Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 05 | Issue 01 | April-2022

# Reformation in Legal System and Governance to Curb Cyber Terrorism

**Dr. Neelkamal Ganesh Battu[1], Dr. Dhwani Patel[2], Dr. Pankti Patel[1], Dr. Swati Kanojia[1]**

**Available online at: www.xournals.com**

Received 5th March 2021 | Revised 30th March 2021 | Accepted 11th April 2021

## *Abstract:*

*Cyberterrorism is the future of terrorist activities, it is driven by the motive of destroying enemies' operational capabilities. They inflict social hatred amongst the people of a community based on status, religion, nationality, etc. It is grouped into 3 main categories Simple – Unstructured, Advanced – Structured and Complex- Co-ordinated. The recent Boll on Cryptocurrency and Regulation of Official Digital Currency 2021 is also being discussed in Parliament. With the due progress of time various amendments are done in the legal system in the Information Technology Act and the Cyber laws. Improvement in governance to restrain terrorist activities have also brought about some changes which will be put forth in the following paper.*

***Keywords:*** *Cyber Terrorism, Cyber Crime, Money Laundering, Cryptocurrency.*

## *Authors:*

1. *Post Graduate student, M.Sc. Forensic Odontology, School of Medicolegal Studies, National Forensic Sciences University, Gandhinagar, Campus Sector 9, Gandhinagar, Gujarat, INDIA*
2. *Assistant Professor, Department of Forensic Odontology, School of Medicolegal Studies, National Forensic Sciences University, Gandhinagar, Campus Sector 9, Gandhinagar, Gujarat, INDIA*

## Introduction

In advancements of technologies, the future wars in the world will not be like the conventional ones on land air, or water; but a Cyber War. In simple words, it is an unlawful act against society on grounds of partisan and communal disharmony through the medium of computers and the internet. The divulgence of Edward Joseph Snowden, an expert who worked in Central Intelligence. He disclosed documents of Global surveillance program run by NSA in co-operation with telecommunication agencies and European Government. These revelations specified that considerable of the NSA scrutiny aimed at India's internal politics and its commercial and strategic interests, exhibiting India's helplessness to cyber prying in all areas. India was 5th amongst the targeted countries.

The wars in the coming times would attack the distinguished sectors of

1. Defense
2. Finance sector
3. Documents of internal and external security
4. Rail and Air Traffic Control Management
5. Satellite and Communication Sector
6. Prime Institutions of Science and Research and Development. **(Janczewski and Colarik, 2007).**

## Reasons for Spread of Terrorism

In times, terrorism spreads swiftly due to the subsequent factors:

1. More technology available to demeanor terror
2. Targets of terrorism are more widespread
3. Sophisticated medium of communication (electronic, print and media and internet) helped terrorists to quickly promote their ideology and hate campaign
4. Intolerance in society by virtue of rising population and declining resources.
5. Increasing globalization of the community International recognition and support to terrorist groups
6. Link in terrorism and systematized crime to earn money. **(Kumar and Anekant, 2019).**

## Financing in Terrorism

Terrorist activities are not directly funded, it is done through a secret medium such as cryptocurrency i.e. digital money formed through code. The track is kept by peer-to-peer internet protocol. It is tenable cord of data or a hash encoded to specify a unit of currency.

Cryptocurrency is gaining the limelight due to failed government policies. The disillusionment with the banking system, the increasing taxation of government on high-income group people so as to disguise the government and to don their investment public is developing interest in cryptocurrency. It is now being considered as digital gold.

Cryptocurrency can however help in reducing financial fraud, decrease corruption, bring development in technology, and in turn boost the economy. As smartphones are the basic need in today's life, it is predicted that cryptocurrency will be the future of the economy. The Committee concluded that the decentralized nature and the obscurity which cryptocurrency provides, make it difficult for law enforcement to track down people involved in the activities. **(Ahmad *et. al*, 2012).**

Block Chain Technology has also been introduced. It is a technology by virtue of which all the data of money transactions is secured and therefore it becomes very difficult to manipulate the data regarding each transaction as all transactions are linked one after the other.

The Parliament of India is conversing the recent trend i.e. the cryptocurrency. The Bill of Cryptocurrency and Regulation of Official Digital Currency 2021 have suggested bringing about the official digital currency being dispensed by The RBI and also condemning non-governmental cryptocurrencies in India.

An organization that is created to fight Money Laundering is The Financial Action Task Force (FATF). It is seen that virtual currency is anonymous when compared to our traditional payment. Hence the risk is more in money laundering and funds for terrorist activities.

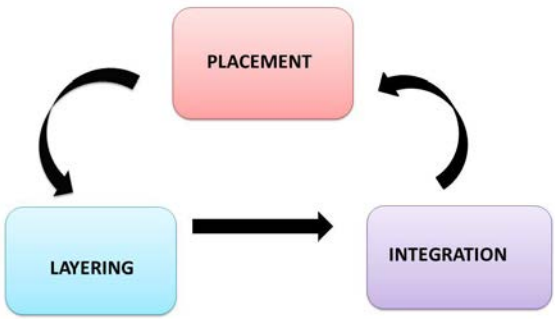


**Figure No. 1 – Money Laundering**

Round Tripping is a new and crucial route through which money is laundered. In this process, money generated in India is transferred to tax-haven countries. Then a company is set up in the tax haven with the black money. This black money is now shown as 'white money and sent back into India as 'foreign investment'. The profits earned in India with this investment are taken to the tax heaven without paying any taxes in India. This is because such investment is exempt from taxation under the Double Taxation Avoidance Agreement. This method of money laundering makes use of loopholes in the capital/stock markets and investments are done via P-Notes (Participatory Notes). Journalist P. Thakurta has exposed this new method of money laundering through a documentary called – 'A Thin Dividing Line'. **(Antonyan *et. al*, 2021).**

Hawala Transaction is a medium of sending money which is purely based on faith and intermediate dealers known as the hawala dealers. The businessman of a country or a person of country A can send money through the hawala trader of country A providing him a code X which he passes on to the hawala trader of country B and in turn to the person of country B with the same code.

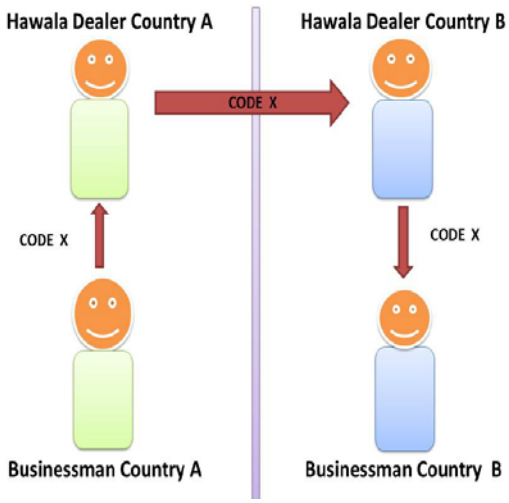


**Figure No. 2 – Hawala Transaction**

**Steps Taken by the Indian Government**

The following steps have been undertaken:

1. Setting up National Critical. Information Protection Center
2. Establishing Center of Excellence in Cryptology.
3. Cyber Forensic Laboratories to be founded in every state.
4. Computer Emergency Response Team (CERT)
5. FIN- CERT i.e. to secure Indian Economy.
6. Cyber Surakshith Bharat Initiative that is the union of various IT companies such as WIPRO, Intel, Microsoft. Knowledge partners are Cert-In, NASSCOM, NIC and Consultancy firm EY and Delloite. **(Kumar and Anekant, 2019).**

**Information and Technology Act 2000**

The word Cyberterrorism was not initially comprised in the act. It has later been added by amendment in the year 2008 in the Section 66 F.

**Policies to be adopted to combat Cyber-Terrorism**

1. Maintaining moral relationships with the perpetrator – We must communicate with those who had been convicted of being in relation with the terrorist and extract information about the future plans.
2. Be updated with the latest technology
3. Adopt best security practices
4. Be aware- The officials and the civilians must be proactive.
5. Make use of prime Security Applications
6. Establish Plans Cooperation with Various Firms and Working Groups
7. Implement Stricter Cyber Laws
8. Encourage Research And Progress **(Jalil, 2003).**

**Effect of Social Media**

There is a vast difference between traditional media. Traditional media has limitations it has restrictions conveying to the public. Whereas on social media the public themselves are the conveyors, there is not a restriction on expression hence any abhorrent posts and blogs can create hatred amongst people which would lead to acts of terrorism. **(Wu and Wang, 2019).**

**Conclusion**

The attacks of 26/11 of Mumbai happen to be an attack of cyber-terrorism. The many aspects connected to cyber terrorism such as critical infrastructure, business, and humans, and taking the complex step to decrease the chances of such attacks from happening and protect everyone. However, all organizations, the government, and the public shall work together with a

strong aspiration to win the battle. Cyber offenses shall be given stricter punishments and must be considered as non-bailable offenses. The fact cannot be denied that it is inevitable and is going to have an endless journey in future wars. With various plans, we will get closer to achieve our main objective which is to have a secure and protective environment.

**Acknowledgement**

Dr. Dhwani Patel, Assistant Professor at National Forensic Sciences University, Gandhinagar, Gujarat, India for her valuable guidance and insights.

## *References:*

Ahmad, Rabiah, et al. "Perception on Cyber Terrorism: A Focus Group Discussion Approach." *Journal of Information Security*, vol. 03, no. 03, 2012, pp. 231–37. *Crossref*, https://doi.org/10.4236/jis.2012.33029.

Antonyan, Elena Aleksandrovna, et al. "Blockchain Technology in Countering Cyber Threats." *SHS Web of Conferences*, edited by A.A. Pavlovna et al., vol. 108, 2021, p. 03008. *Crossref*, https://doi.org/10.1051/shsconf/202110803008.

Jalil, Shamsuddin Abdul. "Countering Cyber Terrorism Effectively: Are We Ready To Rumble?" *GIAC Security Essentials Certification (GSEC)*, 2003.

Janczewski, Lech, and Andrew Colarik "Cyber Warfare and Cyber Terrorism." *Information Science Reference*, 2007. Crossref, https://doi.org/10.4018/978-1-59140-991-5.

Kumar, Ashok, and Vipul Anekant. Challenges to Internal Security. Mc Graw Hill, 2019.

Wu, Chunying, and Juan Wang. "Analysis of Cyberterrorism and Online Social Media." *Advances in Social Science, Education and Humanities Research*, vol. 351, 2019, pp. 925–27. *Atlantis Press*.