



2025

Defending the Digital Battlefield: Indian Army Role in Cybersecurity and Cyber Law

Basil Raju and Jyotirmoy Banerjee

Recommended Citation

Basil Raju and Jyotirmoy Banerjee, *Defending the Digital Battlefield: Indian Army Role in Cybersecurity and Cyber Law*, 4 IJHRLR 249-259 (2025).
Available at www.humanrightlawreview.in/archives/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto Media and Publications administrator. For more information, please contact info@humanrightlawreview.in.

Defending the Digital Battlefield: Indian Army Role in Cybersecurity and Cyber Law

Basil Raju and Jyotirmoy Banerjee

LLM Student, Amity Law School, Amity University, Bengaluru
Assistant Professor, Amity Law School, Amity University, Bengaluru

Manuscript Received
08 Jan. 2025

Manuscript Accepted
11 Jan. 2025

Manuscript Published
14 Jan. 2025

ABSTRACT

In the digital age, cybersecurity has emerged as a cornerstone of national security, transcending its traditional role in corporate defence. The Indian Defence Army recognizes this criticality and has undertaken significant measures to strengthen its cybersecurity framework. This paper examines the multifaceted role of the Indian Army in ensuring cyber resilience, with a focus on protecting networks, securing national infrastructure, and conducting both defensive and offensive cyber operations. Central to these efforts is the establishment of the Defence Cyber Agency, a tri-services entity dedicated to managing and mitigating cyber threats. The Army's initiatives extend to collaborations with government and private entities to safeguard critical infrastructure, such as power grids, transportation systems, and communication networks, from potential disruptions. Acknowledging the growing significance of cyberspace in modern warfare, the Indian Army established the Army Cyber Command (ACC) in 2018. Tasked with protecting military communication systems and developing offensive cyber capabilities, the ACC represents a proactive approach to countering enemy threats. High-profile cyberattacks on India's defense sector have accelerated the development of indigenous systems, spearheaded by the Defence Research and Development Organisation (DRDO). The Army also actively contributes to the enforcement of cybersecurity laws, working with agencies under the Information Technology Act of 2000 and the Cyber Crime Coordination Centre (4C). These collaborations ensure legal compliance and enhance national cybersecurity awareness. Despite notable advancements, challenges remain, including a rapidly

evolving threat landscape and a shortage of skilled cybersecurity professionals. To address these issues, the Army continues to invest in training, education, and expanding its cyber warfare capabilities. Integrating cybersecurity into India's broader military strategy is imperative to counter both traditional and emerging threats, ensuring the nation's preparedness for future cyber warfare challenges.

KEYWORDS

Indian Defense, Digital, Cybersecurity, Cyber Threats

INTRODUCTION

The Indian Defence Army plays a vital role in cybersecurity, protecting the nation's critical infrastructure and sensitive information from cyber threats. In today's digital age, cybersecurity is no longer just a concern for the private sector it's a matter of national security. The Indian Army has recognized this threat and has taken proactive measures to strengthen its cybersecurity capabilities¹. The Indian Army's role in cybersecurity is multifaceted. Firstly, it's responsible for protecting its own networks and systems from cyber-attacks. This includes implementing robust security measures, conducting regular vulnerability assessments, and providing cybersecurity training to its personnel. The Army has established the Defence Cyber Agency (DCA), an integrated tri-services agency responsible for handling cybersecurity threats¹.

Secondly, the Indian Army plays a crucial role in protecting the nation's critical infrastructure, such as power grids, transportation systems, and communication networks. These infrastructures are vulnerable to cyber-attacks, which could have devastating consequences for national security and economic stability. The Army works closely with other government agencies and private sector organizations to identify and mitigate potential cyber threats.

Thirdly, the Indian Army is involved in cybersecurity operations, including cyber intelligence gathering, cyber warfare, and cyber diplomacy. The Army has established a dedicated cyber warfare unit, which is responsible for conducting cyber operations against enemy forces. The Army also engages in cyber diplomacy

¹ ET Gov., *Ability to Wage Cyber War Best Defence against Cyber Attacks from State Level Adversaries - ET Government*, ETGovernment.com, <https://government.economictimes.indiatimes.com/news/secure-india/ability-to-wage-cyber-war-best-defence-against-cyber-attacks-from-state-level-adversaries/100927158> (last visited Jan 2, 2025).

efforts, working with international partners to promote cybersecurity cooperation and develop common standards for cybersecurity.

DEFENCE AND CYBERSECURITY

The present-day theatre of conflict has significantly evolved, transforming the traditional route of physical confrontations into a multifaceted landscape where strategies go beyond mere direct clashes. In the modern era, warfare has become increasingly complex, incorporating a variety of techniques that target an adversary from a distance. These strategies include covert infiltration, psychological warfare, hybrid, and, notably, cyberwarfare.

Among these, cyberwarfare has emerged as an especially potent tool. It has the ability not only to degrade military readiness but also to destabilize the capacity to mobilize forces, highlighting the vulnerability of nations in the digital age². This new paradigm underscores the urgent need for nations, especially India, to reassess their military preparedness in the face of evolving threats, particularly in the realm of cybersecurity.

India, with its vast defense infrastructure and one of the world's largest armed forces, has long been focused on modernizing its military capabilities. The country has invested heavily in upgrading weapon platforms, strengthening infrastructure, and enhancing communication, intelligence, surveillance, and reconnaissance (ISR) systems³. While these efforts have been instrumental in bolstering India's military might, the modern threat landscape requires a shift in focus. The growing prominence of cyber threats, especially from adversaries like China and Pakistan, demands that India not only continue its physical military advancements but also prioritize the development of robust cyber defense mechanisms. Cyberattacks can have devastating consequences, and India's strategic posture is vulnerable unless it develops a formidable cyber defense to

² Cyber Warfare Has Emerged as The Fifth Domain of Warfare, Presenting Unique Challenges to National Security and International Relations. In Light of this, Explain the Concept of Cyber Warfare and Discuss Its Key Features That Distinguish It from Traditional Forms of Conflict - <https://pwnlyias.com/mains-answer-writing/cyber-warfare-has-emerged-as-the-fifth-domain-of-warfare-presenting-unique-challenges-to-national-security-and-international-relations-in-light-of-this-explain-the-concept-of-cyber-warfare-and-disc-2/> (last visited Jan 2, 2025).

³ Shibra Arshad, *Advanced Weapons Added to Military, India Strengthens Power*, Bharat Express (Jan. 1, 2025), <https://english.bharatexpress.com/india/india-strengthens-military-power-in-2024-with-advanced-weapons-184727> (last visited Jan 2, 2025).

complement its conventional military strength.

The importance of cybersecurity has become all the more apparent following a series of high-profile cyberattacks targeting India's defense sector. In 2012, a cyberattack on the Indian Navy's Eastern Command systems demonstrated the vulnerability of India's defense infrastructure to sophisticated cyber threats⁴. The attack, which involved the infection of naval computers overseeing sensitive operations like ballistic missile submarines and maritime activities in the South China Sea, resulted in the theft of classified documents and the transmission of this data to foreign IP addresses. This attack, believed to have originated from China, was just one of many that have targeted Indian defense institutions over the years.

Similar cyber intrusions have also been reported against the Indian Air Force, the National Security Agency (NSA), and other government agencies, with sensitive data being compromised in numerous instances⁵. For instance, in 2010, hackers infiltrated the NSA and the Indian Air Force, stealing classified files and documents⁶. That same year, a massive cyberattack compromised more than 10,000 email addresses of top government officials, including those in the military, the Prime Minister's Office, and key ministries. These incidents underscore the vulnerabilities within India's defense sector and the need for a comprehensive cyber defense strategy.

The nature of these cyberattacks reveals that they are not merely technical breaches but are deeply intertwined with broader geopolitical and economic interests. These cyber intrusions are often motivated by political or economic agendas, with the intent of weakening national security, destabilizing the country, or gaining access to sensitive information. As such, the stakes are much higher, and the potential consequences of these attacks go far beyond simple data theft. A successful cyberattack can cripple a nation's defense systems, sabotage its military readiness, and even jeopardize public safety. The evolving nature of these cyber threats becoming more advanced, frequent, and harder to detect makes it increasingly difficult for traditional defense systems to

⁴ Indian Navy investigates cyber-attack on military PCs, BBC News, Jul. 4, 2012, <https://www.bbc.com/news/technology-18703508> (last visited Jan 2, 2025).

⁵ What is the NSA and how does it work? Search Security, <https://www.techtarget.com/searchsecurity/definition/National-Security-Agency> (last visited Jan 2, 2025).

⁶ National Security Issues in Cyberspace, <http://legalserviceindia.com/legal/article-7497-national-security-issues-in-cyberspace.html> (last visited Jan 2, 2025).

address them effectively⁷

Given these evolving threats, it is crucial that India develops a strategic cyber defense environment that can respond to cyber incidents in real time. This would involve not only protecting its military assets but also ensuring a robust incident response capability that can quickly detect, mitigate, and recover from cyberattacks. The Indian government has recognized the importance of this and has been taking steps to enhance its cybersecurity posture. For instance, India's Defense Research and Development Organization (DRDO) has collaborated with premier institutions to develop an indigenous operating system in response to concerns about reliance on foreign systems, which could be vulnerable to cyberattacks. This initiative reflects India's growing awareness of the need to safeguard its technological assets in the face of increasing cyber threats⁸.

Despite these efforts, significant challenges remain in strengthening India's cyber defense capabilities. One of the key issues is the persistence of zero-day vulnerabilities undiscovered weaknesses in software that can be exploited by cybercriminals and hackers. These vulnerabilities can expose India's weapon platforms, communication networks, and other critical military resources to cyber threats. While substantial investments have been made in upgrading India's military infrastructure, cybersecurity remains a weak link that could undermine the effectiveness of the country's military capabilities.

Furthermore, India's defense sector is vast and spread across diverse regions, which makes it particularly vulnerable to cyberattacks. Protecting all divisions of the military from cyber threats requires a coordinated and systematic approach to cybersecurity. It is not enough to have isolated defense mechanisms in place; India must develop an integrated cybersecurity strategy that spans all branches of its military and other government institutions. This would require substantial investment in both human resources—skilled cybersecurity professionals—and technology, as well as collaboration with international partners to share knowledge and best practices in

⁷ Understanding Cyber Warfare and Its Implications for Indian Armed Forces - Tyagi, R K Col.: 9789382652090 - AbeBooks, <https://www.abebooks.com/9789382652090/Understanding-Cyber-Warfare-Implications-Indian-9382652094/plp> (last visited Jan 2, 2025).

⁸ B. Poornima, *Cyber Preparedness of the Indian Armed Forces*, 10 *Journal of Asian Security and International Affairs* 301 (2023), <https://journals.sagepub.com/doi/10.1177/23477970231207250> (last visited Jan 2, 2025)

cybersecurity⁹

The role of cyberwarfare in modern conflict is not limited to the direct disruption of military operations. Cyberattacks can also be used to create psychological effects, sowing distrust and uncertainty within the population and among military personnel. This can undermine national morale, destabilize governments, and create confusion within the ranks. In the context of India, where national security is often challenged by external threats, the psychological impact of cyber warfare cannot be underestimated. Therefore, cybersecurity must be viewed not only as a technical issue but as a central component of national defense strategy.

The global landscape of military conflict is rapidly changing, and cyberwarfare is set to play an increasingly central role. As nations invest in new technologies, they expose themselves to new vulnerabilities. India's defense sector, while powerful, must adapt to these new realities by investing in cyber defense capabilities that are on par with its traditional military assets. Cyberattacks can strike at any time and with devastating consequences, which means India's military modernization efforts must incorporate robust cybersecurity measures to ensure the nation's readiness to face both conventional and non-traditional threats.

India needs to modernize its military capabilities is as pressing as ever, but this modernization must extend beyond traditional warfare techniques to include the development of advanced cyber defense systems. With increasing cyber threats from countries like China and Pakistan, India's military strategy must shift towards a more holistic approach, encompassing both physical and cyber defense¹⁰. The vulnerability of India's defense infrastructure to cyberattacks, as demonstrated by past incidents, highlights the urgent need for a comprehensive and integrated cyber defense strategy. By strengthening its cybersecurity posture, India can ensure that it remains prepared to defend itself against the evolving threats of the modern battlefield. he Indian Army and its Support in Cybersecurity and Cyber Law

⁹ Securing the Nation Against Internal and External Threats, India Foundation (Apr. 16, 2024), <https://indiafoundation.in/articles-and-commentaries/securing-the-nation-against-internal-and-external-threats/> (last visited Jan 2, 2025).

¹⁰ Cyber Warfare in India: Analyzing Government's Approach to the 4th Dimension of War, (Dec. 31, 2024), <https://apacnewsnetwork.com/2024/12/cyber-warfare-in-india-analyzing-governments-approach-to-the-4th-dimension-of-war/> (last visited Jan 2, 2025).

THE INDIAN ARMY AND ITS SUPPORT IN CYBERSECURITY AND CYBER LAW

The Indian Army, one of the world's largest and most capable military forces, is known primarily for its role in ensuring national security, protecting borders, and maintaining peace and order. However, with the increasing global reliance on technology, cyber threats have emerged as a significant concern. In this digital age, cybersecurity has become integral to national defense strategies. The Indian Army, alongside other branches of the Indian Armed Forces, plays a crucial role in fortifying India's cybersecurity infrastructure and ensuring that cyber laws are adhered to in the country¹¹

This note delves into the Indian Army's involvement in cybersecurity and the application of cyber laws, examining the Army's role in securing critical infrastructure, conducting cyber operations, and supporting the enforcement of cyber regulations and policies.

THE ROLE OF CYBERSECURITY IN NATIONAL DEFENSE

Cybersecurity has emerged as a critical area of defense due to the rapid digitization of military operations, government services, and civilian infrastructure. In India, the Ministry of Defense (MoD) has been working towards improving the country's cybersecurity posture to address the rising threats from cyber-attacks. Cybersecurity, in this context, involves safeguarding computer systems, networks, and data from unauthorized access, attacks, damage, or theft¹²

The Indian Army, with its specialized cyber warfare units, is an integral part of this effort. It works in tandem with other agencies, such as the National Technical Research Organization (NTRO) and the Indian Computer Emergency Response Team (CERT-In), to protect the country's cyberspace from malicious activities, including cyber espionage, cyber-terrorism, and cyber-attacks¹³. The Indian Army's cyber capabilities are essential not only for national defense but also for the protection of critical

¹¹ Yohan Fernandes & Nasr Abosata, *Analysing India's Cyber Warfare Readiness and Developing a Defence Strategy*, (2024), <http://arxiv.org/abs/2406.12568> (last visited Jan 2, 2025).

¹² Hannes Ebert, *Hacked IT Superpower: How India Secures Its Cyberspace as a Rising Digital Democracy*, 19 *India Review* 376 (2020), https://www.academia.edu/104703536/Hacked_IT_superpower_how_India_secures_its_cyberspace_as_a_rising_digital_democracy (last visited Jan 2, 2025).

¹³ National Technical Research Organisation (NTRO), Vajiram & Ravi, <https://vajiramandravi.com/> (last visited Jan 2, 2025).

national assets and information infrastructure.

FORMATION OF CYBER UNITS IN THE INDIAN ARMY

In response to the growing threats in cyberspace, the Indian Army established dedicated cyber units, such as the Army Cyber Group, to monitor and defend against cyber-attacks. In 2018, the Indian Army set up the Army Cyber Command (ACC) to specifically address the challenges posed by cyber warfare¹⁴. The Army Cyber Command is tasked with the responsibility of providing strategic and tactical support in the cyber domain, ensuring that the Army is equipped to handle cyber threats and conduct operations in cyberspace.

The Army Cyber Command works closely with other branches of the Indian Armed Forces to implement a joint strategy for national security, emphasizing the need for information dominance in warfare. This includes cyber surveillance, intelligence gathering, and counter-cyber measures to prevent attacks on military and civilian systems.

THE INDIAN ARMY'S CYBER WARFARE CAPABILITIES

The Indian Army's cyber warfare capabilities are designed to handle both defensive and offensive operations in cyberspace. On the defensive front, the Army aims to safeguard the country's military networks, communication systems, and sensitive data from cyber-attacks that could compromise national security. The Army's cyber experts work in coordination with CERT-In to monitor and neutralize cyber threats, prevent data breaches, and ensure that military communications remain secure.

On the offensive side, the Army has the ability to launch cyber-attacks against enemy networks in the event of a conflict. This would involve disrupting or disabling enemy command and control systems, communication networks, and critical infrastructure. In recent years, there have been reports of countries engaging in cyber warfare, and India's military has been preparing to counter such activities by building robust offensive cyber capabilities. Cyber warfare is a crucial aspect of modern warfare, and the Indian Army's efforts to enhance its cyber capabilities reflect the growing importance of cybersecurity in national defense¹⁵.

¹⁴ Indian Military's Embrace of Cyber Warfare - CASS, (2024), <https://casstt.com/indian-militarys-embrace-of-cyber-warfare/> (last visited Jan 2, 2025).

¹⁵ Web Desk, *INDIA MILITARY'S ADOPTION OF CYBER WARFARE*, International Defence Analysis (Aug. 26, 2024),

CYBERSECURITY TRAINING AND COLLABORATION

To build a highly skilled workforce for cyber defense, the Indian Army places significant emphasis on training its personnel in cybersecurity and cyber warfare. The Indian Army has partnered with various academic institutions and cyber security firms to provide its soldiers with advanced training in ethical hacking, digital forensics, cyber intelligence, and incident response. The aim is to equip the army with the necessary skills to prevent, detect, and respond to cyber threats effectively.

The Army has also collaborated with other arms of the government, such as the Indian Air Force, Navy, and law enforcement agencies, to enhance the country's collective cyber defense capabilities. Joint exercises and training sessions are held regularly to promote collaboration between different stakeholders in the national security ecosystem. These exercises simulate real-world cyber-attacks and provide an opportunity for the Indian Army to test its readiness and responses.

THE ROLE OF CYBER LAW IN INDIA

As cybersecurity issues evolve, there is a growing need for legal frameworks that can govern and regulate cyber activities, especially in terms of cybercrime, cyber warfare, and privacy. The Indian Army, alongside other government agencies, actively contributes to the creation, implementation, and enforcement of cyber laws in India. In India, the primary legal framework governing cyber activities is the Information Technology Act of 2000 (IT Act), which addresses a range of issues, including electronic commerce, digital signatures, and cybercrime. The Act is regularly amended to keep up with the rapid developments in technology and to address emerging cyber threats.

The Cyber Crime Coordination Centre (4C) was launched by the Ministry of Home Affairs in 2020 to coordinate and combat cybercrime¹⁶. The Indian Army, being an important stakeholder in national security, works closely with law enforcement agencies to ensure that cybercriminals are identified and prosecuted under Indian laws. The Army's role also extends to providing cyber law education and awareness to its personnel, ensuring they understand the legal implications of cyber activities. In addition to the IT Act, India is also working towards strengthening its

<https://internationaldefenceanalysis.com/india-militarys-adoption-of-cyber-warfare/> (last visited Jan 2, 2025).

¹⁶ Nisha, *Indian Cyber Crime Coordination Centre (I4C)*, Free UPSC IAS Preparation Syllabus and Materials For Aspirants (Oct. 30, 2024), <https://forumias.com/blog/indian-cyber-crime-coordination-centre-i4c/> (last visited Jan 2, 2025).

framework for cyber warfare laws and international cybersecurity cooperation. The Indian Army is involved in discussions and efforts to develop policies for responding to cyber-attacks and cyberwarfare, with a focus on aligning domestic regulations with global norms and treaties.

SUPPORT FOR NATIONAL CYBERSECURITY INITIATIVES

Apart from its direct involvement in cybersecurity, the Indian Army has been instrumental in supporting broader national cybersecurity initiatives. The Indian government has set up a National Cyber Security Policy to ensure the protection of critical information infrastructure, improve cyber resilience, and promote public awareness about cybersecurity. The Army's cyber units contribute to these efforts by providing strategic advice, expertise, and manpower to implement the policy.

The National Critical Information Infrastructure Protection Centre (NCIIPC), established under the National Cyber Security Policy, works closely with the Indian Army to secure critical sectors such as energy, banking, transportation, and telecommunications from cyber threats. The Indian Army, through its specialized cyber warfare units, provides assistance in safeguarding the country's most vulnerable and strategically significant sectors¹⁷.

CONCLUSION

Despite its significant efforts in cybersecurity, the Indian Army faces several challenges in securing the country's cyberspace. The rapidly evolving nature of cyber threats means that the Army must continuously adapt its strategies and enhance its cyber capabilities. The growing sophistication of cyber-attacks, including state-sponsored cyber espionage and cyber terrorism, requires constant vigilance and rapid responses. Moreover, the shortage of skilled cybersecurity professionals is a challenge faced not only by the Indian Army but also by the entire cybersecurity sector in India. To address this, the Indian Army continues to invest in training and education, aiming to build a robust cadre of cyber experts within its ranks. Looking to the future, the Indian Army will likely focus on expanding its cyber warfare capabilities, improving cyber resilience, and enhancing cooperation with other countries in the global cybersecurity framework. As cyberspace becomes a domain of warfare, the Army's role in protecting India's cyberspace will continue to be critical for national security.

¹⁷ National Critical Information Infrastructure Protection Centre, Government of India, <https://nciipc.gov.in/> (last visited Jan 2, 2025).