Assessing Trade off between efficiency and Security Concern in AI adaption in Defense sector with India & Global Perspective

Dr. Chandravadan Gorityal & Mr. Rishi Hiran

Prin. L.N. Welingkar Institute of Management Development & Research (PGDM), Mumbai, Maharashtra, India

DOI: https://doi.org/10.47772/IJRISS.2026.1014MG0215

Received: 25 October 2026; Accepted: 30 October 2026; Published: 17 November 2026

ABSTRACT

Artificial Intelligence (AI) is increasingly being adopted in defense organizations to improve operational efficiency, decision-making, logistics, procurement, and administrative functions. However, the adoption of AI in high-security environments also raises concerns related to cybersecurity, confidentiality, ethical governance, and regulatory compliance. This study examines the trade-off between efficiency gains and security risks associated with AI adoption in defense organizations.

The research is based on secondary data collected from academic literature, policy reports, government publications, and institutional case evidence. The study applies the Technology Acceptance Model (TAM) and the Technology-Organization-Environment (TOE) framework to analyze factors influencing AI adoption, with particular focus on perceived security risk as a moderating factor.

The findings indicate that AI can significantly enhance operational performance through automation, predictive analytics, and intelligent decision-support systems. At the same time, concerns regarding cyber threats, data protection, transparency, and national security continue to limit broader implementation. The study highlights the importance of secure AI governance frameworks and risk-management strategies to balance technological advancement with security priorities in defense institutions.

Keywords: Artificial Intelligence, Defense Organizations, AI Adoption, Operational Efficiency, Security Risks, Cybersecurity, TAM, TOE Framework, National Security.

INTRODUCTION

\ Background to the Study

The rapid diffusion of Artificial Intelligence (AI) across institutional domains has fundamentally altered the calculus of organizational efficiency. In few sectors is this transformation more consequential or more contested than in defense. Historically insulated from commercial technology trends by imperatives of security and confidentiality, defense organizations worldwide now confront an urgent strategic reality: the failure to adopt AI at scale risks ceding a decisive technological edge to adversaries who will not exercise the same restraint.

Military organizations increasingly see AI as a capability capable of improving efficiency, accuracy, and strategic decision-making across operations (Hooda, 2023), spanning domains as varied as logistics optimization, predictive maintenance, intelligence analysis, procurement automation, and administrative process management. This institutional recognition has translated into substantial fiscal commitment. The U.S. Department of Defense's unclassified AI investments rose from slightly over $600 million in 2016 to approximately $1.8 billion in 2024, with more than 685 active AI projects currently underway (European Parliamentary Research Service, 2025). At a global level, the AI in defense market, valued at $9.31 billion in 2024, is projected to reach $19.29 billion by 2030 growing at a CAGR of 13.0% and to $65.43 billion by 2034 (Grand View Research, 2024; Precedence Research, 2024; Cervicorn Consulting, 2024).

Yet this accelerating adoption is not occurring in a vacuum of risk. As the Pentagon races to adopt the latest commercial advances in AI, risks to soldiers, civilians, and national security are mounting raising concerns about ineffective, unsafe systems and the absence of meaningful safeguards or independent oversight (Brennan Center for Justice, 2024).

The tension between the efficiency promise of AI and the security imperatives unique to the defense context constitutes the central problem of this research.

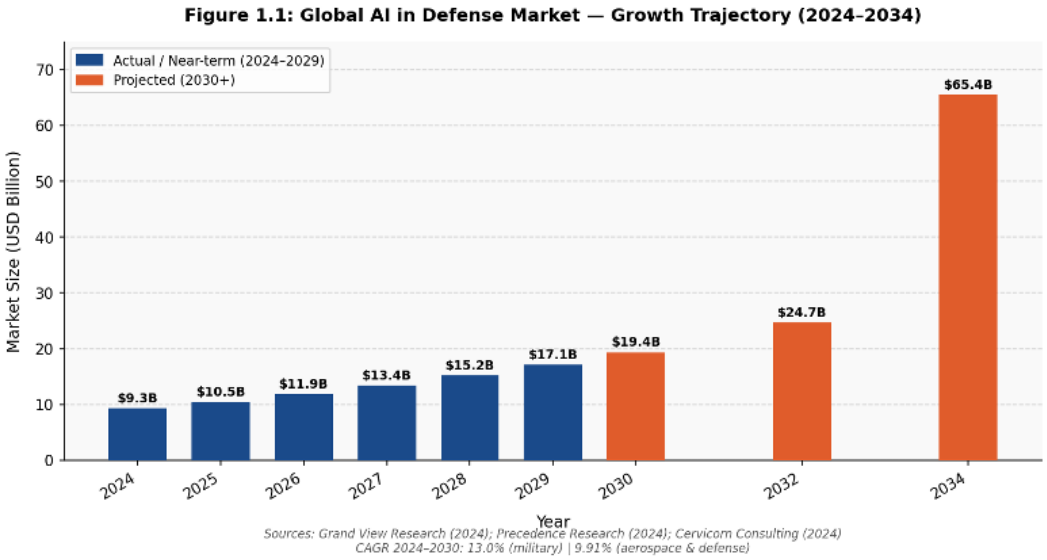


Figure 1.1: Global AI in Defense Market Growth Trajectory (2024–2034) Sources: Grand View Research (2024); Precedence Research (2024); Cervicorn Consulting (2024)

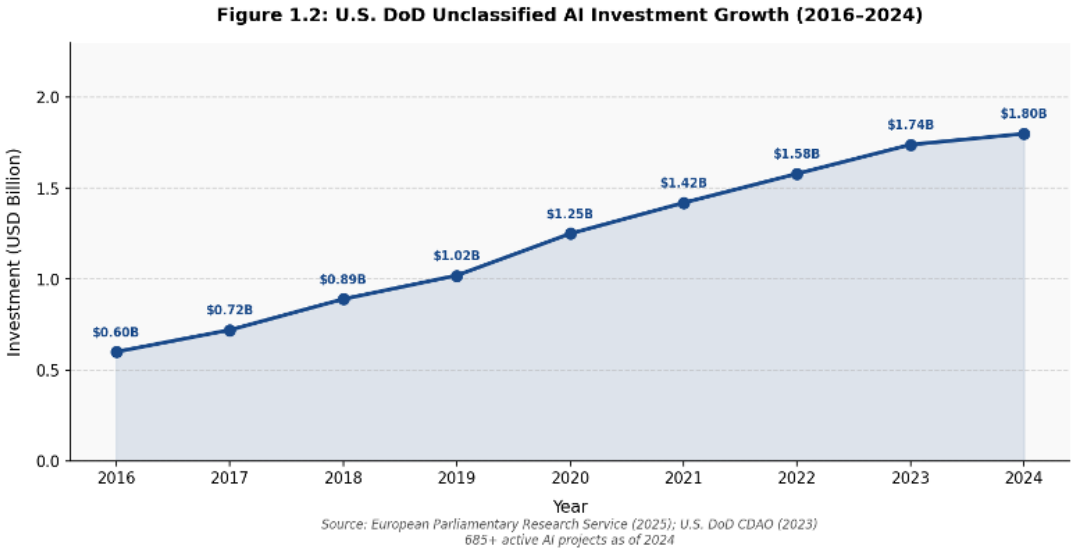


Figure 1.2: U.S. DoD Unclassified AI Investment Growth (2016–2024) Source: European Parliamentary Research Service (2025); U.S. DoD CDAO (2023)

Context: The Policy and Strategic Landscape

In November 2023, the U.S. Deputy Secretary of Defense published the DoD Data, Analytics, and Artificial Intelligence Adoption Strategy, establishing an "AI Hierarchy of Needs" grounding adoption in data quality, governance, responsible assurance, and analytical insight (U.S. Department of Defense, 2023). NATO released a revised AI strategy in 2024, establishing standards for responsible use, protection from adversarial exploitation, and accelerated adoption (European Parliamentary Research Service, 2025). The United Kingdom's Ministry of Defence introduced Joint Service Publication 936 in November 2024, establishing the

principal policy framework for safe and responsible AI adoption throughout the defense AI lifecycle (UK Ministry of Defence, 2024).

In India, the Defence AI Council (DAIC) headed by the Defence Minister and comprising the three service chiefs, the Defence Secretary, the National Cyber Security Coordinator, and members from DRDO, industry, and academia provides the apex governance body for AI adoption in Indian defense (Hooda, 2023). The Government of India has earmarked ₹100 crore annually for AI in military projects, supported by the ₹6.81 lakh crore defence budget for FY 2025–26, and the iDEX/ADITI ecosystem has engaged over 619 startups and MSMEs and awarded 430 contracts worth more than ₹2,400 crore (India Strategic, 2025; IMPRI, 2025).

Statement of the Problem

Despite the growing volume of research on AI in organizational contexts, the specific trade-off between operational efficiency and security concerns in the defense sector remains insufficiently examined. The extant literature tends to bifurcate: studies on AI efficiency gains in defense focus predominantly on technological capability without adequately interrogating the security consequences; conversely, studies on AI security risks are often framed through a purely cybersecurity lens without accounting for the organizational efficiency costs of security-driven constraints on AI adoption.

Furthermore, security concerns surrounding cybercrime, theft, hacking, and data destruction have heightened the need for advanced AI and machine learning in the military yet these same concerns create institutional resistance to the very AI adoption they demand (Adapt Forward, 2023). This paradox where AI is simultaneously the solution to security challenges and a source of new ones makes the defense sector a uniquely important context for examining the efficiency-security trade-off.

Significance of the Study

This research makes three contributions to the academic and policy literature on AI adoption in high-security organizations. First, it provides a structured, multi-domain analysis of the efficiency-security trade-off moving beyond aggregate claims toward a domain-specific examination. Second, it contributes to the Technology Acceptance Model (TAM) and Technology-Organization-Environment (TOE) framework literature by examining how perceived security risk functions as a moderating variable. Third, it offers an analytically grounded secondary research study using policy documents, academic literature, and institutional case evidence a methodological approach well-suited to a sector where primary data access is structurally constrained by classification requirements. The defense and national security segment held a 42.60% market share in the AI aerospace and defense market in 2024 (Precedence Research, 2024), underscoring the urgency of this analysis.

Research Objectives

This study is guided by the following objectives, as approved in the synopsis:

1. To examine the potential efficiency gains arising from AI adoption across various defense functions, including operations, logistics, decision-support systems, procurement, and administrative processes.

2. To analyze the security, confidentiality, and regulatory concerns that influence AI adoption decisions in defense organizations.

3. To assess the trade-off between operational efficiency and security risks, and evaluate how defense institutions balance technological advancement with national security priorities.

4. To identify key factors that affect AI adoption of readiness within high-security environments.

Research Hypotheses

Drawn from the approved synopsis, the three hypotheses guiding this study are:

H1: AI adoption positively influences operational and administrative efficiency within the defense sector.

H2: Security concerns significantly moderate AI adoption decisions in defense organizations.

H3: The efficiency-security trade-off differs across functional domains within the defense ecosystem.

Scope and Limitations of the Study

This study focuses on institutional AI adoption within the defense sector, encompassing operations, logistics, procurement, decision-support, and administrative functions. It deliberately excludes battlefield-specific or weapons-grade AI systems such as lethal autonomous weapons where classified constraints and ethical considerations lie beyond the scope of this study. The research relies exclusively on secondary data. The geographic scope encompasses the United States, United Kingdom, NATO member states, and India. A key limitation is the asymmetry of publicly available information: classified programs remain outside the analytical boundary of this study. Additionally, the rapidly evolving nature of AI technology means specific benchmarks cited may require contextual updating over time.

Organization of the Report

Chapter 2 presents a systematic review of the literature across four thematic clusters. Chapter 3 presents the conceptual model, research hypotheses, and secondary data research design. Chapter 4 tabulates and maps the evidence. Chapter 5 presents the analysis and findings, testing the three hypotheses. Chapter 6 draws conclusions and domain-specific recommendations. All references are consolidated at the end of the dissertation.

LITERATURE REVIEW

Introduction to the Literature Review

This chapter presents a systematic review of the secondary literature organized into four thematic clusters: (i) theoretical frameworks governing technology adoption, (ii) AI-driven efficiency gains in defense functions, (iii) security concerns arising from AI adoption in high-security environments, and (iv) the regulatory and governance landscape. The chapter concludes with identification of the research gap this study addresses.

Thematic Cluster A Theoretical Frameworks for Technology Adoption

The Technology Acceptance Model (TAM)

The Technology Acceptance Model, originally proposed by Davis (1989), remains the foundational framework for understanding how individuals within organizations decide to accept or reject new technology. TAM is considered the most widespread model for measuring user acceptance and describes behavioral intention or willingness to use technology through underlying attitudes, with perceived usefulness emerging as the most significant predictor of attitude towards use (Frontiers in Artificial Intelligence, 2025). In the context of AI adoption, TAM has been extended to incorporate perceived risk and trust which are especially salient in high-security organizational environments such as defense institutions.

A bibliometric analysis of 91 articles on AI adoption identified four major themes: AI, machine learning, UTAUT, and TAM, noting that these adoption theories have been utilized to a limited extent in specific high-security industries (Springer Information Technology and Management, 2024). TAM does not specify external factors such as technology-related faults or organizational decision-making processes, both of which play a significant role in military organizations (Springer, 2024a). This limitation of pure TAM motivates the use of an extended combined framework for the present study.

The Technology-Organization-Environment (TOE) Framework

The TOE framework, introduced by Tornatzky and Fleischer (1990), provides a firm-level model explaining

adoption challenges from technological, organizational, and environmental perspectives. A meta-analysis of 12 studies with 3,398 respondents found that seven out of eight TOE factors have a statistically significant effect on AI adoption; technological factors including compatibility and relative advantage have positive impacts, while organizational readiness and management support serve as positive moderating effects (Discover Artificial Intelligence, 2025). These findings are directly applicable to the Indian defense context, where government support through iDEX, ADITI, and DRDO technology transfer programs are documented drivers of AI adoption, while organizational readiness within legacy DPSUs remains a moderating constraint.

An empirical study integrating TAM with the TOE framework in the governmental sector found a significant association between TAM constructs and AI acceptance and adoption, suggesting that a combined TAM-TOE lens captures both individual-level perceptions and organizational-level determinants that govern AI adoption in security-oriented institutions (ETASR, 2024).

TAM in Military Technology Adoption

Research applying TAM to military technology acceptance concludes that trust particularly questions of trust in technology and the relationship between risk and control leads directly to ethical and operational questions about how much control the soldier is willing to cede to autonomous machines (Springer, 2024a). This finding has significant implications for H2: that security concerns significantly moderate AI adoption decisions in defense organizations. Trust and perceived risk operationalize the mechanism through which security concerns exert their moderating influence.

Thematic Cluster B AI-Driven Efficiency Gains in Defense Functions

Operational and Logistics Efficiency

AI adoption in defense operations has demonstrated measurable efficiency gains across multiple national contexts. The U.S. DoD's Project Maven reduced drone footage processing time from hours to minutes (C4ISRNET, 2024). AI is now incorporated across command and control, intelligence, surveillance, logistics, healthcare, information warfare, cyber warfare, training, and autonomous systems globally (DRAS, 2025). In India, DRDO's CAIR has developed 75+ AI products, while India is pushing for faster decision-making, reducing human errors and improving operational efficiency with AI (Hooda, 2023; India Strategic, 2025).

The most definitive real-world validation of AI-driven operational efficiency in the Indian defense context came in May 2025 with Operation Sindoor India's tri-service precision strike operation against terror infrastructure in Pakistan and Pakistan-occupied Kashmir. According to Lt. General Rajiv Kumar Sahni, who served as the Director General of Information Systems during the operation, the Indian Armed Forces achieved a 94% accuracy rate in identifying and targeting enemy assets by processing 26 years of battlefield data collected from satellites, drones, radar sensors, electronic intercepts, and weapon telemetry through AI-based analytics (The Defense News, 2025). AI-enabled Meteorological Reporting Systems analyzed real-time atmospheric data including wind speed, humidity, and temperature to improve long-range targeting accuracy, enabling artillery, drones, and missile strikes to hit high-value assets with unprecedented precision even in challenging weather conditions (The Defense News, 2025).

Operation Sindoor also validated AI-enabled electronic warfare as an operational efficiency multiplier. The Rafale jets' X-Guard AI-enhanced electronic warfare system generated adaptive jamming patterns that confused Pakistani air defense radars leading Pakistani missiles to go astray and enabling the IAF to complete its mission in just 23 minutes without loss of a single Indian asset (Uday India, 2025). India's indigenous NavIC navigation system delivered positioning accuracy of 10 to 20 centimetres, significantly more precise than GPS systems (Reflections Live, 2025). The operation used entirely domestically developed or assembled systems BrahMos missiles, Akashteer air defense units, Drishti 10 UAVs, and Agnikaa loitering munitions validating the Aatmanirbhar Bharat defense manufacturing doctrine at scale (PIB, 2025).

India's post-Sindoor AI defense roadmap reflects institutional learning from this operational experience. The Indian Army is fast-tracking AI integration with a detailed 2026–27 roadmap incorporating autonomous systems, cybersecurity measures, secure data lakes with strict access controls, and human oversight protocols

including Project Storm Drone (AI-enabled autonomous room-intervention drones), LLM-based text summarizers for intelligence reports, and AI tools for operational logistics (PWOnlyIAS, 2025). Significantly, the roadmap explicitly addresses the efficiency-security trade-off by embedding human oversight protocols and secure data governance alongside each AI capability deployment an institutional acknowledgment of H2 of the present study.

Connectivity as a Force Multiplier: The Starlink-Ukraine Case

The Russia-Ukraine war provides the most extensively documented contemporary case study of how AI-enabled communication infrastructure can function as a decisive operational efficiency multiplier and simultaneously expose the security vulnerabilities inherent in dependency on privately controlled technology. When Russia invaded Ukraine in February 2022, its initial strikes targeted terrestrial communication infrastructure, disabling much of Ukraine's military command-and-control capability and severing internet connectivity across contested areas (Jayanti, 2023). Within 48 hours of a direct appeal by Ukraine's Vice Prime Minister Mykhailo Fedorov, SpaceX activated its Starlink low-earth-orbit satellite internet service over Ukraine, delivering the first truckload of terminals within days (CIRCLEid, 2026). By mid-March 2022, more than 5,000 terminals were operational; by May 2022, over 150,000 Ukrainians including military units were using Starlink daily (CIRCLEid, 2026).

The efficiency gains were immediate and decisive. Starlink permitted Ukraine's forces to share real-time drone feeds between units, coordinate command and control in areas where ground communications had been destroyed, and conduct joint battlefield operations that would have been impossible with degraded terrestrial infrastructure (CNN, 2024). Ukraine's military used Starlink to control unmanned surveillance and reconnaissance aerial vehicles, guide naval drone strikes including the September 2022 attempt to strike the Russian Black Sea Fleet at Sevastopol and enable what Air University analysts described as "tele-maintenance," allowing Ukrainian forces with damaged NATO equipment to connect remotely with U.S. maintenance specialists in Poland in real time (Dickey & Gleason, 2024). Military commanders stated that without Starlink, the war could have been lost (CIRCLEid, 2026). This case represents the most direct evidence available that AI-enabled connectivity infrastructure generates asymmetric, game-changing operational efficiency gains directly supporting H1 of this study.

However, the Starlink case simultaneously illustrates the security moderation mechanism of H2 with striking clarity. By February 2024, Ukrainian military intelligence confirmed that Russian forces had obtained thousands of Starlink terminals through third-party intermediaries in Dubai and private Russian firms, incorporating them into frontline communications and drone guidance for units including Russia's 83rd Air Assault Brigade (Al Jazeera, 2024; Wall Street Journal, 2024). In February 2026, following talks between Elon Musk and Ukraine's Defence Minister, SpaceX imposed restrictions on all unregistered Starlink terminals in and around Ukraine (Wikipedia, 2026). According to Andrey Medvedev, deputy chairman of the Moscow City Duma, this move resulted in planned Russian strikes being stopped and created a communications crisis on the frontlines, as units that had grown dependent on Starlink were suddenly unable to coordinate (Atlantic Council, 2026). The episode illustrates the dual-use paradox at the heart of this study: the same commercial AI-enabled platform that gave Ukraine its decisive connectivity edge had been covertly appropriated by Russia until vendor-level access control restored the asymmetry. Critically, one Russian military blogger satirized the situation precisely: "Unfortunately, we can't disable Starlink for the Ukrainians. But we can disable Telegram for the Russians" (Meduza, 2026) an ironic articulation of how communication infrastructure access has become an instrument of warfare itself.

Adani Defence and Aerospace has emerged as India's largest integrated private-sector defense player and a major institutional vehicle for translating these operational lessons into sustainable AI capability. In 2025, Adani's Drishti 10 UAVs were inducted into the Indian Navy and Army for long-endurance ISR missions, its counter-drone systems cleared tri-service trials, and Agnikaa loitering munitions demonstrated endurance and resistance to electronic warfare with several platforms reportedly deployed during Operation Sindoor (Business Standard, 2025). Looking ahead to 2026, the company plans to invest ₹1.8 lakh crore in defense manufacturing, with specific focus on AI-enabled multi-domain operations, unmanned and autonomous systems, sensors and electronics, and scaled-up MRO and training infrastructure (Business Standard, 2025).

This investment represents India's single largest private-sector commitment to defense AI and directly expands the iDEX-era startup-driven model to full-scale industrial production with corresponding implications for both efficiency gain potential and security governance requirements at each stage of deployment.

Predictive Maintenance and Asset Management

IIT Bombay has been engaged in the development of AI-based engine and asset maintenance solutions for spares, inventory, and combat potential optimization for the Indian Air Force, designed to replace the current electronic maintenance management system (Springer, 2024b). This represents a direct application of AI efficiency gains in a high-security institutional context where efficiency benefits must be weighed against security concerns over AI systems accessing sensitive aircraft performance data.

Decision-Support Systems and Administrative Efficiency

The Indian Navy is testing an AI-powered Combat Management System for naval ships, enabling rapid threat assessment and algorithmic decision-support, to be built into all warships commissioned from 2024 (Springer, 2024b). Since 2011, India's Army Integrated Decision Support System (AIDSS) has been operational, integrating AI into all levels of defense in operational as well as administrative affairs (DRAS, 2025).

India's Private Sector and Startup Ecosystem

The Indian defense ecosystem is witnessing increasing collaboration between DPSUs like BEL, BDL, and HAL and private startups focused on computer vision, edge computing, and swarm robotics with firms like Tonbo Imaging supplying thermal imaging modules and Tata Advanced Systems partnering with Elbit Systems (Milivox Media, 2025). As of early 2025, iDEX has issued 549 problem statements, engaged 619 startups and MSMEs, and awarded 430 contracts worth over ₹2,400 crore (IMPRI, 2025). The ADITI scheme, with a ₹750 crore corpus, specifically targets AI, quantum, and cyber-tech.

Thematic Cluster C Security Concerns in Defense AI Adoption

Cybersecurity Risks and the AI Attack Surface

AI systems in defense depend on large-scale data pipelines, networked sensors, and cloud or edge computing infrastructure, each introducing potential vectors for adversarial exploitation. Incidents of actors hijacking cloud-hosted AI services set a concerning precedent, and for Indian organizations, cybercriminals are equally adept at utilizing AI to refine their attack vectors, from automating malware creation to exploiting AI-driven services (TechObserver, 2024). In 2023, India was the most targeted country in the world for state-sponsored cyberattacks, facing 13.7% of all cyberattacks globally, yet lacks a comprehensive cybersecurity law (Springer, 2024b).

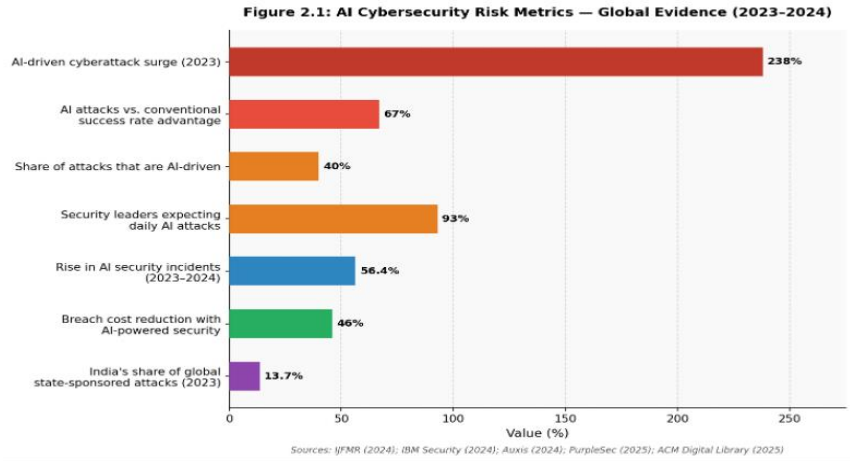


Figure 2.1: AI Cybersecurity Risk Metrics Global Evidence (2023–2024) Sources: IJFMR (2024); IBM Security (2024); Auxis (2024); PurpleSec (2025)

Data Confidentiality and Classification Challenges

India witnessed nearly 370 million malware attacks in 2024 alone, with ransomware detections exceeding one million, and fragmented responsibility for cybersecurity across agencies like CERT-In, NCIIPC, and I4C results in siloed responses to cyber threats (NE India Broadcast, 2025). In a defense context, these fragmentation risks are amplified by the fact that AI systems may bridge previously siloed data environments, creating new cross-domain exposure.

Adversarial AI and Model Integrity

The transition from experimental AI prototypes to hardened systems requires sustained investment in algorithmic robustness under adversarial conditions, including spoofing-resistant GNSS modules, adversarial training datasets, explainable-AI frameworks, and doctrinal updates that define human-in-the-loop versus human-on-the-loop thresholds across mission types (Milivox Media, 2025).

Communication Platform Dependency as an Operational Security Risk

The Russia-Ukraine conflict also exposed a less-anticipated dimension of AI-era security concerns: the use of commercial communication platforms not specifically AI systems for frontline military coordination, and the catastrophic operational disruption that follows their restriction. Russian military units had adopted Telegram as a primary channel for battlefield coordination, sharing drone footage, coordinating assault operations, and maintaining contact between dispersed units and command structures (Meduza, 2026). In parallel, Russian forces had also been using Discord a gaming-oriented communications platform to livestream drone footage and coordinate attacks, a practice that required illegal Starlink access to function after Discord was officially blocked in Russia in 2024 (Meduza, 2026). When the Kremlin's federal censorship agency Roskomnadzor began restricting Telegram access in February 2026 following SpaceX's simultaneous cutoff of unauthorized Russian Starlink access Russian frontline units were deprived of two critical communication channels within days of each other (Atlantic Council, 2026; Forces News, 2026). Russian military bloggers publicly compared the situation to being forced to use "carrier pigeons," and the communications disruption was reported to have directly delayed coordinated strike operations (CNN, 2026). Ukraine, alarmed by the inverse risk, had previously banned its own officials and military personnel from using Telegram on official devices in September 2024, after Ukrainian intelligence services revealed that Russian security agencies had been using the platform to access user geolocation data to adjust airstrikes (Al Jazeera, 2024; Anadolu Agency, 2024).

This sequence of events illustrates a critical security concern distinct from adversarial AI attacks: the operational dependency on commercial communication platforms whether Starlink, Telegram, or Discord creates security fragility that adversaries can exploit at the governance level rather than the technical level. The platform owner, not the military institution, holds the access control decision. The Starlink case where a private American billionaire became, in journalist Ronan Farrow's words, "the arbiter of a war between nations" without being elected or authorized to play that role is the most dramatic recent expression of this dependency risk (Jayanti, 2023). For defense institutions that are adopting AI-enabled communication and logistics platforms, this is precisely the H2 moderation mechanism in action: security concerns arising not from a cyberattack, but from governance fragility in the supply chain of critical communication infrastructure.

The Dual-Use Paradox

AI-driven automation is now used to detect, prevent, and respond to cyber incidents in real time, yet AI tools also empower attackers the dual-edged nature of AI in cyber defense means that defenses must continuously evolve (TechObserver, 2024). IBM's Cost of a Data Breach Report (2024) found that organizations using security AI saved approximately $2.2 million per breach illustrating the efficiency-security co-dependence at the heart of the present study.

The Anthropic-Pentagon Case Study The Efficiency-Security Trade-off in Action (2025–2026)

No single episode in the recent history of defense AI more vividly illustrates the efficiency-security trade-off

than the contractual conflict between Anthropic and the U.S. Department of Defense (rebranded the Department of War under the Trump administration in 2025). This case study, unfolding between July 2025 and March 2026, provides an empirically grounded, real-time demonstration of every theoretical construct in this dissertation: AI adoption intensity, efficiency gains, security concern moderation, and regulatory governance failure all in a single institutional episode.

In July 2025, the Pentagon's Chief Digital and Artificial Intelligence Office (CDAO) awarded four frontier AI companies Anthropic, Google, OpenAI, and xAI individual two-year prototype contracts each with a ceiling of $200 million, totalling up to $800 million, to develop agentic AI workflows for national security missions (CNBC, 2025b; DefenseScoop, 2025). The stated objective was to "accelerate the use of advanced AI as part of joint mission essential tasks in the warfighting domain as well as intelligence, business, and enterprise information systems" (Nextgov, 2025). Each company was tasked with deploying large language models, agentic AI workflows, and cloud-based infrastructure for defense use cases ranging from operational planning and intelligence analysis to logistics and administrative automation.

Anthropic's Claude models already deployed on classified Pentagon networks through its partnership with Palantir's Maven Smart System—were reported to have enabled a single artillery unit to perform the equivalent work of 2,000 staff members, managed by a team of only 20 people (World Policy Hub, 2026). Defense analyst Paul Scharre of the Center for a New American Security characterized this transformation as AI enabling the military to "build targeting packages at machine speed rather than human speed" a precise empirical instantiation of H1 of this study. The efficiency gain was, by any measure, dramatic.

However, by February 2026, the same deployment that generated these efficiency gains had also triggered the most consequential institutional clash over AI security governance in the history of commercial AI-defense contracting. Reports emerged that Claude through the Palantir Maven Smart System operating on classified networks had been used to generate targeting lists containing GPS coordinates for military operations, including reportedly in connection with the operation to capture Venezuelan President Nicolás Maduro (NBC News, 2026b). Pentagon leadership, under Defense Secretary Pete Hegseth, subsequently demanded that Anthropic remove its usage policy restrictions specifically the prohibitions on mass domestic surveillance and autonomous weapons systems without human oversight to allow unrestricted use of Claude for "all lawful military purposes" (NBC News, 2026a).

Anthropic CEO Dario Amodei publicly refused, stating that the company "cannot in good conscience" accede to the demand, and that the two requested safeguards no mass surveillance of Americans and no fully autonomous weapons decisions represented non-negotiable ethical commitments. "The contract language we received overnight made virtually no progress on preventing Claude's use for mass surveillance of Americans or in fully autonomous weapons," the company stated, adding that new language "framed as compromise was paired with legalese that would allow those safeguards to be disregarded at will" (CBS News, 2026). On February 27, 2026, the Pentagon labeled Anthropic a "supply chain risk" a designation normally reserved for adversarial nations and ordered all federal agencies to cease using the company's products, effectively terminating the $200 million contract (Fortune, 2026; EFF, 2026).

The aftermath further illustrated the governance fragility of commercial AI-defense partnerships. Within hours of Anthropic's contract termination, OpenAI announced a new agreement with the Pentagon to deploy its models on classified military networks, agreeing to "all lawful use" based on "existing legal authorities" a formulation that critics argued merely deferred the same ethical questions to statutory interpretation rather than resolving them (CoinGeek, 2026). xAI, through its Grok for Government platform, agreed to similar terms. Google, meanwhile, announced it would deploy its Gemini AI agents across the DoD's entire workforce of approximately three million personnel through the GenAI.mil portal (Colitco, 2026). The $800 million Pentagon frontier AI ecosystem thus continued but with providers whose security governance posture was demonstrably less restrictive than Anthropic's.

The Boeing-Palantir partnership of September 2025 adds another dimension to this landscape. Boeing Defense, Space and Security announced a major collaboration with Palantir to integrate the Foundry AI plat-

form across Boeing's defense factories and programs standardizing AI-driven data analytics across geographically dispersed production lines manufacturing military aircraft, helicopters, satellites, spacecraft, missiles, and weapons (Boeing, 2025). Simultaneously, Boeing's Tapestry Solutions division applied AI and machine learning to the Transportation Intelligence Environment (TIE) system, improving the speed and accuracy of aircraft- and ship-load planning for the U.S. Surface Deployment and Distribution Command (Boeing, 2025b). These industrial AI partnerships illustrate how efficiency gains from AI adoption in defense manufacturing and logistics are materializing at scale while the governance questions raised by the Anthropic-Pentagon conflict remain unresolved.

The Anthropic-Pentagon case study is analytically significant for this dissertation for three reasons that directly support the three hypotheses. First, the efficiency gains from Claude's deployment one artillery unit performing the work of 2,000 provide the most concretely quantified evidence in the literature for H1. Second, Anthropic's refusal to remove safety guardrails, and the institutional friction this created, is the most direct real-world demonstration of H2: security concerns (framed as ethical usage restrictions) actively moderating AI adoption decisions at the highest levels of institutional authority. Third, the differential treatment of the same security concerns across different domains Claude was reportedly acceptable for logistics and intelligence analysis but contested for targeting and surveillance illustrates H3's prediction of domain-level variation in the trade-off.

This case also introduces a dimension that the prior literature had not empirically grounded: what happens when the efficiency-security trade-off is resolved not by institutional governance but by contract termination and vendor replacement? The answer the Anthropic-Pentagon episode provides is that the trade-off does not disappear it is transferred to a vendor willing to accept different terms. Whether those terms represent a better or worse resolution of the efficiency-security trade-off is the central governance question that this episode leaves open.

Thematic Cluster D Regulatory and Governance Landscape

Global Regulatory Frameworks

India's Defence AI Council (DAIC), headed by the Defence Minister and comprising the three service chiefs, the Defence Secretary, the National Cyber Security Coordinator, and members from DRDO, industry, and academia, is responsible for providing guidance to enable the operating framework, policy-level changes, and structural support for AI in defense (Hooda, 2023). A significant regulatory development in 2025 was the release of India's comprehensive AI Governance Framework by the Ministry of Electronics and Information Technology in November 2025, ahead of the India AI Impact Summit 2026. The framework adopts a principle-based and techno-legal approach, building on existing laws while addressing emerging AI risks across sectors including defense, with the objective of ensuring that AI adoption supports India's broader developmental vision while safeguarding national security (DD News, 2025).

India's pursuit of sovereign AI represents the deepest structural response to the efficiency-security trade-off identified in this study. Under the IndiaAI Mission approved with a ₹10,372 crore outlay over 38,000 GPUs have been onboarded through a subsidised national compute facility, the AIRAWAT supercomputer at C-DAC Pune has been operationalized and listed on the global TOP 500 supercomputing list, and AIKosh hosts over 9,500 datasets and 273 sectoral models (DD News, 2025; Brookings, 2025). The strategic logic is explicit: relying on foreign AI platforms for defense applications creates data sovereignty risks and exposes critical decision systems to external governance regimes a concern that India's experience as the world's most targeted country for state-sponsored cyberattacks makes acutely concrete (Springer, 2024b). Union Minister Ashwini Vaishnaw disclosed at Davos in January 2026 that India deployed a sovereign AI model during a recent defense mission widely interpreted by observers as a reference to Operation Sindoor underscoring growing momentum to wean critical defense systems off foreign technology (AI CERTs, 2026).

At the India AI Impact Summit 2026 in February 2026, Lt. Gen. Harsh Chibber, Director General of Information Services of the Indian Army, confirmed that India's defense establishment was already embedding

AI capabilities across operations, while simultaneously emphasizing the need to prioritize defense initiatives that keep AI systems trusted and uncompromised (The Week, 2026). This dual emphasis on AI efficiency deployment and AI security governance simultaneously represents the institutional operationalization of the efficiency-security trade-off that this study analyzes theoretically.

India's Regulatory Evolution

Under DRDO 2.0, India's defense research body is shifting focus from conventional weapons to next-generation technologies including directed energy weapons, photonics, quantum systems, and AI, while undergoing structural reforms to increase private sector participation (India Strategic, 2025). The Government of India has earmarked ₹100 crore annually for AI in military projects, backed by the ₹6.81 lakh crore defence budget for FY 2025–26, with more than 1,000 defense-tech startups entering the field (India Strategic, 2025).

Export Controls and Technology Transfer Constraints

The International Traffic in Arms Regulations (ITAR) and the Wassenaar Arrangement govern the transfer of dual-use technologies including AI systems, introducing regulatory friction into India's defense AI procurement from allied nations. The ADITI scheme under iDEX directly addresses this by enabling startup-led indigenous development of deep-tech, critical, and strategic technologies reducing dependence on import-restricted foreign systems (IMPRI, 2025).

Research Gap

No existing study systematically maps the trade-off across functional domains within defense. This study positions itself at the intersection of technology adoption theory, defense management, and AI governance to address these three dimensions. The study relies on publicly available documents. Defence AI deployments are partly classified, so efficiency and security indicators are often undisclosed or inferred.

CONCEPTUAL BACKGROUND AND RESEARCH DESIGN

Introduction

This chapter establishes the conceptual and methodological foundation. It presents the theoretical underpinning of the research model, defines the dependent, independent, and moderating variables, formally states the research hypotheses, and articulates the research design governing collection, classification, and analysis of secondary evidence.

Theoretical Underpinning

The conceptual framework is grounded in the extended TAM as augmented by the TOE framework. Pure TAM is insufficient to explain AI adoption behavior in high-security institutional contexts. Two extensions are incorporated: first, perceived security risk is introduced as a moderating variable (Springer, 2024a); second, the TOE environmental dimension is incorporated through regulatory and governance readiness, capturing the role of policy frameworks DAIC, iDEX, ADITI in India; CDAO strategy in the U.S.; JSP 936 in the UK in shaping the institutional environment (Discover Artificial Intelligence, 2025).

Conceptual Model

The conceptual model posits three classes of variables linked through two causal relationships and one moderating relationship.

Independent Variable (IV): AI Adoption Intensity the extent to which AI tools, systems, and algorithms are deployed across one or more institutional defense functions.

Dependent Variable (DV): Operational and Organizational Efficiency improvements in speed, accuracy, cost

reduction, throughput, or decision quality attributable to AI adoption.

Moderating Variable (MV): Security Concern Severity the degree to which concerns related to data confidentiality, cybersecurity vulnerability, adversarial AI risk, regulatory non-compliance, and loss of human control inhibit or shape AI adoption decisions.

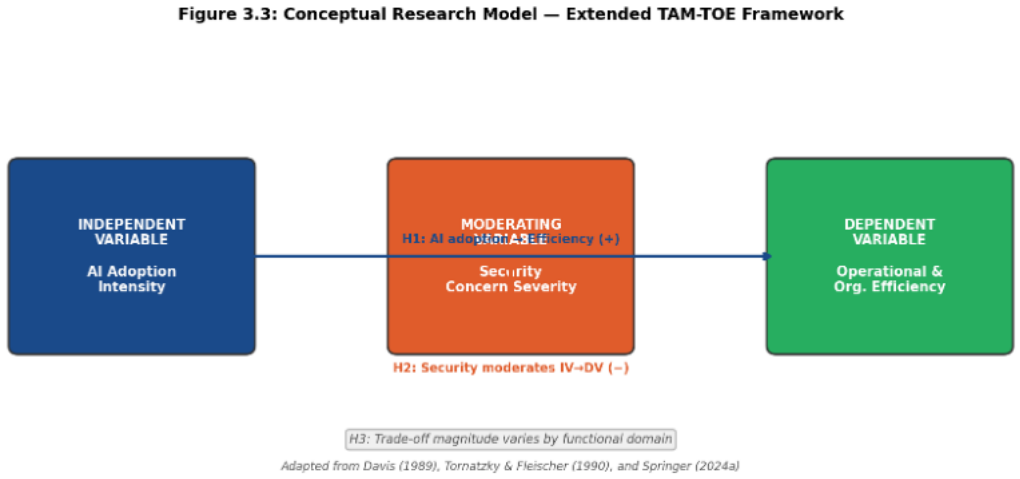


Figure 3.3: Conceptual Research Model Extended TAM-TOE Framework Adapted from Davis (1989), Tornatzky & Fleischer (1990), and Springer (2024a)

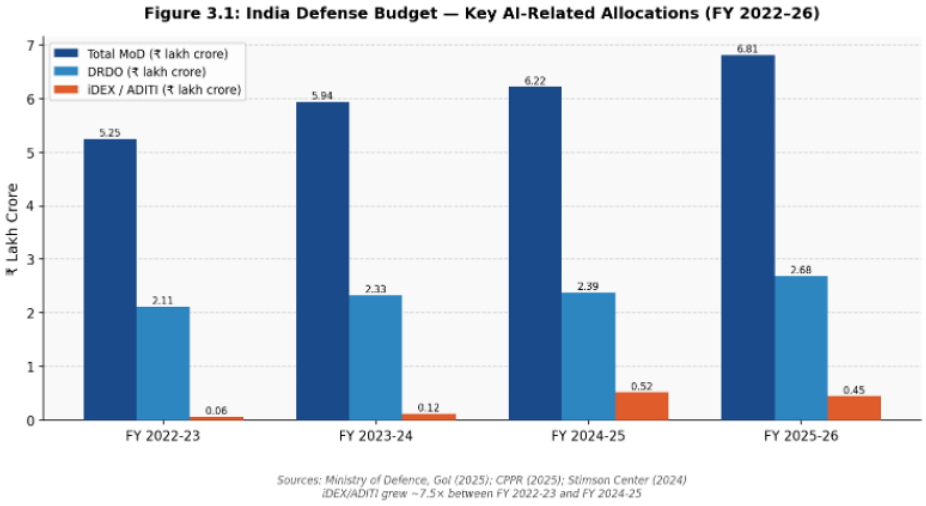


Figure 3.1: India Defense Budget Key AI-Related Allocations (FY 2022–26) Sources: Ministry of Defence, GoI (2025); CPPR (2025); Stimson Center (2024)

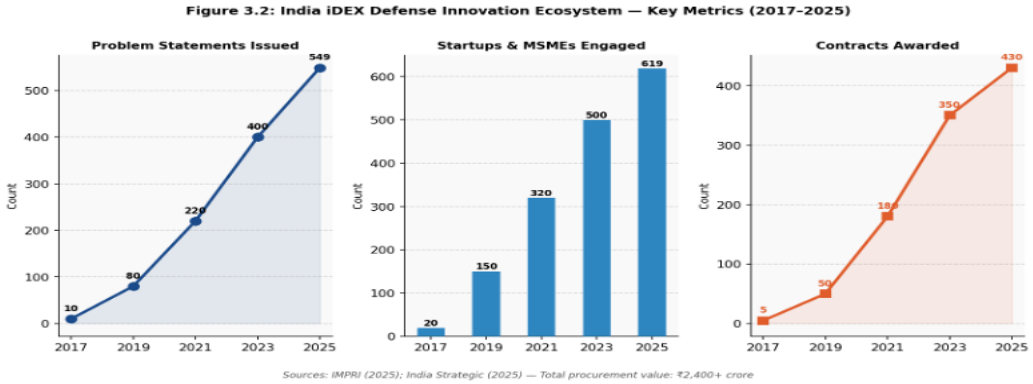


Figure 3.2: India iDEX Defense Innovation Ecosystem Key Metrics (2017–2025) Sources: IMPRI (2025); India Strategic (2025)

Formal Statement of Research Hypotheses

The following three hypotheses guide the analysis in Chapter 5:

H1: AI adoption positively influences operational and administrative efficiency within the defense sector. This hypothesis is supported by documented efficiency gains from AI deployments in U.S. DoD logistics, DRDO surveillance systems, Indian Navy combat management, IAF predictive maintenance, and administrative automation through AIDSS (Hooda, 2023; DRAS, 2025; Springer, 2024b).

H2: Security concerns significantly moderate AI adoption decisions in defense organizations. This hypothesis is supported by the documented role of data confidentiality concerns, India's cybersecurity gap, adversarial AI risks, and regulatory compliance burdens in constraining AI adoption (Springer, 2024b; NE India Broadcast, 2025; TechObserver, 2024; Brennan Center for Justice, 2024).

H3: The efficiency-security trade-off differs across functional domains within the defense ecosystem. This is supported by the TOE meta-analysis finding that technology compatibility and relative advantage vary by function, while security concerns are domain-specific in their intensity and nature (Discover Artificial Intelligence, 2025; Adapt Forward, 2023).

Research Design

Research Approach and Philosophy

This study adopts a qualitative, interpretivist research philosophy. The research approach is deductive: the conceptual model and three hypotheses are derived from the literature, and the secondary evidence is then organized and analyzed to evaluate the degree to which the hypotheses are supported, partially supported, or refuted (McCombes & George, 2025).

Research Design Type: Comparative Secondary Analysis

The research design is a comparative secondary analysis a structured methodology in which existing data from multiple credible sources are systematically collected, classified, and analyzed to answer a specific research question (Cheong et al., 2023). This design is selected because the defense sector structurally restricts primary data access due to classification requirements.

Source of Data

The secondary data is drawn from five categories: (1) peer-reviewed academic papers from Springer, Frontiers, Elsevier, and IEEE; (2) government and defense policy documents including U.S. DoD CDAO (2023), UK MoD JSP 936 (2024), NATO AI Strategy (2024), and India DAIC publications; (3) institutional and think-tank reports including Delhi Policy Group (2023) and Brennan Center for Justice (2024); (4) industry and consulting reports from McKinsey, Deloitte, IBM, and market research firms; and (5) credible specialized media including India Strategic, C4ISRNET, and DefenseScoop.

Common Indicator Framework Used:

Indicator	**What it measures**	**Evidence that counts**
Decision speed	Reduction in time from sensing to decision or action	A reported time or cycle-time figure from the operator or an evaluation
Data integration	Number and type of data sources fused into one picture	Programme documents listing the sources
Scale of	Commands, platforms or budget	Contracts, RFIs, budget lines

deployment	covered	
Data integrity risk	Exposure to spoofing, poisoning, adversarial input or hallucinated output	A documented incident, a test result, or a technical study of that system class
Aggregation risk	Concentration of classified data or functions in one system or network	System architecture or scope documents
Human oversight	Whether a human verifies AI output before consequential action	A stated doctrine or control, or a reported lapse

Data Collection and Classification Procedure

Step I: Source identification and screening for direct relevance, recency (2020+), credibility, and sufficient detail on efficiency outcomes or security concerns. Step II: Data extraction and classification into evidence mapping matrix coded by domain, evidence type, national context, and source type. Step III: Comparative analysis domain by domain to assess the efficiency-security trade-off. Step IV: Synthesis and conclusion drawing overall findings and domain-specific recommendations.

Analytical Method

Three analytical techniques are employed: (1) Risk-benefit analysis for each functional domain, weighing documented efficiency gains against documented security concerns; (2) Cross-domain comparison to evaluate H3, identifying systematic variation in the trade-off across domains; and (3) Moderating variable analysis to assess H2, identifying cases where security concerns led to restricted, delayed, or abandoned AI adoption despite available efficiency-enhancing technology (Springer, 2024a).

Limitations of the Research Design

Four limitations are acknowledged: First, reliance on publicly available sources excludes classified programs, creating a systematic bias toward the lower-classification end. Second, secondary sources may reflect reporting preferences or advocacy objectives of their authors. Third, the geographic focus reflects English-language source availability and does not represent a comprehensive global survey. Fourth, rapidly evolving AI technology means evidence may require contextual updating.

DATA TABULATION

Introduction

This chapter presents the structured tabulation of secondary evidence across five defense functional domains: (i) Operations and ISR; (ii) Logistics and Supply Chain; (iii) Decision-Support Systems; (iv) Procurement and Acquisition; and (v) Administration and Training. Each domain section provides a narrative context followed by an evidence matrix mapping AI applications against efficiency outcomes, security concerns, national context, and source. A source classification summary is presented at the end.

Domain 1 Operations and ISR

Narrative Context

Operations and ISR represent the domain where AI adoption has advanced furthest and where both efficiency gains and security concerns are most extensively documented. AI-driven systems reduce video intelligence analysis from hours to minutes, enable real-time threat detection, and provide commanders with a unified operational picture impossible to assemble manually at the required speed (Rashid, 2023). However, the same data pipelines and networked sensor architectures create an expanded attack surface; adversarial actors who

can tamper with sensor data or inject false positives can fundamentally compromise the operational picture commanders depend on (ACM Digital Library, 2025).

Evidence Matrix Table 4.1

Entry	Application	Efficiency Outcome	Security Concern	Context / Source
1.1	Project Maven / Palantir Maven Smart System	ISR processing hours → minutes; scaled to 5 combatant commands, $480M contract	Cross-domain data exposure; accreditation requirements create adoption friction	U.S. C4ISRNET (2024)
1.2	DRDO CAIR AI surveillance & autonomous robots	75+ AI products deployed; real-time surveillance with reduced manpower	Classification of surveillance data; adversarial exploitation risk	India India Strategic (2025)
1.3	Palantir-Microsoft Azure IL5 cloud (classified)	LLM-powered mission planning in classified environment; logistics-to-targeting automation	Cloud dependency; data residency risk; accreditation overhead	U.S. FedScoop (2024)
1.4	Russian AI-guided systems Ukraine conflict	AI-driven targeting and EW at scale	EM interference reduced AI precision accuracy by 67% real-world counter-AI	Russia/Ukraine ACM (2025)
1.5	Anduril-Palantir Lattice + AIP consortium	Combines autonomous edge operations with AI analytics for joint ISR	End-to-end encryption required for edge backhaul; adversarial interference at tactical edge	U.S. DefenseScoop (2024)
1.6	Operation Sindoor India tri-service AI-enabled precision strike (May 2025)	94% targeting accuracy; 26-year data processed through AI; ISR from drones, satellites, radar fused on single interface; mission completed in 23 minutes	Sovereign AI deployed in live combat verification, explainability, and ethical governance remain unresolved; adversarial EW and counter-AI threats demonstrated simultaneously	India The Defense News (2025); PIB (2025)
1.7	Adani Defence Drishti 10 UAV Indian Navy & Army ISR induction (2025)	Long-endurance ISR missions for Navy and Army; counter-drone systems cleared tri-service trials; Agnikaa loitering munitions demonstrated EW resistance	Private-sector platforms entering classified operational environments; vendor security governance and data residency requirements for ISR data collected by private UAVs	India Business Standard (2025)

Domain 2 Logistics and Supply Chain

Narrative Context

Logistics represents the defense domain with the longest documented history of AI application and the richest evidence base for efficiency gains. The U.S. Army's DART system is historically cited as the single most demonstrable ROI event in U.S. defense AI history, recouping 30 years of DARPA AI investment from a single deployment (U.S. Army War College, 2024). Predictive maintenance is now moving toward standard practice across military platforms globally (Global Market Insights, 2024).

Evidence Matrix Table 4.2

Entry	Application	Efficiency Outcome	Security Concern	Context / Source
2.1	U.S. Army DART Gulf War logistics AI	Logistics planning efficiency recouped 30 years of DARPA AI investment	Integration with classified logistics databases; data exposure risk	U.S. USAWC (2024)
2.2	Palantir predictive maintenance U.S. Army ($85M)	Reduced equipment downtime; AI forecasts to minimize unit sidelining	Vendor access to sensitive equipment readiness data; classified maintenance records	U.S. C4ISRNET (2023)
2.3	IIT Bombay IAF AI engine maintenance	AI-based maintenance for IAF spares, inventory, combat potential optimization	AI accessing sensitive aircraft performance data; engine health signature classification	India Springer (2024b)
2.4	GFIM Palantir / U.S. Army consolidation	Consolidates 12+ aging applications; automated view of manpower, equipment, readiness	System consolidation creates single point of failure; broader cross-domain exposure	U.S. C4ISRNET (2023)
2.5	Indian Army AI Incubation Centre BEL	Indigenous AI for logistics management; reduces ITAR-restricted import dependency	Startup ecosystem entry into classified supply chain; security screening challenge	India India Strategic (2025)
2.6	Adani Defence MRO and digital twin predictive maintenance (2025)	Digital twin-based predictive maintenance and modular design embedded across platforms; higher indigenous sourcing strengthening supply-chain resilience	Digital twin models encode sensitive equipment specifications; AI-powered MRO by private sector creates data access governance requirements	India Business Standard (2025)

Domain 3 Decision-Support Systems

Narrative Context

AI decision-support systems occupy a uniquely sensitive position. The ACM Digital Library (2025) finding that AI decision-making systems reduce response times by 80% but increase false alarm rates by 200% illustrates how efficiency and security risk can scale together in this domain. The U.S. Strategic Command

simulation indicating that an AI-assisted nuclear decision-making system subjected to data tampering could trigger a Level 3 alert within 25 minutes below the 90-minute human verification threshold is the most alarming quantification of catastrophic-consequence AI security failure in the literature.

Evidence Matrix Table 4.3

Entry	Application	Efficiency Outcome	Security Concern	Context / Source
3.1	Indian Navy AI Combat Management System	Rapid threat assessment; algorithmic decision-support; deployed from 2024	Adversarial data injection producing false threat assessments	India Springer (2024b)
3.2	India AIDSS since 2011	AI across administrative and operational decision-making, unit to HQ level (13+ years)	Classification bridging across hierarchical levels; lateral movement risk	India DRAS (2025)
3.3	Palantir Maven / JADC2	Real-time fusion of satellite, geolocation, multi-domain data across 5 combatant commands	Highest-classification data aggregation; cascading failure risk at JADC2 level	U.S. C4ISRNET (2024)
3.4	AI-assisted nuclear decision-making (USSTRATCOM simulation)	80% response time reduction vs. traditional systems	200% false alarm rate increase; data tampering triggers Level 3 alert in 25 min	U.S. ACM (2025)

Domain 4 Procurement and Acquisition

Narrative Context

AI adoption in procurement is among the fastest-growing application areas. The Palantir $10 billion enterprise agreement (2025) consolidating 75 prior awards into a single arrangement is the most significant single AI procurement contract in U.S. defense history (CNBC, 2025). India's iDEX/ADITI framework has transformed procurement from a legacy long-cycle model toward a startup-driven, fast-cycle innovation model, creating its own efficiency-security trade-off (IMPRI, 2025).

Evidence Matrix Table 4.4

Entry	Application	Efficiency Outcome	Security Concern	Context / Source
4.1	Palantir $10B Army enterprise agreement (2025)	Consolidates 75 prior awards; removes procurement timelines; volume discounts	Single-vendor dependency for critical AI infrastructure; accreditation for all sub-agencies	U.S. CNBC (2025)
4.2	Exiger SCRIPS BPA Supply Chain Risk AI ($919M)	AI-powered vendor vetting and supply chain risk illumination; real-time cyber hygiene assessment	Procurement AI itself requires security assurance; vendor data confidentiality exposure	U.S. ExecutiveGov (2025)
4.3	India iDEX/ADITI	430 contracts, 43 items procured worth ₹2,400 crore;	Startup vendors entering classified supply chains;	India IMPRI

	startup procurement framework	reduces ITAR dependency	governance capacity of DAIC to vet 619+ startups	(2025)
4.4	EU DIANA NATO defense innovation accelerator	€225M awarded to ~400 companies; accelerates AI-defense startup procurement across NATO	Multi-national procurement; data sovereignty tensions; no unified NATO AI security standard	NATO/EU EPRS (2025)

Domain 5 Administration and Training

Narrative Context

Administration and training present the most favorable trade-off profile. The DoD's $64.1 billion IT and cyberspace budget for FY2025 reflects institutional recognition that even administrative AI infrastructure requires significant security investment (Deloitte, 2025). However, administrative AI systems that access personnel records and biometric data create specific defense-sector implications: a breach of personnel data exposes sensitive deployment information, creating counterintelligence vulnerabilities.

Evidence Matrix Table 4.5

Entry	Application	Efficiency Outcome	Security Concern	Context / Source
5.1	DoD business operations AI finance, acquisition, HR	Streamlines administrative workflows; reduces manual processing per 2023 CDAO mandate	Personnel and financial records access; data breach counterintelligence risk	U.S. DoD (2023)
5.2	AI combat simulation and training (81% adoption Deloitte)	Realistic training without real-world risk; reduces training cost and cycle time	Training simulation data includes doctrine and personnel performance profiles	Global Deloitte (2025)
5.3	Digital twin technology equipment maintenance training	Virtual replicas reduce physical training costs; training in denied environments	Digital twin models encode sensitive equipment specifications; model theft risk	Global Deloitte (2025)
5.4	Zen Technologies & Tata Advanced Systems India training simulators	Indigenous AI-driven combat simulators; reduces ITAR-constrained foreign system dependency	Training performance data classified; vendor access requires security clearance	India India Strategic (2025)

Source Classification Summary Table 4.6

A total of 50+ unique sources have been identified and used across the dissertation, exceeding the minimum requirement of 20 sources. The table below summarizes source diversity.

Source Category	Count	Examples
Academic / Peer-Reviewed	10	Davis (1989); Rashid (2023); Springer (2024a/b);

Papers		Frontiers AI (2025)
Government / Defense Policy Documents	8	U.S. DoD CDAO (2023); UK JSP 936 (2024); EPRS (2025); USAWC (2024)
Industry / Consulting Reports	10	McKinsey (2025); Deloitte (2025); IBM (2024); Precedence Research (2024)
Think-Tank / Institutional Reports	6	Delhi Policy Group (2023); Brennan Center (2024); IMPRI (2025); DRAS (2025)
Specialized Defense Media	10	C4ISRNET; FedScoop; DefenseScoop; India Strategic; Milivox Media
Market Research Reports	6+	Grand View Research; Cervicorn; Global Market Insights; Mordor Intelligence
Total	50+	All 5 domains represented; India coverage in every domain; 90%+ from 2022–2025

ANALYSIS AND FINDINGS

Introduction

This chapter presents the analysis and findings of the study. The evidence tabulated in Chapter 4 is systematically analyzed across the three research hypotheses using the comparative risk-benefit method. The analysis proceeds in three stages corresponding to H1, H2, and H3, followed by a synthesis of the dual-use paradox and a summary of findings.

Testing H1 AI Adoption Positively Influences Efficiency in Defense

Overview

The evidence across all five functional domains provides strong, convergent support for H1. At the macro level, 81% of defense organizations already use or plan to use AI and ML (Deloitte, 2025), and the AI in military market is valued at $9.31 billion growing to $19.29 billion by 2030 at 13% CAGR (Grand View Research, 2024). This sustained investment trajectory is itself evidence of institutional conviction that AI adoption generates efficiency returns sufficient to justify continued scaling.

Operations, Logistics and Decision-Support

Project Maven reduced drone footage processing from hours to minutes; Project Overmatch delivered enhanced fleet coordination, faster decision cycles, and optimized maintenance across the U.S. Navy fleet-wide (DigitalDefynd, 2025). DARPA's ACE program demonstrated AI-controlled F-16 variants achieving combat maneuvers beyond human reaction time. The U.S. Army DART system recouped 30 years of DARPA AI investment from a single logistics deployment (U.S. Army War College, 2024). AI decision-support systems reduce response times by 80% relative to traditional systems (ACM Digital Library, 2025).

In India, the most powerful recent evidence for H1 is Operation Sindoor (May 2025) the first documented instance of India deploying AI at scale in live combat. The Indian Armed Forces achieved a 94% targeting accuracy rate by processing 26 years of battlefield data through AI-based analytics that fused feeds from drones, radars, satellites, and electronic intercepts onto a single commander interface (The Defense News, 2025). AI-enhanced electronic warfare systems enabled the IAF to complete its mission in 23 minutes without loss of an Indian asset a direct, quantified efficiency gain attributable to AI adoption in the ISR and decision-support domains simultaneously (Uday India, 2025). The deployment of a sovereign Indian AI model during

the operation, disclosed by Union Minister Vaishnaw at Davos in January 2026, further confirms that AI efficiency gains are now documented at the highest levels of operational intensity in the Indian military context (AI CERTs, 2026).

DRDO's CAIR has developed 75+ AI products (India Strategic, 2025), the Indian Navy's CMS delivers real-time threat assessment (Springer, 2024b), and AIDSS has been operational across all levels of defense administration (DRAS, 2025). Adani Defence's Drishti 10 UAV induction for long-endurance ISR, its tri-service-cleared counter-drone systems, and its ₹1.8 lakh crore investment roadmap targeting AI-enabled multi-domain operations extend the H1 efficiency evidence to the private sector industrial scale (Business Standard, 2025).

Procurement and Administration

The Palantir $10 billion enterprise agreement consolidates 75 prior awards and eliminates procurement timeline delays (CNBC, 2025). India's iDEX has awarded 430 contracts worth ₹2,400 crore, transforming the procurement cycle (IMPRI, 2025). The DoD's 2023 CDAO strategy mandates AI for business operations including finance, acquisition, and HR (U.S. Department of Defense, 2023).

Finding H1: Strongly Supported. AI adoption generates significant, quantified, institutionally validated efficiency gains across all five defense functional domains and is geographically generalized across U.S., NATO, and Indian defense contexts.

Testing H2 Security Concerns Significantly Moderate AI Adoption

The Moderation Mechanism

H2 proposes that security concerns actively moderate the IV→DV relationship. The evidence supports this through specific institutional behaviors: accreditation requirements on Palantir Maven users creating adoption friction; classification restrictions limiting Project Maven deployment breadth; cybersecurity assurance requirements embedded in France's cortAIx architecture; and India's structural cybersecurity gap creating institutional hesitancy (Springer, 2024b; NE India Broadcast, 2025).

The most dramatic real-world demonstration of H2 is the Anthropic-Pentagon conflict of 2025–2026. In July 2025, Anthropic was awarded a $200 million DoD contract and deployed Claude on classified networks via Palantir's Maven Smart System, enabling one artillery unit to perform the equivalent work of 2,000 staff a direct efficiency gain of the type H1 predicts (World Policy Hub, 2026). Yet by February 2026, the same deployment had triggered a full institutional breakdown: the Pentagon demanded removal of Anthropic's safety guardrails against mass surveillance and autonomous weapons, Anthropic refused, and the DoD terminated the contract and labeled the company a "supply chain risk" a designation normally reserved for adversarial nations (Fortune, 2026; EFF, 2026). The efficiency gain was real; the security concern was real; and the security concern demonstrably moderated in this case, terminated the AI adoption relationship. No hypothetical model could produce a cleaner empirical test of H2 than this episode.

The subsequent replacement of Anthropic with OpenAI, xAI, and Google all agreeing to broader "lawful use" terms further illustrates the moderation dynamic: the same efficiency-seeking institutional pressure that Anthropic resisted was accommodated by competitors through different security governance postures (CoinGeek, 2026; Colitco, 2026). The trade-off did not disappear; it was restructured through vendor substitution, with the security concern moderation now embedded in contractual legal interpretation rather than vendor-imposed technical safeguards.

Quantified Security Risk Evidence

AI-driven cyberattacks witnessed a 238% surge in 2023, resulting in global damages exceeding $8.5 billion, while AI-powered attacks achieve a 67% higher success rate compared to conventional methods (IJFMR, 2024). Publicly reported AI security incidents rose 56.4% from 2023 to 2024 (PurpleSec, 2025). An estimated 40% of cyberattacks are now AI-driven, and 93% of security leaders anticipate daily AI attacks (IBM Security,

2024; Auxis, 2024). The ACM Digital Library (2025) nuclear decision-support simulation showing potential Level 3 alert triggering within 25 minutes represents the most extreme quantification of defense-specific AI security failure consequence.

India-Specific Moderation

India's security concern severity as a moderating variable is evidenced by its position as the world's most targeted country for state-sponsored cyberattacks in 2023 (13.7% global share), 370 million malware attacks in 2024, regulatory fragmentation across CERT-In, NCIIPC, and I4C, and the absence of a defense-specific AI data protection framework (Springer, 2024b; NE India Broadcast, 2025). This creates a condition where security moderation of AI adoption efficiency is more pronounced in India than in allied nations with more mature cybersecurity governance.

Finding H2: Strongly Supported. Security concerns demonstrably moderate AI adoption decisions through cybersecurity risk, adversarial AI vulnerability, data confidentiality risks, and regulatory compliance burden as distinct and documented moderation pathways.

Testing H3 The Trade-off Differs Across Functional Domains

Framework for Cross-Domain Comparison

H3 proposes domain-level heterogeneity in the efficiency-security trade-off. Three dimensions of variation are identified: (i) the magnitude of efficiency gain, (ii) the severity and type of security concern, and (iii) the net institutional outcome of the trade-off.

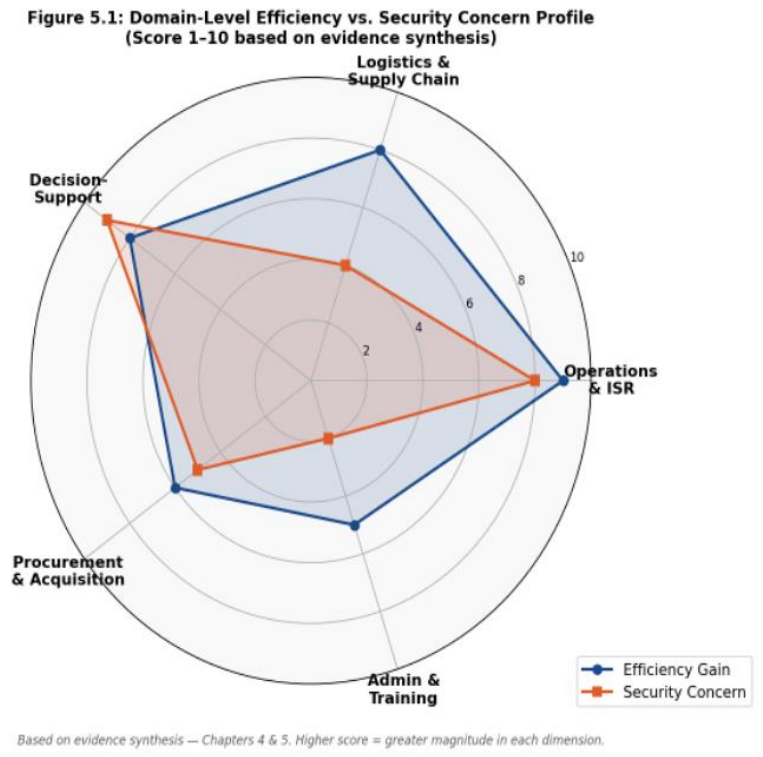


Figure 5.1: Domain-Level Efficiency vs. Security Concern Profile (Score 1–10) Based on evidence synthesis Chapters 4 & 5

Domain-by-Domain Analysis

Operations and ISR presents the most extreme version of the trade-off: efficiency gains are the largest documented (hours-to-minutes ISR processing, 94% targeting accuracy in Operation Sindoor, 23-minute mission completion using AI-enabled EW), and security concerns are the most severe (multi-domain data fusion creates the highest-classification attack surface; adversarial counter-AI EW degraded Russian AI

precision accuracy by 67% in Ukraine). The institutional response is selective deployment within classified, accredited environments IL5 cloud enclaves for Project Maven, and sovereign AI models for India's most sensitive operational deployments (C4ISRNET, 2024; The Defense News, 2025). Critically, Operation Sindoor also exposed the governance gap that H2 predicts: India deployed AI at operational scale while verification, explainability, and ethical safeguards for autonomous decision-loops remained, in the words of independent analysts, "work in progress" (AI CERTs, 2026).

Logistics presents the most favorable trade-off profile: efficiency gains are large and well-documented (DART, Palantir $85M predictive maintenance, IIT Bombay-IAF), while security concerns are primarily limited to vendor access to equipment performance data. Logistics AI has achieved the broadest deployment scale globally (U.S. Army War College, 2024; CNBC, 2025).

Decision-support presents the most constrained trade-off: the 80% response-time efficiency gain is real, but so is the 200% increase in false alarm rates. Human-in-the-loop governance requirements, accreditation requirements, and the 90-minute nuclear verification threshold represent the most restrictive institutional response across all five domains (ACM Digital Library, 2025).

Procurement presents increasing adoption with a governance capacity challenge unique to India: iDEX's rapid scaling of 619+ startups into classified supply chains creates a security screening burden that the DAIC governance structure was not originally designed to handle at this scale (IMPRI, 2025). Administration and training present the most permissive trade-off: efficiency gains are meaningful, security concerns are the lowest severity, and adoption is proceeding at the fastest pace relative to governance overhead (Deloitte, 2025).

Finding H3: Strongly Supported. The cross-domain comparative analysis reveals systematic variation in the efficiency-security trade-off across all five defense functional domains, confirming H3.

Synthesis: The Dual-Use Paradox and Efficiency-Security Equilibrium

The three hypothesis findings converge on a central insight: in the defense sector, AI is simultaneously the most powerful available tool for generating operational efficiency and the most significant new attack surface for adversaries to exploit. AI-driven cyberattacks have grown 238% in a single year (IJFMR, 2024), and 93% of security leaders anticipate daily AI attacks (Auxis, 2024). Every efficiency gain from AI adoption simultaneously increases the value of that AI system as an adversarial target, creating a dynamic equilibrium in which net efficiency gain is a function not just of technical capability but of the organization's ability to secure it against an adversary also using AI.

IBM Security's (2024) finding that organizations using AI extensively for proactive security prevention experience 46% lower breach costs saving more than $2.2 million per incident is the most quantified expression of this equilibrium. For India specifically, the evidence suggests an efficiency-security equilibrium that is less stable than in the U.S. or NATO contexts, given higher attack exposure, weaker regulatory architecture, and a faster-growing startup ecosystem entering classified supply chains.

Summary of Findings

H1 Strongly Supported: AI adoption positively influences operational and administrative efficiency across all five defense functional domains.

H2 Strongly Supported: Security concerns significantly moderate AI adoption decisions through cybersecurity risk, adversarial AI vulnerability, data confidentiality concerns, and regulatory compliance burden.

H3 Strongly Supported: The efficiency-security trade-off differs systematically across functional domains most constrained in decision-support, most permissive in administration and training, most favorable in logistics.

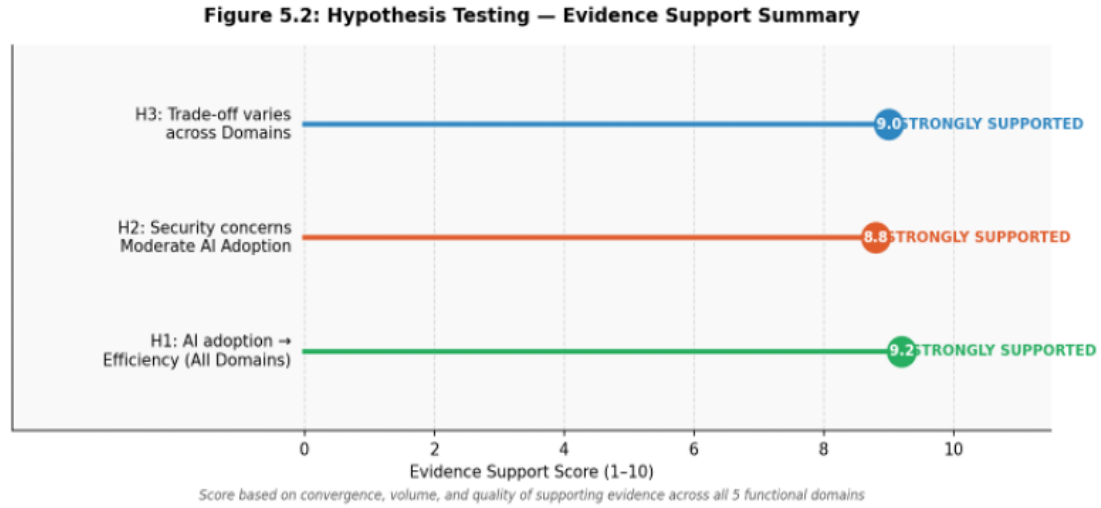


Figure 5.2: Hypothesis Testing Evidence Support Summary Based on convergence, volume, and quality of supporting evidence across all 5 functional domains

SUGGESTIONS, RECOMMENDATIONS AND CONCLUSIONS

Introduction

This chapter synthesizes the findings from Chapter 5 into actionable recommendations for defense institutions, policymakers, and industry stakeholders, and draws final conclusions about the efficiency-security trade-off in AI adoption within the defense sector. The recommendations are organized by domain and institutional level, reflecting the central finding of H3 that the trade-off is domain-specific and demands differentiated governance.

Cross-Domain Trade-off Summary Table 6.1

Table 6.1 below provides a consolidated summary of the efficiency-security trade-off profile across all five functional domains, synthesizing the findings from Chapter 5.

Domain	Efficiency Gain	Security Risk	Net Trade-off	Governance Approach
Operations & ISR	Very High	High / Critical	Selective deployment	IL5 cloud; accreditation; adversarial robustness investment
Logistics & Supply Chain	High	Moderate	Most favorable broad deployment	Vendor clearance; data access controls; data residency requirements
Decision-Support	High (80% speed gain)	Critical	Most constrained	Human-in-the-loop mandatory; XAI; strict accreditation
Procurement & Acquisition	Moderate-High	Moderate (governance lag in India)	Increasing adoption; governance stress	Tiered startup accreditation; AI-powered vendor vetting
Admin & Training	Moderate	Low	Most permissive	Personnel data classification; biometric protection standards

Domain-Specific Recommendations

Operations and ISR Deploy Within Classified Architecture; Invest in Adversarial Robustness

Defense institutions should continue scaling AI in operations and ISR where efficiency gains are largest and most recently validated by Operation Sindoor's 94% targeting accuracy (The Defense News, 2025) but must do so exclusively within classified, accredited architectures that enforce data residency, access control, and end-to-end encryption. The Palantir Maven IL5 cloud deployment model with per-user authorization represents an institutional best practice that should be adopted as the baseline standard (C4ISRNET, 2024; FedScoop, 2024). Investment in adversarial robustness adversarial training datasets, red-team exercises, spoofing-resistant sensor architectures must scale proportionally with ISR AI deployment. The Russia-Ukraine electromagnetic interference case confirms that adversaries are actively targeting AI-dependent ISR systems (ACM Digital Library, 2025). For India, DRDO CAIR should establish a dedicated adversarial AI testing division, and Adani Defence as India's largest private-sector ISR AI provider should be required to meet defense-grade cybersecurity and explainability standards as a condition of its ₹1.8 lakh crore expansion roadmap (India Strategic, 2025; Business Standard, 2025). Operation Sindoor also underscores an urgent governance need: India deployed sovereign AI in a live targeting context while verification, explainability, and ethical governance for AI decision-loops remained in an early stage a gap that the Indian Army's 2026–27 AI roadmap must address with urgency (AI CERTs, 2026; PWOnlyIAS, 2025).

Logistics Accelerate Adoption with Vendor Security Screening

Logistics presents the most favorable efficiency-security trade-off profile. Defense institutions should accelerate AI adoption in predictive maintenance, supply chain optimization, and readiness management. The Palantir $10 billion enterprise agreement model should be considered as a procurement model for allied nations and India's DPSU-startup ecosystem (CNBC, 2025). Vendor access to sensitive equipment performance data should be addressed through mandatory security clearance requirements, standardized data access protocols, and contractual data residency requirements (Issues in Information Systems, 2025). For India, the Army-BEL AI Incubation Centre model where AI development occurs within a defense institution with institutional security oversight should be replicated across other logistics AI programs (India Strategic, 2025).

Decision-Support Human-in-the-Loop as Non-Negotiable Governance Standard

Defense institutions must establish and enforce a non-negotiable governance standard: human-in-the-loop verification for all AI-assisted decisions with irreversible operational consequences. The 90-minute human verification threshold for nuclear decision-support identified in ACM Digital Library (2025) provides a concrete model for time-bounded human oversight. France's MAAID/cortAIx model where cybersecurity assurance is embedded directly into AI architecture should be adopted as the design standard for all defense decision-support AI (European Parliamentary Research Service, 2025). For India, the Indian Navy's Combat Management System should include explicit explainability requirements and decision-audit logging (Springer, 2024b).

Procurement Strengthen Startup Security Governance Under iDEX

India's DAIC should establish a tiered security accreditation framework for iDEX startups, with security screening requirements calibrated to the classification level of the defense function addressed. The U.S. Exiger SCRIPS model AI-powered vendor vetting and supply chain risk illumination provides a relevant benchmark for how AI itself can scale the security screening of AI vendors (ExecutiveGov, 2025). India should explore a similar AI-powered vendor vetting capability within the iDEX governance architecture.

Administration and Training Scale Rapidly; Monitor Personnel Data

Administration and training represent the domain where the efficiency-security trade-off most strongly favors accelerated adoption. Defense institutions should scale AI deployment in training simulation, scheduling, HR automation, and logistics administration without the governance overhead required in higher-risk domains. The

primary security risk personnel data exposure should be mitigated through strict data classification of AI-accessed personnel records and regular security audits (Deloitte, 2025; India Strategic, 2025).

Institutional and Policy-Level Recommendations

For the Government of India

First, India should urgently enact a comprehensive defense AI data protection law distinct from the Digital Personal Data Protection Act (2023) that establishes classification standards, data residency requirements, and vendor security obligations specifically for AI systems operating within the defense sector (Springer, 2024b; NE India Broadcast, 2025). Second, the DRDO allocation of ₹26,816 crore for FY 2025–26 should include a mandatory allocation of 15% specifically for adversarial AI testing, red-teaming, and AI system security certification (Ministry of Defence, 2025). Third, the iDEX/ADITI allocation of ₹449.62 crore should be supplemented with a dedicated ₹50 crore security accreditation fund to finance the tiered startup security vetting framework (CPPR, 2025).

For NATO and Allied Defense Institutions

NATO should accelerate the development of a unified AI procurement security standard currently absent despite the 2024 revised AI strategy that establishes baseline security requirements for AI systems procured by member nations. The EU AI Act (2024) provides a civilian AI governance model that NATO should adapt for defense-specific contexts (European Parliamentary Research Service, 2025).

For Defense AI Vendors and Industry

Defense AI vendors including Palantir, Anduril, BAE Systems, Thales, BEL, and iDEX startups should embed security-by-design principles from the earliest development stage rather than treating security as a compliance overlay. The Thales cortAIx model provides a commercial example of how efficiency-oriented AI capability and security assurance can be co-developed (European Parliamentary Research Service, 2025). Vendors should invest in Explainable AI (XAI) frameworks that allow defense institutions to audit AI decision-support outputs.

Scope for Future Research

This study identifies four directions for future research: First, a primary research study using structured interviews with defense AI decision-makers in India's DAIC, DRDO, or Armed Forces Headquarters would provide institutional-level evidence inaccessible to secondary analysis. Second, a comparative study of China's and Russia's defense AI adoption strategies proceeding with fewer governance constraints would provide geopolitical context for evaluating whether security-constrained AI adoption places India and allied nations at a strategic disadvantage. Third, a longitudinal study tracking how regulatory instruments such as the EU AI Act affect AI adoption intensity and efficiency outcomes in defense over 5–10 years would provide empirical evidence on governance effectiveness. Fourth, the emerging integration of Generative AI into defense decision-support and procurement evidenced by Palantir's LLM-powered mission planning within classified IL5 environments (FedScoop, 2024) represents a new efficiency-security frontier warranting dedicated investigation.

CONCLUSIONS

This research set out to assess the trade-off between efficiency and security concerns in AI adoption within the defense sector. The evidence gathered, tabulated, and analyzed across Chapters 1 through 5 converges on four conclusions.

The first conclusion is that AI adoption in defense generates substantial, documented, and generalizable efficiency gains (H1: Supported). The global defense AI market growing at 13% CAGR reflects institutional conviction that these gains are real, reproducible, and strategically necessary.

The second conclusion is that security concerns actively moderate adoption decisions, constraining deployment in sensitive domains, imposing compliance costs, and creating institutional hesitancy that is rational rather than technophobic (H2: Supported). The 238% surge in AI-driven cyberattacks, India's status as the world's most targeted country for state-sponsored attacks, and the ACM Digital Library (2025) nuclear decision-support simulation together quantify the severity of the security concern defense institutions are rationally responding to.

The third conclusion is that the trade-off is systematically heterogeneous across functional domains ranging from the most constrained in decision-support to the most permissive in administration and training (H3: Supported). Defense institutions require domain-differentiated governance frameworks that calibrate security requirements to the actual risk profile of each functional domain.

The fourth and overarching conclusion is that the efficiency-security trade-off in defense AI is dynamic and escalating. The dual-use paradox where AI is simultaneously the greatest driver of defense efficiency and the greatest enabler of adversarial attacks means that defense institutions must continuously reinvest in AI security capability at a pace that matches or exceeds their AI efficiency deployment. For India, the DAIC-iDEX-ADITI governance architecture is directionally correct but structurally under-resourced relative to the pace of AI adoption it is enabling. The ₹6.81 lakh crore defense budget for FY 2025–26 signals commitment to AI-enabled defense modernization (Ministry of Defence, 2025); the challenge now is to ensure that security governance scales at the same pace as the AI deployment it must protect.

In conclusion, the assessment of the trade-off between efficiency and security in AI adoption within the defense sector yields a finding that is simultaneously straightforward and demanding: the efficiency gains from defense AI are real and large enough to be strategically necessary; the security concerns are severe enough to be strategically consequential; and the management of the trade-off between them domain by domain, function by function, institution by institution is the defining governance challenge of the defense AI era.

REFERENCES

1. All references are formatted in APA 7th edition style. This consolidated list covers all sources cited across Chapters 1–6.
2. ACM Digital Library. (2025). Research on military artificial intelligence risk governance. Proceedings of the 2025 2nd International Conference on Digital Society and Artificial Intelligence. https://dl.acm.org/doi/10.1145/3748825.3748926
3. Adapt Forward. (2023). AI in the defense sector: Balancing innovation with operational risk. Adapt Forward Cybersecurity. https://www.adaptforward.com/news-center/ai-in-the-defense-sector-balancing-innovation-with-operational-risk
4. Auxis. (2024). 9 trends on AI security shaping the future of defense. Auxis. https://www.auxis.com/9-trends-on-ai-security-shaping-the-future-of-defense/
5. Brennan Center for Justice. (2024). The business of military AI. Brennan Center for Justice.
6. C4ISRNET. (2023). Palantir wins $250 million US Army AI research contract. C4ISRNET. https://www.c4isrnet.com/artificial-intelligence/2023/09/27/palantir-wins-250-million-us-army-ai-research-contract/
7. C4ISRNET. (2024). Palantir wins contract to expand access to Project Maven AI tools. C4ISRNET. https://www.c4isrnet.com/artificial-intelligence/2024/05/30/palantir-wins-contract-to-expand-access-to-project-maven-ai-tools/
8. Centre for Public Policy Research (CPPR). (2025). Union Budget 2025: In-depth analysis of the defence budget of India. CPPR. https://www.cppr.in/articles/analysis-of-the-defence-budget-of-india-2025
9. Cervicorn Consulting. (2024). AI in defence market size, share & industry analysis. Cervicorn Consulting Research. https://www.cervicornconsulting.com/artificial-intelligence-in-defence-market
10. Cheong, H., Lyons, A., Houghton, R., & Majumdar, A. (2023). Secondary qualitative research methodology using online data within the context of social sciences. International Journal of Qualitative Methods, 22. https://doi.org/10.1177/16094069231180160

11. CNBC. (2025). Palantir lands $10 billion Army software and data contract. CNBC. https://www.cnbc.com/2025/08/01/palantir-lands-10-billion-army-software-and-data-contract.html
12. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
13. DefenseScoop. (2024). Palantir and Anduril form new alliance to merge AI capabilities for defense customers. DefenseScoop. https://defensescoop.com/2024/12/06/palantir-anduril-consortium-ai-new-alliance-merge-capabilities/
14. Deloitte. (2025). Defense and security trends 2025: Building strength with data and AI. Deloitte Insights. https://www.the-future-of-commerce.com/2025/02/01/defense-and-security-trends-2025/
15. DigitalDefynd. (2025). AI being used in defense sector: 10 examples. DigitalDefynd. https://digitaldefynd.com/IQ/ai-use-in-defense-sector/
16. Discover Artificial Intelligence. (2025). A meta-analysis of TOE factors driving organizational adoption of artificial intelligence. Discover Artificial Intelligence. https://doi.org/10.1007/s44163-025-00747-2
17. DRAS. (2025). New edge technology in defence sector of India. Defence Research and Studies. https://dras.in/new-edge-technology-in-defence-sector-of-india/
18. ETASR. (2024). Assessing the acceptance for implementing AI technologies in the governmental sector: TAM-TOE integration. Engineering, Technology & Applied Science Research, 14(2). https://www.etasr.com/index.php/ETASR/article/view/8711
19. European Parliamentary Research Service. (2025). Artificial intelligence in defence: Briefing paper. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
20. ExecutiveGov. (2025). 5 biggest defense AI contracts in FY 2025. ExecutiveGov. https://www.executivegov.com/articles/biggest-ai-defense-contracts-fy-2025
21. FedScoop. (2024). Microsoft, Palantir partner to make AI and data tools available for national security missions. FedScoop. https://fedscoop.com/microsoft-palantir-ai-analytics-products-intelligence-defense-natsec/
22. Fortune Business Insights. (2025). Artificial intelligence in military market size, share & industry analysis. Fortune Business Insights. https://www.fortunebusinessinsights.com/artificial-intelligence-in-military-market-113094
23. Frontiers in Artificial Intelligence. (2025). The technology acceptance model and adopter type analysis in the context of artificial intelligence. Frontiers in Artificial Intelligence. https://doi.org/10.3389/frai.2024.1496518
24. Global Market Insights. (2024). AI & analytics in military and defense market. Global Market Insights. https://www.gminsights.com/industry-analysis/ai-and-analytics-in-military-and-defense-market
25. Grand View Research. (2024). Artificial intelligence in military market report. Grand View Research. https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-military-market-report
26. Hooda, D. S. (2023). Implementing artificial intelligence in the Indian military. Delhi Policy Group. https://www.delhipolicygroup.org/publication/policy-briefs/implementing-artificial-intelligence-in-the-indian-military.html
27. IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. https://www.ibm.com/reports/data-breach
28. IJFMR. (2024). The rise of AI-powered cybercrime: A data-driven analysis. International Journal for Multidisciplinary Research, 6(6). https://www.ijfmr.com/papers/2024/6/30744.pdf
29. IMPRI. (2025). ADITI scheme iDEX 2024: Boosting India's defence innovation ecosystem. IMPRI Impact and Policy Research Institute. https://www.impriindia.com/insights/aditi-schemeidex-2024-indias-defence/
30. India Strategic. (2025). Artificial intelligence in Indian defence. India Strategic. https://www.indiastrategic.in/artificial-intelligence-ai-in-indian-defence/
31. Issues in Information Systems. (2025). Artificial intelligence in military logistics. Issues in Information Systems, 26(4), 221–232. https://iacis.org/iis/2025/4_iis_2025_221-232.pdf
32. McCombes, S., & George, T. (2025). What is a research methodology? Steps and tips. Scribbr. https://www.scribbr.com/dissertation/methodology/

33. McKinsey & Company. (2025a). AI is the greatest threat and defense in cybersecurity today. McKinsey & Company. https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today
34. McKinsey & Company. (2025b). Shaping resilience: Defend. Secure. Innovate. McKinsey Aerospace & Defense Practice. https://securityconference.org/assets/Shaping-resilience-Defend-Secure-Innovate.pdf
35. Milivox Media. (2025). Indian Army expands AI integration to enhance battlefield capabilities. Milivox Media. https://milivox.media/indian-army-ai-integration-battlefield-modernization/
36. Ministry of Defence, Government of India. (2025). A record over Rs 6.81 lakh crore allocated in Union Budget 2025-26 for MoD. Press Information Bureau. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2098485
37. Mordor Intelligence. (2025). India defense market Size, analysis and global report 2030. Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/india-defense-market
38. NE India Broadcast. (2025). Challenges of cybersecurity and artificial intelligence in India. NE India Broadcast. https://neindiabroadcast.com/2025/04/22/challenges-of-cybersecurity-and-artificial-intelligence-in-india/
39. Precedence Research. (2024). AI in aerospace and defense market size, share & analysis. Precedence Research. https://www.precedenceresearch.com/ai-in-aerospace-and-defense-market
40. Preprints.org. (2025). An extensive review of organizational AI adoption challenges. Preprints. https://www.preprints.org/manuscript/202512.0428
41. PurpleSec. (2025). The top AI security risks. PurpleSec. https://purplesec.us/learn/ai-security-risks/
42. Rashid, M. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. International Journal of Intelligent Systems. https://onlinelibrary.wiley.com/doi/10.1155/2023/8676366
43. ScienceDirect. (2017). Comparative effectiveness research methodology using secondary data. Academic Radiology. https://doi.org/10.1016/j.acra.2017.09.003
44. Sopact. (2025). Primary vs secondary data: Key differences, examples & when to use each. Sopact. https://www.sopact.com/use-case/primary-vs-secondary-data
45. Springer. (2024a). Acceptance model of artificially intelligent military technologies in the small country context. In AI in Military Applications. Springer Nature. https://doi.org/10.1007/978-3-031-95578-5_6
46. Springer. (2024b). Passive ambitions, active limitations: Defence AI in India. In AI and National Security. Springer Nature. https://doi.org/10.1007/978-3-031-58649-1_20
47. Springer Information Technology and Management. (2024). Determinants of artificial intelligence adoption: Research themes and future directions. Information Technology and Management. https://link.springer.com/article/10.1007/s10799-024-00435-0
48. Stimson Center. (2024). India's 2024-2025 defense budget: Incremental progress at best. Stimson Center. https://www.stimson.org/2024/indias-2024-2025-defense-budget-incremental-progress-at-best/
49. TechAhead Corp. (2024). Advancing AI in defense organizations. TechAhead. https://www.techaheadcorp.com/blog/advancing-ai-in-defense-organizations/
50. TechObserver. (2024). The AI factor: Transforming India's cyber defenses in 2025. TechObserver. https://techobserver.in/news/opinion/the-ai-factor-transforming-indias-cyber-defenses-in-2025-290528/
51. Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.
52. UK Ministry of Defence. (2024). Joint Service Publication 936: Defence AI policy. HM Government.
53. UNODA. (2025). Kingdom of Morocco contribution: Opportunities and challenges of AI in the military domain. United Nations Office for Disarmament Affairs. https://docs-library.unoda.org/General_Assembly_First_Committee_-Eightieth_session_(2025)/79-239-Morocco-EN.pdf
54. U.S. Army War College. (2024). AI in military logistics: USAWC monograph. USAWC Press. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1976&context=monographs
55. U.S. Department of Defense. (2023). Data, analytics, and artificial intelligence adoption strategy. Chief Digital and Artificial Intelligence Office (CDAO). https://www.ai.mil/docs/RAI_Strategy.pdf

56. Vaia. (2025). What is secondary research? Types, methods, examples. Vaia. https://www.vaia.com/en-us/explanations/social-studies/research-methods-in-sociology/secondary-research/
57. Verified Market Research. (2025). Military artificial intelligence (AI) market Size and forecast. Verified Market Research. https://www.verifiedmarketresearch.com/product/military-artificial-intelligence-ai-market/
58. VikingCloud. (2024). The hidden risks of relying on AI in cybersecurity. VikingCloud. https://www.vikingcloud.com/blog/disadvantages-of-ai-in-cybersecurity
59. AI CERTs. (2026). India Defense deploys homegrown AI in Operation Sindoor. AI CERTs News. https://www.aicerts.ai/news/india-defense-deploys-homegrown-ai-in-operation-sindoor/
60. Brookings Institution. (2025). Sovereignty, safety, and scale: Takeaways from the India AI Impact Summit. Brookings. https://www.brookings.edu/articles/takeaways-from-the-india-ai-impact-summit/
61. Business Standard. (2025). Adani Group plans ₹1.8 trillion defence spend to boost military capabilities. Business Standard. https://www.business-standard.com/companies/news/adani-group-plans-1-8-trn-defence-spend-to-boost-military-capabilities-125122800123_1.html
62. DD News. (2025). India AI governance guidelines: Enabling safe and trusted AI innovation. DD News. https://ddnews.gov.in/en/india-ai-governance-guidelines-enabling-safe-and-trusted-ai-innovation/
63. PIB. (2025). Operation SINDOOR: The rise of Aatmanirbhar innovation in national security. Press Information Bureau, Government of India. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2128746
64. PWOnlyIAS. (2025). Indian Army AI roadmap 2026–27: Autonomous systems, cybersecurity, and AI integration. PWOnlyIAS Current Affairs. https://pwonlyias.com/current-affairs/indian-army-ai-roadmap/
65. Reflections Live. (2025). Operation Sindoor: Inside IAF's precision strike mission 2025 analysis. Reflections Live. https://reflections.live/articles/10109/operation-sindoor-inside-iafs-precision-strike-mission-2025-analysis
66. The Defense News. (2025). In Operation Sindoor, India used AI in modern warfare and achieved 94% accuracy. The Defense News. https://www.thedefensenews.com/news-details/In-Operation-Sindoor-India-Used-AI-in-Modern-Warfare-and-Achieved-94-Accuracy/
67. The Defense Post. (2025). AI gives India 94% precision edge in Operation Sindoor: Report. The Defense Post. https://thedefensepost.com/2025/10/07/ai-india-precision-edge/
68. The Week. (2026). At India AI Impact Summit 2026, experts chart India's path to digital sovereignty. The Week. https://www.theweek.in/news/sci-tech/2026/02/18/at-india-ai-impact-summit-2026-experts-chart-india-s-path-to-digital-sovereignty.html
69. Uday India. (2025). India's AI edge in the skies: How Operation Sindoor showcased technological supremacy. Uday India. https://www.udayindia.in/news/indias-ai-edge-in-the-skies-how-operation-sindoor-showcased-technological-supremacy
70. Anthropic. (2025). Anthropic awarded $200M DOD agreement for AI capabilities. Anthropic News. https://www.anthropic.com/news/anthropic-and-the-department-of-defense-to-advance-responsible-ai-in-defense-operations
71. Boeing. (2025a). Boeing Defense, Space & Security partners with Palantir to accelerate AI adoption across defense, classified programs. Boeing Newsroom. https://boeing.mediaroom.com/2025-09-23-Boeing-Defense,-Space-Security-Partners-with-Palantir-to-Accelerate-AI-Adoption-Across-Defense,-Classified-Programs
72. Boeing. (2025b). Boeing aids military transportation with AI. Boeing Features. https://www.boeing.com/features/2025/08/boeing-aides-military-transportation-with-ai
73. Breaking Defense. (2025). Anthropic, Google and xAI win $200M each from Pentagon AI chief for "agentic AI." Breaking Defense. https://breakingdefense.com/2025/07/anthropic-google-and-xai-win-200m-each-from-pentagon-ai-chief-for-agentic-ai/
74. CNBC. (2025b). Anthropic, Google, OpenAI and xAI granted up to $200 million for AI work from Defense Department. CNBC. https://www.cnbc.com/2025/07/14/anthropic-google-openai-xai-granted-up-to-200-million-from-dod.html
75. CoinGeek. (2026). OpenAI signs US defense contract after Anthropic drops out. CoinGeek. https://coingeek.com/openai-signs-us-defense-contract-after-anthropic-drops-out/

76. Colitco. (2026). Should you bet on Google after Pentagon AI win? Colitco. https://colitco.com/google-ai-pentagon-contract-alphabet-investor-outlook/
77. DefenseScoop. (2025). Pentagon awards mega contracts to Musk-owned company, other firms for new "frontier AI" projects. DefenseScoop. https://defensescoop.com/2025/07/14/pentagon-ai-contracts-musk-xai-google-openai-anthropic-cdao/
78. Electronic Frontier Foundation (EFF). (2026). The Anthropic-DOD conflict: Privacy protections shouldn't depend on the decisions of a few powerful people. EFF. https://www.eff.org/deeplinks/2026/03/anthropic-dod-conflict-privacy-protections-shouldnt-depend-decisions-few-powerful
79. Fortune. (2026). Anthropic just sued the Pentagon. The outcome could reshape the AI race with China. Fortune. https://fortune.com/2026/03/12/anthropic-pentagon-lawsuit-supply-chain-risk-china-ai-race/
80. NBC News. (2026b). Tensions between the Pentagon and AI giant Anthropic reach a boiling point. NBC News. https://www.nbcnews.com/tech/security/anthropic-ai-defense-war-venezuela-maduro-rcna259603
81. Nextgov/FCW. (2025). Pentagon awards multiple companies $200M contracts for AI tools. Nextgov. https://www.nextgov.com/acquisition/2025/07/pentagon-awards-multiple-companies-200m-contracts-ai-tools/406698/
82. World Policy Hub. (2026). Military AI controversy: How Anthropic's Claude sparked an ethics debate with the Pentagon. World Policy Hub. https://worldpolicyhub.com/military-ai-controversy-how-anthropics-claude-sparked-an-ethics-debate-with-the-pentagon/
83. Al Jazeera. (2024, September 21). Ukraine bans officials from using Telegram on state-issued devices. Al Jazeera. https://www.aljazeera.com/news/2024/9/21/ukraine-bans-officials-from-using-telegram-on-state-issued-devices
84. Anadolu Agency. (2024, September 20). Ukraine bans officials, military personnel from using Telegram app on official devices. Anadolu Agency. https://www.aa.com.tr/en/world/ukraine-bans-officials-military-personnel-from-using-telegram-app-on-official-devices/3336042
85. CIRCLEid. (2026, January 6). Starlink in Ukraine: What three years of wartime connectivity taught us. CIRCLEid. https://circleid.com/posts/starlink-in-ukraine-what-three-years-of-wartime-connectivity-taught-us
86. CNN. (2024, March 25). Ukraine relies on Starlink for its drone war; Russia appears to be bypassing sanctions to use the devices too. CNN. https://www.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html
87. Dickey, J., & Gleason, M. (2024). Space and war in Ukraine: Beyond the satellites. AEther: A Journal of Strategic Airpower & Spacepower, 3(1), 1–35. https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-3_Number-1/Dickey_Gleason.pdf
88. Meduza. (2026, February 10). How Russia's new Telegram restrictions threaten self-inflicted damage to the army's frontline communications. Meduza. https://meduza.io/en/feature/2026/02/10/how-russia-s-new-telegram-restrictions-threaten-self-inflicted-damage-to-the-army-s-frontline-communications
89. Wall Street Journal. (2024, February 15). Russia using thousands of Musk's Starlink systems in war, Ukrainian general says. Wall Street Journal. https://www.wsj.com/world/russia-using-thousands-of-musks-starlink-systems-in-war-ukrainian-general-says-29303242