Heterogeneous Framework for Indian Cybercrime Cases

Ravikumar S. Patel¹ and Dhaval Kathiriya²

¹Mewar University, Chittorgarh, Rajasthan.
²Information Technology, Anand Agriculture University, Anand 388 110, Gujarat-India.

ABSTRACT

The internet has served as the global language of the virtual world since the beginning of the digital world and the Internet in India is increasing rapidly. Internet served seriously in many more areas in current scenario like Trade, education, sports, and research. Internet is treated as coin because it having two sides merits and demerits. A major problem of internet in current scenario is “Cyber Crime”. Here we study and analysis about the current cyber crimes in India through the literature survey, government annual reports, verbal communication with ethical hackers and many more techniques like Questionnaires and from the head of cyber cell from different states in India. We also study and analysis the different cyber crimes case studies which is occurred in different states in India and Indian cyber laws framework is compared with other country framework. So, finally we conclude that, our cyber laws frameworks having some of the vulnerabilities and problems for executing cyber cases compare to other countries. So we propose a heterogeneous approach or model for executing our legal framework smoothly against the cybercrimes in current scenario.

Introduction

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation.[1] Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence, the need for Cyber laws in India. [6]

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. [4] Initially it may seem that Cyber laws are a very technical field and that it does not have any bearing to most activities in Cyberspace.[5] But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. [12]

Cyber law 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. [9] The growth rate of cyberspace has been enormous. 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. [7]

With the spontaneous and almost phenomenal growth of cyberspace, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the absolutely complex and newly emerging legal issues relating to cyberspace, cyber law or the law of Internet came into being. The growth of Cyberspace has resulted in the development of a new and highly specialized branch of law called cyber laws of World Wide Web. [11]

Objectives of the research:

Here, Below We are defines the Objectives of our Research.

A main objective of my research is providing a heterogeneous model means one types of procedures to handle the various cybercrimes in current scenario. In a current scenario Information technology domain grow very high so, we need effective cyber laws in this era. Here below specify the objectives of my research.

<table>
<thead>
<tr>
<th>YEARS</th>
<th>TOTAL CYBER CRIME</th>
<th>PERSON ARRESTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>217</td>
<td>154</td>
</tr>
<tr>
<td>2008</td>
<td>267</td>
<td>178</td>
</tr>
<tr>
<td>2009</td>
<td>411</td>
<td>284</td>
</tr>
<tr>
<td>2010</td>
<td>922</td>
<td>772</td>
</tr>
<tr>
<td>2011</td>
<td>1725</td>
<td>1161</td>
</tr>
</tbody>
</table>

1. Aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.
2. Main objective of our research is providing the legal infrastructure for E-commerce in India.
3. Provides the legal recognition of electronic documents.
4. Acceptability of electronics data or evidence in a court of law.
5. Legal acceptance of digital signatures.
6. Punishment for cyber frauds and crimes.
7. Establishment of cyber regulation advisory committee and the cyber regulation tribunal.
8. Provide the facility of electronic filing maintenance of electronic records.
9. Development of model for security against the different types of cybercrime activities.
10. To develop propose heterogeneous model for the solution of Indian cyber laws infrastructure in current scenario.
Proposed Framework:

Poor information security reduces the competitiveness of nations. Outdated laws and regulation, and enforcement mechanisms for protecting networked information, create an inhospitable environment in which to conduct E-business within a country and across national boundaries. Thirty three of the countries surveyed have not yet updated their laws to address any type of cyber crime. Of the remaining countries nine have enacted legislation to address five or fewer types of cyber crime and have updated their laws to prosecute against six or more of the ten types of cyber crime. India is not updated cyber laws for data interception and computer forgery. [7]

Cyber Law is different from other National Laws. While other National Laws are usually “Territorial” in nature and covers territorial acts or omissions yet Cyber Law governs act or omissions that travel far beyond the national territory. [11] For instance a Cyber Crime may be committed in country X by using computers located at country Y by a resident of country Z. This “International” nature of Cyber Crimes makes it unique and it also requires a “unique treatment”. Here lies the real problem. Cyber Law is essentially “International” in nature whereas its dealings all over the World are “National” in nature. [7] Without “International Cooperation” the National Cyber laws are useless. This brings the importance of an International Cyber Law Treaty of Convention that can provide a “Harmonized Framework” for Cyber Law across the globe. [10] Till now we do not have a “Universally Acceptable” International Cyber Law Treaty or Convention. Even the World community on Human Rights, Cyber Law and Cyber Security must start thinking in this direction as issues like Cyber Warfare, Cyber Terrorism, Cyber Espionage, Cyber Crimes, E-Surveillance, Unlawful Interceptions, etc are “Transnational” in nature. If different Countries would have different laws for these issues, it would be very difficult to truly enforce protective provisions against these menaces at National and International levels. It is high time for UN to seriously consider issues like International Cyber Law Treaty and protection of Human Rights in Cyberspace. [4]

**Case Studies:**

Online cyber criminal markets are putting very sophisticated attack tools into the hands of more low-level attackers, say cyber intelligence specialists.[1] More attackers are now getting their hands on tools like Zeus and SpyEye, according to the cyber intelligence team at the Online threats managed services (OTMS) group of RSA, the security division of EMC.[12] Cyber criminals targeted users of Skype, Face book and Windows using multiple Black holes exploits in October, according to the latest threat report from security firm GFI Software. Researchers uncovered a large number of Black hole exploits disguised as Windows licenses, account verification emails, Skype voicemail notifications and spam messages.[6]

Cross-site scripting (XSS) attacks remain the top threat to web applications, databases and websites, an analysis of 15 million cyber attacks in the third quarter of 2012 revealed. Other top attack techniques are directory traversals, SQL injections (SQLi), and cross-site request forgery (CSRF), according to a web application attack report by cloud hosting firm Fire Host.[1]
Conclusion:
Cyber crime is a very crucial problem in all over the world. Day by day this problem increased and harmful to all countries. Every year millions dollars property hacked by intelligent hackers. And we have only the single weapons for restrict these types of issues and that is cyber laws. Cyber law and cyber space framework are playing important role for restricting the cybercrime every year. Cyber crime is a global problem for all over the world. So, for solving these types’ problems via some proper method and architecture. Because we required some necessary help for different resources like cyber security agencies, police, cyber cell, Interpol, international laws, Indian laws, ISP providers and many more things. So we need some proper format for solving these types of cyber crime in current scenario. So, here we represent one proposed model for solving cybercrimes.

References:
[2]. Ajeet Singh Poonia,” Ethical values and practices for Cyber Society” 978-1-444-5757-12009 IEEE
[4]. Apurba Kumar Roy,” Role of Cyber Law and its Usefulness in Indian IT Industry” 1st Int’l Conf. on Recent Advances in Information Technology 978-1-4577-0697-4/12 2012 IEEE
[5]. S. Aggarwal, ”Evidence Handling in Proactive Cyber stalking Investigations: The PAPA Approach” Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE’05)
[7]. Information technology act 2000, Department of electronics and Information technology.
[12]. “Cyber crime scenario in India”, Dr.B.Muthukumaran, Chief Consultant, Gemini Communication Ltd