

Cyber Crime: Challenges and its Classification

Dr. Ajeet Singh Poonia¹

Associate Professor, CSE

¹Govt. College of Engineering and Technology, Bikaner, India

Abstract

Digital technology is encompassing in all walks of life, all over the world and has brought the real meaning of globalization. At the one end cyber system provides opportunities to communicate and at the other end some individuals or community exploit its power for criminal purposes. Criminals exploit the Internet and other network communications which are international in scope. Situation is alarming; Cyber crime is an upcoming and is talk of the town in every field of the society/system. Theoretically and practically this is a new subject for researchers and is growing exponentially. Lot of work has been done and endless has to be go because the invention or up gradation of new technology leads to the technical crime i.e. the digital or we can say the cyber crime or e-crime. This is because every day a new technique is being developed for doing the cyber crime and many times we are not having the proper investigating method/model/technique to tackle that newly cyber crime.

Keywords:- Digital technology, Cyber crime, Network communications, e-Crime.

1. INTRODUCTION

Crime is a major social and legal problem in the world we live in and population is one of the important factors, influencing incidence of crime. A positive association between the growth in incidence of crime and the population of the country has been experiential[1]. Presently the situation in the world is tough, particularly in context to cyber security part. In current scenario cyber crime is increasing very fast as the technology is growing very rapidly. So the cyber crime investigation is becoming a very complicated task to do without a proper framework. There is wide range of different types of cyber crime today. Solution of each case requires a very complicated task.

2. CONVENTIONAL CRIME

An act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction[2]. So we can say in easy word that, "crime is something that is against the law." Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment"[3].

3. CYBER CRIME

A generalized definition of cyber crime may be "Unlawful acts wherein the computer is either a tool or target or both" [4].

Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cyber crime. Cyber criminal can be motivated criminals, organised hackers, organised hackers, discontented employees, cyber terrorists. Cyber crime can include everything from non-delivery of goods or services and computer intrusions (hacking) to intellectual property rights abuses, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a growing list of other Internet-facilitated offenses. Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done. The anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities[5].

4. REASONS BEHIND THE CYBER CRIME

There are many reasons why cyber-criminals are doing cyber-crime; chief among them are mentioned below:

- A. For the sake of recognition.
- B. For the sake of quick money.
- C. To fight a cause one thinks he believes in.
- D. Low marginal cost of online activity due to global reach.
- E. Catching by law and enforcement agency is less effective and more expensive.
- F. New opportunity to do legal acts using technical architecture.
- G. Official investigation and criminal prosecution is rare.
- H. No concrete regulatory measure.
- I. Lack of reporting and standards
- J. Difficulty in identification
- K. Limited media coverage.
- L. Corporate cyber crimes are done collectively and not by individual persons[5,6].

5. CYBER CRIME CHALLENGES

Endless discussion is there regarding the pros and cons of cyber crime. There are many challenges in front of us to fight against the cyber crime. Some of them here are discussed below:

- A. Lack of awareness and the culture of cyber security, at individual as well as organizational level.
- B. Lack of trained and qualified manpower to implement the counter measures.
- C. No e-mail account policy especially for the defense forces, police and the security agency personnel.

- D. Cyber attacks have come not only from terrorists but also from neighboring countries contrary to our National interests.
- E. The minimum necessary eligibility to join the police doesn't include any knowledge of computers sector so that they are almost illiterate to cyber-crime.
- F. The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the origin of these cyber-crimes[7, 4].
- G. Promotion of Research & Development in ICTs is not up to the mark.
- H. Security forces and Law enforcement personnel are not equipped to address high-tech crimes.
- I. Present protocols are not self sufficient, which identifies the investigative responsibility for crimes that stretch internationally.
- J. Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compare to other crimes.

6. CLASSIFICATION OF CYBER CRIME

There are many types of cyber crime prevailing in the system; broadly we can classify them in to four major categories as discussed below:

6.1 CRIME AGAINST INDIVIDUALS

Cybercrimes committed against individual persons include such types of crimes like transmission of Child Pornography, Harassment of any one with the use of a computer such as e-mail, Cyber Defamation, Hacking, Indecent exposure, E-mail spoofing, IRC Crime (Internet Relay Chat), Net Extortion, Malicious code, Trafficking, Distribution, Posting, Phishing, Credit Card Fraud and Dissemination of obscene material including Software Piracy. The potential harm of such a crime to individual person can hardly be bigger.

6.2 CRIME AGAINST PROPERTY

Another classification of Cyber-crimes is that, Cybercrimes against all forms of property. These crimes include computer vandalism (obliteration of others' property), Intellectual Property Crimes, Threatening, Salami Attacks. This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the amendment is so small that it would normally go unobserved.

6.3 CRIME AGAINST ORGANIZATION

The third type of Cyber-crimes classification relate to Cybercrimes against organization. Cyber Terrorism is one discrete kind of crime in this kind. The growth of internet has shown that the standard of Cyberspace is being used by individuals and groups to pressure the international governments as also to terrorize the citizens of a country. This crime obvious itself into terrorism when a human being "cracks" into a government or military maintained

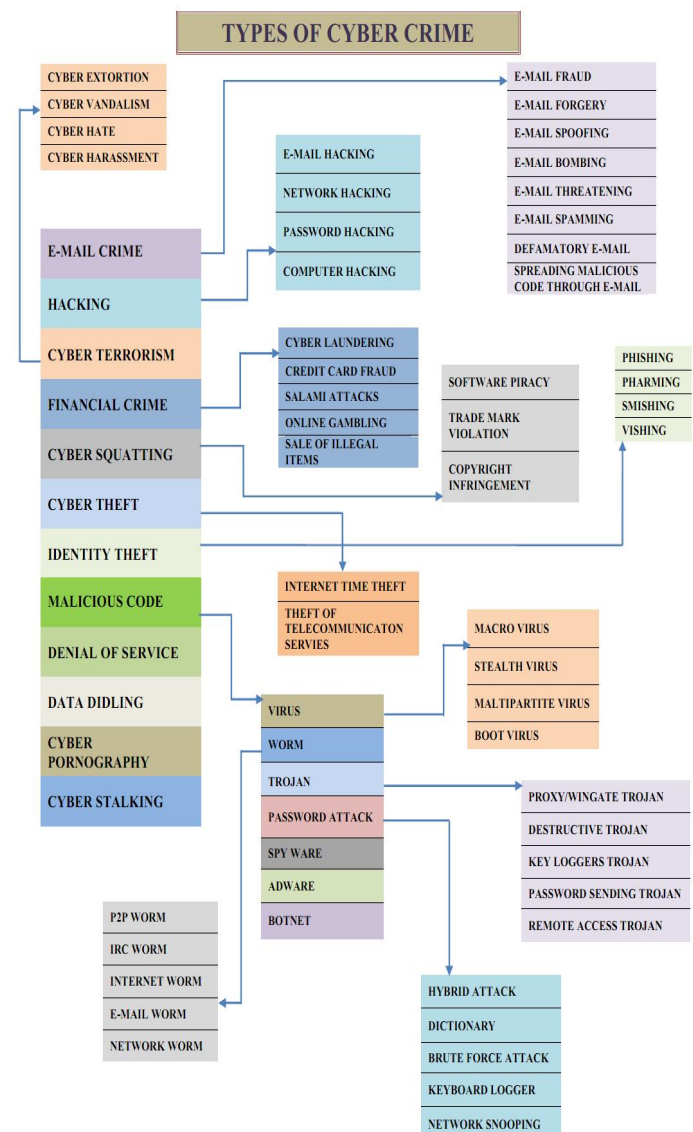
website. It is across the world agreed that any and every system in the world can be cracked.

6.4 CRIME AGAINST SOCIETY

The forth type of Cyber-crimes relate to Cybercrimes against society. In this category forgery, cyber terrorism, web jacking, polluting the Youth through Indecent, Financial Crimes, Sale of Illegal Articles, Net Extortion, Cyber Contraband, Data Diddling, Salami Attacks, Logic Bombs types of crime is included. Forgery currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers. Web Jacking hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

7. TYPES OF CYBER CRIME

As discussed earlier that cyber crime is different from the conventional crime. Same as conventional crime, cyber crime also constitutes of many types. Some of the types of cyber crime as shown in figure 1.1 as the cyber crime evolve with the invention of new technique itself.



8. CONCLUSION

Cyber crime has high potential and thus creates high impact when it is done. It is easy to commit without any physical existence required as it is global in nature due to this it has become a challenge and risk to the crime fighter and vice versa. The borderless nature of ICTs may not allow for rigid regulations and instead challenges the principle of criminal laws. As such, international laws and regulations combined with reliance on technologies are crucial to counter the crime race.

References

- [1] www.uncjin.org/Documents/EighthCongress.html.
- [2] <http://www.thefreedictionary.com/Gun+Crime>).
- [3] Williams, G.L., Glanville Williams Learning the Law, A.T.H. Smith, Editor. 2006, Sweet & Maxwell
- [4] Roshan, N., What is cyber Crime. Asian School of Cyber Law, 2008: Access at - http://www.asclonline.com/index.php?title=Rohas_Nagpal,
- [5] Govil, J., Ramifications of Cyber Crime and Suggestive Preventive Measures, in International Conference on Electro/Information Technology, 2007 IEEE. 2007: Chicago, IL. p. 610-615.
- [6] Jones, A., Technology: illegal, immoral, or fattening?, in Proceedings of the 32nd annual ACM SIGUCCS fall conference. 2004, ACM: Baltimore, MD, USA. p. 305-309.
- [7] Majesty, H., Cyber Crime Strategy, S.o.S.f.t.H. Department, Editor. 2010, The Stationery Office Limited: UK. p. 42.

Author



Dr. Ajeet S. Poonia was born in Rajasthan, India in 1980. He did his Ph.D MNIT, Jaipur, India in 2013 in Cyber Security Domain. He has 13 years of teaching experience . Presently

he is working as an Associate Prof. (Dept. of Computer Science) at College of Engineering & Technology, Bikaner, India. He has written 03 books, and many research papers at International Journals and conferences. He has organized several programs both at National and International level.