CYBER CRIMINALS: A PSYCHOLOGICAL STUDY

Deepika Joshi, Pallavi Gautam and Sundeep Rohilla

Ms Deepika Joshi *and* ***Ms Pallavi Gautam*** *are Asst. Professors (Dept. of IT and Decision Sciences and Dept of OB and HRM respectively at Shiva Institute of Management Studies,, Ghaziabad.)*

Sundeep Rohilla *is Dean, Deptt of IT and Decision Sciences at Trinity College of Management & Technology, Ghaziabad*

Abstract

As we nurture our self with special knowledge and special talent in society, along with that power, comes accountability to use it for the good of that society. Now again the hairline between good & bad is blurred. 'Online Ethics' are the decent values one should follow while working on the net. Unethical tasks through Net may cause a big blunder for the society. Present Era having the outburst of net users, out of which there are few uncanny brains, who are not considered to work for the sake of society or for themselves rather they feel delighted by harming others. Although not having a face-to-face contact but still there may be lots of means to harm others through net. Apart from various known cyber crimes few of the unethical tasks, which may harm others, are Emotional Threatening, Identity Theft & Pedophiles etc. Online ethics in the extensive logic can be understood as that branch of applied ethics, which crams and evaluates such social and ethical impacts of Information Technology. This paper is based on study which helps in understanding the behavioral perspectives of cyber criminals. This paper deals with the various aspects of confrontation of online ethics & the efficacy of cyber law to bring in notice of online users about their online ethical responsibilities.

Ethics refers to a restraint dealing with what is good or bad. Although the two words can be differentiated by looking roughly but looking in the depth & then finding a difference is really a turbulent task. The online unethical task is not for all time a crime. There is an inherent connection between our way of thinking, awareness and the morals we do posses. The reason behind all online unethical tricks may possibly be that we have implemented lots of technical gizmos around us but don't know the standard approach of operating it. This paper uncovers the hairline among the conventional crimes & the Techno-Intellectual Crimes and also tries to get into the depth of reason behind the psyche of a cyber offender. Our Target audiences are Parents, Educators and children.

It is not practical to assume that only children are prone to be affected by poor habits. Although the poor habits can start at any age but yes, its true that because of lack of maturity and knowledge poor habits may target children first because a mature person can differentiate between ethical and unethical sides of behavior up to some extent whereas for the kids we as parents and teachers are responsible for teaching them ethical values and making them aware of the facts that the friendly technology may cause disasters for the society if used wrongly.

Living in a society is governed by some norms of social behavior accepted by all. Although living in a real society and in an e-society is entirely different as in real society we know our boundaries and the socially accepted behavior whereas in e-society boundaries are blurred and we are not aware of the fact that the things we are doing are accepted by the e-society or not.

Computer crime is different from usual crime, it is easy to commit, but tricky to detect and even harder to prove. Computer ethics is a branch of realistic philosophy, which deals with how computing professional should formulate judgments about professional and social conduct.

With the gigantic expansion of the Internet, privacy concerns as well as anxieties about computing expertise such as spy ware and web browser cookies have caused to define ethical behavior in technology.

"Oh what a tangled web we weave, when first we practice to deceive" : ***Sir Walter Scott***

LITERATURE REVIEW

Traditional Theories Behind The Crimes

The foundation for the examination is based on how well traditional psychological theories of crime and deviance explain this new behavior. In order to understand the criminal behavior of cyber criminals, it is necessary to examine the traditional psychological theories of criminal behavior and how they may be applied to develop an understanding of cyber crimes.

Social Process Theory: Social Influences

This theory says that criminal behavior is a function of a socialization process. This incorporated the socio-psychological communication by the criminal with society and collective group.

The main support of this theory stems from the effect of the family on youths who engage in delinquent or violent behaviors. Researcher think there is a linkage between childhood experiences of violence and behavioral problems.

Social Structure Theory: Rundown

Social Structure theories link individual criminal behavior to social class and structural conditions like poverty, unemployment, and poor education. According to social structure theorists, crime is located mainly in lower income classes.(Criminal Justice by Joel Samaha, 7th Edition).

Trait Theory: Basic Nature

Focal point of Trait theory is the sight that criminals have physical or intellectual qualities to differentiate them from abnormal.

The traits may be Genetic as inherited aggressive predisposition, inherited conditions associated with crime such as impulsive personality or Evolutionary Aggression evolved over time.

Rational Choice Theory: Willingness

These offenders are rational in the wisdom that, agreed on a set of morals and viewpoint, they determine the comparative overheads and payback of different available events and, from these reckoning, make a selection to exploit their predictable convenience. Rational choice model believes that the variety of substitutes open to criminals is constrained by the atmosphere or by association within which they make their judgment. Rational Criminals do definitely gain knowledge of methods that facilitates them avoid exposure, i.e., defense measures that should be taken; such as how to pose normal, how to hide things etc.

Social Conflict Theory: Societal Forces

Conflict theory believes that the basic

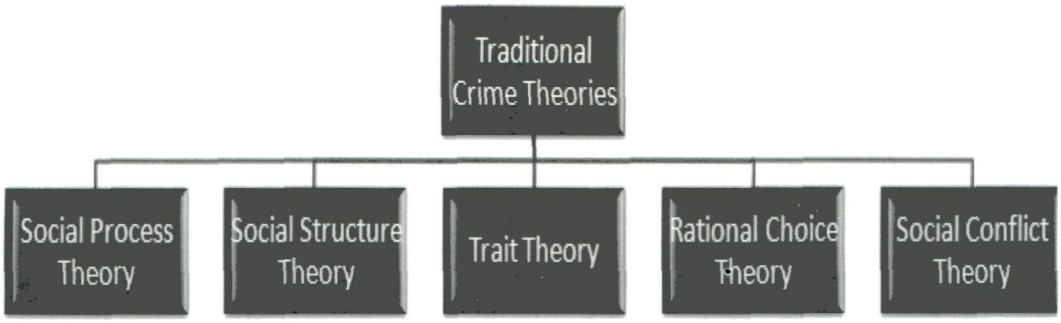

Figure 1 *Source: Criminology: The Core by Larry J. Siegel (Author)*

grounds of crime are the societal and financial forces working contained by people.People belonging to the BPL (Below Poverty Line) cadre try to pull up themselves to the middle segment and middle segment tries to find a pathway towards Upper Segment by increasing their earnings within short span of time. Force of earning more and more money eggs on the taste for crime.

Cyber Criminals Profile

Kids (age group 9-16 etc.)

Although strange to believe but it's true that the most layperson hackers and cyber offenders are youngsters. Those, having little awareness about what emerge to be a lot concerning computer, it is a matter of contentment to have hacked into a computer system or a website. There is also that small anxiety of emerging actually remarkable among friends. These unripe mutineers may also commit cyber crimes without really knowing that something wrong is going to take place out of their deeds.

Organized Hacktivists

These are hackers with a specific motive. Motives will differ significantly and may include monetary gain, nasty harm (e.g. website damage, contradiction of service, spreading viruses and worms), or stealing of network resources such as bandwidth usage, for individual use. In other cases the reason can be that a person influences society to change, or a person sharing his religious feeling and hence motivating people for a religion change. The attacks on approximately 200 prominent Indian websites by a group of hackers known as Pakistani Cyber Warriors are a good example of political hacktivists at work.

Annoyed Employees

No one can believe that a discontented employee can be too hurtful. Before the emergence of technology they were having the opportunity of lockouts and strikes against their bosses but after the computers and the automation of processes has got independence, it has become easier for them to do more harmful for their employers by committing computer related crimes.

Professional Hackers (corporate Espionage)

Due to the All-embracing computerization of processes, business organizations are accumulating all their data & information in

electronic form. Hackers are being employed by the competitors for stealing business secrets and other information that could be beneficial to them. The lure to use skilled hackers for trade spying also trunks from the fact that physical presence required to get access to important documents is turns into useless if hacking can retrieve those.

Criminal Individuals And Organized Crime Rings

Look for financial gain. As more and more financial transactions are carried out online, there are many latent sources of funds. Moreover, there are many ways of hiding identity on the Internet, allowing criminals to act in secret.

Terrorists

Having aspiration to harm or smash up a target as a means of getting a wider and more varied spectator. Cyber bombing is an intentional and/or organized assault on vital information, activities or infrastructure, including organizational networks

Expanded Horizon Of Cyber Crime

International Perspective

To gain an advantage over competitors, many Govt./ Private organizations are hiring ex-military and government agents trained in the art of intelligence gathering techniques, according to a report from the SANS Institute, a Washington-based cyber security training organization.

These individuals are used to head new company divisions whose mission is to spy on competitors and obtain intelligence. *As per the online resource* ***www.isn.ethz.ch/isn/Current-Affairs/Security.../Detail/?id...,*** *Companies spend over US$2 billion annually to gather competitive intelligence, according to the Society of Competitive Intelligence Professionals.*

National Perspective

Cyber Crime in the context of national security may involve Hacktivism (online activity intended to influence policy) nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, virtual sabotage, and software development, traditional Espionage-Espionage or spying involves an individual obtaining information that is measured undisclosed or top secret without the consent of the information holder, or Information fighting which talks about utilization and management of information in getting a competitive advantage over an rival. Information rivalry may engage assortment of strategic information and related activities.

Social Perspective

Cyber Crimes in context of Social Perspective may involve the anti-social blogging or the community sites of the groups misguiding the people or motivating their delinquent behavior for the harm of society. Suppose if there is a community site *where you can make friends and share your* views with, then your information on that site is not safe and may harm you as well as the value system of the society. Identity theft can be considered as one such crime.

Individual Perspective

Individual's interaction, Interdependence and influence among persons affect the individual behaviors and thoughts. In Individual context a mail from unknown source, chaining of mails, abuse mails & Links to pornography sites are most common examples. Although for the person who is web savvy and aware of all these trends of technology there is nothing new in such mails but for the people who are new to the technology and having limited or no knowledge about the terms may get misguided by these mails and unknowingly become the part of these cyber crimes.

New Cyber Crime Theories

Cyber Crime is different from the traditional crime, so are the cyber criminals. We can't compare cyber criminals with traditional criminals. Cyber criminals are highly equipped with the technological knowledge and have a higher IQ level. With a zeal to earn high in short span motivates them for committing cyber crimes. Survival is usually not a major issue adding to their zeal of committing crime. Few of the theories we have identified here tries to do the root cause analysis behind these techno crimes.

BMC Theory: Bulging Middle Class

The Roots of this theory lies in the traditional theory of Social Structure, where we use to say that people commit crime because they are poor but in present scenario the people from middle class are much more prone to the cyber crimes. As indicated in the figure there is an outburst of people entering in the middle segment of the society and competing for an opportunity to move towards the upper class. For attaining their goals they are earning money but you can earn money fast however it will not add to your knowledge as well as your maturity. Few of the reasons behind the middle class's temptation towards the cyber crime are:-

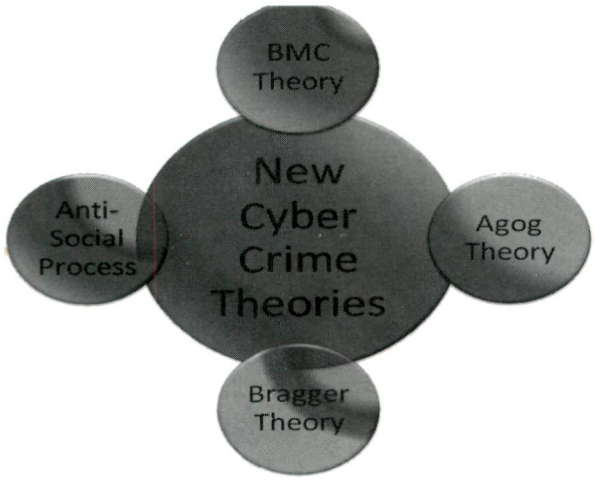

Figure 2 : *New cyber crime theories being introduces here*

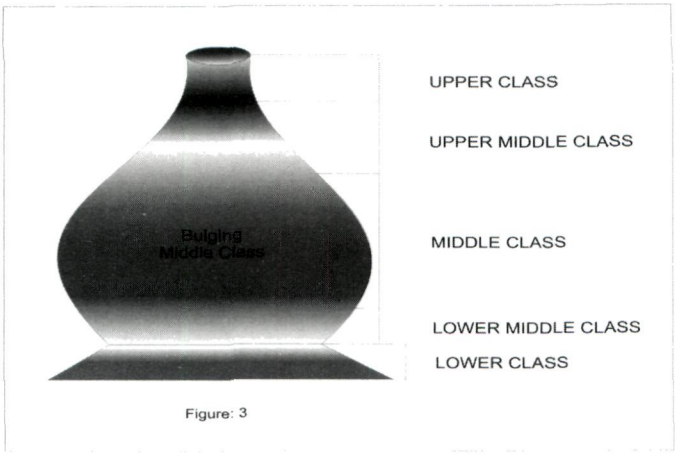

Figure: 3

High Competition For Earning High In Short Time Span

Everyone wants to earn more and more money that too within a short span of time. Humans thirst for money has no satisfaction level. As much as you earn this temptation gets increased. There are n number of players in the game of earning money, So the competition is also high. This endless desire of earning money motivates the humans to get into the mysterious world of cyber crimes. Online Financial Frauds are the simplest example.

Tech Community

Eminence of present globalized era is the backbone of technology. Emergence of latest technologies and their contribution in enhancing the knowledge base of a general user has given birth to the colossal mass of cyber criminals.

Anti-social Process Theory: *Because They Are Being Groomed To Commit the Crime*

This theory highlights the terrorist activities being supported by the technology today. New Techniques has not only given the opportunities to grow rather it has also opened the doors for destructive imaginations. Now-a-days people being targeted on the name of nation or the religion are being Technically/Intellectually equipped and are being groomed to be utilized for the anti-social activities. The more delinquent behavior they possess more they are prone to be utilized for such crimes.

Agog Theory: Curiosity Leads Them To Enjoyment

Curiosity leads the people towards the unknown result. If the results are favorable then the taste of small success kicks their blood and gives them enjoyment. Suppose if a student trying to access a file of **OB Paper** from the server and puts the name of OB Faculty as the password unknowingly he is hacking the password and this hit and trial approach motivates him to repeat the same again and again and the task initiated with a curiosity becomes the enjoyment tool.

Bragger Theory: Impression Making

Self Presentation is all about influencing others to perceive you as an impressive personality as we are always concerned

about our image in others view.

Making a powerful and unique presentation of oneself encourages him to do something different and adventures so that everyone gets attracted towards him. Hacking others password and showing it as a positive trait may change the perception of others and may make them much popular.

Conclusion

Although the traditional crime theory debates that the crime stimulating factors are the Choice, Social process, Heredity & Upbringing, Societal Forces & Mental Disorders but in the present Techno-Era the crime has also changed its articulation so the approach to study these Techno-Crime should differ from those of traditional approaches. Today criminals are much more educated, technically equipped with higher IQ and the targeted people to look upon as criminals (i.e. Poor people) in traditional theories have been overlapped by the Bulging Middle Class theory.

References:

1. ACM SIGCAS, Special Interest Group on Computers and Society, Association for Computing Machinery
2. Handbook of Social Psychology by John D Delameter
3. Criminology: The Core by Larry J. Siegel
4. Introduction to Psychology (7th Ed.) Clifford T. Morgan, Rechard A. King
5. www.legalservicesindia.com
6. www.apro.com.au/docs/BC3_Cybertraps.pdf
7. http://www.cybercrime.gov/
8. http://www.cybercitizenship.org/
9. www.oecd.org/sti/cultureofsecurity
10. http://www.ivf.com/stress.html