CYBER CRIME- CRIME OF NEW ERA

Sandeep Kumar Sharma
Advocate, Delhi High Court

Abstract: As the world marches deeper into the unfathomable passageway of digital revolution, it is becoming apparent that the tremendous benefits of the internet age are being challenged by the formidable menace of cyber-crime. There is no gainsaying in the fact that after terrorism, Cyber-crime is the most debated term of the recent times. Despite endless rounds of deliberations the term cyber crime has been incessantly deifying a globally accepted definition. The word "cybercrime" is the most familiar terms for the internet users, be it individual, corporate, organization, national, multinational or international. The attention accorded cybercrimes is not figment of the imagination or farfetched as on one hand, it is partly rooted in its unavoidable nature as a result of the fact that telecommunications via the cyberspace, is the veritable means by which social interaction, global trade and commerce are transacted; and on the other, the economic losses to which all citizens are exposed whether now or in the nearest future. Aside economic losses the modern trend of cyber- crimes makes the intellectual property rights are the most vulnerable as works of authors and artists are violated through the unauthorized circulation. There has also been an upsurge in instances of piracy, pornography and financial fraud and cheating in relation to commercial transactions conducted online. In this Article different facets of cyber-crime, laws on domestic and International level, challenges before authorities and impact of it will be discussed and intends to bring to the fore a comprehensive study how the menace of cybercrime may effective be dealt globally.

Keywords: Cyber-Crime, Financial Fraud, Intellectual Property, Global Trade, Pornography, Piracy.

Introduction: Today, we are living in the era of Information-Technology, economic, geographical and political barriers are being lowered and technological advancements in communications and commerce are on the increase, affirming that ours world has indeed become a small town. There is no gainsaying that development and growth in Information Technology has made our lives easier and convenient but as every coin has two sides, same is with the latest trend of information and communication technologies, where we use it at the cost of being misused and preyed of fraudsters and technological stratagem.

Undoubtedly, the precipitate and rapid development in the area of information technology and the integration of computer and communication technology have made enormous changes in human lives and information activities but this unbridled growth in technology has also provided a breeding ground for delinquent behavior. Whilst society is enjoying the fruits of technology but at the same time, criminals are deploying stupendous adaptability to derive the greatest benefits out of it. Computers and computer networks are ubiquitous and it may be observed that developments in information and communication technologies are shaping the 21st century. Among the ICTs, the Internet acts as a unifying resource that facilitates the information communication and dissemination activities of the other technologies. From its emergence in 1967 till today, the Internet with its sophisticated applications such as the World Wide Web, electronic mail, media platforms, social networking sites, and others have contributed significantly to the advancement of individuals in different fields of endeavors but it has also become one of the major components and enablers for delinquent and unscrupulous individuals to commit crime and evade identifications and apprehensions by law enforcement agencies. In recent times, Cyber-crime has indeed reached to epidemic proportions and in the absence of uniformity in rules and legal provisions on International Level the growing menace of Cyber-crime cannot be effectively surmounted.

The archaic/ obsolete laws and the rapid development of information and communication technology precisely constitute a contradiction and taking it to the level where it becomes almost impossible to deal

with the problem of cybercrime effectively. Therefore, by merely relying on the traditional laws and legal provisions the menace of cyber delinquency felony cannot be effectively dealt with. The various forms and diverse purposes of cybercrime complicate the formulation of measures to tackle it. Initial concerns about unauthorized access to private information soon expanded into concerns that computers could be used to facilitate further crimes. Threats to property were joined by threats to the security of information, and even to the security of nation. These threats have increased at an alarming scale.

Concept of Cyber-Crime: To begin with the concept it is essential to briefly differentiate between the terms 'Cyber-crime' and Computer- crime'. In parlance both are considered as one and same but the matter of the fact is that the both are neither synonymous nor identical. In parlance 'cybercrime' implies "offences committed through the use of the computer in contrast to 'computer crime' which refers to offences against the computer and data or program therein". Whilst the computer and its content are the primary targets in computer crimes, the meaning of cybercrime is wrapped around the use of a computer or/and the Internet to commit crimes.

Due to dichotomies in jurisdictions and yet addressing the same concept in legal literature, cybercrimes to date, has no globally accepted definition that could possibly encapsulate all the facets of this novel brand of crime, the definitional problem of cybercrime subsists, but one thing that is certain is that most definitions of cybercrime make reference to the Internet; for the sake overcoming the lacuna, cybercrime has been defined as crime committed over the Internet which might include hacking, defamation, copyright infringement and fraud. According to Oxford Dictionary of Law (2002), cybercrime also means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[i] According to legal dictionary 'a criminal offence_on web, offence on the web , a criminal offence regarding the internet, a violation of law on the Internet, an illegality committed with regard to the internet, breach of law on the Internet, computer crime, contravention through the web, corruption regarding internet, criminal activity on the Internet, disrupting operations through malevolent programs on the Internet, electronic crime, Internet crime, sale of contraband on the Internet, stalking victims on the Internet, theft of identify on the Internet."[ii]

According to The Cambridge English Dictionary, Cyber crimes are the crimes committed with the use of computers or relating to computers, especially through the internet. Crimes which involve use of information or usage of electronic means in furtherance of crime are covered under the ambit of cyber crime. Cyber space crimes may be committed against persons, property, government and society at large. In other words it may be defined as a, "Cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern. The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders.[iii]. Cybercrimes may precisely be said to be those species of crime in which computer is either an object or a subject of conduct constituting the crime or it may be even both. Thus, any activity that uses computer as an instrumentality, target or a means for perpetrating further crime, falls within the ambit of cybercrime.

According to UN Congress on Prevention of Cyber Crime and Treatment of Offenders defined cyber as:

i. Narrow Sense: cybercrimes in a narrow sense connotes a computer crime and includes any illegal behavior directed by means of electronic operations that targets the security of the computer systems and the data processed by them.

ii. Broader Sense: cybercrime in broader sense includes all computer related crimes and consists of any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

Typology of Cybercrime: The term "cybercrime" is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or

classification system for cybercrime. One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences,
(i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) computer-related offences; (iii) content-related offences; and (iv) copyright-related offences. This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems", content-related offences; and copy right related offences. The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories. In addition, some terms that are used to describe criminal acts (such as "cyber-terrorism" or "phishing") cover acts that fall within several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime.

Development of Computer Crime and Cybercrime: The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed.

The 1960s: In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology. At this early stage, offences focused on physical damage to computer systems and stored data. Such Understanding cybercrime: Phenomena, challenges and legal response incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university. In the mid 1960s, the United States started a debate on the creation of a central data-storage authority for all ministries. Within this context, possible criminal abuse of databases and the related risks to privacy were discussed.

The 1970s: The 1970s In the 1970s, the use of computer systems and computer data increased further. At the end of the decade, an estimated number of 100 000 mainframe computers were operating in the United States. With falling prices, computer technology was more widely used within administration and business, and by the public. The 1970s were characterized by a shift from the traditional property crimes against computer systems that had dominated the 1960s, to new forms of crime. While physical damage continued to be a relevant form of criminal abuse against computer systems, new forms of computer crime were recognized. They included the illegal use of computer systems and the manipulation of electronic data. The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud. Already at this time, multimillion dollar losses were caused by computer-related fraud. Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases. As the application of existing legislation in computer-crime cases led to difficulties, a debate about legal solutions started in different parts of the world. The United States discussed a draft bill designed specifically to address cybercrime. Interpol discussed the phenomena and possibilities for legal response.

The 1980s: In the 1980s, personal computers became more and more popular. With this development, the number of computer systems and hence the number of potential targets for criminals again increased. For the first time, the targets included a broad range of critical infrastructure. One of the side effects of the spread of computer systems was an increasing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents. The interconnection of computer systems brought about new types of offence. Networks enabled offenders to enter a computer system without being present at the crime scene. In addition, the possibility of distributing software through networks enabled offenders to spread malicious software, and more and more computer viruses were discovered. Countries started the process of updating their legislation so as to meet the requirements of a changing criminal environment. International organizations also got involved in the

process. OECD and the Council of Europe set up study groups to analyse the phenomena and evaluate possibilities for legal response.
The 1990s: The introduction of the graphical interface ("WWW") in the 1990s that was followed by a rapid growth in the number of Internet users led to new challenges. Information legally made available in one country was available globally – even in countries where the publication of such information was criminalized. Another concern associated with online services that turned out to be especially challenging in the investigation of transnational crime was the speed of information exchange. Finally, the distribution of child pornography moved from physical exchange of books and tapes to online distribution through websites and Internet services. While computer crimes were in general local crimes, the Internet turned electronic crimes into transnational crime. As a result, the international community tackled the issue more intensively. UN General Assembly Resolution 45/121 adopted in 1990/145 and the manual for the prevention and control of computer-related crimes issued in 1994 are just two examples.

The 21st Century: As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing", and "botnet attacks", and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP Understanding cybercrime: Phenomena, challenges and legal response 14 (VoIP) communication" and "cloud computing". It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority.[iv]

Scope & Changing Facets of Cyber-Crime: Presently, cyber crime is an ever increasing phenomenon, not only in a particular region but all over the world. The incidence of cyber crime is directly proportional to the level of progress made by a country in computer technology. The report of the United Nations stated that more than 50 % of the websites in the US, Canada and European countries have experienced breach of security and threats of cyber terrorism which threw a serious challenge before the law enforcement agencies.[v] The recent trends of cyber-crime not only limited to the age-old orthodox crimes but its new facet is more dangerous as it has paved a new pay of war and destruction. The new trend that has developed in recent years is that the militants are going for terror training. The Internet has become a key teaching tool for militants who are using it to educate recruits in cyber terrorist's training camps.

The nature and extent of Cyber-crime is kept on changing and danger involves in it increasing at the alarming speed. The changing trend of Cyber-crime and dangers involves in it have been rightly figured out in a latest movie of James Bond series 'Sky fall', in which it has shown that how a person hacks into top secret Government systems, exposes the identities of covert agents online and in one of the most memorable scenes causes an explosion at the heart of MI6 by manipulating sensitive computer systems .Though it was shown in the movie but it was not a far-fetching story and a figment of an imagination of the moviemakers but could be the reality of the present time. The danger and threats of misuse of technology is much graver than the proportion of convenience and ease involved in it. Therefore a cautious and judicious approach needs to be adopted in order to avoid the new generations crime i.e. Cyber Crime. Cyber Warfare and Cyber Terrorism are the new terms which are closely associated with the term Cyber-crime.

What is Cyber Warfare?
The term "cyber warfare" refers to warfare conducted in cyberspace through cyber means and methods. While "warfare" is commonly understood as referring to the conduct of military hostilities in situations of armed conflict, "cyberspace" can described as a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein. Thus, for example, the infection of a belligerent adversary's computer network with a malicious virus would constitute an act of cyber warfare, whereas

the aerial bombardment of a military cyber command would not. The fact that cyber warfare is conducted in cyberspace does not exclude that it may produce kinetic or other non-electronic effects outside the cyber domain and may even be specifically intended to do so by the attacker. For instance, targets of cyber warfare may also include persons whose life, or objects the functionality of which, depends on computer systems, such as certain power stations, means of transport, or persons connected to various kinds of medical, military or professional life-support systems.

What is Cyber Terrorism: The concept and term of Cyber- terrorism first introduced by Barry C. Collin of the Institute for Security and Intelligence in the late 1980's and early 90's but the concept only began to resonate with the general public in the beginning of 21st century when in the year 2000 millennium bugs associated with the date 31.12.2000 aka (Y2K) switch gained wide scale recognition. Cyber terrorism, may be defined as any act of Internet terrorism which includes deliberate and large-scale attacks and disruptions of computer networks using computer viruses, or physical attacks using malware, to attack individuals, governments and organizations. While cyber crime is often motivated by economic gain, and hacking, or internet vandalism, often is done to satisfy the hacker's ego, cyber terror is fueled by an ideology.

Gabriel Weimann, an Internet and security expert who teaches in the University of Mainz in Germany and has studied militant's use of website for nearly a decade, while addressing the Internet security personnel said that, "website and chat room used by militant Islamic Groups like Al-Qaida are not only used for dissemination of propaganda but also for terrorist education. Al-Qaida has launched a practical website that shows how to use weapons, how to carry out kidnapping and how to use fertilizers to make a bomb.[vi]"

Steps on International Level: International treaties, international efforts to address cybercrime and e-evidence as a matter of criminal justice have been pursued since the 1980s, initially by the Council of Europe and the Organisation for Economic Cooperation Development (OECD), and from the mid-1990s also by G8. At the Council of Europe, this led to the adoption of soft-law recommendations providing guidance on the criminalisation of computer-related offences (1989) and on law enforcement powers regarding cybercrime and electronic evidence six years later (1995). These were precursors to the Budapest Convention which was opened for signature in 2001. By 2001 the problems of cybercrime and e-evidence were sufficiently important to warrant an international treaty but cybercrime and information technologies were not yet considered too relevant on national interests and security of states to prevent consensus. At the United Nations, it has not been possible to reach a consensus so far as to whether an international treaty on cybercrime was necessary and feasible and what it would possibly comprise. The matter of "combating the criminal misuse of information technologies" was the subject of a resolution at the UN Congress on Crime Prevention and Criminal Justice in Havana in 1990. It referred to the work of the OECD and the Council of Europe, but no follow-up was given by the UN. In 2001 and 2002, it was taken up again in UN General Assembly Resolutions but at that point, the Budapest Convention had been opened for signature. Subsequently, the question was on the agendas of UN Crime Congresses (in 2005, 2010 and 2015) and annual UN Crime Commissions but not much progress had been made. The Intergovernmental Group of Experts on Cybercrime, established at the Salvador Crime Congress in 2010, "in view of examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime," noted in its most recent meeting in 2013 "broad support for capacity-building and technical assistance" and "diverse views" on options of new international instruments. It would seem that from around 2001, the focus within the UN had shifted from cybercrime as a matter of criminal justice to the protection of critical information infrastructure and cyber or information security as a matter of international security. From 2004, Groups of Governmental Experts (GGEs) have been meeting to examine "existing and potential threats from the cyber-sphere and possible cooperative measures to address them." Though progress is slow at the UN towards norms, rules or principles of "responsible state behaviour" in cyberspace, it is considered the most relevant forum on state-to-state relations concerning cyber security.[vii]

Definite Set of Legal Framework at International Level is the Need of the Hour: Without prejudice to the effectiveness of the extant laws in place to combat cybercrimes, the scourge persists, nay, rather than the laws to curb, or better still, minimize cybercrimes, there is a rise in the frequency and sophistication and the reason for that development, is attributable to the fact that, as efforts are being made to stem the tide of cybercrimes, so are cybercriminals devising methods and means of thwarting global measures targeted at addressing the problem. There may be many reasons/ challenges which comes in the way of effective handling of Cyber-crime. It may be Identity of cybercriminals, actually there is no easy means of identifying who is doing what and where is a user of the Internet is situate at any point in time; the global information system is free and there is no perquisite that needs to be fulfilled, before a user can login to connect with anywhere and anyone across the globe. Further, the other challenge regarding the nature of evidence One other impediment to the enforcement of cybercrime laws wherever attempts are made anywhere across the globe, is the nature of evidence available in the custody of prosecution and the admissibility of same, during the course trial of cybercriminals. Relations between the nations, technical and complex legal provision, which includes extradition agreements. Lack of effective reporting and dearth of data, Cost, time and efforts incurred in investigation and prosecution, Dearth of experts in prosecution of cybercrimes,

Other than anonymity of the offenders one of the biggest impediments to deal with the Cyber-Crime is Jurisdiction. Cybercrime investigations require extensive cross-border coordination. The international legal framework needs to catch up with this reality, when almost every country of the world became victims of an unprecedented Cyber attack which used the ransomware 'Wannacry', the wrongdoers not only attacked the system of the individuals but also caused inconvenience organisations (Government or Private) around the world. But due the limitless reach of the internet it is almost impossible to identify and catch the culprits and to accomplice this task a detailed complex international investigation is needed. However, the existing international legal framework for cooperation on cybercrime is a fragmented one, with no single governance architecture, which complicates investigations and risks leaving the perpetrators at large and criminals always managed to go scot-free under the aegis of these lacunas of law.

The paramount issue with the cybercrime is to not having any proximity between the offender with the victim, which leads to the uncertainty and the ambiguity in the investigation to the crime. As the delinquent may perform his ill-intentions from the one corner of the world without going to the place of offence. Therefore, not having any tangible boundaries and limits of the offence makes almost impossible to reach to the wrongdoer. Because in the virtual world we can reach at any corner of the world and this is where the point of friction between the cyber world and the territorial world begins as in the territorial world there are limitations set up by the sovereignty of the nation which is not the case in the cyber world. A judicial system can function effectively if it is well regulated; it is these regulations that identify every functional aspect of the judicial system including the jurisdiction of the courts. A court in order to deliver effective judgments must have proper and well defined jurisdiction, as without a jurisdiction the court's judgments would be ineffective. The conventional requirement as to a party can sue another is at the place where the defendant resides or where the cause of action arises. This itself is the problem with Internet jurisdiction as on the net it is difficult to establish the above two criteria's with certainty.[viii] Jurisdictional limitations can hamper one of the most challenging aspects of a cybercrime investigation – attribution. Every time a law enforcement agency needs to undertake a cross-border investigation, it has do so through official, and at times bureaucratic, legal channels to request assistance which makes investigations more complicated to navigate. Not only is this process lengthy and convoluted but it also jeopardizes the global evidence gathering process. This is due to the volatile and fragile nature of the electronic evidence which requires agility in its collection while protecting its integrity and maintaining.

Absence of one universal set of legal framework is also contributing a lot in the enormous growth of Cyber-crime. With specific reference to cybercrime, the Council of Europe Convention on Cybercrime (ETS No. 185) otherwise known as the Budapest Convention is a well known subsisting treaty that have a status of international application which entry into force on 1st July 2004.and the point that is being

made is that, if a state is a party to the treaty, but refuses to enforce provisions of the same in its territory, what can other states in the comity do to ensure compliance of the erring state? The non-binding nature and lack of strict enforcement mechanisms of international law is by and large, with respect to cybercrime laws appears to have stultified the enforcement of cybercrime laws.[ix]
As stated above that absence of uniform and definite piece of legal framework on International Level is contributing to reach the cyber crime at the level of epidemic. Since, cybercrimes respects no jurisdiction because it is possible for a delinquent sit in the other extreme corner of the World and perpetrate his act that would have effects in the other corner of the World.

Cybercrimes are borderless, transnational and international crimes and which said crimes, are committed in the cyberspace; but the majority of the laws and policies dealing with cybercrimes to date, are either national or regional; the only law specifically dealing with cybercrimes which is international in character, is the Budapest Convention which for all intents and purposes, is hampered by difficulties associated with international laws, an issue already copiously discussed. Cybercrimes have only one jurisdiction, that is, the entire world; by so doing, the extant laws and policies which are fragmented, national, regional or quasi international cannot possibly cope with the problems engendered by cybercrimes; ipso facto, cybercrime laws shall continue to suffer from enforcement challenges; the only law that can frontally address the menace of cybercrimes, is that law that would have only one jurisdiction, applicable globally, and not until the political will is mustered to enact that universal law, mankind shall continue to be plagued by challenges of enforcement posed to cybercrimes laws.[x]

Indian Perspective: Talking about Indian scenario of cyber space crimes and cyber space laws, there was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology IT ACT, 2000 was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. To make it more strengthen and efficient it was further amended in 2008. Other than this, Indian Computer Emergency Response Team (CERT) is in operation since January, 2004. It is an expert group that handles computer security incidents. Alternative names for such groups include computer emergency readiness team and computer security incident response team. It is the National nodal agency for responding to computer security incidents as and when they occur.

Indian Information & Technology Minister, Shri. Ravi Shankar Prasad, said on March 07, 2017 that the government is open for international collaboration in the field of cyber security and favours handling issue of cyber terrorism in cooperation with other countries. India is willing to have the widest cooperation world over in the quest of cyber security. If Internet has to remain powerful, it must be safe and secure. Few people are using digital technology for terrorism, for hatred, for extremism, and we need to work together,"[xi] India has always been the supporter of the effective and a uniform law against Cyber-crime on an International level but it must be enacted after the due deliberations of all the stakeholders and includes and address the voice and concern of all. India's view reiterated by I&T Minister in April 2017 in Germany at G 20, Digital Minsters Meeting, where Indian counterpart said that India supports better International cooperation of cyber security. India's is showing its concern incessantly at the every platform against the growing danger of Cyber-Crime. In this connection on February 14, 2017, India's permanent member at the UN, Mr. Syed Akbaruddin, has said that the The world body is not ready to act on an anti-terrorism treaty dealing with cyber terrorism and even the Security Council's decisions that impose binding duties on member countries to combat terrorism do not mention cyber attacks. Showing his concern and to reach on atleast on an interim consensus he further added that "If we are not willing to negotiate a treaty on terrorist cyber attacks, can we at least start by clarification of the applicability of certain anti-terrorism treaties to terrorist cyber attacks? India is ready to render its services and perform its part to surmount over the crime of new age i.e. Cyber crime.

Conclusions: Though there are ample amount of laws in force in almost all the nation of the globe but the challenges of enforcement of the said laws, continues because of the issues related to admissibility of evidence, jurisdiction, complexities of laws, bi-lateral agreements, lack of training, anonymity of the offenders etc. In addition to the foregoing, are the absence of a global consensus on the kind of law requires to deal it, the absence of a global consensus on the legal definition of criminal conduct; the inadequacy of legal powers for investigation and access to computer systems, the lack of uniformity between the different national procedural laws concerning the investigation of cybercrimes; the lack of extradition and mutual legal assistance treaties, synchronized law enforcement mechanisms that would permit international cooperation in cybercrime investigations, and existing treaties that take into account, the dynamics and special requirements of these investigations. Therefore, it is need of the hour that all the nation need to bind by a universal law on this issue. Which should have universal applicability with only one jurisdiction, so much that, wherever a cybercrime is committed, the perpetrator can be brought to book, irrespective of where he is situate.

References:

1. http://legal-dictionary.thefreedictionary.com/cybercrime.
2. Prof. Dr. Marco Gercke. "Understanding Cyber Crime: Phenomena, Challenges and Legal Response." ITU Publication, September 2012, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf,last visited on 20/12/2017
3. James Brokenshire. "James Brokenshire speech on Cyber Crime" March 2013 available at https://www.gov.uk/government/speeches/james-brokenshire-speech-on-cyber-crime, last visited on 20/12/2017
4. Nils Melzer, "Cyberwarfare and International Law." 2011 available at http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf last accessed on 19/12/2017
5. Manish Lunker, "Cyber Laws: A Global Perspective" available at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan005846.pdf last accessed on 15/12/2017
6. Ajayi, E. F. G., "Challenges to enforcement of cyber-crimes laws and policy" Vol. 6(1), , August 2016, pp. 1-12 available at http://www.academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210, last accessed on 16/ 12/2017
7. India open to widest cyber security collaboration, says IT minister Ravi Shankar Prasad, March 2017, available at http://www.firstpost.com/india/india-open-to-widest-cyber-security-collaboration-says-it-minister-ravi-shankar-prasad-3320616.html last accessed on 19/12/2017
8. The world is not ready for cyber attacks, India tells Security Council, February 2017 available at http://www.firstpost.com/tech/news-analysis/the-world-is-not-ready-for-cyber-attacks-india-tells-security-council-3697721.html last accessed on 19/12/2017

***