ISSN (e): **2250 – 3005** || *Volume, 07* || *Issue, 02*|| *February – 2017* ||
International Journal of Computational Engineering Research (IJCER)

Cybercrime and its types across globe

[1]soumitri Biswas, [2]sangram Keshari Bedanta
Gandhi Institute of Excellent Technocrats, Bhubaneswar
Oxford College of Engineering and Management, Bhubaneswar, Odisha, India

ABSTRACT
Given the serious nature of cybercrimes, with its implications across the globe it is clear that there is a need for understanding of such crimes in order to find effective solutions to deal with them. Researches in the past have been conducted to find the extent of such crimes and legislative initiatives undertaken by countries to combat these crimes. However, the current challenge is lack of study which can compare and analyze the policies across the globe and which would help in identifying the extent to which they are consistent with each other.
During the course of research it was found that cyber criminals have become more active and not only the extent of risk but also the nature of risk has witnessed a change in recent years. The cyber attackers are now using more sophisticated tools to cause harm and therefore the impacts are also severe. The change for cyber law practitioners in this regard is to work for establishing a criminal justice system which can be applied to the cyber world coordinating the current need with the legal necessity of foresee-ability and the legal exclusion of excessively indistinct, basically undefined cyber offences.
KEYWORDS: Cybercrime, Types of Cybercrime, Global Scenario

I. INTRODUCTION

Introduction to Cybercrime
The term "crime" can be understood as an undesirable act, which results in imposition of legal reprimand for the culprit for any felony against morality, social order or unfair or reprehensible act. The term "offence" has been well defined in the Code of Criminal Procedure to denote an act or omission made punishable by the applicable law prevalent at that time. Thus, Cybercrime can be deduced as a term which encompasses criminal activity which has been carried out with the aid of computers or computing networks, a target or a place of criminal activity and can be used for all ranging from electronic cracking to refutation of service attacks (Goyal, 2012). It is also extended to the conventional crimes in which computers or allied products are employed for carrying out any illegitimate and prohibited activity. The expansion of contemporary technological breakthrough has practically reformed our lives and so does the conventional crimes which shall be committed with ease through usage of technological sources and surpassing the criminal borders. Internet and computer aided networks facilitate committing crime with ease as these provide advantage of discrimination, concealment of identity, bigger magnitude of offence, international approach and evanescent comfort of evidence and convict(s) (McAfee,2011). Cybercrimes primarily entails acts pertaining to unsanctioned access to computer systems, data alterations, annihilation of data, and theft of intellectual property. Cybercrime in the purview of national security may contain politicking, conventional spying or information warfare and allied activities. Pornography, threat emails, imposing someone else's identity, sexual harassment, defamation, SPAM and phishing are crimes which use computer n internet as a tool while virus and worm attack, industrial spying, software piracy and website hacking etc. are crimes where computers are made the targets (Goyal,2012).

II. PROBLEM STATEMENT

Computers have made their presence ubiquitous and each and every aspect of human life is inevitable without computer and internet. Internet and computing enabled a radical transformation of the global society today and have potentially created a virtual world which is at par with the real world. Like the two sides of the coin, in spite of the incredible competence, comfort and facility internet has added to our lives and work, there has been an equal number of adverse effects and disadvantages which have emerged with time and are haunting the online safety and security of people's credentials and vital information. Computer and internet aided crimes are consistently escalating. India is expeditiously evolving as a "talent hotspot" for the international cyber-crime sector due to the downfall in the recruitment demandsoftheconventional softwareindustry,thetemptationofgeneratingeasymoneyandpoorlegislativeenforcement.

Since investigating and combating a cybercrime is a complex task and most of the countries across the globe are adopting best practices towards its. Use of technology and resources, legislative policies and procedures across the globe has been developed to deal with cybercrimes. The objective therefore is to study, analyze and compare the policies and practices adopted across the globe which are used to combat cybercrimes.

III. LITERATURE REVIEW

Cybercrime Scenario across the Globe

At present, different terms have been used to describe the crimes involving computers and internet like; computer related crime, e-crime, online crime, digital crime, and cybercrime (Broadhurst, R. and P. Grabosky, 2005; Smith et al, 2004; Krone, 2005; Pokar, 2004; Kanellis et al 2006; Urbas G., 2004; Furnell S., 2001). Cybercrime in most the nations has been described as a crime which is happening specifically over the networks (internet) (Furnell S., 2001; Kelly J., 2002; Gordon and Ford, 2006; Foreign Affairs and International Trade Canada, 2004). Likewise in United Arab Emirates, Cybercrime has been defined by the Federal Law No (2) of 2006 as "all computer related offences which violate the religious beliefs, or threaten and violate the principles of the country" (Krone, 2005). In Australia under the Cybercrime Act of 2001 cybercrime is defined as "crimes which target computer systems and data within them" (Secretariat of the Parliamentary Joint Committee on the Australian Crime Commission, 2004). In Europe, under the Council of Europe (CoE) Convention on Cybercrime, cybercrime refers to "All offences which are against the confidentiality, integrity and availability of computer data and systems, computer related offences content related offences and offences related to infringements of copyright and related rights" (Council of Europe, 2001). In USA, under the Department of Justice, Computer Crimes and Intellectual Property Section Cybercrimes are "crimes that use target computer networks using viruses, and worms" (Computer Crime and Intellectual Property Section Criminal Division of US,2007).

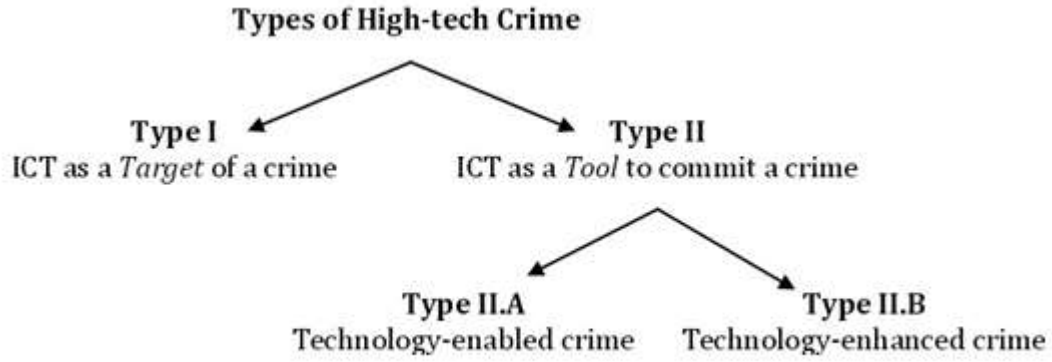
Although Internet has endowed people with a whole fresh virtual bliss, but it has come with both positives and negatives. Internet gives opportunity to the people to enter and network with lot of diverse people irrespective of geographical distance and demographic diversity (Kumar, 2013). The effect of cybercrime is huge across the globe. As per the UK National Hi-Tech Crime Unit (NHTCU), the total cost spend to combat cybercrime in the country in year 2004 was at least US$4.61 billion (Rohde, 2007) which has grown by leap and bounds in the subsequent years and as in year 2013 cost of cybercrime in UK was US$44.96 billion. As per the USA Treasury Department, the proceeds of cybercrimes in the country have overtaken the illegal drug sales with estimated value spend on combating it nearing US$105 billion in 2004 (CNN Money, 2005; Horn P., 2006). As per the study conducted by Norton to understand the scenario of global cybercrime, it was found that India stands at the top position when it comes to spam attacks, at second position in case of virus attacks, and at the third position in case of all kinds of threats. It was also established by this report that around 7 percent (USD 8 billion) of the global price tag (USD 110 billion) of cybercrimes is carried by India alone (Joseph, 2013). The cybercrime cost the country beared was nearly USD 4 billion during 2013.

Types of Cybercrime

The taxonomy of cybercrime is different in different companies, according to Brenner (2004), they can be categorized into three main categories. Other research scholars also comply with this view (Sukhai N., 2004; Koenig D., 2002; Lewis, 2004).

- **Hacking:** Use of computer as target for a criminalactivity;
- **Online Fraud:** Use of computer only as a tool so that criminal activity can be carriedout;
- **Data Storage:** For this kind of criminal activity, the use of computer is incidental to thecrime.

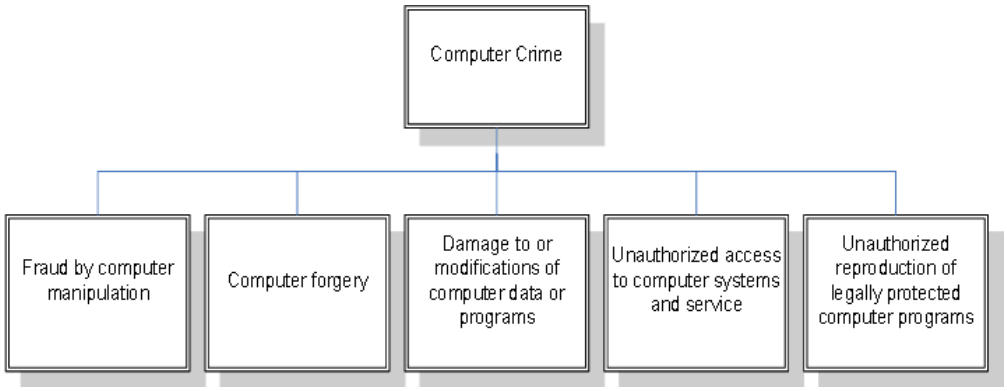
However, there are others who classify computer crimes into only two main categories; i.e. hacking and online fraud. According to Urban and Choo (2008) there are either high-tech crimes which need expertise and can only be conducted by professional criminals and other are simple cybercrimes which can be conducted by common people without them knowing that they are committing a cybercrime. According to the Urban and Choo (2008), the high-tech crimes can be further classified into type 1 and type 2 crimes where the former uses Internet Computer Technology (ICT) to commit thecrime,whileinthelatterICTisusedonlyasatool.Now,thetype2cybercrimeisfurtherdividedintotwotypes;
i.e. technology enabled crime and technology enhanced crime (See Figure 1).



Source: Urban and Choo, (2008)

Figure 1: Classification of Hi-Tech Cybercrimes

However, the classification given by the UN manual on the prevention and control of cybercrimes (1999) has categorized the cyber crimes into 5 major categories (See Figure 2 Although, the UN tries to cover crimes related to computer systems and data attached with it, it does not refers to the crimes which can be facilitated using a computer or computer system.



Source: According to UN, (1999)
Figure 2: Classification of Computer Crimes

In order to resolve this problem, we have referred to the classification given by Council of Europe (CoE) which categorized cyber-crimes into 4 major categories and also sub-categorizes crimes in each of these categories.
Source: According to CoE, (2001)

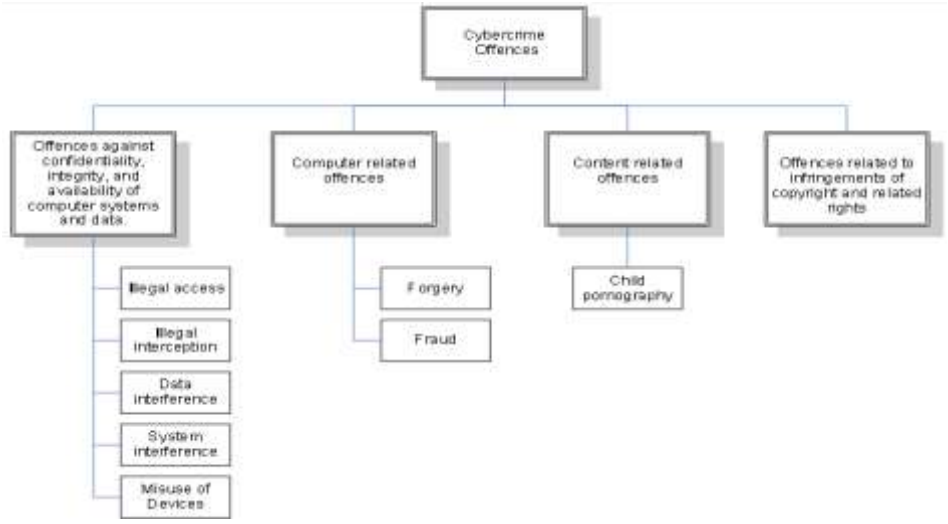


Figure 3: Classification of Computer Crimes by CoE Combating Cybercrime on Global Front

The section reviews the international agencies and the approaches adopted by them to combat cybercrimes. There are many international organizations like UN, European Union (EU), Council of Europe (CoE), Group of Eight (G8), Interpol, who are working towards combatingcybercrimes.

The main purpose of UN is to assist the countries in combating cybercrimes and enhance the international law enforcement collaborations so that the legislation can be strengthened (UN, 2005). The EU works for combating the cybercrimes in 27 European countries and works with well trained academicians and professionals from IT industry to develop standards in order to combat cybercrimes (EU, 2008). Council of Europe is operational is 47 member countries which include USA and Canada, with main purpose of developing cyber laws, ensure the laws are enforced in the member countries and supply global collaborations to non-members so that cybercrime can be combated (CCIPS, 2007). Similarly Group of Eight (G8) has 8 member countries i.e. Canada, France, Germany, Russia, Italy, Japan, UK and USA. The G8 has employed 40 recommendations for the country which can be applied to combat cybercrimes (U.S. Dept. of Justice, 2004). Finally, Interpol i.e. International Criminal Police Organization facilitates the collaboration between all the police forces around the world and comprises of 186 member countries (Interpol, 2007). The system enables the exchange of cybercrimes across the globe as the member countries have direct access to the Interpol's database (Interpol,2007).

The attempts ought be taken to make certain the uniformity in provisions of laws across the countries. This coordination might be accomplished through conventions, recommendations or course of action. For founding criminal offences for the defense of information and communication in cyberspace, legal provisions ought to be put into effect with as much precision and specificity as achievable, and not rely on hazy construal in the current laws (Schjolberg, 2008). The final result must be accomplished just by means of a common concord on combating cybercrime (Li,2008).

The paper collectively come to the point that convicting cybercriminals is indispensable, seeing that they pose a direct threat to likely cybercrime victims' finances, reputation, data and physical uprightness (Lovet, 2009); and as well for the reason that cybercrime has monetary consequences and in a roundabout way promotes conventional violent crime and terrorism, through funding them.

IV. CONCLUSIONS

The research paper presents the concept of cybercrime which in general terms means that cybercrime is any crime that is either committed through computer or where the target of such crime is a computer. The main types of cybercrime include phishing, cybers talking, hacking, and pornography; email spoofing, spams, virus and worm attacks. From the present research it is easily understood that cybercrime is growing at an alarming rate in across the globe and there is a need to bring in measures to combat such cybercrimes. However, the literature revealed that the legal framework in the countries across the globe is not very effective to combat the changing nature of cybercrime, creating the need for newer kinds of cyberlaws.

REFERENCES

[1]. Dalla, H., and Geeta. (2013). "Cyber Crime – A Threat to Persons, Property, Government and Societies." International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 5, May2013.

[2]. Goyal, M. (2012). Ethics and Cyber Crime in India, International Journal of Engineering and Management Research, 2(1), Pp. 1-3

[3]. Joseph, G. (2013). India has 42 mn Cybercrime Victims every Year, Business Standard, June 24,2013.

[4]. Kaur, R. (2013). "Statistics of Cybercrime in India: An Overview." International Journal of Engineering and Computer Science, Volume 2, Issue 8 August, 2013, pp.2555-2559.

[5]. McAfee. (2011). Prospective Analysis on Trends in Cybercrime from 2011 to 2020, White Paper,[online], Available at: http://www.mcafee.com/in/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf [Accessed September 11,2013]

[6]. Mali, P. (2011). Types of Cyber Crimes & Cyber Law in India. CSI Communications, December2011.

[7]. Norton. (2013). 2012 Norton Cybercrime Report, Mountain View: Norton bySymantec.

[8]. PTI. (October 22, 2013). "Cyber criminals cost India USD 4 billion in 2013: Symantec." The Economic Times. Retrieved from: http://economictimes.indiatimes.com/tech/internet/cyber-criminals-cost-india-usd-4-billion-in-2013-symantec/articleshow/24546739.cms

[9]. PwC.(2011).SafeguardingOrganizationsinIndiaagainstCyberCrime,Globaleconomiccrimesurvey,

[10]. Report, Price water house Coopers India.

[11]. Schjolberg, S. Lan, T., Xin, Z., Raduege, H., Grigoriev, D., Duggal, P. and (2008). Global Cyber Deterrence, views from China, the US, Russia, India and Norway, New York: The East WestInstitute