Nine Steps to Indian Security, Confidentiality Privacy & Technology in Cyber Space

Rajeev Kumar Singh*

Abstract

The increasing dependency on cyber space has cropped up concerns associated with understanding the potency of cyber risks which are to a larger extend unguarded and unsecured as the technology is volatile. Cyber security is one of the most critical issues the India faces today. The threats are real and the need is pressing. Despite the best intention of those involved with previous cyber legislative efforts, aAct 2008 Amendment has introduced various beneficial changes into the IT Act, 2000, yet they are not enough to tackle the increasingly growing menace. Cyberspace's dynamic nature must be acknowledged and addressed by polices that are equally dynamic. There is an urgent need to become the technological advancement and cyber-security , wherein intelligentsia has to anticipate, prepare, act, and respond to the cyber risks in all asrata of human life, so as to guarantee effective e-governance, e-commerce and e-communications, thus, protecting cyber space where netizen's safety and security is ensured.

Keywords: Cyber Crime, Cyber Security, Electronic Signature

Introduction

The Indian faces significant cyber security threats includes denial of service, defacement of websites, spam, websites compromise and malware propagation, computer virus and warms, pornography, cyber-squatting and phishing.

A Cyber-crime is now a biggerthreat to India Inc than physical crime. In a recent survey by IBM, a greater number of companies (44%) listedcyber-crime as a bigger threat to their profitability than physical crime (31%). But the available statistics fails to throw actual light upon the real facets of the menace as many cyber-crimes goes unnoticed and unregistered, due to various reasons including lack of legal awareness, a partly of the law enforcement agencies etc. But the facts that cyber- crimes

areincreasing in multitude and are becoming insidiously computer cannot be denied.

The cyber security status quo is unstable, especially when considering the enormous and growing scope of these threats. To mitigate these threats, this paper provides a framework that may provide safeguarding in cyber space to individuals citizens.

Through dynamic and cost effective solution we can make cyber space a safer and more productive place for Indian citizens to pursue the prime minister dreams.

Failure to take responsible action, however, learns the Indian vulnerable to verity of threat. Nation-states such as China, Pakistan, South Korea are more than willing to steal or destroy Indian digital property to further their power or prestige. Non state actors such as Indian Muzzahidin and Hezbollah have also shown the capability to employ cyber methodologies and criminal organizations from around the world, and have acted as hired guns as well as on their own, using cyber tools as their weapon of choice.

In response to the security threats, the Russia, China Israel and North Korea have set up their own cyber armies. America has also established a new cyber command. However, it is unclear what steps have been taken by the Government of India to establish a defence service against cyber-attacks.

In addition to these issues of security for nations and corporations, Indian enacted IT Act in the year 2000, which however failed in effectively tackling cyber-

Rajeev Kumar Singh*
Research Scholar
Chankya National Law University
Patna, Bihar

crimes as it was more inclined towards facilitating electronic commerce. However the amendments made to the original Act through the IT (Amendment) Act of 2008 has brought some changes into the cyber law framework of the country. It has brought forth considerable reformations in the existing law, thereby making cyber-crime a much more serious offence than it was perceived earlier important changes brought in through the amendments.

- Permitting interception of message form mobile phones, computers and other communication devices,
- Blocking of websites in the interest of National security.
- The setting up of a cyber-appellate tribunal.

The amendment has attempted to fill in the gaps which existed in the earlier 2000 enactment. The current Indian IT Law covers provisions relating to cyber frauds and other wrongs committed while using electronic commerce, breach of confidentiality, leakage of data, etc., which were left outside the purview of the earlier enactment. Certain terms left unexplained order the parent law has new been interpretedand explained under the new law, thus giving a wider scope for its application.

Developing challenges that are today's cyber environment. Additionally, any legislation must provide robust protection for privacy and individual freedoms. There are some key components that need to be included in truly effective cyber legislation.

1. **Essential to set up some more agencies like" Cyber police station' specially entrusted with different tasks associated with combating cyber-crime:** Existing agencies involved with the task of combating cyber-crimes in India are an enough. It is essential to set up some more agencies specifically entrusted with efficient tasks associated with combating cyber-crimes which must however work in co-ordination with each other to achieve the ultimate objective. This can be done by establishing separate agencies on the lines of "National infrastructure Protection Centre" of US. A separate centre to take up complains of cyber-crimes over the internet must be set up similar to the "Internet Fraud complaint centre" of US. The department of Justice of US has also setup a separate specialised unit "Computer Crime and Intellectual properly section" to address issues of cyber-crimes. It evaluates problems of cyber- crimes and makes law and policies essential to address such problems. On the other hand, regular police officers are not technically trained to successfully investigate cyber-crimes. There is thus on urgent in all states, through the country. In addition special acquaintance and training of police officers of regular police stations should also be ensured.
2. **Advocating for private sector efforts to promote general awareness, education and training across India:**The Indian people not recognised like American people that there is a problem with securing the cyber domains. The American people hear about it regularly on the news, abstractly, that is there. Here is urgent need of private entities, nongovernmental organizations, along with universities and other research institutes, ought to play a much more active and prominent role in supporting personal cyber safety and community –centric program. Here, must also be viable programs of professional base –level training that is encouraged for the general Non- IT workforce. Since, every job now involves the use of digital dives in some aspects of work; the general workforce must receive continuing education. Apart from this, urgent need of teaching of cyber security as component in school and colleges.
3. **Increase the numbers of IT professionals with security certification:** Information security certification like the certified information systems security professions (CISSP) and the certified information security managers (CISM) may represent the minimum level of taking training that a cyber-security professions needs.
4. **Develop more IT leaders with cyber security expertise:** the India needs more qualified personal in this fields, and specifically in to advanced cyber skill sets, such as code writing, defensive procedures, deep packet inspection, and big data

analysis techniques. A major effort must be made to find the sort of people who can flourish in this field, and give them the opportunity to purpose the high quality education they require.

5. **Cyber security beyond the borders:** The various packets of information tracking over the innumerable remarks in the World Wide Web are not specified as to where they are tracking or who is on the other side of the computer screen. Cyber security is not now, and never will be,issues that our country can solve alone. The solution will require a concreted- and ongoing- collaboration between the Indian a like-minded free nations. Treaties and global governance do not contain bad actors, and should thus not be the focus of Indian or International cyber security efforts. Instead, the India must work with other friendly nations to later bad cyber behavior by raising the costs of such behavior. The first step to effectively conducting a fruitful strategy is to determine an Indian domestic policy on cyber security. I would be foolish to jump into international negotiates until the India has the kind of national conversation that sorts out definitional and policy positions. However, it would be just as foolish to ignore the need to make international connections and establish cooperative relationship in this field. Both should be done as soon as is practical.

6. **Need of legal clarification of scope of certain provisions of IT Act (including section 65, 66A and 66F):** it is essential to regularly update and amend pertinent legal provisions, so that changes in technology affecting the effected implementation of law can be dealt. This call for consistent legal research and development activities and periodical review and revision of law. In addition already existing law and provisions must be properly defined and interpreted to deal with cyber- crimes so that no crimes goes unpunished for the reasons of " insufficiency in law and legal terms and provisions. Whenever It law'sprovisions are silent or fails to address a particular cyber-crime or a related issues , the existing criminal law including IPC and other appropriate enactments must be interpreted to apply and deal with such a crime. Ultimate aim of the law must be to tackle all tippers of cyber-crimes, whether covered under the existingspeciallaw, or not, however by constructing interpreting existing provisions of law. Absence of punishingprovisions in IT Act should not be the ground for acquittalof cyber criminals. This mindexpanded interpretations of terms like "property" in Indian Panel code and requiredexpansion of provisions relating to criminal trespass, mischief, theft, etc. So that it incarcerates new technical features of crimes. The criminal procedure code must be amended so as to facilitate the gathering of evidence and investigation of cyber cries.

7. **Focus on Electronic Signature, Encryption, Monitoring, decryption and Interception in view of National Security:**

   a. An interesting side-effect of the challenge posed by electronic Signatures is that the question of whether a seal can function as a signature becomes relevant. The reason for this is that many of the electronic signature technologies require the signatory to use a numerical key to produce the signature. The smallest useful key area minimum of 56 bit in length, offering a range of numbers between approximately 563,000,000,000,000 and 72,000,000,000,000,000 in decimal notation. These key are too small for adequate security, however, and 128 bit or large r key are more desirable. Number of this size is not easily memorable or easily keyed in without error, and so the key are normally stored on some physical device, such as a memory stick or a smart card.

   b. The recent Amendments to the IT Act, 2000, nearly a decade after the Act came into force; promise to take electronic commerce to the next level by making introducing the concept of technological neutrality. Since electronic signatures are no longer necessarily based on asymmetric cryptology, technical advancement can easily be implemented. These technological advances are most likely

to make electronic signature easier and more secure to use.

c. In the matter of encryption,all over an interesting question is whether the presence of encryption renders the underlying information confidential. As a starting point it would see that if a person goes to the length of encrypting information the information must have a quality about it that is deserving of protection. However there is no authority in law that holds that the mere presence of encryption renders the underlying information confidential.In the case ofMars UK Ltd. VsTeknowledge Ltd., which concerned a coin discriminator mechanism for the sorting of coins in coin operated machines, the defendant reserved engineered the mechanism, a process that required the decryption of encryption program code. One was the question before the court was whether the presence of encryption put the defendant on notice that the encrypted information was confidential.

d. In the matter of Interception , Decryption and monitoring, one of the controversial provisions that has been engrafted into the I.T Act, 2000 by the amendments through the I.T (Amendment) Act, 2008, is the substitution of section 69 that in its new *avatar* grants certain authorities also the power of interception, decryption and monitoring electronic contents including communications (e-mail, online chat or mobile phone communication) " for investigation of any offence" under the sun as against the traditional powers that were highly restricted on few grounds such as, in the interest of the sovereignty or integrity of India.

e. The amendment Act does not deal with the procedure and safeguard for monitoring and collecting traffic data or information by the Central Govt. may prescribe the modes or methods of encryption. As yet no polices or guidelines have been issued pursuant to the power set forth in section 84A.

f. The IT Act 2008 allows the central government to intercept computer communication for investigation of any offence. Section 26 of the Indian Post office Act 1898 grants the government the power to intercept letter or postal articles on the happening of any public emergency or in the interest of public safety or tranquility. Section 5 (2) of the Indian Telegraph Act, 1885 empower the government to intercept land line and mobile phones on the occurrence of any public emergency , in the in the interest of public safety , Sovereignty and integrity of India, security of state, friendly relation with foreign states, public order, or for preventing incitement of the commission of an offence. However the IT amendment Act enlarges of the poser of the central government to embrace interception of information transmitted through any computer resource for the purpose of investigation of any offence. The provision is also vague about the procedure and safeguards that need to be employed when such interception or monitoring or decryption is carried out.

g. The standing committee on information technology , while reviewing the bill , observed that 'public order' and 'police ' are state subjects as per schedule VII of the Constitutions and that the IT Bill should confer powers of interception on the stat governments also in tune with the provisions of section 5(2) of the Indian Telegraph Act, 1885. Therefore interception of information should be for the perception of certain cognizable offence in addition to the already prescribes grounds, instead of the broad sweeping term of 'the commission of any cognizable offence or for investment of any office' used in the Act.

h. The Amendment Act does not deal with the procedure and safeguard for monitoring and collecting traffic data or information by the Central Government it further does not define the procedure and safeguard subject to with blocking access by public to any

information through any computer resource may be carried out.

i. Lack of harmonized definition of the cyber-crimes and lack of international cooperation in tacking the menace is the other problems which require immediate solution.

8. **Use of "Adhar"in social networking sites to prevention of child:** There is a social sites especially porn site creates a page to clarification of age of person able to view the prono graphic image etc. But i the case of 90 percent child below age below than 18 years use pornographic image. This is the major issues for social networking sites. Here is a technique to use "Adhar" to cleafication of actual age by take an Adhar number by user.

9. **Hurdles in the path of combating cyber-crimes:**There is a lack of consensus exists among jurists regarding the definition, nature, ambit and types of cyber- crimes and this is in fat one of the elementaryproblem affecting combating of cyber-crimes. An act of cyber- crimes is not accept as a " criminal wrong " by all , further which law has to deals with the menace is another issues lacing consensus amongst members of legal fraternity. According to some jurists, cyber- crimes are new but traditional crimes committed with the use of new technology and thus they does not require any new or separate law as the traditional criminal itself is sufficient to deal with them, on the other hand, according to some other jurists, cyber-crimes are new forms of crime, having different nature and impact compared to traditional crimes and requires new and separate laws enacted specifically to deal with its investigations and inquires. Though today we have specific provisions dealing with cyber- crimes in Indian It Act, yet many police as well as judicial officers hesitate to register or otherwise deal with the cyber- crimes under it and prefer to do so under IPC, the traditional criminal law of India.

Conclusions

Use of Information Technology in all spheres has helped e-commerce, Internationalconnectivity and communication. But if misused, it can affect the security of nations as well as International community including the security of individuals. More need to be done in order to effectively tackle the growing problem of cyber-crimes. A safe cyber world need a proactive approach to be adopt jointly by Government, Industry Individuals and public at large, which includes adopting and enforcing effective legal provisions, which can effecting counter all forms of cyber-crimes.

"Healthy growth of Information Technology requires a secure environment which can only be ensured by adequate legal provisions and suitable enforcement measures."

References

1. http:www.cert in.org/knowledgebase/annaulreport/annualreport08.pdf.
2. AparnaViswanathan: Cyber Law-Indian and Internatinla perspective, Butterworthswadhwa, LexisNexis, Nagpur, P. 23.
3. Nikhil Pahwa, 'Indian's information Technology (Amendment) Bill passed by LokSabha', http:// wwww.medianama.com/2008/12/223-indians-inforamtion-technology-amedment-bill-passed -by-lok-sabha.
4. The Centre assesses and investigates important threats and incidents relating to intrusion of critical infrastructure.
5. In Us, this Centre established by FBI offers a Central repository system to take up complaints, relating to internet fraud and such information's to quantity fraud patterns and provide timely statistical data of such frauds.
6. Surya Senthil and Lakshmidev: Manual of Cyber Laws, Aditya Book company, Chennai, P. 14.
7. Economic and political weekly, "Dithering over cyber law", Vol 34, No 20 [May 15, 1999) at P 115.