EDITED BY
PANKAJ K JHA, ARUN TEJA POLCUMPALLY,
AND VEDANT SAIGAL

EMERGING DIGITAL TECHNOLOGIES AND INDIA'S SECURITY SECTOR

AI, Blockchain, and Quantum Communications

ROUTLEDGE

EMERGING DIGITAL TECHNOLOGIES AND INDIA'S SECURITY SECTOR

This book is an introductory account for policy makers, academia, and interested readers on the digital technologies on Indian Military. It covers three technologies – AI, Blockchain, and Quantum communications – and provides a detailed account on the military use cases. It evaluates the readiness of Indian Military in these technologies. A foundational text, it not only provides key policy analysis but also identifies the gray areas for the future research in the security studies.

The volume will be essential reading for scholars and researchers of military and strategic studies, especially future warfare, AI and Blockchain, and South Asian studies. It will be of interest to general readers as well.

Pankaj K Jha is Professor with JSIA, O.P. Jindal Global University, and Director of Centre for Security Studies (CSS). He is also Executive Director of CESCUBE, a think tank.

Arun Teja Polcumpally is Technology Policy Analyst at Wadhwani Institute of Technology Policy, Delhi.

Vedant Saigal is Assistant General Manager (University Administrative Services) at the Office of International Affairs and Global Initiatives, O.P. Jindal Global University.

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
Taylor & Francis Group
LONDON AND NEW YORK

Designed cover image: © KanawatTH / Getty Images

First published 2024
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-032-43358-5 (hbk)
ISBN: 978-1-032-77370-4 (pbk)
ISBN: 978-1-003-48270-3 (ebk)

DOI: 10.4324/9781003482703

Typeset in Sabon
by Apex CoVantage, LLC

CONTENTS

TABLES

CONTRIBUTORS

Editors

Dr. Pankaj K Jha – B.A. (Hons.) (University of Delhi); M.A., M.Phil., Ph.D. (Jawaharlal Nehru University, New Delhi)

Pankaj K Jha is Professor with JSIA, O.P. Jindal Global University, and Director of Centre for Security Studies (CSS). He is Executive Director of a research-oriented think tank, known as CESCUBE. Dr. Pankaj K Jha was Director (Research) with Indian Council of World Affairs for more than two and a half years (2014–2017). He had worked as Deputy Director with National Security Council Secretariat (2012–2013). He has been the visiting fellow with Centre for International Security Studies, Sydney University (2009) and Institute for South Asian Studies, Singapore (2006).

He has authored three books on *India and China in Southeast Asia: Competition or Cooperation* (2013) and *India and the Oceania: Exploring Vistas for Cooperation* (2016). His latest book is on *India, Vietnam and the Indo-Pacific: Expanding Horizons* (2020).

Dr. Arun Teja Polcumpally – B. Tech (Electrical), M.A., Ph.D. International Affairs (O.P. Jindal Global University)

Dr. Arun Teja Polcumpally is Technology Policy Analyst at Wadhwani Institute of Technology Policy, Delhi. He was Research Associate at the Centre for Security Studies and Visiting Fellow at the Center for Excellence for AI in Human Security. He formerly had a brief stint as Editor at Jindal Centre for the Global South and an associate at Center of Excellence (CoE) for AI in Human Security, Hyderabad, India. His area of research is the impact of emerging digital technologies like AI and Blockchain on the global power

structure. He also works on the International Relations' theoretical analysis of the technological impacts.

Vedant Saigal – B.A. (Hons.) Global Affairs, M.A. Diplomacy, Law, and Business (Jindal School of International Affairs, O.P. Jindal Global University)

Vedant Saigal is Assistant General Manager (University Administrative Services) at the Office of International Affairs and Global Initiatives, O.P. Jindal Global University. He has a Master's degree in Diplomacy, Law and Business from the Jindal School of International Affairs (JSIA) and a keen interest in Artificial Intelligence and International Security. With a commitment to academic excellence and an unyielding curiosity, he looks forward to contributing to the ever-evolving landscape of Defense and National Security.

Contributors

Sonchita Debnath

Ms. Sonchita Debnath is Doctoral Fellow at Jindal School of Government and Public Policy. Her research tries to understand the community-level factors that determine clean technology's adoption and usage. She has prior research experience with the Government of Maharashtra on mapping food habits among tribals and several other nongovernmental organizations (NGOs) working on impact assessment and designing surveys. She has been invited to various guest lectures within Jindal and outside colleges. She also has experience in teaching at the graduate level.

Rushil Khosla

Rushil is Research Assistant at the Centre for Security Studies.

Poornima Vijaya

Ms. Poornima Vijaya is presently enrolled as Research Fellow at Nehghinpao Kipgen's Centre for Southeast Asian Studies and Ph.D. Scholar at Jindal School of International Affairs in O.P. Jindal Global University. Her research focuses on the changing geopolitical dynamics in the Asia-Pacific region, International Relations theories, middle power politics, and great power rivalry. She tweets @PoornimaVijaya.

INTRODUCTION

Arun Teja Polcumpally

Who wouldn't be interested in the stories of the military and in the events portraying a soldier's valour and bravery? It is expected that to those readers who love to watch movies like *Border, LOC Kargil, Lakshya, URI* and so on, this book will strike a chord. This book is an analytical account of the future of the Indian military. It is divided into two parts. The first part delves into a conceptual understanding of the technological impact on military affairs. It also provides a detailed account on the global competition among digital technologies, emphasising on Russia, China and the US. The second part delves into data-influenced geopolitics and the importance of Artificial Intelligence (AI), block-chain technology and quantum communications in military affairs. Finally, the book explores whether India is ready for such advanced technologies.

The book stresses emerging strategic environments and operational challenges anchored to information technologies. This book builds up an analysis keeping in mind that digitalisation is imperative to improve operational readiness and combat efficiency of the military. In order to provide the Indian Armed Forces with the requisite capacity in the field, it is vital for the organisations involved in the defence sector to run along with the digital curve and make their turns accordingly. For them, to maintain such pace, this book acts as a guide and is also helpful for scholars, defence officials and others contributing to the nation's security. It helps them understand the possible options for India to consider, to become a better digitalized force altogether.

Current Developments Regarding This Research

A search using the keywords "emerging technology" + "national security" + "India" in Microsoft Academic resulted in 1032 search results, and a search

DOI: 10.4324/9781003482703-1

in Google Scholar resulted in 1740 results. Both searches are done between January 1, 2017, and September 7, 2022.

The first 10 pages of the results in Microsoft Academia did not produce any paper on military and digital technologies. Only one paper was found relevant that focused on drone detection, which has an application in the military (Carrio et al., 2018).

Screening of 10 Google Scholar search pages provided a better result than Microsoft Academia. It is found that the research is conducted on public engagements in nano-technology (Barpujar, 2011), exploratory study on Indian space strategy (Chandrashekar, 2016), general implications of AI (Vempati, 2016; Bommakanti, 2020) and Information Technology–based governance and business (Chaturvedi et al., 2011; Ranjan, 2020; Sarkar, 2014). Within the 10 search result pages, there was no research paper on the mapping of revolutionary change in warfare and emerging digital technologies with India as a vantage point. From the search results, it can be established that a potential secondary search is possible on this topic.

This book is divided into two parts. Part I provides a conceptual understanding of technology-induced changes in military affairs. The conceptual explanation will follow the current geopolitical scape of frontier technologies and India's position on adopting digital technology in its military. Part II deals with AI, blockchain and quantum communication technology. Along with this, the cyber security apparatus of India is analysed.

Part I

The first chapter brings in the context for the entire book and describes the difficulties in integrating the frontier digital technologies into the military. While examining the frontier digital technologies and their impact, the chapter argues that the state is still the main agency in conducting international relations. The digital technologies are opined to aid the state to increase its coercive power over the public. This argument has been explained by mapping the digital technologies and the agencies that use them. The chapter maintains that the frontier digital technologies unquestionably change the military affairs and asserts that India should proactively work towards adopting those technologies.

The second chapter introduces the reader to the concepts of Revolution in Military Affairs (RMA). The explanation is provided with information technology as a vantage point and is built on the societal impact of emerging technologies. Taking the discussion to the military, the concepts of revolution, warfare and the changes occurring in how war is/will be waged in the future are explored. An extensive dependence on RAND organisations shows that the chapter is very precise in its analysis. AI technology has been taken as an example to showcase the possibility of RMA in military. After establishing

that the frontier digital technologies can bring an RMA, the second chapter espouses conditions of hybrid warfare. The amalgamation of the traditional military, the usage of local proxy militia, exertion of economic pressure, disinformation campaigns and exploitation of the existing social divisions is called hybrid warfare. Employing coercive information warfare leading to psychological control of the societies has been given a greater importance in the hybrid warfare. The chapter opines that every entity that has control over information technology can wage psychological war on any nation or a specific society. Further, it is asserted that new-generation warfare is won with psychological control over people (Wither, 2016). In such a scenario, using digital technologies to improve national security becomes a desideratum. With the aggregation of emerging digital technologies into the defence, there is an emerging view of having separate cyber and space forces (Winkler et al., 2019). These changes make it evident that the old hard power usage in the war is no longer a viable strategy. It looks like militaries have to use hybrid strategies to achieve a victory and sustain it. Substantiating the argument that frontier digital technologies would bring an RMA, an impressive list of historical revolutions in military has been documented. It is interesting to see that the chapter carefully treads its argument by separating the revolution in military affairs and the revolution in war.

The third chapter argues with the premise that in the anarchical world with rapidly growing technologies, a state has to invest on the research and development of the digital technologies. Those states that do not focus on the innovations of digital technologies, such as AI, blockchain and quantum technology, would forever import the technologies. The main discussion that this chapter brings is the geopolitical competition between the major powers including Russia, the US and China. During the Trump presidency, the aggressive stance of the US against the growing Chinese technology acquisition shows that China is challenging the US supremacy in the knowledge-building domain.

The chapter argues that Chinese Communist Party (CCP) is the major investor in the defence technology research and development in China. Though a surge in private investments is observed, the state has a representation and influence in the decision-making board of private companies. Similarly, the defence industry of Russia is also dominated by the state. It has been observed that Russia is taking steps to encourage research in the technologies like AI through its Advanced Research Foundation (ARF). The US is advanced in terms of research and development, as it allows private industry and pushes huge state funds into the defence research. With a capitalistic orientation of defence industries, the US emerged as a sole superpower after 1991. The emergence of China as a global economic power challenged the US supremacy over the geopolitics. With the current pace of advancements in the digital technologies, the chapter opines that the global rivalry would be between Russia, China and the US.

In the fourth and final chapter of Part I, the strategic implications and the readiness of Indian military are assessed within the context of the advanced digital technologies. The author quickly and precisely traces the Indian military approach and their strategic ploys. The author notes that India consistently changes its strategic stance. It is observed from the period of having a single belligerent in the early 1950s to the state becoming a regional power in the 21st century. As of the year 2022, the chapter asserts that India's greatest military challenge is China's informatisation and intelligentisation. In this context, the fourth chapter discusses the recent developments in the Indian military arsenal and its road map to the military digitisation. It identifies that there are a significant number of projects that are mentioned in the compendium reports of the Army which are not solved and implemented. It is also noted that problems that appear in an annual compendium of reports will reappear in the next year's report. Such tracing helps the reader in understanding the vital areas where digital technologies are required. Finally, this chapter provides a method to observe India's readiness to the changing technologies.

Part II

Part II of the book builds up on the foundations laid by Part I. The introductory chapter of Part II, that is the fifth chapter, provides an analytical description of how digital technologies impact a society. Rather than treading the path of traditional security involving military, this chapter emphasises the threat to the democracy. Before explaining the threat to the democracy, this chapter highlights the importance of data securitisation and its legislation. Perspectives of Yuval Noah Harari and Jamie Susskind are used to strengthen the conceptual and philosophical understanding of the data-based technologies and their impact on the society. This conceptual description is followed by the examination of the phenomenon of perception control. The question whether data becomes a new weapon for the authoritarianism in the democracies is discussed upon in this chapter. This chapter confirms that data-led digital technologies are not only making unprecedented changes in the traditional security institutions but also impact the non-traditional security.

The sixth chapter explores the usage of AI in the Indian Armed Forces and how the military technologies make use of AI for defensive or offensive purposes. The chapter explains the role of AI in the three branches of the Indian Armed Forces, that is, Army, Navy and the Air Force. The challenges faced by Indian defence establishment are explained with an emphasis on additional capital requirement, AI bias. The future warfare is opined more to be hybrid warfare coated with information tactics. In addition, cyber capacities are opined to be an alternative to the nuclear deterrence. The chapter concludes asserting that to achieve battlefield dominance, the military forces

are continuously seeking greater combat effectiveness, and they can do so by establishing more research and development in the field of AI (Pant, 2018).

With the profound understanding of AI and its uses in the Indian Armed Forces, the seventh chapter looks at the other domain known as quantum communications. Similar to the previous chapter, this section of the book will highlight the use of technology in the military. With an international lens, emphasis is laid on the development of the technology in China, India, the US and Europe, and a comparative analysis is provided. The importance of quantum communications and the unparalleled security it offers through the quantum key distribution (QKD) method is explained in detail. Will India be able to become the major cyber power in this century? Will the investments made by India in the field of quantum communications contribute to it becoming the cyber-technology powerhouse? How different is India's position in terms of digital infrastructure from that of the US and China? These questions definitely pose a great scope of relevance in today's highly advancing world. This chapter provides a direction to analyse what these questions demand for and provide an understanding of what the future perhaps brings.

The eighth chapter is about the usage of blockchain technology in the military. The chapter is organized into three different sub-sections that provide an elaborated understanding on history and the whole working of the blockchain technology. The chronological order is that provides a systematic analysis of the whole evolution of the blockchain technology. This chapter explains how this type of technology is being seen as a panacea for all the issues and difficulties that are currently being faced by the system. As the challenges are intertwined with new developments, the chapter throws light on issues that perhaps would help the implementation of technology in the hierarchical system of the military.

The ninth chapter of the book revolves around the social-technical iterations that eventually create a new social. This new social further creates a security threat known as cyber security. This stands as one of the most important chapters of the book as it involves a direct civilian threat through the mode of computers' illegal use of the cyberspace altogether. The significance of this particular chapter is important not only for the officials working in the defence sector but also for the ordinary citizens of a country. Hence, observing the events that cause the cybercrime and lead to various devastating consequences becomes equally important. This chapter does not really look at the comparative analysis of different countries with India but brings them into a common space that is created by threats emerging in the cyber world. As the word suggests, where comes security come threats and challenges; therefore, this chapter emphasises on the cyber security structure of India and espouses on how the country is responding to the upcoming challenges. The development of an ecosystem which is underway in recent years will be

discussed upon. In a nutshell, this chapter aims to provide an initial reading on the cyber security issues and the way in which India dealt with it.

The concluding chapter comments on the aspect of RMA in the digital world. In addition to its comment on the earlier chapters, it asserts that the RMA-level innovations should be carried out to increase the deterrence and non-lethal weaponry. Further, the chapter concludes that the countries that are close to the US would benefit more from the latest digital innovations. While reiterating the RMA, this chapter asserts that the revolution brought by the frontier digital technologies shall bring a complete change in the way command centres operate. With tactical internet, and AI imbibed with data from nano sensors, every minute detail will be considered in taking decisions on the battlefield. Further, all those details will be monitored in the real time by the unit command located away from the field. While detailing the challenges, the chapter focuses on the ethical and operational challenges in implementing the frontier technologies into the military. Closing the book, the concluding chapter opined that India should have a robust cyber security strategy designed on the blueprints of the future laden with frontier digital technologies.

This book is expected to serve all the interested readers with a detailed conceptual note on the revolution in military affairs that is hoped with the frontier digital technologies. With a detailed analysis of the AI, blockchain and quantum communication technologies, this book serves the purpose of providing a foundational reading for all those who work practically on these technologies in the military domain. It helps the readers to identify the problem areas and the potential business areas to capture anchored on these three technologies. Further, the cyber security lacuna and the possible bridging of that lacuna are also analysed. It warps the long discussion of the nine chapters by reiterating the importance of securitisation of the frontier digital technologies.

References

Barpujari, I. (2011). Public Engagement in Emerging Technologies: Issues for India. *Quantum Engagements: Social Reflections of Nanoscience and Emerging Technologies*, 123–137.

Bommakanti, K. (2020). AI in the Chinese Military: Current Initiatives and the Implications for India. ORF Occasional Paper No. 234.

Carrio, A., Vemprala, S., Ripoll, A., Saripalli, S., and Campoy, P. (2018, October). Drone Detection Using Depth Maps. 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (pp. 1034–1037). IEEE.

Chandrashekar, S. (2016). Space, War, and Deterrence: A Strategy for India. *Astropolitics*, *14*(2–3), 135–157.

Chaturvedi, M., Gupta, M. P., and Bhattachrya, J. (2011). Information Security Issues With Emerging Next Generation Networks in Indian Context. *Proceedings of 8th International Conference on E-Governance* (pp. 78–90). Emerald Group Publishing Limited.

Pant, A. (2018). Future Warfare and Artificial Intelligence: Visible Path. IDSA Occasional Paper 4–50.

Ranjan, P. (2020). Industry 4.0 and Industrial Information Services in India: A Proposal. National Seminar on Industry 4.0: A Roadmap for Indian Business, 2018

Sarkar, S. (2014). The Unique Identity (UID) Project, Biometrics and Re-Imagining Governance in India. *Oxford Development Studies*, *42*(4), 516–533.
Vempati, S. S. (2016). *India and the Artificial Intelligence Revolution* (Vol. 1). Washington, DC: Carnegie Endowment for International Peace.
Winkler, J., Marler, T., Posard, M., & Cohen, R. (2019). Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense. *RAND Cooperation*, *43*.
Wither, J. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal*, 73–87.