CONCEPT AND CLASSIFICATION OF CYBER CRIME

RAJEEV KUMAR
Assistant Professor, Faculty of Law, Major S.D. Singh University, Farrukhabad (UP)

ABSTRACT

The internet is one of the most significant inventions in the communication sector with the help of which, people living across the globe can communicate with each other without realising the distances between them.[1] It has diminished the boundaries among people and provides them with opportunities to make better relations at both the personal as well as the professional fronts. From 181.7 million in 2015 to 216.5 million in 2016 and a projected 250.8 million in 2017, the number of social network users in India has grown significantly.

Though, it is a boon on one side, but on the other side, it has created insecurity in the lives of women due to the increasing criminal activities in the virtual world. Security of females of all ages and backgrounds are in a vulnerable position with the emergence of internet. Women are particularly vulnerable to cybercrime and victimisation, which is a serious threat to personal safety.

Keywords: Internet, Unauthorized access, Cyber-crime, Cyber law, Cyberspace, Punish, Network

INTRODUCTION

The word Cyber Crime consists of two words: "Cyber" which donates virtual space and "Crime" which donates as an act which is an offence against the society. So, it can be very well said the cybercrime is a crime done in the virtual world. Cyber Crime has no limitation and it is not bound only to a particular country. It can be across the world, from anywhere and at any time.

In 1820, first cybercrime was reported in France. In that case an act of sabotage was committed by the employees of a textile industry. The first identified cybercrimes were related to computer intrusions and fraud. But with the passing of time, the computer crimes also became advanced and in today's time there is a rapid increase in the cybercrime which is hard to trace, at times.

As a result of ICT's prelude, civilization has been given access to advanced and fast communication. At small, this cutting-edge ICT has supplanted the old routes of communication, allowing us to conduct business with greater ease, speed, convenience, and expediency. It has improved the way trade and commerce is done, and it has pushed trade and commerce to new heights of growth and development along the road. Even though ICT has made it easier for people to communicate, it has also led to an increase in crimes perpetrated via ICT, known as "Cyber Crimes," which has increased the size and scope of Cyber Law.

Legal protection and penalties for the use of ICT for illicit purposes have sounded alarm bells because of the increasing number of instances, methods, and modes used to perpetrate such sporadic crimes through the use of computers. There are two primary goals in this area of law, one of which is to promote the use of ICT and another of which is to prevent the illicit and unauthorized use of ICT.

CYBER CRIME: MEANING AND DEFINITION

It's important to note that "crime" is not a legal term in and of itself. This word has a deeper meaning and connotation when seen in the context of a society rather than the State. In this way, it resists any attempt to define it in a single, predetermined way. The term "wrong,""offence," or "misdemeanor" is often used interchangeably with "felony" our "wrongdoing." Criminality is a social as well as a financial issue. It has been around for as long as humanity has existed. In many ancient literature and legendary stories, crimes against people and the nation as a whole have been discussed, including theft, burglary, treason, and spying, among others.

As one of India's most authentic administrative treatises, Kautilya's Arthashastra, written around 350 BC, examines societal crimes, security measures rulers should take to suppress them, and conceivable crimes in a state. Additionally, it asks for distinct punishments to be given for each of the crimes listed. It also touches on the idea of compensating the victims for their losses. His theory of likely crime discusses how different crimes emerge as a result of changes in society. Crimes against women will rise as a result of the weak position of women in society and the abuse of authority in a specific sector, which will lead to the commission of crimes linked with power-play. As a result, a new type of crime known as "Cyber Crime" has emerged, a result of the rise of ICT. It's important to first comprehend what crime is, and then what cybercrime is, in order to fully grasp what it means.

MEANING OF CRIME

There is no doubt that crime in any form has a negative impact on society. Merriam Webster defines crime as an act or failure to act that violates public law and exposes the offender to criminal liability, especially where the offending act or failure to act is an outright violation of the law. Crime is defined by the Oxford English Dictionary as an act or omission that is regarded bad, humiliating, or wrong; that is, an offence that is subject to a penalty under the law. If an act is done or not done in defiance of public law, it is considered to be a crime. To put it simply, a crime is defined as "a breach of a right, viewed in terms of its potential for harm to society as a whole". According to the Oxford Dictionary, a crime can be defined as a violation of the law that is prohibited by statute or detrimental to the public good. A crime is a violation of the law that is penalized by a governmental body. Criminal law does not have a single, widely agreed definition of "crime," however some statutory descriptions exist for specific purposes.

A common belief is that crime is a legal classification; in other words, a crime is one that has been designated as such by the law in question. A crime or an offence (or criminal offence) may be defined as an act that harms not only an individual or people, but also the community, society, or the State as a whole, according to one definition (" a public wrong”). As a result, they are illegal and punishable under the law.

MEANING OF CYBER CRIME

Digital networks, despite their increasing popularity and ease of use, do come at a price, as the adage goes. Information and Communication technology has a price to pay for its convenience, speed, and ease of use. Cybercrime and digital attack occurrences have risen dramatically as businesses and society increasingly rely on computers and internet-based networking.

For the most part, these attacks are characterized as crimes that involve computers, computers, or networks. Financial scams, computer hacking, obtaining pornographic photos from the internet, virus attacks, email stalking, and the creation of hate-promoting websites are only a few examples of various types of cybercrimes.

In the late 1990s, a computer virus addressed to the general public infected almost 45 million computer users throughout the world, making it the first large case of a cybercrime. Because of the fast spread of the Internet and the digitization of commercial activity, cybercrime has expanded dramatically both in developed and developing nations. From corporate governance to state administration to the level of small shopkeepers computerizing their billing system, we find computers and other electronic gadgets permeating human existence because of the massive technological penetration in practically all spheres of society. We can't imagine doing anything these days without some sort of computer.

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.[2] Physical damage to computer equipment and stored data were the primary offences at this early period. As an example, a 1969 student revolt in Canada resulted in a fire at the institution that destroyed computer data stored there. In the mid-1960s, the United States started a debate on the creation of a central data-storage authority for all ministries.[3] Within this context, possible criminal abuse of databases and the related risks to privacy were discussed.[4]

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.[5] 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.[6] 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.[7] The shift from manual to computer-operated transactions led to another new form of crime – computer-related fraud.[8] Already at this time, multimillion dollar losses were caused by computer-related fraud.[9] Computer-related fraud, in particular, was a real challenge, and law enforcement agencies were investigating more and more cases.[10] 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.[11]

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.[12] 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.[13] International organizations also got involved in the process. OECD140 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.[14] 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.[15] 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 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",[16] and "botnet attacks",[17] and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP (VoIP) communication" and "cloud computing".[18] 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.

FUTURE TRENDS IN CYBER CRIME

The pace at which cybercrime is growing is one of the most disturbing trends. Valerie McNiven, a U.S. Treasury Advisor, has proclaimed "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion." She further added that "cybercrime is moving at such a high speed that law enforcement cannot catch up with it." It seems clear that the issue will only become worse in the next few years, now that professionals have realized the potential windfalls if exploited properly. Recently, there has been significant discussion over the amalgamation of organized criminals and cybercrime. Such a pairing indeed forebodes an ill omen for the near-term future. With most of the criminal groups operating out of Eastern Europe, Russia and Asia, where laws and enforcement are scanty, there seems little hope in containing and neutralizing the threat through traditional means. Phil Williams, a visiting scientist at CERT, summarized the issue succinctly. "The Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime it is difficult to ask for more."

The result that can then be expected will be an increase in sophisticated phishing attacks and other means for identity theft that may be two pronged. For example, using call centres to notify "customers" ahead of time of some issue, and then following up with emails that request personal information. The aggregation of personal information in many third-party data centres will prove to be valuable targets to infiltrate. It is not hard to imagine criminals using data mining techniques to find the most gullible consumers, or tailoring phishing emails for specific people based on their medical, financial or personal history. Identify theft will also move in more automated directions. For example, botnets will become vehicles not just for denial-of-service attacks and spam, but also as giant search platforms for finding personal information, like credit cards and social security numbers. Controllers of the botnets will then receive payment to run queries on their "database."

With professional criminals managing the money laundering and organization of such schemes, it begs to ask where all the technical know-how will come from in order to perform cybercrime. Unfortunately, there are growing numbers of intelligent black-hats with university degrees spread around the globe, many of them operating in countries where legal employment does not pay as well and the chances of being caught are slim. But more troublesome is that it has become easier than ever before to be a hacker capable of inflicting great harm on networks and committing cybercrime. The Internet has created a repository of knowledge where anyone is able to learn the fundamentals of subverting computer systems, with numerous tutorials available that spell out in nearly layman's terms how to perform a buffer overflow or a man in the middle attack. Interestingly, the greatest problem is not those who will take the time to learn and find new exploits. In fact, this group will probably remain a small, highly intelligent network of researchers and security groups focused solely on finding holes in software. In this, it is preordained, that even if someone is motivated to learn how exploits work, finding a new exploit takes a degree of investigation, skill and diligence that most are not willing to invest. The real threat comes from the profound ease at which anyone can run a program like "Metasploit," a framework for running exploits against targets that allows new modules to be imported and run automatically. The attacker literally needs to know nothing about how computers work, besides how to operate one. In fact, for almost all attacks, the hard work is done by a small group of people, and then released into the public domain, allowing almost anyone to just run the attack. Botnets are no longer hand-crafted software made by one group who truly understood the fundamentals, but instead are open-source collaborative efforts that aim to make it as easy as possible to control remote computers, such as Botnet, eggheads and Sharbot, all available from Source Forge.

CONCLUSION

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect a percentage of possible victims. The others need to be automatically protected through measures that do not stress and require considerable participation. Security needs to be easy and effective if it is doing work. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cybercrime will be proportional to real-world crimes, if not better.

WORKS CITED

1. Leonard-Barton, Dorothy, and Kraus, William A. *Implementing New Technology.* United States: Harvard Business School Reprint, 1985.

2. Regarding the related challenges, see: Slivka/Darrow. Methods and Problems in Computer Security. *Journal of Computers and Law*, 1975, page, 217 et seq.

3. Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman. Report of the Committee on the Preservation and Use of Economic Data, 1965, available at: www.archive.org/details/Report Of The Committee On The Preservation And Use Of EconomicData1965.

4. For an overview about the debate in the US and Europe, see: Sieber, *Computer Crime and Criminal Law*, 1977.

5. Stevens. Identifying and Charging Computer Crimes in the Military. *Military Law Review,* Vol. 110, 1985, page 59.

6. McLaughlin. Computer Crime: The Ribicoff Amendment to United States Code, Title 18. *Criminal Justice Journal*, 1978, Vol. 2, page 217 et seq.

7. Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 225 et seq.; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

8. McLaughlin. Computer Crime: The Ribicoff Amendment to United States Code, Title 18, *Criminal Justice Journal*, 1978, Vol. 2, page 217 et seq.; Bequai, Computer Crime: A Growing and Serious Problem, *Police Law Quarterly*, Vol. 6, 1977, page 22.

9. Nycum. Legal Problems of Computer Abuse. *Washington University Law Quarterly*, 1977, page 527.

10. Regarding the number of the cases in early cybercrime investigations, see: Schjolberg, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

11. Third Interpol Symposium on International Fraud, France 1979.

12. BloomBecker. The Trial of Computer Crime. *Jurimetrics Journal*, Vol. 21, 1981, page 428; Schmidt, Legal Proprietary Interests in Computer Programs: The American Experience. *Jurimetrics Journal*, Vol. 21, 1981, 345 et seq.; Denning, Some Aspects of Theft of Computer Software. *Auckland University Law Review*, Vol. 4, 1980, 273 e\t seq.; Weiss, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, page 1 et seq.; Bigelow, The Challenge of Computer Law. *Western England Law Review,* Vol. 7, 1985, page 401; Thackeray, Computer-Related Crimes. *Jurimetrics Journal*, 1984, page 300 et seq.

13. Schjolberg. Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

14. Regarding the transnational dimension of cybercrime see: Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

15. Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

16. The term “phishing” describes an act that is carried out to make the victim disclose

personal/secret information. The term originally described the use of e-mails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions.

17. Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see Wilson, Botnets, Cybercrime, and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

18. Velasco San Martin. Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 et seq.