RAMAIAH UNIVERSITY OF APPLIED SCIENCES

CENTRE FOR NATIONAL SECURITY STUDIES

Civil-Military Fusion in Cybersecurity and Information Warfare

10-09-2025 **Neeraj Singh Manhas**

Abstract

Civil-Military Fusion (CMF) in India’s cybersecurity and information warfare domain represents a strategic convergence of civilian expertise and military capabilities to counter evolving digital threats. This paper argues that effective CMF enhances India’s resilience against cyber-attacks and hybrid warfare by leveraging private sector innovation, academic research, and government coordination. Initiatives like CERT-In, iDEX, and public-private partnerships exemplify this synergy, fostering advanced cybersecurity solutions and information warfare strategies. However, challenges such as bureaucratic inefficiencies and trust deficits hinder progress. By strengthening policy frameworks and collaboration, India can build a robust CMF ecosystem, ensuring national security and technological sovereignty in the digital age.

Keywords

Civil-Military Fusion, Cybersecurity, Information Warfare, India, Public-Private Partnerships

Introduction

Civil-Military Fusion (CMF) represents a strategic paradigm that integrates "civilian expertise" and "military capabilities" to bolster national security, particularly in the domains of "cybersecurity" and "information warfare." This approach leverages the technological prowess of the private sector, academic research, and governmental coordination to create a synergistic defense ecosystem. In India, the escalating frequency and sophistication of cyber threats, exemplified by over 1.5 million cyberattacks on government websites in 2025 with only 150 successes, underscore the critical need for robust cybersecurity measures (India Today, 2025).

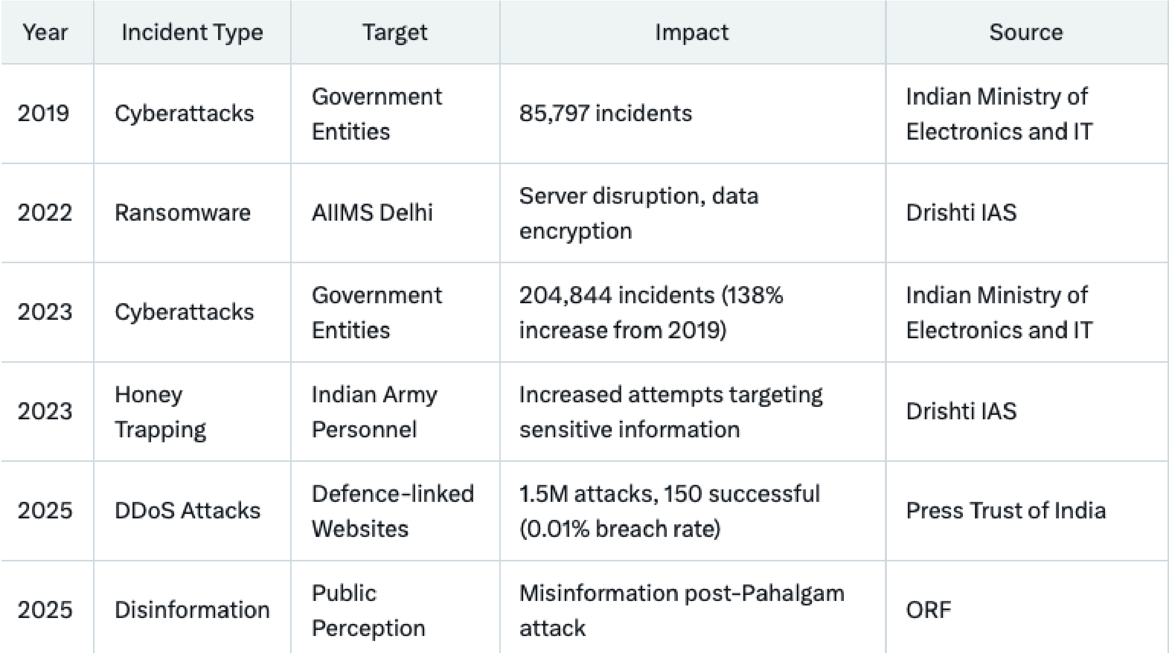
Concurrently, "hybrid warfare," blending conventional and digital tactics like disinformation campaigns post the Pahalgam terror strike, has amplified the urgency for integrated strategies (Sengupta, 2025). This paper argues that effective CMF significantly enhances India's "cyber resilience" by harmonizing civilian innovation with military strategy, yet systemic challenges such as bureaucratic inefficiencies and trust deficits must be addressed to unlock its full potential (Saran, 2022). The study focuses on India's CMF initiatives, examining key policies like the "Innovations for Defence Excellence (iDEX)" program, stakeholder roles including CERT-In and the Defence Cyber Agency, and prospects for future advancements.

The objectives of this paper to analyse the efficacy of CMF in countering cyber threats, identify barriers to its implementation, and propose policy recommendations to strengthen India's cybersecurity framework. Employing a methodology of policy analysis, case studies of recent cyber incidents, and comparisons with global models like those in the U.S. and China, this paper aims to provide a comprehensive understanding of CMF's role in fortifying India's national security landscape against evolving digital and informational challenges.

Cybersecurity and Information Warfare in India

The "cyber threat landscape" in India has grown increasingly perilous, with a surge in cyberattacks targeting "critical infrastructure" such as banking, energy, and defence sectors. In 2024, India recorded 369.01 million malware detections across 8.4 million endpoints, averaging 702 detections per minute, with Trojans and Infectors comprising 68% of threats (Data Security Council of India, 2025).

Table 1: Key Cybersecurity Incidents in India (2019–2025)



Year	Incident Type	Target	Impact	Source
2019	Cyberattacks	Government Entities	85,797 incidents	Indian Ministry of Electronics and IT
2022	Ransomware	AIIMS Delhi	Server disruption, data encryption	Drishti IAS
2023	Cyberattacks	Government Entities	204,844 incidents (138% increase from 2019)	Indian Ministry of Electronics and IT
2023	Honey Trapping	Indian Army Personnel	Increased attempts targeting sensitive information	Drishti IAS
2025	DDoS Attacks	Defence-linked Websites	1.5M attacks, 150 successful (0.01% breach rate)	Press Trust of India
2025	Disinformation	Public Perception	Misinformation post-Pahalgam attack	ORF

Source: Data from CSIS (2025) shows a significant rise in cyberattacks, while the 2025 India-Pakistan conflict highlighted disinformation campaigns (ORF, CAPS India).

Notably, in 2025, over 1.5 million cyberattacks targeted government websites, primarily linked to Pakistan-based groups, though only 150 succeeded, showcasing robust defences (India Today, 2025). "Information warfare" further complicates this scenario, as disinformation and propaganda campaigns, exemplified by fabricated narratives post the Pahalgam terror strike on April 22, 2025, aim to destabilise public trust and national security (Sengupta, 2025). These "hybrid threats," blending cyberattacks with misinformation, were evident when Maharashtra Cyber countered over 5,000 fake news posts. India's "strategic needs" demand integrated "civilian-military efforts" to address these multifaceted challenges, leveraging private sector innovation and military expertise through initiatives like the Innovations for Defence Excellence (iDEX) and the Defence Cyber Agency (DCA).

The National Cyber Security Policy (2013, updated) underscores this necessity, advocating for public-private partnerships to bolster "cyber resilience" (Saran, 2022). In the "global context," India's approach contrasts with advanced CMF models. The U.S. excels with DARPA's deep integration of private tech firms. At the same time, China's Military-Civil Fusion strategy, driven by the PLA's Strategic Support Force, prioritizes state-controlled innovation (Centre for Strategic and International Studies, 2025). India, ranked third-tier globally, shows moderate CMF integration through iDEX and CERT-In but lags in scale and coordination compared to these leaders (Observer Research Foundation, 2023). Strengthening India's CMF framework is critical to counter escalating cyber and informational threats effectively.

The Framework of Civil-Military Fusion in India:

Definition and Scope- CMF in the context of cybersecurity and information warfare refers to the strategic integration of civilian and military resources to enhance India's defense against digital threats and hybrid warfare tactics. CMF leverages "civilian expertise" in technology and innovation alongside military capabilities to develop robust cybersecurity solutions and counter disinformation campaigns. In India, this framework encompasses collaborative efforts to protect critical infrastructure, such as banking, energy, and defence systems, while addressing "hybrid threats" like cyberattacks and propaganda, which have surged with over 1.5 million attacks on government websites in 2025, though only 150 succeeded (India Today, 2025).

Key Stakeholders- The CMF ecosystem involves diverse stakeholders. The government, through the Computer Emergency Response Team-India (CERT-In), coordinates cyber incident responses and fosters public-private partnerships, as seen in its handling of 369.01 million malware detections in 2024 (Data Security Council of India, 2025). The Defence Research and Development Organisation (DRDO) drives technological advancements, collaborating with civilian entities on secure communication systems. The military's Defence Cyber Agency (DCA), established in 2021, spearheads cyber operations, countering threats like those from Pakistan-based APT groups post the Pahalgam terror strike (Sengupta, 2025). The private sector, including tech giants like TCS and Infosys, contributes advanced solutions such as AI-based threat detection, while startups under iDEX develop niche cybersecurity tools. Academia, notably IITs and research labs, supports R&D, partnering with DRDO on projects like quantum cryptography, enhancing dual-use technologies (Observer Research Foundation [ORF], 2023).

Policy Initiatives- India's CMF framework is bolstered by key policies. The Innovations for Defence Excellence (iDEX) program, launched in 2018, funds startups to develop indigenous cybersecurity solutions, with over 100 projects supported, including secure communication platforms (Saran, 2022). The Make in India initiative promotes local manufacturing of defence technologies, reducing import dependency and fostering civilian-military collaboration. The National Cyber Security Policy (2013, updated) provides a roadmap for protecting cyberspace, emphasizing public-private partnerships and capacity building. These policies aim to integrate civilian innovation with military needs, though bureaucratic delays and limited funding pose challenges (Centre for Strategic and International Studies, 2025).

Case Studies- Notable examples illustrate CMF's impact. The development of Bharat Operating System Solutions (BOSS), an indigenous Operating System by C-DAC, exemplifies civilian-military collaboration, offering a secure alternative to foreign software for government and defense use. Another case is the iDEX-funded startup CyRA Technologies, which developed an AI-driven cybersecurity platform for real-time threat detection, adopted by the Indian Army (ORF, 2023). Post-2025 Pahalgam attack, CERT-In and DCA's joint efforts countered over 5,000 disinformation posts, showcasing effective CMF in information warfare

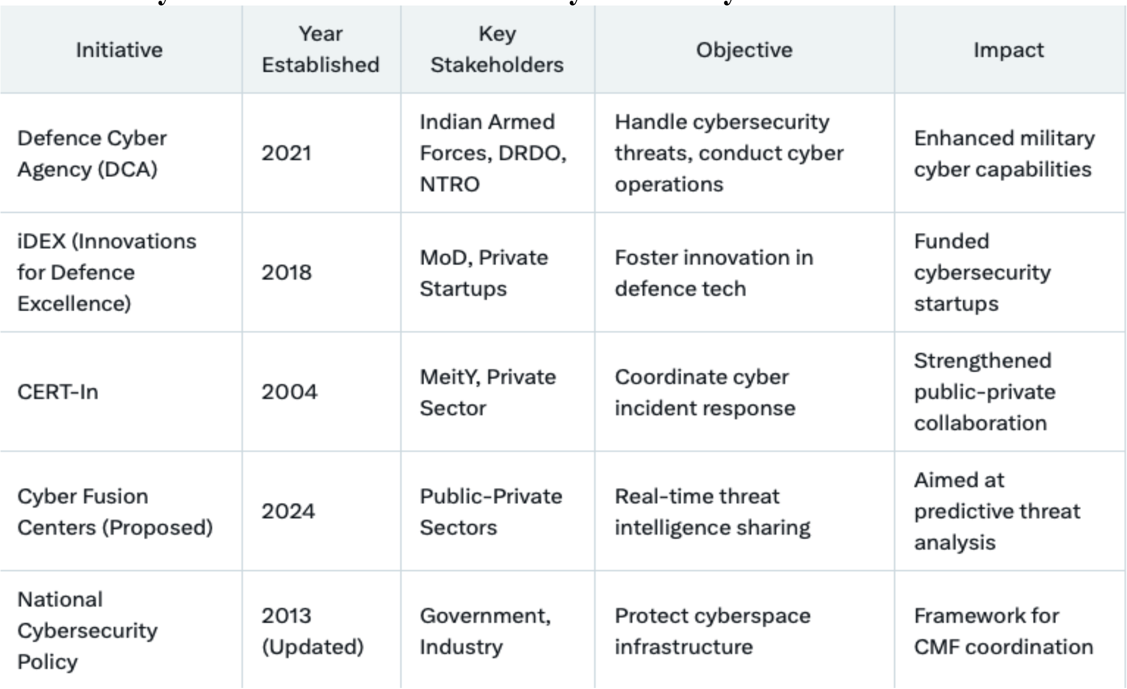
(India Today, 2025). These cases highlight how CMF integrates "indigenous technology" with strategic defense needs, though scaling such initiatives remains a challenge.

India’s CMF framework, while promising, requires stronger coordination to rival global leaders like the U.S., where DARPA seamlessly integrates private sector innovation, or China’s state-driven Military-Civil Fusion (CSIS, 2025). Addressing bureaucratic inefficiencies and enhancing trust between stakeholders will be critical to maximizing CMF’s potential in fortifying India’s cybersecurity and information warfare capabilities.

Opportunities in CMF for Cybersecurity and Information Warfare:

Private Sector Innovation- The "private sector" in India plays a pivotal role in advancing "cybersecurity" through cutting-edge innovations, significantly enhancing the "Civil-Military Fusion (CMF)" framework. Indian tech giants like TCS and Infosys develop "AI-based threat detection" systems and advanced encryption protocols, crucial for safeguarding "critical infrastructure" such as banking and defense networks. For instance, TCS’s cybersecurity solutions have been integrated into government systems, detecting threats in real-time, as evidenced by their role in countering 369.01 million malware detections in 2024 (Data Security Council of India [DSCI], 2025). Startups, particularly those funded by the "Innovations for Defence Excellence (iDEX)," contribute niche technologies like blockchain-based secure data storage, reducing vulnerabilities in military communications. These innovations not only bolster defense capabilities but also position India as a potential exporter of cybersecurity solutions, aligning with the "Make in India" initiative (Saran, 2022).

Table 2: Key CMF Initiatives in India’s Cybersecurity



Initiative	Year Established	Key Stakeholders	Objective	Impact
Defence Cyber Agency (DCA)	2021	Indian Armed Forces, DRDO, NTRO	Handle cybersecurity threats, conduct cyber operations	Enhanced military cyber capabilities
iDEX (Innovations for Defence Excellence)	2018	MoD, Private Startups	Foster innovation in defence tech	Funded cybersecurity startups
CERT-In	2004	MeitY, Private Sector	Coordinate cyber incident response	Strengthened public-private collaboration
Cyber Fusion Centers (Proposed)	2024	Public-Private Sectors	Real-time threat intelligence sharing	Aimed at predictive threat analysis
National Cybersecurity Policy	2013 (Updated)	Government, Industry	Protect cyberspace infrastructure	Framework for CMF coordination

Source: Initiatives like DCA and iDEX reflect CMF efforts, with CERT-In playing a pivotal role in civilian-military coordination.

Academic Contributions- Academia significantly enhances CMF through "research and development (R&D)" collaborations with the military, focusing on "dual-use technologies." Institutions like the Indian Institutes of Technology (IITs) partner with the "Defence Research and Development Organisation (DRDO)" to develop quantum cryptography and secure satellite communication systems. For example, IIT Madras's collaboration with DRDO on AI-driven cybersecurity tools has yielded prototypes for predictive threat analysis, applicable to both civilian and military domains (Observer Research Foundation [ORF], 2023). These partnerships foster innovation in areas like machine learning and big data analytics, critical for countering sophisticated cyberattacks. Academic contributions also extend to training programs, addressing India's cybersecurity workforce gap, estimated at 700,000 professionals (SPS Naval Forces, 2024). Such collaborations ensure that cutting-edge research translates into practical defense applications, strengthening India's "cyber resilience."

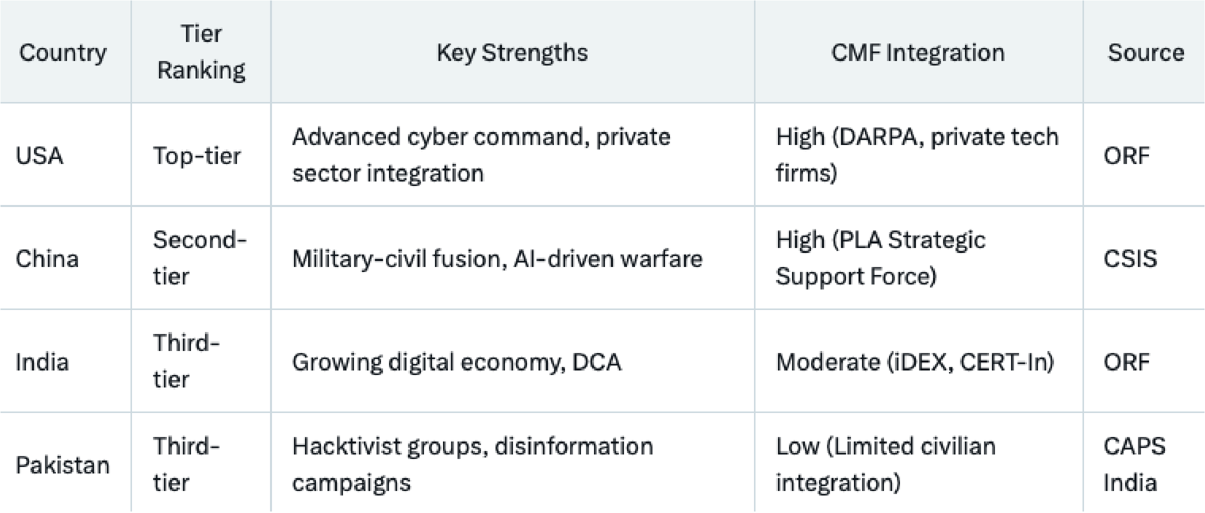
Public-Private Partnerships (PPPs)- "Public-Private Partnerships (PPPs)" are a cornerstone of India's CMF, exemplified by iDEX-funded startups developing "secure communication systems." CyRA Technologies, an iDEX beneficiary, created an AI-powered cybersecurity platform adopted by the Indian Army for real-time threat detection, showcasing successful civilian-military collaboration (ORF, 2023). The "Computer Emergency Response Team-India (CERT-In)" facilitates PPPs by coordinating with private firms to respond to cyber incidents, as seen in its mitigation of over 1.5 million cyberattacks on government websites in 2025, with only 150 successes (India Today, 2025). These partnerships leverage private sector agility and military strategic oversight, creating a robust defense ecosystem. However, scaling PPPs requires streamlined procurement processes and increased funding to sustain innovation (Centre for Strategic and International Studies, 2025).

Information Warfare Capabilities- Civilian expertise in "data analytics" and "social media" significantly enhances military "information warfare" capabilities within the CMF framework. Private firms like Data Weave provide advanced analytics to monitor and counter disinformation campaigns, which surged post the 2025 Pahalgam terror strike, with Maharashtra Cyber neutralizing over 5,000 fake news posts (Sengupta, 2025). Social media platforms, collaborating with the "Defence Cyber Agency (DCA)," employ AI-driven sentiment analysis to detect and mitigate propaganda, as seen in countering Pakistan-linked narratives in 2025. Civilian expertise in natural language processing further aids in identifying "hybrid threats," enabling rapid response to misinformation. These capabilities strengthen India's ability to maintain public trust and national stability during crises (India Today, 2025).

Economic and Strategic Benefits- CMF in cybersecurity yields significant "economic and strategic benefits." The growth of iDEX-funded startups has created thousands of jobs, particularly in tech hubs like Bengaluru, fostering economic development (ORF, 2023). By promoting indigenous solutions like "Bharat Operating System Solutions (BOSS)," CMF reduces India's reliance on foreign software, enhancing "strategic autonomy" and saving billions in import costs (Saran, 2022). Strategically, CMF strengthens India's position in global cybersecurity, with potential to export technologies, as seen in DRDO's collaborations with friendly nations. However, realizing these benefits requires overcoming bureaucratic hurdles and increasing R&D investment to compete with global leaders like the U.S., where DARPA's model drives innovation, or China's state-led fusion (CSIS, 2025). By capitalizing on these opportunities, India can fortify its cybersecurity and assert its role in the global digital landscape.

Challenges to Effective CMF in India- The implementation of "Civil-Military Fusion (CMF)" in India's "cybersecurity" and "information warfare" domains faces significant challenges that hinder its potential to enhance "cyber resilience." Despite progress through initiatives like "Innovations for Defence Excellence (iDEX)" and the "Defence Cyber Agency (DCA)," systemic obstacles must be addressed to fully integrate civilian and military resources. These challenges include bureaucratic hurdles, trust deficits, resource constraints, technological gaps, and regulatory shortcomings, each impeding the seamless collaboration needed to counter escalating cyber threats, such as the 1.5 million attacks on government websites in 2025, with only 150 successes (India Today, 2025).

Table 3: Comparative Cyber Warfare Capabilities (2023)



Country	Tier Ranking	Key Strengths	CMF Integration	Source
USA	Top-tier	Advanced cyber command, private sector integration	High (DARPA, private tech firms)	ORF
China	Second-tier	Military-civil fusion, AI-driven warfare	High (PLA Strategic Support Force)	CSIS
India	Third-tier	Growing digital economy, DCA	Moderate (iDEX, CERT-In)	ORF
Pakistan	Third-tier	Hacktivist groups, disinformation campaigns	Low (Limited civilian integration)	CAPS India

Source: India's third-tier ranking reflects moderate CMF integration compared to global leaders, as per ORF (2023).

Bureaucratic Hurdles- "Bureaucratic inefficiencies" significantly delay policy implementation and procurement processes critical to CMF. The complex approval mechanisms within the Ministry of Defence and other government bodies slow down the adoption of innovative cybersecurity solutions from private startups. For instance, iDEX-funded projects, despite their potential, often face prolonged evaluation periods, limiting the timely deployment of technologies like AI-based threat detection (Saran, 2022). These delays hamper the ability to respond swiftly to evolving threats, such as the 369.01 million malware detections recorded in 2024, necessitating streamlined processes to enhance CMF efficacy (Data Security Council of India, 2025).

Trust Deficits- "Trust deficits" between military and civilian entities pose a significant barrier to CMF. The military's reluctance to share sensitive data with private firms, due to security concerns, limits collaborative development of cybersecurity tools. Similarly, private companies hesitate to disclose proprietary technologies, fearing intellectual property risks. This mutual distrust undermines joint ventures, as seen in limited data-sharing during the response to disinformation campaigns post the 2025 Pahalgam terror strike, where civilian expertise could have bolstered military efforts (Sengupta, 2025). Building trust through transparent protocols is essential for effective CMF.

Resource Constraints- "Resource constraints," particularly in funding and talent, severely limit India's CMF capabilities. The cybersecurity sector faces a shortage of approximately 700,000 professionals, hindering the development and implementation of advanced solutions (SPS Naval Forces, 2024). Additionally, limited government funding for R&D, compared to global leaders like the U.S., restricts innovation in areas like secure communication systems. For example, while iDEX supports startups, its budget is insufficient to scale projects to meet national demands, impacting India's ability to counter sophisticated cyberattacks (Observer Research Foundation, 2023).

Technological Gaps- India lags in adopting "cutting-edge technologies" like quantum cryptography and advanced AI, critical for modern cybersecurity and information warfare. While countries like China and the U.S. invest heavily in quantum computing for secure communications, India's efforts, such as DRDO-IIT collaborations, are still nascent (Centre for Strategic and International Studies [CSIS], 2025). This technological gap leaves India vulnerable to advanced persistent threats (APTs), as evidenced by Pakistan-linked groups exploiting outdated systems in 2025 (India Today, 2025). Accelerating R&D investments is crucial to bridge this divide.

Regulatory Challenges- "Regulatory challenges" further impede CMF, as India's legal frameworks, including the National Cyber Security Policy (2013, updated), lack clarity on data-sharing and collaboration protocols. Ambiguities in cybersecurity laws discourage private sector participation, as firms fear legal repercussions for handling sensitive data. The absence of a comprehensive cyber doctrine exacerbates these issues, limiting coordinated responses to hybrid threats (Saran, 2022). Updating legal frameworks to facilitate secure, transparent collaboration is vital for strengthening CMF.

Addressing these challenges requires concerted efforts to streamline bureaucracy, foster trust, increase resources, advance technology, and reform regulations, ensuring India's CMF framework can effectively counter cyber and informational threats.

Policy Recommendations- To maximize the potential of "Civil-Military Fusion (CMF)" in India's "cybersecurity" and "information warfare" domains, targeted policy interventions are essential to overcome bureaucratic, trust, resource, technological, and regulatory challenges. These recommendations aim to strengthen coordination, incentivize private sector participation, enhance academic involvement, reform legal frameworks, and build capacity, ensuring India's "cyber resilience" against escalating threats like the 1.5 million cyberattacks on government websites in 2025 (India Today, 2025).

Strengthening Coordination- Establishing a dedicated "CMF task force" for cybersecurity, comprising representatives from the "Defence Cyber Agency (DCA)," "Computer Emergency Response Team-India (CERT-In)," private tech firms, and academia, is critical. This task force would streamline decision-making, reduce bureaucratic delays, and foster real-time collaboration, as seen in the need for swift responses to disinformation post the 2025 Pahalgam attack (Sengupta, 2025). Modelled on the U.S. DARPA's coordination mechanisms, it could prioritize joint projects and threat intelligence sharing (Centre for Strategic and International Studies [CSIS], 2025).

Incentivizing Private Sector Participation- To boost private sector involvement, the government should offer "tax breaks" and increased funding for startups under the "Innovations for Defence Excellence (iDEX)." For instance, expanding iDEX's budget could scale projects like CyRA Technologies' AI-driven cybersecurity platforms, which have proven effective in military applications (Observer Research Foundation [ORF], 2023). Financial incentives would encourage firms like TCS to invest in "secure communication systems," reducing reliance on foreign technologies and enhancing economic benefits (Saran, 2022).

Enhancing Academic Involvement- Increasing "research grants" for university-military collaborations, particularly with IITs and DRDO, would accelerate "dual-use technology" development, such as quantum cryptography. Current partnerships, like IIT Madras's AI projects, are underfunded, limiting scalability (ORF, 2023). Dedicated funding programs could bridge this gap, fostering innovation and addressing the 700,000-strong cybersecurity talent shortage (SPS Naval Forces, 2024).

Legal and Regulatory Reforms- Updating "cybersecurity laws" to facilitate secure data sharing between civilian and military entities is vital. The National Cyber Security Policy (2013, updated) lacks clear protocols, deterring private sector participation due to legal ambiguities (Saran, 2022). A revised framework, inspired by global models, should ensure data security while promoting collaboration, as seen in China's structured Military-Civil Fusion (CSIS, 2025).

Capacity Building- Addressing the cybersecurity talent gap requires robust "training programs." Government-backed initiatives, in collaboration with academia and industry, should train professionals in AI, data analytics, and information warfare, reducing the 700,000 workforce deficit (SPS Naval Forces, 2024). These programs would empower stakeholders to counter sophisticated threats effectively.

Conclusion

CMF is pivotal in addressing India's escalating cybersecurity and information warfare challenges, integrating civilian expertise with military capabilities to safeguard critical infrastructure and counter hybrid threats. The surge in cyberattacks, with 1.5 million targeting government websites in 2025, and the proliferation of disinformation post the Pahalgam terror strike, underscore the urgency of robust CMF strategies (India Today, 2025; Sengupta, 2025). This paper has argued that effective CMF enhances India's cyber resilience by leveraging private sector innovation, academic R&D, and military coordination, as seen in initiatives like Innovations for Defence Excellence (iDEX) and the Defence Cyber Agency (DCA) (Observer

Research Foundation, 2023). However, systemic challenges—bureaucratic delays, trust deficits, resource constraints, technological gaps, and regulatory ambiguities—must be addressed to maximize its potential (Saran, 2022; Centre for Strategic and International Studies, 2025). Looking ahead, India has the opportunity to emerge as a global leader in cybersecurity by scaling CMF efforts, drawing inspiration from models like the U.S.'s DARPA while tailoring solutions to its unique context (CSIS, 2025). Sustained investment in indigenous technologies, such as Bharat Operating System Solutions, and expanded public-private partnerships can reduce import dependency and enhance strategic autonomy (Saran, 2022). Policymakers, industry leaders, and academia must collaborate to establish a dedicated CMF task force, increase R&D funding, and reform legal frameworks to foster a resilient digital ecosystem. By addressing the 700,000-strong cybersecurity talent gap and advancing dual-use technologies, India can fortify its defences against evolving cyber threats (SPS Naval Forces, 2024).

References

Centre for Strategic and International Studies. (2025). *The tech revolution and irregular warfare: Leveraging commercial innovation for great power competition*. https://www.csis.org/analysis/tech-revolution-and-irregular-warfare-leveraging-commercial-innovation-great-power

Data Security Council of India. (2025). *India Cyber Threat Report 2025*. Seqrite. https://www.seqrite.com/india-cyber-threat-report-2025/

India Today. (2025, May 13). *Indian government websites targeted by 15 lakh cyberattacks from Pakistan-linked hackers, only 150 succeed*. https://www.indiatoday.in/india/story/indian-government-websites-targeted-15-lakh-cyberattacks-pakistan-linked-hackers-150-succeed-3372983-2025-05-13

Observer Research Foundation. (2023). *India: Crucial cyberwarfare capabilities need to be upgraded*. https://www.orfonline.org/expert-speak/india-crucial-cyberwarfare-capabilities-need-to-be-upgraded

Saran, S. (2022, December 20). *India's critical need for cyber doctrine*. The Daily Pioneer. https://www.dailypioneer.com/2022/columnists/india---s-critical-need-for-cyber-doctrine.html

Sengupta, A. (2025). *Rethinking India's cyber readiness in the age of information warfare*. Observer Research Foundation. https://www.orfonline.org/expert-speak/rethinking-india-s-cyber-readiness-in-the-age-of-information-warfare

SPS Naval Forces. (2024). *Strengthening India's cyber defence*. https://www.spsnavalforces.com/story/?id=1032