CYBER TERRORISM TO THE REFRENCE OF CRYPTO CURRENCY IN INDIA

By Shakti Pandey[*] *& Dr. Vir Vikram Bahadur Singh*[**]

ABSTRACT

Under the above research article, cyber terrorists have studied the incidents of fraud of crypto currency and maintaining the website for crypto currency. In the present context, excessive money is received by terrorist organizations through cryptocurrency by funding in terror account, which is a matter of concern, as well as the risk of terrorist incidents is increasing more and more for all the countries of the world. Terrorism is increasing day by day. Cybercrime has given a new direction to cybercrime, on the other hand, cryptocurrency become a kind of tool for cyber terrorism, through crypto currency by terrorism leaders sitting in the country and abroad, using digital currency in millions of trillions every year the country's economic, Along with loss, social damage is also caused. Terrorists have had one objective since the beginning, loss of life and money to the enemy country, for this reason, by obtaining cryptocurrency, cyber criminal's provide new technical resources to their training centers, online smuggling, and online gambling etc, promote criminal activities. Such a huge amount of crypto currency is cheated by the terrorists, due to which there criminals lure the youth for jobs by giving them a lot of money, the youth also join these jobs without knowing about if and avoid unemployment. By the time a person is aware of this topic ,the youth also get involved in terrorist activities, these topic have been analyzed in the said research work.

Keywords- AI, Cryptocurrency, Terror, Funding, digital, etc.

[*] Ph.D. Research Scholar, Faculty of Juridical Sciences, Rama University, Kanpur Nagar, U.P.
[**] Associate Professor, Faculty of Juridical Sciences, Rama University, Kanpur Nagar, U.P.

I. INTRODUCTION

Increasing in the 21st century, due to digitization, the use of detailed currency in the society is also increasing day by day, because the cost of digital currency in dollars, due to its high value, it has because the first choice of money investors. Ever since the introduction of crypto currency, it has paved the way for a kind of progress for terrorist organizations around the world. Crypto currency is used by various terrorist organizations for ransom, under which these terrorists keep an eye on the data of the security agencies of the big institutions of the country and hack its important data as soon as the opportunity is received fake crypto currency is also sold by terrorists is the crypto currency name of crypto currency, which people get ready to get at a cheap price due to lack of information and loot their hard earned money to these terrorists to get crypto currency.

In this way, digital currency has become the first choice of terrorists, due to digital currency, there has been a large amount of funding in the accounts of terrorists, due to which terrorists have smuggled new technical weapons in terrorist organizations, increasing terrorist activities however, and terrorists get the digital world. Due to the increasing popularity of digital currency; cybercrimes are also increasing in the domain in which crypto jacking, ransom wear, attacks, phishing, hacking have been made very easy. In all criminal cases of extortion etc by cyber terrorists, a fictitious name and address is mentioned to hide their real name and address. Apart from this, these criminals do criminal activities in a chain system together many criminals hack any website.

Which are interconnected with countries and states, due to which there is no information about the real accused, so these organizations continue to carry out their activities, due to which a developing country like India is being cheated in the amount of millions of billions of dollars Along with huge economic losses, the rupee is facing a continuous decline India has been facing the terrorism of terrorist accounts through crypto currency; these activities against India have increased further.

II. HISTORICAL ASPECT

David, the first American cryptographer to use crypto currency, conceived electronic money in 1983, which was known as '**Thai Cash'**. After this, in the year 1995, Digi Cash, it was used to withdraw notes from the bank, software was required to use it in the year 1996, the National Security Agency classified it as Make Mint Anonymous. Published a paper named Cryptography related to electronic case. The said paper was published for the first time in

MIT's[1] ling list. After this, it was published in the American Law Review in 1997. In the year 1998, Wei Money and Nick Szabo accepted Navit Gold as an electronic currency system in the year 1998, it was a kind of trustee electronic cash system in the year 2008 , A peer Electronic Currency was published after this digital currency started I India in 2013 the first circular was issued in the year 2020 Supreme Court declared RBI circular unconstitutional after that 29 January in 2021,the government announced the it would introduce a bill to create a digital currency and ban the privatization of crypto currencies.

After that, in 2022, Fiancé Mister Nirmala Sitaraman clarified that instead of banning the privatization of crypto currencies, it would impose a Tex of 30% while crypto there is no legal provision for currency, due to this, crypto currency, is mostly used in criminal activities, in which black chain due to the fraud business happening in it crypto currency criminal cases are from China, who loot millions of billions of CRYPTOCURRENCY every year.

III. INDIAN PERSPECTIVE

Under the said research article haw cyber terrorist's use digital currency, increasing account funding terrorist's activities by terrorists using crypto currency increasing training centres of terrorists, etc. have been studied. In the present times where, digital technology is use. Due to the increasing digital transactions villages and cities, after the imitative of "Digital India" India is moving towards New India. In other perspective, in the last years, the circulation of crypto currency has become very high in the country and the world, although by both the Government of India and RBI it has not been recognised but crypto currency has been verified as digital currency. On one hand new records are being created by cryptography in addition to decentralization system by making, full use provides theoretical immunity to government interference and manipulation, while according to the REPORT of black chain analytics firm *Chainalysis*, in the year 2019 itself, cyber terrorists looted 2.8 billion through exchanges in Bit coin[2].

There is mainly political reason behind cyber terrorism which can cause immense harm to India's economy. Saver terrorists use computer virus, computer worms, phishing, shattering, programming script, cyber robbery, hacking, black chain system, cyber money laundering, ransom account etc. Funding is done according to the millennium, by which terrorists have reached chemical weapons as well as nuclear weapons in the present time, which is not only a

[1] Massachusetts institute of technology
[2] Crypto currency phishing attack article journal ABP news 5 April 2022.

matter of concern but has become a threat to the whole world from. India Cyber Safety Form According to Spar sky, in the year 2022,[3]the financial threats of banking PC[4]and mobile malware have decreased, while the cases related to crypto currency phishing have increased by 40%in just 1 year.

In 2022, these cases have increased 5,040,520. According to spar sky 's safety expert Olga Sbistunova, the CRYPTOCURRENCY market continues to be get rich quick, despite being hit by problems in the part months. Due to non-fixation of crypto currency standards, a person does not even know about real fake crypto. Scammers adopt a more traditional approach to crypto scams, in which they systematically share a PDF[5] via email using new technology after activating a fake wallet phishing badge. In which it is said that the crypto currency has been registered on the cloud mining platform for a long time and it needs to be withdrawn in large quantities, this account is inactive. Due to which the fake crypto mining platform gets linked as soon as it is connected. The victim is told that in order to withdraw the crypto amount, he will have to fill the form with his card or account number and personal information and also pay the commission. As soon as the victim shares his personal information, the CRYPTOCURRENCY goes from the victim's account to the criminal's account.

Wazir X, Kind X, Zebpay, Coin Switch Kuber and Uno coin exchanges are usually used for investing in crypto currency.[6]To invest in any crypto, you have to enter your personal details on the site of the exchange, through which registration is done. Like a demit account, an Insight. Cyber criminals offer to sell fake crypto at a cheap rote. The person gets trapped in the greed of more profit. In India, the first case of fraud with crypto currency came to notice in 2021, but according to the report of Global cyberattack on 16 May 2017, computer terrorists from about 74 countries come together in the grip of cyber-attack.[7] In which about 100 countries were targeted, in which millions of computers were targeted, simultaneously, this attack was done by rensomware virus, in which 300 to 600 bit coins demanded in ransom. On demanding ransom of crypto currency by cyber terrorists, only if done, if not given, then the data is last forever.

1-According to cyber expert Pawan Duggal-At the time of virus attack, the entire data of computer is completely closed by the cyber criminals, all the files are completely closed, on

[3] Crypto currency and money laundering Drishti article journal 17 November 2022
[4] Personal computer
[5] Portable document format
[6] Investing in crypto currencies article news 18 -3979656,January 2022
[7] Global cyberattack author proves sagar article-2017.

opening the windows only the screen of orange colour invisible, after that the victim receives an SMS, Is sent if you want to open the window then deposit the ransom amount in the form of bit coins on the link provided along with a red warning is also give if you try open the Window the data base of all files will be corrupted. Along with this, money laundering and hawala business is also increasing very fast in India. Money laundering and transitions are increasing very fast.[8]

The issue of cyber activities being carried out by the Falah-A-Insaniat Foundation at the minister of State for planet India was also kept in the Melbourne commence, in which concern has been expressed about the increasing use of crypto currency in the funding of terrorists. For which the Anti Money Laundering Combating the Financing of terrorism has been emphasized to be implemented seriously, as well as the Government of India has also shown full commitment on the matter of the Financial Action Task Force. The data breach of the first currency used in India, reported an average of 176 million, an increase of 6.6 percent compared to previous years, according to the report by IBM[9]data breaches was divided in to four categories, Last Business, Detection and Escalation, notification and Post Breach Response, out of which only Breach Response caused a loss out of 7.1 million, due to which this loss increased from Rs 67.20 million in 2022.

Although the cyberspace Buyers 2022 but the February 2021 report did not focus on India but the February 2021 report of New York based company Chainalysis, data collected in the block chain plat form ,mentioned matters related to India. In which funding has been accepted in the account of terrorists through crypto currency. The use of black chain based crypto currencies is explained in the context of India where virtual assets offer special advantages to crypto criminal's particular many pseudonymous encryption of paper currencies, low-cost access around the word Cyber for terrorists. The use of the world has become very easy.

Terrorist's organization ISIS[10] has used encrypted platforms to recruit terrorists, spread radicalization, dork webs been used and through other frauds of baking, terrorists can raise funds, buy weapons, drug trafficking. Cyber terrorism is defined in Section 66 F of the Information Technology Act 2000, as the complete use of technology to commit terrorist cyber crimes through computers, internet, satellite phones, mobile phones, SMS, Email, internet,

[8] Money laundering hawala business through CRYPTOCURRENCY India News Author Manoj Yadav February 2022
[9] International business machines
[10] Islamic Sate of Iraq &Syria

telephone, electronic banking transactions, fake note business use fake crypto money to increase funding terrorist accounts by causing huge economic loss to the country.

2-Technologies used by terrorists in terrorist incidents in India –E-bomb high energy radiofrequency, guns, high attitude, nuclear, explosion, high power micro bombs, devices RDX bump, although India first implemented the Unlawful Activities (Prevention) Act 1967 to deal with terrorism, followed by TADA 1987, Rasuka 1980, Mecca 1999, was applicable only in Maharashtra and Delhi, POTA 2002, which was applicable only in Karnataka, followed by the Information Technology Act 2000, etc[11].

According to the report of clouded company, there were about 82 cyber-attacks on government websites in India in the year 2022.Which is 8 times more than the year 2021.Atpresent, most cyber-attacks in India are taking place in government institutions only. In a written reply in the Rajay Sabah by the Union Minister for Communications and Information Technology, the explanation has been given in the year 2022-23 about 50 Government websites were hacked, in which the central government had 42 cyber-attacks in the year 2020, 50 in 2021,59 in 2022,respectively,which Were tracked by the Indian computer response team CERT IN. According to the report of CERT IN, 2,83,581 in the year 2020 ,4,32,057 in stopping the scam and how in the year 2020 6,7 in 2021 and 8 data leaks in 2022.

Along with this, there are continuous attempts of cyber-attacks on the India, cyberspace from within the country and from abroad as well as many times attacks are also done by hiding the identity of the system ,according to the statistics of the previous years, out of 53000 incidents of cyberattack , it has increased to 14. According to a report by cyber security firm SPACE IND space, there have been more than 85 cyber attracts in the world in the last 3 months of 2022, out of which 60% have happened only in India. India terrorism has been going on for a long time. In which cyber terrorism in the first case 26/11 Mumbai terror attack, 12 March 1993 Mumbai serial blasts, 13 December 2001 Indian Parliament attack,29 October 2005 Delhi serial bomb blasts, 11 July 2006 Mumbai train blasts, 3 May 2008 Jay Pur blasts, January 2016 Pathankot terrorist attack, etc, the continuous terrorist attacks are a matter of concern for the country, after this , terrorism is getting more strength by using crypto currency, which is continuously leading to heavy losses to the country.

[11] Tech desk news Amar Ujala journal 4Feb 2022

3-Delhi AIIMs server hacking case 23 November 2022 –The said case is about the hacking of about 5000 computers of Delhi AIIMs, in which 50 servers were also hacked. AIIMs, of Delhi contains health data of about four corer patients, including big industrialists and politicians of the country and abroad. This dada hacking took about 8 days. In was carried out by hackers from china and Hong Kong, in the said case, 200 corer rupees crypto currency was sought as ransom, although Delhi police's Intelligence Fusion and Strategic Operation and CERT-IN, by the Central Bureau of ransom, but the fear of data hacking again is a matter of concern.

- In the year 2022, in the case of Spice Jet server hacking, the airlines 'servers were victimized, due to which many flights had to be cancelled and dozens of flights had to be rescheduled, in which case the spice Jet Company had to pay cores of rupees ransom to the hackers.
- Year 2022 oil India Hacking in this case, 57 curare cryptocurrency was crypto currency was demanded by hacking the server of Oil India in Assam, although in this case, without paying money, it was successful in controlling the server.
- October 2020 hackers the servers of Haldiram Company and took over the company's files, systems, data and applications by malware attack, in return the company gave 7.5 million US dollars to the hackers.
- After taking over the network of power distribution companies in cyberattack on electricity companies of Andhra Telangana the year 2019, the hackers demanded 6 bit coins, at that time the cost of 6 bit coins was Rs 2400000 which the company had to pay.

In INDIA, the cases of hacking companies' websites and getting ransom are increasing. A Scam related to Bit coin Ponzi Scheme come to notice in sutra district of Gujarat, in which about of $ 3 billion of **INVESCO**[12] was drowned. In which Diamond merchant, In which diamond merchant, property, dealer, some involved, the Gujarat are also involved, the complaint of the said case was made by a property

Dealer named Shailesh Bhatt according to which he was kidnapped by some policeman, in which 200-bit coins were taken from him. A ransom was demanded, which cost about 18 lakh dollars in this case 8 policemen were also complicit. In India, only new dimensions regarding crypto currency are being considered to take concrete steps to impose law and regulation of

[12] American independent investment management company

official digital currency bill, tax etc. To ban crypto currency, but no concerts steps have been taka, but cyber–Bit coin has become a major means of earning money for criminals, not only in India but all over the world, crypto transactions have become a means of funding for cyber criminals.

IV. INTERNATIONAL PERSPECTIVE

Money laundering to account for 15%of cybercrimes in 2021, according to block chin Analysis Company china ALTCE [13]and incidents of terrorism come to notice in the year 2018, 7.1 billion US dollars of CRYPTOCURRENCY fraud took place, in the year 2019, this damage was 1.2 billon US dollars in the first 3 months, in the year 2022 according to the report of Chainalysis, 125system of crypto currency fraud were hacked. During this fraud of 3.8 billion was done worldwide, this fraud was done by hackers of North Korea.

This includes fraud of 7 billion to Us on July 15 2020, twitter accounts of celebrities like Joe Warden, Barak Obama, Elon Musk, Bill Gites, Jeff Bezos, Contro West, Michael Bloomberg and Kresh etc. were hacked by haceks. In this case Twitter account was hacked for about 6 hours by hackers send message to transfer to a violet wallet in which amount will be doubled hackers spread message on Twitter until this amount increases to 10,000 According to US research report I the world by 2025 cybercrime will be around $ 10.5 trillion in 2031, losses to cybercrime victim alone from rensomware attacks will be around $ 265 billion a year Token developers encourage unsuspecting users to invest in a particular and then shut it down, leaving the victimized investor empty handed. US researches put the loss due to these incidents at $ 3 trillion in 2015. That is projected to grow by 15% $ 10.5 trillion in 2025.[14] In March 2020, Delhi polices special call arrested a Kashmiri couple from Okla., where Zeb Sami and Hina Bashir Weg were arrested, both of these criminals of were buying and selling arms and explosives in large quantities to ISIS terrorists sitting in Syria.

In this case, it was found from the bit coin address obtained from the ISIS operative that a large amount of crypto currency has been used to buy these weapons. In the year 2019, at the No money for terror conference held in Melbourne, Australia, the Indian Minister of State for Home Affairs, Reddy, and Financial Action Task Force Anti- Cyber Activities to stop the cyber activities of Falah-E-Insaniat Foundation and stop the funding of terrorism with emerging

[13] A large Ion Collider Experiment
[14] American research report year 2025 Article journal Regina Mihindu Kularia 12 August 2022

technologies. Emphasizing on the uniform implementation of money laundering, combating the financing and television system in the world, terrorists are resorting to cyber technologies to spread terror around the world, as well as the main means of raising frauds, according to cyber companies in cybercrime, the terrorist organization ISIS used encrypted platforms to raise funds for terrorists, purchase weapons, use the dark weapons, use the dark web to spread radicalism, etc.

In the current environment, financing of terrorism is more dangerous than terrorism which is funded by means and method. Countries like Pakistan, China, and Hong Kong are giving full protection to terrorists. Terrorists hide their personal identity and spread radical material. Dark net use system in which the use of virtual assets like CRYPTOCURRENCY is increasing, it is very important to know the button of activities running on the dark net, as well as narcotics are a major medium of finance in terror in present times. The main example of which is smuggling from neigh boring courtiers Nepal and Bangladesh. Due to increasing terrorist funding day by day, it is a matter of concern for the economy of the former world. Cyber terrorism was first done in the year 1944 to destroy the communication lines of Germany. In the year 1980 -1990, the cyber war started through the internet, before this, form the year 1977, terrorists stared threatening other nations sitting in any nation by creating their own website.[15] The use of worlds such as terrorises. Cyber space, etc. had started, which is a matter of great concern for both the social and economic environment at the world level.

V. CONCLUSION

Under the above research paper, the losses caused by the financial funding of terrorist organization through crypto currency have been studied in India and internationally. India has been fighting terrorism since last decades, in which infiltration from neighbouring country Pakistan has been done. The main one is according to a research done by the professor of Israel University, from the beginning of the internet around the world, criminal activities can be done sitting in any country any hindrance through virtual medium. [16] Hacking and crypto currency have become a basic medium for terrorist organizations. At present, thousands of terrorist organizations around the world work wholeheartedly only for hacking. Major terrorist organization are ISIS, Laskare-E-Taiba, Jaise -E -Mohammed, Al qaeda,G-Force Pakistan, Death to India, Pakistan FBH, online Syndicate, Silver Lord Kill India etc. are continuously

[15] Social media cyber crime book attack on Germany communication lines by terrorists page no 65
[16] Israel University Professor's report

spreading terror by dangerous terrorist organizations. On the other hand, china which is at the first place in the world in the cyber world, that country is also keeping an eye on the data of VIP people in the world. Account, even of after major incidents like hacking of former US President Barrack Osama's website, no concrete steps have been implemented to stop terror funding.

Although on 18 November 2022, the Home Minister expressed concern for the financing of terrorism at the No Money for Terror Conference in New Delhi but at present, even after so many criminal incidents, crypto currency has neither been taken again, but the privatization of crypto currency has not been banned, while Chain, which is known for crypto currency. But banned in our country as well as a large amount of crypto currency from other countries is taken as ransom by cyber –attacking Chinese hackers, the Indian Finance Minister also proposed a tax of 30% on crypto currency, but when there is no control of RBI on crypto currency, nor is it inn common practice at the social level, so that our daily routine done not depend on digital currency. The state and the central government have the some right on the above currency. This capitalist has already weakened the Economy of a developed country like India by incidents of money laundering, banking fraud etc. in India, even after this the government has given recognition to currency like cryptocurrency.

Terrorism financing through currency, recruitment terrorists smuggling purchase of dangerous tools, even in today's time, due to the financing of terrorism, drones and nuclear weapons have reached, yet in the present time there is no need to implement rules globally. Only talks are held in conferences for crypto currency, the government is giving importance only to tax benefits, while not only India but the whole world is on the target of terrorists but there is no common law to stop the financing of terrorists by any country. Not made especially India which has been victim of terrorism since year's strict law regarding crypto currency as well as steps like demonetization need to be taken Dark net use should by terrorists Radicalizing Indian youth against nationality and hiding identity and stopping financing to stop terrorist activates, as well as strict laws and technological changes are also necessary to be implemented.

VI. SUGGESTION

- There is a need to take important steps like demonetization regarding crypto currency in India.
- Privatization of that fake crypto currency can be stopped.
- RBI and central and state governments should have general control over crypto currency.

- The value of crypto currency should be set uniformly.
- Technological and legislative framework should be firmly implemented in the context of crypto currency.
- To prevent terrorist financing, a uniform law and treaty should be implemented at the international level.
- Cyber security agencies should make technical efforts to prevent misuse of new Technology.
- There is a need to establish cooperation and coordination at the international level.

****