ISSN: 0974-5823 Vol. 7 No. 3 March, 2022

International Journal of Mechanical Engineering

IS INDIA'S CYBER-SECURITY AN OUTDATED SYSTEM ON LIFE-SUPPORT?

Ankitesh Kumar Jha[1], Aditi Kumari[2], Prof. (Dr.) Poonam Rawat[3], Prof. (Dr.) Anil Kumar Dixit [4] , Dr. Radhey Shyam Jha[5]

[1]Student, Law College Dehradun, Faculty of Uttaranchal University, Dehradun, Uttarakhand;
E-mail ID: ankiteshjha.jha@gmail.com
[2]Student, Law College Dehradun, Faculty of Uttaranchal University, Dehradun, Uttarakhand;
E-mail ID: kumari.aditi0307@gmail.com
[3]Professor, Law College Dehradun, Faculty of Uttaranchal University, Dehradun, Uttarakhand;
E-Mail ID: hodlaw@uttaranchaluniversity.ac.in
[4]Professor, Law College Dehradun, Faculty of Uttaranchal University, Dehradun, Uttarakhand;
E-Mail ID: anil@uttaranchaluniversity.ac.in
[5]Associate Professor, Law College Dehradun, Faculty of Uttaranchal University, Dehradun, Uttarakhand
E-Mail ID: radheyjha@uttaranchaluniversity.ac.in

ABSTRACT

This article presents a brief analysis of the present condition of Indian cyberspace and the laws that govern it. It is an attempt to go through the decisions already made, as well as the necessary steps required to protect the privacy of Indian citizens as well as to build firewalls that safeguard India's critical infrastructure. A subtle discussion of the facts and figures from the past, and what is there to learn from them, so that the Internet becomes a safer place for the people. Finally, the article brings up the question of whether the government may access anyone's data under the pretence of national security.

Cyber security is the application of technology, processes, and policies to protect electronically advanced systems from cyber attacks. Its purpose is to reduce the danger of cyber-attacks while also protecting systems and system-related applications against unauthorised access.(IT Governance, 2016)

India's cyber security is governed by the Information Technology Act, 2000 which was later amended in 2008 but can a field that evolves at such a rapid pace, be governed by acts and statutes that are amended or updated after a span of eight full years?

Keywords: C*yber security, Cyber security threats to India, India's domestic internet stability, data breaches in India, right to privacy.*

INTRODUCTION

Cyber security protects computers, smart phones, and computer networks, including the internet, from physical and virtual security risks. With developing information technology, there are two categories of threats. The first is the danger of illegal access to digital equipment with the goal to modify, destroy, or misuse the information accessible on that system, causing havoc with the intended service related to that system. The second threat is 'the authorised use of cyber tools to aid, organise, and facilitate terrorist attacks and undertake or assist devastating physical damage to life, property, and national assets,' which is still being investigated by digital professionals, statisticians, intelligence communities, and corporate giants that are based completely over the Internet.(Indian Infosec Consortium, 2014)

The International Telecommunication Union (ITU) has released the Global Cyber Security Index (GCI) 2020, which is a performance-based assessment of five cyber security criteria, including legislative measures, technological measures, organisational measures, capacity development, and collaboration.

The United States was in the first place, followed by the United Kingdom and Saudi Arabia. India was ranked as the world's tenth best country in the index, with a fourth-place finish in the Asia Pacific area.

CYBER SECURITY IN INDIA: CHALLENGES & ISSUES

1. Lack of Proper Legislation:

Amidst all of the initiatives and legislation, people continue to commit crimes online. Online transactions and financial transactions are common, making them a prime target for criminals. Despite a number of preventative steps, similar crimes continue to occur. Furthermore, as previously stated, rules vary per sovereign nation, allowing criminals to leave and making it hard for authorities to pursue the guilty.

2. Challenges related to Implementation:

According to recent NCRB data, there has been a rampant increase in cyber-crimes in India. The data recorded an increase of 11.8 per cent rise in cyber-crimes in the year 2020. Further, as the COVID era began, people globally became more dependent on the internet. As a result, there was a rise in Internet traffic resulting in more creative data crimes and leakage of personal data of billions of users worldwide.

- ***Over 45 Lakh Customers Affected in Cyber-Attack On Air India:***

An appropriate example of such a data breach is the incident where the servers of Air India got hacked. India's state-run airline, Air India, was the target of a significant cyber assault. Passengers' personal information, such as credit card numbers and passport numbers, was also obtained in this incident. Other foreign airlines may also be affected by this cyber assault. According to the news agency ANI, the data from August 26, 2011, to February 3, 2021, has been tampered with. Name, date of birth, phone number, passport information, ticket information, and credit card information are all included. About 45 lakh people's personal information was exposed as a result of this assault.

- ***The vaccination portal Co-WIN app was also targeted by hackers:***

The government of India created an application for the registration of vaccination doses for its citizens. Although, this application was also hacked by vigilantes from China and South Korea. The hackers created many fake apps with the same name on Google Play Store. These applications were further used by hackers to steal the personal data of people.

- ***Breach of data in India's Healthcare Industry:***

Medical information for more than 120 million Indian patients has been exposed, according to recent research issued by the German cyber security firm Green bone Sustainable Resilience. Breach Candy Hospital and Utkarsh Scans in Mumbai are among them. The hacked medical information, according to the claim, has been rendered publicly available over the internet. As per the research, Maharashtra leads the country in terms of data breaches involving patient medical information. Greenbone Sustainable Resilience's initial study, released in October 2019, found major data leaks, including CT scans, X-rays, and MRIs, as well as patients' photographs have also been shared.(Rawat, Jha, Tiwary, & Waraah)

- ***The problem of data protection***

Data is as vital as money in the twenty-first century. Many multinational corporations (Google, Amazon) are attempting to access India due to its large population. As a result, concerns such as data sovereignty, data localization, and internet governance must be addressed. The digital economy currently accounts for 14-15 per cent of India's overall GDP, with the goal of reaching 20 per cent by 2024.As a result, concerns such as data sovereignty, data localization, and internet governance must be addressed.

- ***Deficiencies in the Cyber Security Approach***

A scarcity of human resources: The Indian Armed Forces, Central Police Organizations, and Law Enforcement Agencies lack experienced personnel who are familiar with the technical elements of the different software and hardware necessary in this area.

In addition, Artificial Intelligence (AI), Blockchain Technology (BCT), and Machine Learning (Machine) Knowledge of cutting-edge technologies such as learning (ML), data analytics, cloud computing, and the Internet of Things (Internet of Things-loT).

3. Challenges Related to National Security:

There are three basic dimensions of cyber security from the standpoint of national security: exploitation, defence, and offensive.

- The first is a contemporary sort of espionage that entails detecting adversary networks' hardware and application weaknesses in order to gather important information. However, it is not just for passive reasons, since massive volumes of data may be "exfiltrated" and utilised to sabotage military operations.
- The second step is to put in place safeguards to make it harder for attackers to degrade, disable, or destroy protected networks. The third step is to take steps to "preventively" or "pre-emptively" disable offensive capabilities that are designed to be used in cyber-attacks. (Kshetri, 2015) Advances in information and communication technologies, as well as their widespread usage, have resulted in an ever-increasing reliance on cyberspace and its infrastructure, putting societies and economies at greater risk of disruption.
- Policymakers and civil society have grown more cognizant of cyber threats such as cyber frauds, cyber espionage, and cyber terrorism, and even acts of cyber war have been identified. Many of the hazards in and emerging from cyberspace may be classified as potentially systemic risks, meaning they are fraught with high levels of uncertainty, complexity, and ambiguity. As a result, the likelihood and potential damage of an occurrence cannot be accurately estimated. The origins of potential losses are difficult to pinpoint, and an incident might have far-reaching consequences across nations. (Prasad & Kumar, 2022)
- Expert opinions on cyber threats and their potential consequences vary greatly. Because a scientific evaluation of the situation is impossible owing to a lack of objective assessment, socio-political perceptions of cyber dangers are weighted much more heavily. It is clear that we are becoming increasingly reliant on cyberspace and the internet. Over two years ago, India included over 100 million internet users. Add in the 381 million internet-enabled mobile phone subscribers and the rising ease with which all kinds of gadgets access the internet.

In the five years spanning 2005 and 2010, the number of internet users more than quadrupled, to well over 2 billion. These figures are increasing at an exponential rate, indicating the internet's expanding reach and our growing reliance on it. In one manner or another, most of us utilise and rely on cyberspace in our job and daily lives.

4. Deterrent Issues in Policy Making:

The government establishment is grappling with a number of difficult issues that will require time and effort to overcome. These are some of them:

1. Declaratory policy — In the middle of a significant data breach against Defence forces, central command systems, electric power grids, financial networks, or other components of military force or key infrastructure, the government has no official government policy publicly communicating what are the options available at their disposal. Should a declaratory policy exist, and if so, what should it contain? Should we, for example, designate unacceptable categories of "serious cyber-attack," so-called "red lines," that would almost certainly result in a massive retaliatory response? (Sharma, 2021)
2. Deterrent policy – For most of the nuclear era, deterrence strategy has been refined to affect adversary behaviour in irregular, conventional, and even nuclear combat. Are these principles relevant in the cyber arena, where attribution of the assault can be difficult to determine and cyber-attack damage can range from little (e.g., delaying email delivery) to major (e.g., crippling the nation's military preventative measures)?
3. Authorities and Responsibilities — If cyber assaults on defence forces or key infrastructure originate from another country, a response will almost certainly include a breach of that country's sovereignty. What legal authority do you have to carry out such operations? Furthermore, there is a significant time lag between getting sufficient legal powers (which can take weeks or months) and the necessity for national security personnel to quickly respond (which might take minutes or hours). How may this temporal gap be addressed most effectively?
4. Civil liberties protections – The policy and legal sectors are at odds when it comes to cyber security. Given the difficulties in determining where cyber assaults begin, and the probability that some of these attacks may originate in India, how can we design successful policies that nevertheless protect our citizens' civil

freedoms, whether formulated by our government or by our citizens? What conditions would justify the government monitoring its people's cyber communications, or, if necessary, degrading or disabling these systems?

5. Oversight – What role does the government play in supervising executive branch cyber activities? What kind of laws should be adopted so that our cyber security is strengthened rather than harmed?

5. Challenge of Preserving the Right to Privacy:

The right to privacy is one of the unspoken rights that the Indian judiciary has understood to exist under the terms of Article 21 despite the fact that it is not expressly stated in the Constitution. It is critical to remember that the Indian judiciary does not only acknowledge the right to privacy; it also recognises informational privacy as an important aspect of the right to privacy (Chaterjee, 2019)

- ***Data Privacy:***

The major concern is that it was revealed in September 2013 that the Indian government has been secretly using Lawful Intercept & Monitoring (LIM) technology. Mobile providers in India, in particular, have implemented their own LIM systems, allowing the government to conduct so-called "lawful interception" of calls. Mobile carriers may be obliged to give subscriber verification to the Department of Telecommunications' Telecom Enforcement, Resource, and Monitoring (TERM) cells in order to facilitate this. Such an act is both a major threat to personal data protection rights as well as a necessity to protect the National Security of India(Singh, 2013). Because the government has authority over the LIMs, it can send commands and extract any data it wants through the Internet pipe without informing anyone except some within the government who execute the Internet traffic surveillance commands. Further, it has been found that the links to the Internet are in an "always-live" state thereby conducting any data transfer as may suit their needs.

The result of such a breach in the name of national security can have grave consequences. The government in power holds an infinite amount of data over its citizens, so much so that they can create an online duplicate of every citizen and further use that data to manipulate laws, win elections and God knows what else. (Gercke, 2009)

CYBER-SECURITY MEASURES OF INDIA

India's reliance on the internet has grown at a fast rate during the previous decade. The exponential growth of the internet has generated a reliance on it, and cyber security issues have emerged. At the same time, it increases vulnerability, making information warfare a threat. Information warfare has evolved from a purely militarily worry to a big business issue in the last two decades. As a result, it is critical for India to foresee and plan for countermeasures by enacting legislation and establishing various institutions to address the issues posed by the expansion of the internet and the digitization of government(Clinical Infectious Diseases, 2012).

LEGISLATIVE STEPS TAKEN BY THE GOVERNMENT

There have been many efforts made by the government in both legislative and administrative fields to strengthen national cyber security as well as make the internet a safer place for individuals.

- ***Indian Penal Code***

The Indian Penal Code has been rigorously amended in the past decade to match the changing times. In the present era, a thief looking for money does not steal cash from homes but calls up people and by targeting their specific needs draws out money from their pockets in a fraudulent manner.

Several sections of the Indian Penal Code have been amended to widen their scope and cover the crimes in general as well as more advanced ways of committing the same crimes. For example, Section 292 was originally intended to address the selling of obscene materials, it has developed in the digital age to address a variety of computer crimes. This clause also governs the electronic publishing and dissemination of obscene content, sexually explicit activities, exploitative acts involving children, and other similar acts.

As of now, the government has begun the process of stringently amending the Indian Penal Code as well as the Code of Criminal Procedure for better identification of cyber-crimes and crimes in general.

- ***Information Technology Act, 2000:***

In July 1998, the Department of Electronics recommended statutes to control and govern and overwatch technology-based systems through a bill, especially the Internet due to pertaining threats to National Security. Later, with the formation of the Information Technology Ministry, the process of securing the cyberspace of India was expedited. On 16th December 1999, the recommendation by the Department of Electronics was brought up before the House. The Ministry of Commerce recommended further alterations in the bill to be modified to fit in accordance with the W.T.O. Obligations. Keeping this in mind, the Ministry of Law as well as the Ministry of Commercial Affairs forged a Joint Draft which was recommended to the 42-member Parliamentary Standing Committee. Once the I.T. Ministry had reviewed the draft bill, the Union Cabinet approved the I.T. Bill, 2000 on May 13th, 2000. The bill was further passed by each of the Houses of Parliament on 17th May. 2000 and got the assent of the President on June 9th, 2000. Finally, the Information Technology Act, 2000 came into force on October 17th, 2000. (History of cyber law in India, 2005)

It was held by the Apex Court a year after the passing of the Act stating that the UNCITRAL Model Law and the Arbitration and Conciliation Act, 1996 are not identically drafted, further the Court stated that as a result of differences between the two the Model Law, as well as related judgements and literature, cannot be used to interpret the Act. (Konkan Railway Corporation Ltd. v. Rani Construction (P.) Ltd., 2022)

- ***Personal Data Protection Bill, 2019***

Following a lengthy and bitterly debated public discussion, the Indian government submitted the Personal Data Protection Bill in Parliament on December 11, 2019. While the Bill lays out the legal framework for personal data governance (including the creation of a regulator, the Data Protection Authority), it also mentions non-personal data, requiring mandatory sharing of non-personal or anonymized data to assist the Central Government in better target service delivery or formulate evidence-based initiatives. This is clear if far from unique, an allusion to non-personal data in the Indian setting. (Marda, 2020)

ADMINISTRATIVE ACTIONS TAKEN

Establishment of Institutions

- ***National Informatics Centre***

The creation of the National Informatics Centre (NIC) by the Indian government in 1976 was the first move in this direction. The major goal of this centre was to deliver information technology solutions to state and federal government agencies. NIC, as a service provider, monitors network events for the prevention and detection of harmful activity on the network. Intrusion Prevention Systems (IPS), Anti-Virus solutions, Firewalls, and Application Firewalls are all protected by the NIC (Krist, Narrandes, Pridham, Yogalingam, & Matheson, 2014)

- ***Indian Computer Emergency Response Team (CERT-In)***

The Indian government established the Indian Computer Emergency Response Team (CERT-In) in 2004, which is the most integral ingredient of India's cyber community. There are comparable setups in about 62 nations throughout the world, including Asia, Europe, and North and South America (Krist, Narrandes, Pridham, Yogalingam, & Matheson, 2014). Its major goal is to safeguard the security of India's cyberspace by improving the security of the country's information and communications infrastructure through proactive action and effective coordination geared at preventing and responding to security incidents. The CERT-In establishes a panel of auditors to deal with IT-related security concerns, and all businesses operating in the nation are subjected to this third-party assessment. On the other side, the high level of connectedness and reliance on the IT industry has resulted in an increase in crime, necessitating the creation of legislation to safeguard people.

PLANS AND POLICIES

- ***National Cyber Security Strategy 2020***

The goal of this policy is to enhance cyber security and awareness by implementing a better audit system. The cyber auditors will maintain a tight lid on various corporations' security aspects. Also, cyber preparedness to

monitor cyber security readiness is included in the policy. There has also been a proposal of a distinct budget for cyber security, with the objective of generating synergy between specific duties.

Cyber crisis response simulations would be undertaken on a regular basis under the policy, understanding that cyber-attacks might happen at any time. A cyber preparation index is planned as part of the policy to track cyber security readiness. A distinct budget for cyber security has been proposed to provide synergy between the responsibilities and duties of several agencies with the necessary domain expertise.

- ***Other Major Policies***

The government adopted the 'National Cyber Security Policy, 2013', which established the 'National Critical Information Infrastructure Protection Centre (NCIIPC)' for the protection of sensitive data. There is a provision for imprisonment ranging from two years to life imprisonment, as well as fine.

Awareness Programmes

The government has created the 'Information Security Education and Awareness: ISEA' programme in order to develop human resources in the field of information security at various levels. A 'Cyber Swachhata Kendra' has also been established to deal with cybercrimes in the country in a coordinated and effective way. It is part of the Government of India's Digital India effort, which is overseen by the Ministry of Electronics and Information Technology (Meity).

5. JUDICIAL PERSPECTIVE

The Supreme Court issued one of the most important decisions on the privacy concerns in the matter of ***District Registrar v. Canara Bank*** (District Registrar v. Canara Bank, 2005). In this case, the validity of a section of the A.P. Stamps Act was challenged. In situations of fraud or neglect of any obligation owed to the government, the challenged clause gave specific state authorities the authority to search and seize records, registers, books, or papers in the possession of any public officer. In this instance, the privacy of a customer's records is maintained by an organization that works in the financial domain.

The Supreme Court of India ruled that the challenged provision was unconstitutional because it failed to meet the constitutional rationality requirements set out in Articles 14, 19, and 21. (Maneka Gandhi v Union of India , 1978) The triple test established in the landmark case of ***Maneka Gandhi v. Union of India*** states the requirement that any law infringes on 'personal liberty' under Art. 21 meet three criteria: firstly, a process must be prescribed; secondly, one or more of the fundamental rights guaranteed by Article 19 must be upheld by the procedure, This might be useful in a specific case, and finally, it also must be subjected to liability testing in accordance with Article 14. This triple test was found to be failed by the contested provision. The Court also determined that the term "privacy" applied to the individual rather than the location. It makes no difference whether the financial records were kept at a citizen's residence or in a bank.

Shreya Singhal v. Union of India (Shreya Singhal v. Union of India, 2012) is a historic case that has had a significant impact on the growth of Indian information technology legislation. The Supreme Court of India addressed the core value imbibed in Article 19(1)(a) of the Constitution of India in this case. In this case, the constitutionality of section 66Aof the I.T. Act 2000, which provides for penalties for delivering inflammatory communications by communication services and other means, was challenged. For a variety of reasons, the outcome of this case is a benchmark in the archival records of the Supreme Court. The Court went to the point of ruling a censorship statute established by Parliament to be completely unconstitutional. The judgement expanded the extent of Indian citizens' right to freely express themselves and limited the State's ability to restrict this freedom unless in the most extreme situations.

6. CONCLUSION AND SUGGESTIONS

India has made strides in data protection and privacy by enacting a variety of legislative and regulatory measures. To make matters worse, the majority of threats come from state-sponsored organisations seeking to disrupt key infrastructure in the oil and gas, energy, military, and telecommunications sectors. Because the majority of crucial information is held there, attacks will begin there, with the goal of stealing all of it, making the nation's countermeasures apparent.

With growth comes power, and with power comes responsibility. As we talk about responsibilities the goal is to make people aware and vigilant of the threats that come their way when they become in charge of how they utilise the internet services. A huge section of society isn't educated enough on these matters to ever understand that sharing a small amount of information on the web might cause irreversible damage to their identity or personal data. A futuristic approach, keeping in mind that people of all sections of the society and age groups access the internet, needs to be put forth and implemented so that we have a safe, digitalised India.

As we talk about internet usage, we can't miss out on the fact that the traffic on the internet increased many folds after our nation was hit by the covid wave. Offices, schools, banks, everything started functioning online. The dependency of people on the internet has become insanely high. This calls for a far better functioning cyber security structure.

It is the era of the internet; traditional warfare might not be able to protect what we aim to keep safe. Massive breakthrough in policies, tackling the need of the hour, and raising the budget for cyber security is the need of the hour.

REFERENCES

1. Chaterjee, S. (2019). Is data Privacy a Fundamental Right in India. *International Journal of Law and Management*.
2. Clinical Infectious Diseases. (2012, June 15). *IDSA, 54*(12).
3. District Registrar v. Canara Bank, (2005) 1 SCC 496 (Supreme Court 2005).
4. Gercke, M. (2009, April). Understanding Cybercrime: A Guide for Developing Countries. (I. -D. Division, Ed.) *International Telecommunication Union*, 63. Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf
5. *History of cyber law in India*. (2005). Retrieved 05 03, 2022, from www.indiancybersecurity.com: http://www.indiancybersecurity.com/cyber_law_history_india.php
6. Indian Infosec Consortium. (2014). India's Cyber Security : Conference Proceedings of Ground Zero Summit. In S. K. rath. New Delhi: Synergy Books India. Retrieved from https://www.academia.edu/28471869/India_s_Cyber_Security_Conference_Proceeding_of_Ground_Zero_Summit_2014
7. *IT Governance*. (2016). Retrieved 04 22, 2022, from itgovernance.co.uk: https://www.itgovernance.co.uk/what-is-cybersecurity
8. Konkan Railway Corporation Ltd. v. Rani Construction (P.) Ltd., AIR 2002 SC 778 (Supreme Court of India 2022).
9. Krist, M., Narrandes, R., Pridham, K. F., Yogalingam, J., & Matheson, F. (2014, April 15). MCIT Evaluation Report. *Toronto Mobile Crisis Intervention Team (MCIT) Program Implementation Evaluation Final Report*.
10. Kshetri, N. (2015). India's Cybersecurity Landsacpe: The roles of private sector and public-private partnership. *IEEE Security and Privacy 13:3*, 16-23.
11. Maneka Gandhi v Union of India , (1978) 1 SCC 248 (Supreme Court 1978).
12. Marda, V. (2020, 10 15). *Ada Lovelace Institute*. Retrieved 04 14, 2022, from www.adalovelaceinstitute.org: https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/
13. Prasad, S., & Kumar, A. (2022). Cyber Terrorism. *Non-traditional Security Concerns in India*, 53-73.
14. Rawat, D. P., Jha, D. R., Tiwary, A. P., & Waraah, U. (n.d.). Data Breach in Heathcare Industry: An Infringement of Right to Privacy.
15. Sentanos, M. (2020, 11 17). *CrowdStrike*. Retrieved from 2020 Global Security Attitude Survey Takeaways | CrowdStrike: https://www.crowdstrike.com/blog/global-security-attitude-survey-takeaways-2020/

16. Sharma, R. (2021). 10 India's Cybersecurity Concepts and Policies. *Facets of India's Security*.
17. Shreya Singhal v. Union of India, W.P. (Cr.) No. 167 of 2012 (Supreme Court 2012).
18. Singh, S. (2013, 06 6). India’s surveillance project may be as lethal as PRISM. *The Hindu (National)*. New Delhi. Retrieved 03 26, 2022, from The Hindu: https://www.thehindu.com/news/national//article60417581.ece
19. UNGA Resolution. (1966). *United Nations: Commission on International Trade Law (UNICITRAL).2205 (XXI).* United Nations.