INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBER SECURITY IN INDIA: CURRENT STATUS AND FUTURE PROSPECTS

AUTHORED BY: SOUMYADEEP SARDAR

ABSTRACT

Cybersecurity is a vital part of our interconnected world, protecting individuals, organizations and nations from evolving cyber threats. This article examines the current state of cyber security in India and assesses the prevailing challenges and initiatives. Analyzing the cyber threat landscape, the research examines the existing regulatory framework and its effectiveness. Challenges including infrastructure constraints, lack of skills and lack of public awareness are identified, paving the way for a comprehensive understanding of the cyber security barriers faced by India.

The paper examines both government and private initiatives, emphasizing national cybersecurity policies and corporate cybersecurity practices. It also explores collaborative efforts within and across national borders and highlights the need for a collective approach to cyber resilience. In the future, new technologies will be explored and recommendations will be made to strengthen the regulatory framework, improve training and competency programs, and promote international cooperation.

Case studies provide valuable insights that illustrate successful cybersecurity implementations and provide lessons learned from past incidents. By providing a comprehensive overview of cyber security in India, this article aims to contribute to the ongoing debate on strengthening digital landscapes. The conclusion confirms the importance of proactive measures and emphasizes the need to constantly adapt to the dynamic cyber security landscape.

ISSN: 2582-6433

INTRODUCTION

In an era dominated by digitization and interconnected technologies, the development of cyberspace has brought unprecedented opportunities for innovation and communication. However, this digital revolution has also created new and complex challenges, especially in the area of cyber security. As an emerging economic powerhouse with a rapidly growing digital footprint, India finds itself at the forefront of navigating this complex landscape of cyber threats and vulnerabilities.

The interconnected nature of our globalized world means that the impact of cyber threats knows no boundaries. India, with its huge population, diverse industries and increasing reliance on technology, has become a prime target for cyber-adversaries seeking economic gain, geopolitical advantage or simply disrupting critical infrastructure. Therefore, understanding the current state of cyber security in India is crucial not only for the country and its economic well-being, but also for national security.

This article aims to provide an in-depth analysis of cyber security in India by examining the prevailing challenges, the existing regulatory framework and initiatives by both the government and the private sector. By examining the threat landscape, infrastructure limitations and shortage of skilled professionals, we aim to create a comprehensive picture of the country's cybersecurity landscape. In addition, we delve into case studies to learn valuable lessons from both successful cybersecurity implementations and incidents that have shaped India's trajectory cyber resilience.

Against the background of rapid technological development, the publication also considers the future prospects of cyber security in India. This includes assessing the potential impacts of new technologies, making recommendations to strengthen the regulatory framework, and highlighting the need for cooperation at both national and international levels.

Starting with this research, it becomes clear that the journey to a secure cyberspace in India requires not only a strong regulatory and technological infrastructure, but also a collective and proactive approach by all stakeholders.[1]

[1] https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/india.html

ISSN: 2582-6433

STATEMENT OF PROBLEM

Under this research paper the problem which going to be discussed is related to cybersecuriy and cyber crime.

As India is rapidly progressing on its digital transformation journey, the increasing dependence on information technology has exposed the country to many cyber security challenges, both in the near and future. The evolving nature of cyber threats combined with existing vulnerabilities creates a multifaceted problem that requires comprehensive understanding and strategic intervention.

OBJECTIVE OF STATEMENT

The objective of the study is:

- The aim of this research is to examine the assessment of current threats landscape and cyber bullying.
- To analyze the evaluation of regulatory framework in India.

HYPOTHESIS

The effectiveness of cyber security measures in India directly affects the country and its resilience to evolving cyber threats, and a comprehensive and adaptive cyber security strategy that includes regulatory frameworks, skilled workforce development and technological innovation will significantly improve securing of the digital landscape both now and in the future.

RESEARCH QUESTIONS

- What is the current state of the cyber threat landscape in India, and how has it evolved in recent years?
- How are emerging technologies, such as artificial intelligence, the Internet of Things, and 5G, influencing the cybersecurity landscape in India?
- How can public awareness and education on cybersecurity be improved in India, and what role does it play in building a cyber-resilient society?

ISSN: 2582-6433

RESEARCH METHADOLOGY

The research method used for the study is Doctrinal method of research . It starts by adopting a proposition as a focal point or beginning point. The law is then located in statutes, judicial rulings, and discussions in commentaries, books, journals, and debates. reads them thoroughly, examines them, makes his observations, and writes them down. It may provide a set of formulations or highlight the purpose behind the proposition and suggest what it should be based on the examination of the same.

SCOPE OF LIMITATION

Cybersecurity includes measures to protect digital assets, including data, networks, systems and applications, from unauthorized access, attack and damage.This includes the security of critical infrastructures such as power grids, communications networks and financial systems to ensure the uninterrupted operation of essential services.Cybersecurity faces challenges in keeping pace with the rapidly evolving tactics and techniques of cybercriminals, making it difficult to anticipate and prevent every type of cyber threat.

CYBERSECURITY

India and its rapid digital transformation has brought unprecedented opportunities, but has also exposed the country to growing cyber threats. The current state of cyber security in India reflects a dynamic landscape where challenges and advances coexist. Currently, the country faces a number of cyber threats, including phishing attacks, ransomware and data breaches. The government has taken significant steps to address these challenges. Initiatives such as the National CyberSecurity Policy aim to strengthen the country's position and cyber security. In addition, the establishment of the Cyber Crime Coordination Center in India demonstrates the commitment to improve cooperation between law enforcement agencies and the private sector.

All governments in the world, including our own, are concerned about cyber security. India in particular is facing a growing number of cyber security challenges and it is important that it takes ownership of them. According to a recent analysis of global cyber crime by the Economic Times, cyber attacks cost the government nearly Rs. 1.25 million euros per year.

ISSN: 2582-6433

Another Kaspersky study highlights that the number of cyber attacks in India increased from 1.3 million to 3.3 million in the first quarter of 2020. The highest number of attacks was recorded in India, with 4.5 million in July 2020. Recently, the Reserve Bank of India (RBI) banned the MasterCard payment system for failing to maintain data.

The threats posed by the Internet are almost limitless, and the most effective way to combat them is to implement a cybersecurity policy. The government must devote significant resources to securing critical information assets. State and cyber security legislation must be updated to take into account the legal rules and respond to the challenges caused by rapidly developing technologies.[2]

CURRENT STATUS OF CYBER SECURITY IN INDIA

The current state of cyber security in India is characterized by a complex interplay of challenges and advances. The country's increasing reliance on digital technologies in administration, business and communication has opened up new opportunities for cyber threats. Various types of cyber attacks such as phishing, ransomware and data breaches targeting both individuals and organizations have increased in India. One of the major challenges is the population's limited awareness of cyber security, which increases the vulnerability to manipulative attacks. In addition, there is a shortage of qualified cyber security professionals in the country, highlighting the need for robust training programs to bridge the skills gap. To meet these challenges, the Government of India has taken several measures to strengthen the country and its cyber security.

The National Cyber Security Policy is a comprehensive framework that outlines strategies to improve cyber security at both national and organizational levels. The establishment of India's Cybercrime Coordination Center (I4C) is an important step to strengthen cooperation between law enforcement agencies and the private sector to effectively combat cybercrime. However, the effectiveness of these measures is still under review, and the need for continuous improvement of cyber security infrastructure is increasingly recognized. The private sector also has a crucial role to play in shaping India's current state of cyber security. Industries are increasingly investing in cybersecurity measures to protect sensitive data and critical infrastructure. However, the

[2] https://www.upguard.com/blog/cybersecurity-regulations-india

ISSN: 2582-6433

changing nature of cyber threats requires constant reassessment of security strategies. The government and financial sectors have been a particular target, prompting regulators to impose strict cyber security guidelines on banks and financial institutions.

Overall, the current state of cyber security in India is characterized by a mix of proactive activities and ongoing challenges. While the government has shown commitment through policy frameworks and collaborative initiatives, addressing the skills gap, raising awareness and adapting to the changing threat landscape remain critical for the country to achieve a strong cybersecurity posture. Continued efforts and investments are needed to secure India's digital assets and ensure a secure cyberspace for its citizens and businesses.

CHALLENGES IN INDIAN CYBERSECURITY

India's cyber security landscape faces a number of challenges that reflect the complex and evolving nature of the digital threat landscape. One of the most important challenges is the rapid digitization of various sectors without simultaneously strengthening the cyber security infrastructure. As businesses, public services and individuals increasingly adopt digital platforms, the attack surface of cybercriminals expands, increasing the risk of cyber incidents.

A critical concern is the lack of qualified cybersecurity professionals in the country. The need for experts who can understand, implement and manage strong cyber security measures is outstripping the current supply. This skills gap is exacerbated by the lack of comprehensive cybersecurity training programs, leaving organizations vulnerable to sophisticated cyber threats. Bridging this gap is imperative for India to create a skilled workforce that can proactively defend against cyber attacks.

Another major challenge is the proliferation of outdated technology and old systems, especially in critical sectors such as healthcare, energy and transport. These older systems often lack the necessary security features and are more vulnerable to exploitation by cybercriminals. The slow pace of system renewal and modernization is a major obstacle to ensuring a sustainable and secure digital infrastructure. The growing threat of state-sponsored cyber attacks is also a major concern. As geopolitical tensions rise, nation states are increasingly using cyber operations to gain influence or strategic advantage. In a geopolitically significant way, India will become a

ISSN: 2582-6433

prime target for such cyber campaigns, requiring a robust and adaptive defense strategy at the national level.

Social engineering attacks, especially phishing, continue to be a challenge in India's cyber security environment. Cybercriminals often exploit people's lack of cybersecurity to gain unauthorized access to sensitive data or deliver malware. Public awareness and cybersecurity education are critical to mitigating this human-centric vulnerability. Additionally, India's cyber security regulatory framework is still in its infancy and gaps and ambiguities need to be addressed. Clear and comprehensive regulations are needed to ensure that organizations across industries follow standardized cybersecurity practices and reporting mechanisms.

In short, India's cybersecurity challenges are multifaceted, ranging from a lack of skilled professionals and outdated infrastructure to a changing threat landscape and geopolitical tensions. Addressing these challenges requires a concerted effort by government agencies, private companies and educational institutions to strengthen the nation and its cyber defences, foster innovation in cyber security practices and create a sustainable digital ecosystem for India and the future.

INITIATIVES AND STRATEGIES

The Government of India has recognized the growing importance of cyber security and has implemented several initiatives and strategies to improve the country's cyber resilience. Some notable efforts include:

- National Cyber Security Policy (NCSP): The government drafted the NCSP to provide a comprehensive framework to address the challenges posed by cyber threats. The policy outlines strategies and measures to strengthen cyber security at the national, organizational and individual levels.
- India CyberCrime Coordination Center (I4C): The establishment of I4C marks a concerted effort to coordinate and improve cyber security efforts across the country. It aims to act as a nodal agency for law enforcement agencies, enabling them to effectively fight cybercrime through more effective collaboration and information sharing.
- CERT-In (Computer Emergency Response Team - India): Under the Ministry of

ISSN: 2582-6433

Electronics and Information Technology, CERT-In plays a vital role in responding and mitigating cyber security incidents. It provides early warning and response to various cyber threats and helps organizations and individuals facing cyber attacks.

- National Critical Information Infrastructure Protection Center (NCIIPC): NCIIPC focuses on securing critical information infrastructure, including the energy, transportation, and financial sectors. The center formulates and implements policies and strategies to improve cyber security in critical sectors.
- Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center): Launched as part of the Digital India initiative, the center aims to create a safe and clean cyberspace for users. It provides tools and services to detect and clean up malware infections, helping to create a safer online environment.
- National Cyber Security Coordinator (NCSC): The appointment of the National Cyber Security Coordinator reflects the Government's commitment to strategic planning and coordination in the field of cyber security. The NCSC plays a key role in implementing the National Cyber Security Policy and promoting collaboration between various stakeholders.
- Public-Private Partnerships: The government recognizes the importance of collaboration and encourages public-private partnerships in cyber security. This requires working closely with industry stakeholders to share threat intelligence, best practices and jointly develop strategies to reduce cyber risks.
- Skill Development Initiatives: The government has launched skill development programs to address the shortage of experienced cyber security professionals. These programs aim to improve workforce skills through cybersecurity education and training.
- International Cooperation: The Government of India is actively engaged in international cooperation on cyber security issues. Cooperation with other countries, international organizations and participation in forums promotes a global approach to cyber threats.

Together, these initiatives demonstrate the government's commitment to create a secure and sustainable cyberspace for India. However, constant effort, constant innovation and the ability to adapt to new threats are crucial to being a pioneer in the dynamic field of cyber security.

ISSN: 2582-6433

FUTURE PROSPECTS AND ROCOMMENDATION

Employment of cybersecurity or information security analysts is projected to grow 31 percent between 2019 and 2029, much faster than the average for all occupations. Cyber security analysts are expected to be in high demand as these analysts need to create innovative solutions to prevent hackers from stealing critical information or causing problems with computer networks.

Skills needed to ensure cyber security:

- Intrusion detection
- Malware analysis and removal
- Programming
- Black hat thinker
- Risk analysis and mitigation
- Cloud security
- Security analysis[3]

CASE STUDIES

1. Pune Citibank MphasiS Call Center Fraud

Some ex-employees of BPO arm of MPhasiS Ltd MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber crime cases that raised concerns of many kinds including the role of "Data Protection".

The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".

ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in ITA-2000.

Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to

[3] https://fieldeffect.com/blog/what-is-the-future-of-cyber-security

ISSN: 2582-6433

the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2. THE CASE OF SONY.SAMBANDH.COM

India was first convicted of cybercrime in 2013. It all started after a complaint by Sony India Private Ltd, which operates a website www.sony-sambandh.com that targets Indians living abroad. The website allows NRIs to send Sony products to their friends and relatives in India after paying for them online. The company is obliged to deliver the products to the respective recipients. In May 2002, someone logged into a website using the identity of Barbara Campa and ordered a Sony Color Television device and wireless headphones, according to a cybercrime case investigation. He gave his credit card number for payment and asked to deliver the products to Arif Azim in Noida. The credit card company cleared the payment correctly and the transaction was processed. After following due diligence and inspection procedures, the company delivered the products to Arif Azim. During the delivery, the company took digital photos of Arif Azim accepting the delivery. The transaction was closed at the time, but a month and a half later the credit card company informed the company that it was an unauthorized transaction because the real owner refused the purchase. The company filed a complaint about the online fraud with the central police, which registered a case under sections 418, 419 and 420 of the Indian Penal Code. The matter was investigated and Arif Azim was arrested. An investigation revealed that Arif Azim, while working in a call center in Noida, gained access to the credit card number of an American citizen, which he misused for the company and the website. The CBI recovered a color TV and wireless headphones in this unique internet fraud case. In this case, the CBI had evidence to support its claim, so the accused pleaded guilty. The court convicted Arif Azim under Sections 418, 419 and 420 of the Indian Penal Code, the first conviction for cyber crimes. At the same time, the court found that since the accused was a 24-year-old boy and was convicted for the first time, he had to be lenient. Accordingly, the court released the accused on one year's probation. The verdict has huge implications for the entire nation. Apart from being the first judgment on cybercrime, it showed that the Indian Penal Code can be effectively applied to certain categories of cybercrimes not covered by the Information Technology Act, 2000. Secondly, such a judgment sends a clear message to all that the law cannot to be taken blindly.

ISSN: 2582-6433

3. The Bank NSP case

One of the leading cyber crime cases is the Bank NSP case where a bank management trainee was engaged to be married. The pair exchanged several emails on the company's computers. After some time they broke up and the girl created fraudulent email IDs like and "indianabarassociations" and sent e-mails to the boy's overseas clients. He used the bank's computer for that. The boy's company lost a large number of customers and sued the bank. The bank was responsible for emails sent through the bank and the system.

4. Andhra Pradesh Tax Case

The dubious tactics of a prominent Andhra Pradesh businessman were exposed after department officials seized computers used by the accused in one of India's many online fraud cases. The owner of a plastic company was arrested and the detectives of the vigilance department recovered 22 million rupees in cash from his house. They asked him to explain within 10 days whether the cash remains in the account. The defendant presented 6,000 coupons to prove the legitimacy of the transaction and thought that his crime would go unnoticed, but after a careful examination of the coupons and the contents of his computers, it was revealed that they were all made after the attacks. It was later revealed that the accused ran five companies under the name of one company and used fake and computerized vouchers to show sales data and save taxes.[4]

CONCLUSION

Overall, the state of cyber security in India reflects both commendable work and ongoing challenges. The rapid digitization of various sectors has opened new frontiers of possibilities, but has also opened the country to the increased threat of cyber threats. The Government of India has responded with proactive initiatives such as the National Cyber Security Policy, the creation of the Indian Cyber Crime Coordination Center (I4C)[5] and various public-private partnerships.

However, challenges remain, such as a lack of qualified cyber security professionals, outdated technology in critical areas, and the constant evolution of cyber threats. Bridging the skills gap, improving infrastructure and fostering a culture of cyber security awareness are essential for

[4] https://www.cyberralegalservices.com/detail-casestudies.php
[5] https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

ISSN: 2582-6433

India and its continued digital development. Going forward, the future prospects for cyber security in India look promising. Continued efforts to improve education programs with the integration of new technologies such as artificial intelligence will create a safer digital future for India. A commitment to international cooperation and information sharing further strengthens the nation's commitment to combating global cyber threats.

As India moves into the complexities of the digital age, a holistic approach that combines technological advances, regulatory frameworks and a well-informed public is essential. By addressing these challenges and building on existing initiatives, India can emerge as a global leader in cyber security, securing its digital assets and ensuring a safe and sustainable cyberspace for its citizens and businesses. Constant vigilance, adaptability and cooperation are key to strengthening India's and #039's defenses against ever-evolving cyber threats.