International Journal of Social Research and Development
www.socialsciencejournal.net
Online ISSN: 2664-8709, Print ISSN: 2664-8695
Received: 22-07-2024, Accepted: 21-08-2024, Published: 05-09-2024
Volume 6, Issue 2, 2024, Page No. 21-24

A review on cyber security and national defense policies in India

Aakuthota Srinivasulu
Assistant Professor, Department of Public Administration & HRM, Kakatiya University, Hanamkonda, Telangana, India

Abstract
In an era marked by rapid technological advancements and increasing digitization, cyber security has emerged as a critical component of national security for India. Prime Minister Narendra Modi launched the Digital India campaign, a key initiative of the Government of India aimed at digitally empowering citizens by enhancing connectivity, expanding access, and promoting the electronic delivery of government schemes and services to the general public. This initiative is crucial in advancing a systematic program for integrating information and ensuring that every citizen benefits from digital advancements. India progresses with digitalization, it faces various challenges, including data localization and cyber threats. To address these concerns, the Indian military is in the process of establishing a cyber command to strengthen the cybersecurity of its defense systems. This cyber command will involve the creation of a parallel hierarchical structure, positioning it as a central stakeholder in safeguarding the nation's digital infrastructure. The country faces a multifaceted threat landscape characterized by cyber attacks from state and non-state actors, targeting vital sectors such as defense, finance, energy, and critical infrastructure. This paper explores the evolution of India's cyber security strategies and their integration into national defense policies. India has taken significant strides in fortifying its cyber security framework, evidenced by the establishment of the National Cyber Security Policy, the creation of the Indian Computer Emergency Response Team (CERT-In), and the implementation of various cyber laws and regulations. These measures aim to safeguard national assets, protect citizens' data, and ensure the integrity of digital systems. This paper analyzes key cyber incidents that have shaped India's cyber security policies, evaluates the effectiveness of current defense strategies, and provides recommendations for future enhancements. By addressing legal, ethical, and technical challenges, India can strengthen its cyber security posture and safeguard national security in the digital age.

Keywords: Cybersecurity, digital age, defense digital age strategies, national security, technical challenges

Introduction

India's journey toward establishing a robust cybersecurity framework has been driven by the rapid digitalization of its economy and the growing threat landscape. As a country with over a billion internet users and a burgeoning digital economy, India faces significant challenges in safeguarding its digital infrastructure. This has necessitated the development of comprehensive cybersecurity systems and policies to protect critical information, ensure data privacy, and secure cyberspace.

India has experienced rapid digitalization across nearly every aspect of public life. With over 1.15 billion phones and more than 700 million internet users, these numbers continue to grow. This expansion has significantly increased access to financial services, even in rural areas. Initiatives like Make in India and Digital India are driving positive economic impacts nationwide. Both private sector and government entities have developed digital service delivery mechanisms, resulting in a synergistic effort that is producing impressive outcomes. For instance, in 2021, India's Unified Payments Interface (UPI) processed 39 billion transactions totaling $940 billion—accounting for more than 30% of the country's GDP. The digital payment systems in India saw a substantial growth of 26.2% in volume during the 2020-21 period.

This rapid digitalization has also created a critical reliance on the resilience of interconnected networks and systems. A successful cyberattack on a vital asset, such as the power grid, could have a cascading effect, disrupting communications, transportation, and even threatening the health and safety of citizens. Both the government and private sector are keenly aware of these risks, including the capabilities and intentions of potential adversaries. Over the past decade, several concrete measures have been implemented to prevent, detect, and mitigate the impact of cyberattacks.

India's journey toward establishing a robust cybersecurity framework has been propelled by two powerful forces: the rapid digitalization of its economy and the increasingly sophisticated and pervasive nature of cyber threats. These factors have created a complex landscape where both opportunities and risks are growing at an unprecedented pace, making the need for strong cybersecurity measures more urgent than ever.

Rapid digitalization of the Indian economy

Over the past decade, India has experienced a remarkable digital transformation, driven by government initiatives, private sector innovation, and widespread adoption of digital technologies across all sectors of society. This digitalization process has reshaped the Indian economy in several key ways:

Widespread Internet access

India is home to one of the largest and fastest-growing populations of internet users in the world, surpassing over a billion people. This growth has been facilitated by the proliferation of affordable smartphones, expanded mobile internet coverage, and government initiatives like Digital India, which aims to connect every corner of the country to the internet. The increase in internet penetration has opened up new economic opportunities, enabling millions to participate in the digital economy.

Expansion of digital services
The digital economy in India has flourished, with digital platforms becoming integral to everyday life. Services such as digital payments, e-governance, online education, telemedicine, and e-commerce have seen exponential growth. The government's push for digital financial inclusion through platforms like the Unified Payments Interface (UPI) has revolutionized the way transactions are conducted, making cashless payments more accessible to a broader segment of the population.

Growth in digital infrastructure
India has invested heavily in building a robust digital infrastructure, including data centers, fiber optic networks, and cloud computing platforms. This infrastructure supports the country's digital economy and enables businesses to operate more efficiently, scale rapidly, and innovate in ways that were previously impossible. The development of smart cities, which integrate digital technologies to improve urban living, is another example of how digitalization is transforming India's physical and economic landscape.

The growing cyber threat landscape
As India's digital footprint has expanded, so too has the landscape of cyber threats. The country's increasing reliance on digital technologies has made it a prime target for cybercriminals, state-sponsored hackers, and other malicious actors. This evolving threat landscape presents several significant challenges:

Rise in cyber attacks
India has witnessed a significant rise in cyberattacks, ranging from data breaches and ransomware attacks to phishing schemes and denial-of-service (DoS) attacks. These incidents have targeted both individuals and critical infrastructure sectors such as banking, telecommunications, healthcare, and energy. The growing frequency and sophistication of these attacks highlight the vulnerabilities in India's digital infrastructure and the need for robust cybersecurity defenses.

Emergence of sophisticated threat actors
The cyber threat landscape is no longer dominated by lone hackers. It now includes well-organized criminal syndicates, state-sponsored hacking groups, and ideological hacktivists, all of whom possess advanced tools and tactics. These actors are often motivated by financial gain, political objectives, or the desire to cause disruption. Their activities pose a serious threat to national security, economic stability, and public trust in digital systems.

Increasing concerns over data privacy
With the vast amount of personal and financial data being generated, stored, and processed online, data privacy has emerged as a major concern. High-profile data breaches and the misuse of personal information have raised questions about the adequacy of existing data protection measures. The growing importance of data in the digital economy, coupled with the potential for misuse, underscores the need for strong data privacy regulations and practices.

The necessity for comprehensive cybersecurity systems and policies
In response to the twin pressures of rapid digitalization and a growing cyber threat landscape, India has recognized the critical need to develop and implement comprehensive cybersecurity systems and policies. These efforts are aimed at achieving several key objectives:

Protecting critical information infrastructure
The protection of critical information infrastructure (CII) is a top priority for India's cybersecurity strategy. CII includes vital sectors such as banking, telecommunications, defense, energy, and transportation. These sectors are the backbone of the nation's economy and security, and any disruption to their operations could have catastrophic consequences. To safeguard these assets, India has established agencies like the National Critical Information Infrastructure Protection Centre (NCIIPC), which is tasked with identifying and protecting CII from cyber threats.

Ensuring data privacy and security
In an era where data is often referred to as the new oil, the protection of personal data is of paramount importance. India has been working on enacting comprehensive data protection laws, such as the Personal Data Protection Bill (PDPB), which aim to regulate the collection, storage, and processing of personal data. These laws are designed to ensure that individuals have control over their personal information and that organizations handling such data are held accountable for its protection.

Securing cyberspace for all
India's approach to cybersecurity is not limited to protecting critical infrastructure and data; it also includes efforts to secure cyberspace for all citizens. This involves promoting cybersecurity awareness, improving digital literacy, and fostering a culture of security across all levels of society. Initiatives like Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) have been launched to help individuals and organizations detect and mitigate cyber threats. Additionally, the government has introduced regulations that require businesses, especially those in the digital space, to implement stringent cybersecurity measures and report any security incidents.

Fostering international cooperation
Cybersecurity is a global challenge that requires international cooperation. India has been actively engaging with other countries, international organizations, and private sector partners to share information, best practices, and technologies to combat cyber threats. This collaboration is essential for addressing transnational cybercrime, enhancing cyber resilience, and developing global norms for responsible behavior in cyberspace.

Building cybersecurity capabilities
Recognizing the shortage of skilled cybersecurity professionals, India has prioritized the development of cybersecurity capabilities. This includes investments in cybersecurity education and training, the establishment of research and development centers, and the promotion of cybersecurity startups. The goal is to create a pool of experts who can lead the country's efforts in defending against cyber threats and developing innovative solutions to emerging challenges.

Cyber security system in India

National critical information infrastructure protection centre (NCIIPC)

Established under Section 70A of the Information Technology Act, 2000, NCIIPC is responsible for protecting critical information infrastructure in India. It identifies critical sectors such as banking, defense, telecommunications, transport, and energy, and works to safeguard them from cyber threats.

Indian computer emergency response team (CERT-In)

CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. It plays a vital role in the protection of India's cyber infrastructure and issues guidelines, advisories, and vulnerability notes.

Cyber swachhta Kendra (botnet cleaning and malware analysis centre)

Launched by the Ministry of Electronics and Information Technology (MeitY), this initiative aims to create a secure cyberspace by detecting botnet infections and enabling citizens to clean their systems.

National cyber coordination centre (NCCC)

The NCCC is an operational cybersecurity and e-surveillance agency in India. It monitors the cyber traffic and communication metadata to identify threats and coordinate responses to counter cyber-attacks.

National cyber security policy (NCSP) 2013

The NCSP 2013 was India's first comprehensive policy document outlining the country's approach to cybersecurity. It emphasizes the need to protect information, build secure and resilient systems, and foster a culture of cybersecurity awareness.

Key Objectives

- To create a secure cyberspace ecosystem.
- To strengthen the regulatory framework.
- To develop capabilities for addressing threats and securing cyber infrastructure.
- To promote research, education, and public awareness.

Personal data protection bill (PDPB)

Though not enacted yet, the PDPB aims to regulate the collection, storage, and processing of personal data, ensuring individuals' privacy and data security. It mandates stringent requirements for data protection, data localization, and provides a framework for the protection of personal information.

Draft national cyber security strategy 2021

This draft policy outlines the next phase of India's cybersecurity approach, focusing on the need for a centralized and coordinated response to cyber threats, enhancing India's capacity to deal with cybercrimes, and fostering international cooperation.

Information technology (intermediary guidelines and digital media ethics code) rules, 2021

These rules impose greater responsibility on social media platforms and digital media entities to ensure the safety, security, and accountability of content online. They include provisions for addressing grievances, identifying the originator of unlawful content, and removing content that threatens national security.

Challenges and future directions

Despite these frameworks, India faces numerous challenges in cybersecurity, including the rapidly evolving nature of cyber threats, the shortage of skilled cybersecurity professionals, and the need for greater public-private collaboration. Moving forward, India's focus will likely be on strengthening its legal and regulatory frameworks, investing in cybersecurity infrastructure, enhancing international cooperation, and fostering a culture of cybersecurity awareness across all sectors.

In conclusion, India's cybersecurity systems and policies reflect a proactive approach to addressing the growing cyber threats. As digitalization continues to expand, these systems and policies will need to evolve to address emerging challenges and ensure the protection of India's digital assets.

Conclusion

India’s journey toward establishing a robust cybersecurity framework is a dynamic and ongoing process, driven by the need to protect its rapidly expanding digital economy and address the challenges posed by an increasingly complex and diverse cyber threat landscape. The development of comprehensive cybersecurity systems and policies is not just a response to current challenges but also a proactive measure to secure India’s digital future. As the country continues to embrace digital technologies, the importance of a resilient and adaptive cybersecurity framework cannot be overstated. This framework will be crucial in ensuring that India’s digital transformation is both safe and sustainable, allowing the nation to reap the full benefits of the digital age while mitigating the risks associated with it.

Recommendations

To improve the cyber security posture of the nation and its assets, a whole-of-nation approach must be followed. This requires a comprehensive national risk assessment in line with the criticality of Indian assets and capabilities of the adversaries. It must be done by engaging stakeholders and creating a trusted information-sharing mechanism.

A clear governance structure for organizations mandated with cybersecurity and cyber crisis management, with a proper mandate clarifying roles and responsibilities of different bodies, should be established to take stock of existing policies practices and capabilities.

Stakeholders Including different state and central government departments, law enforcement and even corporates should also be engaged through a wide consultation and information-sharing mechanism to create baseline security benchmarks, and test them by organizing regular security drills, thereby augmenting incident response capabilities.

The government must act as a facilitator and create a public-private partnership and lay adequate stress on user awareness and education. Most importantly, privacy and security should be balanced while handling cybercrime and fostering R&D to maintain a position of dominance in the cyberspace.

References

1. Aiyengar SRR. National Strategy for Cyberspace Security. New Delhi: KW Publisher, 2010.
2. Athavale D. “Cyberattacks on the Rise in India.” The Times of India, Pune, 2014.

3. Bamrara A, G Singh, M Bhatt. “Cyber Attacks and Defence Strategies in India: An Empirical Assessment of the Banking Sector.” International Journal of Cyber Criminology,2013:7(1):49–61.
4. Dilipraj E. “India’s Cyber Security 2013: A Review.” Centre for Air Power Studies,2013:97(14):1–4.
5. DSCI. Analysis of National Cyber Security Policy (NCSP–2013). New Delhi: Data Security Council of India, 2013.
6. Government of India. Discussion Draft on National Cyber Security Policy. New Delhi: DIETY, 2011.
7. Government of India. “National Telecom Policy (NTP) – 2012.” Ministry of Communication and Information Technology (NTP). New Delhi, 2012. http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final_0.pdf.
8. IANS. “69 Percent of Cyberattacks Targeted at Large Companies in India: Report.” Business Standard, New Delhi, 2014.
9. IDSA. India's Cyber Security Challenges. New Delhi: Institute of Defence Studies and Analyses, 2012.
10. ITU. Series-X: Data Networks Open System Communication and Security, Overview of Cybersecurity ITU-T X.1205, Geneva: ITU, 2009.
11. Joseph J. “India to Add Muscle to Its Cyber Arsenal.” Times of India, New Delhi, 2012.
12. Kaushik RK. “Cyber Security Needs Urgent Attention of Indian Government,” 2014. http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html.
13. Kumar AV, KK Pandey, DK Punia. Facing the Reality of Cyber-Threats in the Power Sector. Bangalore: Wipro Technologies, 2013.
14. Kumar R, N Mukherjee. Cyber Security in India: A Skill-Development Perspective. New Delhi: Communication Multimedia and Infrastructure, 2013.
15. Manoharan N. “India’s Internal Security Situation: Threats and Responses.” India Quarterly: A Journal of International Affairs,2013:69(4):367–381.
16. Patil PR, Bhosale DV. “Need to Understand Cyber Crime‟s Impact over National Security in India: A Case Study.” Online International Interdisciplinary Research Journal,2013:3(4):167–171.
17. Pillai P. “History of Internet Security.” http://www.buzzle.com/articles/history-of-internet-security.html.
18. Pubby M. “China Hackers Enter Navy Computers, Plant Bug to Extract Sensitive Data.” The Indian Express, New Delhi, 2012.
19. Reddy KS. “Anonymous Takes Down MTNL Website.” The Hindu, New Delhi, 2012.
20. Reich PC, ed. Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization. IGI Globa, 2012.
21. Shuran L, D Hui G Su. “Analyses and Discussions of the Blackout in Indian Power Grid.” Energy Science and Technology,2013:6(1):61–66.
22. Singh A. “Over 10,000 Email IDs Hit in ‘Worst’ Cyberattack.” The Indian Express. New Delhi, 2012.
23. Singh H, JT Philip “Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems.” Economic Times, New Delhi, 2010.