IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Evaluating The Effectiveness Of India's National Cyber Security Policy (2013) In The Era Of AI And Iot

Mr. Swapnil S. Kumare[*1]

[*1]Research Scholar, Department of Public Administration, Dr. Babasaheb Ambedkar Marathwada University, Chhatrapati Sambhajinagar, Maharashtra, India

Abstract

India's National Cyber Security Policy (NCSP) 2013 was a landmark initiative aiming to secure the nation's cyberspace. However, with the rapid proliferation of Artificial Intelligence (AI) and the Internet of Things (IoT), the policy faces unprecedented challenges. This paper evaluates the NCSP 2013's effectiveness in addressing contemporary cyber threats posed by AI-enabled systems and interconnected IoT devices. Through qualitative content analysis and comparative policy review with updated frameworks from the EU and USA, this paper finds that while NCSP 2013 laid foundational principles, it lacks adaptability to emerging technologies. The study concludes with targeted suggestions for policy renewal, enhanced institutional capacity, and public-private partnerships.

Keywords: Cybersecurity Policy, India, Artificial Intelligence, Internet of Things, National Cyber Security Policy 2013, Policy Evaluation, Emerging Technologies.

1. Introduction

Cybersecurity is now a cornerstone of national security due to increasing digitization. India's National Cyber Security Policy (NCSP) 2013 was introduced to create a secure and resilient cyberspace. However, this decade-old policy was framed in a pre-AI and pre-IoT era, making it increasingly obsolete in the face of evolving cyber threats.

Cybersecurity has emerged as an indispensable pillar of national security, especially in the context of rapid technological convergence and digital transformation. In the 21st century, governments, corporations, and individuals are increasingly reliant on interconnected digital platforms for critical operations, making cyberspace both a strategic asset and a battleground for sophisticated cyber threats (World Economic Forum, 2021). The Indian government, acknowledging the growing cyber threat landscape, introduced the National Cyber Security Policy (NCSP) in 2013 as a foundational framework to ensure a secure and resilient cyberspace. This policy sought to promote a culture of cybersecurity, protect critical information

infrastructure, encourage public-private collaboration, and enhance capacity building (Ministry of Electronics and Information Technology, 2013).

However, the NCSP 2013 was conceived in a technological environment that preceded the widespread integration of Artificial Intelligence (AI), Machine Learning (ML), and the Internet of Things (IoT). These technologies, while revolutionizing industries and public service delivery, have also introduced novel vulnerabilities such as autonomous decision-making risks, algorithmic manipulation, and hyperconnected attack surfaces (Rai, 2022). Unlike traditional cybersecurity concerns that focused on network security and malware defense, the new paradigm involves proactive threat intelligence, ethical AI regulation, and real-time response mechanisms. The policy, therefore, does not adequately address emerging cyber risks like AI-powered phishing, deepfake proliferation, and IoT-enabled surveillance breaches. This has rendered the NCSP 2013 increasingly obsolete and inadequate in the face of evolving cyber-physical threats, thereby necessitating a comprehensive policy overhaul aligned with current technological realities and international best practices (CERT-In, 2023; European Union Agency for Cybersecurity, 2019). Therefore, we have to study about policies.

1.2 Objectives of the Study

a. To assess the relevance and limitations of NCSP 2013 in the context of AI and IoT (MeitY, 2013; Rai, 2022).
b. To compare India's approach with global best practices (EU, USA) (ENISA, 2019; White House, 2023).
c. To provide policy recommendations for an updated cybersecurity framework (World Economic Forum, 2021).

2. Methodology

This research adopts a qualitative analytical method:
- Content Analysis of NCSP 2013
- Comparative Review of international frameworks like the US National Cybersecurity Strategy (2023) and EU's Cybersecurity Act (2019) (White House, 2023; ENISA, 2019).
- Secondary data from government reports (MeitY, CERT-In), international think tanks (WEF, ITU), and scholarly articles.

3. Detailed Policy Analysis

3.1 Key Features of NCSP 2013

- Securing cyberspace and critical information infrastructure
- Protection of personal data and privacy
- Capacity building and skill development
- Establishment of CERT-In and National Critical Information Infrastructure Protection Centre (NCIIPC)

4. Global Comparative Analysis

Country/Region	Policy/Framework	Key Features / Strategies
USA	National Cybersecurity Strategy (2023)	- 'Defend forward' strategy - Public-private intelligence sharing - AI threat modeling - IoT device certification
European Union	Cybersecurity Act (2019)	- Establishes ENISA (EU Agency for Cybersecurity) - Cybersecurity certification schemes for products/services
India (Lessons)	Takeaways from Global Frameworks	- Real-time threat response ecosystem - Legal framework for AI misuse - Centralized cybersecurity command structure

4.1 USA – National Cybersecurity Strategy (2023)

- Emphasis on 'defend forward' strategy and public-private intelligence sharing.
- Dedicated focus on AI threat modeling and IoT device certification.

4.2 European Union – Cybersecurity Act (2019)

- Establishes ENISA (European Union Agency for Cybersecurity).
- Introduces cybersecurity certification schemes for products and services.

4.3 Lessons for India

- Need for a real-time threat response ecosystem.
- Legal provisions to regulate AI misuse (e.g., algorithmic bias, facial recognition misuse).
- Institutional restructuring for centralized cybersecurity command.

5. Findings

- NCSP 2013 is outdated in technological terms; it lacks operational clarity in AI and IoT integration.
- The policy is too generic, lacking enforcement mechanisms and sector-specific strategies.
- India's cybercrime and digital forensics capabilities remain underdeveloped.
- Absence of a national AI Ethics Framework or IoT device standardization policy.

Challenges:

Issue	Policy Gap
Autonomous AI systems	No guidelines for AI ethics, deepfake prevention, or algorithmic accountability
IoT proliferation	Absence of device-level security standards or data-sharing protocols
Cyber Threat Intelligence	Limited integration with AI-enabled real-time detection tools
International Collaboration	No clear mandates on cross-border data flows or cyber diplomacy

6. Policy Recommendations

1. Formulate NCSP 2.0 with specific AI and IoT modules, including ethical guidelines(Rai, 2022).
2. Establish a Cybersecurity Regulatory Authority to oversee tech risk assessments and audits.
3. Introduce mandatory IoT security standards for manufacturing and import(ENISA, 2019).
4. Launch AI-powered threat detection systems at national and state levels.
5. Enhance cyber diplomacy to negotiate international treaties on AI weaponization and data flows(ITU, 2022, pp 56).
6. Public-Private Collaboration Models for cybersecurity R&D and capacity building.
7. Incorporate cybersecurity in school and university curriculum for foundational awareness.

7. Conclusion

India's cybersecurity landscape has undergone a radical transformation driven by increased internet penetration, digital governance initiatives, and the rapid deployment of emerging technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT). The scale, complexity, and frequency of cyberattacks have grown exponentially, affecting not just individual users, but also enterprises, public institutions, and critical infrastructure. Despite this evolution, India's existing cybersecurity policy framework, anchored in the 2013 document, has not adequately adapted to these emerging realities. The NCSP 2013, although visionary for its time, lacks comprehensive guidelines for contemporary challenges like algorithmic bias, AI-based misinformation, autonomous cyberweapons, and hyperconnected IoT ecosystems.

As a result, the policy proves insufficient both in scope and structural design, offering neither the enforcement mechanisms nor the dynamic regulatory tools required to tackle 21st-century cyber threats. It fails to provide sector-specific cyber norms, lacks robust incident response coordination, and does not include mechanisms for international cyber cooperation or AI governance. While NCSP 2013 successfully laid the foundational principles of cyber governance—such as the creation of institutional bodies like CERT-In and promotion of awareness and capacity building—it now needs to evolve into a more proactive, technology-aware, and future-resilient national strategy. To remain secure in the global digital ecosystem and to align with frameworks like the US National Cybersecurity Strategy (2023) or the EU's Cybersecurity Act (2019), India must undertake a comprehensive policy overhaul. This would involve drafting a new NCSP 2.0 that integrates AI ethics, IoT security, real-time cyber threat intelligence, and legal reform, thus fortifying India's position in global cyber diplomacy and digital resilience.

References:

CERT-In. (2023). Annual Report. Ministry of Electronics and Information Technology, Government of India.

Chakraborty, S. (2021). Urban Cyber Risk in India: Policy Void and Practical Risks. Indian Journal of Urban Affairs, 10(2), 34–48.

ENISA. (2019). Cybersecurity Act. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

European Union Agency for Cybersecurity. (2019). Cybersecurity Act. https://www.enisa.europa.eu/

ITU. (2022). Global Cybersecurity Index. International Telecommunication Union.

MeitY. (2013). National Cyber Security Policy. Government of India.

Ministry of Electronics and Information Technology. (2013). National Cyber Security Policy. Government of India.

Singh, V. (2020). IoT Regulation in India: Challenges and Opportunities. Cyber Law Review, 8(1), 67–85.

Ministry of Electronics and Information Technology. (2013). National Cyber Security Policy. Government of India.

Rai, S. (2022). AI and Cybersecurity: Regulatory Perspectives. Journal of Digital Policy, 11(3), 104–120.

White House. (2023). National Cybersecurity Strategy of the United States.

World Economic Forum. (2021). Global Cybersecurity Outlook.