Identifying The Challenges Of Criminal Justice System While Responding To Cyber Economic Crime

Balsing Rajput,
PhD Research Scholar,
School of Law, Rights and Constitutional Governance,
Tata Institute of Social Sciences, Mumbai, India

Abstract: The Internet has become an integral part of the life and business. It has contributed to a change in society, significant impact on business, manufacturing, service industry, government services, critical infrastructure, security setup and other fundamental aspects of modern society. Mobile technology, Internet, cloud computing and advances in networking through fourth and fifth generation technology has brought everything on the palmtop. With the advancement in the technology, more use and reliability on the Internet in various businesses and government services has contributed to the increase in cybercrime. Criminals are harnessing the Internet for committing the crime. Economic gain is the primary motive to commit the crime. Now, cyber economic crimes are the significant portion of the cyber crimes in India. Cyber crimes and cyber economic crimes are increasing at an alarming rate in India. Mumbai, being a financial capital, accounts for more number of cyber economic crimes in India. While responding to the new phenomenon of the cyber economic crime, traditional criminal justice system is facing various challenges. Technical, Operational, Legal, and Human resource are main four types of challenges that all the stakeholders of the criminal justice system facing while dealing with cybercrime

Index Terms **– Cyber Crime, Cyber Economic Crime, Criminal Justice System.**

1. INTRODUCTION

The Internet has gone beyond imagination since its inception in 1989 and has become the most significant technological advancement in the world. The Internet has become an integral part of the life and business. Today the world is more connected as compared to any point in history. Computer science and digital technology have revolutionized the world. "The World Wide Web (www)" has now transformed the world into a global village. Digital communication and interaction have covered nearly two-thirds of the world population. Same way, it has contributed to a change in society, significant impact on business, manufacturing, service industry, government services, critical infrastructure, security setup and other, fundamental aspects of modern society. Thus, the Internet has revolutionized the world in different ways; it has facilitated e-commerce, virtual community through social networks, online education, and online entertainment, online services, and products and other essential activities.

Jang and Lim (2013) mentioned that Information Technology (IT) and the Internet have helped overcome the barriers of time and space to connect to each other in cyberspace. Today Information and Communication Technology (ICTs) is omnipresent, and demand for Internet-enabled technology has driven computer technology-enabled products. Now cars, buildings, electricity distribution, transportation, military services, logistics of society are all dependent on Information and Communication Technology (Gercke 2014)(Jang and Lim 2013)

Mobile technology, Internet, cloud computing and advances in networking through fourth and fifth generation technology has brought everything on the palmtop. Everyone from rich to poor and urban to rural areas is using mobile, and all work from office to shopping is being carried out using mobiles online. The Internet is one of the fastest growing sectors in India. Telecom regulatory authority of India report mentions that overall Tele-density in India is 86.25 at the end of October 2016. The urban area subscription is 642.37 million and the rural subscription 460.57 million. The total wireless subscriber base is 1,078.42 million in 2016. It shows that India is one of the top countries in the world in the use of telephones, which is basic infrastructure for Internet (Report of Telecom Regulatory Authority of India 2017)

Now, most of the financial activities in the business and personal life are being carried out through online medium. Thus criminal activities are also increased on the online medium. Cyber Crime is a global phenomenon, and India is no exception to it. Cyber economic crimes are heavily present in India. The development of specialized software's for commercial crimes by criminal networks have raised the possibilities of cybercrime in many folds, the primary motive for this remains the financial gain (Broadhurst and Chang 2012).

2. CONCEPTUAL FRAMEWORK

It is very important to understand the key concepts of the field, before identifying the challenges faced by the various stakeholders of the criminal Justice system. Interconnected computer system with Internet creates the virtual world. Cyberspace is the one such concept we need to understand, as all activates related to cyber economic crime takes place in cyberspace.

2.1. Cyber Space

Cyberspace is a fact of daily life. The word "Cyberspace" has been in our lexicon for three decades, since William Gibson, who used this term to describe "a consensual hallucination" in his science fiction novel, "*Neuromancer*". Libicki (2009) described that the concept of the cyberspace is contentious and plastic. Cyberspace can be described as analogues to the Internet. It can be further clarified that cyberspace is an agglomeration of individual computing devices that are networked to one another and same network to outside network and devices. Cyberspace is a virtual medium and further explained as one far less tangible than ground, water, air, or even space (Libicki 2007)(Libicki 2009)

2.2. Cyber Crime

With the advancement in the technology and more use and reliability of computer machines in various businesses and government installations, the quantum of this crime is increasing. Many organizations and scientists have attempted to define the cybercrime, but there is no accepted precise definition of 'cybercrime.' Cybercrime activity may consist of traditional crimes (fraud, theft, extortion) or 'new' types of criminal activity (denial of service attacks, malware) "(Brenner and Clarke 2005).

Cyber Crime is a type of crime that involves the abuse of Information Technology. Cyber Crime is categorized and defined in two ways at tenth UN Congress on Prevention of Crime and Treatment of Offenders: (1) "Cyber Crime in a narrow sense (computer crime): Any illegal behavior directed utilizing electronic operations that targets security of computer systems and data processed by them. (2) Cyber Crime in a broader sense (computer-related crime): Any illegal behavior committed utilizing or about, a computer system or Network (Tenth United Nations Congress 2000). Another definition offered is Cybercrime can be regarded as "computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks" (Thomas and Loader 2000). A practical definition of cyber crime is given by Kshetri (2010) as "Cyber Crime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules or regulations" (Kshetri 2010).

2.3. Economic Crime

In the crime sphere of India, economic crime amount to 4.8 % of the total crime. With the advancement in the technology and more use and reliability of computer machines in various businesses and government installations, the quantum of this crime is increasing. Even though, there is mention of crimes of economical nature in Indian literature, the concept of the economic crimes was first introduced the by Sociologist Edwin Sutherland coined the term "white collar crime" in 1939. Sutherland defined white-collar crime as a crime committed by a person of respectability and high social status in the course of his occupation (Sutherland, 1942), (Sutherland 1945). Economic Crime is defined as an illegal act (or a constantly evolving set of acts) generally committed by deception or misrepresentation (fraud) by someone (or a group), who has specialized professional or technical skills for the purposes of personal or organizational financial gain or to gain (or attempt to gain) and an unfair advantage over another individual or entity (Gordon, 1996).

2.4. Cyber Economic Crime

The commission of the economic crime using the various tools of computer and Internet is now growing. This has given rise to a new class of crime within the cybercrime domain that is Cyber economic crime (CEC). Virtual financial crime is part of cybercrime. The percentage of cybercrime for economic gain or motive has been increasing. It is where financial crimes such as fraud, money laundering, online scams, phishing, etc. take place on the Internet. It is part of the cybercrime umbrella (Chambers-Jones 2012).

While studying the concept of the Cyber economic crime it has been considered that Economic and cybercrime are part of the more significant concept of the crime. Financial crimes are more related to economic aspects of the crime. While Cybercrime is nothing but the use of the computer as a tool, target or to facilitate to commit the crime. The cyber and Financial crimes have an enormous impact on the technology, and are driven by technology and its vulnerabilities. Cyber economic crimes are those crimes, which, are perpetrated using cyber technology but primarily for financial gains.

In Indian setup, there is not a clear-cut division of the cyber economic crime by National Crime Records Bureau, but from the characteristics and sections of the law applied it can be segregated. IT Act 2000 is also a special law for information Technology enabled crimes. Cybercrimes comes with three legal blends in India. One purely under Information Technology Act, 2000, another Indian Penal Code (IPC) coupled with IT Act 2000. The third one is Special Local Law (SLL) coupled with IT Act 2000. Last and most complex is IPC coupled with special laws and IT act. (National Crime Records Bureau 2015)

There are no sections in the IT act, which covers the criminal acts like Cheating, fraud, and breach of trust, which covers mainly cyber economic crimes. Thus, Crimes having connotations of financial aspect attracts the IPC sections of cheating, fraud, and forgery and counterfeiting in addition to the IT act sections if the act is carried out using a computer or facilitated by the computer or internet. Offenses are covered as per Indian penal code, and IT Act or special acts in combination and these acts has been considered as cyber economic crimes in Indian Set up. In a nutshell as per the NCRB data classification cybercrime cases with IPC and SLL sections are considered as Cyber Economic crimes (National Crime Records Bureau 2015). Increasing use of social media and personal devices in the workplace, cybercrime was the third most prevalent economic crime in India in 2010, and now in 2016, Cybercrime climbs to the second spot for affecting organizations economically. The interesting aspect about opportunities to commit the fraud in India is highest and twice the global to commit the fraud (PWC Fraud survey of India report, 2010) (PWC Global Economic Crime Survey and PWC 2016) (KPMG India Fraud Survey 2012).

2.5. Criminal Justice System

Criminal justice system followed for the dispensation of the justice in criminal matters is basically the adversarial system of common law, which is established by British rule (Thilagaraj and Kala 2013). Today, Criminal justice system consists of some set of institutions under different systems of control and accountability (N. R. M. Menon 2002). Pillars of the criminal justice administration are Police, Courts, prosecutors, defense lawyers, forensic experts, and correctional systems. Criminal Procedure Code 1973 is the primary law, which defines the role and responsibility of the stakeholders in the criminal procedures.

Figure.1 Various Stakeholders of Criminal Justice System in India

Fig.1 depicts various stakeholders of the criminal justice system and roles of various stakeholders are different as per the legal framework and responsibility distributed in the criminal justice system. Law Enforcement agencies are the first respondent. Police registers the First Information Report and then investigates. Detection of the perpetrators, arrest of the accused and filing the charge sheet is the responsibility allotted to the police. Taking measures to prevent the crimes is also allotted to the police. Forensic laboratories are responsible for analysis of the evidences and submit the report to the investigation agency and courts. Prosecution

department is responsible for presenting the case in court of law on behalf of the state. Defense lawyers and Bar renders legal services to accused for their defense in the court of law. Judiciary is the central agency; all the work revolves around it. The primary task of the judiciary is conducting the trial of the case. The correctional system comes in the picture once accused is convicted and sent to jail for correction. Challenges faced by these stakeholders have been elaborated in this study.

2.6. Legal Framework for Cyber Economic Crimes

Principle act for criminal activities in India is Indian Penal Code 1860, which deals with all the major criminal acts. Information Technology Act, 2000, amended in 2008 is the special act, which deals with the criminal acts committed using information technology. Criminal Procedure Code, 1973 is the primary procedural code, which is standard for all the criminal trials with some variations if provided in any special act. Indian Evidence Act 1872 is the primary Evidence Act, which is also applied for all the trials of the economic crimes. These laws also handle crimes with economic connotations; there is no special law for economic crimes in India. Legal Challenges has been identified considering the above set of laws in this study.

3. RESEARCH DESIGN AND METHODOLOGY

Study of this new class of the crime has not been carried out in Indian set-up, as this is newly emerging crime. The present study is the exploration of the phenomenon of this new class of crime and response of the criminal justice system to the cyber economic crimes. There is a tremendous gap of knowledge regarding the investigation, prosecution, and trial of these offenses in India. Rational of this research is to fill the gap and explore this phenomenon. The present study is conducted in Mumbai City of Maharashtra State being the economic capital of India and as it reports the number of economic offenses. The reference period of study was decided to fix a time frame of 15 years that is from the inception of the IT act 2000.

3.1. Methodology

A mixed methodology is followed to carry out the research. Quantitative method is being used to study the trend of cyber Economic crimes. Data has been collected from government agencies like National Crime Records Bureau, New Delhi and State Crime Records Bureau, Pune, Maharashtra Cyber-office, Crime Branch, Mumbai Police and other government, non-government sources. Analysis of the Data collected from above sources has been used to understand the phenomenon of CEC.

To understand the phenomenon and identify challenges of cyber economic crime in India exploratory qualitative study has been carried out, which includes the personal visits and observations. To identify the response, problems and challenges encountered by various stakeholders in-depth personal interviews of key informants and Focused Group Discussion has been carried out with all the stakeholders like investigating agency, prosecuting agency, the victim, criminals, judiciary and academician, cybersecurity professionals.

4. CYBER ECONOMIC CRIMES IN INDIA

4.1. Incidences of Cyber Economic Crimes in India

The quantum of the cyber economic crime in total crime sphere is very small, but it is remarkable that the percentage of share is increasing at alarming speed each year due to use of mobile and computer technology in every sphere of life. Incidences of the total cybercrime cases registered or reported to the law enforcement agencies are collected from NCRB data from the year 2002 to the year 2016 are presented in the table. The IT act was passed in 2000, and actual registration of cases started as per IT act form 2002.

Table 1 Total Cyber Crime Incidences from 2002 to 2016

Total Cyber Crime Incidences from 2002 to 2016				
Jurisdiction	IT Act	IPC	SLL Act	Total
India	35292	14760	460	50512
Maharashtra	3059	5827	21	8907
Mumbai	219	2771	6	2996

The analysis of the data from Table 1 shows that in total 50512 incidences of cyber crime took place in India from 2002 to end of 2016. Maharashtra accounted for 16 % of the total incidences of the cybercrime in India and Mumbai city has witnessed 6 % of the total incidences that India registered in total. It is important to notice that these are the recorded incidences by the law enforcement agencies but, there may be many incidences which have not been informed to law enforcement agencies or after receiving might not have been converted to First Information Report.

.

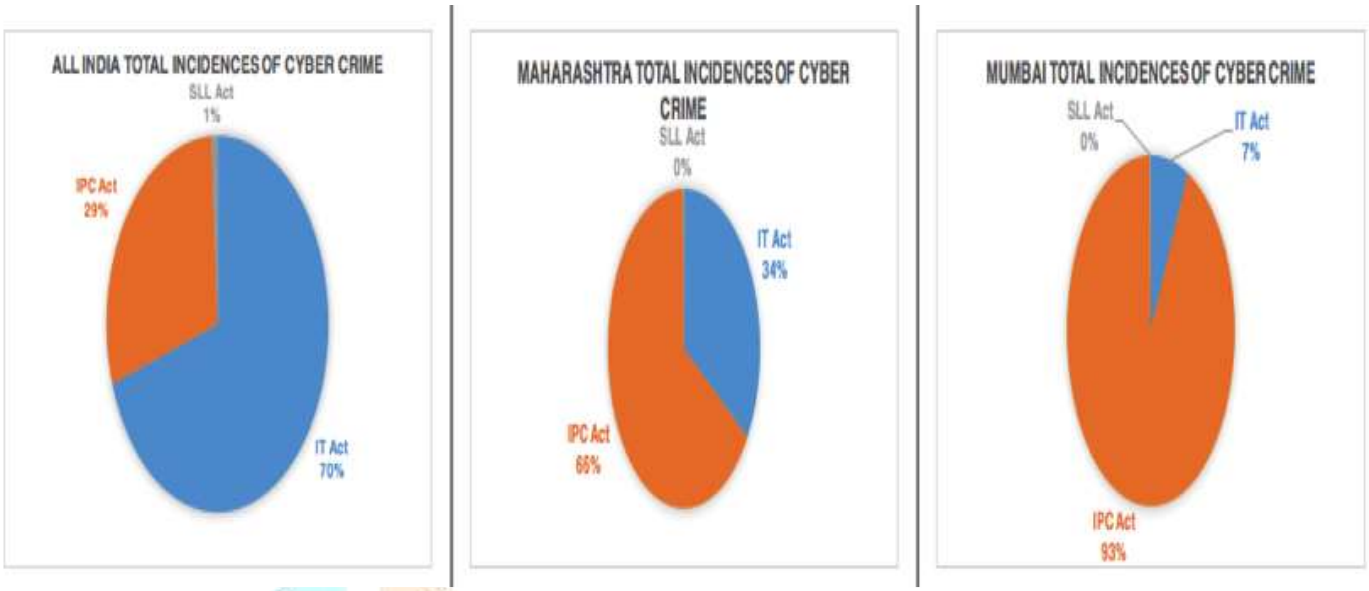

Figure 2 Share of Cyber Economic Crime in Cyber Crimes in India

Fig.2 shows cybercrimes registered with different acts all over India. From the analysis of the data of Fig.2, it is noticeable that cases registered with IT act are dominating with 70% of the overall figures and cases of cyber crimes registered with IPC Act are 29 % of the total cases. SLL cases are decidedly less or negligible amounting to 1 % of the total incidences of the cybercrime in India from 2002 to 2016. Thus, it can be concluded that Cyber Economic crime cases which are (IPC and SLL) cases, together are 30% of the total Cybercrime cases registered in India from the enactment of the IT Act in the year 2000. In Maharashtra, pattern of cybercrime cases is reverse as compared to India. In Maharashtra, out of the total registered cases of cybercrime, 66 % of the cases are Cyber Economic crime cases (IPC +SLL). In Mumbai, this pattern further deepens and takes very vivid shape depicting 93 % of the total cases registered are Cyber economic crime cases (IPC and SLL) and only 7% cases are registered with pure IT act. Cyber Economic crimes are dominant in Mumbai and Maharashtra as compared to India. The share of Cyber Economic crime cases is more than 66% in Maharashtra and 93% in Mumbai in total cybercrime cases registered from the enactment of the IT act.

4.2. **Cyber Crime and Cyber Economic Crime Trends**

Mapping of the total number of total Cybercrime cases (IT Act + IPC + SLL) registered each year over a period of 15 years (2002 to 2016) is carried out.

Figure 3 Cyber Crime Trends over 15 years

Fig.3 clearly shows that up to 2008 the rate of registration was low and steady for all and number of cases registered in Mumbai and Maharashtra were low, but after 2008 the rate of cybercrime cases has increased. In 2009, there is 50 % rise in cases as compared to previous year in India. In general, from 2008 to 2015 there is more than 50% rise each year as compared to previous year. In Maharashtra and Mumbai, the rise is 313 % and 225 % respectively, which is phenomenal. The rising trend is continuous in India and Maharashtra up to 2015. With respect to Mumbai, there is no continuous rise, but abruptly there are falls in 2011 and 2013. This can be attributed to the amendment in the IT act in 2008 to make it more flexible, and more number of offenses were included. It is also noticeable that after 2014 there is a drop in the rate of increase of cybercrime in India. The graph shows that rate of increase in India is significant. The general trend of cybercrime cases is increasing each year with alarming proportion.

4.3. Trends in Cyber Crimes IPC, IT act, SLL cases In India, Maharashtra, and Mumbai

The general trend observed is that up to 2008 there is no significant presence of Cybercrime and Cyber Economic crime cases. After 2008, the highest growth rate is observed in IT act cases in India.

Fig. 4 shows that Up to 2008, Cyber Economic crime cases (IPC cases) at Maharashtra and Mumbai are negligent, but there is a significant presence of Cyber Economic crime cases (IPC cases) at India level. After 2008, the cases of Cyber Economic crime cases (IPC cases) have raised significantly in Maharashtra and Mumbai as compared to IT act cases. Highest growth is observed in IPC cases in Maharashtra and Mumbai.

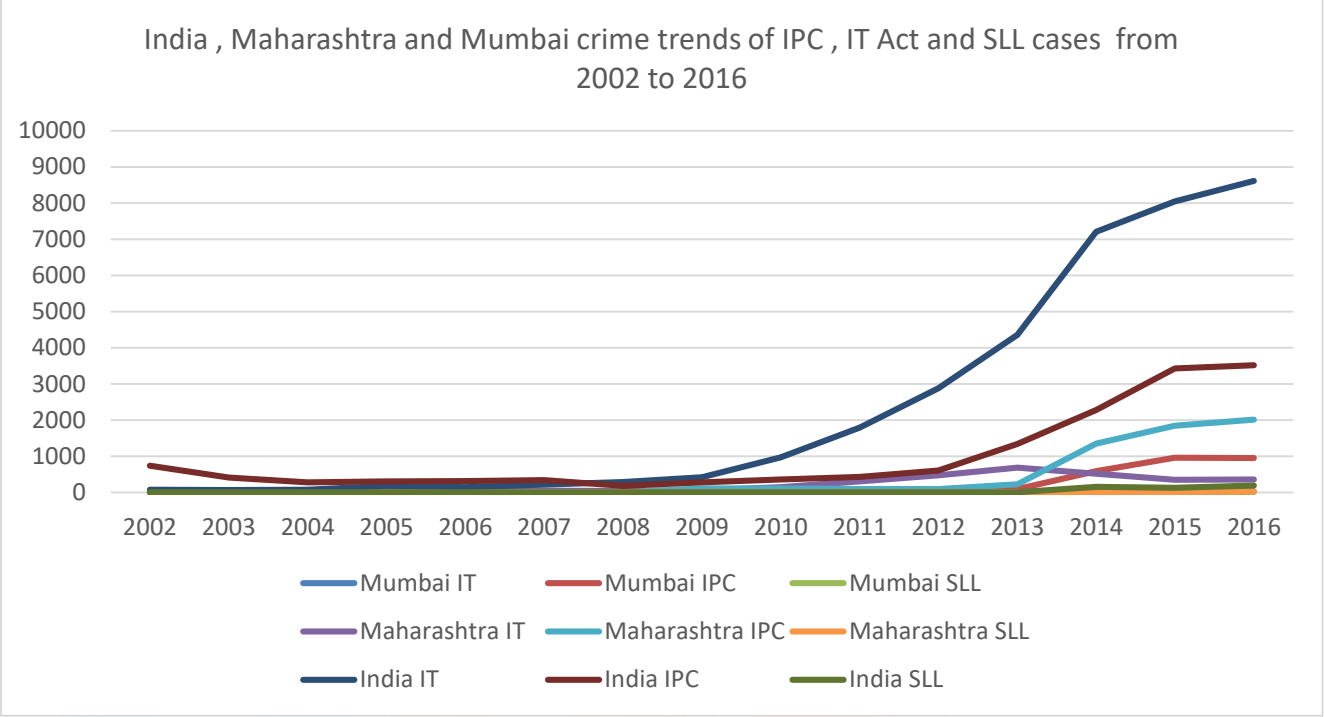

Figure 4 Trends in Cyber Crimes IPC, IT act, SLL cases In India, Maharashtra, and Mumbai

5. CHALLENGES INDENTIFED

Challenges have been identified from various stakeholders of the criminal justice for responding to Cyber Economic Crimes. All the stakeholders have to process the cases of cyber economic crimes. Fig. 5 depicts overall picture of challenges faced by various stakeholders of Criminal Justice System. Technical, Operational, Legal, and Human resource are man four type of challenges that all the stakeholders of the criminal justice system are facing while dealing with cybercrime. An earlier study conducted regarding prevention and control of cyber crimes in India also concludes four types of problems like technical, legal, operational and jurisdictional (Godara 2011).

Figure 5 Challenges faced by various stakeholders of Criminal Justice System

5.1 Technical Challenges

5.1.1 Lack of IT Infrastructure

All the stakeholders in the criminal justice system are not having adequate and advanced information technology hardware and software. Cyber forensic equipment's for investigation and evidence analysis is lacking at police establishments and forensic laboratories. Quality of investigation is impacted adversely due to Lack of tools and technology.

5.1.2 The anonymity of Internet

Anonymity is the dominant feature of the Internet, and this encourages the criminal behavior. It also created a significant hurdle for investigation agency to trace, locate and identify the accused. It has been rightly noted that Internet has become a conduit for the criminal activities due to its anonymity (Wall 2010).

5.1.3 Dark Web and illegal Trade

Heinous crimes in the physical world have been now shifted to the cyber world due to fast-encrypted communication, anonymity and global reach. Dark web uses a browser like Tor, which makes the tracing nearly impossible for investigation agency. Due to technical hurdles, it has become a challenge to stop the illegal activities on Dark web for law enforcement agencies.

5.1.4 Encrypted and peer-to-peer communication

Internet application like WhatsApp and Telegram provides fast and encrypted communication. To trace and recover such communication in crimes is very important, but due to technical problems, it not possible. This challenge has kept many crimes undetected. These applications have now become primary tools of communication for criminals.

5.2 Legal Challenges

5.2.1 Jurisdiction Issue

Cyber Crime is a borderless crime. The virtual world does not recognize physical boundaries. Anyone from anywhere can commit a crime anywhere is the unique characteristics of the cybercrime. Due this problem, fixing the jurisdiction of the crime is a very complicated issue for the criminal justice system. In the virtual world, the victim may be in one state, the IT set up may be in other state and the criminal may be in the third state, is such situation locating correct jurisdiction for prosecution is challenging. United Nations agency has also conducted a detailed study of cybercrime and identified a jurisdictional issue as a major challenge. It has suggested for development of model provisions for fixing the jurisdiction of cybercrime to provide a common base in all countries (United Nations Office on Drugs and Crime 2013). The government of India has acknowledged the problem of jurisdiction and is creating a common portal as per Supreme Court direction for reporting of the cybercrime (Ministry of Home Affairs 2018).

5.2.2 No legal Provisions for the new form of crimes

Information Technology Act 2000 is the special act to tackle the cybercrime. IT act was enacted in 2000 and amended in 2008. It is important to note that basic premise of the law is not prevention of cybercrime but to foster the e-commerce in the country. Due to this objective, there are many criminal acts, which has not been covered under the law. The new evolving technology used for crime and Criminal acts like cyber defamation, cyberstalking and trolling are not covered in this law. There is demand for amendment in the IT act 2008 to include more crimes. Draft national policy on the criminal justice of government of India also mentions about the reclassification of the codes and creation of the new code for economic crimes in the country (M. N. R. Menon 2007).

5.2.3 Section 65 B Certificate

Section 65(b) certificate as per Indian Evidence Act is the major hurdle in case of Foreign Service provider sharing evidence. Foreign companies work as per their law of the land. These companies do not issue section 65(b) certificate to investigation agencies, due to which court rejects the evidence. To achieve the conviction, this has become a significant challenge. There is need to amend section 65 (b) of the Indian evidence to make electronic evidence more acceptable in courts.

5.2.4 International Information Sharing / Collaboration

In information technology domain with the introduction of Internet and cloud technology, all the information and data is stored in various parts of the worlds. There is no physical constraint to store the information in the country. It is also important to note that there is no specific legal arrangement for localization of data generated in India. Many times servers are located in USA or European Countries for email and social media applications. At international level information sharing takes place as per Mutual Legal Assistance Treaty (MLAT) and other international agreements. Investigations are pending for necessary information and evidence from service providing companies from the foreign land. Criminals are having no constraint, as cyber economic crime is a borderless crime, but law enforcement agencies are facing a major problem of collection of information from foreign countries. United Nations office on drugs and crime studied the issues of cybercrime in 2013 has concluded reliance on traditional and formal international cooperation is not working in case of cybercrime to get a timely response for obtaining evidence (United Nations Office on Drugs and Crime 2013).

5.3 Operational Challenges

5.3.1 Investigation of Cybercrime

There is a provision in Section 78 of Information Technology Act 2008 for investigation of Cybercrime by Police officer of the inspector rank. The field level this provision has proved to be a major challenge, as at police station level officer of the rank of Police inspector are very few. This creates a tendency of non-registration of cybercrime cases at police station level. At Police station Police inspector rank officer is responsible for administration and supervision of the police station, which gives very few time for investigation. Provision should be changed, and officer of the rank of sub-inspector should be entitled to the investigation of Cybercrime.

5.3.2 Non-co-operation form service providers

Challenge of Prevention cybercrime: Prevention of cyber economic offenses over Internet has become a big challenge. As the regulator in one country blocks even the pages, things are visible using the Virtual Private network. There is no state control over the Internet, and no single agency controls the Internet. Thus, prevention of criminal activities over Internet has become a significant challenge as considering the nature of the Internet.

5.3.3 Pendency of cases

Pendency due to the shortage of Manpower and infrastructure is a big challenge for forensic laboratory and judiciary. Cases take nearly year and more to reach to the logical conclusion. Pendency is the major challenge. The root cause for this challenge is a paucity of technical tools and lack of skilled human resources.

5.3.4 Lack of Coordination of Various Stakeholders

Criminal Justice system consists of many known and unknown contribution of various institutions and persons to bring the one case to the logical conclusion and accord justice to the victims. However, the irony is that all the organizations work in a silo and have very less harmonization and synchronization. The study conducted on the challenges of coordination in cybercrime and cyber security has also proved that there is Need for harmonization of various stakeholders of the criminal justice system (Jang and Lim 2013). Coordination with Service providers and intermediaries is also a major challenge to get evidence at the right time. Most of the time these companies deny information for various reasons creating hurdle in the investigation.

5.4 Human Resource Challenges

5.4.1 Lack of Skilled Manpower

Criminal justice system is traditional and not having the adequate skilled human resources for cyber economic crimes, as it is a new phenomenon. There is a gap between the number of offenses registered and a number of officers available for dealing with it with all the stakeholders. There is immense workload of existing cases of traditional crimes and officers are finding it difficult to deal with the cyber economic crimes due paucity of skilled human resources.

5.4.2 Training and Capacity Building

Present frequency and quantum of training are not adequate for meeting needs of new technology. Every day various new crime forms are evolving, and the technology change is so fast in the domain of Information technology that every year new technology is coming, which is creating challenges for the training of staff. The parliamentary committee on information technology has also identified the problem of training of human resources cybercrime and suggested separate nodal agency for cybercrime (LokSabha Secretariat 2017).

5.4.3 Technology and Knowledge Gap

There is technology and knowledge gap for new forms of crime and technology with the traditional Criminal justice system. There are no settled techniques, laws and Standard operating procedures for dealing with emerging technologies, which posing as a big challenge. There are very few case laws, cases studies, forensic tools, and technologies with criminal justice system in India; thus there is knowledge gap in the system, as a system is more accustomed to deal with traditional forms of crime.

6. CONCLUSION

The Internet has become an integral part of the life and business. The quantum of the cyber economic crime in total crime sphere is very small, but it is remarkable that the percentage share is increasing at alarming speed each year due to use of mobile and computer technology in every sphere of life. The general trend is that cybercrime is increasing, and Rate of increase of cybercrime in India is significant. Technical, Operational, Legal, and Human resource are man four type of challenges that all the stakeholders of the criminal justice system facing while dealing with cybercrime

7. REFERENCES

[1] Brenner, Susan W, and Leo L Clarke. 2005. “Distributed Security: Preventing Cybercrime.” The John Marshall Journal of Information Technology & Privacy Law 23 (4). http://repository.jmls.edu/jitpl/vol23/iss4/1.

[2] Broadhurst, Roderic, and Yao-Chung Chang. 2012. "Cybercrime in Asia: Trends and Challenges." Asian Handbook of Criminology, 1–26.
[3] Chambers-Jones, Clare. 2012. "Cyber Economic Crime and Commonwealth Laws." Law Governance and World Order, no. 2012: 373–81. doi:10.1504/IJIPM.2013.053451.
[4] Gercke, Marco (International Telecommunication Union). 2014. "Understanding Cybercrime: Phenomena, Challenges and Legal Response Purpose."
[5] Godara, Samiksha. 2011. "Prevention and Control of Cyber Crime in India: Problems, Issues, and Strategies." Maharshi Dayanand University, Rohtak.
[6] Jang, Yunsik Jake, and Bo-young Lim. 2013. "Harmonization among National Cyber Security and Cybercrime Response Organizations: New Challenges of Cybercrime." arXiv:1308.2362 [Cs], no. 2010: 1–15. http://arxiv.org/abs/1308.2362%5 Cnhttp://www.arxiv.org/pdf/1308.2362.pdf.
[7] KPMG India Fraud Survey, India. 2012. "India Financial Crime Survey Report 2012."
[8] Kshetri, Nir. 2010. "The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives." The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives, 1–251. doi:10.1007/978-3-642-11522-6.
[9] Libicki, Martin C. 2009. Prepared for the United States Air Force. Cyber deterrence and Cyberwar.
[10] Libicki, Martin C. 2007. Conquest in Cyberspace. Cambridge University Press. doi:10.1017/CBO9780511804250.
[11] LokSabha Secretariat, Delhi. 2017. "42 Second Report of Standing Committee on Information Technology." Vol. 1939. New Delhi.
[12] Menon, Madhava N. R. 2007. "Committee Report on National Policy on Criminal Justice." New Delhi. http://mha.nic.in/sites/upload_files/mha/files/pdf/DraftPolicyPaperAug.pdf.
[13] Menon, N.R.Madhava. 2002. Criminal Justice India Series, Vol. 4 (HB). Edited by Madhava N.R. Menon. First Edit. Allied Publishers private limited in collaboration with National University of Juridical Sciences, Kolkata. https://books.google.co.in/books? id=DY6FEMoIeqsC.
[14] Ministry of Home Affairs, GoI. 2018. "Advisory on Cyber Crime Prevention and Control." New Delhi: Ministry of Home Affairs, Government of India.
[15] National Crime Records Bureau, GoI. 2015."Crime in India -2015." http://ncrb.nic.in/StatPublications /CII/CII2015/Chapters.htm.
[16] PWC Global Economic Crime Survey, and PWC. 2016. "Adjusting the Lens on Economic Crime Preparation Brings Opportunity Back into Focus."
[17] Report of Telecom Regulatory Authority of India, GoI. 2017. "Telecom Regulatory Authority of India." http://www.trai.gov.in/sites/default/files/Telecom Sub_Eng_pr.03_09-01-2017_0.pdf.
[18] Sutherland, Edwin H. 1945. "Is 'White Collar Crime ' Crime ?" American Sociological Review 10 (2): 132–39. http://www.jstor.org/stable/pdf/2085628.pdf.
[19] Tenth United Nations Congress, Secretariat of. 2000. "Prevention of Crime and the Treatment of Offenders." In Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, iii, 43. Vienna: United Nations. https://digitallibrary.un.org/record/455669?ln=en.
[20] Thilagaraj, R, and N Kala. 2013. "No Title." The Indian Police Journal LX (1): 90 to 104.
[21] Thomas, D, and B D Loader. 2000. "Cybercrime: Law Enforcement, Security and Privacy in the Information Age." London: Routledge.
[22] United Nations Office on Drugs and Crime, Vienna. 2013. "Comprehensive Study on Cybercrime." United Nations Office on Drugs and Crime. http://www.unodc.org/documents/ organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf.
[23] Wall, David S. 2010. "The Internet as a Conduit for Criminal Activity." Information Technology and The Criminal Justice System, no. March: 77–98. doi:10.2139/ssrn.740626.