The Clarion Volume 6 Number 1 (2017) PP 51-56
The Clarion
International Multidisciplinary Journal
ISSN : 2277-1697

Cyber security and cyber laws in India : focus areas and issue areas.

Ujjal Pathak
Gauhati High Court, Guwahati, India

Abstract

The twin concepts of cyber security and cyber laws are fast becoming one of the most relevant areas of interestfor the Indian Government as well as the Indian public in general. In a country such as ours which is taking fledgling yet resolute steps towards digitisation of her economy, the concept of cyber security becomes important for two reasons. The first reason is the fact that India's physical infrastructure has a long way to go in terms of protecting and resisting cyber -attacks. The second reason is that for a majority of Indians the concept of digitisation, e-transactions etc. have begun to assume importance only very recently. Therefore in the interests of both the Nation as well as its people, the efforts towards creatinga foolproof cyber security web backed by an effective cyber law framework and improving them from time to time must be continuous in nature.

Keywords: Cyber security, Cyber laws, digitisation, e-transactions, cyber- attacks.

1. Introducation

Cyber security and cyber laws are best understood as being two sides of the same sword, acting as a weapon in order to defend against the menace of cyber-crime. Cyber security, which is also known by the term IT (Information Technology) security refers to the combination of software systems, protocols and even individuals that work to protect computer systems from damage or theft especially of the hardware, software or the information stored inside the computer system. Cyber security is becoming a part of every nation's security strategy because it serves to protect vulnerable sectors of a nation's economy such as financial and trading systems, aviation, energy sector, software sector, customer devices and so on. These can be targeted by enemy nations during wars in the form of large scale "cyber-attacks" thereby crippling the victim nation.

It is an obvious fact that many sectors of our nation's economy would come to a standstill if any cyber- attack did in fact take place. This is because of the ever increasing computerisation of most if not all sectors of our economy. This is where cyber security steps in. Its' importance is only expected to grow due to the permeation of internet and internet enabled devices as well as other forms of wireless networks in almost all levels of the society.

The other side to the concept of cyber security i.e. cyber law consists of two aspects, namely Information Technology law and Cyber law itself. Of the two, IT law is broader nature and includes laws governing the sale, manufacture and use of digitised information and software. In a broader sense it covers the legal aspects of the Information Technology realm. Cyber law, on the other hand is a narrower term which includes all the legal issues relating to the internet itself.

The twin concepts of cyber security and cyber laws work hand in hand to tackle the everpresent menace of cybercrime. Put simply, any criminal activity, the commission of which involves a computer or internet can be called as a cybercrime. The eventual target can be other individuals, other networks or other computer systems. There are cybercrimes of different types, too numerous infact. All of them have the ability

Corresponding author : ujjalpathak5@gmail.com
DOI number: 10.5958/2277-937X.2017.00008.9

to cause immense harm, with victims beginning from individual nations and ending at individual persons, subsequently causing immense hardships.

The virtual world has assumed great importance in today's lifestyle. Nations as well as their citizens are becoming more and more dependent on the internet for uncountable tasks. To use the internet requires the use of computers or other compatible devices which are vulnerable to different types of cyber- attacks. Therefore software development to ensure the security of such devices must be given a continuous push and at the same time; must be backed by a strong legal framework that acts as a deterrent against possible wrong doers.

The above paragraph represents an idealistic solution. However the picture is far from rosy in India. Despite significant improvements to the legal framework, the current legal framework is inadequate to address all aspects of information technology. Experts are attributing this to a 'toothless' IT Act 2000 (amended 2008) that has been ineffective in tackling the problem of cybercrimes.[1]There are several such cyber 'grey areas' that exist not just in the legal framework of India but in other countries also. These require continuous attention for the benefit of everyone concerned.

2. Objective

This paper is a humble attempt to shed some light on the focus areas covered by cyber security and cyber laws and the issues facing them today. In the 21st century, an era of globalisation, cyber space and Internet are literally king. Transactions worth billions, transfer of extremely sensitive information etc. take place on a daily basis through the medium of Internet. One may well imagine the losses that nations or individuals will face if these become the target of criminals. This paper tries to explain the present cyber security and cyber law framework of India, its workings and the problems being faced by it. It represents a sincere attempt at increasing awareness regarding the importance of these two very important concepts for India.

3. Methodology

This paper involved a certain amount of research, which was essentially doctrinal in nature. There was heavy use of both primary and secondary sources in order to arrive at a clearer understanding of the topic at hand and the critical issues with which the topic is confronted with. Legislations, latest news, reports were liberally made use of as reference tools. The research is library oriented. Other secondary sources such as books, magazines, general websites etc. were of great help in providing substance to what was initially only a rough sketch of the topic at hand. While researching the topic, namely, cyber security and cyber law, critical, comparative and analytical methods were employed in arriving at a successful conclusion.

4. Analysis

4.1 The cyber realm and it's associated problems

In simple terms, cyberspace or cyber-realm refers to an imagined environment in which communication between millions of computer networks occur. This environment is not tangible. We cannot perceive it, yet it is all around us and binds us together in many different ways. The term cyberspace, indeed all terms beginning with 'cyber' began to gain popularity in the 1990s with the increasing spread of the internet and other forms of digital networking and communication systems.

Cyberspace can also be described as a global network of an immense scale, facilitated by the internet. It is used to perform numerous tasks such as transacting money, conducting business, sharing information, creating media, conducting discussions and so on. The list of activities is far too numerous to recount individually. This illustrates the important part that the cyberspace plays in our day to day lives and activities. Not surprisingly, the popularity, utility and vast sums of money flowing through the cyberspace networks have made it a prime target of unethical individuals or groups of individuals, thereby exposing it to different types of crimes.

Cyber-crime is best described as unlawful activities involving the internet, computers or other networks which are committed by individuals or groups of individuals with the intention of stealing money, information or even sensitive data and/or impairing the operations of a website or service which depends heavily upon the internet. Apart from these, there are other crimes such as cyber-terrorism, cyber-stalking and cyber-harassment etc. which target other users of the internet. These are also included within the ambit of cyber-crimes as well.

India being a fledgling country in the area of digitisation, internet use, cyber awareness etc. is particularly vulnerable to cyber- crime. Even if we ignore the all- pervading aspect of the general lack of digital awareness among the vast majority of Indian citizens, there are other factors at play here. The police officers, who are essentially the first persons to whom

victims of cyber- crimes reach out to, must be thoroughly educated and familiarised with the latest trends of cyber space. The reason behind this is that many new areas such as banking, insurance and other financial servicesare increasingly getting computerised. Specialised cyber-crime cells operating in every district connected to each other is the need of the hour. Sadly, at present they operate only on a state by state basis, with one cell in each state. There is an urgent need to create subordinate cells of each state cell in every district or at least in a majority of the districts.

However the problems facing the Indian cyberspace are not limited to the enforcement agencies. There is an urgent need to strengthenthe legal framework that seeks to identify, arrest and penalise the perpetrators of cyber- crimes. At present all issues pertaining to computers, computer networks, information technology are governed by the Information Technology Act, 2008. It is a comprehensive act indeed. However, of particular attention is chapter 11 of the said Act which deals with the offences covered under the Act. Even a cursory glance through the chapter will make it clear to the reader that there are quite a few crimes for which stronger penalties are required. An example would be section 66E of the said Act which provides for punishments for violation of privacy amounting to imprisonment of only three years with a fine of two lakh Rupees. In addition, the Act must also include provisions for taking action against other nations who commit cyber- crimes against our nations' cyber infrastructure. These are new and emerging trends in cyberspace which have come into focus post the famous 'Wiki Leaks' incident. These trends must immediately reflect themselves in the subsequent amendments to the Act. Only by such prompt action can out legal framework remain in a position of strength.

4.2 Cyber security : Introduction and relevance

Cyber security is essentially the entire body of technologies, practices and operation procedures which work together with the aim of protecting networks, programs, sensitive- data, computers and other critical cyber infrastructure from unauthorised access or attack by hostile individuals or groups.

Cyber security operates at both micro and macro level. The simple act of installing an anti-virus software in ones' home computer system is an act of cyber security at the micro level. The act of forming a 'Response team' of experts to deal with cyber- attacks on our critical infrastructure by other nations is an act of cyber security at the macro level. Essentially speaking, every step that individuals or nations take, no matter how big or small, comes within the ambit of cyber security.

The concept of security for communications has come a long way, right from the use of coded ciphers used by Julius Caesar for transmitting messages, to the creation of the famous 'Enigma' machine for encoding messages used by the Germans in World War 2, to the creation of the first 'computer worm' by Robert Morris in 1989 to attack computer networks and his subsequent detection and arrest. Since that time until today, vast changes have taken place in the cyber security scenario and provisions.

The relevance of cyber security cannot be over-emphasised. Put simply, the concept of a safe cyber space cannot be imagined without the concept of cyber security.

Cyber security includes a variety of software tools, some of which are mentioned below-

1. Nmap, which can be used to detect network vulnerabilities.
2. OpenSSH, which acts as a safe conduit for users of computers, laptops whenever they wish to access an insecure network.
3. TrueCrypt, which is essentially an encryption software for storing sensitive information.

Tools such as the ones mentioned above go a long way in ensuring cyber security for individual users.

Cyber security is assuming increasing relevance in the present day scenario owing to the broad spectrum of threats confronting the Indian cyber space today. Different types of cyber- attacks such as virus attacks, worm attacks, Distributed Denial of Service (DDoS) attacks, hacking operate with only one aim in mind, that is, to cripple a nation economically and militarily and also to cause immense hardships and inconvenience to its citizens. Almost all national critical institutions such as banking institutions, energy sector, hospitals, education sector and defence sector have a heavy internet use and presence. Therefore having a strong cyber security framework assumes great importance.

In addition to the above, with information flowing through boundaries of different legal systems connected to different networks around the globe, there is a growing need to protect sensitive and personal information. Thus it is safe to say that the importance of cyber security is only bound to increase in the coming years.

4.3 Challenges with respect to Indian cyber security

Presently India faces multiple challenges from numerous cyber threats. This is because of the fact that a vast majority of the cyber space is unregulated and cyber- crime is becoming increasingly easy and cheap to commit. The situation is such that one can buy hacking software off the shelf also.

India's sojourn with Information Technology began as early as 1975, with the setting up of the National Informatics Centre (NIC) to provide IT solutions to the Government of India. Since that time, policies such as the New Internet Policy of 1998, National Broadband Plan,2010 have seen internet users grow to approximately 100 million. In addition the National Broadband Plan,2010 aims to bring high speed internet connectivity to over 160 million households. Provisions have also been made for monitoring the newly laid fibre optic networks by establishing dedicated state and national level agencies.

All these measures serve to increase the number of persons who are used to and are connected to the Internet. This implies a significant increase in the number of potential victims as well as attackers also. Without even realising it, we are slowly becoming more and more vulnerable. The rapid growth in the cyber sector has literally left both the Government as well as private entities scrambling for answers. They are yet to map out the scope of cyber security because it is highly fluid and dynamic in nature. Threats emerge almost on a real time basis.

Presently India's cyber security framework is exposed to a large number such as cyber terrorism, cyber warfare, cyber- espionage and cyber- crimes. These can be done by other nations or people operating individually. They have the ability to bring our entire nation to a standstill. The purpose of stating such facts is not to cause alarm but rather to make the reader aware of the fact that such problems may occur at some point if adequate precautions are not taken.

Protecting a nation through cyber security is not an easy task. It requires planning, up to date technology, public private partnerships and resources. Above all there must be a strong national will to tackle the menace of cyber-crimes. Cyber security as a policy must be given priority by the Government. This will prove to be of great importance in the seemingly endless battle against cyber-crime and also in securing India's cyberspace.

4.4 Cyber law : Introduction and relevance

Cyber law is one of the newest and fastest growing fields of law in India. It borrows from various traditional branches of law yet it is a unique field of law in its own right. By nature, it is a multidisciplinary law as it includes both civil and criminal aspects of law.

Cyber law in a nutshell can be defined as the collection of laws, rules and other legal issues relating to the Internet. This is different from the related concept of IT law which is the law governing the dissemination, transfer and control of information flowing through the Internet.

The novelty of cyber law can be ascertained from the fact that it was only in 1970 that the first computer specific legislation was passed namely, the Data Protection Act, 1970 in the German state of Hesse.[2]InIndia the concept of cyber law is a very recent phenomenon. Our cyber laws are mostly grouped together under the Information Technology Act, 2008, which came into force on 17th October 2000. It is the primary cyber law dealing with cyber- crimes. It provides for penalties for a large number of offences relating to the internet, computers and their misuse. With regard to official policy pertaining to cyber space, India follows the National Cyber Security Policy which which came into force on 2 July, 2013. It is a comprehensive framework which seeks to protect critical public and private networks from cyber-attacks. It provides a sort of technical and legal backing to institutions and individuals who wish to protect themselves against cyber- attacks. It aims to achieve all this by following a set of strategies which include strengthening the regulatory framework governing internet use, securing digital governance services, strengthening security systems and most importantly, creating awareness among the public about cyber security and cyber risks.

Strong laws and policies governing internet use is the need of the hour in a fledgling digital nation such as India. Therefore the present laws and policies have great relevance, both as a sort of baseline for further improvements and also to protect the individuals that fall within their ambit while they are operational. India has a long way to go with regard to fully securing its cyber infrastructure from cyber- attacks. Until this is done, the abovementioned cyber laws and policies can fill up the void and provide sufficient deterrence to would be cyber attackers.

4.5 Cyber law challenges in India

Globally, the problem with making a regulatory

framework for internet lies in its openness and low barriers. There are simply too many variables at play here. As mentioned before, the numbers of internet users are projected to go upward, with present use approximately 100 million. Regulating such a huge user base is definitely a tough challenge. Problem with the cyber law realm in India is the gap between what is actually committed on paper and what is actually implemented. For example- the cyber- crime unit of Bengaluru Police receives 200 complaints each year, out of which only 10% are solved; a majority are yet to be tried in courts, those that reach the courts do not reach a verdict since the perpetrators of the crime have fled India.[3] The Information Technology Act, 2008 in the form of section 75 specifically provides for jurisdiction over an accused committing an offence in India, though the internet server is located outside India. However this relief can be said to exist only on paper because there is no explanation as to how the section shall come into operation.

The above example is the best way to illustrate the Government's problem in implementing the laws relating to cyber space. However in all fairness, we must take into account the fact that the Government has to walk a delicate line, balancing the right to privacy of its citizens which is a fundamental right and the national cyber security needs of India. Nevertheless there are certain changes that must be made as soon as possible to the laws in order to remain in a position of strength. Chief among these are the provision of Information Technology Act, 2008 which make all cyber- crimes, save a few, bailable offences. The framers of the law do not seem to have taken the extreme harm caused by certain cyber- crimes into consideration while framing the Act.

Therefore the main issues faced by Indian cyber law regime have mostly to do with the Information Technology Act, 2008 which has many chinks in its armour and needs immediate strengthening.

4.6 Recommendations

India's cyber space will get a definite shot in its arm if certain changes are made to its cyber security policy and also to its existing cyber laws. At present the cyber security scenario in India is one of chaos. Among the people there is a not altogether unfounded fear of being a victim of hacking or other such cyber-crime. The issue involving the cyber space is so vast that it is obvious to any keen observer that the law enforcement mechanisms are not responding quickly enough to the new and different types of threats which are appearing on a day to day basis. Ideally, what should have been done is that greater attention should have been given to ensuring that cyber threats to critical sectors are quickly identified and removed but this has not been the case. Therefore instead of adopting a piecemeal approach to cyber security, a 'Comprehensive Cyber Security Policy' is required. At present there are a number of stake holders in the arena of cyber security such as the National Information Board, Ministry of Defence, Department of Telecom, Computer Emergency Response Team and many more. This is merely a recipe for chaos. The need of the hour is to create an autonomous and accountable agency that can monitor every spectrum of the cyber space in India. This must be included in the realm of the comprehensive cyber security policy mentioned above. Apart from creating such an agency, the policy must include many other elements such as building secure cyberspace by using up to date technology, identifying threats on a real time basis, creating a pool of people who can deal with such threats and so on.

Apart from the above, the cyber law framework must also be modified to meet with present day threats. There is a lot of room for development in India's primary cyber law i.e. the Information Technology Act, 2008. Although it provides a framework, it does not address the current situation prevailing in India. It must specify in detail, the process of identifying, prosecuting and penalising a person convicted of a cyber- crime. The focus must be on the 'hows' instead of the 'whats.' In addition, the present scenario where many cyber offences are of a serious nature, yet considered bailable offences must be changed and the quantum of punishments increased. Change can only come in the Indian cyber security scenario when both the Government as well as the people realise the gravity of the situation and take adequate steps to address the same.

5. Conclusion

At present India stands at a unique crossroads of opportunity. She boasts of a large pool of internet savvy individuals and groups in the form of software engineers, app designers, Internet based start-up companies. The Government, in close co-operation with such individuals and groups must work together to develop credible long term solutions to improve internet security for the nation as well as its citizens also. We possess the financial resources, the manpower and most importantly the political will to take such strong measures. What is required is the agreement of all the

stakeholders on a unified set of policies and laws which will serve to protect us against the ever present threats of cyber-crimes. The need for united effort has never been greater.

References

www.dnaindia.com/scitech/Hariszargar/Wed. 3 April, 2013-10.48 AM New Delhi; Accessed on 6.1.2017.

Dhawesh Pahiya: *Cyber Crimes and the Law,* Article appearing in www.LegalIndia.com/cyber-crimes-and-the-law. Accessed on 4.1.2017.

India's Cyber Security Challenge, IDSA Task Force Report, March 2012, P. 22, Article appearing in www.idsa.in. Accessed on 5.1.2017.

□□□