

Evolution and Growth of Cyber Crimes: An Analysis on the Kerala Scenario

S S KARTHIK KUMAR

Research Scholar
Department of History
University of Kerala
sskarthikkumar.666@gmail.com
9895415366

Crime is a common word that we always hereof in this era of globalization. Crimes refer to any violation of law or the commission of an act forbidden by law. Crime and criminality have been associated with man since time immemorial.

Cyber crime is a new type of crime that occurs in these years of Science and Technology. There are a lot of definitions for cyber crime. It is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. In addition, cyber crime also includes traditional crimes that been conducted with the access of Internet. For example hate crimes, telemarketing Internet fraud, identity theft, and credit card account thefts. In simple word, cyber crime can be defined as any violence action that been conducted by using computer or other devices with the access of internet.

History of the Evolution of Cyber Crime

Back in the 1960s, the term “computer” would bring to mind images of large, bulky mainframes, machines whose inner workings were, for many, cloaked in mystery. Only select parts of our population had direct access to computers, building the mystical aura surrounding computers, what they did and the type of knowledge needed to operate them.

But With IBM’s introduction of its stand-alone “personal computer” in 1981, some of the layers of mystery about computers had been peeled away

exposing many of the rewards of quick data access and manipulation that, up to that time, had been realized by few. Today it is estimated that more than 53 million households have personal computers, over 50% of the nation's household, and that the demographics of owners are finally beginning to reflect the overall demographics of the general population.

The process of criminalization of human behaviour judged to be harmful to the public is typically one that builds slowly in common law jurisdictions. Momentum gained through problem identification and pressures exerted by special interest groups can easily span decades before undesirable actions are classified as "crime". In some instances, this process is accelerated through the occurrence of certain "catalyst events" that capture the attention of the public and the attention of lawmakers.¹

In the case of computer crime, legislators grew increasingly attentive in the 1980s as businesses became more dependent upon computerization and as catalyst event cases exposed significant vulnerabilities to computer crime violations. Cases like the Ian Murphy invasion of White House switchboards to hack into classified military files underscored the seriousness of computer crimes and, thus, helped speed along the enactment of the Computer Fraud and Abuse Act of 1986 to replace laws that proved to be inadequate in addressing computer crime.

In 1996, the Economic Espionage Act of 1996 was signed into law to, in large part stunt the affect that the incredible growth of the Internet was having on the frequency of theft and destruction of trade secrets.²

In India, Cyber laws are contained in the Information Technology Act 2000, which address computers and computer-related aspects in the category of crimes by means of computers and crimes against computers.

Recent global cyber crime incidents have heightened fears, and the Intelligence agencies are preparing against coordinated cyber attacks that could

disrupt rail and air traffic controls, electricity distribution networks, stock markets, banking and insurance systems etc.

In India, the amount of people using computers have grown tremendously, by the last few years, now a P.C,³ is a very common sight in almost every home, and even if there isn't one at home the residents are subjected to its use elsewhere, cafes, libraries etc, to check on different factors in their lives, that which the electronic media is being a big part of, like Registering Exams, Bank payments, Bill payments etc..., all of which have been made online.

These advances have made every day life easier to the public, and at the same time expose them to the ever changing and adapting world of Cyber crime, and by the years go by more and more people are falling, and being trapped in this world of Tech-crimes, this can be better understood by analyzing the Statistical data which provides details regarding the crimes committed, the types of crimes committed, and the number of people falling victim to these crimes.

As of late 2010, Kerala had been ranked the top position for cyber crimes in India by NCRB,⁴ (National Crimes Records Bureau). It has to be said that education is the reason behind this rise in crimes reported, as people are being more aware and conscious to be able to report crimes as they identify them. And as there is an increase in the reporting of crimes, more cases are being registered and justice brought to the victims, as more cases are being registered, Kerala stands on the top positions in the NCRB charts, as the total registered crime is the main criteria behind NCRB ratings.

Unfortunately, it is not possible to calculate the true social and financial impact of cyber crime. This is because most crimes go unreported. As most people are ashamed for their personal reasons, and in the case of any Businesses, they would refrain from reporting as it would hamper their business credibility. And so, it is impossible to gather data and statistics that

could give a clear picture of the overall Socio-Economic impact of these Cyber crimes.

CAUSES FOR INCREASING CYBER CRIMES IN KERALA

It is the socio-cultural Economic Standard, which provides the basis for deciding whether individual behaviours come under the category of conformity or deviance. Increasing importance has been given to Socio-Cultural Economic factors in criminal behaviour. Thus the concept of conflict, which has been a form of interaction by the formal school of sociology, has been used by several sociologists for applying differential crime rates in given communities.

As there is little disagreement, to the importance of Socio-Cultural factors behind Criminal behaviour, what is attempted here, is to examine the Socio-Economic conflicts of Cyber crime, as it is understood that the concept of Conventional Crime and Cyber crime is the same and they only differ in the mode of execution.

Literacy, Education and Cyber crime

The literacy rate of Kerala in the year 2001 was 90.86%, which gives strength to the fact as Kerala as a highly literate state. And in the case of cyber crimes being reported for the year, there is no data available with regards to that as the concept of cyber crimes was newly introduced to the judicial system via the IT Act of 2000.

In the year 2011 the literacy rate in Kerala was given as 93.91%. At the same time the cyber crimes cases reported in Kerala was totalling to 245. And in the reports by NCRB in 2012 shows a total of 312 cyber crime cases being reported in Kerala. This may not indicate a direct relation that literate people are committing more crimes, but the awareness and attitude towards crime is changing. People are more aware of crime and what facilities are made for the

protection from crime. Through the influence of literacy most of the crimes are being reported.

And the educated unemployed in Kerala should help the growth of cyber crime, as they have the necessary tool that is needed to commit a cyber crime, as they possess Education, of the normal kind, and of computer education. In 2008, the total percentage of engineering graduates, diploma and ITI holders, is 97.5% of the total percentage of professional and technical work seekers in Kerala, and the number of cyber crime cases registered in Kerala was a total of 67. In 2010, when the total percentage was 98.1%, the cyber crime cases registered was 156. And in 2012, when the total percentage is 97.1%, the registered crime is 312.

Here even though data regarding all professional and technical work seekers are given, only Engineering graduates and diploma holders along with ITI certificate holders are given importance in the relative study with Cyber crime cases registered in the state, as these educated unemployed, possess higher cyber knowledge which can be used in committing cyber crimes.

Although inconclusive, we can never prove that these work seekers who have knowledge of technology and the capability to commit cyber crimes actually does these crimes. As here it can only be imagined that the possession of knowledge and the denial of employment, along with economic reasons can or might make some or a few of these educated persons commit to the road of cyber crime, even though one can never prove this true.

CONCLUSION

Statistics produced by the SCRB shows that in 2002, just 2 years after the Indian IT act was passed, Kerala reported 4 registered cases, and from that 2 arrests were made, and the following years cases reported had grown but cases registered had shrunk. As in 2008, when special amendments were made to the IT act, the year saw 67 cases being registered and 32 arrests made under IT act.

From 2008 onwards the number of cases registered in the state have grown tremendously, in 2010 the total registered case comes to 156 and 109 arrests were made. By 2012 the total registered case is 312 and 175 arrests were made. From this we can clearly see that the cyber crimes in the state have risen dramatically during recent years.

We may say that there are many inherent factors that attract and facilitate their activities in the cyber space. Sometimes for money and sometimes for fun, but the criminals are bound to be attracted towards the cyber world. Cyber criminals have no dearth of motivation for committing crimes. The advantage of anonymity is the most advantageous among them. The motivational factors in cyber world are similar to that of traditional world of crimes. They could be greed, lust, power, revenge, adventure and desire to taste the forbidden fruit.⁵ Unlike perpetrators of a traditional crime, the greed of money or similar monetary lust may not always be a factor of motivation. The motive in cyber world may be malice, mischief or revenge and fun also.

Through the statistics available it's possible to know that these cyber crime cases that are present in the society are not going to reduce or stop growing, but only increase, and only in an ever faster pace. We can never know for sure what the cause for the rise in these specific crimes in state is due to, even through a generalized study on the cause for the increase in cyber crimes. As the cases that are being registered in the state, put forward the accused that are of different age groups and of different social and economic background. And this diversity can help understand that the normal generalization on the cause for increase of this crime cannot be put forward. And by words of N. Vinayakumaran Nair, Assistant Commissioner of Police, State Hi-Tech Cell, it is lack of awareness of the law and the provisions put in place in the judiciary that makes people continue to misuse the internet, which result in more cases being reported and registered.

Notes and References

- 1 Abraham D. Sofaer, Seymour E, “*The Transnational Dimension of Cyber Crime Terrorism*”, 2001, p.67
- 2 *Jones Telecommunications & Multimedia Encyclopedia*, Computer Fraud,
Available at www.digitalcentury.com/encyclo/update/comfraud.html
- 3 Personal Computer
- 4 National Crimes Records Bureau
- 5 S.L Kataev, *Criminalistic and Social Aspects: Cyber Criminality*;
<http://www.crime-researchorg./eng/library/kataev-1-eng.htm>