International Journal of Advanced Science and Technology
Vol. 29, No. 11s, (2020), pp. 2722-2733

Changing Dimensions in the Menace of Cyber Crime; a Contemporary Situational Analysis

Prayaga M.A*
ICSSR Doctoral Fellow in Public Administration 2019, Department of Political Science, University College, University of Kerala, Kerala.
**prayagadeepuvedathrey@gmail.com*

Abstract

Process of globalization furnished the entire planet into a more considerable vend where the matter of inventiveness is under the grip of dearth. The Pertaining state of affairs urges every authority to supplant its subsisting mechanism accordingly. Unanticipated upsurge in the figure of crimes related to cyber field need to be affixed with the pace of the effect of globalization mechanisms. Put it differently, the forces that have precipitated the global march of this phenomenon are the selfsame inclusive conditions that laid the stone for the absolute widening of e-crime. These conditions can be figured as unregulated interdependence, digital connectivity and deterritorialization that contain the manifold occurrence of cybercrime. It is quite pertinent to regard this menace from the lens of socio discursive standpoint in order to balance the social order of this era. In this paper an attempt has been made to scrutinize the impact of globalization and effect of after days on the cybercrime and some suggestions have been made for the need of changes in our administrative mechanism to cope up with the octopian spread of this menace.

Keywords: Cyber Crime, Lockdown, Digitalisation, ICT, Globalization.

Introduction

A news headline in March 2013 read, 'Rs 50 lakh stolen by cyber criminal from the bank account of a US – based Director of the ICICI Bank'. The largest and number one private sector bank of India is not able to protect even the account of one its directors from cyber risks. This is a headline which sweeped media for a period before 7 years. Another news headline in one of the renowned newspaper read as 'Significant Increase in Cyber Crimes against Women during Lock down.' Recently Delhi Police got to arrest the Instagram group administrator of a virtual group, 'Bios Locker Room' as an effect on their continuous abrupt abusive text messages and increased morphed nude pictures spread. This not only shows the level of risks within one of the best information spread gadgets in the world, it also points out the helplessness of these institutions. Information technology has doubtlessly expanded the speed, the precision, and the capacity of growth and business today whereas the menace of cyber threats is exceptionally soaring. Right from the treasury to defense, no department of the most advanced country, the US, is safe from cyber threats today! What can be said about the risks in developing countries? (Ramesh, 2013, p.89).

Even in the days of COVID 19, no IT enabled services are free from malwares and cyber threats. The biggest novel challenge of these policy makers as well as policy implementers is how to deal with the sudden upsurge of this menace which is swiping the good effects of this web services. Globalization has come out as a leading characteristic hallmark of the new millennium and it has thus turned an ineluctable actuality in today's society. No clique and public can abide off the beaten track from the forces of globalization. It is a new and contemporary stage of development of capitalism over the world. Globalization is a process of social change in which geographical and cultural barriers are being reduced. This breakdown of barriers is the result of transportation, communication and electronic communication. It is this border breakdown which bombarded the stigma of cyber growth in most of the societies

(Friedman and Singer, 2014, p. 281-296). Thus people are in relentless march to get imbibed to a mono culture which is shining in the grips of the gleam of so called globalization mechanism. This entire gamut resulted in the widespread march of electronic media and thereby prepared the ground to sow the seeds of all sort of menace of this new media. It is no longer a theoretical concept that has turned into an idea where a research is required to cope up with the black effects of the spread of the menace Dewanji, 2020). This is contemplated as the need of hour in overcoming the threat of the phenomenon.

The activity of cyber crime is that the use of computer as an instrument for illegal ends, like committing fraud, trafficking in kiddies porn and property , stealing identities, or violating privacy. Use of the internet has become wider and deeper as the computer has become central to commerce, entertainment, and government. Owing to the early and widespread adoption of computers and the internet, most of the earliest victims and villains of cyber crime were in the US (Stalling, 2005, p.45). But by the 21st century, hardly a hamlet remained anywhere in the world that had not been touched by cyber crime of one sort or another – the menace has spread everywhere. There are now different names for different cyber crimes, such as Computer Network Intrusions, Password Sniffers, Industrial Espionage, Cyber Fraud, Cyber Stalking, Computer Sabotage, Identity Theft, Spam, Phishing, Password Cracking, Hacking, Cyber Squatting, Software Piracy, Digital Bulling, Cyber Terrorism, to name the important ones (Ramesh,2013,p.90-91).

Indian Scenario

In India Cyber crimes are doubling with extra pace when an account had taken during 2017 statistics. This is based on the report of statistics released by the National Crime Record Bureau (NCRB) in October this year. Karnataka had the highest rate of cybercrime, followed by Assam, Telangana, Maharashtra, and Uttar Pradesh. India recorded over 9,500, 11,500 and 12,000 cases of cybercrime in 2014, 2015 and 2016 respectively (HT, 2020). After a delay of two years the data was compiled for the year 2017 by the Centre for which it blamed states in updating the statistics data promptly. The report further adds that about 56% of cyber crime cases registered were on fraud related complaints (12,213 out of 21,796 cases), which was followed by sexual exploitation cases of 6.7% (1,460 cases) (Viswakarma, 2017,p.43-46).

Publishing/transmitting of material containing sexually explicit under the IT Act

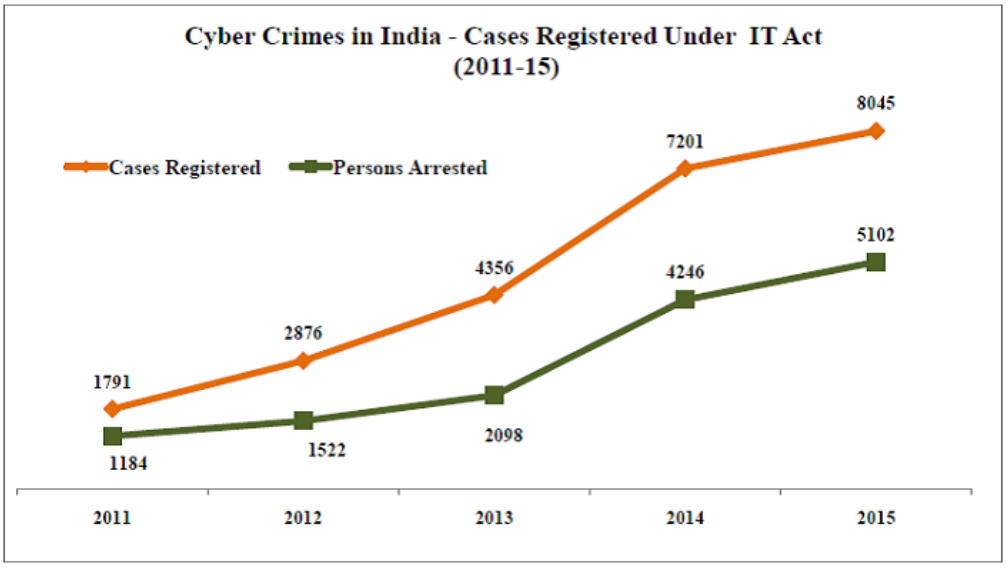
NCRB has divided this section into three parts. The first two, Section 67A, Section 67B of the IT Act, deal with publishing/transmitting sexually explicit content and depiction of children in a sexually explicit way respectively, in electronic form. The exact offence for the third section was not clearly specified in the report.

Publishing material which contain sexually explicit act on the internet (Sec67A)		Publishing material that depicts children in a sexually explicit act (Sec67B).		Publication of obscene sexually explicit act in electronic form.	
Assam	92	Uttar Pradesh	16	Uttar Pradesh	517
Karnataka	42	Assam	8	Assam	288
Telangana	35	Madhya Pradesh	7	Karnataka	157
Maharashtra	27	Himachal Pradesh	4	West Bengal	90

Odisha	24	Rajasthan/Tamil Nadu	2	Haryana	83
Total India	401	Total India	46	Total India	1768

Source: NCRB Annual Report 2017

When we take an account of total number of offenses based on the IT Act of India the highest need to be credited in Uttar Pradesh, which is followed by Karnataka with 3,152 cases, Rajasthan of 950, Assam with 941 and Maharashtra with 586 registered cases. If we take an account of total cases registered all over the country the figure reaches 13,635 cases.



Source: en.wikipedia.org

Cyber stalking or bullying of women/children (Sec 354D IPC)

Cases related to cyber stalking or cyber bullying are not yet registered in the North-eastern states such as Arunachal Pradesh, Manipur, Meghalaya, Mizoram, Nagaland, Sikkim, and Tripura.

State	No. of Cases
Maharashtra	301
Andhra Pradesh	48
Haryana	27
Telangana	26
Madhya Pradesh	25
Total India	542

Source: NCRB Annual Report 2017

Cases related to violation of privacy in cyberspace under the IT Act

In 2017, Assam had the highest number of cases (60) registered for violation of privacy. On the other hand, Uttar Pradesh had 47 such cases, Karnataka had 38, Kerala had 35 and Maharashtra had 22 registered cases. States such as Bihar, Jharkhand, Goa, Chhattisgarh, Jammu & Kashmir (now union territories), Meghalaya, Manipur, Nagaland, Odisha, Tripura, and Punjab did not have any case registered related to violation of privacy on the internet. The total number of such cases registered was 245.

Cyber terrorism (Section 66F) under the IT Act

There were 13 registered cases related to cyber terrorism across the country. Himachal Pradesh had 5 registered cases related to cyber terrorism, which was the highest in the country. While Assam had 4, other states such as Kerala, Tamil Nadu, and West Bengal had one each.

Frauds related to ATM, online banking, One Time Password (OTP) under section 465, 468-471 IPC

ATM		Online Banking Frauds		OTP Frauds	
Maharashtra	598	Maharashtra	345	Madhya Pradesh	122
Bihar	324	Odisha	116	Andhra Pradesh	62
Odisha	168	Telangana	111	Telangana	61
Uttar Pradesh	120	Uttar Pradesh	69	Uttar Pradesh	18
Telangana	56	Gujarat	42	Rajasthan	16
India total	1543	India total	804	India total	334

Source: NCRB Annual Report 2017

Fake news on social media (Sec. 505) under the IT Act

Statements leading to public mischief are related under Section 505 of Indian Penal Code. As per the report, a total of 170 cases were registered for cases related to fake news on social media platforms. List for the top five states has been given below:

State	**No. of Cases**
Assam	56
Uttar Pradesh	21
Madhya Pradesh	1
Odisha	13
Kerala	12

Total India	170

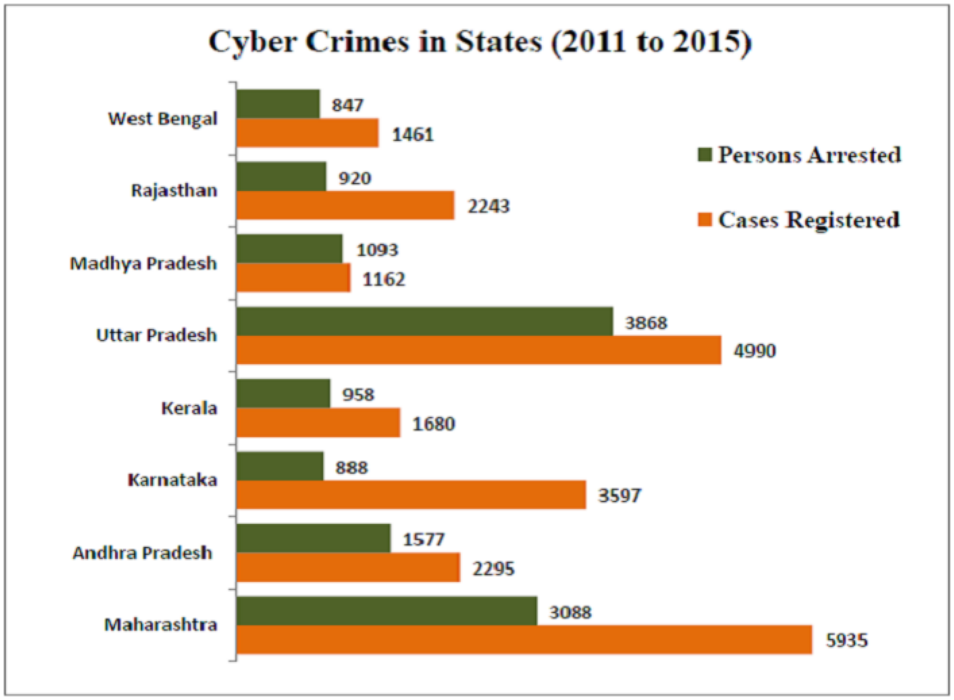
Source: NCRB Annual Report 2017

Online gambling under the IT Act cases

States such as Andhra Pradesh, Arunachal Pradesh, Assam, Bihar, Chhattisgarh, Goa, Himachal Pradesh, Tamil Nadu, Rajasthan, West Bengal, and Tripura did account for any registered case for online gambling. Details for the top five states have been given in the table below:

States	No. of cases
Jharkhand	16
Madhya Pradesh	10
Uttar Pradesh	3
Maharashtra/ Punjab	2
Karnataka	1
Total India	45

Source: NCRB Annual Report 2017



Source: Researchgate .net

It is universally true that every coin has two sides likewise for internet also it has got both advantages and disadvantages. In India the electronic based service is showing an unprecedented growth

paving way for the rise of new opportunities in almost every field. Crime related to cyber field is an illegitimate activity that is perpetrated while using a computer network more clearly, the internet. Additionally cyber crime inculpates the breakdown of privacy or impairment to the computer system properties (Dewanji, 2020). In our country most of cyber crime cases are enacted by educated persons consequently, the crime prevention and maintenance also requires more concern.

Our nation is marching hard to get started with the project of Digital India to the best of its potentialities and the sources of this initiative depend upon greatest connectivity with mere cyber security hazards. This often is considered a problem for us as we casted a poor track of record in cyber security related matters (HT, 2020).

Source: www, economictimes.com

Moreover, according to present statistics by Home Ministry, 71780 cases of cyber frauds were reported in the year 2013, compared to 22,060 such reported in 2012, which clearly showcases that the cases are pacing up and situation is alarming. If we look into the recent report released by the government, a total of 28.481 websites of Indian origin got hacked by different groups spread around the world (2017 report). The report also well read that there has been an increase of more forty percent in the registration of case related to cyber crime in India during the last two – three years.

Global Scenario

The globe is acquiring into more and more complicated in the sense that it is all the time a catch up game with cyber criminals. Everybody requires understanding that they are constituted of the same ecosystem. Today there is total paucity in different parts of the ecosystem which contain three main stakeholders, the general public, the private sector and the public sector. On account of a lot of happenings, including the Snowden incident which occurred a few years before, these three stakeholders do not maintain faith among themselves (Stalling, 2005, p.75-76).

Before wireless networks existed, the only way you could hack a company's corporate network was to somehow get access to the wired network. But today you can sit on a laptop next to the company's premises and hack into the wireless network without even having to set foot in the building. A further that is going to initiate more in the situation is the complete industrial internet and the Internet of Things (Yadav & Kiyawat , 2016, p.80). This day the electricity grid is altogether secluded from the common general internet. Whereas, the electricity grid turns smarter there need be more points of contact among the general public internet. The day is not so far when we could see that the hackers being able to get into

electricity grid , or facing a day when airports are closed by them, or ATC signals getting their way and so on. Moreover, the world as it gets more unified whatever Hollywood has shown in the last twenty years will literally become actuality.

Today the cyber world became an aligned form of living without which we are not able to carry on with our day to day life. The dependency on them is growing in a faster pace along with an increase in the mode of reliability of human mind also. The area did facilitate anytime use anywhere its IT services for the customers for improving the efficiency of our work which in turn began to rise as a major emerging threat for us (Desai, 2020). The government agencies and institutions all over the world started to react to the situation by taking necessary caution steps in the form of different Acts and Statutes. Our Police mechanism of India too started special cell which is completely responsible for creating and spreading awareness among public in these matters and thereby reducing the measure of threat within public (Dashora, p.247-253).

Extent of the Menace

Creation of novel technologies into the society often welcomes neo criminal minded chances whereas few new methods of crime. The very fact which differentiates cyber based crime from that of traditional type of fraud activity is the utilization of digital facilities but at the same time we should remember that this technology alone is inadequate to cope up with the changing facets of the level of internet based crimes (Deepak, 2020). Often the perpetrators don't require the gadgets in hand to commit such deed of frauds or to violate our privacy, even years before the cyber entry this existed.

Cyber crime, especially involving the internet, represents an extension of existing criminal behavior alongside some novel illegal activities. As the process of globalization has increased the levels and dimensions at which the nations of the world are interacting today, the threats of this crime have also multiplied in dimension. It seems as if greater globalization leads to greater hazards of cyber crime (Ramesh,2013, p 89). Cyber crime, in most cases, is an attack on information about individuals, corporations, or governments- the attacks are not on a physical body, they take place on the personal or corporate virtual body, which is a set of information about people and institutions on the 'net'. If we look into our everyday life in this era of computer our virtual self are indispensable and it reminds us that we similarise a bundle of just numbers or as identifiers in this gadget database which is either of government or of any private corporations. This crime highlights the centrality of networked computers in pour lives, as well as the fragility of such facts as identities (Kamath, 2000, p.56-61).

Today the serious threat faced by law enforcement institutions in dealing with matters related to this is the crime's exhibition of non – local character. This actually poses a major question in the mode of cooperation among nations concerning this issue. If a person accesses child pornography, is that individual committing a crime in a nation where such material is illegal? Where exactly does cyber crime take place? The concept of Cyber space can be figured as a more grounded genre of the space where wireless conversation are happening somewhere among different people through the medium of conversation (Desai, 2020). As a planet, spanning network, the internet offers the criminals multiple hiding places in the real world as well as in the network itself. Moreover, like an individual moving on the field leaving marks which can be followed a by a trained tracker the cyber hackers do leave such clues about their base in spite of their effective attempts to cover their doings. In order to follow such clues across national boundaries, though, international cyber crime treaties must be ratified (Ramesh,2013, p.92).

Checking the Menace

The nature of such crimes crosses physical frontiers of any nation this makes the necessity of an effectual and associated international coordination in coping and handling this menace. One nation,

whatever is the level of its digital preparedness, cannot stop such crimes from happening (Meeuwisse, 2015, p.95). The western nations who faced the initial victimization of these events took the stepping step in handling such cases. A preliminary international treaty in dealing cyber crime got drafted in 1996 by the Council of Europe which was jointly done by governments of US, Canada and Japan.

Around the world, civil liberties' groups immediately protested provisions in the treaty requiring internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Cyber Crime Convention (CECC) was signed by 30 nations. Additional protocols, covering terrorist activities and racist and xenophobic cyber crimes were proposed in 2002 (Ramesh, 2013, p.87-94).

At the international level, many attempts have been made under the over arching United Nation Commission on International Trade Law (UNCITRAL) but they have till now been inconclusive. In late 2010, the UN rejected a Russia backed proposal for a treaty on cyber crime, despite widespread agreement that closer international co-operation is vital in a world more closely connected by global computer networks (Stalling, 2015, p.45). Nations had a consensus on the point that there has been growth in legitimate cross-border computing, such as cloud computing. Talks at the UN were unable to reconcile differences between developing countries and the most advanced capitalist countries, led by the EU, US, and Canada. A UN advisory committee would consider conducting a study on cyber crime, legislation, and therefore the enforcement. The mechanism would bring countries that are working closer and to lead in the years which may open a new method to start a initial talk among nations for a global agreement, but such event will take further years (Ramesh, 2013, p.92).

The Government of India, in order to check the crime, has also adopted some of the clauses of the UNICITRAL and passed the Information Technology Act, 2000. The Act, besides defining cyber crimes into two categories of liabilities – civil and criminal – has given legal recognition to:

i. Digital Signatures, which include acceptance in lieu of hand written signatures
ii. Electronic Records, which include retention, attribution, acknowledgement and dispatch , and security
iii. Creation of an infrastructure for issuance and regulation of digital signature certificates
iv. Creation of a cyber regulations appellate tribunal
v. Amendments in existing laws to give recognition to electronic documents
vi. Offences and penalties for cyber crimes

As India is moving towards greater computerization and putting more and more functions on the internet, from administration to surveillance to developmental programs (the idea of Aadhar – linked delivery of benefits to the beneficiaries), the threats of cyber crime are increasing day by day. Before things take an ugly turn, the country needs to put in place an effective mechanism to check and prevent the rising menace of cyber crime. India has already started work on a dedicated network for the country which will not be dependent on the 'world wide web' (www) – the National Knowledge Network. However, this network does not provide India 'immunity' from cyber attacks from external sources, as this network has to be linked in any case to the 'world wide web' to get connected with the world out there. Yes, it will provide a high degree of independence to the country in the case of attack on the 'www' itself – as the concern of a possible terror attack on it has increased in recent times (Ramesh,2013, p.90).

Combating the Menace

In the past ten years the crimes around the world is comparatively rising its way directly into the scenario of information. Today internet credit card number fraud is widely recognized as well formed dangers which require urgent attention. The wide reported structures of crime so far figured by government mechanism are related to child pornography, fraud and e mail abuses. A sudden jump in the

change of cyber menace took in the form of cyber terrorism which got the grip after September tragedy (Choudhary & Basak, 2013, p.121, 123). 1820 is the year in which the first cyber crime got recorded. This is not quite surprising as the ever base of today's computer the abacus was around the land since 3500 B.C in India, Japan and China. However, the era of modern computer took into action with the invention of analytical engine by Charles Babbage.

The story of 1820's first crime recording goes from the production of a loom by Joeseph Marie Jaccquard, a textile manufacturer from France. He used the device for getting a repetition of many steps in the process of weaving specially fabrics which resulted in unwanted fear among his employees regarding their fear of loss traditional employment. When they felt a threatening call in their livelihood they committed acts of sabotage in order to discourage the employer from his further dependency of new technology. This, in broader aspect, is considered as the first recorded cyber crime (Stalling, 2005, p.225).

The arena of crimes related to cyber field could credit its origin and existence to the up surging dependence on the gadgets in our present day lives. Thus the very incidences gave a new impetus to the field id computing into a more criminal intruding nature rather than a sinister implication (Choudhary and Basak, 2013, p.123). There exist certain globalized occurrence which are cutting at light speed over borders and often executed by perpetrators who are often strenuous to unearth and even every so often unfeasible to spot. These situations can be listed as cyber terrorism, cyber warfare and cyber crime. Combating such activities and perpetrators require not only well built domestic footing and capabilities but also comparably brawny capabilities. The event also requires robust cooperation system among states and their different institution (Friedman & Singer, 2014, p.203).These situations can light national security additionally other interests of a state which every government need to be well aware of. To tackle with such situation the most prior initiation is the formation of a global action strategic plan.

States while formulating these actions should incorporate international standards and measures that contain enforcement methods which could be applied across for disseminating and sharing information that need to be put in place sooner rather than later. Many international forums like UN and various agencies came forward and took the lead in generating mechanism to tackle with the bad impacts of cyberism and to get into a consensus with different nations approach (Meeuwisse, 2015, p.135). These efforts till date have had limited impression and which require more initiations. Cyber terrorism, Cyber crime and Cyber warfare give rise to existent and notable warning to national security of any country. It's high time to commence a mixed approach by taking into consideration of the regional peculiarities and wrapping it along with the international standards and process, thereby, an incorporated mechanism to tackle the situation could be set out. (Ramesh, 2013, p.89-91).

Conclusion

A human mind dimension is inscrutable and is not attainable to do away with cyber crime from the cyber extent which is utterly viable to check. If we take an account of past event we could realize that so far no legislation did succeed in completely banish this menace from the globe. The only concern available at the moment is to make people conscious of the situation and do inculcate an awareness of their duties and rights in reporting a situation of such crime on tie. Laws concerning the matter need to be applied properly and checked stringently accordingly. Undoubtedly the Act concerning the balancing of cyber activity and related laws is a historical step in the cyber world (Dashora, 2011).

In bygone days due to the alarming upsurge of cyber attacks on all most all fields there happened to be a tendency of more forms of in industry and states on raising an apparatus to amplify their dimensions in combating this menace of cyber malpractices, cyber espionage, cyber terrorism and cyber warfare. The situation also contains a major transfer of funds, efforts and centre of attention to these

areas. (Deepak, 2020). Several nations are generating cyber defense mechanisms within their national security institutions and intensifying their cyber capabilities by creating a staunch cyber warfare unit within the ambience of their defense institutions. The other force is at the initial scene of getting aware of the timely need of being alert to cope with this rising menace.

The realm of cyber field is composite, multi complex, and continuously progressing. States today are progressively trying to create cooperation among domestic state cyber institutions and academic by accepting the interpretative interlink among the different actors and reinstate the requirement for cooperation and innovation (Desai, 2020). Contemporary age ensures that traditional mechanisms of cyber security are inappropriate to combat the menace of cyber crime. Consequently, there is a demand to conceive mechanism that is proactive in nature and aid in recognizing and averting cyber crimes.

If we take an account of past events, cyber crimes have turns fiercer, enlightened and potentially debilitating for individuals, institute and countries. The current difficulty faced by the enforcement mechanism concerning the tackling of this menace is that it finds difficult to scan and put an end to the act in the cyber space as the on doers of these incidents are faceless and sustain low budget to execute such a crime considering that, the cost of inhibiting the act is more costly and high. The count of target is increasing each day due to the expanding of dependence in the internet. These days the multitude of cyber crime is often changing from the previous computer hacking style to a much diversified form like theft of data, child pornography, Critical Information Infrastructure (CII) attacks and so on (Yadav & Kiyawat, 2016,p.130). Our country is fetching more vulnerable choices to this menace due to fast pace of the process of digitalization and escalation of mobile data without complementing the speed of cyber security measures and cyber hygiene process. Today we stand third position in facing cyber crime incidents after the United States and China.

As per official data, one cyber crime is getting reported every ten minutes (2017 report). The need of the hour is to facilitate a framework for addressing cases related to cybercrime for timely apt solution of concerning matters as developed by some nations. In India an inter ministerial commission Phone Frauds got constituted under the Ministry of Home Affairs in September 2017, still more miles to go in tackling this issue. Another step in this matter is the setting up of centres of Cyber Swechhta Kendra which is regarded as a right management in the making of a secure cyber ecosystem (Kamath, 200, p.220). However, such initiations require a lot more background work to prepare a realm of tools that each Indian could trust and could use to shield their delicate date. At present India maintain MoU with countries like Bangladesh, Israel, Japan, Russia, Singapore, Spain, Maysia, Usbekistan, US, Vietnam and the European Union in the areas of cyber crime and cyber fraud. India should march ahead to increase collaboration with different countries in this arena. The act would result in as much more coordinated and consumed mode of governance on cyber concerning matters and enhance in capacity buildings at different measures which will prompt us to accomplish efficacious and timely cyber crime management mechanisms at every levels (HT, 2020).

The most striking duty of law at this moment is to find a total balance strategy among shielding its citizens from the act of crime and in infringing them on their very rights. In the march of period always there will be new and unforeseen threads to stay forward of cyber criminals and terrorists of the field. The situation could be tackled effectively only through partnership and cooperation among citizens and government. Yet our nation did take a lot of measures to wipe out the menace of cyber crime still, the cyber law cannot purvey to be static, it has to run with the changing time and should come out from the cocoon of status quo and should wear the attire of pro activeness clothed with adaptability which is the prime requisite of the moment.

COVID 19 apps that are used by different states are not aptly tested and these days they are host to many cyber related crimes even in this most crucial time. There is an urgent need for structural adjustment, personnel motivation, technological development, training and attitudinal changes among the

law enforcing personnel. Besides, the world immediately needs evolving of a global mechanism to check the expanding and perpetually changing face of cyber crime.

References

1. Chander, Harish. (2012). *Cyber Laws and IT Protection*, New Delhi: PHI Learning.
2. Choudhary, Rajarshi and Basak, Somath. (2013). Cyber Crimes – Challenges and Solutions, *International Journal of Computer Science and Information Technologies*, 4(5), 715-732.
3. Dasguptha, M.(2009). *Cyber Crime in India: A Comparative Study*, Kolkata: Eastern Law House Private Ltd.
4. Dashora, Kamini. (2011). Cyber Crime in the Society, Problems and Preventions, *Journal of Alternative Perspectives in the Social Sciences*,3,1,240-259.
5. Duggal, Pavan. (2004). *Cyber Law : the Indian Perspective*, New Delhi: Saakshar Law Publications.
6. Friedman, Allan and P.W. Singer. (2014). *Cyber Security and Cyber War, What Everyone Needs to Know*, USA: OUP.
7. Gupta, M P, Prabhat Kumar and Jajit Bhattacharya. (2004). *Government Online – Oppurtunitiesand Challenges*, New Delhi: Tata McGraw Hill Publishing Company Limited.
8. Halder, Debarati and Jaishankar, Karuppannan. (2014). *Cyber Crime and the Victimization of Women ; Law, Rights and Regulations*, UK: Cambridge Scholars Publishing.
9. Halder, Debarati and Jaishankar, Karuppannan. (2016). *Cyber Crimes Against Women in India*, New Delhi: Sage Publications.
10. K, Jaishankar . (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*, USA: Taylor and Francis Group.
11. Kamath, Nandan. (2000). *Law Relating to Computers, Internet, and E-commerce: A Guide to Cyber laws and the Information Technology Act, 2000*, New Delhi: Universal *Law* Publishing Company Pvt. Limited.
12. Meeuwisse, Raef. (2015). *Cybersecurity for Beginners*, US: Cyber Simplicity Ltd.
13. Mishra, S.S, Pani, N, and Sahu,B.S. (2004). *Modern System of governance: Good Governance Vs E- Governance*, NewDelhi : Anmol Publications.
14. Singh, Ramesh. (2013). *Contemporary Essays*, NewDelhi : Mc Graw Hill Education (India) Private Limited.
15. Stallings, William. (2005). *Cryptography and Network Security; Principle and Practice*, US: Prentice Hall.
16. Jeevan,Deepak. (2016,May 09). Is Cybercrime Inevitable in a Connected World?, *Yale Insights.* Retrieved from https://insights.som.yale.edu/insights/is-cybercrime-inevitable-in-connected-world
17. Vishwakarma,Nishitha. (2017, Oct 25). Cybercrime Cases Double in 2017, 56% Cybercrime Cases for Fraud Motive: NCRB 2017 Report, *Mediana.* Retrieved from https://www.medianama.com/2017/10/223-cybercrime-ncrb-2017/
18. Deepak, Pinto. (Feb 23, 2020). India Stands Third Among Top 20 Cyber Crime Victims, Says FBI Report. The New Indian Express. Retrieved from
19. https://www.newindianexpress.com/nation/2020/feb/23/india-stands-third-among-top-20-cyber-crime-victims-says-fbi-report-2107309.html
20. Dewanji, Sanika. (April 20,2020). Cyber Crime in India- Statistics and Facts. *Statista*. Retrieved from https://www.statista.com/topics/5054/cyber-crime-in-india/
21. HT Correspondent. (May 16,2020). 37 Cyber crime Cases Registered in Pune Region during Lockdown Period. *Hindustan Times*. Retrieved from https://www.hindustantimes.com/cities/37-

cybercrime-cases-registered-in-pune-region-during-lockdown-period/story-3aw80FX4bUSOBSKzrGsn7M.html
22. Desai, D, Ronak. (May 19, 2020). Cyber Crime in Insia Surges Amidst Corona Virus Lock Down. *Forbes*. Retrieved from https://www.forbes.com/sites/ronakdesai/2020/05/14/cybercrime-in-india-surges-amidst-coronavirus-lockdown/#8f65d6c392e2.