Emerging Digital Technologies and India's Security Sector: AI, Blockchain, and Quantum Communications
Edited by Pankaj K. Jha, Arun Teja Polcumpally and Vedant Saigal, Routledge, 2024, pp. ix+166

Meghna Pradhan*

In an era where digital technologies are rapidly transforming socio-political and economic tapestry, the book *Emerging Digital Technologies and India's Security Sector: AI, Blockchain, and Quantum Communications* offers key insights into integration of Artificial Intelligence, cybersecurity, blockchain and quantum communications into military operations. Edited by Pankaj K. Jha, Arun Teja Polcumpally and Vedant Saigal, this book provides a comprehensive analysis of how these frontier technologies are reshaping military strategy, particularly from the perspective of their adoption and potential in India.

The book has been divided into two parts. Part I, comprising four chapters, aims at creating the framework for analysis of how frontier technologies have been integrated into military affairs. Part II of the book builds upon that framework, to expand upon the current status of integration and use of digital technologies in Indian military apparatus.

* Ms Meghna Pradhan is a Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi.

ISSN 0976-1004 (print); 2583-7567 (online)

Journal of Defence Studies, Vol. 18, No. 4, October–December 2024, pp. 382–388

In the Part I of the book, Arun Teja Polcumpally lays the groundwork for discussion on frontier technologies within the context of state and military in the first chapter titled 'Frontier Technologies Will Enhance the "Power" of the State'. The ubiquity of Information and Communications Technology (ICT) has strengthened globalisation, private entities and State power. Shift in the centre of innovation from military to private players has led to States leveraging technologies to monitor and control public behaviour. These trends have increased authoritarianism with potential for control beyond territorial boundaries due to global interconnectivity. Major powers like China and the US have recognised these trends, and are increasingly investing in their research and development of disruptive technologies. India generates vast data, but lack of local storage, absence of indigenous critical hardware, software, social and mass media platforms and a reactive cybersecurity leaves it open for exploitation. India needs to anticipate future warfare and invest in emerging technologies to modernise its military approach.

In the next chapter titled 'War, Hybrid War, and Revolution in the Military', Arun Teja Polcumpally focuses on Revolution in Military Affairs (RMA), emphasising that technology can be called RMA only if its integration leads to significant structural and organisational shift in military operations and warfare doctrines. War may be defined as 'an armed conflict between parties for political ends', and modern warfare is hybrid, which combines conventional tactics with digital technologies for psychological tactics. In terms of Buzan's securitisation theory, information technology-related issues are increasingly framed as national security issues, thereby attracting significant investments in cybersecurity and new military doctrines. There is a need for adaptive strategies to address the interplay between innovation and security, as frontier technologies revolutionise both offensive and defensive military capabilities.

In the chapter 'Quest for Military Supremacy–the United States vs. China vs. Russia', Poornima Vijaya analyses the increasing complexity in strategic rivalries between China, US and Russia, that encompasses conventional and emerging technologies for military. China has been aggressively pursuing development of disruptive technologies for dual-use and ensuring civil–military integration under Xi Jinping. Russia has leveraged its competitive advantage in nuclear and weapon delivery systems, while developing hybrid warfare capabilities. US focuses on institutional agility, innovation and maintaining overall military dominance. The discussion largely focuses on US, China and Russia, but notes how India has not been an exception. The global powers develop strategies to deter wars, grow arsenals for nuclear and conventional weapons, and conduct indirect actions like cyber-attacks, simultaneously.

Arun Teja Polcumpally draws from works of Jamie Susskind and Yuval Noah Harari on data and perception control in the chapter 'Non-Traditional Security + Data: The Road Not Taken'. While new technologies have varying impact on military affairs, data remains fundamental functionary to all of them. Technologies are now able to capture and analyse granular behavioural data, which may be exploited to wield unprecedented power over society, influencing perceptions and behaviours. Susskind believes that dominance of data-driven technology affords ability to control and manipulate perception, thereby conferring power. Harari posits that data defines intelligence, and may enable AI to surpass humans and undermine democratic values. Cases like Cambridge Analytica illustrate how data-driven technologies pose a significant global non-traditional security threat. India must find a balance between fostering innovation and protecting privacy in the digital, data-driven age.

In the Part II of the book, the chapter titled 'Artificial Intelligence and Its Probable Military Disruptions', by Vedant Saigal, discusses the potential of data-based technologies (particularly AI) in the Indian military. India unveiled Digital India initiative in 2020, with the aim to boost investment and development of AI, cybersecurity and robotics. This has a multi-sectoral impact, including in the armed forces. Use cases include mapping oceanic topography and enhancing nautical capabilities in Navy, autonomous refuelling and swarm drones in Air Force, Lethal Autonomous Weapon Systems and exoskeletons in Army, semiotics for self-learning machines, and enhancing cybersecurity. While deficient resources, reliability and poor cybersecurity are significant challenges to AI in India, it is indubitable that AI will revolutionise warfare, and human–AI collaboration is an inevitable future.

The chapter 'Quantum Communications in Indian Armed Forces' by Rushil Khosla encapsulates the significance of quantum technology, particularly for cybersecurity. Cybersecurity is a booming industry, evidenced by states' increasing data legislations to secure it within their territory. Technologies like Quantum Key Distribution (QKD) are finding a use case as an 'unbreakable shield' for securing sensitive military and government communications, as well as citizens' privacy. The advantage of quantum computing over traditional methods lies in the abilities of qubits to store multiple data simultaneously. Global developments in quantum technologies are being spearheaded by countries like China, US, EU and even India, and is reshaping global politics. The US–China rivalry affords India an opportunity to leverage its engineering prowess to not just develop quantum technology, but become a non-contentious, alternate hub for cyber power.

In 'Application of Blockchain Technology in Military Affairs', Sonchita Debnath posits the utility and potential of blockchain technology across sectors, with focus on military. The technology, rooted in quantum mechanics and thermodynamics, has evolved since the 1970s, with significant contributions from Ralph Merkle and Satoshi Nakamoto. Blockchain essentially works as a distributed ledger, and utilises algorithms like Proof of Work (PoW) and Proof of Stake (PoS) to ensure security. Blockchains provide varying levels of transparency and decentralisation, based on whether it is public, private or consortium. China, EU, US and Russia have invested in blockchain and incorporated them in military affairs aspects like securing communications, supply chain management and cyber defence. Blockchain technology has potential for being of strategic importance to modern defence systems due to their immutable and transparent recordkeeping.

Vedant Saigal and Arun Teja Polcumpally have analysed the importance of cybersecurity in India in their chapter 'Cyber Security Structure in India' from a lens of securitisation theory in national interests. India has been propelled by IT sector for economic and critical infrastructure development, assisted by initiatives like Digital India. Attacks on these private and public sector critical infrastructure has necessitated cybersecurity for India. Yet, India remains plagued with issues such as lack of cyber-defence environment and architecture, absence of indigenous critical hardware and software, absence of indigenous hardware and software development programmes, poor cybersecurity literacy, insufficient policies and state's potential abuse of cyberspace. In terms of military, cyberattacks such as 2012 hack against the Indian Navy's eastern command computer systems highlight the need for a robust cyber-defence environment. India must muster its cybersecurity framework, create awareness, foster public–private partnerships and undertake capacity-building to safeguard national security.

In the chapter 'Is India Ready With The Digital Army?', Arun Teja Polcumpally describes the drivers of military technology integration in India. India's reasons for military power have transitioned from post-independence focus on maintaining superiority over Pakistan, to becoming a regional power with multilateral cooperation. While China has also become a rival, India lacks competitive advantage due to limited investment in defence technology development, infrastructure limitations, and reliance on imports, with indigenous AI and quantum technologies still underdeveloped. India has made headway into military technology through indigenous developments such as LCA, Akash and Pinaka, as well as through international cooperation in projects such as BrahMos, but there has been no true digital revolution in military due to lack of focused research and development, indigenous innovation and integration of advanced technologies like AI and blockchain. India needs to pursue indigenous development, intelligentisation and modernisation of military to remain competitive.

Pankaj K. Jha draws conclusion of the book by drawing from US example of emphasis on emerging technologies like AI, blockchain and quantum communications for national security, and comparing it with Indian outlook. While India has made efforts like Ministry of External Affairs' NEST division to inculcate new technologies in military strategies, it does face challenges in terms of private–public partnership, funding and poor integration and policies for new technologies. Nevertheless, India has kept its focus on leveraging new technologies for its military to usher in RMA, with emphasis on deterrence and non-lethal capabilities, aligning with global trends in military technology advancements.

The book *Emerging Digital Technologies and India's Security Sector: AI, Blockchain, and Quantum Communications* stands out for its ability to integrate practical aspects of emerging technologies within theoretical frameworks, making it a valuable resource in understanding the broader geopolitical and security implications. The authors offer valuable insights by placing frontier ICT technologies in the context of International Relations theories, such as using Buzan's securitisation theory to describe how states justify investment in innovation for national security, or using realist theory of power to address the limits of India's IT Act, 2000. Moreover, the book provides a detailed exploration of disruptive technologies like AI, cybersecurity, blockchain and quantum computing, not only by just describing where they are being used within military, but also explaining how these technologies work, so we gain a better understanding of their applications.

The book notably presents a relative picture of India's position in integrating new technology into military *vis-à-vis* global players like the US, China and Russia, which lets the reader draw comparison and adjudge India's potential as an emerging technology power within the larger geopolitical context. However, a deeper analysis of how India's strategic autonomy and commitment to resource efficiency could be leveraged in the face of the geopolitical rivalries described in the book, particularly to aid in making disruptive technologies more sustainable for civil as well as military use, would have been a valuable addition.

The book, while extensive in its approach, is not without its limitations. In framing the book's discussion heavily around the control and protection of data, the scope of military applications for technologies like Lethal Autonomous Weapons Systems (LAWS) and quantum computing feels limited. The focus on data securitisation overlooks critical debates on the broader and more complex aspects of these technologies, such as how state control does not extend to predicting outcomes in LAWS, or how quantum computing can be used not just for cybersecurity, but to also dismantle even the blockchains which were, until recently, considered almost impregnable.

In several chapters, there is a duplication of argument regarding ubiquity and importance of technology, especially in military sphere. This is inevitable, given that the chapters have been contributed to by multiple authors. Another issue is of narrative inconsistencies, exemplified by conflicting outlook on the role of the first mover advantage in technology deployment.

One aspect that remains missing in the book is the lack of coverage on indigenous developments in the emerging technologies. While the book is primarily about military integration of technologies within India, most of the focus for technologies like blockchain and quantum computing has been on other countries. There is very little mention of the progress India has made, where India stands with respect to the frontier nations, who is leading development and integration of emerging technologies for Indian military, what are the various weaknesses and hindrances for Indian technological development, etc. More importantly, bolstering of Indian technological milieu is seen from the lens of its defence inputs; Rafale has been argued to be an important upgrade to India's military technology, but their import did little to increase India's actual technical capabilities. The military technology developments should have focused more in indigenous developments, such as using innovation in LCA technology through projects such as Tejas MK-1, Tejas MK-1A, TEDBE, AMCA, etc., as examples instead of Rafale. Given that the reference point for the book is Indian military, not addressing aspects and extent of indigenisation is a significant missed opportunity. The chapters themselves could also have described how the respective technologies can be grown further, rather than limiting to their strategic implications.

Nevertheless, this text comes at a critical juncture, when development and deployment of frontier ICT-based technologies for defence and security is gaining traction. This book is a valuable addition to the narrative around new technologies in military affairs, and will serve as a valuable text for scholars, defence policymakers and military personnel alike, into India's current and potential use of AI, blockchain and quantum communications.