International Journal of Law
ISSN: 2455-2194
www.lawresearchjournal.com
Volume 2; Issue 1; January 2016; Page No. 27-29

Cyber Crimes: A review

Dr. A Guravaiah

Ph. D., Senior Faculty in Law, Andhra Christian College of Law, Guntur, Andhra Pradesh, India.

Abstract
The growth of cyber space has resulted in the development of a new and specialized branch of Law called cyber laws, laws of internet and World Wide Web cyber criminals constitute of various groups (or) categories as against individuals against organizations and against society. Unfortunately our cybercrime police stations have not been able to come up to the expectations of the public due to take of awareness of the subject. Many times the police have refused to cases and often made the complaint run from pillar to post to even lodge a complaint so in this circumstances the Govt. stepping up the ante to address the growing threat of cybercrime in the country. The Govt. is expected to have its own resource to take protective measures, the common man when affected would run to the cybercrime police stations for relief. This realization that there is a security threat to the country's armed forces has already been recognized by my other countries in world.

Keywords: What are cybercrimes, categories of cybercrimes cybercrimes in India, preventive measures of cybercrimes

Introduction

Cyberlaw is a new phenomenon having emerged much after the onset of Internet. Internet grew in a completely unplanned and unregulated manner. Even the inventors of Internet could not have really anticipated the scope and far reaching consequences of cyberspace. Internet is growing rapidly and with the population of Internet doubling roughly every 100 days, Cyberspace is becoming the new preferred environment of the world.

With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. The growth of Cyberspace has resulted in the development of a new and specialized branch of law called Cyberlaws- Laws of the Internet and the World Wide Web.

There is no one exhaustive definition of the "Cyberlaw". However simply put, Cyberlaw is a term which refers to all the legal and regulatory aspects of internet and the World Wide Web. Anything concerned with or related to, or emanating from, any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyberlaw [1].

There is apparently no distinction between cyber and conventional crime. However on a deep introspection, there exists a fine line of demarcation between the conventional and cybercrime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cybercrime. The sine qua non for cybercrime is that there should be an involvement, at any stage, of the virtual cyber medium [2].

Hart in his work -"The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cybercrime.

The cyber criminals constitute of various groups/category which include children and adolescents between the age group of 6–18 years, organised hackers, Professional hackers/crackers and discontented employees. The cybercrime can be committed through any electronic device.

The cybercrime may be broadly divided against three groups:

1. **against individuals**
   a. Harassment via e mails
   b. Hacking
   c. Dissemination of obscene material
   d. Defamation
   e. Transmitting virus
   f. Unauthorized control over computer systems

2. **against organizations**
   a. Hacking
   b. Pirating software
   c. Cyber terrorism against Government organization

3. **against society**
   a. Pornography
   b. Polluting the society especially, youth through obscene and pornographic material
   c. Cyber trafficking

Holocene epoch of cybercrimes in India

India is celebrating 60 years of Independence. At this point of time it is natural for us to focus on the security of the nation. In the current Digital era where "Governance" as well as "Business" is increasingly being led, the discussion on security of the nation is not complete without a discussion of the Cyber Space in which e-Governance and e-Commerce take place.

Cybercrime is now a bigger threat to India Inc than physical crime. In a recent survey by IBM[3], a greater number of companies (44%) listed cybercrime as a bigger threat to their profitability than physical crime (31%). The cost of cybercrime stems primarily from loss of revenue, loss of market capitalization, damage to the brand, and loss of customers, in that order. About 67% local Chief Information

Officers (CIOs) who took part in the survey perceived cybercrime as more costly, compared to the global benchmark of 50%.

Of late, both manufacturing and service sector has undergone a rapid changes followed by a series of fundamental developments. Most noteworthy among them is the rapid development and advancement in Information Technology as well as communication system. This has changed the concept of online activities, and has been instrumental behind broadening the dissemination of financial information along with lowering the cost of many financial activities. Information Technology and communication networking systems have revolutionized the functioning of all sectors. Even though the situation prevails, today there is a threat namely crimes through networking and communication devices. Increase in hi-tech crime "Cybercrime has been on rise, no doubt and it is fuelled in large part by an increase in software security flaws and in the number of home computers being used against their owners' wishes to distribute spam, spyware and viruses.

Bangalore India‘s cyber woes claim fifth spot in a worldwide ranking of countries afflicted with cybercrime, claims a report by the Security and Defence Agendas (SDA) and MacAfee. The report, “Cyber Security”, the Vexed Question of Global Rules, states that premium on Internet privacy in the country is quite low. The report also states that India is well aware that cyber affects the reputation of the country which does business with foreign investors who invest heavily in cyber security. It furthers raises a grave issue of lack of single operator to effectively control Internet, telecom and power sectors [4].

Our attention is usually drawn on “Cyber Security” when we hear about “Cyber Crimes”. Our first thought on “National Cyber Security” therefore starts on how good is our infrastructure for handling “Cyber Crimes”. In the corporate sector, the focus of “Cyber Security” is more on “Information Security” and prevention of unauthorized access to the Corporate Information systems or denial of access to the systems by authorized persons. The e-Governance and e-Commerce sector as well as the Individuals who use Computers and Mobiles are also concerned about Cyber Crimes and how it affects them.

Retrospective view on infraction of Cyber Security

If we reflect on some of the recent incidents of Cyber Security breaches, we can get an idea about how the security threats arise.

An incident which was of significance was the report by a recent Symantec survey which revealed that firms in the Indian Financial services industry lost heavily in 2010 due to phishing attempts, theft of proprietary information and denial of service attacks [5].

Another incident of importance to occur recently was the dramatic demonstration of the power of SMS/Phone spoofing through websites. In a well published TV programme, a Chartered Accountant from Ahmadabad showed how he could put through a call in the name of the home minister of the country to another minister. A third incident of significance was the fact that the web server of National Police Academy, Hyderabad was found to have been penetrated and a phishing website had been hosted there on [6].

These incidents indicate the high levels of risks that Indian Cyber Space is encountering today. They also highlight the fact that the security professionals in the various organizations that have been attacked have failed in securing their networks and exposed the country to grave risks.

Causes to be perceived

Unfortunately, our Cyber Crime police stations have not been able to come up to the expectations of the public due to lack of awareness of the subject. Many times, the Police have refused to register cases and often made the complainant run from pillar to post to even lodge a complaint. The confusion arises since some Cyber Crime Police stations do not recognize any crime coming under IPC as Cyber Crimes even if they have been committed with the use of Cyber tools. They are under the false impression that they exist only to take care of offences under Information technology act alone. Public are therefore losing faith in the Law enforcement‘s ability to protect Cyber space.

In the few cases where Cyber Crime cases have been initiated, lack of coordination between different Police stations has frustrated the investigation. In some cases when the investigation trail goes abroad, CBI is not coming forth with its own support and the investigations reach a dead trail. When Cyber Crimes are committed with mobile network, it is often difficult to convince the mobile service providers that they are responsible for assisting the Police in the investigation. Many of them do not even recognize mobile crimes as Cyber Crimes and therefore fail to appreciate their legal obligations. In the private sector, whenever crimes are reported, companies are more concerned about their own reputation than public good and they do everything within their powers not to register a complaint nor enable a proper investigation.

Conclusion

Guarding and protecting the cyber arena is the biggest and immediate challenge IT gurus are faced with. Government is also stepping up the ante, to address the growing threat of cybercrime in the country. While the Government is expected to have its own resources to take protective measures, the common man when affected would run to the Cyber Crime Police stations for relief. This realization that there is a security threat to the country‘s armed forces has already been recognized by many other countries. In developing countries like India, it is the need of hour for the lawyers to understand the depth of cybercrimes and thus to defend in the court of law thereby allowing corporate sectors to set up their own cyber lawyers. To accomplish this, appropriate measures have to be taken to increase the awareness of the nature of such crimes among the novice in the field of law which can be done by distinguishing Cybercrimes as a separate entity. Hence, it is the time to fortify Cybercrimes Police stations and Cyber Courts in all districts and state capitals in the country in order to solve the baffling threat of Cyber Crimes.

References

1. www.Cyberlaw India.com. Downloaded on 9th August 2012.
2. Kumar Vinod. Conventional and cybercrimes.
3. IBM survey on cybercrimes. Featured articles on CIOs. The Economic Times 2009.
4. Brigid Grauman. Cyber-security: the vexed question of global rules-an independent report 2012.

5. Symantec security check report. Information Week News Network, 2011.
6. John Leydon. Indian police academy hosts a phishing site. Enterprise Security 2007.