Cyber Crimes with Digital Technology

Mr. Naveen Kumar

(Research Scholar, HGU)

Introduction-

Digital technology has brought the real meaning of globalization in all over the world at large by encompassing it in all walks of life.

This technological emergence helped the peoples to communicate with their dear one, who lives world apart. With this expansion in the growth of technology the term ‘Cyber’ became more familiar to the people and this evolution of Information Technology (IT) gave birth to the cyber space.

With the evolution of cyberspace, it started to provide opportunities to all the people to get access any information or data storage with the use of internet facilities because the internet has become one of the greatest inventions in the field of communication.

It has been rightly said that the whole world has become a global village with the advent of internet. But this cyber system has been proved of having two sided effects, at the one side it provides opportunities to communicate and on the other side it is being used by the cyber criminals for exploiting others with the help of the Internet and other communications technology which are global in nature.

Today the misuse of the internet has been widely spreading for committing the crimes on cyberspace which are known as cyber crimes or computer related crimes or internet related crimes or e-crimes.

Cyber Crimes are nothing but crimes of the real world perpetuated in the medium of computer and hence there is no difference in defining a crime in cyber world and real world. Only the medium of crime is different.

Cyber crime is "international" or "transnational" there are ‘no cyber-borders between countries'. Computer crime, cyber crime, e-crime, hi-tech crime or electronic crimes are generally refers to criminal activity on the cyberspace where a computer or network is used as a tool or target or as incidental to crime.

Cyber crime, and cyber attacks or remotely controlled attacks affect our daily lives hence no government, public and private sector can afford to ignore. E-crime observably requires that the cyberspace be regulated in order to achieve independent, in depth analysis of the phenomena and of course accomplish cyber justice and deterrence.

It is increasing day- by day due to the lack of internationally harmonized legislation, penalty, increasing knowledge and expertise of cyber criminals, the lagging behind of the law enforcement agencies, judiciary, legislators, prosecutors, academia etc. and specially due to the failure of victims to report such crime incidents seriously.

Objectives:

The aim or purpose for study of Cyber Crime which we want to search into a problem for collecting relevant information and data. To identify problem is that which gives us the power and energy to solve that because it has been rightly said that every problem has in it the seeds of its own solution. The objectives of this research work are to explain all the important facet of the cyber crimes comprehensively at national and international level. The main objectives of the present study are discussed as following:

a) to trace the history and background of the origin of cyber crimes.

b) Lack of comprehensive cyber legislation to tackle the cyber crimes.

c) Lack of proper implementation of existing cyber laws both at national and International level.

d) Lack of awareness among general public and the law enforcement agencies both at national and international level.

e) Lack of three important elements for combating cybercrimes namely; identification, classification and the effective counter-measures.

f) Lack of the universal legal framework which should be adopted globally, backed by specialised and fully equipped law enforcement mechanisms and appropriate awareness among masses.

g) Lack of sufficient cyber laws on the issue of jurisdiction at national level.

h) Lack of co-ordination between three main components namely; law enforcement, adjudication and correction leads to an insufficient utilization of resources and retards the process of justice and also these are frequently operate in a disorganized manner with little knowledge of what the other segments are doing.

i) Lack of cyber courts and proper technical training to investigating officers, prosecutors, judges and advocates both at national and international level.

j) Lack of multi-threat security systems and adoption of foolproof computer procedures in organizations both at national and international level.

Comparative Study of Cyber Crime

The research design of this study is based on analytical and comparative approaches. In the present research work the researcher intends to determine whether any inadequacies or gaps exist in the cyber laws of India, United States of America (USA) and United Kingdom (UK) and also proposes to study the emergence of judicial trends in the interpretation of existing cyber laws. In the present research work, the relevant information is collected both from primary and secondary sources of law.

From the primary sources the researcher has mainly relied upon the cyber legislations of the countries i.e. India, United States of America and United Kingdom, decided case laws of the courts of India, USA and UK, Law Commissions Reports and all the possible information available on the official websites. From the secondary sources the researcher has also relied upon the text books on cyber law by eminent authors of these three countries as mentioned above, law dictionaries, legal journals, law reviews, magazines and newspapers and legal doctrines etc.

a) Review of related literature to know the work already done by others.

b) The analysis of case laws.

c) Further through comparative study the researcher intends to analyze the existing cyber laws of India, USA and UK in order to understand, explain and draw conclusion from it and also to critically analyze it to draw the inadequacies and to express opinion on rational basis.

Conclusion of comparative study

The present research work put its eye not only on the understanding of the concept of cyber crime but also explains the factors responsible for the emergence of these types of crime both at national level. The understanding of the factors responsible for cyber crimes in society will help to find out the sufficient means to stop these factors in future and to overcome the situation.

The way to overcome these crimes can be done through Comprehensive Cyber Laws, Education, Policy making, Technical training and Awareness. All the above ways to handle cyber crimes either are having very significant work. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber attacks.

It covers that all the wrongful and illegal activities on the cyber space by using internet or networks should be treated as crime and the prosecution of the offender must be sought.