UNDERSTANDING MODUS OPERANDI OF THE CYBER ECONOMIC CRIME FROM PEOPLE-PROCESS-TECHNOLOGY FRAMEWORK'S PERSPECTIVE

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

Abstract : Cyber economic crimes are technological crimes. The internet has engulfed the world and therefore their topology, geographical limits, complexity, technology used and protocols were also started to modify and expand. Thus, due to evolving technology, different kind of vulnerabilities in the technology has started to pop up. The processes of the economic transaction are misused for illegal gain. It is not the technology but man behind the machine is the culprit to exploit all this. Technology is incomplete without the people and processes. These three important aspects, the people, process and technology together create the holistic understanding of the entire spectrum of the activities and players in the criminal activities in cyber economic crime. Technology has a great impact on the financial crimes. Modus operandi can be classified into three type as technological vulnerabilities, Weaknesses in Human mind and lacunas in the processes. The interpretation in this way covers all the methods and ways of the crime. People-Process-Technology framework perspective provides holistic perspective for classifying and understanding the modus operandi of Cyber economic crimes. All the three components of people –process and technology frameworks are equally responsible for crime. This perspective should be considered for deciding for prevention strategy.

Index Terms – Cyber Crime, Cyber Economic Crime, Modus Operandi, People-Process-Technology

1. INTRODUCTION

In the early nineties, the digital development made possible to store data massively and given unlimited computation power. This caused to interconnect the computers to talk each other over the telephone lines, commonly called as computer network. This experiment was first done at USA under the DARPA project. Slowly the size of network engulfed the world and therefore their topology, geography limits, complexity, technology used and protocols were also started to modify and expand. Thus, due to evolving technology, different kind of vulnerabilities in the technology has started to pop up.

With this the issue of internet/ web order management, legal opinions, human behavior & usability issue, and appearance of dark web cybercrimes are central to the discussions of many governments. Initially the government and individuals does not consider it to be as a global threat, rather it was treated as a regular crime done through digital means. But, now with cyber physical threats, serious and large scale economic crimes, which can destabilize economies; individuals but governments also come to conclusion that they require serious measures, controls, training and laws to tackle the cybercrime. Cyber Economic Crime is dominant type of the cybercrime. This paper tries to elaborate the modus operandi of the cyber economic crime from people-process and technology frameworks' perspective.

2. 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 named as 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.

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 stakeholder's 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, cyber security professionals.

3. CONCEPTUAL FRAMEWORK

This section deals with conceptual framework of the study. Major concepts like Cyber Crime, economic crime, Cyber Economic Crime and modus operandi are defined.

3.1 CYBER CRIME

Many organizations and scientists have attempted to define the cybercrime, but there is no generally accepted precise definition of 'cybercrime.' Cybercrime activity may be consist of traditional crimes (fraud, theft, extortion) or 'new' types of criminal activity (denial of service attacks, malware) "(S. W. Brenner and Clarke 2005). Cyber Crime is a type of crime that involves the abuse of computer or 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 by means of electronic operations that target security of

computer systems and data processed by them.
(2) Cyber Crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or Network (Tenth United Nations Congress 2000)
Further Definitions of "Cybercrime," from its nature has been presented, which is an amorphous term and at its greatest breadth. Gordon and Ford have attempted to define the Cybercrime from the involvement of human factor's perspective as: "any crime that is facilitated or committed using a computer, network, or hardware device." Thus, in this definition researchers have considered broad spectrum, as the device may be agent or facilitator to the crime or target of the crime; it has been further considered that crime can be committed by computer only or from non-virtual locations (Gordon and Ford 2006).
The terms "cybercrime," "computer crime", "Information Technology crime," and "high-tech crime" are often used inter-changeably to refer to two major categories of offenses: The first category is that the **computer is the target** of the offence; the other category consists of **traditional offenses** -- such as theft, fraud, and forgery – that are committed with the assistance of or by means of computers, computer networks and related information and communications technology. Generally used the broad definition of "cybercrime," referring to offenses falling into either category (Goodman 1996).

3.2 CONCEPT OF ECONOMIC CRIME

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). Sutherland's work focused mainly on offenses committed in furtherance of professional activities by executives, senior employees. Later it was established by the Gies (1992) that all kind of employees or all kind of persons not only persons with respectability are committing the white-collar crime. Gordon (1996) has attempted to elucidate the concept of the economic crime form different way as compared to Sutherland. 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 special professional or technical skills for the purposes of personal or organizational financial gain or to gain (or attempt to gain) an unfair advantage over another individual or entity (Gordon, 1996).

Croall (2001) argued that in Sutherland's definition words of the like 'persons of respectability and high social status' and crime committed in the course of an occupation which limits some crimes committed in the economic world. He is of the view that class and occupation are the not the key features of the economic crime It has been argued that image white-collar offender is very often projected as of the 'crimes of the powerful' and committed by the corporation or high-status, or respectable business offender can mislead in terms of variety and type of the white collar crimes. Thus all categories of the people can commit the crime (Croall 2001), (Croall 1989).
Financial crime from the Indian perspective can be understood form the various reports and government documents. Mallimath Committee on Reforms of Criminal Justice System in its report has defined the economic crime considering the future offences too that it is an illegal act (or set of acts) generally committed through misrepresentation or outright deception by an individual or a group with specialized skills, whether professional or technical with a view to achieving illegal, financial gain, individually or collectively. The definition covers law, banking and accounting, management and others professions. The frauds and crimes like Banking, non-Banking financial frauds, Stock Market crimes, Smuggling, Money Laundering, Intellectual Property Rights (IPR) related offences, Insurance and Health frauds, Information Technology related offenses (cyber-crimes), Theft and misuse of Credit card & identity and Corruption (Mallimath 2003)

National Crime Records Bureau (NCRB) of India mentions that Economic offenses form a separate category of crimes under criminal offenses. These are alternatively called as white/blue collar crimes. It has been pointed that Economic offences not only inflict pecuniary losses on individuals but also damage the national economy and have security implications as well. Various economic crimes like smuggling of narcotic substances, counterfeiting of currency and valuable securities, financial scams, frauds, money laundering and Hawala transactions, etc. evoke serious concern about their impact on the national security (National Crime Records Bureau 2015). The concept explained in the NCRB's report more of functional and practical.

3.3 CONCEPT OF CYBER ECONOMIC CRIME

For the present study, cyber economic crime is considered a crime, which has common traits of Economic, and cybercrime. While studying the concept of the Cyber economic crime it has been considered that Economic and cybercrime are part of the bigger 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 tool, target or to facilitate to commit the crime. The cyber and Financial crimes have great impact of the technology, are driven by technology and its vulnerabilities. Cyber economic crimes are those crimes, which are perpetrated using cyber technology but basically for financial gains.

Virtual financial crime, Cyber economic crimes, online frauds, online cheating is nothing but cyber economic crimes with different names. Basic modus operandi and motive of all these crimes are to get illegal financial gains. Cyber economic crimes have characters of both the crimes. Indian researcher has defined the concept as Any dishonest and fraudulent activities in cyberspace using new multimedia technology in the era of communication convergence for wrongful gain and to cause wrongful loss to the victim who is prohibited by the criminal law is 'Cyber fraud' (Panda 2007)

Virtual financial crime or cyber financial/economic crime is such a criminal act, where acts of fraud money laundering, cyber fraud takes place over the internet/ virtual medium. Cybercrime is nothing but any criminal activity-taking place via the Internet, smart phone or other electronic means. Virtual financial crime is part of cybercrime. 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)

The role and status of the offender have very little significance for some types of crime perpetrated in cyberspace. It has been argued that regarding the Cyber Economic criminals that there is nothing inherently "Sutherlandian" about it. As persons of respectability do not only commit, but the spread of digital technology has made computers accessible to the masses as well as to the elites; thus any one can commit the crime. Key to the white-collar crime was an opportunity. Availability of digital technology in the modern workplace and with masses has created a range of new opportunities to commit a crime. All kind of opportunities is available to ordinary workers, not just those of high social status. Thus The digital technology has provided ordinary workers and others with abundant criminal opportunities (Grabosky and Walkley 2007).

The impact of the cyber economic crime is far-reaching and large on the economies. A United Nations Office on Drugs and Crime (UNODC), conducted a Comprehensive Study on Cybercrime in 2013, according to that the perceptions of law enforcement institutions around the world are, financial-driven acts, such as computer-related fraud or forgery, make up around one-third of acts across almost all

regions of the world. A number of countries mentioned that 'fraud in electronic commerce and payment,' 'fraud on auction sites such as eBay,''advanced fee fraud' (Nigerian fraud), 'cybercrime targeting personal and financial information' and 'fraud scheme through email and social networking sites' were particularly predominant. It is further emphasized that the financial impact of such crime is significant on the economies (United Nations Office on Drugs and Crime (UNODC) Report 2013).

National Crime Records Bureau has considered a pragmatic and practical model for differentiating the cybercrime and cyber economic crime. Further, it has also differentiated the Economic crimes from the cyber Economic crimes. NCRB considers Economic offenses as a separate category of the offenses under criminal offenses schema. Thus NCRB devotes separate chapter for Economic offenses in the crime in India yearbook, which is a compendium of the crimes statistics. The categorization is basically based on the legislations for the economic offenses. Conceptually the NCRB considers that the Economic offenses are those offenses, which cause monetary losses to the individuals as a victim and also heavily affect the national economy of the country. Thus, the offenses, which are directly benefitting the offenses to gain the monetary gain, has been considered as Economic offenses. Various types mentioned are counterfeiting of currency and stamps, smuggling of artifacts and valuable things, trade in Narcotics substances, financial scams, money-laundering crimes are considered as Economic crimes.

In India, NCRB considers the cybercrime as a new class of crime. The basic reason for this is these are crimes are in existence due to extensive use of the information technology for catering different serves online. NCRB schema of categorization publishes cyber crimes in a separate chapter and within cyber crime makes finer differentiation based on the available legislation for the various types of the crime.
National Crime Records Bureau(2015) collected data under three separate heads in India.

i) Cases registered under the Information Technology Act 2000.
ii) Cases registered under the IPC related to cyber crimes (mainly offenses facilitated by computer)
iii) Cases registered under Special and Local Laws (SLL), which have the component of cybercrime.

The primary objective of the IT act 2000 was to create a favorable environment for e-commerce and commercial use of the Information technology for businesses. Thus there are many crimes, which are not deafened in the IT Act 2000 or amended Act of 2008. These offenses are covered as per Indian penal code, and IT Act in combination.

There are no sections in the IT act, which covers the criminal acts like Cheating, fraud, and breach of trust, which covers mainly 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. In case of special local laws, these laws are formulated for the specific criminal act, and when such specific criminal acts are carried out using cyber technology, then they attract the IT act and SSL sections. All the headings in the Crime in India, which contains the IPC and SLL crimes, are having financial implications. Thus, Cybercrimes with IPC sections and special local laws are considered Cyber Economic crime in this study.

3.4 QUNTUM OF CYBER ECONOMIC CRIME

Cyber Crime is a global phenomenon, and India is not an exception to it. Cyber economic crimes are heavily present in India. The rapid growth has been observed in the use of the Internet in Asia. More than tenfold increase has been found in penetration of Internet in China, Indonesia, and India since 2002. It has been further reported that it has also been accompanied by a significant rise in cybercrime. The development of special software's for commercial crimes on criminal networks have raised the possibilities of cybercrime in many folds, the main motive for this remains the financial gain (Broadhurst and Chang 2012).
Identity theft is one of the most prevalent crimes in India; recently the frequency of identity theft incidents has increased. Increasing use of social media and personal devices in the workplace, cybercrime was now 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 in India to commit the fraud 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).

4. PEOPLE-PROCESS-TECHNOLOGY FRAMEWORK

Cyber economic crimes are technological crimes. The processes of the economic transaction are misused for illegal gain. It is not the technology but man behind the machine is the culprit to exploit all this. **Technology is incomplete without the people and processes.** These three important aspects, the people, process and technology together create the holistic understanding of the entire spectrum of the activities and players in the criminal activities in cyber economic crime as depicted in Fig.1.

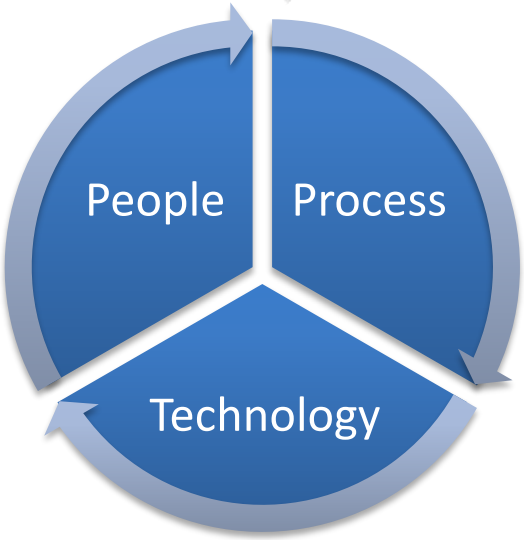

Figure 1 People Process and Technology Framework

People

The people are the most important aspect of the framework. Irony is that this is the weakest link in the framework from security and crime point of view.

The People and the Process must also be considered in order for a holistic solution to exist. The people part of the equation represents the user needs. These are the ultimate consumers/ users of technology for doing work.

Process

The processes refer to regulations and laws that are available for using the technology. The criminal laws and procedural laws are also part of this stack. The loopholes in the regulations or laws are used by the criminals to commit the crime so that they can go un-punished. These loopholes are weaknesses in process fuels the intentions of the criminals and create hurdles for criminal justice system to trial, prevent and investigate the crimes.

Technology

Interestingly the cyber technology is the basic to this conundrum. The technology plays three different roles, as tool, as target and as facilitator in the process of crime. Cursing the technology for cybercrime will be a skewed thought process. Technology plays a pivotal role in the various changes in the society. Information technology has now changed communication, transportation, financial transaction and service delivery. Thus, technology has become central to the development of the human race.

5. CONCEPT OF MODUS OPERANDI

Merriam Webster Dictionary has defined the term Modus operandi a method of procedure "The best approach" or it has further being elaborated as "a distinct pattern or method of operation that indicates or suggests the work of a single criminal in more than one crime"

Oxford dictionary also stressed in its definition that "A particular way or method of doing something

Is called as Modus Operandi "

Thus, modus operandi is the way crime is committed or method of commitment of crime. This method is dependent on various variable like technology available at target and with criminal, habits and knowledge of person committing crime and of victim and processes, rules, regulations that govern the technology and behavior of the people.

Traditionally the technology has not been the dominant variable in the process of crime, but with rise of information and computer technology, it has engulfed all walks of life. This technology has played a pivotal role for enablement. Traditional Crime modus and cyber crime modus when compared it is vividly visible that in cyber crimes technology and its vulnerability and its prowess has played a dominant role in crime. Cyberspace is the tool to commit the old crimes in a new way. Cybercrime basically differs in modus operandi as compared to traditional crime (S. Brenner 2010). Thus, Brenner has concluded that the cyber is the tool to commit old crimes.

6. EFFECT OF TECHNOLOGY ON CRIME

Technology has a great impact on the financial crimes. It is visible from the history that there is a very close relationship between technology and crime. Financial crime committed using cyber technology are increasing. The computer technology and Internet have changed over a period of time, but the basic idea of the crime and intention of committing the crime is same. Internet and network technology have provided vast opportunity for committing a crime on the global scale with very fast speed (Asudani 2014). The nature and architecture of the Internet create the possibility of criminal and deviant activities over it. The penetration of Internet is now growing in all parts of India and village in India in particular. The digital dividing is fast closing, and due to cheap rates of network and hardware all the sections of the society, income groups, ethnic groups, age groups are now able to get connected to the Internet technology.

Nagarajan and Khaja (2012) have mentioned that with the advent of technology and growth of education, white-collar crimes are on the rise, being protected by professionals finding loopholes in the judiciary and support from the government indirectly. This has created a nexus where people from almost all walks of life have started forming a group to do white collar crimes and being protected by professionals in law. This has lead to a situation where the small timers have become white-collar criminals. Talking about the prevalence of white-collar crimes in India, they are spreading like rapid fire in every sphere of society. Committee on Reforms of Criminal Justice System in its report mentioned that in recent days accused are well educated and informed uses sophisticated weapons and advanced techniques to commit the crime and not leaving any trace of the evidence behind (Mallimath 2003).

6.1 CYBER CRIME TYPES BASED ON MODUS OPERANDI

There are **three** ways cybercrimes are committed a) A computer may be the **"object"** of a crime. b) A computer may the **"subject"** of a crime. c) A computer may be an **"instrument"** to commit the traditional crime (Jacobson and Green 2002). Carter (1995) has also classified depending upon the modus, in which the **computer is the target:** include the activities like theft of intellectual property, data from the computer, harm to the operating systems and programs running on the computer. The second category is computer being **instrumental in committing crime than its processes**. Offenses in this category are fraudulent use of Automated Teller Machines (ATM), credit/ debit card frauds. The Third category is the computer is **not an essential part of the crime, but it is related to the criminal act**. Thus **Computer is incidental to crime. Offenses where** drug offenders may use computers to record information of their activities of money laundering, trafficking, and other illegal activities. The fourth category of crimes is the proliferation of crimes using computers. These crimes are like software piracy, black marketeering (Carter 1995).

The role of the human has been highlighted in some studies. **Gordon and Ford (2006)** have opined that the primary factor of involvement of human or not human. This will facilitate the understanding of the crime's technological and human dynamic perspectives. He attempted to create a conceptual framework for cybercrime a technical and societal perspective. In the crime continuum one side are the crimes are entirely due to technology and another side the due to entirely human element responsible for the crime. Most of the crime happens in the middle of the continuum.

One thought process is that these crimes are mostly of two types one is **technological in nature**, and another is having **distinct human element** in the criminal activity. Vulnerabilities in the system are exploited in technological type of crime. Another classification has also stressed two modes of computer crimes as **computer-assisted** and **computer-focused** (Furnell 2001). A motivational model of cyber Crime classification has been proposed which mentions two factors determinants and motivational factors of both conventional crime and cybercrime are same, and they only differ in the medium of perpetration of the crime (Ngafeeson 2010). The motivation of the hackers can

be divided into following categories challenge, money, revenge, ideology, espionage, mischief, ego (Furnell 2001).

7. UNDERSTANDING MODUS OPERANDI FROM PEOPLE-PROCESS-TECHNOLOGY

The modus operandi is criminal specific and crime-specific. The technology vulnerability and tools are major contributors to the selection of particular modus operandi. It is very established fact in the criminology that every criminal has his own methods of committing the crime. Many respondents expressed in detail about modus operandi of the criminals and said that cyber Economic crimes are technology driven crimes. Perpetrators try to find the vulnerability in the technology and exploit the vulnerability.

Empirical data through in-depth interview of key stakeholders shows that there are three basic constituents in this domain of technology-driven business or information technology is driven services namely technology, procedures/ regulations and human resources or people working/ using the technology. Thus, perpetrators find out lacunas in above three. Empirical data of in-depth interviews and data form various stakeholders shows that perpetrators use vulnerabilities in technology or lacunas in procedure or regulations and deception or psychological hack of the human mind to commit a crime.

Thus modus can be interpreted in following three ways as depicted in Fig.2.

7.1 TECHNOLOGICAL VULNERABILITIES

There are various security vulnerabilities in the technology used for transacting financial business or services using information technology. The technology consists of hardware, software and networking components. Thus, vulnerability in any of above three is exploited to breach the application security and commit the crime. To use such modus requires greater technological skill and understanding of the technology. Various crimes like data breaches, hacking of application, ransom ware, and banking Trojan applications use such modus operandi. This modus is technology driven and can be patched. This may be called as Technology modus operandi.

Crimes are facilitated by crime ware (software used to commit the crime) programs like keystroke loggers, viruses, rootkits or Trojan horses into the user's computer system. theft or manipulation of data or services via hacking or viruses, identity theft, data breaches, and bank or e-commerce fraud based upon stolen credentials, phishing attempts via software (Gordon and Ford 2006).

Figure 2 People –Process-Technology Classification

7.2 LACUNAS IN THE PROCESSES

To complete the business transaction user follows various processes. Even delivery of various online services companies, banks, organizations, and governments follow certain procedures. The perpetrators commit the crime by exploiting gaps and lacunas in this procedures or guidelines formulated by regulators or governments. The lacunas in the laws are also covered in this category. Forgery of the documents, fake websites, data harvesting methods, lacunas in banking and finance regulations are examples of this modus operandi.

7.3 WEAKNESSES IN HUMAN MIND

Users are the most sought-after target by the criminal. Human mind and habits have many weaknesses. Human trusts each other in the physical world same way that trust is transpired in the cyberspace. Criminal uses techniques of deception and psychological hacks to cheat the users. Phishing scams and romance frauds are well-known examples of this type of modus operandi. Social engineering is clearly used by criminals as most used modus operandi. Social engineering is also one of the famous modus operandi, which collects the available information from Internet or social media to cheats the user. This method is rampant in online frauds and cheating scams. Psychological manipulation of the user is one of the modus to deceive and get money online. Cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, planning terrorist activities online are crimes with more human element (Gordon and Ford 2006). Cybercrimes like fraud, data/ information theft, unauthorized private work, misuse of personal data, Software piracy, sabotage, and pornography are more related to human element.

8. CONCLUSION

Form the above details it can be concluded that modus operandi can be classified into three type as technological vulnerabilities, Weaknesses in Human mind and lacunas in the processes. The interpretation in this way covers all the methods and ways of the crime. People-Process-Technology framework perspective provides holistic perspective for classifying and understanding the modus operandi of

Cyber economic crimes. All the three components of people –process and technology frameworks are equally responsible for crime. This perspective should be considered for deciding for prevention strategy.

9. REFERENCES

[1] Asudani, Pratibha. 2014. "Social Networking Sites and Cyber Crime : A Study of Adolescents of Jaipur City." The IIS University, Jaipur.

[2] 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.

[3] Brenner, SusanW. 2010. "Cybercrime Criminal Threats from Cyberspace," 248. http://books.google.com/books?id=gsWQ-xgbLbUC&pgis=1.

[4] Broadhurst, Roderic, and Yao-chung Chang. 2012. "Cybercrime in Asia: Trends and Challenges." Asian Handbook of Criminology, 1–26.

[5] Carter, D L. 1995. "Computer Crime Categories: How Techno-Criminals Operate." FBI Law Enforcement Bulletin 64 (7). http://www. fbi. gov: 21–27.

[6] 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.

[7] Croall, Hazel. 1989. "Who Is the White Collar Criminal ?" British Journal of Criminology 29 (2): 157–74. https://watermark.silverchair.com.

[8] ———. 2001. "Understanding White Collar Crime." Open University Press, 1–25.

[9] Furnell, Steve. 2001. "The Problem of Categorising Cybercrime and Cybercriminals." In "survival 1n the E-Conomy .. P" 2nd Australian Information Warfare & Security Conference 2001, edited by William Hutchinson, Matthew Warren, and Janice Burn, 29–37. Edith Cowan University CHURCHLANDS WESTERN AUSTRALIA. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7758&context=ecuworks#page=38.

[10] Goodman, Marc D. 1996. "Why the Police Don't Care about Computer Crime." Harv. JL & Tech. 10. HeinOnline: 465.

[11] Gordon, Sarah, and Richard Ford. 2006. "On the Definition and Classification of Cybercrime." Journal in Computer Virology 2: 13–20. doi:10.1007/s11416-006-0015-z.

[12] Grabosky, Peter, and Sascha Walkley. 2007. Computer Crime and White Collar Crime. Edited by Hn Pontell and G Geis. International Handbook of White-Collar and Corporate Crime. Springer Science Media publication. doi:10.1007/978-0-387-34111-8.

[13] Jacobson, Heather, and Rebecca Green. 2002. "Computer Crimes." American Criminal Law Review 39 (2). HeinOnline: 273.

[14] KPMG India Fraud Survey, India. 2012. "India Financial Crime Survey Report 2012."

[15] Mallimath, V. S. 2003. "Justice Mallimath Committee on Reforms of Criminal Justice System." Vol. I. http://mha.nic.in/sites/upload_files/mha/files/pdf/criminal_justice_system.pdf.

[16] National Crime Records Bureau, GoI. 2015. "Crime in India -2015." http://ncrb.nic.in/StatPublications/CII/CII2015/Chapters.htm.

[17] Ngafeeson, Madison. 2010. "Cybercrime Classification: A Motivational Model." Edinburg. http://swdsi.org/swdsi2010/SW2010_Preceedings/papers/PA168.pdf.

[18] Panda, Manirani. 2007. "Prevention and Control of Cyber Crimes in India: A Socio-Legal Study." University of Calcultta.

[19] PWC Global Economic crime Survey, and PWC. 2016. "Adjusting the Lens on Economic Crime Preparation Brings Opportunity Back into Focus."

[20] Sutherland, Edwin H. 1945. "Is ' White Collar Crime ' Crime ?" American Sociological Review 10 (2): 132–39. http://www.jstor.org/stable/pdf/2085628.pdf.

[21] 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.

[22] United Nations Office on Drugs and Crime (UNODC) Report, New York. 2013. "Comprehensive Study on Cybercrime." United Nations Office on Drugs and Crime, no. February: 1–320. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.