master database structure for counter-terrorism purpose connecting databases of various core security agencies under the Government of India collecting comprehensive patterns procured from 21 different organizations. This combined data will be made available to 11 central agencies, which are: Research and Analysis Wing (R&AW), National Investigation Agency (NIA), Intelligence Bureau (IB), Central Bureau of Investigation (CBI), Financial Intelligence Unit (FIU), Central Board of Direct Taxes (CBDT), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), Narcotics Control Bureau (NCB), Central Board of Indirect Taxes and Customs (CBIC) and Directorate General of GST Intelligence (*National Intelligence Grid to Be Ready by Early 2020*, 2019).

9. Cyber Security Research and Development Centre of India

Cyber security research and development centre of India is a project that is going to be fulfilled in India. The operations and implementation of Research and development centre will be controlled by the National Security Council Secretariat (NSCS). The rising occurrences of ATM/debit card data breach in addition to the number of cyber threats from neighbouring countries made it mandate for the Indian Government to set-up cyber security research & development centre. The centre expects to set-up centre of excellence, inter-operability research facility to assess the developed software and hardware products. This initiative is taken to safeguard national interest and security and accordingly limiting reliance on few countries for technology and equipment (*Indian Government to Set-up Cyber Security Research & Development Centre*, 2020).

VI. REASONS FOR THE PROLIFERATION OF CYBER TERRORISM IN INDIA

Despite the fact, that has a standard framework to forestall the cyber terrorism the quantity of cybercrimes is increasing day by day. This is extremely obvious from the report of the National Crime Records Bureau. NCRB gives the number of reported crimes only however truly it might be to an ever-increasing extent. Why India is increasingly vulnerable to cybercrimes. The primary reasons for this vulnerability are the following:

i. The wide use of Cyberspace
ii. Cheap internet facilities
iii. Unawareness on security issues
iv. Drawbacks of Existing Laws

v. Lack of Unified international rules and regulations
vi. Cyberspace is boundary less
vii. Lack of cyber security experts in concerned level such as the legislature, executive and judiciary
viii. Lack of proper guidelines for the use of cyberspace
ix. Lack of cyber ethics

VII. SUGGESTIONS TO COMBAT CYBER TERRORISM

India is vulnerable to cyber terrorism but by ensuring proper measures she can overcome the vulnerability. Even though we cannot avoid cyber terrorism as it is we can prevent the wild growth of it by an adequate cyber policy. The suggestions to combat cyber terrorism are following.

1. Create proper awareness to the public about the security issues in cyberspace and ask them to strengthen their cyberspace with security features such as strong antivirus software, use of the official version of the software, avoidance of popup messages and websites, proper updating of password etc.
2. The government and concerned agencies should promote ethical hackers. Ethical hackers can find out the loopholes in the system and software and they can suggest prevention too.
3. Modification of the existing rules related to the cyberspace is mandatory. Rules and regulations should be updated according to the development of technology.
4. Unified and strong international rules and regulations will help to decrease the spread of cyber terrorism. At present, there is no unified law at international level. Cyber laws in one nation are differing from others. This helps the culprits to escape from the punishments.
5. Control over social media is necessary to prevent cyber terrorism. At present, the government is trying to implement some regulations over the use of social media. By this, we can prevent fake accounts, false propaganda, online harassment etc.
6. The policymakers and the implementing agencies should make use of the help of the experts in cyberspace. Their help can improve the preventive system.
7. Proper training related to the use of cyberspace must be implemented. Most of the common people in India are not aware of the use of cyberspace. Cyber literacy must be promoted by the government.
8. Adequate value education related to the cyberspace should be included in the curriculum. The youth and children should be aware of how they can respect others in the virtual world.
9. The government and other agencies should establish strong firewalls in government and other vital websites/networks.
10. Regular conducting of cyber security audit by government and other cyber security agencies can prevent cyber terrorism.

VIII. CONCLUSION

The modern world cannot be free from cyberspace. Cyberspace is growing every day. New technology and features of cyberspace give the human being a new experience at every time. India holds a prime position in utilizing the benefits of cyberspace. The cheap data plans and the affordable handsets cause for the present hike in the use of cyberspace in India. According to the latest report of the Mobile Broadband India Traffic Index average data consumption per user in India grew to over 11 GB a month and overall data traffic increased by 47% in 2019 (*Indians on Average Consume over 11GB Data per Month,* 2020). Besides, the dream project of DIGITAL INDIA and different digital administration helped the growth of cyberspace in India. This wide use of cyberspace makes India more vulnerable to cyber terrorism both national and international. Both national and international cyber terrorism are a potential threat to national security in India. People and other stakeholders of the society should be properly sensitized about the menace of Terrorism and its possible impact on National security in India. Need to establish a strong working relationship and coordination between centre and states in sharing of information and other vital strategies in order to deal with cyber-terrorism. Further, the union government should take over the responsibility to maintain all the vital and confidential data including those data being maintained by the state government, so that we can minimise the menace of cyber terrorism in future.

IX. REFERENCES

[1] Behera, N. (2019, March 13). India third most prone to cyber attacks with 76% firms hit in 2018: Study. *Business Standard India*. https://www.business-standard.com/article/companies/india-third-most-prone-to-cyber-attacks-with-76-firms-hit-in-2018-study-119031300652_1.html
[2] Centre to revamp it act. (2020, February 26). *The Hindu*. https://www.thehindu.com/business/Industry/centre-to-revamp-it-act/article30925140.ece

[3] Chopra, R. (2019). *In India, WhatsApp is a weapon of antisocial hatred*. The Conversation. http://theconversation.com/in-india-whatsapp-is-a-weapon-of-antisocial-hatred-115673

[4] *Crime in India 2018*. (2019). National

[5] Crime Records Bureau.

[6] *Cyber Security in India. Opportunities for Dutch companies*. (2018). Netherlands Business Support Office. https://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in-India.pdf

[7] *Cyber Swachhta Kendra: Home*. (2019). https://www.cyberswachhtakendra.gov.in/

[8] *Details about Indian Cyber Crime Coordination Centre (I4C) scheme | Ministry of Home Affairs | GoI*. (2020). https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

[9] Dutta, P. (2020, February 1). 6 Biggest Ransomware Attacks that Happened in India. *Kratikal Blog*. https://www.kratikal.com/blog/the-6-biggest-ransomware-attacks-that-happened-in-india/

[10] Government setting up centralised monitoring system for lawful interception: Ravi Shankar Prasad. (2016). *The Economic Times*. https://economictimes.indiatimes.com/news/economy/policy/government-setting-up-centralised-monitoring-system-for-lawful-interception-ravi-shankar-prasad/articleshow/52111222.cms

[11] *Indian female politicians face online abuse: Study*. (2020). https://www.aljazeera.com/news/2020/01/indian-women-politicians-face-online-abuse-study-200124051521323.html

[12] *Indian Government to Set-up Cyber Security Research & Development Centre*. (2020). TechSci Research . https://www.techsciresearch.com/news/1912-indian-government-to-set-up-cyber-security-research-development-centre.html

[13] *Indian—Computer Emergency Response Team*. (2020). https://www.cert-in.org.in/

[14] *Indians on average consume over 11GB data per month: Nokia*. (2020). The Hindu Business Line. https://www.thehindubusinessline.com/info-tech/indians-on-average-consume-over-11gb-data-per-month-nokia/article30930377.ece

[15] Khetarpal, S. (2018). *Data theft increased by 783% in India in 2017, says study*. Business Today. https://www.businesstoday.in/technology/news/data-thefts-increased-783-percent-india-2017-gemalto-breach-level-index-study/story/277905.html

[16] Mary Koshi, S., & Biswas, T. (2017). *"Need Jihad, Not Prayer": Isis Recruiter's Whatsapp Message In Malayalam*. NDTV.Com. https://www.ndtv.com/kerala-news/take-up-sword-kerala-engineer-turned-isis-man-abdul-rasheeds-chilling-voice-message-1705871

[17] Nandikotkur, G. (2015). *India Opens Cyber Coordination Centre*. Bank Info Security. https://www.bankinfosecurity.asia/india-opens-cyber-coordination-centre-a-8100

[18] *NATGRID: Explained: What is the national intelligence grid?* (2019). Times Now News.Com. https://www.timesnownews.com/india/article/what-is-the-national-intelligence-grid/488258

[19] *National Cyber Crime Reporting Portal*. (2020). Ministry of Home Affairs. https://cybercrime.gov.in/Default.aspx

[20] *National Cyber Crime Reporting Portal Launched For Citizens to Report Cyber Crimes Online*. (2020). News18. https://www.news18.com/news/tech/national-cyber-crime-reporting-portal-launched-for-citizens-to-report-cyber-crimes-online-2454259.html

[21] *National Intelligence Grid to be ready by early 2020*. (2019). India Today. https://www.indiatoday.in/india/story/national-intelligence-grid-to-be-ready-by-early-2020-1601949-2019-09-22

[22] Nehla Hani, M., & Rajan, A. (2018). A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack. *International Journal of Pure and Applied Mathematics*, *19*(17), 1617–1636.

[23] Ojha, S. (2017). *How isis recruits in india revealed by 20 mumbai men among others*. NDTV.Com. https://www.ndtv.com/india-news/how-isis-recruits-in-india-revealed-by-20-mumbai-men-among-others-1688398

[24] Pujari, A. (2016). *Cyber Terrorism. World Wide Weponisation!* TN Police Sesquicentennial Anniversary Souvenir.

[25] Sharma, N., & Mary Koshy, S. (2019). *Raids In Kerala Amid Probe Against ISIS Unit, 3 Suspects Questioned*. NDTV.Com. https://www.ndtv.com/india-news/anti-terror-raids-in-kerala-as-part-of-probe-against-isis-unit-3-suspects-being-questioned-2029826

[26] Taneja, K. (2019, November 21). God's own Khilafat? Why Kerala is a hotspot for ISIS in India. *ThePrint*. https://theprint.in/pageturner/excerpt/god-own-khilafat-why-kerala-is-isis-hotspot-in-india/320945/

[27] *Three more dead bodies found at Delhi*. (2020). ManoramaOnline. https://www.manoramaonline.com/news/latest-news/2020/03/01/three-more-dead-bodies-found-at-

delhi.html

[28] Xynou, M. (2014). India’s Central Monitoring System (CMS): Something to Worry About? —The centre for internet and society. *The Centre for Internet and Society*. https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about