INDIA'S CYBER VULNERABILITIES: TIME TO REVAMP THE STATUS QUO

Written by ***Lokesh Vyas* & Dakshesh Kapoor*****

** 4th Year B.Com LLB Student, Institute of law Nirma University Ahmedabad*

*** 4th Year B.Com LLB Student, Institute of law Nirma University Ahmedabad*

ABSTRACT

In the era of Internet, "threat" has become an undeniable candor of the 21st century. In cyber epoch, where everyone is witnessing incessant cyber war, the strong cyber security has become the need of the hour not only for an individual but also for a nation. The cyber security threats are working as an impetus to make the countries better in terms of technology. The advent of internet has given birth to a new kind of threat i.e. cyber security threat and increased its number in the list that a country is likely to face. This threat is more lethal than other existing traditional ones because today almost every country manages itself through the medium of cyber space. Any threat to the cyber space of a nation is capable of devastating its economic, political and social terrain. India is still in salad days when it comes to cyber security. This paper highlights the issues and challenges to India's cyber security and demonstrate the need to revamp the status quo in order to ameliorate the concerns regarding cyber security threats and attacks. Additionally, the paper also stiffens India's need for a robust cyber infrastructure to enter in a new digital era. Pertinently, cyber security attacks are leading to massive data breaches keeping the privacy of every individual at stake. Rapid cyber attacks have spiked the level of concern for cyber security. Today, the concern for security threats is compelling big companies and organizations to spend more money in cyber security insurance. Recently, Radicalization of cyberspace remains a big challenge for societies like India which lacks feasibility to accept digitalization in Toto. Thus, the paper aims to critically evaluate the trends of cyber security, its threats and analyze India's viability to adopt ambitious transitions which are speculated to be adopted. Moreover, the authors

have also have attempted to analyze India's viability to become a complete wholly digitalized country.

INDIA'S CYBER SPACE IN TROUBLED WATER

The word *cyber* has been in vogue for last few decades. The word cyber is a condensed form of the word *cybernetics* which means the study of communication and control systems in living beings and machines. The word *cybernetic* comes from the Greek word *kubernētēs*[i], which implies steersman.

Ours is the era of technology where people have become accustomed to cyber space and technology. There is a direct relationship between usage of Internet of Things and cyber threats which means the more we rely on cyber space or electronic mediums the more the cyber threats we face. Beginning from the micro unit i.e. individual to macro level i.e. a nation, the role of internet and the reliance on the same cannot be denied. No system in the world is immune from hacking and is safe until it is hacked. The accelerating use of internet has given birth to a new branch of law known as *Cyber Law*.This era of internet has provided human beings with new set of problem known as cyber terrorism whose existence is based on the Internet. At this point of time doing away with the Internet is also not feasible because it has become the need of the hour and its positive facades cannot be overlooked. Cyber crimes can be categorized in three ways that are against person e.g. leaking someone's personal photos, against property e.g. hacking websites and distorting data and, against government.[ii] The last one is the most lethal one as it challenges the safety of the whole country e.g. hacking governmental or military websites and leaking information to enemy countries. Generally, cyber criminals commit crime for the money but there are people who enjoy doing this activity and love harassing people by misusing their cyber expertise. Till now there is no universal law which addresses all sorts of cyber crimes. Every other day a new cyber crime pops up and surpasses the evilness of previous cyber crimes.

As per the recent data, India was ranked third in the list of countries where the highest number of cyber threats were detected, and 2nd in terms of targeted attacks in 2017,[iii] according to security software firm Symantec. Globally, India was ranked 2nd with respect to spam and phishing (misleading emails, weblink etc) and 3rd among the countries which are most impacted

by network attacks. Moreover, Indian stood 4th in the list of countries which are attacked by ransom ware.[iv]

While assigning a global rank malware, spam, phishing, bots, network attacks, web attacks, ransomware and cryptominers are taken into account. As per the official data the number of cyber crimes has increased in 2016 in comparison to 2015. There was a hike of 6.3% in 2016 with more than 12000 cyber incidents.[v] Many cyber incidents go unreported,[vi] every year which means that India is more cyber vulnerable than it appears to be. As per data of CERT-In, the number of cyber security incidents reported in 2014 was 44,679 which went up to 49,455 in 2015 and in the next year 2016 it raised to 50,362. 27,482 cyber incidents were recorded till June 2017.[vii] Furthermore, recently Indian cyber security firm named *Quick Heal Technologies* claimed to have detected over 48,000 ransomware attack attempts within the country in total. In furtherance of the same, India became the 3rd Worst Hit Country by *WannaCry* Ransomware with approximately 50,000 PCs Affected.[viii] The dream of becoming cashless economy has also attracted cyber crimes in India. After demonetization the number of cyber crimes has also spiked because the cashless economy gave an impetus to more usage of e-commerce and e-transaction resulting in the more number of cyber security incidents. According to the data of the Indian Computer Emergency Response Team (CERT-In), during the period of November, 2016 to June, 2017, 50 incidents affecting 19 financial organizations have been reported.[ix] According to the report of The Economic Times, at least one cybercrime was reported every 10 minutes in India in the first six months of 2017 from global ransomware attacks that hit hundreds of systems to phishing and scanning rackets which is higher than a crime every 12 minutes in 2016.[x] Recently Reliance Jio faced unauthorized access to one part of its database, and then hackers managed to steal Union Bank's access codes for the society for Worldwide Interbank Financial Telecommunications (SWIFT). Moreover, as per recent news an unnamed offshore hacker made an unauthorized login to Axis Bank, 17 million users' record of Zomato was hacked from its database, meanwhile Renault India was also hit by ransomware wannacry. Furthermore, IRCTC government's online portal witnessed data theft from its website. Furthermore Yes bank and Bank of Maharashtra also witnessed cyber attacks.[xi]

The present chapter elucidates the cyber security incidents happened in past few years. Moreover, it expatiates the cyber vulnerability of India and the effect of demonetization on

cyberspace. In furtherance of the same, the chapter questions the viability of complete digital/cashless economy of India.

PRIVACY: A MYTH

Stephane Nappo - "*It takes 20 years to build a reputation and few minutes of cyber-incident to ruin"*

The increasing number of cyber security incidents and data breach legitimizes the words of Stephane Nappo. The 21st Century has undoubtedly been the era of vast technological advances. This has led to a wide spread data consumption and transfer vide various electronic devices. The dark side to this era is uninterrupted, perpetual and persistent data monitoring of every individual throughout the world. The reason for this data monitoring can indeed be weighed upon. However, it's imperative to understand the extent to which such data monitoring the Governmental or Non-Governmental agencies have the right to encroach upon our personal space. Often the consent for such data-monitoring is given unknowingly because we are very much accustomed to cyberspace. Moreover, the consent is often worded surreptitiously with the elusive intent to deceive the consent giver. A common example to this could be the applications we download on our smartphones; the consent is given without an ounce of reading to what the applications are actually doing. It has indeed been the case that some apps have been involved in collection of data without the consent of an individual. This data collection could be in the form of (Search History, Images, Contacts, and Users Habits etc.). Moreover, seemingly the most reputed social media platforms have been involved in sharing & selling data with private agencies. Facebook is one such example which was allegedly involved in two vast data scandals which nearly affected 2.19 billion people of the world. India is claimed to have the highest number of Facebook user in the world,[xii] which means the India is under the biggest threat of data protection breach.

In the light of the aforementioned situations it becomes imperative to understand the extent to which various companies encroach upon our personal space. In India, this becomes essential because of the vast technological eco-systems being developed for consolidation of citizen data i.e. Aadhar Card. The Right to Privacy was recognized as natural/intrinsic and fundamental right as a part of Article 21 with the aim to protect the life and liberty of the citizens.

Section 43A, of the Information and Technology Act added by an Amendment in the year 2008 deals with the *"implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain"*. Moreover, Section 72A, of the aforementioned Act provides for "*imprisonment for a period up to three years and/or a fine up to Rs. 500,000 for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract."*

A judgment passed by a seven-judge bench of the Hon'ble Supreme Court declared 'Privacy' as a fundamental right.[xiii] Right to privacy is a fundamental right regardless it does not mean that it is an absolute right, the underlying assumption behind privacy is that there needs to be a demarcation line between ethical citizen monitoring and encroachment by organizations on the life of an individual.

Considering EU's GDPR (General Data Protection Regulations) as counterpart of the Indian data protection and privacy helps in drawing a sound inference about the data protection regime in India. The GDPR focuses on ensuring that users know, understand, and consent to the data collected about them. Under GDPR[xiv] humongous uncomprehdable pages won't suffice and companies must be clear and concise about what they are collecting. The companies collecting the said data would have to ensure that the user understands why the data is being collected and how it is used. Moreover, consumers will gain the right to access data that companies store about them, the right to correct inaccurate information, and the right to limit the use of decisions made by algorithms, among others. This would ensure that the user is aware of the data which is collected, circulated and utilized from his smart phone. These steps were taken to ensure the data protection of Individuals.

Coming to the Indian laws section 2 (w) of IT act defines the intermediary The Information Technology Amendment Act 2008 has clarified the position of intermediary by including the Telecom service providers, internet service providers, web-hosting service providers in the definition of intermediaries. In furtherance of the same search engines (Google etc.), online-payment sites (paytm etc.), online auction sites, online marketplaces and cyber cafes have also come under the purview of intermediary. Section 79 of IT act (Amendment) 2008 exempts the intermediaries from certain liabilities when such liability arises due to the act of third party and intermediary is oblivious to the same. This could destroy the user's reputation, cause loss to

companies or lead to damaging the user's reputation.[xv] For instance hackers were able to access personal information of 57 million Uber drivers for which the company had to pay $100,000 to hackers.[xvi] It becomes evident that even the biggest of Multinational companies are at the behest of hackers. According to a research conducted by Symantec Corporation U.S.A nearly 65 % adults have been a victim of cyber-crime.[xvii]

When it comes to India, where steps and initiatives are being taken to ensure total digitization the existence of a sustainable technological eco-system becomes more important. In a scenario where the collection of the largest user biometric data is taking place the first and foremost question arises is viability of a suitable eco-system and infrastructure in response to current technological needs and threats.[xviii] India has been the most susceptible of cyber-attacks.[xix] In a research, it was found that 70% of the financial institutions in India believe that they are ill-equipped to face a cyber-attack.[xx]According to a report published by the National Crime Records Bureau there were nearly 12000 major cyber-crimes which took place in India.[xxi] It was also found through this report that a majority of cyber-crimes in India were not investigated. The level of data protection is so weak that even downloading a ringtone or something as simple as changing wallpaper would lead to sharing personal data without.[xxii]

Due to lack of specific legislations regarding data protection in the country, it is accomplished through a patchwork of legislation. The Information Technology Act (2000) (IT Act) and the Information Technology (Amendment) Act 2008, being the major patches, i.e. the primary legislation regarding data protection in the country. The former contains provisions for the protection of electronic data, and also penalizes 'cyber contraventions' and 'cyber offences'. Following it, in 2008 two new sections were incorporated into the IT Act by amendment, providing remedy to persons who have been the victim or are likely to face a loss on due to inadequate protection. The gravity of these cyber-crimes must be taken into consideration.[xxiii]

Then there is the *Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983* which prohibits public financial institutions from divulging any of their clients' information except according to laws of practice and usage.

The *Prevention of Money Laundering Act (*2002) mandates the banking companies, financial institutions and intermediaries to furnish the information relating to prescribed transactions, and which can also be shared, in the public interest with other government institutions. The *Credit Information Companies (Regulation) Act 2005 and The Credit Information*

Companies Regulations 2006 are also present for regulating share and exchange of credit information by credit agencies with third parties, prohibiting any kind of disclosure of data received by a credit agency unless required by any law in force.

Also, under the *Payment and Settlement Systems Act (*2007), RBI is designated as a supervising authority over payment systems in India, but in no manner allowed to disclose the contents of any document or any information provided to it. In addition to the above stated statutes, some other smaller patches to ensure data protection are property rights provided by the Copyright Act (1957). Furthermore, in some cases Code of Criminal Procedure (1973), the Indian Telegraph Act 1885, the Companies Act (1956), the Competition Act (2002) is also ardently relevant.

This chapter demonstrated the actual scenario of privacy in our country. Data protection framework of our Indian is still in its salad days require a lot of development in order to cope up with the increasing pace of cyber crimes. Moreover, this chapter expatiates that how the privacy is just myth and how we are being tracked every day. The accelerating use of Internet of Things has also increased the threats of cyber attacks and minimizes the data protection of an Individual. Today, Privacy has become a utopian thing and has lost it in instantaneous universal email communication and spying, with millions of CCTV cameras throughout the globe with pervasive warrantless spying.

INDIA'S CYBER-SPACE: A FRAGILE REGIME

"There are finite cyber criminals in the infinite cyber space"

Today, the reach of cyber attacks has surpassed the point where such attacks were only limited to personal safety now the cyber security means the security of a nation.[xxiv] The advancement of technology has given birth to cyber weapons. Today both government and private organizations work in cyberspace. Cyber criminals are not limited by the boundaries because cyber crimes take place in a virtual world. A person sitting in one corner of the globe can wreak havoc to other corner of the globe. This is how cyberspace works with no boundaries and no restrictions. We live in a cyber-age where every place is warfare; one mouse click is enough to erase a place from the map. Cyberspace is an intangible human construction which possesses the power to deface physical objects without having its own tangible existence. This intangible

nature of cyberspace works as a camouflage for cyber criminals and enables them to escape the hands of law. Cyber space immunizes cyber criminals by the virtue of anonymity. The increasing use of cyberspace has given birth to new words like cyber-terrorism and cyber-warfare. The words terrorism and war are already lethal and gruesome in their present connotation ergo; prefix cyber has bolstered their gravity and thereby make them more gruesome than their traditional nature. Many times question arises whether the laws of armed conflict (LOAC) apply on cyber issues. The answer to the same is affirmative. This was clarified by International Court of Justice in 1996 in its Nuclear weapons advisory opinion that LOAC is applicable to any use of force regardless of the weapons employed. The expression cyber warfare includes deterrence, defense and offense. Cyber warfare can be engaged by states, by agents of state, or by non states actors. It does not necessarily mean terrorism but depending upon the situation it can be interpreted to include terrorism.[xxv] Terrorism has always been the bone of contention for the human kind, this is something which facilities killing of human beings by human beings. Cyber terrorism is more dangerous than one could ever imagine its aftermaths are more morbid than the actual terrorism and it is increasing day by day.

Some scholars have argued that cyber attacks better a nation in terms of its cyber security because the expectation of a cyber attack creates an impetus for the nation to create a more robust cyber infrastructure for itself thereby bolsters its cyber security and the nations that never witness cyber attacks find themselves at a weaker position eventually.[xxvi] Various national and international agencies and organizations are trying to tackle with this menace and the various investigation agencies of the countries are finding it very difficult to control it because it is extremely difficult to find the culprit. Cyber space empowers a person to hide his identity. Interestingly, there are not many cyber criminals because it is only a small sect of people all over the word who possess the enough cyber expertise to commit cyber crimes. Appositely, these are the people are actually are hard to find. Other cyber criminals are not so expert therefore they can be easily tracked when properly investigated. Cyber-attacks are not novice to the Internet of Things (IoT). Today, the IoT are deeply entwined in our lives and societies which had made it imperative to go ahead and take this issue seriously.[xxvii]

Beginning with the wars, we went to world wars, then we witnessed cold war and now we all are victim of code war. This is never ending and ever increasing war. The more technological

we become the more deadly this war becomes. Today physical presence is not required to decimate a person or a thing mere cyber infiltration to the relevant system is enough to serve your purpose.

There are many kinds of cyber attacks like Backdoor, Denial-of-service attacks, Direct-access attacks, Eavesdropping, Spoofing, Tampering, Privilege escalation, Phishing, Clickjacking, Social engineering. Etc. Once Michael Mullen said *'the single biggest existential threat that's out there, I think, is cyber'*and the recent incidents fortifes what he said. The rising number in computer systems and the accelerating reliance on cyber space by the individuals, businesses, industries and governments attracting a large number of cyber crimes every day. Considering this scenario it can be concluded that every system is at stake and working under the threat of cyber attack. There have been instances in the past where financial systems (cyber attack on YES bank[xxviii]), utilities and industrial equipment (meltdown and spectre vulnerabilities are design flows and are found in late 2017, they exist in every computer system made in last 20 years)[xxix], aviation, consumer devices, large corporations (Facebook – Cambridge Analytica issue where facebook is alleged to breach the privacy of data protection of its users)[xxx], automobiles, government, Internet of things (IoT) and physical vulnerabilities, medical systems (around 5 lakh pacemakers were recalled by the US Food and Drug Administration because of fear of attack on the cyber security of those devices which enables the attackers to run the batteries down or even alter the patient's heartbeat)[xxxi] have been hacked by cyber criminals. Once they hack a website they can access all the data and acquire all the information which is not supposed to come put in general public. This information can also be against the actual owner; hackers can delete these data or leak it. In both the cases the one who suffers is the owner of the data. Nowadays, a new trend has come where cyber attackers ask for the money in lieu of the data hacked this is nothing but the demand for ransom. Such cyber attacks are called ransomware.

When government's website or data is hacked the problem becomes more severe because it impacts the nation in two ways majorly. Firstly, it leaves the impression among the civilians that their country is vulnerable in term of cyber security and creates a feeling of insecurity among them. Moreover, on the international platform it defaces the image of country. Secondly, it challenges the sovereignty and integrity of the country because infiltrating into the cyber system of a nation attracts the enemy countries to take advantage of the cyber

vulnerability. Cyber crimes are not confined in boundaries therefore it becomes very difficult to find the attackers, this allows third party to take unjust benefit of the enmity of two countries. A few months ago when a government website named mod.nic.in was alleged to be hacked, people suspected that it was the work of Chinese hackers whereas some called it the work of Pakistani cyber experts but till now no conclusive proof is found that can prove the identity of the actual criminal hacker. Later, it was said that there was no hacking but just a technical glitch.[xxxii] This shows that how the absence of conclusive proof of the identity of the cyber criminal eases the work of unjust person to fulfill its ulterior motive.

According to Indian Computer Emergency Response Team (CERT-In), the total number of 22,207 Indian websites was hacked during April 2017 to January 2018 out of including 114 were the government websites. Moreover, National Informatics Centre (NIC) claimed that during 2017 total number of 74 government websites hosted on NICNET was hacked during 2017 and in 2018 (till February) there were 6 government websites that were hacked on NICNET.[xxxiii] These data demonstrate the current scenario of cyber vulnerability of Indian. In furtherance of the same, approximately 1,500 government websites had been hacked in 6 years (between January 2010 and December 2015) as per the data from the Information Technology Ministry. Furthermore, 700 websites related to central or state government had been hacked in past 4 years.[xxxiv] Following is the of India's cyber vulnerability observed in the recent past.

CASE STUDIES

1. **Rajya Sabha Website: -** A few months ago, a group of hackers posted screenshots of Rajya sabha websites to stiffen their claim that they had unauthorized access to a section of the Rajya sabha website which could only be logged in by its members and administrators of the website. In this instance, they also managed to hack the inbox of the email id of BJP president cum President Amit Shah a Rajya Sabha member. National Informatics Centre (NIC) possess domain over the Rajya Sabha website.[xxxv]
2. **Ministries' Websites: -** In April 2018, many government websites including Ministry of Defense, law, labor, and external affairs were hacked. Chinese were alleged behind this incidence but no conclusive proof was found. Later on, it was said it was just a technical error or hardware problem and no cyber attack.[xxxvi]

3. **National Security Guard (NSG): -** In January 2017, suspected Pakistan-affiliated operatives hacked the website of NSG and posted obscene and unjust comment for the prime minister of India. These hackers identified as 'Alone Injector'. They defaced the home-page of the website with anti-India content.[xxxvii]
4. **Indian Army: -** Principal Comptroller of Defense Accounts (Officers) (PCDAO) website was reportedly hacked in 2015 which disabled the army officials from accessing their salary details on the website. The PCDAO website contains the personal details of the officers like their exact areas of posting, the units they belong to, PAN card numbers and bank account details and other relevant sensitive information.[xxxviii] Furthermore, in 2011 the official site of the Indian Army was hacked anonymous hacker. This hacker/s not only hacked the website but also managed to bring down the entire server of the NIC. The hacker claimed to have access to all the data and threatened to leak it. Moreover, the attacker also said that the attack is to better the situation of the country with respect to rising corruption.[xxxix]
5. **Indian Railways: -** In 2017, a microsite of the Railnet page of the Indian government was hacked by al-Qaeda a terrorist group. It was said to be done in a demonstration of the terrorist group's ability to break in government's cyber territory. This cyber attack came along with a writing which read "Message to the Muslim People in India from AQIS (sic)".[xl] This cyber attack brought an 11-page message for Indian Muslims and was pertaining to Jihad.[xli] The hacked page of Indian Railways belongs to the Bhusawal division of Personnel Department of Central Railways.
6. **MTNL website: -** In 2013,on the eve of Pakistan's Independence Day i.e. 14th augustMTNL Mumbai website was said to be hacked by a Pakistani hacker**.** Its homepage showed a message *Happy Independence Day Pakistan.* In furtherance of the same, the hacker also hacked some of the Pune based websites such as the Pune Traffic Police website i.e. *www.punetrafficpolice.gov.in* and *Janwani.org* (it addresses the development of the Pune). This act was done by the hacker who is called *Mr. Creep*. He not only hacked these websites but also left a link to his Facebook profile.[xlii]

7. **State Governments' websites: -** in 2015, Pakistan group of hackers attacked the website of the Gujarat Education Department. They posted derogatory remarks about the Indian Prime Minister on the homepage of the website *(vidyasahayakgujarat.org.).*[xliii] In 2016, the Karnataka police department's official

website was hacked. The hackers were allegedly to be Pakistani hackers. These hackers not only hacked the website but also pasted a Pakistani flag on the homepage of the website.[xliv] In 2015, Government of Kerala's witnessed a cyber attack on its official website *(www.kerala.gov.in).* It was hacked hackers who are alleged to be Pakistani hackers. Hackers put a picture on the homepage where the national flag was shown as being burned and posted a message which read as *"Pakistan Zindabad"* and *"security is just an illusion."* It was said that this is done by a hacker called *"Faisal 1337."*[xlv]

The abovementioned list of cyber attacks is not an exhaustive one but just gives an idea of what is happening around us and the gravity of cyber threats we are surrounded by. No country can spare itself from cyber threats and cyber crimes; even America which is considered to be the most powerful country of the world has been subjected to cyber crimes and threats. Even The National Aeronautics and Space Administration (NASA) had faced cyber attacks.[xlvi] Even after securing the powerful position in the international platform it spends large chunk of its funds on the security which implies the gravity of this problem.

This chapter elucidates the threats that cyberspace offers. In this chapter, researchers presented the data and establish the cyber vulnerability of nation. Moreover, the chapter also explains as to how the cyber security attacks compromise the security of the whole nation and answers that why cyber security and robust cyber infrastructure is the need of the hour.

MEASURES ADOPTED TO CURB CYBER ATTACKS

From a mere 23 reported cases in 2009 to around 96,383 cases reported till September 2014,[xlvii] the pace with which the cyber crimes has increased is flabbergasting. According to the Indian Computer Emergency Response Team (CERT-In), the year 2017 had a total number of cyber security incidents were 53081 which were higher than the total cyber incidents of the years 2014 (44679), 2015 (49455), 2016 (50362).[xlviii] Today, with the increasing number of cyber attacks on the government and non government websites it would not be wrong to conclude that every cyber system in the world is the focal point of cyber criminals and capable of being attacked. Reasons behind hacking can be both blatant and latent. Many times cyber attacks take place to fulfill the ulterior political or social motives but the most important thing is to curb these attacks by developing a robust infrastructure which needs to be updated timely.

With the proliferation of Information Technology (IT), the the painstaking issue of cyber attacks has also redoubled. The Information Technology (IT) Act 2000 followed by the Amendment Act of 2008 has been sedentary for long, and on top of it jurisprudential development over the past few years is almost zilch. The IT act, 2000 is the watershed moment in Indian's cyber regime but is not wide enough to deal with upcoming cyber issues. The 2008 amendment to IT Act does not really bring about much change regarding encryption. It expanded the scope of the government's power to order decryption.[xlix] The IT act 2000 mainly deal with the offences such as damage to computer, computer system, etc.[l] Tampering with Computer Source Documents,[li] Computer Related offenses,[lii] sending offensive messages through communication service,[liii] identity theft,[liv] cheating by impersonation by using computer resource,[lv] violation of privacy,[lvi] Cyber Terrorism,[lvii] publishing or transmitting obscene material in electronic form,[lviii] failure/refusal to comply with orders,[lix] failure/refusal to decrypt data,[lx] securing access or attempting to secure access to a protected system[lxi], misrepresentation[lxii], for breach of confidentiality and privacy[lxiii], For disclosure of information in breach of lawful contract.[lxiv]

Moreover there are some provisions of Indian Penal Code (IPC), 1860 which address some of the cyber issues such as section 506 i.e. sending threatening messages by email, section 500 Sending defamatory messages by email, section 465 i.e. Forgery of electronic records, section 420 i.e. Bogus websites, section 465 i.e. cyber frauds Email spoofing, section 384 i.e. Web-Jacking. Other cyber crimes such as online sale of Drugs and online sale of arms are dealt in 'NDPS Act'[lxv] and 'Arms Act'[lxvi] respectively.

2013 was the year of purple hours for Indian cyber regime. In this year, India government came up with National Cyber Security Policy 2013 with an aim to monitor and protect information and strengthen defenses from cyber attacks. The policy was brought to ensure a secure and buoyant cyberspace for its citizens, businesses and the government.

All policy matters pertaining to information technology; Electronics; and Internet (except licensing of Internet Service Provider), Cyber Laws, administration of the Information Technology Act 2000 and other IT related law come under the purview of Ministry of Electronics and Information Technology (MeitY). In January 2004, The Indian Computer Emergency Response Team (CERT-In) was established under Section 70B of the Information Technology Act, 2000. Its functions include forecast and alerts of cyber security incidents,

emergency measures for handling cyber security incidents, Coordination of cyber incident response activities, Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents and, such other functions relating to cyber security as may be prescribed.[lxvii]

In 2014, the Prime Minister's Office created the position of the National Cyber Security Coordinator. In 2016, in retaliation to the cyber attacks by hacker group 'Legion' MietY took some vital steps such as use of National Payment Corporation of India (NPCI) to audit the financial sector, review and strengthening of the IT Act, directives to social networking site Twitter to strengthen its network, and directives to all stakeholders of the financial industry including digital payment firms to immediately report any unusual incidents. In furtherance of the same, RBI has mandated all the Indian banks to comply with cyber security guidelines. Moreover, the government has started Information Security Education and Awareness (ISEA) project which aims to develop human resource in the area of Information Security at various levels.[lxviii] Furthermore, in 2017 India's Computer Emergency Response Team (CERT-in)[lxix] came up with 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre) a new desktop and mobile security solution for cyber security in India which aims to curb the cyber attacks in India and better the cyber security infrastructure of India.

This chapter dealt with the steps taken by India in response to the increasing cyber security violations in India. It briefly elucidated the current cyber infrastructure of India and how it is inadequate to the cyber threat

CONCLUSION

The paper highlights the need to revamp Indian status quo with regard to cyber security which has been under constant cyber threat. This paper does not intend to ignore the efforts taken by government to curb cyber attacks and improve the cyber infrastructure of India yet the research proved the hypothesis that India is still not in a position to become digitized country. By this paper, researchers attempt to present the actual scenario of digitalization. Before taking any step in a country government should do a cost benefit analysis and both pros and cons should be taken into consideration while at a sound conclusion. The researchers tried to prove that when the government websites are not competent enough to fight cyber attackers, it would not

be justified to expect a layman to accept total digitalization. Though the government made a little effort a few years back and drafted a National Cyber security Policy in the year 2013, which apparently created considerable interest in the country as well as abroad, particularly in view of India's position as an exponentially growing business process subcontracting destination. Unfortunately, progress on the policy was thwarted for unknown reasons, reflecting government's lethargic attitude in providing untainted, robust and impermeable law on the matters.

The groundswell of opinion in favor of change is unmistakable but still 2016 was a mixed bag of both encouraging as well as distressing changes, but overall none of these developments resulted in substantially overhauling or repairing the incompetent statutory law. There has nothing significant in contrast to what was being legitimately expected from the authorities for long, except the introduction of the Aadhar Act, providing privacy to be a fundamental right of every citizen under the Constitution. The country also witnessed the government amending the Income Tax Act 1961–2017, aiming to curb tax evasion and money laundering, by mandating the taxpayers to link their Permanent Account Numbers (PANs) for filing income-tax returns, open bank accounts and conduct financial transactions beyond a threshold.

Reading this list of legislations might make it seem that the government is worried about and keen to bring changes in this area, all these laws remain sword in a scabbard without proper implementation and execution. This is high time when we needed to sit and ponder over the solution to the rising problem.

REFERENCES

[i] Simon Rey Atkinson et.al, *Cyber-Transparencies, Assurance and Deterrance,* http:// www.researchgate.net/profile /Simon_Atkinson5/publication/260736040_Cyber_Transparencies_Assuranceand_Deterrence/links/59ffb694458515d0706e3011/Cyber-Transparencies-Assurance-and Deterrence.pdf?

[ii] Cyber Crime – A Threat to Persons, Property, Government and Societies, Er. Harpreet Singh Dalla, Ms. Geeta, International Journal of Advanced Research in Computer Science and Software Engineering 3 (2013) http://ijarcsse.com/Before_August_2017/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

[iii] India third most vulnerable country to cyber threats, Yuthika Bhargava accessed on 10 June 2018 http://www.thehindu.com/news/national/india-third-most-vulnerable-country-to-cyber-threats/article23437238.ece

[iv] Internet Security Threat Report ISTR Volume22, Symantec accessed on 5 June 2018 https://www.symantec.com/content/dam/symantec/docs/infographics/istr-5-1-en-in.pdf

[v] COST OF CYBER CRIME STUDY 2017 INSIGHTS ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE, Ponemon accessed on 11 June 2018 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[vi] Many cybercrime cases not investigated, Vijaita Singh accessed on 6 June 2018 http://www.thehindu.com/news/national/many-cybercrime-cases-not-investigated/article21235628.ece

[vii] India hit by 34 ransomware attacks, Minister Chaudhary tells Lok Sabha, accessed on 8 June 2018 http://www.thehindu.com/news/national/india-hit-by-34-ransomware-attacks-minister-tells-ls/article19309469.ece

[viii] India 3rd Worst Hit Country By WannaCry Ransomware With Close To 50,000 PCs Affected By Attack, Jayesh Shinde last accessed on https://www.indiatimes.com/technology/news/india-3rd-worst-hit-country-by-wannacry-ransomware-with-close-to-50-000-pcs-affected-by-attack-321791.html

[ix] Total of 50 cyber attack incidents reported in financial sector: Govt, accessed on 10 June 2018 (https://indianexpress.com/article/technology/tech-news-technology/50-cyber-attack-incidents-reported-in-financial-sector-govt-4777350/)

[x] Cybercrime spiked after demonetisation, say experts, Komal Gupta, last accessed on 18 June 2018, (https://www.livemint.com/Industry/M8z9KNBBPbN6AFc8j0NF5M/Cybercrime-spiked-after-demonetisation-say-experts.html)

[xi] How India Inc is losing its cybersecurity war, Vinod Mahanta and Sachin Dave, last accessed on 18 June 2018, (https://economictimes.indiatimes.com/tech/internet/how-india-inc-is-losing-its-cybersecurity-war/articleshow/61074845.cms)

[xii] Leading countries based on number of Facebook users as of April 2018 (in millions) https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/

[xiii] Justice K.S. Puttaswamy(Retd.) V Union of India And Ors , WRIT PETITION (CIVIL) NO 494 OF 2012

[xiv] GDPR Portal: Site Overview, https://www.eugdpr.org/

[xv]THE 17 BIGGEST DATA BREACHES OF THE 21ST CENTURY, Taylor Armending Accessed on 12th May 2018 (https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html)

[xvi] SELENA LARSON, UBER's MASSIVE HACK: WHAT WE KNOW, ACCESSED ON 23rd May 2018 (http://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html)

[xvii] Norton Cybercrime Report: The Human Impact (https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf)

[xviii] PRESS TRUST OF INDIA, RAJNATH CONCERNED OVER INTERNET MISUSE, SEEKS MEASURES TO IMPROVE CYBER SECURITY, accessed on 20th June 2018 (https://www.hindustantimes.com/india-news/rajnath-concerned-over-internet-misuse-seeks-measures-to-improve-cyber-security/story-s2BwfEwL5NIKsm8lOAIBsN.html)

[xix] INDIAN COMPANIES MORE PRONE TO CYBER ATTACK, 60 PERCENT UNREGULATED SOFTWARE, accessed on 28th May 2018 (https://indianexpress.com/article/technology/tech-news-technology/indian-companies-more-prone-to-cyber-attack-malware-spyware-software-unregulated-research-4698723/)

[xx] White Paper of the committee of experts on a Data Protection Framework for India, (http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf)

[xxi] NCRB Releases Data on Cybercrime Rise, Experts Fear Figures do Not Reveal Real Picture, Aishwarya Kumar, accessed on 24th May, 2018 https://www.news18.com/news/india/ncrb-releases-data-on-cybercrime-rise-experts-fear-figures-do-not-reveal-real-picture-1597555.html

[xxii] STUDY SHOWS SOME ANDROID APPS LEAK USER, Priya Ganapati accessed on (https://www.wired.com/2010/09/data-collection-android/)

[xxiii]Simon Rey Atkinson et.al, Cyber-Transparencies, Assurance and Deterrance, http:// www.researchgate.net/profile /Simon_Atkinson5/publication/260736040_Cyber_Transparencies_Assuranceand_Deterrence/links/59ffb694458515d0706e3011/Cyber-Transparencies-Assurance-and Deterrence.pdf?

[xxiv] Bring on the Cyber Attacks – The Increased Predatory Power of the Restrained Red Queen in a Nation-state Cyber Conflict, Burk, Rosemary A., and Jan Kallberg., The Cyber Defense Review 1(2016), 61-72.

[xxv] Cyber Warfare, Gary D. Solis, Military Law Review 219 (2014), 1-52

[xxvi] Bring on the Cyber Attacks – The Increased Predatory Power of the Restrained Red Queen in a Nation-state Cyber Conflict, Burk, Rosemary A., and Jan Kallberg., The Cyber Defense Review 1(2016), 61-72. (http://www.jstor.org.ezproxy.nujs.ac.in/stable/2626735)
[xxvii] Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Mohamed Abomhara and Geir M. Køien, Journal of Cyber Security 4, 65–88 (https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_414.pdf)
[xxviii] RBI fines YES Bank for failing to report cyber security attack on its ATM network, Riddhi Mukherjee, accessed on 15 June 2018 (https://www.medianama.com/2017/10/223-rbi-fines-yes-bank-failing-report-cyber-security-attack-atm-network/)
[xxix] What are Meltdown and Spectre? Here's what you need to know, Jon Masters, accessed on 15 June 2018 (https://www.redhat.com/en/blog/what-are-meltdown-and-spectre-heres-what-you-need-know)
[xxx] The Facebook and Cambridge Analytica scandal, explained with a simple diagram, Alvin Chang (https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram)
[xxxi] Hacking risk leads to recall of 500,000 pacemakers due to patient death fears, Alex Hern, accessed on 15 June 2018 (https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update)

[xxxii] Ministry of Defence website hacked by suspected Chinese hackers, Nirmala Sitharaman says action initiated, last accessed 17 June 2018 (https://www.firstpost.com/india/ministry-of-defence-website-hacked-by-suspected-chinese-hackers-nirmala-sitharaman-says-action-initiated-4421029.html)
[xxxiii] Over 22,000 Indian websites hacked between Apr 2017-Jan 2018, last accessed 18 June 2018 (https://timesofindia.indiatimes.com/business/india-business/over-22000-indian-websites-hacked-between-apr-2017-jan-2018/articleshow/63203998.cms)
[xxxiv] Multiple Government Websites Down, Hacking Suspected, accessed on 13 June 2018 (https://thewire.in/government/defence-ministry-website-hacked)
[xxxv] Hackers claim to breach Rajya Sabha website, access Amit Shah's member account, Abhishek Dey last accessed on 18 June 2018 (https://scroll.in/latest/872638/hackers-claim-to-breach-rajya-sabha-website-access-amit-shahs-member-account)
[xxxvi] Defense, Law And Home Ministry Websites Down, Official Says "Hardware Problem" last accessed on 17 June 2018 (https://www.ndtv.com/india-news/defence-ministry-website-hacked-leads-to-an-error-page-1833811)
[xxxvii] National Security Guard website hacked, defaced with abusive message against Narendra Modi, accessed on 17 June 2018 (https://www.firstpost.com/india/national-security-guard-website-hacked-defaced-with-abusive-message-against-narendra-modi-3183196.html)
[xxxviii] INDIAN ARMY SITE HACKED: DOES INDIA HAVE THE RIGHT ATTITUDE TO TACKLE CYBER-CRIME?, Karrishma Modhy accessed on 12 June 2018 (https://www.firstpost.com/tech/news-analysis/indian-army-site-hacked-does-india-have-the-right-attitude-to-tackle-cyber-crime-3666607.html)
[xxxix] NIC SERVERS AND INDIAN ARMY OFFICIAL WEBSITE HACKED, Anuradha Shetty accessed on 10 June 2018 (https://www.firstpost.com/tech/news-analysis/nic-servers-and-indian-army-official-website-hacked-3584775.html)
[xl] NSG portal hacked, defaced with abusive messages, accessed on 15 June 2018 (https://indianexpress.com/article/india/nsg-portal-hacked-defaced-with-abusive-messages/)
[xli] Al Qaeda Hacked An Indian Government Website And Left A 11-Page Message, Ritu Singh accessed on 12 June 2018 (https://www.scoopwhoop.com/Al-Qaeda-Just-Hacked-An-Indian-Government-Website-And-Has-Left-A-11Page-Message-For-Muslims/#.uqda57y1m)
[xlii] MTNL, PUNE TRAFFIC POLICE WEBSITES HACKED AND DEFACED BY PAKISTANI HACKER, Nishtha Kanal accessed on 11 June 2018 (https://www.firstpost.com/tech/news-analysis/mtnl-pune-traffic-police-websites-hacked-and-defaced-by-pakistani-hacker-3634279.html)
[xliii] PAKISTANI HACKERS DEFACE GUJARAT GOVERNMENT WEBSITE: REPORT, accessed on 10 June 2018 (https://www.firstpost.com/tech/news-analysis/pakistani-hackers-deface-gujarat-government-website-report-3662361.html)
[xliv] KARNATAKA POLICE WEBSITE 'HACKED' BY PAKISTANI HACKERS accessed on 15 June 2018 (https://www.firstpost.com/tech/news-analysis/karnataka-police-website-hacked-by-pakistani-hackers-2-3683547.html)
[xlv] GOVERNMENT OF KERALA WEBSITE WAS HACKED BY 'SUSPECTED PAKISTANI HACKERS', accessed on 19 June 2018 (https://www.firstpost.com/tech/news-analysis/government-of-kerala-website-was-hacked-by-suspected-pakistani-hackers-3671943.html)

[xlvi] NASA says was hacked 13 times last year, Reuters Staff, accessed on 11 June 2018 (https://www.reuters.com/article/us-nasa-cyberattack/nasa-says-was-hacked-13-times-last-year-idUSTRE8211G320120303)
[xlvii] INDIAN ARMY SITE HACKED: DOES INDIA HAVE THE RIGHT ATTITUDE TO TACKLE CYBER-CRIME?, Karrishma Modhy accessed on 12 June 2018 (https://www.firstpost.com/tech/news-analysis/indian-army-site-hacked-does-india-have-the-right-attitude-to-tackle-cyber-crime-3666607.html)
[xlviii] CYBER WARFARE, Institute of Defense Studies and Analysis, accessed on 15 June 2018 (https://idsa.in/taxonomy/term/85)
[xlix] Strategic national measures to combat cybercrime: Perspective and learnings for India, EY accessed on 20 June 2018 (http://www.ey.com/Publication/vwLUAssets/ey-strategic-national-measures-to-combat-cybercrime/$FILE/ey-strategic-national-measures-to-combat-cybercrime.pdf)
[l] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 43.
[li] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 65.
[lii] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 66.
[liii] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 66 A.
[liv] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 66 C.
[lv] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 66 D.
[lvi] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 66 E.
[lvii] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 66 F.
[lviii] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 67.
[lix] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 68.
[lx] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 69.
[lxi] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 70.
[lxii] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 71.
[lxiii] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 72.
[lxiv] Information Technology Act, 2000, No.21 of 2000, Acts of Parliament, (June 9, 2000), § 72 A.
[lxv] The Narcotic Drugs and Psychotropic Substances Act, 1985, No. 61 of 1985, Acts of Parliament (Aug. 23, 1995)
[lxvi] Arms Act, 1959, No. 54 of 1959, Acts of Parliament (Oct. 1, 1995).
[lxvii] ICERT, http://meity.gov.in/content/icert
[lxviii] INDIAN GOVERNMENT HAS TAKEN A SLEW OF MEASURES TO TACKLE CYBER ATTACKS: IT MINISTER, accessed on 14 June 2018 (https://www.firstpost.com/tech/news-analysis/indian-government-has-taken-a-slew-of-measures-to-tackle-online-scams-it-minister-3658649.html)
[lxix] A Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian Cyber Security Ecosystem, the centre for Internet & society, https://cis-india.org/internet-governance/files/cert-ins-proactive-mandate.pdf