Challenges and Analysis in Cyber Crime

Dr. Pranav Patil
Assistant Professor, Department of Computer Science, M. J. College, Jalgaon, Maharashtra, India

Abstract: Digital technology is about all walks of life, all over the world and has brought the real meaning of globalization. Once end cyber system provides opportunities to communicate and at the other end some individuals or community utilize its command for criminal purposes. Criminals exploit the Internet and other network communications which are international in scope. Condition is alarming; Cyber crime is an upcoming and is the talk of the town in every field of the society or system. Theoretically and practically this is the latest subject for researchers and is growing exponentially. A lot of work has been done and continuous has to be gone because the invention or up gradation of new technology leads to the technical crime. The digital or we can say the cyber crime or e-crime. This is because every day a new technique is individual developed for doing the cyber crime and lots of times we are not having the proper investigating method or technique to tackle that newly cyber crime.

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

1. INTRODUCTION

Crime is a most important social and legal problem in the world we live in and population is one of the important factors, influencing the occurrence of crime. A positive association between the growth in the numbers of crime and the residents of the country has been observed. Presently the condition in the world is tough, particularly in context of cyber security part. In current scenario cyber crime is growing very rapid as the technology is growing very fast. So the cybercrime analysis is becoming a very complicated task to do without a proper framework. There is a large range of different types of cyber crime in our day. Solution of each case requires a very difficult task.

2. CONVENTIONAL CYBER CRIME

An act committed or omitted in contravention of a law forbidding or commanding it and for which punishment is imposed upon certainty. So we can say in simple word that, "crime is something that is beside the law." Crime is a common and economic occurrence and is as old as the human society. Crime is a legal concept and has the permit of the law. Crime or an offence is a legal incorrect that can be followed by criminal proceedings which may result into punishment.

3. CYBER CRIME

A generalized meaning of cyber crime may be "Unlawful acts wherein the computer is either a tool or target or both". Cyber Criminal is a who commits an illegal act with a guilty intention or commits a crime in context to cyber crime. Cyber criminals can be motivated criminals, organised hackers, organised hackers, discontented employees, cyber terrorists. Cyber crime can contain everything from non-delivery of goods or services and computer intrusions (hacking) to logical property rights abuses, economic espionage (theft of trade secrets), online extortion, international money rinse, identity theft, and a growing list of other Internet-facilitated offenses. Further, it is not easy to identify instantly about the crime technique used and to answer questions similar to where and when it was done. The ambiguity of the Internet makes it is the best channel and instrument for many organized crime activities.

4. REASONS BEHIND THE CYBER CRIME

There are lots reasons why cyber-criminals are doing cybercrime; chief with them are mentioned below:

- For the sake of recognition.
- For the sake of sudden money.
- To fight a cause one thinks he believes in.
- Low marginal cost of online movement due to global reach.

- Catching by law and an enforcement agency is less effective and more expensive.
- A new chance to do legal acts using technical architecture.
- Official investigation and criminal prosecution are rare.
- No solid regulatory measure.
- Lack of reporting and standards
- Difficulty in identifying
- Limited media
- Commercial cyber crimes are done as a group and not by individual persons.

5. CYBER CRIME CHALLENGES

Endless language is there concerning the execs and cons of cyber crime. There square measure several challenges ahead people to fight against the cyber crime. A number of now mentioned below:

a) Lack of consciousness and also the culture of cyber security, at individual also as structure level.
b) Lack of trained and qualified hands to use the counter measures.
c) No e-mail account policy particularly for the defense forces, police and also the security activity personnel.
d) Cyber attacks have come back not solely from terrorists however conjointly from the nearest countries opposing to our National benefit.
e) The minimum required eligibility to hitch the police doesn't contain any information of computers space so they are virtually illiterate to cyber-crime.
f) The speed of cyber technology changes all the time beats the progress of govt. sector so they are ineffectual to spot the idea of those cyber-crimes.
g) Promotion of analysis & Development in ICTs is not up to the mark.
h) Security services and enforcement personnel are not readys to deal with high-tech crimes.
i) Present protocols are not self enough, that identifies the inquiring responsibility for crimes that enlarge internationally.
j) Budgets for security purpose by the govt. notably for the coaching of function, security personnel's and examiners in ICT square measure fewer than compare to alternative crimes.

6. CLASSIFICATION OF CYBER CRIME

There are many kinds of cyber crime existing within the system; generally, we are able to classify them into four major classes as mentioned below:

6.1 CYBER CRIME AGAINST INDIVIDUALS

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

6.2 CYBER CRIME AGAINST PROPERTY

One more classification of Cyber crimes is that, Cybercrimes against all forms of property. These crimes include computer harm, Intellectual Property Crimes, Threatening and Salami Attacks. This kind of crime is normally established in the financial institutions or for the purpose of committing financial crimes. An important characteristic of this type of offence is that the amendment is so small that it would normally go unobserved.

6.3 CYBER CRIME AGAINST ORGANIZATION

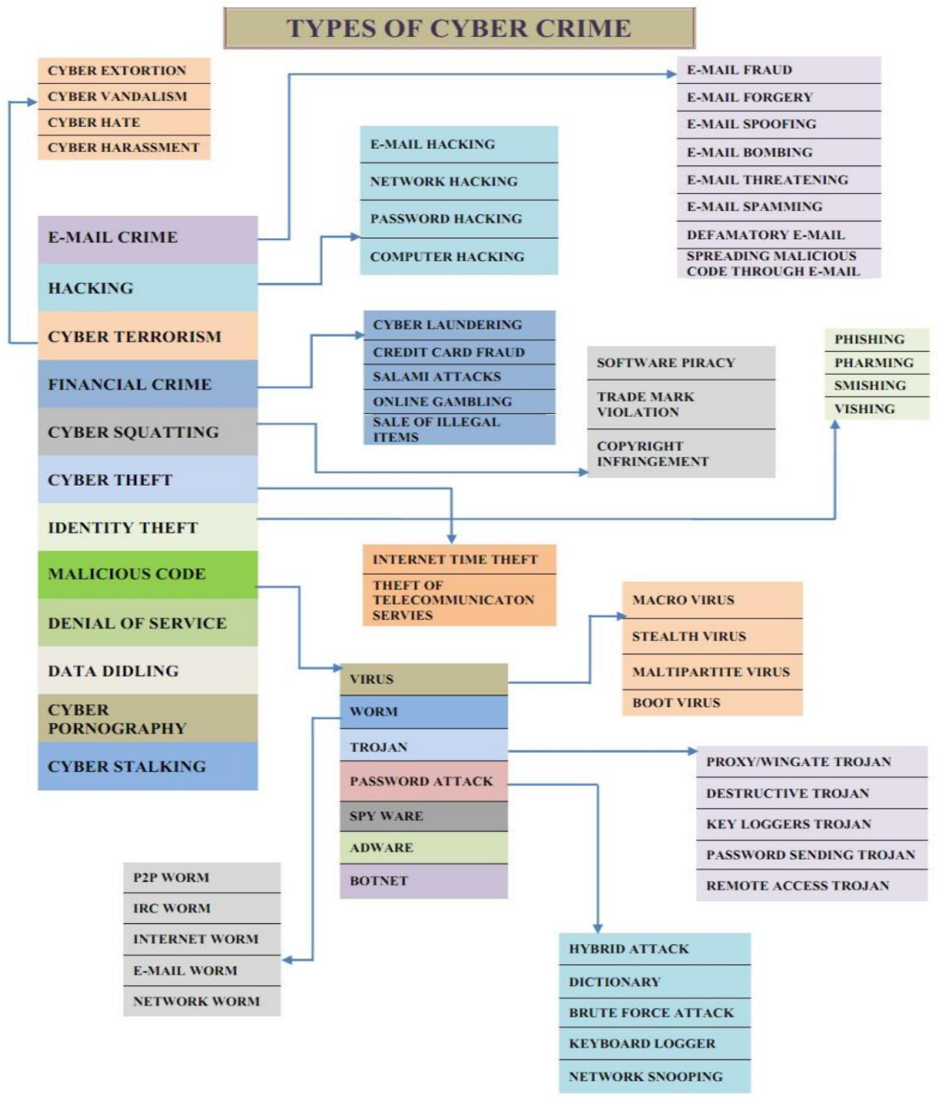
This type of cybercrime classifying communicates to Cybercrimes against the organization. Cyber Terrorism is one separate kind of crime in this kind. The expansion of the internet has shown that the standard of Cyberspace is being used by individuals and groups to force the international governments as also to terrorize the citizens of a country. This crime clears itself into terrorism when a human being "cracks" into a government or military maintained website. It is across the world approved that any and every system in the world can be cracked.

6.4 CYBER CRIME AGAINST SOCIETY

The Cyber-crimes communicate to Cybercrimes beside society. During this kind forgery, cyber terrorist act, internet jacking, polluting the Youth through Indecent, monetary Crimes, Sale of black-market Articles, web Extortion, Cyber Contraband, information Diddling, sausage Attacks, Logic Bombs forms of crime is enclosed. Fake currency notes, revenue stamps, score sheets etc is cast exploitation computers and prime quality scanners and printers. Internet Jacking hackers gain access and manage over the website of another; even they alter the content of website for fulfilling political objective or for cash.

7. TYPES OF CYBER CRIME

As discussed earlier that cyber crime is special from the conventional crime. Same as predictable crime, cyber crime also constitutes of lots of types. Some of the types of cyber crime as shown in following figure, the cyber crime evolve with the design of new technique itself.



8. CONCLUSION

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

References

[1] Majesty, H., Cyber Crime Strategy, S.O.S.F.T.H. Department, Editor. 2010.
[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] www.uncjin.org/Documents/EighthCongress.html.
[5] Roshan, N., What is cyber Crime. Asian School of Cyber Law.
[6] 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.
[7] 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.