iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67872

www.ijraset.com

Call: ☎08813907089 | E-mail ID: ijraset@gmail.com

Indian Cyber Security and Defence: A Comprehensive Analysis

S Sudhip[1], I Roshan Singha[2], Mohammad Atif[3]
School of Computer Science and Information Technology Jain-Deemed-To-Be University Bengaluru, India

Abstract: The rapid digitization of India's economy, governance, and military infrastructure has made cybersecurity a critical pillar of national security. With increasing cyber threats from state-sponsored actors, hacktivists, and cybercriminals, India has been actively strengthening its cyber defence mechanisms. This research paper provides an in-depth analysis of India's cybersecurity and defence policies, institutional frameworks, and operational strategies. It examines the roles of key agencies such as the Indian Computer Emergency Response Team (CERT-In), the National Cyber Security Coordinator (NCSC), and the Defence Cyber Agency (DCA). The paper also evaluates India's National Cyber Security Policy (2013) and the proposed National Cyber Security Strategy (2020), highlighting advancements and gaps. Additionally, the study explores India's international collaborations, challenges in cyber warfare, and future directions for enhancing cyber resilience. The findings suggest that while India has made significant progress, a more cohesive strategy, skilled workforce, and advanced cyber defence technologies are essential for safeguarding national interests in the digital age.

Keywords: Cybersecurity, Cyber Defence, Indian Defence Policy, CERT-In, NCSC, DCA, Cyber Warfare, National Security.

I. INTRODUCTION

The 21st century has witnessed an unprecedented expansion of cyberspace, transforming how nations operate economically, politically, and militarily. India, as one of the fastest-growing digital economies, faces escalating cyber threats ranging from espionage and financial fraud to cyber warfare and terrorism. The cyberattack on the Union Bank of India (2016), the power grid breach in Mumbai (2020), and recurring cyber intrusions in defence networks underscore the urgency of robust cybersecurity measures.

II. POLICY FRAMEWORK FOR CYBERSECURITY IN INDIA

A. *National Cyber Security Policy (2013)*

India's first structured cybersecurity policy, the NCSP 2013, aimed to create a secure digital ecosystem. Key provisions included:

- Establishing CERT-In as the nodal agency for cyber threat response.
- Promoting public-private partnerships for cybersecurity R&D.
- Encouraging best practices in IT infrastructure.
- Setting up the National Critical Information Infrastructure Protection Centre (NCIIPC).

B. *Draft National Cyber Security Strategy (2020)*

The proposed NCSS 2020 seeks to address gaps in the 2013 policy by emphasizing:

- Offensive Cyber Capabilities – Developing tools for cyber counterstrikes.
- Critical Infrastructure Protection – Mandating security audits for power grids, banking, and telecom sectors.
- Cyber Diplomacy – Strengthening collaborations with QUAD, ASEAN, and INTERPOL.
- Workforce Development – Expanding cybersecurity education through initiatives like "Cyber Surakshit Bharat."

III. INSTITUTIONAL FRAMEWORK FOR CYBER DEFENCE

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

Primary Role: National agency for cybersecurity incident response.

Functions:

- Monitoring cyber threats in real-time.
- Issuing advisories to government and private entities.

- Conducting cyber drills like “Cyber Swachhta Kendra.”

IV. FUTURE ROADMAP AND RECOMMENDATIONS

A. Strategic Enhancements Needed

- Unified Cyber Command: Merging CERT-In, DCA, and NCIIPC under a single authority.
- Cyber Defence Budget Increase: Allocating at least 10% of defence spending to cybersecurity.
- International Collaboration: Joining NATO’s Cooperative Cyber Defence Centre (CCDCOE).

B. Cybersecurity Landscape in India

India ranks among the top targets for cyber threats, with increasing incidents of cyber espionage, data breaches, and financial fraud. The 2021 Pegasus spyware scandal, the ransomware attacks on AIIMS in 2022, and persistent hacker activities targeting banking institutions indicate the evolving complexity of cyber threats. Additionally, the rise of state-sponsored cyber warfare has forced India to bolster its cyber defense mechanisms.

C. Impact of Cyber Threats on National Security

Cyber threats are no longer limited to financial fraud and data breaches; they have evolved into a direct challenge to national security. India's defense infrastructure, power grids, and communication systems are frequently targeted by advanced persistent threats (APTs). The 2020 Mumbai power grid failure, suspected to be linked to a cyberattack, underscores the vulnerabilities in critical infrastructure. Addressing these challenges requires an integrated approach that combines technology, policy, and human expertise.

D. Case Studies on Cyber Policy Implementation

Several countries have successfully implemented comprehensive cyber strategies that India can learn from. For example:

- The United States' Cybersecurity and Infrastructure Security Agency (CISA) actively coordinates between the government and private sectors, offering a model for public-private partnerships in cybersecurity.
- The European Union’s GDPR policy has strengthened data protection laws, which India aims to replicate with the forthcoming Data Protection Bill.
- Israel’s proactive approach in cybersecurity defense, with a dedicated National Cyber Directorate, demonstrates the effectiveness of centralizing cyber operations.

E. Challenges in Cyber Coordination

Despite the establishment of multiple cyber agencies, there exists fragmentation in coordination. The overlapping responsibilities between CERT-In, NCIIPC, and DCA often lead to inefficiencies. A more streamlined structure under a unified cyber command could enhance response times and improve intelligence sharing.

F. India’s Cyber Offensive Capabilities

While India has traditionally focused on cyber defense, there is increasing emphasis on offensive cyber capabilities. Reports suggest that the Defence Cyber Agency (DCA) is developing tools for cyber counterattacks, which could play a critical role in deterrence. The establishment of secure cyber intelligence hubs and AI-powered threat detection systems are steps in this direction.

G. Role of Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) is revolutionizing the cybersecurity landscape. Machine learning algorithms can identify anomalies in network traffic, predict cyber threats, and automate incident response. The integration of AI in India's cyber defense framework could significantly enhance threat detection capabilities.

H. Expanding Cybersecurity Workforce

India faces a severe shortage of cybersecurity professionals, with an estimated demand of over one million experts. To bridge this gap, initiatives like the ‘Cyber Shikshaa’ program and collaborations with academic institutions are crucial. Integrating cybersecurity courses into higher education curricula and offering specialized certifications could strengthen the talent pool.

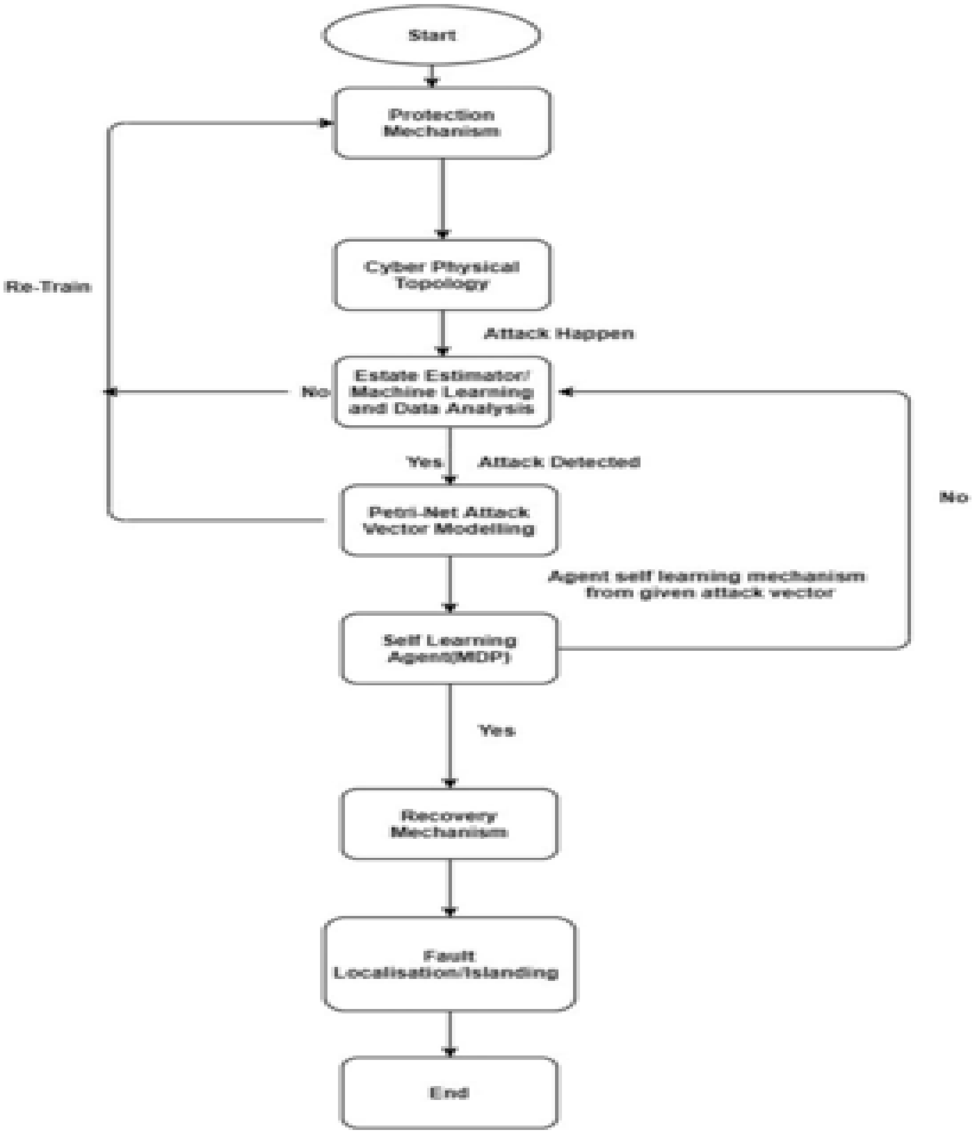

Start
Protection Mechanism
Re-Train
Cyber Physical Topology
Attack Happen
No
Estate Estimator/ Machine Learning and Data Analysis
Yes
Attack Detected
No
Petri-Net Attack Vector Modelling
Agent self learning mechanism from given attack vector
Self Learning Agent(MDP)
Yes
Recovery Mechanism
Fault Localisation/Islanding
End

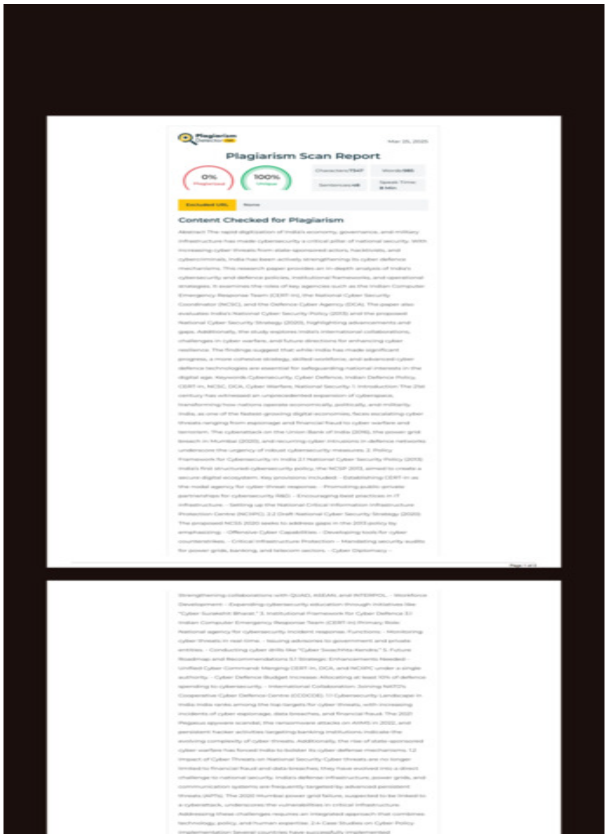
Fig: 1.1

V. CONCLUSION

India has made commendable progress in cybersecurity, but the evolving threat landscape demands a more proactive and integrated approach. Strengthening policy enforcement, enhancing military cyber capabilities, and fostering global partnerships will be crucial. The upcoming National Cyber Security Strategy (2020) must address these gaps to position India as a leader in cyber defence.

REFERENCES

[1] CERT-In, 'Annual Cyber Threat Report,' 2021.
[2] Government of India, 'National Cyber Security Policy,' 2013.
[3] Ministry of Defence, 'Defence Cyber Agency: Objectives and Functions,' 2019.
[4] CERT-In, "Annual Cyber Threat Report," Government of India, New Delhi, 2021.
[5] Government of India, "National Cyber Security Policy," Ministry of Electronics and Information Technology, New Delhi, 2013.
[6] Ministry of Defence, "Defence Cyber Agency: Objectives and Functions," Government of India, New Delhi, 2019.
[7] Cybersecurity and Infrastructure Security Agency, "Public-Private Partnerships in Cybersecurity," U.S. Department of Homeland Security, Washington, 2020.
[8] European Union, "General Data Protection Regulation (GDPR)," Official Journal of the European Union, 2016.
[9] Israel National Cyber Directorate, "Annual Cybersecurity Report," Government of Israel, Tel Aviv, 2022.
[10] National Institute of Standards and Technology, "Artificial Intelligence for Cybersecurity," NIST Special Publication, U.S. Department of Commerce, 2023.
[11] Ministry of Skill Development and Entrepreneurship, "Cybersecurity Workforce Development Strategy," Government of India, New Delhi, 2022.



Plagiarism Detector.net

Mar 25, 2025

Plagiarism Scan Report

0% Plagiarized

100% Unique

Characters:7547	Words:985
Sentences:48	Speak Time: 8 Min

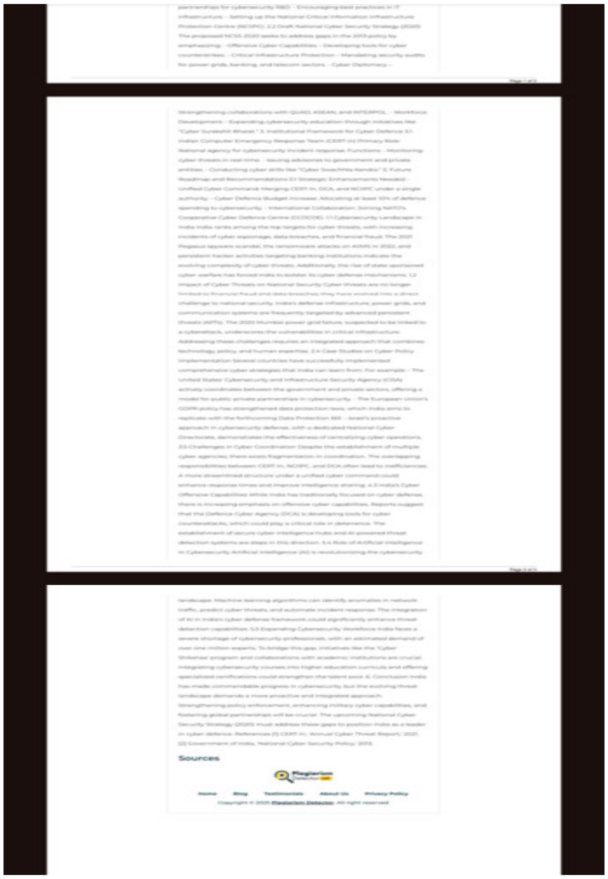
Excluded URL	None

Content Checked for Plagiarism

Abstract: The rapid digitization of India's economy, governance, and military infrastructure has made cybersecurity a critical pillar of national security. With increasing cyber threats from state-sponsored actors, hacktivists, and cybercriminals, India has been actively strengthening its cyber defence mechanisms. This research paper provides an in-depth analysis of India's cybersecurity and defence policies, institutional frameworks, and operational strategies. It examines the roles of key agencies such as the Indian Computer Emergency Response Team (CERT-In), the National Cyber Security Coordinator (NCSC), and the Defence Cyber Agency (DCA). The paper also evaluates India's National Cyber Security Policy (2013) and the proposed National Cyber Security Strategy (2020), highlighting advancements and gaps. Additionally, the study explores India's international collaborations, challenges in cyber warfare, and future directions for enhancing cyber resilience. The findings suggest that while India has made significant progress, a more cohesive strategy, skilled workforce, and advanced cyber defence technologies are essential for safeguarding national interests in the digital age. Keywords: Cybersecurity, Cyber Defence, Indian Defence Policy, CERT-In, NCSC, DCA, Cyber Warfare, National Security 1. Introduction The 21st century has witnessed an unprecedented expansion of cyberspace, transforming how nations operate economically, politically, and militarily. India, as one of the fastest-growing digital economies, faces escalating cyber threats ranging from espionage and financial fraud to cyber warfare and terrorism. The cyberattack on the Union Bank of India (2016), the power grid breach in Mumbai (2020), and recurring cyber intrusions in defence networks underscore the urgency of robust cybersecurity measures. 2. Policy Framework for Cybersecurity in India 2.1 National Cyber Security Policy (2013) India's first structured cybersecurity policy, the NCSP 2013, aimed to create a secure digital ecosystem. Key provisions included: - Establishing CERT-In as the nodal agency for cyber threat response. - Promoting public-private partnerships for cybersecurity R&D. - Encouraging best practices in IT infrastructure. - Setting up the National Critical Information Infrastructure Protection Centre (NCIIPC). 2.2 Draft National Cyber Security Strategy (2020) The proposed NCSS 2020 seeks to address gaps in the 2013 policy by emphasizing: - Offensive Cyber Capabilities - Developing tools for cyber counterstrikes. - Critical Infrastructure Protection – Mandating security audits for power grids, banking, and telecom sectors. - Cyber Diplomacy –

Page 1 of 3

Strengthening collaborations with QUAD, ASEAN, and INTERPOL. - Workforce Development - Expanding cybersecurity education through initiatives like "Cyber Surakshit Bharat." 3. Institutional Framework for Cyber Defence 3.1 Indian Computer Emergency Response Team (CERT-In) Primary Role: National agency for cybersecurity incident response. Functions: - Monitoring cyber threats in real-time. - Issuing advisories to government and private entities. - Conducting cyber drills like "Cyber Swachhta Kendra." 5. Future Roadmap and Recommendations 5.1 Strategic Enhancements Needed - Unified Cyber Command: Merging CERT-In, DCA, and NCIIPC under a single authority. - Cyber Defence Budget Increase: Allocating at least 10% of defence spending to cybersecurity. - International Collaboration: Joining NATO's Cooperative Cyber Defence Centre (CCDCOE). 1.1 Cybersecurity Landscape in India India ranks among the top targets for cyber threats, with increasing incidents of cyber espionage, data breaches, and financial fraud. The 2021 Pegasus spyware scandal, the ransomware attacks on AIIMS in 2022, and persistent hacker activities targeting banking institutions indicate the evolving complexity of cyber threats. Additionally, the rise of state-sponsored cyber warfare has forced India to bolster its cyber defense mechanisms. 1.2 Impact of Cyber Threats on National Security Cyber threats are no longer limited to financial fraud and data breaches; they have evolved into a direct challenge to national security. India's defense infrastructure, power grids, and communication systems are frequently targeted by advanced persistent threats (APTs). The 2020 Mumbai power grid failure, suspected to be linked to a cyberattack, underscores the vulnerabilities in critical infrastructure. Addressing these challenges requires an integrated approach that combines technology, policy, and human expertise. 2.4 Case Studies on Cyber Policy Implementation Several countries have successfully implemented



partnerships for cybersecurity R&D. - Encouraging best practices in IT infrastructure. - Setting up the National Critical Information Infrastructure Protection Centre (NCIIPC). 2.2 Draft National Cyber Security Strategy (2020) The proposed NCSS 2020 seeks to address gaps in the 2013 policy by emphasizing: - Offensive Cyber Capabilities - Developing tools for cyber counterstrikes. - Critical Infrastructure Protection – Mandating security audits for power grids, banking, and telecom sectors. - Cyber Diplomacy –

Page 1 of 3

Strengthening collaborations with QUAD, ASEAN, and INTERPOL. - Workforce Development - Expanding cybersecurity education through initiatives like "Cyber Surakshit Bharat." 3. Institutional Framework for Cyber Defence 3.1 Indian Computer Emergency Response Team (CERT-In) Primary Role: National agency for cybersecurity incident response. Functions: - Monitoring cyber threats in real-time. - Issuing advisories to government and private entities. - Conducting cyber drills like "Cyber Swachhta Kendra." 5. Future Roadmap and Recommendations 5.1 Strategic Enhancements Needed - Unified Cyber Command: Merging CERT-In, DCA, and NCIIPC under a single authority. - Cyber Defence Budget Increase: Allocating at least 10% of defence spending to cybersecurity. - International Collaboration: Joining NATO's Cooperative Cyber Defence Centre (CCDCOE). 1.1 Cybersecurity Landscape in India India ranks among the top targets for cyber threats, with increasing incidents of cyber espionage, data breaches, and financial fraud. The 2021 Pegasus spyware scandal, the ransomware attacks on AIIMS in 2022, and persistent hacker activities targeting banking institutions indicate the evolving complexity of cyber threats. Additionally, the rise of state-sponsored cyber warfare has forced India to bolster its cyber defense mechanisms. 1.2 Impact of Cyber Threats on National Security Cyber threats are no longer limited to financial fraud and data breaches; they have evolved into a direct challenge to national security. India's defense infrastructure, power grids, and communication systems are frequently targeted by advanced persistent threats (APTs). The 2020 Mumbai power grid failure, suspected to be linked to a cyberattack, underscores the vulnerabilities in critical infrastructure. Addressing these challenges requires an integrated approach that combines technology, policy, and human expertise. 2.4 Case Studies on Cyber Policy Implementation Several countries have successfully implemented comprehensive cyber strategies that India can learn from. For example: - The United States' Cybersecurity and Infrastructure Security Agency (CISA) actively coordinates between the government and private sectors, offering a model for public-private partnerships in cybersecurity. - The European Union's GDPR policy has strengthened data protection laws, which India aims to replicate with the forthcoming Data Protection Bill. - Israel's proactive approach in cybersecurity defense, with a dedicated National Cyber Directorate, demonstrates the effectiveness of centralizing cyber operations. 3.5 Challenges in Cyber Coordination Despite the establishment of multiple cyber agencies, there exists fragmentation in coordination. The overlapping responsibilities between CERT-In, NCIIPC, and DCA often lead to inefficiencies. A more streamlined structure under a unified cyber command could enhance response times and improve intelligence sharing. 4.3 India's Cyber Offensive Capabilities While India has traditionally focused on cyber defense, there is increasing emphasis on offensive cyber capabilities. Reports suggest that the Defence Cyber Agency (DCA) is developing tools for cyber counterattacks, which could play a critical role in deterrence. The establishment of secure cyber intelligence hubs and AI-powered threat detection systems are steps in this direction. 5.4 Role of Artificial Intelligence in Cybersecurity Artificial Intelligence (AI) is revolutionizing the cybersecurity

Page 2 of 3

landscape. Machine learning algorithms can identify anomalies in network traffic, predict cyber threats, and automate incident response. The integration of AI in India's cyber defense framework could significantly enhance threat detection capabilities. 5.5 Expanding Cybersecurity Workforce India faces a severe shortage of cybersecurity professionals, with an estimated demand of over one million experts. To bridge this gap, initiatives like the 'Cyber Shiksha' program and collaborations with academic institutions are crucial. Integrating cybersecurity courses into higher education curricula and offering specialized certifications could strengthen the talent pool. 6. Conclusion India has made commendable progress in cybersecurity, but the evolving threat landscape demands a more proactive and integrated approach. Strengthening policy enforcement, enhancing military cyber capabilities, and fostering global partnerships will be crucial. The upcoming National Cyber Security Strategy (2020) must address these gaps to position India as a leader in cyber defence. References [1] CERT-In, 'Annual Cyber Threat Report,' 2021. [2] Government of India, 'National Cyber Security Policy,' 2013.

Sources

Plagiarism Detector.net

Home Blog Testimonials About Us Privacy Policy

Copyright © 2025 Plagiarism Detector. All right reserved