The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 5 | May 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

AI, Big Data, and Cybersecurity in Defence: A Strategic Review

Dr. Harsimran Kaur

Assistant Professor, Defence and Strategic Studies, RIMT University, dr.simran.rimt@gmail.com

Rosetta K Fomba

M.A. Defence and Strategic Studies, RIMT University Rosettafomba847@gmail.com

ARTICLE DETAILS

Research Paper

Accepted: 27-05-2025

Published: 10-06-2025

Keywords:

Cybersecurity, National Security, Digital Warfare, AI Ethics, Defence innovation

ABSTRACT

In an increasingly digitized world, the convergence of Artificial Intelligence (AI), Big Data, and cybersecurity is reshaping the landscape of national defence and strategic planning. This review paper explores how these technologies are being integrated into defence systems, the opportunities they offer, and the challenges they pose for military and strategic decision-making. AI enhances threat detection, predictive analysis, and autonomous operations, while Big Data enables the processing of massive volumes of information crucial for real-time responses. However, the growing reliance on these technologies also introduces new vulnerabilities, such as algorithmic bias, data breaches, and sophisticated cyberattacks. This paper critically examines existing literature and strategic doctrines to assess how countries, particularly major powers, are adapting their defence strategies to manage these evolving cyber threats. It also highlights the need for robust cybersecurity frameworks, ethical considerations, and international cooperation to ensure the responsible and secure use of AI and Big Data in defence contexts. By providing a comprehensive overview of current trends, gaps, and future directions, this review contributes to a deeper understanding of the strategic implications of emerging technologies in the domain of national and international

security.

DOI : https://doi.org/10.5281/zenodo.15658797

Introduction

In the 21st century, warfare and national security have expanded far beyond traditional battlefields. The rapid advancement of digital technologies has given rise to new domains of conflict, where data, algorithms, and networks play a central role. Among these technologies, Artificial Intelligence (AI) and Big Data analytics have emerged as critical tools in modern defence strategies. Their integration into military systems is transforming decision-making, surveillance, intelligence gathering, threat detection, and even combat operations. At the same time, this growing dependency on digital infrastructure has made cybersecurity a top strategic priority, as state and non-state actors increasingly target cyber networks to compromise national security. AI enables the automation of complex tasks, real-time data analysis, and the development of predictive models that can anticipate enemy actions or detect cyber intrusions with high precision. Big Data, on the other hand, allows defence agencies to collect, process, and analyse massive amounts of structured and unstructured data from various sources, including satellites, drones, communication systems, and open-source intelligence. When effectively combined, these technologies can significantly enhance situational awareness and operational efficiency in defence environments. However, this technological evolution also presents significant challenges. The integration of AI and Big Data systems increases the attack surface for cyber threats, raises ethical concerns regarding the use of autonomous weapons, and introduces questions about data privacy, accountability, and control. Furthermore, the lack of international norms governing cyber warfare and the weaponisation of AI creates a volatile strategic environment. In this context, it becomes essential to critically examine how AI, Big Data, and cybersecurity intersect in the defence sector, and what strategic implications this convergence holds for national and global security. This review aims to synthesise existing literature, analyse current practices and trends, and identify gaps in strategy, policy, and preparedness. The study focuses not only on technological capabilities but also on the broader strategic, ethical, and geopolitical dimensions of using AI and Big Data in defence.

Literature Review

1. The Integration of AI in Defence Systems

Artificial Intelligence is transforming defence operations by enabling faster and more accurate decision-making, automating threat detection, and improving the efficiency of surveillance and reconnaissance. Militaries across the world are investing heavily in AI for both strategic and tactical purposes. According to Horowitz, Allen, Kania, and Scharre (2018), AI is being used in autonomous drones, intelligent command systems, and predictive analytics for cyber threat management. The U.S. Department of Defence has outlined AI as a critical capability for future warfare, emphasising its potential to enhance battlefield situational awareness and reduce response time (U.S. DoD, 2020). China and Russia have also acknowledged the strategic significance of AI, incorporating it into their military modernisation programs (Kania, 2019). However, the integration of AI in military applications raises ethical questions about autonomous weapons and the delegation of life-or-death decisions to machines (Cummings, 2017). These concerns underscore the need for governance frameworks and accountability mechanisms.

2. Big Data as a Strategic Asset in National Security

Big Data analytics has emerged as a cornerstone of modern defence planning and intelligence operations. The ability to collect, process, and analyse vast datasets from sources like satellites, sensors, social media, and electronic communication allows defence agencies to detect patterns, forecast threats, and make evidence-based decisions in real time (Gandomi & Haider, 2015). Big Data is especially useful in counterterrorism, cyber threat intelligence, and border surveillance. For example, India's Defence Research and Development Organisation (DRDO) and agencies like the National Technical Research Organisation (NTRO) are exploring Big Data tools to improve national surveillance and strategic planning (Sharma & Kumar, 2021). However, the management of such large volumes of data brings challenges related to data quality, interoperability, and security. Without proper infrastructure and cyber hygiene, the benefits of Big Data could be undermined by system vulnerabilities or data breaches.

3. Cybersecurity: The Invisible Battlefield

The increasing reliance on digital technologies in defence has made cybersecurity a critical pillar of national security. Cyber-attacks targeting military databases, defence contractors, or critical infrastructure can cause significant disruption, data leaks, or even strategic failure. States are now developing cyber commands and offensive cyber capabilities to defend their digital assets and project

power in cyberspace (Healey, 2013). The 2007 cyber attack on Estonia and the 2015 breach of the U.S. Office of Personnel Management (OPM) are often cited as watershed moments that highlighted the vulnerabilities of state cyber infrastructure (Libicki, 2009). In response, countries like Israel have made cybersecurity a central focus of their national defence policy, integrating it into both military doctrine and public-private partnerships (Senor & Singer, 2009).

National Cyber Security Policy of India (2013) laid the groundwork for developing indigenous cyber capabilities, though experts argue that significant gaps remain in coordination, infrastructure, and skill development (Singh & Raghavan, 2020). The need for robust cyber hygiene practices, real-time monitoring, and continuous investment in cyber defence technologies is now more urgent than ever.

4. Strategic and Ethical Challenges in the Convergence of AI, Big Data, and Cybersecurity

The convergence of AI, Big Data, and cybersecurity presents both opportunities and risks. While it enhances a nation's ability to anticipate and neutralise threats, it also increases complexity and potential unintended consequences. AI-driven systems trained on biased or incomplete data can make flawed decisions, while Big Data analytics may violate privacy norms or generate false positives that lead to unnecessary actions (O'Neil, 2016). Also, the lack of international norms and treaties governing cyber warfare and AI in defence creates a legal and strategic vacuum. There is growing concern that unchecked development could lead to an arms race in autonomous and cyber weapons, making conflict escalation more likely (Taddeo & Floridi, 2018). Scholars emphasise the need for interdisciplinary collaboration between technologists, strategists, ethicists, and policymakers to ensure that emerging technologies serve national interests without compromising democratic values or global stability (Brundage et al., 2018).

Research Methodology

This study employs a qualitative, thematic literature review methodology to explore the strategic role of Artificial Intelligence (AI), Big Data, and cybersecurity in the defence sector. The objective is to synthesise existing knowledge and provide a structured overview of current trends, gaps, and strategic implications of these technologies in national and international defence contexts.

Data Sources and Collection

- Data was gathered from a wide range of credible secondary sources, including:
- Peer-reviewed journal articles from databases such as ScienceDirect, JSTOR, Taylor & Francis, and IEEE Xplore
- Official government publications (e.g., U.S. Department of Defence, Indian Ministry of Defence)

Selection Criteria

- Publications were selected based on the following criteria:
- Relevance to the themes of AI, Big Data, cybersecurity, and defence strategy
- Publication between 2013–2024
- Inclusion of either theoretical frameworks or empirical case studies
- Authoritativeness of the source (e.g., scholars, government agencies, recognised policy institutes)

Analytical Framework

- A thematic analysis was used to categorise the literature into four key themes:
- AI applications in defence strategy
- Big Data and its military utility
- Cybersecurity challenges in national defence
- Ethical, strategic, and policy concerns

The literature was reviewed, annotated, and synthesised to identify emerging trends, technological impacts, strategic responses, and potential research gaps.

Conclusion

The intersection of AI, Big Data, and cybersecurity is fundamentally reshaping the nature of defence strategy and national security. AI offers real-time decision-making and automation, Big Data enables strategic intelligence at unprecedented scales, and cybersecurity is the linchpin that ensures the integrity and resilience of these systems. Together, these technologies offer immense potential but also introduce new vulnerabilities, ethical dilemmas, and strategic uncertainties. This review reveals that while technologically advanced nations are making significant progress in integrating these tools, there remain critical gaps in policy, infrastructure, and international governance. As cyber threats become more complex and geopolitical tensions intensify, defence establishments must adopt a proactive, ethical, and

collaborative approach to the use of emerging technologies. There is a pressing need for continued research, cross-sectoral dialogue, and global cooperation to ensure these technologies are used in ways that enhance security while minimizing risks. Future studies should focus on regional preparedness, comparative strategies, and the development of normative frameworks to govern the military use of AI and cyber capabilities.

References

- Brundage, M., et al. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute.
- Cummings, M. L. (2017). Artificial intelligence and the future of warfare. Chatham House.
- Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, 35(2), 137–144.
- Healey, J. (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association.
- Horowitz, M. C., Allen, G. C., Kania, E. B., & Scharre, P. (2018). Strategic competition in an era of artificial intelligence. Center for a New American Security.
- Kania, E. B. (2019). AI weapons and China's military innovation. Brookings Institution.
- Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.
- O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown Publishing Group.
- Senor, D., & Singer, S. (2009). Start-up Nation: The Story of Israel’s Economic Miracle. Twelve.
- Sharma, A., & Kumar, A. (2021). Big Data and National Security: Indian Perspectives. Journal of Strategic Studies, 43(2), 198–214.
- Singh, M., & Raghavan, R. (2020). India's cyber security strategy: Issues and challenges. ORF Occasional Paper, Observer Research Foundation.
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751–752.
- U.S. Department of Defense (2020). Summary of the 2018 Department of Defense Artificial Intelligence Strategy. https://www.defense.gov/