Vivekananda International Foundation

Cryptocurrencies

A New Scourge of Terror Financing

Abhinav Pandya

VIF Brief - August 2018

About the Author

Abhinav Pandya is a policy analyst who specialises in counterterrorism and geopolitics having more than seven years of experience in public policy, counterterrorism, electoral politics and the development sector in India and the US. He regularly writes for Policy Perspectives Foundation, Fair Observer, Huffington Post, Indian Military Review, Indian Defence Review, The Quint and The Express Tribune. He has also written an evaluation paper on the counterterrorism committee of the UN. Pandya is currently working as Strategic Advisor with Vidya Bhawan Society, Udaipur.

Cryptocurrencies

A New Scourge of Terror Financing

Abstract

Considered the advanced frontiers of terror-financing, bitcoins have already raised serious concerns regarding the future of the global financial system. Over the last eight years, the use of bitcoins has risen exponentially from an average of 100 transactions per day in 2009, to 282,000 transactions per day in 2017.[1] Understandably, the global counter-terrorism community has expressed serious concerns over the use of cryptocurrencies by the Islamic State[2] and other terrorist groups for terror financing.

Fortunately this trend is still not very widespread. In fact, the evidence of such use is at best anecdotal. However, with the evolution of technology and the sophistication of the much sought-after features of speed, anonymity and non-traceability, and the increasing difficulties in using formal banking systems and hawala, the use of cryptocurrencies for terror-financing might increase and completely alter the landscape of terror financing.

This essay examines some of the recent cases of the use of virtual currencies for terror financing, the factors which may facilitate the use of cryptocurrencies in terror-financing, the current discourse in the counter-terrorism community and the likely future scenario. It will conclude by making a set of recommendations for addressing the challenge.

Funding terror

For about two years now, an underground website, *Silk Road*[3] has been used by several drug dealers, money launderers, and other illicit vendors to deal in drugs and other illegal goods and services. It also offers services in computer hacking, malicious software, fake licences, passports, social security cards, utility bills, car insurance documents, credit card statements and other false identification documents. The site operated on the 'darkweb', an encrypted area of web, with access for only specialised browsers and mostly used by cyber criminals, money launderers, terrorists, dissidents and journalists to avoid detection. It uses TOR (The Onion Router), an encryption software that is needed to access the 'darkweb'. It can be downloaded through the TOR website. It provides online anonymity by hiding the user's IP address[4] and accepts payments in bitcoins.

Any further analysis of the use of cryptocurrencies requires the lay reader to learn the basic difference between the 'darkweb' and the 'deepweb'. As mentioned

above, the 'darkweb' is an encrypted area of web with access only for specialised browsers that is mostly used by terrorists and cyber-criminals. In other words, the 'darkweb' consists of hidden IP addresses that may need a special software to access. The 'darkweb' uses an encryption software that makes the users and location anonymous. Further, the 'darkweb' is a small fraction (0.01 per cent) of the 'deepweb', which contains all the material that is inaccessible through standard search engines[5]. The 'deepweb' usually contains benign sites such as password-protected email accounts, paid subscription services like Amazon Prime and the sites that can be accessed through an online form.[6]

In 2016, the Ibn Taymiyya media centre[7], the online jihadi unit of Gaza, launched social media campaigns to garner funds through bitcoins. Earlier, in June 2015, a Virginia teen was posting instructions on twitter[8] on how to donate to Islamic State (IS) by using bitcoins. In June 2017, the *Wall Street Journal* reported that a Syria-based Indonesian[9] militant was using PayPal and bitcoins to fund the IS, according to the Indonesian security agencies. A jihadist monitoring website reported that an organisation named *Al-Sadaqah*[10] (Arabic for voluntary giving) was soliciting funds to the value of $750 in November 2017 for relief work in Syria. The Al-Sadaqah campaign was circulating through Al Qaida linked social media channels like Facebook and the Telegram messaging app. On November 6, 2017, *Dawaal Haqq*[11] (Arabic–Invitation for Truth), the Islamic news agency and a pro-jihadist website, sought donations on Facebook through bitcoins. In December, pro-IS websites like *Akhbaar-al-Musalmin*[12] (Arabic for news of the Muslims), and *Isdarat*[13] were soliciting funds through bitcoin donations. *Isdarat* can be viewed on the 'darkweb' only through a TOR (The Onion Router) browser and hence is not accessible on the surface web.

What is a cryptocurrency?

Cryptocurrency, also referred to as 'virtual currency' or a 'non-fiat currency', does not have government backing. It does not have the status of a legal tender. The US treasury department's FinCEN (Financial Crimes Enforcement Network) defines virtual currency[14] as " … a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction".

These new forms of currency—with names like Bitcoins, Ripples, Monero and Zcash are very real. They have populated our cyber space. They have the potential to revolutionise the global financial transaction system by bypassing governments, thus making them truly global. They also make huge promises of financial inclusion by extending financial services to unbanked individuals, avoiding complicated paperwork and clerical procedures. However, they also have characteristics that make them highly attractive to cyber criminals, money launderers of all sorts, drug-smugglers and terrorists.

How do they work?

Cryptocurrencies do not exist in the form of physical banknotes or coins. They are created by two methods: (a) the creator decides the number of the units of currency needed, creates them and releases them all at once; (b) the second method is that of bitcoins – which is a complex process of creating currency over a period of time, but the total number of coins that will ever exist is determined *a priori*. Bitcoins are created or 'mined' by working on complicated mathematical codes. Specialised computers and custom-designed chips (called Application-Specific Integrated Circuits or ASICs) are used to solve mathematical problems to mine bitcoins. These days the criminals are also using 'botnets', (a network of compromised computers) to perform the mining calculations. Of late, instances of software applications being developed for mobile devices for mining bitcoins[15] have also come to light.

To buy, sell, or use bitcoins, the user needs a digital wallet which is offered by several organisations (virtual currency exchanges) on the internet. Alan Brill and Lonnie Keane in their paper, 'Cryptocurrencies: The next Generation of Terrorist Financing'[16] , define the digital wallet[17] as a "computer programme that sends, receives and stores the codes that represent the currency". Some organisations also offer 'offline digital wallets' which allow the user to save cryptocurrencies like bitcoins on their personal devices. In case the storage mechanism of the device fails and the wallet is not backed up, the virtual currency may just disappear. For the purpose of authentication, a verifiable email address and a phone number, that can send and receive messages, are needed for setting up a digital wallet. It can even be an anonymous prepaid phone.

After the wallet is set up, one can decide on the amount of virtual currency required and how much it will cost in terms of the real-world currency that the exchange accepts. Payment can be made in the form of a cash deposit to a designated bank and account number. After the bitcoins are acquired they can be stored in the digital wallet associated with the user's bitcoin address, designated by a complex string of letters and numbers. A bitcoin address is similar to a bank account number. It is the only requirement for conducting online transactions of this nature. It does not reflect any identifying information, thus offering complete or pseudo-anonymity. Then, one can use the virtual currency to make payments or receive them. A bitcoin transaction involves transfer of value between the bitcoin wallets and it is recorded in the public ledger, better known as the 'blockchain'[18] . Later, the bitcoins can be exchanged for the sovereign/government currency through a money exchanger.

What makes the virtual currencies attractive to cybercriminals, money-launderers, and terrorists?

The world of crime and terrorism always looks for channels that guarantee anonymity and non-traceability of monetary transactions. Virtual currency offers

anonymity in transactions, as there is no need to produce any document validating one's identity. In the bitcoin network, users are identified by an alphanumeric public key and not by their names. It offers global reach as the system permits any amount of money to be transferred from anywhere to anywhere in terms of physical location. One can be physically present in country A, start a transaction on the internet to convert the national currency of country B via a virtual currency exchange operating in country C, and transfer the virtual currency to a wallet in country D. The cryptocurrency could be transferred to the ultimate user's wallet in country E who might go through the exchange operating in country F and convert it into the currency of country G (Brill, Alan & Keene, Lonnie) Further, it offers speed and non-reversibility which implies that the person sending the money will not be able to 'unsend' it or reverse the order. It is cheap and easy to use, and for the authorities extremely difficult to track the transactions. Further, since it is entirely a computer programme, there is always the potential to enhance the security systems and anonymity in response to the tightening grip of law-enforcement authorities and financial regulatory bodies.

However, hard cash is still the most preferred way for funnelling money. Terrorists use the hawala mechanism[19] for cash transfers because it guarantees anonymity. However, the speed, irreversibility and the instant nature of the transactions offered by the bitcoins gives them an edge over hawala in many ways. There are also several factors that make virtual currencies unattractive to terrorists and criminals. Some of these are:-

- The rapidly changing and unpredictable nature of value of the virtual currencies
- The virtual currency stored in digital wallets is vulnerable to theft, by insiders and hackers both.
- Converting national currencies into virtual currencies and vice versa or to goods and services is always a challenge as it is difficult to find trustworthy organisations that can do it.
- The potential inability to transfer sovereign currencies to or from virtual currencies because of supply, demand and cost issues. It could be that at a particular time when one wants to make a transaction, there is no buyer, at any cost.
- The increasing interest and expertise in virtual currency tracking and the tightening grip of government regulators and law-enforcement authorities.

Current State of Affairs

Notwithstanding the increasing official scrutiny and regulatory oversight, virtual currency is revolutionising the global financial system. China, home to world's largest bitcoin mines[20], is finding it extremely difficult[21] to ban their use. The bitcoin-

charts.com reported that in 2013 itself there were 12 million bitcoins[22] in circulation in China. In India also, bitcoins are driving profiteers crazy.

Sathwik Vishwanath, the founder of Unocoin[23] the bitcoin platform, reported that they were gaining 7000 to 8000 users each day in December 2017. As virtual currency is gaining wide acceptance and popularity, governments have become cognisant of its wide-ranging presence and its potential to change the global financial landscape. They are also fearful that such currencies will be used by criminal groups and terrorists. As observed earlier in this essay, the innovative features of privacy, efficiency, speed, and cost-benefits make cryptocurrencies highly attractive to terrorists and criminals for shifting money outside of the traditional and regulated banking and money transfer services. Digital currencies can be used for general funding, money laundering, to pay for personnel, pay for logistics and other elements of any terror machine. False identification documents like passports, social security cards, and driver's licences, and weapons and explosives can be obtained by using cryptocurrencies on the 'darkweb'.

However, a number of counter-terrorism experts believe that, the use of virtual currencies in terror financing is still not widespread. David Carlisle[24], an independent consultant with the British think-tank RUSI (Royal United Service Institute) opines that so far, the evidence of the use of bitcoin technology in terror financing, remains anecdotal at best. He rules out the possibility of the widespread use of the bitcoin technology by terrorists in the present and in the near future, as they have several other reliable financing streams. He further says that the terrorist could just be 'testing waters[25]' and an 'overreaction could stifle an important new financial technology[26]' . The complaint by Indonesian agencies is the first specific official complaint, about the use of bitcoins in terror financing.

There are several factors which restrict the use of bitcoins by terrorists. First of all, the anonymity offered by bitcoins is only partial. It enables a financial transaction without identifying the user, but it does not allow user privacy. All transactions are recorded in the 'blockchain' ledger which is in the public domain and hence auditable. The law-enforcement agencies and regulatory bodies are able to track such transactions and the money trail can be used to identify the ultimate user.

Secondly, terrorist organisations like the IS used to control huge territories and thus raise money through taxation, extortion, selling antiquities and oil smuggling[27]. The IS has however suffered severe territorial loses and therefore it seems a bit unlikely that it will go for any widespread usage of bitcoin technology for fund transfers in the immediate future. Also, the IS requires huge amounts of money which are difficult to transfer through bitcoin technology.

Thirdly, the IS-controlled regions are war-torn. Hence, there are hurdles in the form of the lack of advanced internet facilities and a network of virtual currency exchanges.

Fourthly, organisations like the Hezbollah, Lashkar-e-Taiba, Jaish-e-Muhammad, Taliban and Hamas mainly depend on state financing[28]. Al Qaida raises money through foreign donations. Further, the Middle East and North Africa, where most of the terrorists presently operate, are under served by advanced internet facilities and virtual currency money exchanges. Furthermore, even the terrorist cadres in the above mentioned areas and another hub of terrorism, i.e. the Af-Pak region, are not tech-savvy enough to work efficiently and comfortably with the bitcoin technology.

Fifthly, the 'lone wolf' attackers in Western countries are self-inspired and mostly self-financed[29]. They need small sums of money which they generally raise through accessible financial services that include student loans, unemployment benefits and cash and payday loans. With such easily accessible financial services, there is no pressing need for them to take recourse to bitcoin technology. Some of them have raised money through kickstarter-like campaigns[30] but the use of virtual currencies for fund-raising is not a very popular option with them.

Sixthly, governments have also responded in myriad ways such as imposing a complete ban on the use of virtual currencies in some cases and bringing the virtual currency world under official oversight and monitoring. In the US, the FinCEN[31], responsible for the enforcement of compliance with the Bank Secrecy Act[32] (BSA), US's counterterrorism and money laundering statute, issued a guidance to clarify the applicability of the regulations implementing BSA to persons "creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies". The new guidelines bring the administrators and exchangers of virtual currencies under the category of money transmitters as defined by the FinCEN. As a result, they will have to fulfil the registration requirements and an array of Anti-Money Laundering Counter -Terror Financing (AML/CTF) provisions of recordkeeping and reporting. They will also have to file Suspicious Activity Reports (SARs) and verify customer identities just like other money transmitters and will have to cooperate with law-enforcement agencies in specific cases of investigation.

Further, the IRS (Internal Revenue Service)[33] Notice (2013-14) defines virtual currencies as property, not as money. It implies that as in the case of other properties, the users of virtual currencies will have to maintain all the records. For example, whenever any user pays a bill in virtual currency, the user will have to calculate the gain and loss on the virtual currency and pay the tax on the gains, if any. Bringing such entities dealing in virtual currencies under the purview of US tax laws will compel them to strictly comply with the requirements of record keeping, failing which they will face criminal and civil penalties.

In 2013-14, Thailand and China took effective measures[34] prohibiting banks from dealing in virtual currencies. The Danish Financial Supervisory Authority issued a warning against the use of virtual currencies. Similarly the Russian[35] and Indonesian central banks[36] also declared bitcoin transactions to be illegal. In other countries, efforts have begun to bring the virtual currency exchanges under the purview of AML/ CTF regime which makes it mandatory for them to comply with customer due diligence and KYC (Know Your Customer) procedures.

Last but not the least, countries leading the counter-terrorism-finance efforts are highly sophisticated and advanced in cyber technology. They have the technological capability to exploit the vulnerabilities of virtual currencies such as the vulnerabilities of the computers used to hacking, social engineering and physical destruction, just like other normal computers.

However, cyber technology is continuously evolving and even terrorist-financing methods are not static. Tightening the AML/CTF regimes and increasing regulatory oversight over conventional channels like hawala might induce the terrorists to shift the financing and transfer of funds to the more anonymous and difficult-to-decipher terrains of the 'darkweb' and virtual currencies. Further, with the evolution of more sophisticated technologies guaranteeing higher degrees of anonymity and user -friendliness, the terrorists may find it convenient, cheaper and risk-free to use crypto-currencies for terrorist financing activities. In addition, territorial losses and shrinking revenue base may compel the IS to adapt to the changing circumstances by adopting bitcoin technology. Similarly, with the advancement of bitcoin technology, the Al Qaida may also shift from using the hawala route to using bitcoins to solicit funds. In fact, most of the reported cases of bitcoin use by terrorists thus far relate to soliciting of donations, as discussed earlier in this essay. Hence, the large-scale adoption of bitcoin technology by terrorists may be the worst-case scenario but, then it can be a reality in the not-so-distant future.

As has been the case with instant messaging apps like WhatsApp, Telegram and Signal, which have continuously upgraded their older versions with more secure and better encryption facilities, virtual currencies can also evolve promising higher degrees of anonymity and privacy. Privacy-enhancing tools like 'Mixers' and 'Tumblers' are already giving a hard-time to law-enforcement agencies. Some of the new virtual currencies like Zcash and Monero[37] - which do not indicate the sent and received amounts and the value transferred on public ledgers - already provide better anonymity and privacy features and are extremely difficult to track. Zcash[38] is expected to offer offline transactions which mean that they will be unrecorded, making it almost impossible to track those money transfers. And such transfers can take place even in areas which lack speedy internet access.

Over time, terrorists will also eventually become adept in handling cyber technologies and the 'darkweb'. They can buy false passports, credit cards, utility bills,

arms, bombs, drones and sensitive data and the other materials in the illicit market on the 'darkweb', using bitcoins and other virtual currencies. False passports could help them cross borders with ease, acquire houses and establish a foothold in the target country. In fact, the process has already begun. For example, 'Fund the Islamic Jihad without Leaving a Trace[39]' is a 'deepweb' page that invites donations for jihad at a particular bitcoin address. A PDF document (posted online) entitled, *bitcoin wa sadaqat al-jihad*[40]" (bitcoin and the charity of the violent physical struggle), is a guide to the use of 'darkweb' for financial transactions. Investigations have revealed that weapons used in the Paris attacks were supposedly acquired from a 'darkweb' store. And, there are reports indicating that the 'darkweb' is also being used by terrorist organisations to sell human organs in the online black markets.

Despite varying motivations, there is a strong possibility that the world of cybercrime and terror may converge for the generation and handling of finances. Cybercriminal groups could launder terrorist money and undertake cyber operations, malware and ransomware campaigns for financing terrorism. Europol has already come across instances of growing cooperation between terrorist groups and the underworld of crime. Yaya Fanusie[41], former CIA counter terrorism analyst, recommends that law -enforcement agencies should look out for the terrorists' technical adaptation and growing nexus with the crime world.

Recommendations

Virtual currencies present a grave challenge to international security and intelligence communities and their efforts to disrupt and dismantle terror-financing infrastructures. In fact, virtual currencies represent the advanced frontiers of terror financing. Due to the anonymity, speed and instantaneous nature of the transactions, it is difficult for counter-terrorism analysts to track such illicit activity. Though the worst-case scenario has not unravelled yet, it can be a fast approaching reality. In response, some countries have already banned these and others have tried to bring these under regulatory oversight, as discussed above in the article.

Experts have made some recommendations for developing robust mechanisms for tracking and preventing the use of virtual currencies for terror financing. Alan Brill and Lonnie Keane recommend adopting an investigative[42] approach for tracking virtual currency transactions. They suggest that governments and inter-governmental bodies must invest in the training and upgrading of the cyber technology skills of counter-terrorism analysts, to address the challenge of the use of virtual currencies in terror financing. They must build an expert-cadre that understands the nuances of virtual currency transactions as cryptocurrencies are not yet totally anonymous. They are still pseudo-anonymous and there are various data points that could enable experts to track such transactions and identify the end users. For example, virtual currency transactions need third-party mediation which is a worldwide peer-to-peer network of partici-

pants, who validate all transactions. In such a decentralised accounting system, each network participant has to maintain the entire transaction history online.

One, in the case of bitcoins, the ledger recording all the transactions i.e. the blockchain is public. Following the trail of such online transactions can be immensely helpful in tracking the human actors behind them. Further, the money exchanges dealing in virtual currencies are always a point of vulnerability. In the case of the 'Silk Road' also, the exchanges were the weak link. In January 2014, the US Attorney's Office for the Southern District of New York initiated legal proceedings[43] against the bitcoin exchange service operator, Robert Faiella[44] for running an exchange service directly on Silk Road[45] which helped the users convert the cash into bitcoins anonymously (Brill, Alan, Keene, Lonnie; Page 21). In case of inter-exchange transactions, the trail between digital wallets is in the public domain and can be successfully used for tracking the terror financing machinery. However, transactions between parties on a single private exchange are not available on the global transaction directory for public consumption. Hence, intelligence agencies are advised to keep a tab on the activities of the existing and emerging underground private exchangers. Further, during investigations, the exact time of the transfer and the amount of the transfer can also provide robust links and clues for the overall investigation. Last but not the least, the regulatory agencies should also factor in the problem of the volatility of the companies that could be used as evidence. For example, largest Bitcoin exchange Mt.Gox, based in Tokyo, suddenly suspended all virtual and real exchanges and filed for bankruptcy. It claimed that hackers had stolen millions of dollars' worth of bitcoins[46]. The takeaway for the investigators is that they should always be aware that the companies they are looking for as evidence are volatile and they might not be there when they are required as evidence. The main lesson of this example for governments is that they have a major responsibility to regulate the cryptocurrency market to capitalise on the gains and avoid the negatives of the technology.

Two, in the wake of the terrorist migration to the 'darkweb[47]' there is an acute need for crafting sophisticated and advanced tools to track and monitor the illicit activities on the 'darkweb' by terrorist and criminal elements. For example, the DAPRA[48] (American Defence Advanced Research Projects Agency), uses MEMEX[49] (search engine for the deepweb) software for the better cataloguing of deep websites[50]. It was originally developed to track human trafficking activities on the 'deepweb' but by the same logic, the software can also be used to track other illegal activities on the 'deepweb'.

Three, the FATF (Financial Action Task Force) recommendations[51] for countering money laundering and terror financing need to be updated to bring virtual currencies within their ambit. Its latest recommendations include nine special items for combat terror financing. As an inter-governmental body, it can play a very effective role in coordinating the efforts of the world community for checking the use of virtual cur-

rency for terror financing. It can disseminate a standard template of the best practices for the tracking, reporting, and monitoring of suspicious virtual currency transactions and help, prevent its use in terror financing.

Four, creation of non-governmental and self-regulatory organisations at the national and international levels will ensure freedom, or rather a semblance of freedom, from government interference, as generally sought by the virtual currency community. And, they can enforce the consumer protection and transactional integrity norms and rules agreed upon by cryptocurrency users in a particular country and its official regulatory bodies[52].

Five, enhance cooperation, knowledge-sharing, and skills-sharing between the agencies involved in combating terrorist financing. Such cooperation at the international level, facilitated and coordinated by an inter-governmental body like FATF, can be immensely helpful in synergising efforts in the field of data collection and analysis to produce optimum results.

Six, it is recommended that agencies should keep a vigil on the emergence and evolution of new virtual currencies and private underground exchanges dealing in virtual currencies. Non-compliant private exchanges, those who do not abide by anti-money laundering and KYC practices, are likely to emerge in regions with weak regulatory structures such as parts of Africa and the Middle East. The intelligence agencies should keep a close watch on such regions. The idea behind this suggestion is that the creation of new virtual currencies and private exchanges is generally undertaken by individuals and organisations engaged in money laundering and cyber-crime looking for better anonymity, speed, and user-friendliness. Hence a close watch on such entities can be very useful in tracking their activities.

Seven, intelligence agencies should also keep an eye on organisations targeting recruits with high levels of computer science skills.

Eight, a broad range of laws dealing with financial and cybercrimes provide ample scope for bringing offenders within the ambit of law. It may not be possible to take the bull by its horns, i.e. prove the direct involvement of funds and individuals in terrorism, but the options of dealing with such entities through tax laws and regulatory violations can be a very effective tool for deterring their actual activities.

None, security and regulatory agencies can coordinate with Internet Service Providers (ISPs) to collect information about individuals who download encryption software like TOR. But there are chances of abuse since the state might use these to crackdown on political activists who also use encryption software. However, in a democratic country activists have the freedom to operate so they do not seek high levels of anonymity. The encryption software is mostly used by criminals, so the method recommended above could prove useful.

Conclusion

Bitcoin technology has already sent tremors through the global financial order. There is widespread use of bitcoins in diverse environments. In some places, they provide attractive investment opportunities whereas in others it has been used to buy a pizza or a plane ticket. The price of one bitcoin is about $20,000. Besides, bitcoins offer a truly global financial system. They offer tremendous potential for financial inclusion by providing the banking and financial services to the unbanked and underbanked population. Hence, the reality, the increasing popularity and the revolutionising potential of this technology cannot be denied. However, the same features also make it an extremely useful channel for the criminals and terrorists. Besides this, there are inherent risks in the use of virtual currencies. Hacking, the irreversibility of payments and the lack of human interface makes it a risky venture. The collapse of Mt.Gox, the bitcoin exchange of Tokyo with the loss of millions of dollars, is an example of such inherent risks. Some countries have gone for the outright banning of such currencies, but banning this technology can only be a temporary option and at best an anti-evolutionary reaction.

The challenge for governments is to harness the advantages offered by the technology in terms of financial inclusion and fast, safe and low-cost global fund transfers; but at the same time prevent its abuse by cybercriminals, money launderers, and terrorists. Governments will have to be sensitive towards the double-edged nature of this technology and continue to develop sophisticated skill-sets to track and counter suspicious transactions.

India: A Special Case

India is in a unique position in that it provides a fertile ground for all kinds of illicit activities on the 'darkweb', including money laundering and terror financing through virtual currencies. India has better internet infrastructure in terms of equipment, connectivity, attitudes and skills, as compared to the Middle East and Africa and is witnessing a fintech boom. The *Fair Observer*[53], a US-based global media outlet, observes that explosion of smartphone users and a world-class digital infrastructure are fuelling the rapid growth of fintech in India. Online payment systems like PayTM, Google Tez, UPI[54] (United Payments Interface), Samsung Pay and Amazon Pay have populated the transactions domain. A Google and Boston Consulting Group (BCG) report titled *Digital Payments 2020*[55] states that digital payments in India will exceed $500 billion by 2020, up from $50 billion in 2016.

The bitcoin bubble has also taken the Indian market by storm, as discussed earlier in this essay. Zebpay, a bitcoin exchange[56], reported that in the last months of 2017 they were adding 300,000 to 400,000 users on its exchange every month, as compared to 150,000 in June and July. A multitude of factors such as the inefficient banking system, huge profits, a large unbanked and underserved population, deep smartphone

penetration, increasing access to internet, a booming e-commerce market and a large talent pool which understands both technology and financial services, are driving people towards the online payments systems and the bitcoin technology.

However, at the same time, India already has a flourishing grey market and underground economy where all kinds of illicit materials including weapons, drugs and other materials can be easily bought. The Bitcoin technology makes it easier, faster, safer and even comfortable for such an underground economy to operate. Moreover India's financial regulatory structures, and AMP/CTF monitoring and surveillance capabilities are not sufficiently developed. The law-enforcement agencies and intelligence agencies are understaffed, poorly equipped and insufficiently skilled to tackle such high-tech cases of cyber fraud and disruption[57].

In most Indian states, the state of cyber cells is pathetic and the general awareness of technology among the officer cadre and the lower-level functionaries is not up to the mark. Additionally, over the years, the grip of the AML/CTF regime over the formal banking system and conventional money-transfer systems such as hawala and MSBs has strengthened. Hence, there is a strong likelihood of criminal and terrorist elements migrating to the 'deepweb' and shifting to bitcoin technology.

In this background, the following measures are strongly recommended for consideration:-

- Investing heavily in raising a skilled and smart cadre of tech-savvy analysts and officers to respond to the fast-evolving technology. The official agencies will always have to be ahead of the criminal world in technological terms.
- Creating a high-tech intelligence and counter-terrorism infrastructure by roping in experts from finance, technology, geopolitics and behavioural psychology with razor-sharp intuitive analytical skills and a profound understanding of the nuances of crime and terror world. This needs out-of-the-box thinking and the willingness to break the shackles of convention.
- The states need to create robust cyber cells and financial crime units. Most state level police and administrative officers have an extremely poor understanding of terrorism issues and least of all terrorism financing.

Is India ready and willing to break the status quo? It's a difficult question to answer. The current system of hiring spies, police officers, diplomats, and finance officers though a colonial-era system based on the one-size-fits-all dictum, leaves no space for innovation, creativity, and specialisation. Certainly, in our sense, we cannot wait for another bomb to go off.

End Notes:

1. Micah Zenko, "Bitcoins for Bombs," Council on Foreign Relations. August 2017. Accessed April14 2018 https://www.cfr.org/blog/bitcoin-bombs
2. Ian McKendry, "ISIL May be Using Bitcoins, FinCEN's Calvery Says," *American Banker*. November, 2015. https://www.americanbanker.com/news/isil-may-be-using-bitcoin-fincens-calvery-says
3. Hope Reese, "How the founder of the Silk Road made millions on his illegal startup on the Dark Web?," *Tech Republic.* May 2017. https://www.techrepublic.com/article/how-online-marketplace-silk-road-became-the-craigslist-for-illegal-drugs/
4. Andy Greemberg, "The Grand TOR-How To Go Anynymous Online?," *Wired.* September,2017 https://www.wired.com/story/the-grand-tor/
5. Cydney Granan, "What's The Difference Between the Deepweb And the Darkweb?," *Encyclopedia Britannica.* Accessed July 14 2018 https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web
6. Ibid.
7. Levi Maxey, "Terror Finance in the Age of Bitcoin," *The Cipher Brief.* June 2017. https://www.thecipherbrief.com/article/tech/terror-finance-age-bitcoin
8. The United States Department of Justice. https://www.justice.gov/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil
9. Resty Woro Yuniyar, "Bitcoin, PayPal used to Finance Terrorism, Indonesian Agency Says," *Wall Street Journal.* January 2017. Accessed April14 2018 https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198
10. Yaya Fanusie, "Terror Networks Eye Bitcoin as Cryptocurrency's Price Rises," *The Cipher Brief.* December, 2017. https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises
11. Ibid.
12. The Meir Amit Intelligence and Terrorism Information Center, "Drive for Bitcoin Donations on an ISIS Affiliated Website," December, 2017. http://www.terrorism-info.org.il/app/uploads/2017/12/E_235_17.pdf
13. Fn x.
14. United States Department of Treasury. FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies," Accessed April 14 2018 https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering
15. Chris Brook, "Google Removes Bitcoin Mining Android Malware from Play," *Threat Post.* April 2014. https://threatpost.com/google-removes-bitcoin-mining-android-malware-from-play/105740/

16. Alan Brill & Lonnie Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing*," Defense Against Terrorism Review.* COE-DAT. 2014. http://www.coedat.nato.int/publication/datr/volumes/datr9.pdf

17. Coin Base Support, "What is a Bitcoin wallet?," Accessed April 14 2018. https://support.coinbase.com/customer/portal/articles/1831937-what-is-a-bitcoin-wallet-

18. Fn xvi.

19. Abhinav Pandya & C.D. Sahay, "Terror Financing and the Global CTF Regime," Vivekananda Foundation. January, 2017. http://www.vifindia.org/occasionalpaper/2017/january/27/final-terror-financing-and-the-global-ctf-regime

20. Joon Ian Wong, "Chinese money dominates Bitcoin, now its companies are gunning for Blockchain tech," Quartz. Oct.2017. https://qz.com/1072907/why-china-is-so-hot-on-bitcoin/

21. Gabriel Wildau, "Bitcoin proves hard to kill in China," *The Financial Times*, November, 2017. Accessed 14 April 2018 https://www.ft.com/content/d576e4e4-c374-11e7-a1d2-6786f39ef675

22. Olga Kharif, "Bitcoins Climb to Record on Wider Acceptance, China Trade," *Bloomberg Technology*. November, 2013. Accessed April 14 2018 https://www.bloomberg.com/news/articles/2013-11-06/bitcoin-climbs-to-record-on-wider-acceptance-china-trade

23. Kat Hopps, "Bitcoin News: Is crypto banned in India? Is cryptocurrency legal in India? ," *Express.* February. 2018. Accessed April14 2018 https://www.express.co.uk/finance/city/918028/Bitcoin-news-is-cryptocurrency-legal-India

24. David Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic," *RUSI.* March 2017, Accessed April14 2018https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic

25. Ibid.

26. Ibid.

27. Peter R Neumann, 'Don't Follow the Money," F*oreign Affairs*. July/August 2017. https://www.foreignaffairs.com/articles/2017-06-13/dont-follow-money

28. Ibid.

29. David Manheim, Patrick Johnston, Josh Baron, and Cynthia Dion-Schwarz, "Are Terrorists Using Cryptocurrencies?," *Foreign Affairs*. February 2018. https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies .

30. Ibid.

31. Fn xvi.

32. US Department of Treasury, "BSA and Related Regulations", https://www.occ.treas.gov/topics/compliance-bsa/bsa/bsa-regulations/index-bsa-regulations.html

33. Ibid.

34. Fn xvi.
35. Sam Bourgi, "Russia bans Bitcoin exchanges, according to central bank," *Hacked.* October, 2017. https://hacked.com/continue-reading/
36. Reuters, "Indonesia bans use of Bitcoins, other virtual currencies," February, 2014. Accessed April14 2018 https://uk.reuters.com/article/uk-indonesia-bitcoin/indonesia-bans-use-of-bitcoins-other-virtual-currencies-idUKBREA150HV20140206
37. Fn vii.
38. Fn xxix.
39. Gabriel Weimann, "Terrorist Migration to the Dark Web," ***Perspectives on Terrorism***. June, 2016. Accessed April14 2018 http://www.terrorismanalysts.com/pt/index.php/pot/article/view/513
40. Fn xxxix.
41. Fn vii.
42. fn xvi.
43. Fn xvi.
44. US Office of the Attorney of the Southern District of New York https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-bitcoin-exchangers-including-ceo
45. Benjamin Weiser, "Ross Ulbricht, Creator of Silk Road website, is Sentenced to Life in Prison," *New York Times.* May 2015. Accessed April14 2018 https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html
46. CCN, "$400milliom hack, Japanese Cryptocurrency exchange Halts Withdrawals as theft Rumors Mount," Accessed April14 2018 https://www.ccn.com/400-mil-hack-tokyo-based-crypto-exchange-halts-withdrawals-prices-sink/
47. Fn xxxix.
48. Richard, "Deep Web Search Engine "MEMEX" Boost Up*," Dark Web News*. June 2018. Accessed July 12 2018 https://darkwebnews.com/deep-web/deep-web-search-engine-memex-boost/
49. Wade Shen, "MEMEX," Defense Advanced Research Projects Agency. US Accessed July12 2018 https://www.darpa.mil/program/memex
50. Fn xlviii.
51. FATF, "International Standards on Combating Money Laundering and Financing of Terrorism and Proliferation-the FATF Recommendations," Accessed May14 2018 http://www.fatfgafi.org/publications/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html

52. Fn xvi.

53. Knowledge Wharton, "What's Driving India's FinTech Revolution?," *Fair Observer*. February, 2018. http://www.fairobserver.com/region/central_south_asia/india-fintech-whatsapp-tech-news-headlines-today-30980/

54. Ibid.

55. Boston Consulting Group, "Digital Payments 2020," July 2016.Accessed July 12 2018 http://image-src.bcg.com/BCG_COM/BCG-Google%20Digital%20Payments%202020-July%202016_tcm21-39245.pdf

56. Nupur Anand, "The Ongoing Bitcoin Boom is Drawing Indian Investors like Never Before," *Quartz*.November,2017. https://qz.com/1141021/the-bitcoin-boom-is-drawing-indian-investors-like-never-before/

57. Abhinav Pandya, "In India, Wahabi Extremism is a Ticking Timebomb,"*Swarajya* . Accessed July 12 2018 https://swarajyamag.com/politics/in-india-wahhabi-extremism-is-a-ticking-time-bomb.

(*The paper is the author's individual scholastic articulation. The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to be correct).*

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org, Website: http://www.vifindia.org
Follow us on twitter@vifindia