Legal Framework for Cyber Crimes in India and Beyond

Raagini Sharma
(RIEAS Senior Analyst)

Abstract

Internet and communication technology in the 21st century has become the backbone of social, economic and cultural world transcending the geographical barriers and impacting almost all the affairs of mankind. The use of the internet is increasing exponentially and penetrating all the spheres of the government institutions, military defence, scientific organisations, corporate world, educational establishments and almost all bodies of the institution. Data has become a prime commodity to extract relevant information from and then inflict damage to personnel and institutions, causing partial or whole paralysis of the Information Technology ("IT") systems and influence the targets to behave in a manner intended by the perpetrators. Big data, Internet of Things (IOT), 3-D Technology, e-commerce and other existing and emerging technologies related with internet, bring with them a flip side of being used as a tool for cyber-crimes. Hence, there is a need for stringent and well-defined cyber laws with robust regulations to arrest and limit the expansion of cyber-crimes. In India, there is a lack of tough laws, forceful regulatory bodies and political power to combat the cyber-crimes. It is time that the nation comprehends the gravity of threats posed by cyber-crimes with its full spectrum and accordingly sensitize the potential victims to develop a system to fight it. The country immediately needs to address these threats, arrest its expansion and devise means to control its ugly head, given that the technological environment is advancing at a breakneck speed.

Keywords - Cyber-crimes, cyber laws, Information Technology (IT), cyber warfare.

Introduction

The continuing worldwide onslaught of corona pandemic, with no respite or solutions to tide over the situation in the near sight has forced all to look out for options to do their businesses. In the wake of corona catastrophe, **WFH (Work from Home)** has almost become a panacea to overcome the obstacles of social distancing that is universally implemented to arrest the spread of pandemic. The conduct of almost all businesses in corporate, government, and non-

governmental sectors has radically shifted to online transactions. Even imparting of education online has become a new normal. The internet has become a lifeline, and the working-world without it cannot be dreamt of. The internet, on one hand, has provided the alternate solution to most of the business communications and governmental work, however; on the other hand, the exponential exploitation of internet has given almost a limitless playfield for the **computer hackers, cyber-stalkers, data-stealers and their likes** to exploit the sophisticated, subtle and non-conspicuous virtual world to carry out their **cybercrimes**.

As against the traditional crimes, cybercrimes are committed using computers and the internet as aids and targets as well. In its domain, comes the banking frauds, deceitful business transactions, stealing of confidential data of state and government organisations, child pornography, copyright infringements and unimaginable several more crimes which are committed in real-time, impacting one and all. The impacts are far-reaching, sometimes with global consequences and are not easy to be dealt with. This has driven countries to actively pursue broad-ranging responses to lessen the attacks of privacy infringements and cybercrimes that the virtual world faces today. Each country's obligation towards the securitisation of their cyber-world should be so stringent so as not to allow or severely restrict the cybercrimes in order to ensure that the functionality of the systems are not compromised. For this, the systems must have the robustness to combat the various modes of cybercrimes in a proactive manner rather than in a response mode.

Amidst the pandemic, the dependence on the virtual management of work has expanded. Hence, the requirement of cyber resilient organizations has become top priority. Cyber-crime may be characterized as an umbrella term as within its domain are several and different kinds of crimes viz **cyber-dependent and cyber-authorized crimes, cyber hacktivism, cyber-espionage etc**. To overcome the threats posed by the internet world, there are different measures which the developed countries have initiated. The US Department of Homeland Security and the United Kingdom National Cyber Security Centre have been focusing on the magnitude, frequency and the relevance of cyber-attacks during the Covid-19 Pandemic. Measures have been instituted with the inventiveness of the use of patched and updated software and operating systems, encrypted hard-drives, automatic screen locks and VPN (Virtual Private Network). Several countries have initiated legal and regulatory requirements securing the systems from financial or data losses. The **General Data Protection Regulations (GDPR)** and **Network and Information system (NIS)** have been deployed by the United Kingdom. The main criteria is to implement cyber-security processes within the framework of laws, reducing the risk factor.

Since 1998, when its first nuclear missile was launched, India has been receiving threats on the website of Bhabha Atomic Research Centre (BARC) (Patil and Bhosale 2013). The 2010 cyber-attacks were one of the most significant attacks in the country in which more than 10,000 government officials' emails were hacked. The beginning of the 21st Century signalled the progression of cyber law in India with the enactment of the **Information Technology (IT) Act, 2000**.

Cyber security is essential to protect all of us. The government needs to implement strict laws, rules and policies, especially when one knows that there would always be a competitive race between the technologies to assist committing cyber-crimes with the ones to prevent these. However, if the counter cyber-crime technologies are backed up by firm laws and rules of the land, the devil of cyber-crime may be tamed if not fully demolished. The legal framework for cyber-crimes should be a fine mix of punishments which are preventive, deterrent and retributory in nature.

The paper, highlights about the laws and initiatives taken by the government such as Cyber Swachh Kendra, Cyber Surakshit Bharat, National Critical Information Infrastructure Protection Centre and Personal Protection Data Bill. China's cyber warfare against the world will also be briefly covered to examine the gravity of the attacks and the ways to combat these aided by the technologies and the laws of the land. The paper focuses on upon the quantum of cybercrimes in India at present and growth in the future; the legal frame work and the modus operandi within the legal framework that would suit India best to control the risk factors generated by the cybercrimes.

Cyber Laws in India

The last decade of the 20th century became a turning point as most of the countries opened their doors for free international trade. The birth of globalization gave the countries an opportunity to craft their future in terms of monetary stability. IT backed up by computers and seamless communication started to become a necessity and world wide web (www) created a sense of wonder without realizing the limitless potential as also hazards and dangers to be known in near future. Alongside all this, e-commerce demonstrates a great future. Antecedent to this era, all the trade transactions were in writing and through the means of post which changed dramatically with the advent of internet. The boost of email communications made the United Nations to take action on data protection. On that account, United Nations Commission on International Trade adopted a "Model Law" in 1996. In essence, at present, IT has made the world literally, a global village and the flat world in the words of Samuel Huntington. It has enhanced every sphere and sector of the society like economy, commerce, social and educational sectors.[1]

At the dawn of millennium, a sound and rugged framework was the urgent requirement in India to arrest the expansion of cyber-criminal activities. There was a need for new encryption and privacy policies. Every time there is a terrorist attack in the country, from Mumbai attack-26/11 to Pathankot, a breach of data has taken place. India's infrastructure has been found to be cyber-porous and prone to all kinds of digital interventions. With the increase of internet frauds, the laws in India were found to be non-existent or best quite sluggish to knuckle down the crimes. The excess utilization of internet has amplified the apprehension on the present-day legal issues.

[1] Umejiaku and Anyaegby, (2016), *"Legal Framework for the enforcement of cyber law and cyber ethics in Nigeria",* International Journal of Computers and Technology, Vol-15, No.10.

In the beginning of the 21st century, Indian parliament passed an act on e-commerce known as **Information Technology (IT) Act, 2000**, ("the Act") which became the primary cybercrime law in India. It was also recognised by the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) and was endorsed by the UN General Assembly by a decree dated 30 January 1997. According to the IT Act, the legal sanctity should prevail on matters of electronic communications, business transactions, trade and commerce, but it was only limited to computer systems and networks. It also highlighted that all the barriers should break when it comes to development, but the legality over any subject should be upheld as an utmost priority. The Act deals with various issues such as legal recognition of electronic documents, and digital signatures, cyber offenses and contraventions and justice dispensation systems for cybercrimes.

Hacking has been properly defined in Section 66 of the Act as, "*Whosoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking."*[2] The two important sections in the Act (Amended) are "**cyber contravention** i.e. Section 43(a)" and "**cyber offences** i.e. Section 63-74" where the government has the sole authority to prosecute and penalise any individual or group who is behind the breach of data. Other than the Act, there are other legislations which existed before and dealt with data security, the Companies Act (1956), Copyright Act (1957) and Code of Criminal Procedure (1973). It was only in 2019, that the Personal Data Protection Bill was passed, as compared to basic right which gets implemented only in theory.

When the Act was implemented as a directive in the country, the courts acknowledged the digital records and manuscripts, be it digital signature, electric form or electronic recordings. Section 65B states that

> "*Any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied:*
> *(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly .... by lawful persons;*
> *(b) the information ...derived was regularly fed into the computer in the ordinary course of the said activities;*
> *(c) throughout the material part of the said period, the computer was operating properly ..... and .....a certificate signed by a person responsible."*

Cyber law expert and advocate at the Supreme Court of India,_(name of expert) claims that - ***"The push towards building massive IT infrastructure that will transform the country into a connected economy and realise the vision of Digital India,***

[2] https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technology-act-2000--some-perspectives?

necessitates the need for strong cyber security mechanism to keep the citizen data safe and secure."[3]

With the technological advancements in IT and related fields, data has become a prime commodity on which many businesses, banking transactions, government institutions, scientific processes etc. are dependent. Consequent to this dependency, it has also become easy to steal and tap data. Data has thus become hugely susceptible and accessible to the perpetrators of cybercrimes. **The Act was hence, amended in 2008**. It is strange that in both the Acts, IT Act of 2000 and the IT Amendment Act of 2008, "cybercrimes" are not defined. On 29th October 2009, the new amended Act was enforced. The priority of privacy stands at the top of the table; it is also mentioned in the Article 21 of the Constitution of India. In terms of cyber space, data protection also is an enumerating factor. In 2018, the Srikrishna Committee gave a report, which was later transformed as the **Personal Data Protection Bill 2018**.

Internet is about abolishing boundaries and not about creating them. The new law opens up a Pandora's Box for conflict on jurisdiction.[4] The key features of IT Amended Act, 2008 were to introduce information security, define cybercafé, make digital signature technology neutral, bring out the importance of Computer Emergency Response Team (CERT-IN), inclusion of few other cybercrimes such as child pornography and cyber terrorism and authorize police to investigate cyber offences. *"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb"*, the gravity of cyber-attacks has been well brought out by National Research Council, (Computers at Risk, 1991) way back.

According to Dr. Pavan Duggal, a specialist in cyber law, cybercrimes can be described into three categories, firstly cybercrimes against persons like child pornography or harassment. An apt cybercrime to quote is the case of the Melissa virus wherein the Melissa that was a mass mailing macro virus, was released by the perpetrators in March 1999 targeting Microsoft and Outlook based systems and created huge network traffic of pornographic sites along with logins. The virus spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused 80 million dollars in damages to computers worldwide. [5] Second category of cybercrimes is against the property, like loss of technical database which is done through corporate cyberspace and third category is cybercrimes against government, this can be seen in case of terrorist threats to citizens of country, infringing government documents and stealing of confidential data.

Be it bank account details, login details, medical records or digital identity, all can be infringed in cyber space. This phenomenon of illegal grabbing of data is not a new scenario. To get justice, if one is a victim of cybercrime, as per the Act, the court needs to give full compensation. Cyberspace along with outer space have become the unique realms for the developed armed powers to explore and know adversary's intent and cause huge financial and

[3] https://www.expresscomputer.in/magazine/dedicated-legislation-for-cyber-security-is-needed-pavan-duggal/13378/
[4] Duggal, P (2000), *"India Passes Its First Cyberlaw With Draconian Powers",* Available at: https://www.zdnet.com/article/india-passes-its-first-cyberlaw-with-draconian-powers/
[5] Babu, Maya (2004), *"What is Cyber-crime?",* Computer Cyber-crime Centre, Available at- http://www.crime-research.org/analytics/702/

material losses apart from unbalancing them psychologically. Evaluating that most countries seek to retain or expand their footprints in outer space, it could be an effective strategic decision for India to take preventative measures to deny the effect of any cyber-attack on its critical space assets such as satellites, base stations, command centres and long-range weapons.

Internal and External Threats

The proliferation of militant attacks over the last few decades has raised questions regarding border protection. The Internet and cyber-methods offer an avenue for terrorists, hackers, nations and organised crime organisations to attack and destroy the government credibility and cause changes to citizens' perceptions. Cyber-attacks have huge potential to cause massive damage to the infrastructure of a country and its population. These assaults can be highly critical in situations of crisis. Cyber-attacks on hospitals can refuse access to hospital staff which may contribute directly to the death of patients. This is what happened in Ukraine. The Ukrainian electricity providers suffered significant power shortages on 23 December 2015.

The Ministry of External Affairs (MEA) is responsible for working with other countries on international policy concerns and overseeing the adoption of international agreements on internet-related concerns. Law enforcement also faces problems during cyber-crime investigations as such investigations can lead to clashes between states over sovereign immunity control and lack of global partnership.

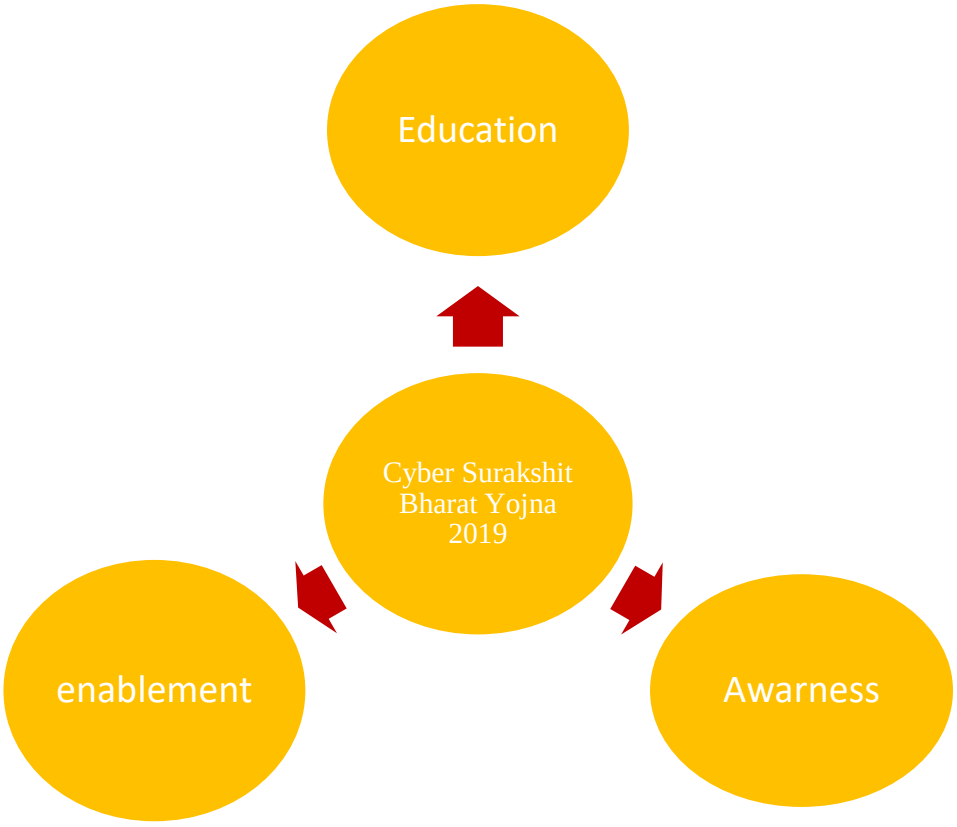
Initiatives Taken by India Government to Curb Cyber Threats

To preserve India's online information, communications and financial sites from cyber-attacks, the Government of India needs to start working quickly and effectively in solidarity with other ministries, such as the Ministry of Defence and the Ministry of Housing and Urban Affairs. **Cyber Surakshit Bharat Yojna 2019,** the vision of 'Digital India' changed the course of India's development. Ministry of Electronics and Information Technology (MEITY) launched **Cyber Security Bharat**. It is the first public-private partnership initiated by the government to secure the country. Cyber Surakshit Bharat aims to ensure awareness about cybercrimes and adequate safety measures to be taken for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments. [6] The Cyber Surakshit Bharat scheme was launched in cooperation with National e-Governance Division (NeGD) and various industry partners in India.[7] The partners involved in the origination of this scheme include chief IT companies like Intel, Microsoft, Redhat, WIPRO and Dimension Data. The knowledge partners of Cyber Surakshit Bharat Yojana include NIC, Cert-In, FIDO Alliance, NASSCOM and leading consultancy firms EY and Deloitte.[8]

[6] https://www.microsoft.com/en-in/about/cybersecurity-surakshit-bharat.aspx
[7] https://www.gibl.in/government-scheme/cyber-surakshit-bharat-yojana.html
[8] Ibid

Initiatives taken by India towards drafting cyber laws and establishing regulatory bodies and creating synergy between these are as follows: -

- Penalties for cyber-crime offences are subject to various statutes such as the Indian Evidence Act (IEA) and the Indian Penal Code (IPC). New policies on cyber offences have been adopted by the MEA and the Ministry of Home Affairs (MHA). MEITY has been at the core of the implementation of security policy, including the **National Cyber Security Strategy (2013)** and **Draft Encryption Policies (2015)**. **Computer Emergency Response Team - India (CERT-IN)**, India's leading cyber-security firm, is now under the ambit of MEITY. Government departments such as the National Sensitive Information Infrastructure Security Centre (NCIIPC) are also helping to deter such incidents. Due to the dynamic nature of cyberspace, there is now a need for these initiatives to be unified under the National Cyber Security Policy.



- **National Critical Information Infrastructure Protection Centre [NCIIPC]** is an agency established corresponding to section 70A of the IT Act, 2008. It is aimed at promoting a stable, secure and durable Information System for vital sectors of the country. The organisation is regularly involved in cyber security activities to track the status of cyber security in critical areas of cyber security.

- **Personal Protection Data Bill,** the law on personal data security, was enacted by the Parliament of India in 2019. The bill was forwarded to the Joint Parliamentary Committee for a thorough review. It aims to provide for the privacy of personal data of persons, to set up a system for the collection of such personal data and to set up a Data Privacy Body for that purpose.

China: A Viable & Potential Threat in Cyberspace Domain

China's dominance over cyber space has increased with People Liberation Army (PLA) and Strategic Support Force policy of independent cyber organisation and changing the course of fighting by gaining information without getting traced. With this independence, the ability of China's warfare towards the world has increased many folds apart from the conventional spaces of warfare that are land, sea and air. Information warfare has vitally altered the ways the conventional wars have been fought. On 23 May 2017, a Sukhoi 30 aircraft crashed on India-China Border in North East, which IAF inquiry later opined was cyber attacked, presumably by China.[9] Union Bank of India heist 2016, data theft at Zomato 2017 and Petya Ransomware attack, 2017 are all carried out by China, that too, not from the mainland China but as a proxy from other countries like Vietnam or Philippines. These cyber threats add a new dimension to the warfare. Informationization has become the key factor in enhancing war fighting capability of the armed forces. China frequently defines the word "Integrated Network Electronic Warfare" (INEW) to denote a coordinated view of information warfare, including electronic warfare (EW), virtual network warfare, and psychological warfare.

Risks to the Indian defence industry typically emerge from entities with political, commercial, or pseudo-political motivation which adversely impacts the national security, public safety, and commercial well-being of society. In 2010, the world faced the largest cyber-attack in which more than 10,000 email addresses of top government officials were compromised. There is thus an inescapable need to establish a cyber-security environment in order to safeguard the technology and resources of the defence industry in real time with respect to the provision of safety and incident response.

Cybercrime Deterrence

Good training and tactical drills in cyber security / warfare needs to be enhanced and strengthened at a wider range. Individuals need to be trained in this era where each one of us is dependent on it. Infrastructure, warfighting tenets and to recover after the attack, cyber deterrence by India needs to be taken seriously. Internet trends and ongoing behaviour in dark web needs to be monitored throughout to protect the country. Young children and specially the

[9] Naveen Goud, Cybersecurity Insiders, accessed at https://www.cybersecurity-insiders.com/china-cyber-attacks-indian-sukhoi-30-jet-fighters/

youth, the future of the country gets cyber-attacked. Close cooperation is required between the countries to counter cybercrimes. All over the world, there is a standard way of building the computer and laptop except the adapter and medium of language. This standardization can be an advantage to lower the threat. The innovations resulting from technological standardisation go way beyond the globalisation of technologies and services and could contribute to the harmonisation of national legislation. However, as illustrated by the discussions on the First Protocol to the Convention on Cybercrime of the Council of Europe, "the standards of national law are evolving much more slowly than technological advances.

Cyber Security as a Career

The shortage of trained data security experts is as much a problem for developed countries as it is for India. The developed countries are however, taking promising steps to overcome this challenge. Australia and the US are investing heavily in promoting people to choose cyber security as a career. In particular, Australia has launched a range of programmes under the Cyber Protection Plan to counter the lack of qualified cyber professionals. It is the government's responsibility to promote career options in this field.

Conclusion

Cybercrimes are a new class of crimes, contingent on IT and related technologies. Throughout the world, countries are reintroducing or replacing varied propositions and laws towards an attempt to control cyber-violations and cyber-crimes. Cyber warfare is indeed a very cost-effective way to degrade the enemy's war fighting potential. Justifiably, in the digital age, IT usage has been an essential element of combating activities, a part of the fabric of combat ideologies of security and assault strategies. It is high time that countries need to put stringent regulatory regimes to prevent the computer data to be hacked, stolen, vandalised, manipulated or altered by the perpetrators to cause the financial, material or psychological damage to intended targets be it citizens, infrastructure, government institutions or corporate houses. Along with the stringent cyber laws, the constant monitoring and surveillance of cyber space is a must for timely interventions to curb the cybercrimes. In the wake of exponential increase in cybercrimes, India needs new age cyber laws and security resolutions to combat this menace save we are ready to the pay heavy price economically, militarily, culturally and above all psychologically.

References:

1. Regina Mihindukulasuriya, India was the most cyber-attacked country in the world for three months in 2019, The Print, 03 March 2020, accessed at https://theprint.in/tech/india-was-the-most-cyber-attacked-country-in-the-world-for-three-months-in-2019/374622

2. Saurabh Tewari China's Cyber Warfare Capabilities, USI Journal, April 2019 – June 2019, accessed at https://usiofindia.org/publication/usi-journal/chinas-cyber-warfare-capabilities/

3. Steve Snyder, What is the difference between Cyber resilience and cyber security, OpenText(9th June, 2020) https://blogs.opentext.com/cyber-resilience-vs-cyber-security/

4. Margot Rouse, What is Hacktivism?, Search Security (July, 2018) https://searchsecurity.techtarget.com/definition/hacktivism

5. Akash dhanjani, "Case Brief Shreya Singhal v/s Union of India, 2015" available at: https://lawbriefs.in/case- brief-shreya-singhal-v-s-union-of-india-2015/