# Correlation of Cyber Crime and Demonetization

**Shruti Bajaj[1], Dr. Rajesh Kumar Singh[2]**
**PHD STUDENT[1], PRINCIPAL[2]**
**PUNJAB TECHNICAL UNIVERSITY KAPURTHALA[1], SUSCET TANGORI MOHALI[2]**

***ABSTRACT***
*Cybercrime is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Issues surrounding these types of crimes include hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming. Cyber security is the area that deals with protecting from cybercrime. It requires coordinated efforts throughout an information system. This paper discusses the correlation of Cyber Crime and Demonetization and also the impact of demonetization on Cyber Crime. Cyber security is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide. Demonetization is the act of stripping a currency unit of its status as legal tender. It occurs whenever there is a change of national currency. The current form or forms of money is pulled from circulation and retired, often to be replaced with new notes.*

**Keywords- Cybercrime, Cyber security, Demonetization.**

## I.INTRODUCTION

Cybercrime, or computer crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copy infringement unwarranted mass-surveillance, child pornography, and child grooming. [1]

In 2016, the Indian government decided to demonetize the 500- and 1000- rupee notes, the two biggest denominations in its currency system; these notes accounted for 86% of the country's circulating cash. With little warning, India's Prime Minister Narendra Modi announced to the citizens on Nov. 8 that those notes were worthless, effective immediately – and they had until the end of the year to deposit or exchange them for newly introduced 2000 rupee and 500 rupee bills.

Chaos ensued in the cash-dependent economy as long, snaking lines formed outside ATMs and banks, which had to shut down for a day. The new rupee notes have different specifications, including size and thickness, requiring re-calibration of ATMs: only 60% of the country's 200,000 ATMs were operational. Even those dispensing bills of lower denominations faced shortages.

The government's goal was to combat India's thriving underground economy on several fronts: eradicate counterfeit currency, fight tax evasion, eliminate black money gotten from money laundering and terrorist-financing activities, and to promote a cashless economy. Individuals and entities with huge sums of black money gotten from parallel cash systems were forced to take their large-denomination notes to a bank, which was by law required to acquire tax information on them. [2].

The rest of the paper is organized as follows. Cyber security in the time of demonetization is explained in section II. Effect of demonetization in India is presented in section III. Human impact of demonetization in India is explained in section IV. Concluding remarks are given in section V.

**II. CYBER SECURITY IN THE TIME OF DEMONETIZATION [3]**

People with polarized opinions argued it out with each other, debating the pros and cons of the move. People are only bothered about the lack of currency in the banks and ATM machines but completely silent over the cashless hurricane that awaits them. Twitter accounts of a few celebrities were hacked and the media portrayed it as if this was the worst cyber-attack that could happen. The vast experience in cyber security reveals that it is certainly done by some local actor to create media buzz or political turbulence.

Although important, these are not the kind of attacks we need to be worried about. The people in India are yet to experience the worst of the cyber-attacks. Consider a situation when people start losing their hard-earned money to lone wolf hackers targeting individual consumers, because they lack even basic knowledge to protect their online accounts, e-wallets, or debit cards from unsophisticated social engineering or phishing attacks. At the same time, imagine the chaos that would result from the breaches at major banks by the organized cybercrime groups.

These criminal gangs would exfiltrate customer data and possibly even transfer the real money from their high net worth customer accounts to the accounts outside the country. These groups could even bring the banks down to their knees thus collapsing financial infrastructure if immediate actions are not taken by the government, banking sector as a whole, and each individual bank.

These are just two kinds of the threats which India is vulnerable to. In addition, it is also equally susceptible to other kinds of major cyber threats faced by other countries. First, the cyber espionage that involves unauthorized intrusions into government and corporate networks to steal sensitive information of strategic or commercial value from organizations like ISRO or DRDO. Second, the cyber-attacks by the state and non-state actors aimed towards causing temporary disruptions of networks and services like Sensex or telecommunication systems. Third, cyber war, which is a systematic, large-scale assault carried out on critical infrastructures to render them dysfunctional, have a debilitating impact on dependent services like power systems in one or multiple metro cities or a large-scale attack on banking systems and ATMs, bringing them to a grinding halt, and leading to widespread panic and chaos. The National Cyber Security Policy 2013 falls short of what is required to develop an effective cyber security capabilities.

**2.1 Disjointedness of Cybercrime-**

The disjointedness of the National Cyber Security Policy 2013 is palpable from the stark contrast between the vision, objectives, and the strategy to achieve them. The policy does not lay out concrete measures that need to be undertaken to achieve the stated objectives. The first and foremost objective is to protect information infrastructure in cyberspace through reduction of vulnerabilities. Yet, the strategy does not lay out any concrete plan for CERT-In for real-time identification and patching up of vulnerabilities. The CERT-In maintains a database of the vulnerabilities, which in no means is real-time.

The policy calls for protection of 'National Critical Information Infrastructure' by creating a national and sectoral 24x7 mechanism through National Critical Information Infrastructure Protection Centre (NCIIPC). Three years have passed since the adoption of the policy and the NCIIPC is still in its infancy working under the aegis of National Technical Research Organization (NTRO). The policy even fails to identify what sectors will come under critical infrastructure. While in the United States, the law has clearly identified 16 sectors under critical infrastructure, whereas in India none of the infrastructure has been identified as critical. The debit card breach that occurred in the month of October and affected 3.2 million consumers is a glaring example of the costs cybercrime can impose on financial institutions and the individual consumers.

The cyber security policy calls for early threat warning and vulnerability management. However, it fails to talk about a centralized threat intelligence platform that would enable sharing of cyber threat

information in real time among different organizations, thus empowering them through real-time cyber situational awareness. The policy talks about inculcating cyber awareness and building cyber security manpower of around 5,00,000 through education and training, yet neither a concrete plan has been outlined on how to build it, nor any action has been taken to build the cyber warriors pipeline. The policy also does not talk about promoting indigenous solutions to the cyber threats that India faces.

### 2.1 To catch up with cybercrime India needs to perform the following steps [3]-

The cyber threat that India faces is not merely potential in nature but real with high risk. To catch up with the threat, India needs to undertake some essential steps:

- India should develop a centralized threat intelligence platform through public-private partnership because of the efficiency and expertise that private sector brings with itself. The platform can be clustered based on group of organizations in a particular sector facing similar threats. For example, in banking sector, government could partner with existing global information sharing networks like Financial Services Information Sharing and Analysis Center (FS-ISAC) for sharing threat and vulnerability information with peer banks, conduct contingency planning exercise and enhance collaboration among other banks.
- In fact, earlier this month, FS-ISAC and Monetary Authority of Singapore (MAS) announced that they will collaborate to establish an Asia Pacific (APAC) Regional Intelligence and Analysis Centre to encourage regional sharing and analysis of cyber security information within the financial services sector. The establishment of the center will strengthen the APAC cyber security ecosystem by providing deeper capabilities in cyber intelligence gathering and analysis for enhanced in-region intelligence support.
- Additionally, the government needs to overhaul this space by introducing a cyber-framework that matches global standards. They reduce the scope for innovation and force compliance. But to have a sustainable system, there needs to be some baseline for banks and other critical infrastructure sectors to implement foundational cyber controls. There should be a starting point and given the lack of interest in cyber security among organizations in India thus far, the government needs to take the first step. A similar approach was followed in the United States when banking regulators proposed FFIEC guidelines to introduce risk management framework for financial institutions.
- Several cyber bills have been introduced in the US Senate and House in the past decade. Last year, US Congress passed a cyber-security information sharing bill, known as Cyber security Act of 2015, which required certain government agencies to share cyber security threat information with private entities and develop a strategy to ensure that a cyber-incident affecting critical infrastructure entities will not result in catastrophic regional or national effects on public health or safety, economic security, or national security
- Finally, programmes like Digital India and the goal of cashless economy cannot be successfully achieved unless the common man is aware of cyber issues. In India, 82 percent of the population is vulnerable to physical disasters but 100 percent to cyber disaster, because people lack basic cyber awareness. A systematic campaign needs to be undertaken for inculcating cyber awareness among the Indian public especially the rural people.

## III. EFFECT OF DEMONETIZATION IN INDIA

### 3.1. Demonetization foils cyber criminals plans (Pune) [4]-

The increasing inaccessibility to ATMs and more user vigilance since the government decided to demonetize Rs 500 and Rs 1,000 notes has ruined the plans of most cyber criminals. There has been a sudden dip in the number of complaints on digital transaction frauds with the Pune cybercrime cell since demonetization. This, despite an increase in the usage of credit, debit cards and net-banking payments.

### 3.2. Cybercrime cases shoot up post demonetization (Hyderabad) [5]-

As the month of December draws to a close, the rate of cybercrimes that was considerably low before demonetization is rising sharply, said by cybercrime cops. "Following demonetization, many people were forced to take to online payments to meet their daily needs. Mobile wallets like Paytm have witnessed a spike in their user base. Post-demonetization of the Rs 500 and Rs 1,000 notes, a majority of banks, mobile applications and e-wallets have been targeted by scamsters," said Pavan Duggal, a supreme court advocate and an expert in cyber law.

### 3.3. Crime branch gears up to deal with cybercrimes after demonetization (Cuttack) [6]-

Anticipating cybercrimes after demonetization, the state crime branch has geared up to deal with the situation. Crime branch on Saturday organized a special training programme to make police personnel aware about the emerging forms of cybercrime in the age of cashless economy and ways to deal with such cases in an efficient manner. After demonetization, cashless economy has become the buzzword. Even Centre and state governments are encouraging people to make maximum use of credit cards, debit cards, internet banking and digital payment solutions. In such scenario, crime branch strongly anticipates a sudden spurt in cybercrimes and has started preparations to tackle the situation.

### 3.4. Cybercrime rate drops post demonetization in city (Vishakhapatnam) [7]-

Post demonetization of Rs. 500 and Rs. 1000 notes, the Cyber Crime Police station here expected a spurt in the cybercrime rate. But it turned out to be the other way round. “There is sudden drop in the cybercrime rate and in the last 10 days no fresh case has been reported. In normal times, we would record at least two cases per day”, Inspector of Cyber Crime Police Station K. Satyanarayana Rao said. After notifying that Rs. 500 and Rs. 1,000 notes would no longer be legal tender there has been a huge rush at the banks to exchange the old notes and withdraw small change. “Many have switched to online banking to save time and avoid the rush, and this prompted us to be cautious, as there were many first time online bankers, who included senior citizens and from rural areas.

According to Head of the Department of Computer Science of Andhra University College of Engineering P.V.G.D. Prasada Reddy, online transactions would increase from now and cyber criminals will be on the prowl. Apart from securing the systems, the process must be more user-friendly. The authorities concerned should think of incorporating regional language in the user interface. Rural people will benefit from this move, he said. Moreover, to make the system simpler and security-proof, the interface should also be made voice enabled. This apart, the government should now also think of organizing mass training camps to educate the people, especially the rural people, to enable them to use the online system more securely, said Prof. Prasada Reddy. As per the National Crime Record Bureau Visakhapatnam city, has been ranked second after Bangalore in the country to record maximum number of cybercrimes since 2011[7].

### 3.5. Cybercrimes up by 51 per cent in India, Maharashtra, AP, Karnataka top list (New Delhi) [8]-

Andhra Pradesh, Karnataka and Maharashtra have occupied the top 3 positions when it comes to cybercrimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries. According to the latest report by National Crime Records Bureau (NCRB) for the previous year - 2013, 681 cybercrime

related cases have been registered in Maharashtra, which has seen a 44.6 per cent rise in cybercrimes when compared to 2012.

Andhra Pradesh with 635 cases registered in 2013 has also seen a 48 per cent rise when compared to 2012. Karnataka with 513 cases registered in 2013 has seen a 24.5 per cent rise when compared to 2012. Uttar Pradesh with 372 cases registered in 2013 is in the fourth place. It has seen a huge rise of 81.5 per cent in just one year. Kerala is in the 5th place with 349 cases registered in 2013.

Among the bigger states Tamil Nadu and Bihar have very few cybercrime related cases. Just 54 cases have been registered in Tamil Nadu and just 23 cases have been registered in Bihar in 2013. Gujarat and Odisha have also registered just 61 and 63 cases respectively in 2013. In a positive development, the Northeastern states of Mizoram, Nagaland and Sikkim have not seen a single cybercrime related cases in 2013.

**3.6. Demonetization clicks as not one cybercrime plain in last 10 days (Thane) [9]-**

Demonetization seems to have caused a dip in online fraud cases as not a single complaint has been registered. "After the government ban on Rs 500 and Rs 1,000 notes, many citizens have started using plastic money. They have also started visiting their banks on a regular basis and keeping a check on their account books to exchange or deposit money. Also, they have been in constant touch with the banks. Owing to this there have been no fraud calls by common posing as bank representatives calling to ask people's bank account details or telling them that their cards have expired," said Sanjay Sawant, senior inspector from the Thane cyber cell.

## IV HUMAN IMPACT OF DEMONETIZATION [10]

**4.1. Black money-**

At one stroke the Prime Minister has choked the supply of black money stacked inside the country. Of the Rs 17 lakh crore of total currency in circulation in the country, black money is estimated at mind-boggling Rs 3 lakh crore. Black money is nothing but a plunder of the nation. Black money operators run a parallel economy which shakes the very foundation of the Indian economy. With Modi's demonetization move, all domestic black money will either be deposited into the banks with heavy penalty or be simply destroyed.

**4.2. Economy-**

Demonetization will have a huge resultant effect on the Indian economy. The clean-up of illegal cash will help turn around the economy. First, it will bring more borrowings to the exchequer, improve inflation outlook and increase India's gross domestic product (GDP). Second, it will revive investment opportunities and give a fillip to infrastructure and the manufacturing sector. Third, it will help reduce interest rates and lower income tax rate.

**4.3. Note bank politics-**

In the run up to the crucial assembly elections in Uttar Pradesh, Punjab, Goa and Uttarakhand, Prime Minister Modi's demonetization announcement has come as a shock and awe for the political parties and politicians for whom black money is a lifeline. The pulling out of the old Rs 500 and Rs 1,000 currency notes will help make the election process clean and transparent. But it has brought tough times for the political parties and politicians who believe in the idea of purchasing votes in exchange for notes.

**4.4. Real estate cleansing-**

It is said that real estate is an industry built on black money. The extent of black money floating around in the sector is huge. According to an estimate at least 40 per cent of real estate transactions in Delhi-NCR are in black. Modi's demonetization move will curtail the flow of black money into the real estate sector. This will help in making the much needed correction in the sector.

**4.5. Hawala transactions-**

Demonetization has crippled the hawala rackets. Hawala is a method of transferring money without any actual money movement. Hawala route is used as a means to facilitate money laundering and terror financing. Hawala rackets run again on black money. With black money suddenly being wiped out of the market, thanks to demonetization, hawala operations have come to a grinding halt. According to an India Today report, one of the hawala operators in Mumbai has destroyed currency notes worth about Rs 500 crores.

**4.6. Counterfeit currency-**

Demonetization has dealt a death blow to the counterfeit Indian currency syndicate operating both inside and outside the country. Counterfeit currency seriously devalues the real worth of Indian currency. A study conducted by Indian Statistical Institute, Kolkata on behalf of the National Investigation Agency suggests that fake Indian currency notes amounting to Rs 400 crore are in circulation in country at any given point of time and around Rs 70 crore fake notes are pumped into Indian economy every year. The estimation is based on recovery and seizure made by various agencies. But the actual figure could be much larger. A One India report, quoting an Intelligence Bureau dossier, says fake Indian currency worth Rs 12 lakh crore has pumped into Indian financial system over the years.

**4.7. Terror financing-**

Terror financing is sourced through counterfeit currency and hawala transactions. This is how terror financing works. Fake currency circulation is routed through a multi-layered network of hawala operators which are closely linked to satta and smuggling of drugs, opium and arms. Indirectly, they all end up financing terrorism. In addition, the terrorists collect huge donations and then route the money through hawala transactions.

**4.8. Maoism-**

Maoist sympathizer's call Modi's demonetization move an "undeclared financial emergency". There are reasons to it. Demonetization has hit the Maoists and their movement hard. Black money is the oxygen for Maoists. According to an estimate, Maoists manage to raise Rs 300 to Rs 400 crore annually through donations, levy and extortions. The illicit money is used to purchase arms and ammunition, food and medicine and daily essentials, apart from distributing it among the ranks and the cadre.

**4.9. Kashmir unrest-**

The four-month-long unrest in Kashmir valley is on a backburner, thanks to demonetization. No stone pelting on security forces has been reported in Kashmir ever since the demonetization announcement was made. An intelligence estimate suggests that Pakistan sends Rs 1,000 crore annually to the separatists for fuelling unrest in Kashmir. The money is transferred through hawala route.

**4.10. North-East insurgency-**

Demonetization has severely affected the multiple militant groups operating in the North-East. According to intelligence estimate the north-eastern insurgent groups together have a corpus of Rs 400 crore annually.

## V. CONCLUSION

The idea of demonetization is good but it has to be taken into consideration that most of the **black money is kept in the form of land, buildings or gold or kept abroad.** Demonetization is an established practice in monetary policy to tackle black money. The Prime Minister has explained why this is a financial surgical strike. It was meant to be suddenly implemented. In the past, demonetization has taken place twice but it fails because the idea is to tackle the black money existing in circulation. **India is also largely a cash economy. The cash transactions in this economy are far more than the total number of electronic transactions done on a daily basis**. The black money in circulation is like a steroid in the economy which keeps the demand going gives a feeling that everything is working well**. The problem is that investment is not taking place in the economy and the rate of growth of capital**

**formation is down. The only way to bring this up is to divert more funds into investments which will happen when the cost of capital comes down.** So far, it can be said that this is a historical step and should be supported by all. One should look at the bigger picture which will definitely fetch results in the long term in future.

**REFERENCES**

[1] [Online].Available: https://en.wikipedia.org/wiki/Cybercrime.
[2] [Online].Available:http://www.investopedia.com/terms/d/demonetization.asp.
[3][Online].Available:https://yourstory.com/2017/01/cyber-security-in-the-time-of-demonetisation/.
[4][Online].Available:http://timesofindia.indiatimes.com/city/pune/Demonetisation-foils-cyber-criminals-plans/articleshow/55780057.cms.
[5] [Online].Available:http://timesofindia.indiatimes.com/city/hyderabad/Cyber-crime-cases-shoot-up-post-demonetisation/articleshow/56129277.cms.
[6] [Online].Available:http://timesofindia.indiatimes.com/city/bhubaneswar/crime-branch-gears-up-to-deal-with-cyber-crimes-after-demonetisation/articleshow/56039764.cms.
[7] [Online].Available:http://www.thehindu.com/news/cities/Visakhapatnam/Cyber-crime-rate-drops-post-demonetisation-in-city/article16677201.ece.
[8] [Online].Available:http://www.news18.com/news/india/cyber-crimes-up-by-51-per-cent-in-india-maharashtra-ap-karnataka-top-list-698814.html.
[9] [Online].Available:http://timesofindia.indiatimes.com/city/thane/Demonetization-clicks-as-not-one-cyber-crime-plaint-in-last-10-days/articleshow/55501637.cms.
[10][Online].Available:https://www.google.co.in/webhp?sourceid=chromeinstant&rlz=1C1NHXL_enIN729IN729&ion=1&espv=2&ie=UTF-8#q=patriot.