Cyber Laws: Issues and Legal Consequences

Manju Sharma
Assistant professor
National Institute of Technology, Kurukshetra, Haryana (INDIA),
manjusharmaknl@gmail.com

Abstract

Cybercrime, e-crime or Internet frauds etc. refer to the illegal activity where a single system or whole network is involved. Cybercrime is emerging as a profession these days, with the advancement of technology and the Internet being incognito in nature, has made possible for individuals with low technical expertise to make money illegally without leaving their homes. These threats are increasing every day, in fact the 2014 has witnessed some of the biggest attacks of all time and according to predictions the situation is about to worsen in the future. These increasing crimes give rise to the need of cyber laws and the concern of the government authorities. This paper gives an overview of the Cyber legislation of few countries alongwith their issues and legal consequences. Here the sufficiency and the extent to which these laws provide us protection is discussed. These laws are not able to keep pace with the rapidly changing cybercrime scenario.

Keywords: Cyber Space, Cyber Crime, Data theft, Identity theft, Hacking, System Intrusion.

1. Introduction

When Internet came into existence sany of its developers would barely have thought that someday it will become a ground for criminal activities and frauds. According to a report by McAfee predicting the threats in 2015, there will be a significant increase in the attacks during this year. The report stated that the target might be devices like webcams with weaker security. McAfee stated that threats like "ransomware" are also growing, these attacks block the data and compels the user to make payment for that data and compromises the operating systems of mobiles. The anonymous nature of the Internet also plays a major role in these criminal activities. Thus, arises the need of cyber laws. We can define Cyber laws as the description of legal aspects in accordance with the communication technology or the Cyber space i.e., "Internet". These laws are an effort to map the laws applicable in material world over the Internet world. Cyber laws concern everyone.

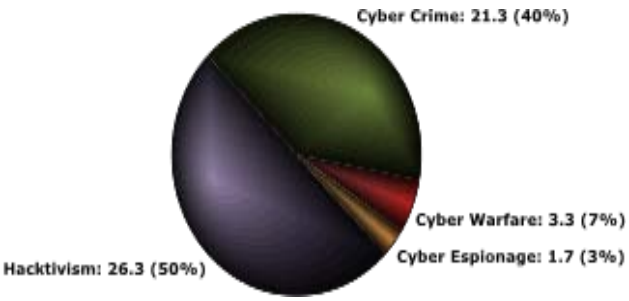

Figure 1 Major motivation behind cyber attack

The Internet having military and academic origins has now become an ultimate medium used in almost all aspects of our day to day tasks such as, social networks, online transactions etc., thus, every activity of an individual in the cyberspace has legal aspect [1].

2. Emerging cyber crime trends in recent years

Most recently in 2015, Facebook, Instagram and Tinder all went down at 5:15 pm for about an hour. Although, the officials were denying the possibility of any kind of attack saying that this occurred due to some configuration changes which were recovered very soon, the evidences contradict to this, fig. 2. shows a snapshot of the Internet traffic of that evening, which shows that large traffic coming from Asia and South America towards coast of US where most of the Facebook servers are located. A group called the Lizard Squad claimed to take the responsibility of the attack, and a day before this incident, this group claimed to have hacked the Malaysia Airlines system [2].

iCloud hacking was also a major scam of 2014, accounts of many celebrities were compromised. Another grand attack was Sony hacking. The hackers successfully compromised the network of the Hollywood movie studio, Sony Pictures and were successful in obtaining various confidential files, these files are now available at file sharing network and can be downloaded (these are mainly downloaded by journalists). This scam started a word war between North Korea and USA and initiated many political events [2].

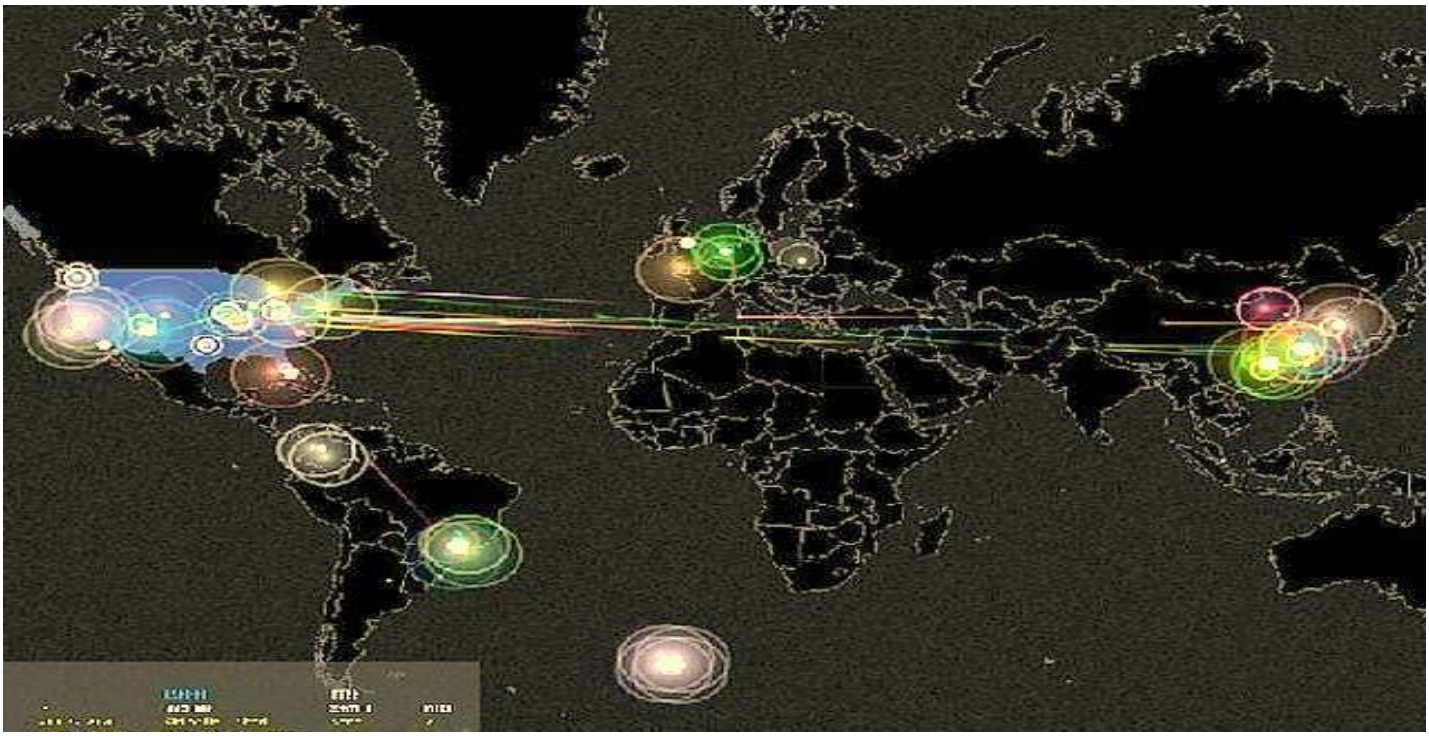

Figure 2 Traffic Activity to take down facebook [3]

The hacking of Gmail accounts which took place in Sept. 2014 compromised about 5 million user accounts, approx. 100,000 of which were loaded up on a Russian site. The eBay hacking incident in which hackers compromised accounts of employee at eBay, and got the contact information of about 233 million customers, caused eBay to request all its customers to change their passwords.

These attacks drew the concern of the government of various countries towards computer systems and networks. In the International Conference on Cyber law, Cybercrime & Cyber Security which was held in India in November 2014, featured some major challenges which affect the crossway of Cybercrime with Cyber laws and security and led to several recommendations for stakeholders. In 2014, it was once again witnessed that cyber laws all over the world are still lagging behind to deal with the emerging cyber crime trends [3].

In 2014, emergence of the dark web was marked and cybercrime emerged as an economy model in the dark web came into picture. During this year FBI was successful in closing down Silk Road 2.0 (Silk Road 1.0 was closed in 2013). It was shown that the current status of cyber laws and policies requires lot of amendments and strengthening or it will not be able to convict the cyber criminals [3,4].

3. Cyber laws in India

Incorporating Cyber laws aim to set some guidelines and patterns to control the transactions carried out on the web and categorize them as legal or illegal and punishable. The IT act of 2000 provides a legal structure all form of electronic information is validated and cannot surpass the legal effect.

3.1 Scope and Applicability

The scope and applicability of ITA-2000 was enhanced by an amendment passed in 2008. India is the 12country across the globe which has cyber legislation apart from countries like USA, Japan, Malaysia, Singapore etc. The ITA-2000 provides legal policies which provide a legal effect on information. From the point of view of Indian e-commerce many positive provision are provided by Indian cyber legislation. This act declared email as a legal mode of communication which can be demonstrated and verified in the court of law. Digital signatures were also given legal validity. Under the legislation corporates can now have required remedies in case of their systems or networks being compromised.

3.2 ITA 2000

The IT Act 2000 was passed to update the old laws and facilitates measures to handle cybercrimes in better way. A brief overview of the law is given below [5]:

Table 1: Cybercrimes and their legal actions

TYPES OF CRIME	LAW AND PUNISHMENT
Hacking	Imprisonment extended up to 3 years, or fine of 5 lacs or both.
Spreading malware, Email Spoofing	Cognizable and bailable with the permission of the court before prosecution and trail by any magistrate
Identity Theft	Imprisonment which can be extended up to 3 years, or fine up to 1 lacs or both.
Email Spoofing	Victim can file a complaint in the nearest police station. If crime is proved accused shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to the fine which may extend to one lakh rupees.
Pomography	For first conviction: imprisonment extendable up to 5 year and fine up to 10 lacs. For second conviction: imprisonment extendable up to 7 year and fine up to 10 lacs.

3.3 IT Amendment Bill 2008

The word 'communication devices' was added which covered cell phones or other devices which can be used to transmit any kind of text, audio, video etc. However, ITA- 2000 defined 'digital signature', but the description was not capable to cover all the aspects and thus the term 'Electronic signature' was defined in ITA-2008 as a legally valid mode of executing signatures which includes digital signatures, biometrics and other forms of electronic signatures. The term "hacking" used in Section 66 has been replaced by "data theft". The section deals with issues like sending of offensive texts, fake origins of messages, stealing of electronic signature and identity [6].

3.4 National Cyber Security Policy 2013

The Cyber Security policy of 2013 aimed to develop a secure cyberspace for the citizens, organization and Government. The primary objectives of this policy were [7]:

1. To develop a secure cyberspace that protects information and information infrastructure and builds trust in IT Sector.

2. To promote the security of the cyberspace globally by enhancing cooperation and to develop effective public private relations and partnerships through technical cooperation.

3. To form a workforce of about 500,000 skilled cyber security professionals in the next 5 years and improve the visibility and integrity of ICT products by establishing a body for validation and testing of such products.

4. To protect the information while in process, storage or transmission so as to protect the privacy of citizens and reducing economic losses

3.5 Issues not covered in ITA

Besides, several advantages provided by this Act, it is still not sufficient and has several loopholes, some of them are [4]:

1. The law does not mention anything regarding the Intellectual Property Rights, there are no policies and rights related to copyrighting, trade marking or patenting of electronic records, domain names holders.

2. There is no mention of any policies regarding the issue of payment gateways over the Internet.

3. The act provide the Deputy Superintendent of Police full investigation power for the cybercrime cases, thus the corporate organizations cannot escape the torment from the side of the DSP.

4. Cyber law in USA

In the United States, cyber laws are adopted at both state and national level. There are certain regulations regarding the distribution of authority between these two levels [8].

4.1 Scope and Applicability

In United States' cyber legislation the regulations refer to various types of cybercrimes. It is considered an offense to get unauthorized access to a government computer and get confidential information, causing damage to a computer by some malicious program or getting illegal access, to harm a system in order to get financial benefits etc. All the fifty states are free to have their own legislative authorities and there is no such rule that laws should be uniform or consistent. Some of enactments like, Restatements and the Model Penal code which are developed by private associations and were

presented to the states for adopting them so that legislation will be uniform.

5. Cyber law in Europe

The Council of Europe [9] was established in 1949 with an objective of strengthening human rights and democracy and promotes and upholds the rule of law in Europe. It has 43 members which comprises of all the states of the European unions.

5.1 Scope and Applicability

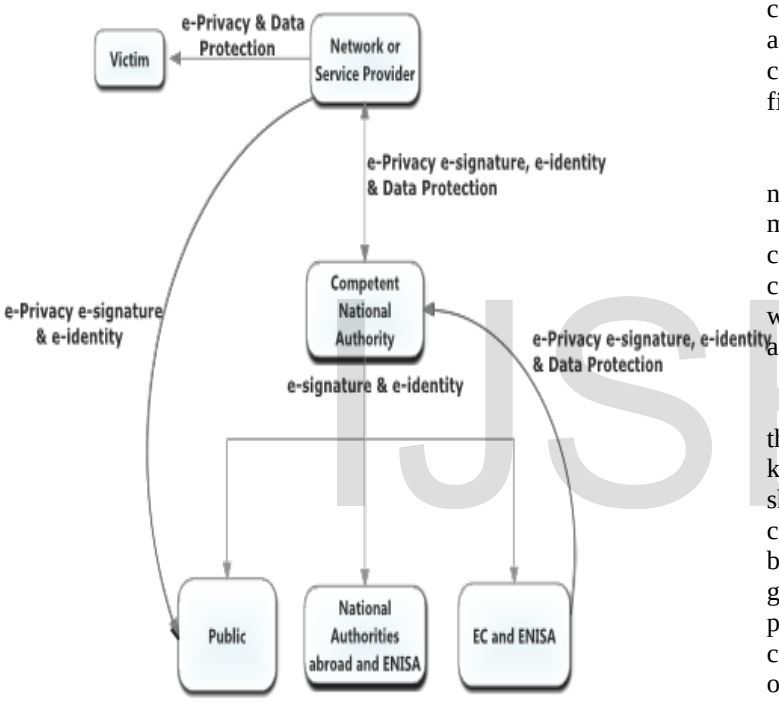

Figure3: The existing EU legislation incident reporting

6. Analysis, Results and Discussion

On relating the Indian law with the law of developed nations the proper requirement for the Indian law can be analyzed. Data are not of same need and importance; it varies from one another on the basis of utility. So we require creating separate categories of data having different importance values, as the U.S have. Moreover the provisions of IT Act basically deal with extraction of data, destruction of data, etc. Companies cannot get full protection of data through IT Acts which ultimately forced the private companies to enter into separate private contracts to secure their data. These contracts have the same applicability as the general contract. Despite the efforts being made for having a data protection law as a separate discipline, our legislature have left some lacuna in framing the bill of 2006. The bill has been drafted wholly on the structure of the UK Data Protection Act whereas today's requirement is of a comprehensive Act. Thus it can be suggested that a compiled drafting of a data protection bill based on US laws would be more favourable to today's requirements.

7. Conclusion

Cybercrimes circumscribe a variety of activities which likely to be illegal which includes spamming, harassment, child pornography, cyber stalking, phishing scams, denial-of-service attacks where the computer can be used as a target or tool or both. The governments around the globe are taking various actions to deal with cybercrimes, but the cyber law critics warn the governments of the consequences of over activism over the Internet. Some of the researchers have claimed that the government policies hinder in their efforts to find the vulnerabilities in the Internet infrastructure.

The technical root of cybercrimes such as computers, networks and Internet are same for all the countries which means that the nature of cybercrime is same in all the countries. This makes the international cooperation of the countries to deal with cybercrime necessary. Cyber laws deal with all the phases of e-commerce and transactions and every activity going on in the cyberspace have a legal perspective.

People are becoming more and more dependent on the Internet which means that criminal activities will also keep on increasing. The laws making bodies of the nation should always keep in mind the rate to development of the cybercrimes and the laws should be able to minimize them to best possible extent. Thus, it is the responsibility of the government and the law makers to make sure that every perspective and issues of cybercrime have been included in the cyber laws which will enable the consistent and lively growth of the laws.

REFERENCES

[1] Cyber Laws India.net , "Cyber laws in India", Available at: http://www.cyberlawsindia.net/cyber-india.html, Last accessed: April 2016.

[2] New.com, "Facebook, Tinder and Instagram all down", Available at: http://www.news.com.au/technology/online /facebook-tinder-and-instagram-all-down/story-fnjwnhzf 1227198626109 , Last accessed: April 2016.

[3] Business Standard, "Emerging Global cyber Law Trends 2014" Available at: http://www.business-standard.com/article/ technology/emerging-global-cyberlaw-trends-in-2014-115010500301_1.html, Last accessed: April 2016.

[4] Mondaq, "Cyberlaws: An Indian perspective", Available at: http://www.mondaq.com/india/x/257328/Data+Protection+Privacy/An+Overview+Of+Cyber+Laws+vs+Cyber+Crimes+In+Indian+Perspective , Last accessed: January, 2015.

[5] Information Security Awareness, “Cyber Laws of India”, Available at: infosecawareness.in/cyber-laws, Last accessed: April 2016.
[6] “The Information technology (Amendment) Bill 2008”, Government of India, December 2008.
[7] “National Cyber Security Policy-2013”, Ministry of Information and Communication Technology, July, 2013.
[8] S. W. Brenner, “State Cybercrime Legislation in the United States of America: A Survey”, Available at: http://jolt.richmond.edu/v7i3/article2.html, Last accessed: January, 2015.
[9] M. Dekker, C. Karsberg, B. Daskala, “Cyber incident reporting in EU”, European Network and Information security agency, August, 2012.