Cyber - Crime and Cyber Criminals: A Global Perspective

Meenakshi John[1], Jatin Kumar Lal[2], S. Dominic Rajkumar[3]

ST. Andrew's College, Gorakhpur - Uttar Pradesh, India

Abstract: ***Cybercrime has caused immense harms to individuals, organizations and to the Government. The present generation has been characterized by massive technological innovations. The digital age has taken over the social, political, and economic dimensions of human life. Worldwide, there is a rise in the use of electronic gadgets. The immense advances in digital technologies have led to significant growth in criminality, especially in cyberspace. Cybercrimes have grown progressively with perpetrators innovating newer and sophisticated techniques every day. Despite the measures taken by the international community to control the effects, cybercrimes have continued to rise across the world. This paper deals with the common areas where cybercrime usually occurs and the different types of cybercrimes that are committed every day.***

Keywords: Cybercrime, hacking, computer fraud, Viruses, Worms, Trojans, Cyber stalking

1. Introduction

Crime is an unlawful act which is punishable by a state (en. wikipedia. org). However, certain purposes have no statutory definition provided. Crime is also called as an offense or a criminal offense. It is harmful not only to some individual but also to the community or the state. Cybercrime is emerging as a serious threat. Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks (Gandhi, V. K.2012, Krausz& Walker, 2013, Alghamdi, 2020). It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. Along with the phenomenal growth of the Internet, the growth of cybercrime opportunities has increased manifold. As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few.

Alsmadi, (2019) acknowledges that there is no clear definition of cybercrime in the academic milieu. Some quotas have referred to it as "electronic crime, " "computer crime, " and "computer - related crime. " Cybercrime in the context of national security may involve activism, traditional espionage, or information warfare and related activities. Cybercrime detection methods and classification methods have come up with varying levels of success for preventing and protecting data from such attacks. Several laws and methods have been introduced in order to prevent cybercrime and the penalties are laid down to the criminals. However, the study shows that there are many countries facing this problem even today and United States of America is leading with maximum damage due to the cybercrimes over the years.

According to the survey from 2001 to 2021, the amount of monetary damage caused by cybercrime reported to the Internet Crime Complaint Center (IC3) increased significantly. In the last reported period, the annual loss of complaints referred to the IC3 amounted to 6.9 billion U. S. dollars, up from 1 billion U. S. dollars in 2015. The Cyber Security Breaches Survey of 2018, 40% of businesses worldwide have been a victim of cybercrime. The research projects that up to six trillion dollars per year could be lost in the hands of cybercriminals. This study examines the various forms of cybercrimes worldwide and why there is a rapid increase in such activities. The study also recommends various measures and recommendations to curtail cybercrime incidents. They include the introduction of a concrete legal framework, establishment, and strengthening of cybercrime law enforcement organizations complete with high technology monitoring devices and modern infrastructure.

2. Forms of Cybercrimes

A computer is an indispensable tool for almost all cyber - crimes. However, as more devices are enabled to communicate with the Internet, the hackers arsenal of tools is likely to multiply. A computer can be the target of the offense, the tool used in the offense, or may contain evidence of the offense. The different uses of computer will result to the criminal statutes. When a computer is the target of the offense, the criminal goal is to steal information from, or cause damage to, a computer, computer system, or computer network. There has been numerous scholarly work in the past that has aimed at defining cybercrime through different phases of history and under various circumstances. Bernik, (2014) highlights cybercrime as illegal behavior that is carried out by electronic operations and seeks to target computer systems and data processed by the devices. Among the first people to write about computer crime was Donn Parker who was considered the first national expert on computer security in the United States. Parker defined it as computer abuse saying it involves intentional acts in which victim (s) suffer a loss while others make a profit. It has also been proved that perpetrators are not always be after profit. There is also another group of cybercriminals known as "hacktivists". These are people who protest organizations' policies and practices. For example in 2010 the Anonymous hacktivist group attacked Mastercard, Visa, and Paypal in retribution for stopping donations to WikiLeaks (Grispos, 2019).

1) Hacking

Gupta (2019) has defined hacking as gaining unauthorized access or compromising systems to get access. While hacking may be characterized as criminal in some countries, there is a need for information security experts with the knowledge of hacking to counter cyber threats in the fields of business, politics, social media, and national security. There are three main types of hackers, according to Gupta, (2019). The first type of hackers is the white hat hacker who defends systems from other attackers. They are authorized, and they are mainly known for the provision of security. The second type is the black hat hacker who works without authorization. This caliber of hackers is also known as malicious hackers, and they act without the permission of any kind. The third type is the Grey hat hacker; whose sword is double - edged. They can be both offensive and defensive, depending on the benefits.

2) Computer Fraud

This form of cybercrime is also known as “phishing. ” It involves situations in which perpetrators pose as representatives of an organization, aiming directly at bank customers (Doyle, 2011). Older communication tools like telephones and postal mail were previously the instruments used to scam and defraud people. Today, modern tools like email, text messages, and social media chats have replaced traditional methods and are now used to commit cybercrime. Fraudsters impersonate legitimate senders such as bankers and they can get away with essential credentials such as usernames, passwords, and account numbers. In this form of cybercrime, the fraudsters manually target recipients through texts that are sent out in bulk with the sender hoping to ploy unsuspecting victims into sharing their personal data. Cybercriminals may also act to be promoting deals that appear too good to be true. They may pretend to offer victims "investment" opportunities upon which after some time they dazzle away with victims' funds.

3. Malicious Code – Viruses, Worms and Trojans

3.1 Viruses

A virus is a program that modifies other computer programs. These modifications ensure that the infected program replicates the virus. Not all viruses cause damage to its host. A virus is typically spread form one computer to another by e - mail, or infected disk. However, a virus cannot infect another computer until the program is executed. A common method of virus execution is when a computer user is tricked into opening a file attacked to an e - mail, thinking the file is a harmless program coming from a friendly source. The most popular example of virus is the Melissa virus which was launched in March 1999. The Melissa virus was hidden in a Microsoft word attachment that appeared to come from a person knows to the recipient. The program activated a macro that tread the first fifty e - mail addresses located in the Microsoft Outlook e - mail program and e - mailed itself to the fifty addresses. The virus was estimated to have caused $80 million in damages.

3.2 Worms

A worm is standalone program that replicates itself. A worm can wind its way throughout a network system without the need to be attached to a file, unlike viruses. For example, I love You worm in 2001 was estimated the loss caused to be $US 10.7 billion.

3.3 Trojan Horses

A Trojan Horses is an innocent looking computer program that contains hidden functions. They loaded onto the computer’s hard drive an executed along with the regular program. However, hidden in the innocent program is a sub - program that will perform an unauthorized function. A Trojan horse is the most common way in which viruses are introduced int computer systems. For example, Back Orifice 2000 is a program designed for misuse and attack on another computer

3.4 Cyberstalking

Cyber stalking is when a person is followed and pursued online. Their privacy is invaded, their every move watched. It is a form of harassment and can disrupt the life of the victim and leave them feeling very afraid and threatened. Stalking or being 'followed' are problems that many people, especially women, are familiar with. Sometimes these problems (harassment & stalking) can occur over the Internet. This is known as cyber stalking. A stalker could be of either sex.

3.5 Financial crimes

This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

3.6 Unique Challenges

As traditional criminals will use the computer technology, the nature and features of the cybercrime will bring new challenges for the Governments and policy makers due to; Anonymity;

- Global reach (including issues of jurisdiction, disparate criminal laws and the potential for large scale victimization);
- The speed at which crimes can be committed;
- The volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints, trace evidence or DNA; and
- The high cost of Investigations.

Cyber Laws in India

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e - commerce in India. The cyber laws have a major impact for e - businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

4. Conclusion

Criminal behavior on the Internet, or cybercrime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already features in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes and we must be prepared to deal with this new challenge.

Acknowledgements

The authors would like to thank the Principal and the Secretary of the college for the constant encouragement and support.

References

[1] en. wikipedia. org/wiki/Crime

[2] Alsmadi, I. (2019). Cyber intelligence. The NICE Cyber Security Framework, 75 - 90. https: //doi. org/10.1007/978 - 3 - 030 - 02360 - 7_5 [3]

[3] Bernik, I. (2014). Cybercrime. Cybercrime and Cyberwarfare, 1 - 56. https: //doi. org/10.1002/9781118898604. ch1Krausz, M., & Walker, J. (2013). The true cost of information security breaches and cybercrime. IT Governance Publishing.

[4] Alghamdi, M I.2020. A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide. International Journal of Engineering Research & Technology 9 (6): 731 - 735.

[5] Doyle, C. (2011). Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws. DIANE Publishing.

[6] Grispos, G. (2019). Criminals: Cybercriminals. Encyclopedia of Security and Emergency Management, 1 - 7. https: //doi. org/10.1007/978 - 3 - 319 - 69891 - 5_80 - 1

[7] Gupta, S. (2019). Ethical hacking terminologies. Ethical Hacking – Learning the Basics. https: //doi. org/10.1007/978 - 1 - 4842 - 4348 - 0_1