FROM COORDINATION TO COMMAND

A STUDY OF INDIA'S DEFENCE CYBER AGENCY IN THE ERA OF CYBER WARFARE

Tanvi Anil Vedak
Department of Information and Cyber Security
Guru Nanak Khalsa College of Arts, Science & Commerce, Matunga East, Mumbai, Maharashtra 400019

Abstract: As of 2026, the nature of geopolitical conflict has increasingly shifted from traditional, kinetic warfare to operations in the digital domain, prompting a significant transformation in India's national security framework. This study explores the operational growth and strategic relevance of India's Defence Cyber Agency (DCyA). Initially established as a coordinating body, the agency has gradually evolved into a tri-service command with the capability to undertake a wide range of cyberspace operations, including both defensive and offensive measures. The paper further examines the role of the "Joint Doctrine for Cyberspace Operations (2025)" in shaping a more unified military cyber strategy, along with the adoption of indigenous technologies such as MayaOS to reduce reliance on external supply chains and enhance security.

Using a qualitative approach based on secondary data and recent examples of grey-zone conflicts, the research evaluates how effectively the DCyA integrates cyber operations across different military domains. The findings indicate that while the agency has improved coordination among the armed forces, issues such as shortage of skilled personnel and overlapping responsibilities with civilian cyber institutions remain key concerns. The study concludes by proposing a forward-looking framework focused on proactive cyber deterrence to strengthen India's digital sovereignty.

Keywords: DCyA, Cyber Warfare, Grey-Zone Warfare, MayaOS, Joint Doctrine, National Security, India, Defence Cyber Agency, Cyber Defence, Cyber Security, Information Warfare, Cyber Deterrence, Critical Infrastructure Protection, Cyber Threat Intelligence (CTI), Security Information and Event Management (SIEM), Artificial Intelligence in Cybersecurity, Military Cyber Operations, Network Centric Warfare, Digital Sovereignty, Cyber Resilience, Advanced Persistent Threats (APT), Multi-Domain Operations, Indigenous Technology, Cyber Strategy, Cyber Command, Information Assurance.

Chapter 1. Introduction

The nature of modern warfare has undergone a fundamental transformation, where conflicts are no longer initiated solely through visible military force but increasingly through covert actions in cyberspace. The opening phase of many contemporary conflicts is marked not by physical confrontation, but by the silent penetration of critical information infrastructure (CII), including power grids, communication networks, and defence systems. These cyber intrusions often remain undetected for extended periods, allowing adversaries to gather intelligence, disrupt operations, or prepare the ground for future escalation.

In the context of the Indo-Pacific region in 2026, India faces a complex and evolving cyber threat landscape. State-sponsored actors, particularly those employing Advanced Persistent Threats (APTs), have demonstrated the capability to conduct long-term, targeted cyber campaigns against strategic assets. These threats are not limited to military systems but extend to civilian infrastructure, creating a blurred boundary between war and peace. As a result, cyberspace has emerged as a critical domain of national security, demanding a

coordinated and forward-looking response.

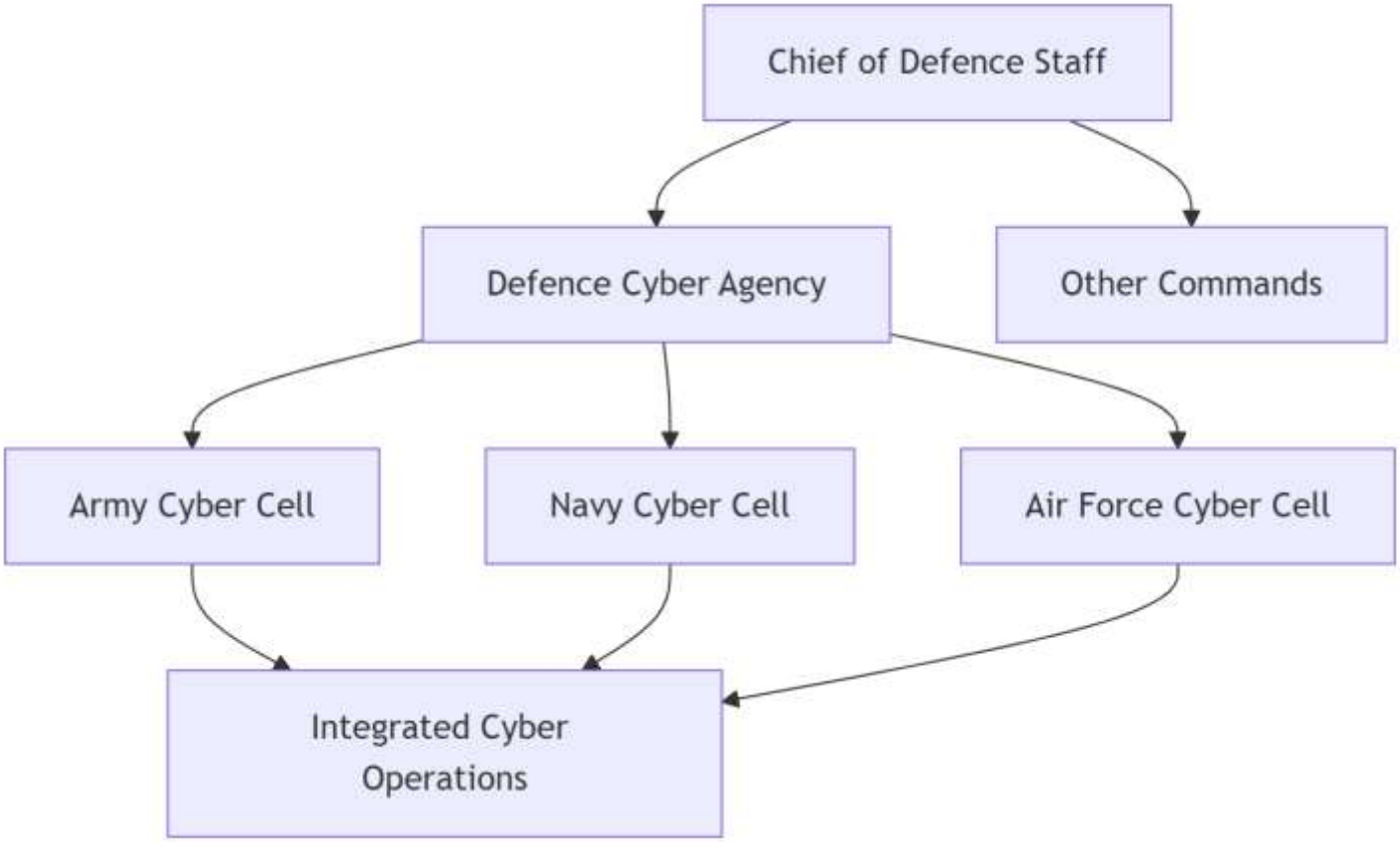


Fig. 1: Structure of DCyA

1.1 Background

The establishment of the Defence Cyber Agency (DCyA) represents India's strategic response to the growing importance of cyber warfare. Prior to its formation, cyber capabilities within the Indian armed forces were distributed across separate units within the Army, Navy, and Air Force. This fragmented approach often resulted in limited coordination, duplication of efforts, and inefficiencies in responding to complex cyber threats.

To address these challenges, the DCyA was conceptualized as a joint command structure, bringing together cyber resources and expertise from all three services under a unified framework. The objective was to enhance interoperability, streamline decision-making, and enable a more cohesive approach to cyber defence and operations. Over time, the agency has evolved beyond a coordinating body into a functional command capable of conducting both defensive and offensive cyber operations. This transition reflects a broader recognition within India's defence establishment that cyber capabilities are integral to modern military effectiveness.

1.2 Problem Statement

Despite the progress made through the establishment of the DCyA, significant challenges remain in adapting to the rapidly evolving nature of cyber threats. Traditional cybersecurity measures, which largely focus on perimeter defence and reactive responses, are increasingly inadequate in the face of sophisticated, AI-driven malware and autonomous attack systems. Adversaries are now leveraging artificial intelligence to develop more adaptive and resilient cyber tools, capable of bypassing conventional security mechanisms.

In this context, the DCyA faces the critical task of shifting from a purely defensive posture to a more proactive strategy often described as "active defence." This approach involves not only detecting and mitigating threats but also anticipating adversarial actions and, where necessary, engaging in pre-emptive or counter-offensive measures. However, the adoption of such strategies raises important legal and ethical considerations, particularly in relation to international norms governing state behaviour in cyberspace. Balancing operational effectiveness with adherence to these norms presents a complex challenge for policymakers and military planners alike.

1.3 Scope of the Study

This paper focuses on the evolution of the Defence Cyber Agency between 2021 and 226, a period marked by significant developments in both cyber threats and India's response mechanisms. The study examines the agency's organizational structure, its operational capabilities, and its role within the broader framework of national security.

Particular attention is given to the concept of a "whole-of-nation" approach to cybersecurity, which emphasizes coordination between military, governmental, and civilian stakeholders. In an era where cyber threats often target interconnected systems spanning multiple sectors, such an integrated approach is essential for effective defence. By analyzing the DCyA's role within this framework, the paper seeks to assess its contribution to enhancing India's cyber resilience and its preparedness to address future challenges in the digital domain.

The study of cyber warfare has gained significant attention in recent years, particularly as nations increasingly recognize cyberspace as a critical domain of conflict. This literature review is structured around three key pillars: the theoretical foundations of cyber warfare

within the framework of the Revolution in Military Affairs (RMA), the evolution of India's cyber defence architecture, and a comparative analysis of global cyber commands.

Chapter 2. Literature Review

2.1 Pillar 1: The Revolution in Military Affairs (RMA)

The concept of the Revolution in Military Affairs (RMA) refers to the transformative impact of technological innovation on the nature of warfare. Traditionally, warfare has been understood through classical theories, including those of Carl von Clausewitz, who introduced the idea of the "fog of war" to describe the uncertainty and unpredictability inherent in military operations. In the context of cyberspace, this concept has taken on new dimensions.

Unlike conventional battlefields, cyber operations are characterized by anonymity, speed, and a lack of physical boundaries. The "fog" in cyber warfare is intensified by difficulties in attribution, where identifying the source of an attack is often complex and time-consuming. This ambiguity allows adversaries to operate below the threshold of conventional warfare, making cyber conflict a preferred tool in grey-zone strategies.

Recent scholarship has also explored the growing linkage between cyber and kinetic operations, often referred to as "cyber-kinetic" integration. Studies suggest that cyber operations can act as force multipliers by disrupting enemy communication systems, disabling critical infrastructure, or influencing decision-making processes before or during physical engagements. For instance, cyber attacks on power grids or satellite systems can significantly weaken an adversary's operational capabilities without direct military confrontation. This evolving relationship underscores the need for integrated strategies that combine cyber and traditional military capabilities.

2.2 Pillar 2: The Indian Context

India's approach to cyber defence has evolved gradually, shaped by both internal assessments and external threat perceptions. The establishment of the Defence Cyber Agency (DCyA) can be traced back to recommendations made by key policy and defence reform committees.

The Naresh Chandra Task Force emphasized the importance of strengthening India's national security architecture through better coordination among the armed forces. It highlighted the need for specialized agencies to address emerging domains such as cyber and space.

Similarly, the Shekatkar Committee recommended significant reforms to enhance operational efficiency and reduce redundancies within the defence system. One of its key suggestions was the creation of integrated commands to improve jointness among the services. These recommendations played a crucial role in shaping the decision to establish the DCyA as a tri-service organization.

Prior to the formation of the DCyA, cyber capabilities within the Indian military were largely fragmented, with each service maintaining its own cyber units. This lack of integration limited the effectiveness of cyber operations and created challenges in coordination. The creation of the DCyA marked a shift towards a more unified and structured approach, enabling better resource utilization and strategic planning.

2.3 Pillar 3: Global Benchmarking

To understand the significance of India's Defence Cyber Agency, it is essential to compare it with similar organizations in other major powers. Globally, countries such as the United States and China have established dedicated cyber commands with distinct organizational models.

The United States Cyber Command operates as a unified combatant command with a strong emphasis on both offensive and defensive cyber operations. It benefits from significant resources, advanced technological capabilities, and close integration with intelligence agencies such as the NSA. This model reflects a highly centralized approach to cyber warfare, with a clear chain of command and defined operational roles.

In contrast, China's People's Liberation Army Strategic Support Force adopts a more integrated approach, combining cyber, electronic warfare, and space operations under a single entity. This structure enables China to conduct multi-domain operations with a high degree of coordination, reflecting its emphasis on informationized warfare.

India, however, has chosen a different path by adopting a functional command model for the DCyA rather than establishing a separate "Cyber Force." This approach allows for the integration of cyber capabilities within the existing military framework while maintaining flexibility and cost efficiency. Given India's unique strategic environment and resource constraints, this model enables gradual capability development without the need for extensive structural changes.

However, this approach also presents certain limitations. Compared to the more centralized models of the United States and China, the DCyA may face challenges in achieving the same level of operational autonomy and resource allocation. Nevertheless, it represents a pragmatic step toward strengthening India's cyber defence capabilities while aligning with its broader defence strategy.

Chapter 3. Objectives of the Study

The primary objective of this study is to critically examine the role and effectiveness of India's Defence Cyber Agency (DCyA) within the broader framework of national security and cyber warfare. As cyber threats continue to evolve in complexity and scale, it becomes essential to assess whether existing institutional structures and strategies are adequate to address these challenges.

Firstly, the study aims to evaluate the structural efficiency of the DCyA in promoting tri-service "jointness" among the Indian Army, Navy, and Air Force. Given that cyber operations often require seamless coordination across multiple domains, the ability of the DCyA to integrate resources, intelligence, and operational capabilities is a key area of analysis. This includes understanding how effectively the agency reduces inter-service silos and enhances unified decision-making.

Secondly, the research seeks to analyze the impact of the Joint Doctrine for Cyberspace Operations (2025) on India's overall cyber strategy. In particular, it focuses on how the doctrine influences the balance between defensive measures and offensive cyber capabilities. The study explores whether the doctrine enables a more proactive approach to cyber threats while remaining aligned with international norms and strategic priorities.

Finally, the study aims to identify the technological and infrastructural challenges that hinder the development of fully indigenous cyber defence systems. Despite ongoing efforts to promote self-reliance, dependence on foreign technologies and supply chains remains a concern. This objective examines existing gaps in research, development, and implementation, and highlights the need for strengthening domestic capabilities in cybersecurity.

In order to systematically evaluate the effectiveness and strategic relevance of India's Defence Cyber Agency (DCyA), this study proposes the following hypotheses. These hypotheses are designed to be tested through qualitative analysis of available data, case studies, and existing literature on cyber warfare and defence mechanisms.

Chapter 4. Hypotheses

H1: The transition from a service-specific cyber structure to a unified Defence Cyber Agency has significantly improved the speed and efficiency of India's response to cross-border cyber threats.

This hypothesis is based on the assumption that a centralized, tri-service framework enhances coordination and reduces delays that were previously caused by fragmented command structures. By integrating cyber capabilities across the Army, Navy, and Air Force, the DCyA is expected to facilitate quicker decision-making, better information sharing, and more effective incident response during cyber incursions.

H2: The implementation of indigenous software solutions, such as MayaOS, contributes to reducing vulnerabilities associated with foreign supply chains and strengthens national cyber resilience.

This hypothesis reflects the growing emphasis on technological self-reliance in India's defence sector. Dependence on external software systems can expose critical infrastructure to hidden backdoors or supply-chain attacks. The adoption of domestically developed platforms like MayaOS is therefore expected to act as a deterrent against such threats by ensuring greater control, transparency, and security within defence networks.

Chapter 5. Research Methodology

This study adopts a qualitative descriptive research design to examine the structure, evolution, and operational effectiveness of India's Defence Cyber Agency (DCyA). A qualitative approach is considered appropriate for this research as it allows for an in-depth understanding of institutional frameworks, policy developments, and strategic responses in the domain of cyber warfare. Rather than relying on numerical data alone, the study focuses on interpreting patterns, trends, and insights derived from authoritative sources.

5.1 Data Sources

The research is primarily based on secondary data, collected from credible and publicly available sources. Key sources include official press releases and publications from the Ministry of Defence (MoD), which provide insights into policy decisions, operational developments, and strategic priorities related to cyber defence. In addition, reports from the Parliamentary Standing Committee on Defence (2024–2026) have been analyzed to understand government perspectives, budget allocations, and institutional challenges associated with the DCyA.

Another important source is the Joint Doctrine for Cyberspace Operations (2025), which outlines India's strategic approach to cyber warfare. This document serves as a foundational reference for understanding the doctrinal shift towards integrated and proactive cyber operations. Supplementary information has been gathered from academic journals, policy papers, and reputable cybersecurity reports to provide a broader analytical context.

5.2 Research Tools and Techniques

To enhance the depth of analysis, the study incorporates Open-Source Intelligence (OSINT) tools and bibliometric analysis techniques. OSINT tools are used to collect and examine publicly available data related to cyber incidents, threat actors, and

vulnerabilities affecting Indian defence infrastructure. These tools enable the identification of patterns in cyber attacks, particularly those associated with Advanced Persistent Threats (APTs).

Bibliometric analysis is employed to track trends in cybersecurity research and reporting over a five-year period. By analyzing the frequency, sources, and thematic focus of published material, the study gains insights into the evolving nature and sophistication of cyber threats targeting India. This approach also helps in identifying gaps in existing research and areas that require further investigation.

5.3 Analytical Approach

The collected data is analyzed using a descriptive and interpretative framework, focusing on identifying key themes such as institutional efficiency, technological capability, and strategic preparedness. Case-based analysis is also used to examine specific cyber incidents and their implications for national security. This multi-layered approach ensures a comprehensive understanding of the DCyA's role within India's cyber defence ecosystem.

5.4 Limitations of the Study

While the study relies on credible sources, it is important to acknowledge certain limitations. Due to the sensitive nature of defence-related information, access to classified data is restricted, which may limit the scope of analysis. Additionally, cyber incidents are often underreported or attributed with uncertainty, making it challenging to establish definitive conclusions in some cases.

Chapter 6. Technology Analysis

The effectiveness of any modern cyber defence organization depends largely on the technologies it deploys and its ability to adapt to evolving threats. In the case of India's Defence Cyber Agency (DCyA), the current technical posture reflects a gradual shift towards self-reliance, predictive security, and secure communication frameworks. Three key technological developments—MayaOS, Chakravyuha, and Quantum Key Distribution (QKD)—illustrate this transition and highlight the agency's focus on strengthening cyber resilience.

6.1 MayaOS: Towards Indigenous Operating Systems

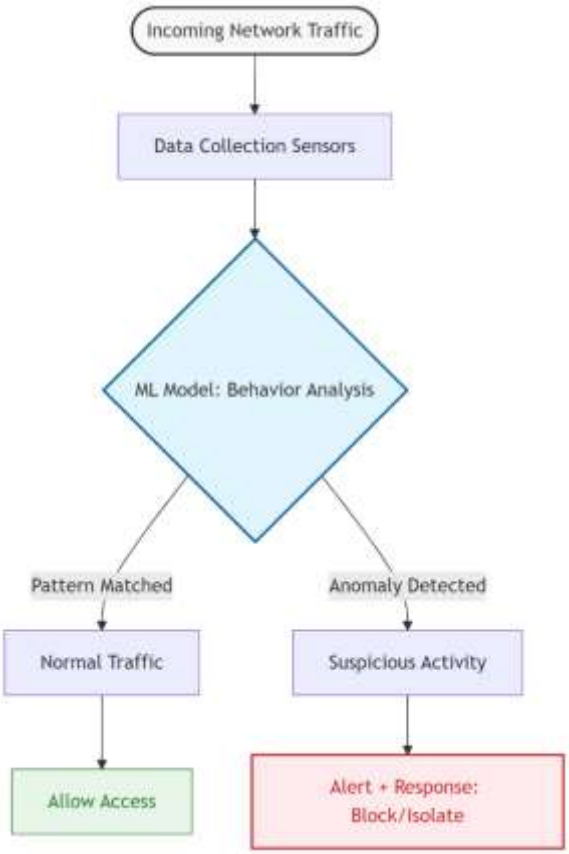
One of the major steps taken by the DCyA is the adoption of MayaOS, an indigenously developed operating system based on the Ubuntu platform. The primary objective behind this transition is to reduce dependence on foreign software, particularly widely used commercial operating systems, which may pose potential security risks. In defence environments, even a minor vulnerability or hidden backdoor can have serious consequences, including unauthorized access to sensitive data or disruption of critical operations.

By deploying MayaOS across military networks, the DCyA aims to establish greater control over system architecture, security updates, and data integrity. An indigenous operating system allows for customized security configurations tailored to defence requirements, thereby minimizing exposure to external threats. Although the transition involves challenges such as compatibility and user adaptation, it represents an important step toward achieving technological sovereignty in cybersecurity.

6.2 Chakravyuha: AI-Driven Threat Detection

Another significant development is Chakravyuha, an artificial intelligence-based Endpoint Detection and Response (EDR) system. Traditional cybersecurity tools often rely on known threat signatures, which limits their ability to detect new or previously unseen attacks. In contrast, Chakravyuha leverages machine learning algorithms to identify abnormal patterns in network behavior, enabling it to detect potential threats at an early stage.

This system is particularly relevant in addressing zero-day vulnerabilities, which are exploited before developers can issue patches or updates. By continuously analyzing data and learning from evolving attack patterns, Chakravyuha enhances the DCyA's ability to move from reactive defence to predictive security. This shift is crucial in modern cyber warfare, where attackers frequently use advanced techniques to bypass conventional security measures.



6.3 Quantum Key Distribution (QKD): Securing Communication Channels

Secure communication is a critical component of military operations, especially in scenarios where command and control systems must remain operational under all circumstances. To address this need, the DCyA has begun exploring the use of Quantum Key Distribution (QKD) for establishing highly secure communication links between New Delhi and various command headquarters.

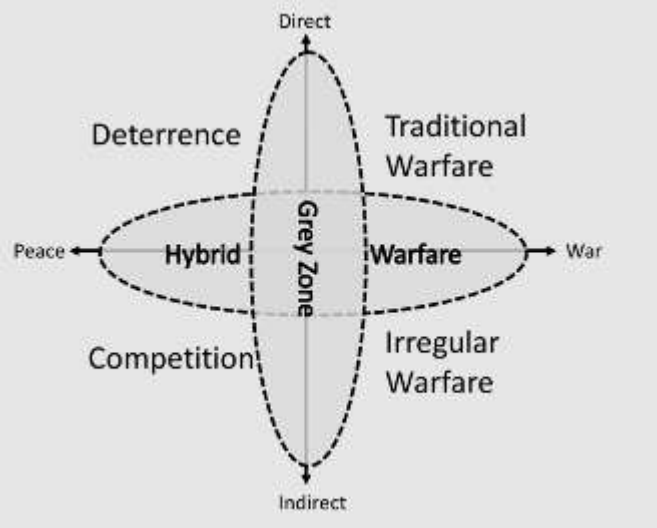
QKD uses principles of quantum mechanics to generate encryption keys that are theoretically immune to interception or decryption. Any attempt to eavesdrop on the communication alters the quantum state of the transmitted data, immediately alerting the system to a potential breach. This makes QKD a promising solution for protecting sensitive military communications against both current and future threats, including those posed by quantum computing.

6.4 Overall Assessment

Together, these technological initiatives reflect a broader strategic shift within the DCyA toward proactive, resilient, and indigenous cyber defence mechanisms. While each technology addresses a specific aspect of cybersecurity—system integrity, threat detection, and secure communication—their combined implementation strengthens the overall defence ecosystem. However, successful deployment will depend on continuous investment, skilled personnel, and effective integration across different operational layers.

Chapter 7. Data Analysis and Findings

The analysis of available data and recent cyber defence exercises provides important insights into the operational effectiveness of India's Defence Cyber Agency (DCyA). By examining simulated exercises, real-world incidents, and strategic trends, this section highlights key findings related to the agency's performance, existing gaps, and evolving deterrence capabilities.



7.1 Finding 1: Tactical Success in Exercise Cyber Suraksha

One of the most notable indicators of the DCyA's growing capability is its performance in joint cyber defence exercises such as Cyber Suraksha (2025). Data from this exercise suggests a significant improvement in threat detection and response efficiency, with approximately a 40% increase in successful identification of adversarial activities during Red Team simulations.

This improvement reflects enhanced coordination between different service branches and better utilization of advanced monitoring tools. The use of simulated attack scenarios allows the agency to test its preparedness against sophisticated threats, including multi-layered intrusions and stealth-based malware. The observed increase in detection rates indicates that the DCyA is gradually transitioning from a reactive approach to a more proactive and intelligence-driven defence posture. It also demonstrates the effectiveness of continuous training and integration of modern cybersecurity tools in strengthening operational readiness.

7.2 Finding 2: The Grey-Zone Gap

Despite these advancements, the analysis reveals a critical vulnerability in the form of a "grey-zone gap," particularly in the interface between military and civilian cyber infrastructure. Incidents and threat assessments related to the 2025 power grid disturbances highlight the challenges associated with protecting interconnected systems that span both defence and civilian domains.

While the DCyA has developed robust mechanisms to secure military networks, the broader national infrastructure—such as energy, telecommunications, and transportation—often involves multiple stakeholders, including private entities and civilian agencies. The lack of seamless coordination and standardized security protocols across these sectors creates potential entry points for adversaries. This gap is especially significant in grey-zone conflicts, where attackers deliberately operate below the threshold of open warfare to exploit systemic weaknesses without triggering a conventional response.

7.3 Finding 3: Deterrence by Denial

Another important finding relates to the concept of "deterrence by denial," wherein the cost and complexity of executing successful cyber-attacks are increased to discourage adversaries. The DCyA has adopted strategies such as the deployment of honeypots, which are decoy systems designed to attract and monitor malicious actors. These systems not only help in identifying attack patterns but also provide valuable intelligence on adversary tactics, techniques, and procedures.

As a result, attackers are forced to invest more time and resources while facing a higher risk of detection. This shift alters the cost-benefit calculation for adversaries, making cyber-attacks on Indian military infrastructure less attractive. Although deterrence in cyberspace is inherently complex and difficult to quantify, the growing sophistication of defensive measures suggests that the DCyA is contributing to a more secure and resilient cyber environment.

7.4 Overall Interpretation

Overall, the data indicates that the DCyA has made meaningful progress in enhancing India's cyber defence capabilities, particularly in terms of operational readiness and threat detection. However, the persistence of coordination challenges and the evolving nature of cyber threats underscore the need for continuous improvement. Strengthening collaboration between military and civilian sectors, along with further investment in advanced technologies, will be essential for sustaining and expanding these gains.

Chapter 8. Challenges

Despite notable progress in strengthening India's cyber defence posture, the Defence Cyber Agency (DCyA) continues to face several structural, technological, and legal challenges. These issues not only affect its operational efficiency but also influence its long-term strategic effectiveness in an increasingly complex cyber threat environment.

8.1 Human Capital Constraints

One of the most pressing challenges for the DCyA is the shortage and retention of skilled cybersecurity professionals. The rapid expansion of the global technology sector has created intense competition for talent, often resulting in a "brain drain" from government and defence institutions to private corporations. Skilled experts in areas such as artificial intelligence, malware analysis, and cyber forensics are frequently attracted by higher salaries, better working conditions, and more flexible career opportunities in the private sector.

This talent gap can limit the DCyA's ability to develop and maintain advanced cyber capabilities. While training programs and recruitment initiatives are being introduced, retaining experienced personnel remains a significant concern. Addressing this issue requires not only competitive incentives but also the creation of a dynamic and research-oriented work environment within defence organizations.

8.2 Legal and Policy Challenges

Cyber operations operate in a domain that is still largely unregulated at the global level. The absence of a universally accepted international "cyber treaty" creates ambiguity in defining norms, responsibilities, and acceptable responses to cyber attacks. This legal vacuum complicates the process of attributing attacks to specific actors, particularly when adversaries use sophisticated techniques to mask their identity.

For the DCyA, this lack of clear legal frameworks poses challenges in determining the scope and limits of offensive cyber operations. Retaliatory actions must be carefully calibrated to avoid escalation or violation of international law. Additionally, differences in national policies and the absence of standardized protocols make international cooperation in cyber defence more difficult.

8.3 Integration with Legacy Systems

Another major challenge lies in the integration of modern cybersecurity solutions with existing legacy infrastructure within the armed forces. Many systems currently in use, particularly in naval and air-force operations, were developed decades ago and were not designed with contemporary cyber threats in mind. These older systems may lack basic security features, making them more vulnerable to exploitation.

Upgrading or replacing such infrastructure is often a complex and resource-intensive process. Compatibility issues between new technologies and older hardware can hinder seamless implementation of advanced cyber defence protocols. Moreover, operational constraints may limit the ability to take critical systems offline for upgrades or testing. As a result, the DCyA must find ways to secure these legacy systems while gradually transitioning to more modern and resilient architectures.

8.4 Overall Assessment

These challenges highlight the multifaceted nature of cyber defence, where technological advancements must be supported by strong human resources and clear policy frameworks. While the DCyA has made significant strides, addressing these issues will be essential to ensure sustained effectiveness in the face of evolving cyber threats.

Chapter 9. Future Study and Conclusion

9.1 Future Scope for Research

While this study provides a comprehensive understanding of the structure and functioning of India's Defence Cyber Agency (DCyA), several important areas remain open for further research. One significant direction is the ethical and strategic implications of autonomous cyber weapons. As artificial intelligence continues to be integrated into cyber operations, questions arise regarding accountability, control, and the potential risks of unintended escalation. Future research can explore how international norms and domestic policies can address these concerns while balancing innovation with responsibility.

Another emerging area is the role of private actors, often referred to as "cyber mercenaries," in regional and global conflicts. In the South Asian context, the involvement of private cybersecurity firms, hacktivist groups, and state-sponsored non-state actors is becoming increasingly visible. Understanding their influence on cyber warfare dynamics, attribution challenges, and escalation patterns can provide valuable insights for policymakers and defence planners.

Additionally, future studies can examine the long-term impact of indigenous technologies on India's cyber resilience, as well as the effectiveness of public-private partnerships in strengthening national cybersecurity frameworks. Comparative studies involving other nations may also help in identifying best practices and areas for improvement.

9.2 Conclusion

In the contemporary security environment, cyber capabilities have become an essential pillar of national defence rather than an optional enhancement. The establishment and evolution of the Defence Cyber Agency (DCyA) reflect India's recognition of this shift. By 2026, the agency has made considerable progress in integrating the cyber capabilities of the Army, Navy, and Air Force into a unified structure, thereby enhancing coordination, efficiency, and operational readiness.

However, the journey toward achieving true "cyber self-reliance" is still ongoing. Challenges related to technological dependence, talent retention, and institutional coordination continue to require sustained attention. In particular, the development and deployment of indigenous solutions must be supported by consistent funding, policy support, and a robust research ecosystem.

Furthermore, the absence of a comprehensive and rapidly evolving legislative framework poses limitations on the scope and effectiveness of cyber operations. Strengthening legal and policy mechanisms will be crucial for enabling timely responses and ensuring accountability in cyberspace.

Looking ahead, the DCyA must move beyond a primarily defensive role and position itself as a proactive and innovative force in the global cyber domain. Transitioning from a "gatekeeper" that focuses on protection to a "trendsetter" that shapes cyber strategy and norms will be key to maintaining strategic advantage. In doing so, the agency can play a central role in safeguarding India's digital sovereignty and contributing to stability in the broader international cyber environment.

Chapter 10. References

Ministry of Defence. (2025). Joint Doctrine for Cyberspace Operations. Government of India.

This official doctrine outlines India's strategic vision for conducting cyber operations, emphasizing jointness among the armed forces and the integration of offensive and defensive cyber capabilities.

Press Information Bureau (PIB), Government of India. (2024). Implementation of MayaOS across Defence Networks.

This report provides details on the adoption of indigenous operating systems within defence infrastructure, highlighting efforts toward technological self-reliance and secure digital ecosystems.

Singh, A. (2026). The new frontier: India's digital command. Journal of Strategic Studies, 44(2), 215–232.

This article examines the evolution of India's cyber command structure and analyzes the strategic importance of digital warfare in modern military planning.

Parliamentary Standing Committee on Defence. (2025). Report on Cyber Preparedness of the Armed Forces. Government of India.

This report evaluates the readiness of India's defence forces in handling cyber threats and provides recommendations for improving institutional coordination and infrastructure.

Kshetri, N. (2022). Cybersecurity in India: Regulations, governance, and challenges. Telecommunications Policy, 46(3), 102–118.

This paper discusses the broader cybersecurity landscape in India, including regulatory frameworks and the challenges associated with securing critical infrastructure.

Tikk, E., Kaska, K., & Vihul, L. (2010). International Cyber Incidents: Legal Considerations. NATO Cooperative Cyber Defence Centre of Excellence.

This work explores legal aspects of cyber warfare and provides a framework for understanding international norms and challenges in cyber conflict attribution.

Bajpai, K., & Mattoo, A. (2019). The Peacock and the Dragon: India-China Relations in the 21st Century. Oxford University Press.

This book provides context for India-China strategic competition, including the growing importance of cyber capabilities in bilateral tensions.

Maurer, T. (2018). Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press.

This book analyzes the role of non-state actors in cyber conflicts and their implications for national security and international stability.