OPEN ACCESS
Scholars Bulletin
Abbreviated Key Title: Sch Bull
ISSN 2412-9771 (Print) |ISSN 2412-897X (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Subject Category: Law

Illegal Access to a Computer System: White Collor Crime in India

Jitender K Malik*, Dr. Sanjaya Choudhury

Department of Law, Bhagwant University, Ajmer, Rajasthan, India

DOI: 10.36348/sb.2020.v06i12.003 | **Received:** 09.11.2020 | **Accepted:** 18.12.2020 | **Published:** 30.12.2020

***Corresponding author:** Jitender K Malik

Abstract

Many jurisdictions encourage the adoption of electronic commerce by enacting statutes that enable contractual dealings to be conducted electronically, and also allows people to use an electronic signature to satisfy any legal requirement. Even the electronic transfer of land is covered under certain statutes as in the case of the Indian Information Technology Act, 2000. However, in the era of globalization; and in the absence of any geographical boundaries for the cyberspace, such new legislations also raise some questions: for how long will these statutes be valid? What are the boundaries of these statutes? Who should be forced to follow them? Most of these questions are unanswerable today. The exponential growth of the internet and online activity raise a number of legal questions. How does copyright apply to digital content? How can national laws apply to cyber wrongs in cyberspace? Can privacy and data protection exist on the cyber space? Can electronic commerce really be secure? Can cyberspace be regulated by one, or by many authorities? In seeking to apply the law to the Internet, problems arise owing to the fact that most laws largely apply to the pre-cyber space world. As the technology improves and ownership of home computers increases, one competently navigate his way around cyberspace, downloading information, reading and writing to newsgroups, and receiving and sending emails. Cyberspace represents the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication. The present Study attempts a comprehensive definition of the term 'cyberspace,' traces out the evolution and growth of cyber space; and enumerates the pros and cons of information technology. In traditional and online trading environments, consumers are entitled to have their privacy respected. While shopping on the internet; most people typically do not think about what is happening in the background. In the modern era of electronic technology, people want to get their work done quickly with little effort. At times, people forget or ignore the legal and ethical values of their actions. Consequently, cyber wrongs in different forms are increasing day by day: cracking/hacking, e-mail spoofing, spamming/Denial of Services (DOS attacks), carding (making false ATM Debit and Credit cards), cheating and fraud, assault by threat, impersonation, intellectual property rights (IPR) infringements (software piracy, infringement of copyright, trademark, patents, domain names, designs and service mark violation, theft of computer source code, etc.), online gambling and other financial crimes including the use of networking sites and phone networking to attack the victim by sending bogus mails or messages through internet, forgery, URL hijacking or squatting (using the domain name of another person in bad faith), cyber vandalism (destroying or damaging the data when a network service is stopped or disrupted), virus transmission, internet time thefts, pornography, cyber terrorism etc-the list is endless. Customer information has to pass through several hands; and the safety and security of a customer's personal information lies within the hands of the business. Therefore, security and privacy of the information are a major concern. E-commerce has a tremendous impact on copyright and other intellectual property rights (IPRs).

Keywords: Cyber space, Cyber Crimes, Internet, Netizen.

INTRODUCTION

In traditional and online trading environments, consumers are entitled to have their privacy respected. While shopping on the Internet; most people typically do not think about what is happening in the background. Customer information has to pass through several hands; and the safety and security of a customer's personal information lies within the hands of the business. Therefore, security and privacy of the information are a major concern [1-4]. At times, people forget or do not consider the legal and ethical values of their actions. Consequently, cyber wrongs in different forms are increasing day by day: cracking/hacking, e-mail spoofing, spamming/Denial of Services (DOS attacks), carding (making false ATM Debit and Credit

cards), cheating and fraud, assault by threat, impersonation, intellectual property rights (IPR) infringements (software piracy, infringement of copyright, trademark, patents, domain names, designs and service mark violation, theft of computer source code, etc.), online gambling and other financial crimes including the use of networking sites and phone networking to attack the victim by sending bogus mails or messages through internet, forgery, URL hijacking or squatting (using the domain name of another person in bad faith), cyber vandalism (destroying or damaging the data when a network service is stopped or disrupted), virus transmission, internet time thefts, pornography, cyber terrorism etc-the list is endless. Generally, a trademark can be owned by an individual, a company, or any sort of legal entity. When someone else tries to use that trademark without authorization, it could be considered an illegal dilution of the distinctive trademark. If someone uses a trademark in such a way as to dilute the distinctive quality of the mark or trade on the owner's reputation, the trademark owner may seek damages [5-10]. In the cyberspace, domain name infringements are rampant. The growth of the e-commerce is indicative of the increasing receptiveness of the public but has also brought the issues that the legal system of the country has been faced with. Now internet has become a basic necessity for every household in most cities, the e-commerce industry has come a long way. The legal system has constantly tried to catch up especially with the enactment of the various rules under the IT Act to deal with a host of issues emerging from the use of internet. Moreover, the IPR issues in e-commerce transactions have taken a new form with users finding ways not only easily to duplicate material but also mislead other users [11-16]. Though India has started dealing with it by enacting IT Act, 2000 but, it still lacks a lot as no specific legislation governs online transactions and IPR issues in India. The Information Technology Act, 2000 provides for the admissibility of electronic records and sets out offences and penalties for cybercrimes, etc. But, this is just an enabling statute to facilitate online transactions and thus has to be read in conjunction with the Contract Act in order to determine whether an online transaction constitutes a valid contract or not [17-20].

The power of the Web to reach the world carries with it a variety of legal issues, often related to intellectual property concerns, privacy, decency, etc. Authorities seeking to apply their laws in traditional ways or to expand legal control over international links face many challenges due to the global nature of the Internet. Therefore, there is an urgent need for a comprehensive policy and an effective legal frame work to regulate cyber crimes. The present study primarily intends to address the pitfalls in the present legal system and to evolve a strategy to regulate cyber crimes in India [21-25].

Cyber Crimes against Women in India

It is a significant contribution to socio-legal research on online crimes targeting teenage girls and women. It shows how they become soft targets of trolling, online grooming, privacy infringement, bullying, pornography, sexual defamation, morphing and so on. The authors address various raging debates in the country such as how women can be protected from cybercrimes; what steps can be taken as prevention and as recourse to legal aid and how useful and accessible cyber laws are [26].

Banks are offering many services of which, the electronic mode is becoming popular amongst Banks and their customers. Presently, these are in the form of ATMs, credit & debit cards, online transactions, net banking, mobile banking, e-commerce, new payment systems etc. As more and more services of banks are offered in electronic mode, they must be aware of the risks due to possible misuses of new technology based services and various online channels. It has become important that the bankers, particularly who are dealing with I.T. and online channels, would be well versed with the various cyber crimes and frauds which may occur in offering these services. To safeguard the interest of the banks and their clients, a banker who is dealing in such services should have thorough knowledge and understanding about cyber crimes and how to mitigate a fraud and prevent eventualities in future. The book; Cyber Crimes and Fraud Management provides an overview of various types of cyber crimes and how to alleviate such crimes [27].

At a time when there are still a number of voices calling for the Internet to remain a law-free zone, a whole bundle of conflicts have already emerged, many of which have found their way to lawyers and the courts in a substantial number of different jurisdictions. It surely now cannot be doubted that the Internet, like any other place in the world where people come together and follow their own interests, needs rules to be developed for the handling of such conflicts. Lawyers have already reacted and have created a new area of law--commonly called "law of the internet" or "cyber law." This area, however, is still far from being strictly defined. It touches on many existing areas of law, but at the same time it deals with a wholly new medium--cyberspace--which itself is subject to constant change and development. Under these circumstances, it is not surprising that in a number of cases the predictions as to how this law will look at some selected moment in the future are vague and uncertain [28-30].

Police Investigation Powers, Tactics and Techniques is a benchmark and best-practice model and regarded as the ‘Bible’ for professional investigation in India. Anchoring himself firmly on the ever-contested space of Indian law and legal processes, and drawing substantive support from his rich and varied experience

as a law enforcement officer in the police department, the author, has sought to fulfill the legitimate requirements of police officers, advocates, judicial officers, social activists, NGOs, gender activists and the general public. The author's utopian ideal that no innocent person should be punished and no offender should go unpunished is the dominant message of the book. The citation of more than 800 landmark judgments of various High Courts and the Supreme Court for the period 1965-2016 in the appropriate chapters is another outstanding feature of the book [31-35].

The principle of dual criminality also poses difficulties, if the offence is not criminalized in one of the countries involved in the investigation. Offenders may be deliberately including third countries in their attacks in order to make investigation more difficult. Criminals may deliberately choose targets outside their own country and act from countries with inadequate cybercrime legislation. The harmonization of cybercrime-related laws and international cooperation would help. Two approaches to improve the speed of international cooperation in cybercrime investigations are the G8 24/7 Network and the provisions related to international cooperation in the Council of Europe Convention on Cybercrime [36].

Due to the transnational dimension of the Internet and the globalization of services, an increasing number of cybercrimes have an international dimension. Countries that desire to cooperate with other countries in investigating cross-border crime will need to use instruments of international cooperation. Taking into account the mobility of offenders, the independence from presence of the offender and the impact of the offence shows the challenge and the need for a collaboration of law-enforcement and judicial authorities. Due to differences in national law and limited instruments, international cooperation is considered to be one of the major challenges of a globalization of crime. Within a comprehensive approach to address cybercrime, countries need to consider strengthening their ability to cooperate with other countries and making the procedure more efficient [37, 38].

The Group of Eight (G8)

In 1997, the Group of Eight (G8) established a "Subcommittee on High-tech Crimes" dealing with the fight against cybercrime. During their meeting in Washington DC, United States, the G8 Justice and Home Affairs Ministers adopted ten Principles and a Ten-Point Action Plan to fight high-tech crimes. The Heads of the G8 subsequently endorsed these principles, which include [39]:

1. There must be no safe havens for those who abuse information technologies.
2. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.
3. Law-enforcement personnel must be trained and equipped to address high-tech crimes.

In 1999, the G8 specified their plans regarding the fight against high-tech crimes at a Ministerial Conference on Combating Transnational Organized Crimes in Moscow, Russian Federation. They expressed their concerns about crimes (such as child pornography), as well as traceability of transactions and trans-border access to stored data. Their communiqué contains a number of principles in the fight against cybercrime that are today found in a number of international strategies. One of the practical achievements of the work done by expert groups has been the development of an international 24/7-network of contacts requiring participating countries to establish points of contact for transnational investigations that are accessible 24 hours a day, 7 days a week. At the G8 Conference in Paris, France in 2000, the G8 addressed the topic of cybercrime with a call to prevent lawless digital havens. Already at that time, the G8 connected its attempts for international solutions to the Council of Europe's Convention on Cyber crime (the "Convention on Cyber crime") [40, 41].

The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors [42, 43]."

The meeting of the G8 Justice and Home Affairs Ministers was followed by the G8 Summit in Moscow, where the issue of cyber terrorism was discussed. The summit declaration calls for measures in the fight against cyber terrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists" [44].

United Nations and the United Nations Office on Drugs and Crimes

The United Nations has undertaken several important approaches to address the challenge of cybercrime. While in the beginning its response was limited to general guidelines, the organization has in

recent times dealt more intensively with the challenges and legal response [45].

UN Convention on the Rights of the Child (CRC), 1989

The United Nations Convention on the Rights of the Child, adopted in 1989, contains several instruments aiming to protect children. It does not define child pornography, nor does it contain provisions that harmonize the criminalization of the distribution of online child pornography. However, it calls upon Member States to prevent the exploitative use of children in pornographic performances [46].

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography

The Optional Protocol not only addresses the issue of child pornography in general, but explicitly refers to the role of the Internet in distributing such material. Child pornography is defined as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. The Optional Protocol requires the parties to criminalize certain conduct – including acts related to child pornography: "producing, distributing, disseminating, importing, exporting, offering, selling or possessing child pornography [47].

Intergovernmental Expert Group on Cybercrime (2011)

Following the decision of the Member States to call upon UNODC to set up an intergovernmental working group, the first meeting of the group was held in Vienna in January 2011. The expert group included representatives of Member States, intergovernmental and international organizations, specialized agencies, private sector and academia. During the meeting the members of the expert group discussed a draft structure for a comprehensive study analysing the issue of cybercrime, as well as the response. With regard to the legal response, a number of members underline the usefulness of existing international legal instruments, including the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime, and the desirability of elaborating a global legal instrument to address specifically the problem of cybercrime. It was agreed that the decision on whether a global instrument should be developed will be made after the study was conducted.

The main problem for developing countries is the fact that the establishment of such contact point is mandatory. While for developed countries establishing and maintaining such a contact point will most likely not be challenging utilising a specialized police force dealing with cybercrime in night and day shifts, is however a challenge for countries where the specialized police force dealing with cybercrime consists of only one single police man. In those cases the obligation will require significant investments. That the accession to and implementation of the Convention does not have associated costs for the countries, as was recently stated by a Council of Europe representative at a conference in the Pacific is therefore only accurate if indirect costs, e.g. for maintaining a 24/7 contact point or for implementing technology to record traffic data in real time, are excluded [48].

It was one of the key intentions of the Convention to provide a comprehensive legal approach that addresses all relevant areas of cybercrime. But comparing the Convention with other approaches – especially the Commonwealth Model Law on Computer and Computer-related Crime as well as the EU instruments such as the E-Commerce Directive, shows that important aspects are missing. Examples are provisions dealing with the admissibility of electronic evidence or with the liability of Internet Service Providers (ISPs). Especially the missing provision of an, at least, basic regulatory framework related to the admissibility of electronic evidence has significant consequences as electronic evidence is widely characterized as a new category of evidence. And unless a country has other instruments in place or its courts hold such evidence admissible, the country might not be able to sentence any offenders despite having fully implemented the Convention.

Finally, a new international approach could – in addition to including basic standards that are similar in the different legal approaches – focus on a gap analysis to identify areas that are not yet sufficiently addressed, and thus criminalize certain cybercrime-related acts and define procedural instruments that are not yet covered by existing instruments. Since 2001, a number of important developments have taken place. When the Council of Europe Convention on Cybercrime was drafted, "phishing," "identity theft" and offences related to online games and social networks were not as relevant as they have since become. A new international approach could continue the harmonization process by including further offences with a transnational dimension.

As pointed out previously, cybercrime is a truly transnational crime. Having regard to the fact that offender can, in general, target users in any country in the world, international cooperation of law enforcement agencies is an essential requirement for international cybercrime investigations. Investigations require means of cooperation and depend on the harmonization of laws. Due to the common principle of dual criminality, effective cooperation first requires harmonization of substantive criminal law provisions in order to prevent safe havens. In addition, it is necessary to harmonize

investigation instruments, in order to ensure that all countries involved in an international investigation have the necessary investigative instruments in place to carry out investigations. Finally, effective cooperation of law-enforcement agencies requires effective procedures on practical aspects. The importance of harmonization triggers the need for participation in the global harmonization process, which is therefore at least a tendency, if not a necessity, for any national anti-cybercrime strategy.

Despite the widely recognized importance of harmonization, the process of implementing international legal standards is far from being completed. One of the reasons why national approaches play an important role in the fight against cybercrime is that the impact of the crimes is not the same everywhere. One example is the approach taken to combat spam. Spam-related e-mails especially affect developing countries. This issue was analysed in an OECD report. Due to scarcer and more expensive resources, spam turns out to be a much more serious problem in developing countries than in western countries. The different impacts of cybercrime, together with existing legal structures and traditions, are the main reasons for a significant number of legislative initiatives at the national level which are not, or only partly, dedicated to the implementation of international standards.

In times of technical globalization this may seem like a slightly surprising discussion, as anybody wishing to connect to the Internet needs to make use of the (technical) standard protocols in place. Single standards are an essential requirement for the operation of the networks. However, unlike technical standards, the legal standards still differ. It must be questioned whether national approaches can still work, given the international dimension of cybercrime. The question is relevant for all national and regional approaches that implement legislation which is not in line with existing international standards [49].

A lack of harmonization can seriously hinder international investigations, whereas national and regional approaches which go beyond international standards avoid problems and difficulties in conducting international investigations. There are two main reasons for a growing number of regional and national approaches. The first is legislative speed. Neither the Commonwealth nor the Council of Europe can force any of their Member States to use their instruments. In particular, the Council of Europe has no instrument to instruct a signatory of the Convention on Cybercrime to ratify it. The harmonization process is therefore often considered to be slow compared to national and regional legislative approaches.

Unlike the Council of Europe, the European Union has means to force Member States to implement framework decisions and directives. This is the reason why a number of European Union countries which signed the Convention on Cybercrime in 2001, but have not yet ratified it, have nevertheless implemented the 2005 EU Council Framework Decision on attacks against information systems. The second reason is related to national and regional differences. Some offences are only criminalized in certain countries in a region. Examples are religious offences. Although it is unlikely that an international harmonization of criminal law provisions related to offences against religious symbols would be possible, a national approach can in this regard ensure that legal standards in one country can be maintained.

National approaches face a number of problems. In regard to traditional crimes, the decision by one country, or a few countries, to criminalize certain behaviours can influence the ability of offenders to act in those countries. However, when it comes to Internet-related offences, the ability of a single country to influence the offender is much smaller as the offender can, in general, act from any place with a connection to the network. If they act from a country that does not criminalize the certain behaviour, international investigations as well as extradition requests will very often fail. One of the key aims of international legal approaches is therefore to prevent the creation of such safe havens by providing and applying global standards. As a result, national approaches in general require additional side measures to be able to work. The most popular side measures are criminalization of the user in addition to the supplier of illegal content, and of services used in the committing a crime.

One approach is criminalization of the use of illegal services in addition to the sole criminalization of offering such services. The criminalization of users who are located inside the jurisdiction is an approach to compensate for the lack of influence on providers of the services who act from abroad. A second approach is the regulation and even criminalization of offering certain services within the jurisdiction that are used for criminal purposes. This solution goes beyond the first approach, as it concerns businesses and organizations which offer neutral services that are used for legal as well as illegal activities. An example of such an approach is the United States Unlawful Internet Gambling Enforcement Act of 2006.

CONCLUSION

Issues related to cyber-crime, virtual currency (bit-coin), Internet blocking, sexting, child pornography, surveillance, cyber terrorism, encryption, digital India, social media, cyber security have been discussed in the legal context. Further, considering the nature of the subject and the international perspective, it provides a comparative analysis of corresponding

provisions in other jurisdictions. Hundreds of judgments, including that of Shreya Singhal, Aadhaar, Bazee, etc. have been interwoven seamlessly to underline the way judges have been weaving technology with judicial wisdom and coming out with judicial interpretation of various facets of technology.

REFERENCES

1. Zanini, M., & Edwards, S. J. A. "The Networking of Terror in the Information Age". In Arquilla, J., & Ronfelt, D. (Eds), Networks and Netwars, 30.
2. Zanini, M., & Edwards, S. J. A. "The Networking of Terror in the Information Age". In Arquilla, J., & Ronfelt, D. (Eds), Networks and Netwars, 45.
3. Sussmann, M. A. (2013). The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium. Duke Journal of Comparative & International Law, (9).
4. "Cyber Thieves are Caught, But Conviction is Wobbly", Hindustan Times, August 9, 2006, 18.
5. Justice, Y. S. (2010). Cyber Laws, Universal Law Publishing Co. Pvt. Ltd.
6. A & M Records Inc v. Napster Inc, 114 F. Supp 2d 896 (N.D. Cal 2000).
7. Kabushiki Kaisha Sony Computer Entertaining v. Stevens, 2002 FCA 906.
8. MGM Studios Inc. v. Grokster Ltd., 545 US 193.
9. Vivek, S. (2010). Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication.
10. Vivek, S. (2010). Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 172.
11. Vivek, S. (2010). Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, 173.
12. Vishwanath, P. (2010). Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, Central Law Agency Publication, Allahabad.
13. Vishwanath, P. (2010). Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, Central Law Agency Publication, Allahabad, 166.
14. Nandan, K. (2012). Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., New Delhi.
15. Nandan, K. (2012). Law relating to Computers, Internet and E-commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., New Delhi, 52.
16. Dasgupta, M. (2014). Cyber Crime in India: A Comparative Study, Eastern Law House Publication, Kolkata.
17. Dasgupta, M. Cyber Crime in India: A Comparative Study, Eastern Law House Publication, Kolkata, 200, 8.
18. Verma, S. K., & Raman, M. (2004). Legal Dimensions of Cyber Space, Indian Law Institute Publication, New Delhi.
19. Verma, S. K., & Raman, M. (2004). Legal Dimensions of Cyber Space, Indian Law Institute Publication, New Delhi, 1.
20. Verma, S. K., & Raman, M. (2004). Legal Dimensions of Cyber Space, Indian Law Institute Publication, New Delhi, 2.
21. Vakul, S. (2010). Information Technology: Law and Practice, Universal Law Publication Co., New Delhi.
22. Vakul, S. (2010). Information Technology: Law and Practice, Universal Law Publication Co., New Delhi, 251-53.
23. Vakul, S. (2010). Information Technology: Law and Practice, Universal Law Publication Co., New Delhi, 257.
24. Vakul, S. (2010). Information Technology: Law and Practice, Universal Law Publication Co., New Delhi, 260.
25. Rodney, D. R. (2016). Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet), Wadhwa Publication, Nagpur.
26. Chaubey, R. K. (2009). An Introduction to Cyber Crime and Cyber Law, Kamal Law House Publication, Kolkata.
27. Agarwal, S. C. (2001). "Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements", pp. 4-11, CBI Bulletin, 2001 Feb.
28. Agarwal, S. C. (2001). "Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements", pp. 4-11, CBI Bulletin, 2001 Feb. P. 08.
29. Agarwal, S. C. (2001). Training on Cyber Law, Cyber Crime and Investigation by Police: Need of Awareness and Requirements, 4-11, CBI Bulletin, 2001 Feb. 09.
30. Abhimanyu, B. (2010). "Cyber Crime and Law in India", 16-30, Indian Journal of Criminology and Criminalistics.
31. Dalal, A. S. (2010). "Jurisdiction in Cyberspace", 37-56, M.D.U. Law Journal.
32. Malik, J. K., & Choudhury, S. (2018). The Criminals In A Cyber Environment Using Computer Networks. International Journal Of Current Innovation Research, 4(12):1416-1422.
33. Netizen is a person who is associated with the computer. Available on http://www.wisegeek.com/what-is-a-netizen.htm, Retrieved on 21 November, 2013.
34. "Total number of Websites, Available on http://www.internetlivestats.com/total-number-of-websites/., Retrieved on 21 November, 2014.
35. Sharma, B. R. (2006). Computer Crimes: Scientific Criminal Investigation, 27, Universal Law Publishing Co.

36. Amarnathan, L. C. (1999). Crimes Related to Computer Network, 39, CBI Bulletin, February.
37. Chetan, S. (2015). Fundamentals of Information Technology, 341, Kalyani Publishers.
38. "Inventing the Web: Tim Berners-Lee's 1990 Christmas Baby", Posted on November 24, 2010 by Eric Rumsey, Available on http://blog.lib.uiowa.edu/hardinmd/2010/11/24/inventing-the-web-tim-berners-lees-1990-christmas-baby/. Retrieved on 21 March 2012.
39. EC: Council Directive 2008/114/EC, of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the need to Improve their Protection, EC, Brussels, Belgium, 2008.
40. Thomas, D., & Loader, B. D. (2000). Introduction. In Thomas, D., & Loader, B. D. (Eds), Cybercrime: Law enforcement, Security, and Surveillance in the Information Age, 3, Routledge, New York.
41. (United States Code Congressional and Administrative News, 98th Congress, Second Session, 1984, Oct. 19, volume 2; par. 3077, 98 STAT. 2707 [West Publishing Co., 1984]).
42. Dunnigan, J. F. (2003). The Next War Zone: Confronting the Global Threat of Cyberterrorism, Citadel Press, New York.
43. Collin, B. (1996). The Future of Cyberterrorism, Proceedings of 11th Annual International Symposium on Criminal Justice Issues: The University of Illinois at Chicago.
44. U. N. Counter-Terrorism Implementation Task Force, Report of the Working Group on "Countering the Use of the Internet for Terrorist Purposes", 8 (February 2009), Available on http://www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf. Retrieved on 30 June 2012.
45. Malik, J. K., & Choudhury, S. (2019). Cyber Space-Evolution & Growth. East African Scholars Journal of education, Humanities and Literature, 2(3):170-190.
46. Malik, J. K., & Choudhury, S. (2019). A Brief Review on Cyber Crime-Growth and Evolution. Pramana Research Journal, 2019; 9(3): 242.
47. Malik, J. K., & Choudhury, S. (2018). Policy Considerations in India Against Cyber Crime. International Journal of Recent Scientific Research, 9: 12(A), 29811-29814.
48. Malik, J. K., & Choudhury, S. The Criminals In A Cyber Environment Using Computer Networks. International Journal Of Current Innovation Research, 4(12):1416-1422.
49. Malik, J. K., & Choudhury, S. (2018). Cyber Crimes- Policy in India, International Research Journal of Human Resources and Social Sciences, 5(4):554-565.