INTERNATIONAL RELATIONS RESEARCHES
Homepage: https://iisajournals.ir/
Iranian International Studies Association

Applications of artificial intelligence in the evolution of military and security strategies

Mansour Mansouri, Department of political Science, Lam.C., Islamic Azad University, lamerd, Iran. 609999271@iau.ir
AliMohamad Haghighi, Corresponding Author, Department of political Science, Lam.C., Islamic Azad University, lamerd, Iran.. am.haghighi@iau.ac.ir
Amin Ravanbod, Department of political Science, Lam.C., Islamic Azad University, lamerd, Iran.aravan@iau.ir

Article Info
Article Type:
Reserch Article

Date received:
2025/11/09

Date approved:
2026/ 03/17

ABSTRACT

This research was conducted with a qualitative approach and using semi-structured in-depth interviews with experts in the fields of artificial intelligence, security, and strategic studies. The data from the interviews were analyzed through open, axial, and selective coding, and finally, 32 primary applications of artificial intelligence in the military and security fields were identified. In the next step, these applications were integrated into the form of 12 main capabilities, and finally, through a conceptual abstraction process, four final applications were extracted at the macro-strategic level. This integrated approach has enabled the passage from the level of individual applications to the level of strategic capabilities and macro-security consequences. The research findings show that AI plays a pivotal role in shaping information and cognitive superiority, intelligent security decision-making and governance, operational sustainability and defense readiness, and digital security and cyber resilience. The results also indicate that the strategic value of AI lies not in its insular uses, but in the synergyits information, cognitive, cyber, and institutional capabilities. From a theoretical perspective, this research contributes to the development of the security and AI literature by providing a multi-level conceptual framework, and from a practical perspective, it can be used as an analytical roadmap for policymakers and security institutions in the evolution of defense strategies.

Cite this Article: Mansouri,M , Haghighi,A and Ravanbod,A . (2026). Applications of artificial intelligence in the evolution of military and security strategies. International Relations Researches, 15(4), 199-230. doi: 10.22034/irr.2026.593238.2887

Publisher: Iranian Association of International Studies
DOI: 10.22034/irr.2026.593238.2887

Introduction

The rapid development and diffusion of Artificial Intelligence (AI) are fundamentally transforming the strategic and defense environment. Unlike earlier technological innovations that primarily enhanced specific military capabilities, AI increasingly affects the broader architecture of security, including intelligence, decision-making, deterrence, crisis management, military readiness, cyber operations, and cognitive competition. This transformation challenges conventional assumptions about how strategic advantage is generated and exercised. Traditional defense strategies have largely relied on material capabilities, human expertise, hierarchical decision-making, and reactive responses to emerging threats. AI, by contrast, enables the continuous processing of large volumes of data, real-time analysis, predictive assessment, adaptive decision-making, and integration across different levels of security governance. Despite the expanding literature on AI and national security, much of the existing research remains focused on technical applications, individual operational capabilities, or specific military technologies. Consequently, the strategic implications of AI and its potential to transform defense doctrines and security governance have received comparatively less systematic and integrated attention.

This study addresses this gap by identifying, coding, integrating, and conceptually organizing the major applications of AI in the transformation of defense and strategic strategies. Rather than treating AI as a collection of isolated technological tools, the study conceptualizes it as a transformative enabler capable of restructuring the logic of security, strategic decision-making, military preparedness, and defense governance. The central argument is that the strategic value of AI does not primarily derive from individual applications but from the synergies created among informational, cognitive, operational, cyber, and institutional capabilities.

Theoretical Framework

The study adopts a capability-oriented and multi-level theoretical approach to explain how AI contributes to strategic transformation. The analytical framework distinguishes three interconnected levels: individual AI applications, integrated strategic capabilities, and overarching strategic functions. This conceptual progression makes it possible to move beyond an application-centered understanding of AI toward a capability-centered and ultimately strategy-centered interpretation.

At the first level, AI applications represent specific functions through which artificial intelligence can be employed in military and security affairs. At the second level, related applications are integrated into broader capabilities, such as intelligence superiority, strategic decision-making, operational resilience, cyber security, cognitive operations, and national resilience. At the third level, these capabilities are synthesized into broader strategic functions that can reshape defense doctrines and security governance.

From this perspective, AI is understood not merely as an instrument for increasing operational efficiency but as a potential driver of a transition from reactive to anticipatory security. Predictive analytics, simulation, real-time information processing, and adaptive learning can enable security institutions to identify emerging threats, assess alternative scenarios, and allocate resources before threats fully materialize. At the same time, AI expands the strategic importance of the cognitive domain, where the ability to interpret information, manage narratives, identify disinformation, and understand patterns of public perception becomes increasingly relevant to national security.

Methodology

This research employs a qualitative methodology based on semi-structured in-depth interviews with experts in Artificial Intelligence, strategic studies, and defense and security studies. The purpose of the interviews was to identify the principal applications and strategic functions of AI across different dimensions of military and security affairs. The collected data were analyzed through a systematic process of open, axial, and selective coding. Open coding was initially used to identify distinct applications and concepts emerging from the expert data. Through axial coding, conceptually related applications were subsequently grouped into broader categories representing integrated capabilities. Finally, selective coding was employed to identify the overarching strategic functions that best explain the relationship among these capabilities and the transformation of defense strategies. This iterative process resulted in the identification of 32 initial applications, their consolidation into 12 major capabilities, and their subsequent integration into four overarching strategic applications. The resulting framework therefore provides a three-stage analytical structure connecting specific technological applications to strategic capabilities and, ultimately, to broader transformations in defense and security strategy.

Results and Discussion

The findings demonstrate that AI has a broad and multidimensional impact on military and security affairs. The identification of 32 distinct applications indicates that AI operates simultaneously across tactical, operational, and strategic levels, thereby weakening traditional boundaries among these levels. These applications include intelligence analysis, threat prediction, crisis management, cognitive operations, intelligent logistics, adaptive training, cyber security, and other functions associated with defense preparedness and security governance. An important finding is that individual applications generally have limited strategic significance when considered independently. Their transformative potential emerges primarily when they are integrated into complementary networks of capabilities. The second stage of analysis consolidated the 32 initial applications into 12 major capabilities. This transition from an application-oriented to a capability-oriented perspective demonstrates how AI can structurally enhance intelligence, strategic decision-making, operational sustainability, cyber security, cognitive operations, and broader

forms of national resilience. The findings suggest that AI becomes a genuine strategic advantage when these capabilities are developed in alignment with overarching national-security objectives and embedded within institutional decision-making architectures.

At the final level, the 12 capabilities were integrated into four overarching strategic functions: (1) informational and cognitive superiority; (2) intelligent strategic decision-making and security governance; (3) operational sustainability and defense preparedness; and (4) digital security and cyber resilience. Together, these four dimensions indicate the emergence of a new model of security power characterized by interconnectedness, data dependence, anticipation, and adaptability.

The first major dimension, informational and cognitive superiority, demonstrates that AI is transforming the meaning of information superiority. Strategic advantage increasingly depends not simply on possessing information but on the capacity to process, interpret, prioritize, and transform vast quantities of data into actionable knowledge. AI can therefore contribute to the development of a cognitive battlespace in which public perceptions, narratives, disinformation, and information flows become increasingly important components of national security.

The second dimension concerns intelligent decision-making and security governance. AI can strengthen coordination among different levels of decision-making, from tactical and operational levels to national strategic institutions. By providing continuous analytical support and scenario assessment, AI can contribute to more adaptive and evidence-based decision-making. Nevertheless, this capability also creates institutional, legal, ethical, and governance challenges. The increasing integration of AI into security decision-making requires mechanisms capable of ensuring accountability, transparency, appropriate human oversight, and responsible data governance.

The third dimension, operational sustainability and defense preparedness, illustrates AI's potential to improve logistics, training, resource allocation, simulation, crisis management, and organizational readiness. These capabilities can increase the adaptability of defense institutions and allow them to respond more effectively to rapidly changing strategic environments.

The fourth dimension, digital security and cyber resilience, highlights AI's growing importance in protecting digital infrastructures and strengthening the ability of states and defense organizations to anticipate, detect, and respond to cyber threats. Cyber resilience consequently becomes an integral component of broader strategic resilience rather than a narrowly technical security function.

Collectively, these findings support the proposition that AI can contribute to a transition from reactive security toward anticipatory and adaptive security. The integration of predictive capabilities, simulation, and real-time analysis increases the possibility of identifying emerging threats before they fully materialize. This transformation has significant implications for deterrence, crisis management,

defense-resource allocation, and strategic planning. It also suggests that future military superiority may depend increasingly on the capacity to generate and utilize knowledge rapidly rather than exclusively on numerical or hardware superiority.

Conclusions and Suggestions

The study concludes that Artificial Intelligence should be conceptualized as a transformative strategic enabler rather than merely a technological instrument. Its significance lies in the interaction and cumulative effects of informational, cognitive, operational, cyber, and institutional capabilities. The proposed framework demonstrates how 32 specific applications can be systematically integrated into 12 major capabilities and, ultimately, four overarching strategic functions. This multi-level framework contributes to the literature by connecting technological applications with broader transformations in defense strategy and security governance. The findings also indicate that the strategic adoption of AI cannot be reduced to technological investment. Effective transformation requires simultaneous attention to data governance, institutional capacity, ethical standards, human capital, and appropriate mechanisms of human oversight. Defense organizations that acquire AI technologies without developing the institutional and human capacities necessary to integrate them into decision-making processes may fail to realize their strategic potential. Accordingly, policymakers should pursue an integrated approach that combines AI development with robust data-governance frameworks, interdisciplinary human-capital development, ethical and legal standards, cyber-resilience mechanisms, and institutional reforms. Defense organizations should also prioritize interoperability and integration among AI-enabled capabilities rather than developing isolated technological applications. Finally, future research should empirically examine the proposed framework across different national security systems and compare how institutional structures, strategic cultures, and levels of technological development shape the adoption and strategic consequences of AI. Such comparative research can further clarify the conditions under which AI generates sustainable strategic advantage and the circumstances in which its diffusion may instead create new forms of vulnerability and strategic instability.

Keywords: Artificial Intelligence, Defense Strategies, Smart Governance, War Technology.

.

پژوهش های روابط بین الملل
Homepage: https://iisajournals.ir/

کاربردهای هوش مصنوعی در تحول استراتژی های نظامی و امنیتی

منصور منصوری گروه علوم سیاسی، واحد لامرد، دانشگاه آزاد اسلامی، لامرد، ایران.609999271@iau.ir
علی‌محمد حقیقی نویسنده مسئول، گروه علوم‌سیاسی، واحد لامرد، دانشگاه آزاد اسلامی ، لامرد، ایران.am.haghighi@iau.ac.ir
امین روانبد گروه علوم‌سیاسی، واحد لامرد، دانشگاه آزاد اسلامی ، لامرد، ایران.aravan@iau.ir

درباره مقاله

نوع مقاله:
مقاله پژوهشی

کلیدواژه‌ها:
هوش مصنوعی،
استراتژی‌های دفاعی،
حکمرانی هوشمند،
فناوری جنگ

تاریخچه مقاله
تاریخ دریافت: ۱۴۰۴/۸/۱۸
تاریخ پذیرش: ۱۴۰۴/۱۲/۲۶

چکیده

تحولات شتابان هوش مصنوعی، استراتژی‌های دفاعی و راهبردی را به‌طور بنیادین دگرگون کرده و الگوهای سنتی تصمیم‌گیری، بازدارندگی و حکمرانی را با چالش‌های جدیدی مواجه ساخته است. با وجود گسترش پژوهش‌ها در این حوزه، بخش عمده مطالعات بر کاربردهای فنی و عملیاتی هوش مصنوعی متمرکز بوده و نقش آن در سطح راهبردی و دکترین‌های دفاعی کمتر به‌صورت نظام‌مند بررسی شده است. پژوهش حاضر با هدف شناسایی، کدگذاری و تلفیق کاربردهای هوش مصنوعی در تحول استراتژی‌های دفاعی و راهبردی انجام شده است. این تحقیق با رویکرد کیفی و از طریق مصاحبه‌های عمیق نیمه‌ساختاریافته با خبرگان حوزه‌های هوش مصنوعی، مطالعات راهبردی و دفاعی انجام شد. داده‌ها با استفاده از کدگذاری باز، محوری و انتخابی تحلیل گردید. یافته‌ها منجر به شناسایی ۳۲ کاربرد اولیه، تلفیق آن‌ها در قالب ۱۲ قابلیت اصلی و استخراج چهار کاربرد کلان راهبردی شد. نتایج نشان می‌دهد هوش مصنوعی نقش اساسی در ایجاد برتری اطلاعاتی و شناختی، تصمیم‌گیری و حکمرانی هوشمند، پایداری عملیاتی و آمادگی دفاعی، و امنیت دیجیتال و تاب‌آوری سایبری ایفا می‌کند. همچنین، ارزش راهبردی هوش مصنوعی بیش از آنکه ناشی از کاربردهای منفرد باشد، حاصل هم‌افزایی میان قابلیت‌های اطلاعاتی، شناختی، سایبری و نهادی آن است. این پژوهش با ارائه چارچوبی مفهومی و چندسطحی، به توسعه ادبیات هوش مصنوعی و مطالعات راهبردی کمک کرده و می‌تواند به‌عنوان مبنایی برای سیاست‌گذاری و تحول استراتژی‌های دفاعی مورد استفاده قرار گیرد. افزون بر این، نتایج بر ضرورت هم‌زمانی توسعه فناوری با حکمرانی داده، ملاحظات اخلاقی و توانمندسازی سرمایه انسانی تأکید دارد.

استناد به این مقاله: منصوری,منصور , حقیقی,علی محمد و روانبد,امین . (۱۴۰۴). کاربردهای هوش مصنوعی در تحول استراتژی های نظامی و امنیتی. پژوهش های روابط بین الملل, ۱۵(۴), ۱۹۹-۲۳۰
doi: 10.22034/irr.2026.593238.2887

مقدمه

در دهه‌های اخیر، هوش مصنوعی به یکی از مهم‌ترین فناوری‌های تحول‌آفرین قرن بیست‌ویکم تبدیل شده است؛ فناوری‌ای که دامنه تأثیر آن از حوزه‌های اقتصادی، صنعتی و پزشکی فراتر رفته و به یکی از ارکان اصلی قدرت ملی، امنیت ملی و رقابت‌های ژئوپلیتیکی میان کشورها تبدیل شده است. در گذشته، توان دفاعی کشورها عمدتاً بر شاخص‌هایی نظیر حجم نیروهای نظامی، تجهیزات رزمی، توان لجستیکی و قدرت تسلیحاتی استوار بود، اما در عصر دیجیتال، این مؤلفه‌ها به‌تنهایی تضمین‌کننده برتری راهبردی نیستند. امروزه سرعت پردازش اطلاعات، توان تحلیل کلان‌داده‌ها، پیش‌بینی رفتار دشمن، تصمیم‌گیری هوشمند، مدیریت خودکار عملیات و مقابله با تهدیدات پیچیده سایبری به عوامل تعیین‌کننده قدرت دفاعی کشورها تبدیل شده‌اند. در چنین شرایطی، هوش مصنوعی نه صرفاً یک فناوری پشتیبان، بلکه یک مؤلفه بنیادین در بازتعریف استراتژی‌های دفاعی و راهبردی محسوب می‌شود.

تحولات اخیر در محیط امنیت بین‌الملل نیز اهمیت این موضوع را دوچندان کرده است. ظهور جنگ‌های ترکیبی، نبردهای شناختی، عملیات اطلاعاتی، حملات سایبری، سامانه‌های خودمختار، پهپادهای هوشمند، تسلیحات مبتنی بر یادگیری ماشین و رقابت قدرت‌های بزرگ برای دستیابی به برتری فناورانه، ماهیت تهدیدها را نسبت به گذشته به‌طور اساسی تغییر داده است. در چنین محیطی، برتری نظامی دیگر صرفاً به برخورداری از تجهیزات پیشرفته وابسته نیست، بلکه توانایی تبدیل حجم عظیم داده‌ها به دانش، آگاهی موقعیتی، پیش‌بینی تهدیدها و تصمیم‌گیری سریع و دقیق، نقش تعیین‌کننده‌ای در موفقیت راهبردی کشورها ایفا می‌کند. ازاین‌رو، بسیاری از دولت‌ها سرمایه‌گذاری گسترده‌ای در توسعه کاربردهای هوش مصنوعی در حوزه‌های دفاعی، اطلاعاتی و امنیتی انجام داده‌اند تا بتوانند مزیت رقابتی خود را در محیط پیچیده امنیتی حفظ کنند. در سطح عملیاتی، هوش مصنوعی کاربردهای متعددی از جمله تحلیل اطلاعات، شناسایی الگوهای تهدید، کنترل سامانه‌های خودمختار، مدیریت عملیات رزمی، پشتیبانی لجستیکی، دفاع سایبری، تحلیل تصاویر ماهواره‌ای، پیش‌بینی تحرکات دشمن و تصمیم‌یارهای فرماندهی را در بر می‌گیرد. با وجود این، اهمیت واقعی هوش مصنوعی زمانی آشکار می‌شود که این کاربردهای پراکنده در قالب قابلیت‌های راهبردی یکپارچه شوند و بتوانند فرآیندهای کلان دفاعی، امنیتی و حکمرانی را متحول سازند. به عبارت دیگر، ارزش راهبردی هوش مصنوعی تنها در خودکارسازی فعالیت‌ها یا افزایش سرعت پردازش اطلاعات خلاصه نمی‌شود، بلکه در ایجاد هم‌افزایی میان اطلاعات، شناخت، تصمیم‌گیری، فرماندهی، امنیت سایبری و مدیریت منابع دفاعی نهفته است. با وجود گسترش سریع

تحقیقات درباره هوش مصنوعی، بررسی ادبیات پژوهش نشان می‌دهد که بخش عمده مطالعات موجود بر توسعه الگوریتم‌ها، طراحی سامانه‌های هوشمند، کاربردهای فنی، یادگیری ماشین، بینایی ماشین، سامانه‌های تسلیحاتی یا دفاع سایبری متمرکز بوده‌اند. در مقابل، مطالعاتی که بتوانند این کاربردهای متنوع را در قالب یک چارچوب راهبردی جامع دسته‌بندی، تلفیق و تبیین کنند، بسیار محدود هستند. بسیاری از پژوهش‌ها هر یک تنها بخشی از مسئله را مورد توجه قرار داده‌اند؛ برای مثال، برخی صرفاً بر سامانه‌های خودمختار، برخی بر امنیت سایبری، برخی بر فرماندهی و کنترل، و برخی دیگر بر تحلیل اطلاعات تمرکز کرده‌اند. این رویکردهای جزیره‌ای موجب شده است که تصویر جامعی از نقش هوش مصنوعی در تحول استراتژی‌های دفاعی و راهبردی شکل نگیرد.

از سوی دیگر، تحول استراتژی‌های دفاعی تنها به فناوری وابسته نیست، بلکه ابعاد مدیریتی، سازمانی، نهادی، حقوقی، اخلاقی و حکمرانی نیز در آن نقش اساسی دارند. استقرار موفق سامانه‌های هوش مصنوعی مستلزم وجود زیرساخت‌های داده، نظام‌های تصمیم‌گیری انعطاف‌پذیر، چارچوب‌های قانونی، ملاحظات اخلاقی، امنیت اطلاعات، توسعه سرمایه انسانی متخصص و سازوکارهای حکمرانی هوشمند است. در نتیجه، تحلیل کاربردهای هوش مصنوعی بدون توجه به این ابعاد، نمی‌تواند تصویری کامل از ظرفیت‌های تحول‌آفرین آن ارائه دهد. همین موضوع ضرورت توسعه چارچوب‌هایی را آشکار می‌سازد که بتوانند علاوه بر کاربردهای فنی، پیامدهای راهبردی و نهادی هوش مصنوعی را نیز تبیین کنند.

در فضای رقابت‌های راهبردی کنونی، کشورهایی که بتوانند هوش مصنوعی را در تمامی سطوح برنامه‌ریزی، تصمیم‌گیری، فرماندهی، مدیریت بحران، دفاع سایبری، تحلیل اطلاعات و پیش‌بینی تهدیدها به‌صورت یکپارچه به کار گیرند، از مزیت رقابتی پایدارتری برخوردار خواهند شد. در مقابل، کشورهایی که فاقد چنین قابلیت‌هایی باشند، با کاهش سرعت واکنش، ضعف در تحلیل محیط، افزایش آسیب‌پذیری سایبری، کاهش کارایی تصمیم‌گیری و افت بازدارندگی مواجه خواهند شد. بنابراین، شناخت دقیق ابعاد کاربردی هوش مصنوعی در تحول استراتژی‌های دفاعی، نه‌تنها یک ضرورت علمی، بلکه یک نیاز راهبردی برای نظام‌های دفاعی و امنیتی محسوب می‌شود.

با وجود اهمیت این موضوع، همچنان شکاف نظری قابل‌توجهی در ادبیات پژوهش وجود دارد. تاکنون چارچوبی جامع که بتواند کاربردهای متنوع هوش مصنوعی را از سطح مصادیق عملیاتی به سطح قابلیت‌های کلیدی و در نهایت به کارکردهای کلان راهبردی ارتقا دهد، کمتر ارائه شده است. فقدان

چنین چارچوبی موجب شده است که سیاست‌گذاران، مدیران دفاعی و برنامه‌ریزان راهبردی درک منسجم و نظام‌مندی از نقش هوش مصنوعی در تحول دکترین‌های دفاعی و امنیتی نداشته باشند.

بر این اساس، پژوهش حاضر کاربردهای هوش مصنوعی در تحول استراتژی‌های دفاعی و امنیتی ایران و اسرائیل را بررسی می‌کند. انتخاب این دو کشور به دلیل موقعیت ژئوپلیتیکی و تفاوت‌های ساختاری آنها در توسعه فناوری‌های نظامی اهمیت دارد و می‌تواند الگوهایی برای سایر کشورها فراهم کند. این تحقیق با شناسایی ظرفیت‌ها و محدودیت‌های هوش مصنوعی، آثار آن بر تصمیم‌گیری راهبردی و امنیت ملی را تحلیل خواهد کرد و به دنبال پاسخ به این سؤال است که هوش مصنوعی چگونه می‌تواند تحول استراتژی‌های نظامی کشورها را شکل دهد و ایران و اسرائیل چگونه از آن برای تقویت توان دفاعی و امنیت ملی خود استفاده می‌کنند.

۱. ادبیات تحقیق

فناوری هوش مصنوعی در دهه اخیر به یکی از عوامل اصلی تحول در حوزه نظامی و امنیتی جهان تبدیل شده است و کشورها در راستای منافع ژئوپلیتیکی خود، به دنبال بهره‌گیری از آن برای تقویت توان دفاعی و تهاجمی هستند (Miailhe, 2018). ظهور پهپادهای پیشرفته، سامانه‌های زمینی بدون سرنشین و الگوریتم‌های تحلیل داده، ماهیت طراحی و اجرای عملیات‌های نظامی را دگرگون کرده است (Frizon, 2022; Lindholm, 2022). پهپادها با انجام مأموریت‌های شناسایی و حمله در فواصل دور و سیستم‌های خودران با کاهش ریسک انسانی، به تصمیم‌گیری سریع و عملیات تاکتیکی مؤثر کمک می‌کنند (Lindholm, 2022). همچنین تحلیل کلان‌داده و اطلاعات سایبری به ابزاری حیاتی برای پیش‌بینی رفتار دشمن و طراحی سناریوهای راهبردی تبدیل شده و رقابت جهانی در عرصه فناوری‌های نوین نظامی را تشدید کرده است (Martin, 2023; NATO Science & Technology Organization, 2020).

در چنین شرایطی، هوش مصنوعی علاوه بر نقش در مدیریت تهدیدات، در سیاستگذاری امنیت ملی نیز اهمیت یافته است (Akrami, 2024). قدرت‌های بزرگ نظیر آمریکا، چین و روسیه با سرمایه‌گذاری سنگین به دنبال تثبیت برتری نظامی خود هستند (Nocetti, 2020; Bradford, 2023)، و این روند فشار مضاعفی بر کشورهای منطقه‌ای مانند ایران و اسرائیل وارد کرده است تا هم توان دفاعی خود را ارتقاء دهند و هم از آسیب‌پذیری سایبری جلوگیری کنند (Precedenceresearch, 2023; Roth, 2019). رقابت بر سر الگوریتم‌ها و فناوری‌های هوش مصنوعی همچنین به شکل‌گیری «جنگ داده‌ای» و تهدیدات اطلاعاتی پیچیده منجر شده است (Martin, 2023; Betul Yucer, 2023). در سطح عملیاتی، هوش

مصنوعی در تحلیل داده‌های میدان نبرد، شناسایی تهدیدات، خودکارسازی دفاع و تصمیم‌گیری سریع کاربرد گسترده دارد (Sarker, 2022; Bousquet, 2022). ایران و اسرائیل نیز با توجه به شرایط خاص امنیتی، از این فناوری در سامانه‌های موشکی، پهپادهای رزمی و هشدارهای زودهنگام بهره می‌گیرند و با توجه به تجربیات قدرت‌های بزرگ، به دنبال افزایش دقت عملیاتی و کاهش هزینه‌های انسانی هستند. با این حال، تهدیدات نوینی مانند حملات سایبری و جنگ اطلاعاتی نشان می‌دهد که اتکا به تجهیزات فیزیکی بدون توسعه الگوریتم‌های هوشمند کافی نیست (Frizon, 2022; Lindholm, 2022).

هوش مصنوعی به عنوان شاخه‌ای از علوم کامپیوتر، توانایی تحلیل داده‌های پیچیده، پیش‌بینی نتایج و خودکارسازی تصمیم‌گیری‌ها را فراهم می‌آورد و به همین دلیل در حوزه نظامی و امنیتی اهمیت ویژه‌ای یافته است. از منظر نظری، هوش مصنوعی می‌تواند به سه سطح راهبردی، عملیاتی و تاکتیکی در ارتش‌ها و سازمان‌های امنیتی کاربرد داشته باشد؛ در سطح راهبردی، الگوریتم‌های هوشمند با تحلیل کلان‌داده‌ها و شبیه‌سازی سناریوهای مختلف، امکان پیش‌بینی تحولات ژئوپلیتیکی و تهدیدات امنیتی را فراهم می‌کنند، در سطح عملیاتی به بهینه‌سازی منابع و مدیریت عملیات‌ها کمک می‌کنند و در سطح تاکتیکی، سیستم‌های خودران مانند پهپادها و خودروهای بدون سرنشین، تصمیم‌گیری سریع و دقیق در میدان نبرد را ممکن می‌سازند. به این ترتیب، هوش مصنوعی نه تنها ابزاری برای خودکارسازی عملیات‌هاست، بلکه بستری برای تحول مفهومی و استراتژیک در دفاع و امنیت ملی فراهم می‌آورد. از منظر نظریه‌های ژئوپلیتیک و امنیت بین‌الملل، کاربرد هوش مصنوعی در نظامی‌گری موجب تغییر موازنه قدرت و ایجاد رقابت‌های نوین میان کشورها شده است. نظریه‌های کلاسیک قدرت و بازدارندگی، که بر توازن تسلیحاتی و قدرت نظامی مبتنی هستند، در عصر هوش مصنوعی نیازمند بازبینی شده‌اند؛ زیرا فناوری‌های هوشمند می‌توانند بازدارندگی غیرمتعارف، تهدیدات سایبری و عملیات اطلاعاتی پیچیده ایجاد کنند که پیش از این در چارچوب سنتی تحلیل نمی‌شدند. این تحول موجب شده است که کشورها برای حفظ امنیت ملی و افزایش اثربخشی استراتژی‌ها، علاوه بر سرمایه‌گذاری در تجهیزات فیزیکی، به توسعه الگوریتم‌ها، داده‌های کلان و تحلیل‌های پیش‌بینی‌کننده نیز توجه کنند. در نتیجه، مبانی نظری این پژوهش بر تقاطع علوم کامپیوتر، امنیت ملی و ژئوپلیتیک بنا شده است و نقش هوش مصنوعی در تغییر ساختار قدرت و تصمیم‌گیری‌های راهبردی را مورد توجه قرار می‌دهد. علاوه بر این، نظریه‌های مدیریت ریسک و تصمیم‌گیری هوشمند نیز اهمیت کاربرد هوش مصنوعی در حوزه نظامی را توضیح می‌دهند. هوش مصنوعی با توانایی تحلیل حجم عظیمی از اطلاعات و ارائه سناریوهای مختلف، امکان ارزیابی ریسک

و مدیریت بحران را به صورت بهینه فراهم می‌آورد. این توانمندی، به ویژه در شرایط عدم قطعیت و پیچیدگی میدان نبرد، موجب کاهش خطاهای انسانی و افزایش سرعت و دقت تصمیم‌گیری می‌شود. بر اساس این مبانی، هوش مصنوعی می‌تواند به عنوان ابزاری برای همگرایی استراتژی‌های دفاعی و امنیتی با اهداف کلان ملی مورد استفاده قرار گیرد و ضمن بهبود کارایی عملیاتی، سطح پاسخ‌دهی کشورها به تهدیدات نوین را ارتقا دهد. در نهایت، کاربردهای عملی هوش مصنوعی در امنیت ملی و نظامی را می‌توان در سه حوزه اصلی شناسایی کرد: شناسایی و تحلیل تهدیدات، خودکارسازی سامانه‌های دفاعی و تقویت توان بازدارندگی و تصمیم‌گیری راهبردی. پژوهش‌های پیشین نشان می‌دهند که کشورهایی که در بهره‌گیری از هوش مصنوعی پیشرو هستند، توانایی واکنش سریع به تهدیدات، بهینه‌سازی منابع دفاعی و افزایش دقت عملیات‌ها را دارند، در حالی که کشورهایی که از این فناوری عقب هستند، در معرض آسیب‌پذیری بیشتر و محدودیت در تصمیم‌گیری راهبردی قرار دارند. بنابراین، مبانی نظری این پژوهش بر ادغام فناوری هوش مصنوعی با اصول راهبردی و امنیت ملی بنا شده است و چارچوبی برای تحلیل مقایسه‌ای ایران و اسرائیل در بهره‌گیری از این فناوری فراهم می‌آورد. در ادامه به بیان پیشینه تحقیقات در داخل و خارج از کشور پرداخته شده است: سیمبر و همکاران (۱۴۰۴) در پژوهشی با عنوان «تحلیل نقش هوش مصنوعی در استراتژی دفاعی و پیامدهای آن برای امنیت ملی و جهانی (مطالعه موردی چین، روسیه و آمریکا)» با رویکرد تحلیلی-تطبیقی نشان می‌دهند که نفوذ فناورانه هوش مصنوعی فراتر از بهبود کارایی عملیاتی است و ساختارهای راهبردی و موازنه قوا را در سطح بین‌الملل مجدداً شکل می‌دهد؛ پژوهش با تشریح نمونه‌های برجسته از سه قدرت بزرگ، تأکید می‌کند که سرمایه‌گذاری‌های متمرکز در حوزه‌های داده‌محور، سامانه‌های خودکار تصمیم‌گیر و توانمندسازی عملیات اطلاعاتی، موجب ایجاد مزیت‌های آشکار در حوزه پیش‌آگاهی، شتاب تصمیم‌گیری و اثربخشی رزمی شده است. از منظر نظری، نویسندگان با پیونددادن مفاهیم قدرت نرم و قدرت سخت به ظرفیت‌های هوش مصنوعی، استدلال می‌کنند که AI می‌تواند مرزهای راهبردی سنتی را مات کند و حوزه‌های جدیدی چون جنگ‌های سایبری-شناختی را تقویت نماید؛ از منظر پیامدی، مقاله پیامدهای پیچیده‌ای همچون افزایش سرعت رقابت تسلیحاتی، تضعیف شفافیت راهبردی و بروز چالش‌های جدید در حقوق بین‌الملل و بازدارندگی را پررنگ می‌سازد. روش‌شناسی مبتنی بر تحلیل اسنادی و بررسی سیاست‌های رسمی این کشورها به مؤلفان امکان می‌دهد نشانه‌هایی از جهت‌گیری‌های بلندمدت را استخراج کنند و نشان دهند که سیاست‌گذاری‌های فناورانه-امنیتی در سه کشور ناهمگن است؛ این

ناهمگنی خود موجب تفاوت در کاربری‌های عملیاتی و ساختارهای نظارتی شده و پیامدهایی را برای ثبات نظام بین‌الملل ایجاد می‌نماید. در نهایت، تحقیق به‌طور مکرر ضرورت بازنگری در چارچوب‌های راهبردی، ارتقای مکانیسم‌های شفافیت بین‌المللی و توجه به ابعاد اخلاقی–حقوقی را به عنوان پیش‌شرط‌های مدیریت موثر این فناوری در حوزه دفاعی برجسته می‌سازد. مهدوی کیا (۱۴۰۴) در مقاله «بررسی قابلیت‌های هوش مصنوعی برای کاربردهای دفاعی–امنیتی جمهوری اسلامی ایران» با رویکرد ترکیبی (کمی – کیفی)، قابلیت‌های هوش مصنوعی در عرصه‌های مختلف دفاعی مانند تحلیل داده‌های بزرگ، شناسایی تهدیدات سایبری، پدافند هوایی، شناسایی، امنیت لجستیکی و مدیریت نظامی را تحلیل کرده است. نتایج نشان می‌دهد که AI می‌تواند دقت تصمیم‌گیری را بالا ببرد، منابع نظامی را بهینه کند و خطاهای انسانی را کاهش دهد، اما زیرساخت‌های فناوری، امنیت اطلاعات و مدیریت ریسک همچنان چالش‌های جدی هستند. تقی پور جاوی (۱۴۰۴) در مقاله «تأثیر هوش مصنوعی بر ماهیت جنگ‌های آینده» با روش تحلیلی و اسنادی، استدلال می‌کند که هوش مصنوعی مولفه‌های کلاسیک جنگ (مثلاً خشونت، شانس، و ابعاد سیاسی) را تغییر خواهد داد. بر اساس نتایج، کاربرد AI در حوزه نظامی می‌تواند باعث تشدید قابلیت جنگاوری، افزایش پیچیدگی عملیات و تحول راهبردی در ماهیت نبرد شود.

عظیمی‌زاده و همکاران (۱۴۰۴) در پژوهشی با عنوان «طراحی الگوی فرماندهی و کنترل هوشمند ارتش جمهوری اسلامی ایران مبتنی بر کلان‌داده» با تمرکز بر ظرفیت‌های بومی‌سازی سامانه‌های C2 هوشمند، مدلی مفهومی–کاربردی پیشنهاد می‌دهند که تلفیق کلان‌داده، یادگیری ماشین و لایه‌های تصمیم‌سازی انسانی را به‌عنوان هسته معماری فرماندهی آینده تعریف می‌کند. این کار با تحلیل نیازمندی‌های سازمانی و محدودیت‌های فناورانه موجود در ساختارهای نظامی ایران، نشان می‌دهد که پیاده‌سازی C2 هوشمند نیازمند اصلاحات بنیادین در حوزه جمع‌آوری داده، استانداردسازی فرمت‌های اطلاعاتی، امنیت داده‌ها و توسعه نیروی انسانی متخصص است؛ پژوهش به‌تفصیل به نقش لایه‌های تبیین‌پذیری (XAI) و مکانیزم‌های نظارتی انسانی اشاره کرده و تاکید می‌نماید که حفظ «انسان در حلقه» در مراحل حساس تصمیم‌گیری جهت کاهش ریسک‌های اخلاقی و حقوقی حیاتی است. از منظر کاربردی، الگوی پیشنهادی مراحل گام‌به‌گام انتقال از وضعیت سنتی به معماری داده‌محور را تشریح می‌کند و پیشنهاداتی عملی برای پیاده‌سازی پایلوت‌های منطقه‌ای، معیارهای ارزیابی عملکرد و سنجش اثربخشی ارائه می‌دهد؛ همچنین مقاله به چالش‌های پیاده‌سازی مانند مسائل زیرساختی، سرمایه‌گذاری بلندمدت و مقاومت سازمانی می‌پردازد و راهکارهایی برای مدیریت تغییر فرهنگ سازمانی و ایجاد اکوسیستم تعامل بین ستاد و

صنعت دفاعی پیشنهاد می‌کند. دهقانیان و همکاران (۱۴۰۴) در پژوهشی با عنوان «تحلیل و بررسی تاثیر هوش مصنوعی بر عمق استراتژیک کشورها» با بهره‌گیری از رویکرد تحلیلی-توصیفی مفهوم «عمق استراتژیک» را بازتعریف می‌کنند و نشان می‌دهند که فناوری‌های هوش مصنوعی با فرایندهای اطلاعاتی-تحلیلی و اتوماسیون عملیات، قابلیت گسترش یا تضعیف عمق استراتژیک را دارند. مطالعه با تفکیک ابعاد توانی (شامل قابلیت پیش‌آگاهی، توانمندی پاسخ‌دهی و تداوم عملیات) و ابعاد ساختاری (سیاست‌گذاری، زیرساخت داده‌ای و آموزش نیروی انسانی) نشان می‌دهد که ملی‌هایی که سرمایه‌گذاری و چارچوب حقوقی مناسب را ایجاد کرده‌اند، می‌توانند از هوش مصنوعی برای ایجاد لایه‌های دفاعی پنهان، افزایش توان بازدارندگی از راه دور و اعمال فشار راهبردی بهره ببرند؛ در مقابل، کشورهایی با ضعف در زیرساخت داده‌ای یا خلل در هماهنگی بین نهادها با خطر تبدیل‌شدن به بازیگران آسیب‌پذیر در مواجهه با دشمنان داده‌محور مواجه خواهند شد. پژوهش همچنین به شواهدی از تغییر در تئوری‌های کلاسیک توازن قوا اشاره دارد و استدلال می‌کند که هوش مصنوعی عامل تغییر در مفهوم فاصله جغرافیایی، زمان واکنش و پوشش اطلاعاتی شده که در مجموع عمق استراتژیک را تحت تأثیر قرار می‌دهد. خسروی و همکاران (۱۴۰۴) در پژوهشی با عنوان «استفاده از هوش مصنوعی در شبیه‌سازی و آموزش نظامی» به‌صورت مفصل نشان می‌دهند که ادغام فناوری‌های یادگیری عمیق، واقعیت مجازی/افزوده و الگوریتم‌های بازخورد مبتنی بر داده می‌تواند کیفیت آموزش نظامی را به طور قابل ملاحظه‌ای ارتقا دهد و توانایی‌های تصمیم‌گیری در شرایط پیچیده و پرفشار را بهبود بخشد. مطالعه تجربی و توصیفی ارائه‌شده در این پژوهش حاکی از آن است که شبیه‌سازی‌های داده‌محور با سناریوهای پویا و یادگیری تقویتی می‌توانند خطای انسانی را کاهش داده و زمان لازم برای دستیابی به سطوح عملکرد مطلوب را کوتاه کنند؛ علاوه بر این، قابلیت‌های تحلیل رفتار اپراتورها توسط سامانه‌های هوشمند، زمینه‌ساز برنامه‌های آموزشی شخصی‌سازی‌شده و تمرینات مبتنی بر نیازهای واقعی رزمی می‌گردد. نویسندگان همچنین به ملاحظات اخلاقی و امنیتی مانند محافظت از داده‌های حساسی که در پلتفرم‌های شبیه‌سازی تولید می‌شوند، خطرات ایجاد وابستگی بیش از حد به ابزارهای شبیه‌سازی و ضرورت تضمین قابلیت انتقال مهارت‌ها از محیط شبیه‌سازی به میدان واقعی اشاره کرده و راهکارهایی برای طراحی برنامه‌های آموزشی مقاوم و قابل ارزیابی ارائه می‌دهند.

نظری (۱۴۰۳) در مقاله «هوش مصنوعی و تحول بنیادین در سیاستگذاری‌های امنیتی-دفاعی» با رویکرد توصیفی-تبیینی بررسی می‌کند که هوش مصنوعی چگونه توان انسان‌ها در تصمیم‌گیری راهبردی امنیتی

را دگرگون می‌سازد. او نشان می‌دهد که تحلیل داده بزرگ و تصمیم‌گیری خودکار مبتنی بر الگوریتم‌های AI می‌تواند سیاستگذاری امنیتی را تسریع کند و تصمیم‌گیران را قادر سازد تا در سطوح ملی و بین‌المللی با تهدیدات نوین هوشمندانه‌تر مواجه شوند.

نورمحمدی و تقی‌پور (۱۴۰۳) در پژوهشی با عنوان «تأثیر هوش مصنوعی بر ماهیت جنگ‌ها از منظر سیاست‌های راهبردی دولت‌های آمریکا، چین و روسیه» به تحلیل تطبیقی نگرش‌های راهبردی سه قدرت بزرگ در برابر تحولات ناشی از AI می‌پردازند و استدلال می‌کنند که هر یک از این بازیگران با تکیه بر مزیت‌های نسبی خود (پیشینه فناورانه، منابع داده‌ای و ساختارهای حکمرانی) دکترین‌های متفاوتی را دنبال می‌کنند که در مجموع شکل و ماهیت جنگ‌ها را بازتعریف می‌کند. مقاله نمایانگر آن است که آمریکا به سمت تمرکز بر ادغام هوش مصنوعی با عملیات اطلاعاتی و شبکه‌های فرماندهی-کنترل حرکت می‌کند، چین توسعه سریع ظرفیت‌های هوش‌مصنوعی را به‌عنوان جزء راهبرد ملی صنعتی و نظامی در پیش گرفته و روسیه بر استفاده تاکتیکی از سایبری و سیستم‌های ارزان‌تر و چابک‌تر تمرکز دارد؛ این تفاوت‌ها به تغییر در الگوهای مواجهه، طراحی تسلیحات و تعریف اهداف جنگی منجر شده است. نویسندگان همچنین بر ضرورت بازنگری در تئوری‌های بازدارندگی و قوانین درگیری مسلحانه تاکید کرده و هشدار می‌دهند که سرعت تصمیم‌گیری خودکار و عدم شفافیت الگوریتمی می‌تواند آستانه بروز درگیری‌های ناخواسته را کاهش دهد.

ریاضی و بیابانی (۱۴۰۳) در پژوهشی با عنوان «الگوی تهدیدات فناوری‌های نوین نیروی زمینی ارتش جمهوری اسلامی ایران» به تبیین تهدیدات خاص مرتبط با ورود فناوری‌های نوین در حوزه زمینی (اعم از سامانه‌های هوشمند، پهپادها و سیستم‌های ارتباطی داده‌محور) می‌پردازند و چارچوبی برای اولویت‌بندی تهدیدات بر اساس شدت، احتمال وقوع و قابلیت‌های مقابله‌ای ارائه می‌دهند. پژوهش با تلفیق تحلیل ریسک و بررسی تجربه‌های منطقه‌ای، نشان می‌دهد که تهدیدات فناورانه دارای جنبه‌های چندبعدی—شامل نفوذ سایبری، اخلال در حسگرها، جنگ الکترونیک و بهره‌گیری دشمن از داده‌های باز—هستند و پاسخ مؤثر نیازمند توسعه همزمان ظرفیت‌های دفاع سایبری، آموزش نیروها و بازسازی ساختارهای لجستیکی و ارتباطی است. همچنین مؤلفان پیشنهاد می‌کنند که نیروی زمینی باید ضمن نوسازی سامانه‌ها، مدل‌های تهدید-پاسخ مبتنی بر داده طراحی کند تا از هم‌افزایی فناوری‌های نوین به‌نحو مؤثر برای کاهش آسیب‌پذیری بهره گیرد. پیرمحمدی و همکاران (۱۴۰۳) در پژوهشی با عنوان «تکنوژئوپلیتیک و تغییر الگوهای سنتی جهانی در حوزه فناوری‌های دیجیتال؛ چشم‌اندازی استراتژیک

برای ایران» به تبیین چگونگی تأثیر تحولات فناورانه بر ساختارهای ژئوپلیتیکی سنتی می‌پردازند و استدلال می‌کنند که فناوری‌های دیجیتال از جمله هوش مصنوعی به عنوان عامل تغییر هژمونیک عمل می‌کنند که مرزهای جغرافیایی را کم‌اهمیت و اهمیت شبکه‌های داده، زیرساخت‌های فضایی و زنجیره‌های تأمین فناوری را افزایش می‌دهد. مقاله به تشریح فرصت‌ها و تهدیداتی می‌پردازد که برای ایران در این فضای نوظهور قابل تصور است؛ از جمله ظرفیت ارتقای خودکفایی فناورانه، بهره‌برداری از بازارهای منطقه‌ای و بهبود توان بازدارندگی دیجیتال، در برابر مخاطراتی چون تحریم‌های فناورانه، وابستگی به زنجیره‌های خارجی و فشارهای سیاسی–اقتصادی که می‌تواند دسترسی به فناوری‌های حیاتی را محدود کند. از منظر سیاست‌گذاری، نویسندگان توصیه‌هایی در جهت تدوین راهبرد ملی فناوری، سرمایه‌گذاری در توسعه نیروی انسانی و تقویت همکاری‌های منطقه‌ای ارائه می‌دهند.

انصاری و همکاران (۱۴۰۳) در پژوهشی با عنوان «تاثیر هوش مصنوعی بر جنگ و قواعد حقوق بین‌الملل با تاکید بر نهج‌البلاغه» پژوهشگران به بررسی ابعاد اخلاقی و حقوقی کاربردهای نظامی هوش مصنوعی پرداخته‌اند و تلاش کرده‌اند دیدگاه‌های فقهی–اخلاقی را در ترکیب با حقوق بین‌الملل انسانی برای ایجاد چارچوبی بومی‌پذیر ارائه کنند. این کار با مرور موازین اخلاقی کلاسیک و آموزه‌های نهج‌البلاغه، مباحثی چون مسئولیت‌پذیری در تصمیم‌گیری خودکار، حفظ کرامت انسانی در میدان نبرد و ضرورت نظارت انسانی بر استفاده از زور را برجسته می‌سازد؛ نویسندگان اظهار دارند که بدون بازتعریف سازوکارهای پاسخ‌گویی و شفافیت در سامانه‌های AI، خطر نقض اصول حقوق بین‌الملل و ایجاد آسیب‌های غیرنظامی افزایش می‌یابد. نتیجه‌گیری مقاله بر لزوم ایجاد مقررات داخلی و بین‌المللی منطبق با ارزش‌های اخلاقی و حقوقی تأکید دارد و پیشنهاد می‌دهد که مبادلات علمی و حقوقی با نهادهای بین‌المللی می‌تواند به تدوین چارچوب‌های اقتضایی کمک نماید. اسماعیلی و میارعباسی (۱۴۰۳) در پژوهشی با عنوان «بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی–امنیتی جمهوری اسلامی ایران» حوزه‌هایی مانند پردازش زبان طبیعی، تحلیل رفتار شناختی، و سیستم‌های تصمیم‌یار شناختی را به عنوان محورهای بالقوه کاربرد در دفاع ملی معرفی می‌کنند و نشان می‌دهند که علوم شناختی می‌تواند به طراحی عملیات روانی–شناختی، تحلیل تهدیدات انسانی و بهینه‌سازی تعامل انسان–ماشین در محیط‌های میدانی کمک کند. پژوهش با تحلیل نمونه‌های موردی و تبیین سناریوهای کاربردی، ظرفیت‌های این فناوری‌ها را در افزایش دقت عملیات اطلاعاتی و کاهش هزینه‌های تصمیم‌گیری بیان می‌دارد؛ در عین حال به مخاطراتی مانند سوءاستفاده از فناوری‌های تاثیرگذار بر ادراک جمعی و امکان بروز پیامدهای اخلاقی و

حقوقی اشاره می‌کند. در پایان، مقاله ضرورت ایجاد سیاست‌های راهبردی جهت هدایت پژوهش و توسعه علمی در این حوزه و تقویت پیوند میان دانشگاه، نهادهای پژوهشی و صنایع دفاعی را مورد تأکید قرار می‌دهد.

الله‌ویسیان و همکاران (۱۴۰۳) در پژوهشی با عنوان «بررسی نقش هوش مصنوعی در توسعه استراتژی‌های فرماندهی و کنترل انتظامی در جنگ شناختی» به تحلیل بکارگیری AI برای تقویت توانمندی‌های انتظامی در مواجهه با تهدیدات شناختی می‌پردازند و نشان می‌دهند که سامانه‌های تحلیل داده و تولید پیام می‌توانند نقش محوری در شناسایی، پیشگیری و پاسخ به عملیات اطلاعاتی و نفوذ روانی ایفا کنند. مطالعه با بررسی مفاهیم «جنگ شناختی» و سازوکارهای حمله شناختی، پیشنهاد می‌کند که ادغام ابزارهای پیش‌بینیگر مبتنی بر یادگیری ماشین با ساختارهای فرماندهی انتظامی موجب بهبود زمان واکنش، دقت هدف‌گیری اطلاعاتی و هماهنگی بین نهادهای ذی‌ربط خواهد شد؛ با این وجود، نویسندگان هشدار می‌دهند که کاربرد این تکنیک‌ها بدون چارچوب‌های اخلاقی–حقوقی و مکانیزم‌های شفافیت ممکن است به تضعیف اعتماد عمومی و تضییع حقوق مدنی منجر شود. در پایان، مقاله مجموعه‌ای از توصیه‌های عملی برای توسعه الگوریتم‌های قابل‌ارائه توضیح (XAI)، سیاست‌های محافظت از داده و برنامه‌های آموزشی ویژه پرسنل انتظامی ارائه می‌نماید. قوامی‌پور و محمودی (۱۴۰۳) در پژوهشی با عنوان «تاثیر استراتژی‌های جنگ هوشمند مبتنی بر هوش مصنوعی بر مطالعات امنیت ملی، منطقه‌ای و جهانی» به بررسی آثار راهبردی ظهور جنگ هوشمند می‌پردازند و به‌ویژه تاکید می‌کنند که این نوع از جنگ با تلفیق عملیات فیزیکی، سایبری و شناختی می‌تواند چارچوب‌های سنتی تحلیل امنیت را دگرگون سازد. مقاله نشان می‌دهد که مطالعه جنگ هوشمند نیازمند رویکردی بین‌رشته‌ای است که هم عناصر فنی (سامانه‌ها و الگوریتم‌ها) و هم عناصر اجتماعی–سیاسی (ساختارهای حکمرانی، اعتبار بین‌المللی و حقوق) را درنظر بگیرد؛ نویسندگان با بررسی موردی چند منطقه، تغییر در نحوه شکل‌گیری تهدیدات و ضرورت بازتعریف مفاهیمی مانند حوزه عملیاتی و بازدارندگی را برجسته می‌سازند. همچنین پیشنهاد می‌شود که پژوهش‌های آینده باید بر تعامل بین بازیگران غیردولتی، شرکت‌های فناور و نهادهای حاکمیتی تمرکز کنند تا الگوهای نوظهور تهدید و پاسخ مشخص‌تر شود. جهان‌دیده‌هو میرفخرائی (۱۴۰۳) در پژوهشی با عنوان «کاربرد هوش مصنوعی در بخش نظامی؛ مطالعه موردی: ایالات متحده آمریکا و چین» با رویکرد تطبیقی نشان می‌دهند که هرچند هر دو کشور در مسیر ادغام AI در نظامی‌گری سرمایه‌گذاری‌های کلان انجام داده‌اند، اما الگوها، اولویت‌ها و ساختارهای سازمانی متفاوتی

را دنبال می‌کنند که منجر به خروجی‌ها و آموزه‌های متباینی شده است. مقاله با پرداختن به حوزه‌های تحقیق و توسعه، نوآوری صنعتی، و چارچوب‌های قانونی، نتیجه می‌گیرد که ایالات متحده بر نوآوری مبتنی بر اکوسیستم باز و هم‌افزایی میان دانشگاه–صنعت–نظامی تکیه دارد، در حالی که چین با رویکردی دولت‌محور و برنامه‌ریزی مرکزی سعی در تسریع و تمرکز توسعه توانمندی‌های نظامی–فناورانه دارد؛ این تفاوت‌ها در نهایت بر سرعت به‌کارگیری سامانه‌ها، استانداردهای نظارتی و تعاملات بین‌المللی تاثیرگذار بوده است. مقاله همچنین به تبعات منطقه‌ای این رقابت فناورانه اشاره نموده و بر نیاز به بازنگری در دیپلماسی فناوری و مکانیزم‌های کاهش تنش تأکید می‌کند.

رستمی (۱۴۰۱) در پژوهشی با عنوان «شناسایی و معرفی ظرفیت‌های کاربردی هوش مصنوعی در توسعه مضمون‌های راهبردی در سازمان‌های نظامی» با مرور ظرفیت‌های عملیاتی AI در سطوح تاکتیکی تا راهبردی، مجموعه‌ای از زمینه‌های کلیدی را برای کاربرد مستقیم فناوری در سازمان‌های نظامی معرفی می‌کند؛ این زمینه‌ها شامل تحلیل اطلاعاتی به‌صورت بلادرنگ، افزایش اتوماسیون در مدیریت لجستیک، بهینه‌سازی برنامه‌ریزی رزمی و توسعه ابزارهای پشتیبانی تصمیم‌گیری است. رستمی بر اهمیت ایجاد چارچوب‌های نهادی برای هدایت پژوهش و انتقال فناوری از آزمایشگاه به میدان تأکید می‌نماید و نشان می‌دهد که بدون سیاست‌گذاری هماهنگ، سرمایه‌گذاری‌های جزیره‌ای ممکن است منجر به تکه‌تکه‌شدن قابلیت‌ها و ناکارآمدی در سطح عملیاتی شود. علاوه بر این، مقاله ضمن ارائه پیشنهادهایی برای تقویت ظرفیت‌های داخلی از طریق آموزش نیروی انسانی، توسعه اکوسیستم استارتاپی–صنعتی و ایجاد معیارهای اندازه‌گیری عملکرد، ضرورت توجه به امنیت داده و تاب‌آوری در برابر حملات سایبری را یادآور می‌گردد. متیوس و کولز (۲۰۲۵) در تحقیق خود با عنوان «نقش هوش مصنوعی در امنیت سایبری نظامی: بینش داده‌ها و روش‌های ارزیابی»، به بررسی نحوه کاربرد فناوری‌های هوش مصنوعی در حوزه امنیت سایبری نیروهای مسلح پرداخته‌اند و نشان می‌دهند که هوش مصنوعی نه‌تنها می‌تواند در شناسایی تهدیدات پیشرفته و تحلیل داده‌های شبکه‌های نظامی موثر باشد، بلکه قابلیت ارزیابی اثربخشی سامانه‌های دفاع سایبری را نیز فراهم می‌کند. این مطالعه با بهره‌گیری از روش تحلیل داده‌های بزرگ و نمونه‌های عملیاتی، نشان می‌دهد که پیاده‌سازی الگوریتم‌های هوشمند در امنیت سایبری منجر به افزایش سرعت واکنش در برابر حملات، کاهش خطاهای انسانی و بهبود تصمیم‌گیری راهبردی می‌شود. پژوهش همچنین به چالش‌هایی همچون نیاز به داده‌های معتبر، پیچیدگی شبکه‌های نظامی و خطر وابستگی بیش

از حد به الگوریتم‌ها اشاره کرده و راهکارهایی برای مدیریت این محدودیت‌ها ارائه می‌دهد، که اهمیت همگرایی بین تحلیل داده، هوش مصنوعی و سیاست‌های امنیتی را برجسته می‌کند.

آسیمن و همکاران (۲۰۲۵) در تحقیق خود با عنوان «سامانه‌های تسلیحاتی مبتنی بر هوش مصنوعی و آینده جنگ‌های مدرن» بر تحولات بنیادین در طراحی و به‌کارگیری تسلیحات نظامی با بهره‌گیری از هوش مصنوعی تمرکز دارد و نشان می‌دهد که این فناوری قادر است سرعت تصمیم‌گیری، دقت هدف‌گیری و توانمندی‌های پیش‌آگاهی نیروها را به طور چشمگیری افزایش دهد. پژوهشگران با تحلیل روندهای نوین تسلیحاتی و برنامه‌های توسعه نظامی در چند کشور پیشرفته، بر ضرورت بازتعریف دکترین‌های دفاعی و تغییر الگوهای سنتی جنگ تأکید می‌کنند و بیان می‌دارند که ورود هوش مصنوعی به میدان نبرد موجب تغییر توازن قدرت، ایجاد تهدیدات جدید و افزایش اهمیت نوآوری فناورانه در سیاست‌های امنیتی می‌شود. فغانی و قریشی (۲۰۲۵) در تحقیق خود با عنوان «استفاده از هوش مصنوعی در سلاح‌های نظامی: از منظر اصول حقوق بشردوستانه و فقه اسلامی» به تحلیل ابعاد اخلاقی و قانونی کاربرد هوش مصنوعی در تسلیحات پرداخته‌اند و نشان می‌دهند که هرچند فناوری‌های خودکار و هوشمند می‌توانند دقت عملیاتی و کاهش تلفات غیرنظامیان را ارتقا دهند، اما رعایت چارچوب‌های حقوق بین‌الملل و آموزه‌های فقهی برای تضمین مشروعیت و اخلاقیات حیاتی است. پژوهش با ارائه نمونه‌های موردی و استدلال‌های نظری، ضرورت طراحی الگوریتم‌ها و سامانه‌های تصمیم‌گیر شفاف و قابل توضیح را برجسته می‌سازد و تأکید می‌کند که ترکیب بینش‌های فقهی و حقوقی می‌تواند مسیر توسعه کاربردهای نظامی هوش مصنوعی را با حداقل ریسک حقوقی و اخلاقی هدایت کند.

شابیر و همکاران (۲۰۲۵) در پژوهشی با عنوان «نقش هوش مصنوعی در کاربردهای نظامی خاورمیانه و پیامدهای آن بر امنیت منطقه‌ای با تأکید بر منازعه ایران و اسرائیل» با رویکرد توصیفی–تحلیلی بررسی می‌کنند که چگونه رقابت فناورانه ایران و اسرائیل در حوزه‌های پهپادی، جنگ سایبری، سامانه‌های هوشمند هدف‌گذاری و تحلیل داده، موجب تغییر الگوهای امنیتی و افزایش بی‌ثباتی منطقه شده است. نویسندگان نشان می‌دهند که اسرائیل با اتکا بر زیرساخت‌های فناورانه و شبکه‌های داده‌محور، از هوش مصنوعی برای شتاب تصمیم‌گیری عملیاتی و عملیات اطلاعاتی بهره می‌برد، در حالی که ایران با توسعه پهپادهای رزمی و سامانه‌های سایبری مبتنی بر الگوریتم‌های یادگیری ماشین، به دنبال بازدارندگی نامتقارن است. مقاله تأکید می‌کند که این رقابت نه‌تنها بر توازن منطقه‌ای اثر گذاشته، بلکه امنیت کشورهایی همچون ترکیه را نیز تحت تأثیر قرار داده و شکل جدیدی از تهدیدات مبتنی بر AI را در خاورمیانه

ایجاد کرده است. فاریس (۲۰۲۵) در مقاله‌ای با عنوان «هدف‌گذاری الگوریتمی در تقابل ایران و اسرائیل» با رویکرد تحلیل نظامی–فناورانه توضیح می‌دهد که چگونه هوش مصنوعی در فرآیندهای هدف‌گذاری، شناسایی اهداف و تحلیل عملیات رزمی توسط دو طرف مورد استفاده قرار می‌گیرد. نویسنده با بررسی نمونه‌های عملیاتی نشان می‌دهد که اسرائیل از سامانه‌های هدف‌گذاری الگوریتمی برای افزایش دقت حملات و کوتاه‌کردن چرخه تصمیم‌گیری بهره می‌گیرد، در حالی که ایران با توسعه مدل‌های تشخیص الگو و سامانه‌های هوشمند دفاعی، تلاش دارد ساختار بازدارندگی خود را تقویت کند. مقاله بیان می‌کند که این تحول تکنولوژیک علاوه بر افزایش سرعت و دقت عملیات، چالش‌هایی جدی در حوزه اخلاق نظامی، کنترل غیرمتمرکز تسلیحات و ریسک خطاهای الگوریتمی ایجاد کرده و موجب تغییر ماهیت رویارویی میان دو کشور شده است.

سکستون (۲۰۲۵) در گزارشی تحلیلی با عنوان «هوش مصنوعی و تحول جنگ سایبری نامتقارن: یافته‌هایی از تقابل ۲۰۲۵ ایران و اسرائیل»توضیح می‌دهد که چگونه هوش مصنوعی باعث تغییر الگوهای جنگ سایبری میان ایران و اسرائیل شده است. او با بررسی رخدادهای اخیر در این منازعه نشان می‌دهد که استفاده دو طرف از الگوریتم‌های پیش‌بینی حملات، تولید محتوای خودکار برای جنگ روانی، و طراحی بدافزارهای هوشمند، جنگ سایبری را از یک نبرد صرفاً فنی به یک نبرد شناختی–اطلاعاتی تبدیل کرده است. یافته‌ها نشان می‌دهد که اسرائیل با بهره‌گیری از سیستم‌های یادگیری ماشین در دفاع سایبری و نفوذ، به دنبال برتری اطلاعاتی است؛ در مقابل، ایران با استفاده از تاکتیک‌های نامتقارن مبتنی بر AI، از جمله حملات هوشمند به زیرساخت‌های حیاتی و عملیات نفوذ چندلایه، توانسته است موازنه‌ای نسبی ایجاد کند. گزارش بر پیامدهایی همچون تشدید فضای بی‌ثباتی، افزایش آسیب‌پذیری زیرساخت‌های غیرنظامی و تغییر شکل رقابت قدرت در خاورمیانه تأکید دارد. نیازی (۲۰۲۵) در تحقیق خود با عنوان «نظامی‌سازی هوش مصنوعی و پیامدهای آن برای امنیت جهانی – دیدگاه نظریه استراتژیک» بر بررسی پیامدهای راهبردی و ژئوپلیتیکی تسلیح هوش مصنوعی تأکید دارد و نشان می‌دهد که ادغام هوش مصنوعی در ساختارهای نظامی کشورها می‌تواند توازن قدرت جهانی را بازتعریف کرده و خطر رقابت تسلیحاتی سریع را افزایش دهد. نویسنده با تحلیل نظریه‌های استراتژیک و نمونه‌های تاریخی، استدلال می‌کند که استفاده گسترده از هوش مصنوعی در عملیات نظامی، محدودیت‌های زمان واکنش و فاصله جغرافیایی را کاهش داده و موجب پیچیدگی سیاست‌های بازدارندگی و تصمیم‌گیری راهبردی می‌شود، در نتیجه فشار بر دیپلماسی و نیاز به مقررات بین‌المللی نوظهور افزایش می‌یابد.

نادم (۲۰۲۵) در تحقیق خود با عنوان «رقابت تسلیحاتی هوش مصنوعی و ثبات راهبردی بین هند و پاکستان» به بررسی اثرات هوش مصنوعی بر توازن راهبردی در منطقه آسیای جنوبی می‌پردازد و نشان می‌دهد که رقابت فناورانه می‌تواند تعادل بازدارندگی سنتی را مختل کند و خطر تشدید درگیری‌های ناخواسته را افزایش دهد. پژوهش با تحلیل سیاست‌های دفاعی و توسعه سامانه‌های خودکار در هر دو کشور، بیان می‌کند که عدم شفافیت و سرعت تصمیم‌گیری الگوریتمی موجب پیچیدگی در مدیریت بحران و افزایش اهمیت گفتگوهای دوجانبه و مکانیسم‌های اعتمادسازی شده است.لیبل (۲۰۲۵) در تحقیق خود با عنوان «تأثیر هوش مصنوعی بر بدنه افسران» به بررسی تغییرات نقش، مهارت ها و آموزش افسران نظامی در مواجهه با فناوری‌های هوشمند می‌پردازد. پژوهش نشان می‌دهد که ادغام هوش مصنوعی در تصمیم‌گیری‌های تاکتیکی و استراتژیک باعث تغییر وظایف سنتی افسران، افزایش نیاز به مهارت‌های فناورانه و تحلیل داده و ضرورت بازآموزی مستمر شده است. همچنین مقاله به چالش‌های اخلاقی و روانی ناشی از وابستگی به سامانه‌های هوشمند و کاهش استقلال تصمیم‌گیری انسانی اشاره می‌کند.

ویلز و جفرسون (۲۰۲۵) در تحقیق خود با عنوان «مدل قدرت نوین و چابکی دفاع ملی ایالات متحده» بر نحوه استفاده از هوش مصنوعی برای افزایش انعطاف‌پذیری و سرعت واکنش نظامی تمرکز دارد. پژوهش نشان می‌دهد که هوش مصنوعی امکان تحلیل سریع داده‌ها، پیش‌بینی تهدیدات و هماهنگی بین بخش‌های مختلف دفاعی را فراهم می‌کند و چابکی راهبردی کشور را بهبود می‌بخشد، در حالی که نیاز به بازنگری ساختارهای فرماندهی و سیاست‌گذاری در راستای بهره‌برداری مؤثر از فناوری برجسته می‌شود. سرناتونی و همکاران و همکاران (۲۰۲۵) در تحقیق خود با عنوان «اسطوره، قدرت و توانمندی: بازاندیشی هوش مصنوعی، ژئوپلیتیک و جنگ» تحلیل می‌کنند که هوش مصنوعی نه تنها ابزار نظامی، بلکه عامل بازتعریف قدرت و سیاست بین‌الملل است. مقاله نشان می‌دهد که هوش مصنوعی می‌تواند نقش محوری در شکل‌دهی به تصمیمات استراتژیک، تقویت نفوذ ملی و تغییر ساختارهای سنتی جنگ داشته باشد و همزمان موجب پیچیدگی و عدم اطمینان در سیاست‌های جهانی شود.

پاندی (۲۰۲۵) در تحقیق خود با عنوان «هوش مصنوعی در جنگ: پیامدهای اخلاقی و ملاحظات راهبردی» به بررسی اثرات راهبردی و اخلاقی کاربرد هوش مصنوعی در عملیات نظامی می‌پردازد. نویسنده با تحلیل سناریوهای مختلف جنگ‌های مدرن، استدلال می‌کند که بهره‌گیری از فناوری‌های هوشمند نیازمند تدوین چارچوب‌های اخلاقی و راهبردی دقیق برای جلوگیری از سوءاستفاده و تشدید

تنش‌هاست. عباس و همکاران (۲۰۲۴) در تحقیق خود با عنوان «انقلاب در جنگ: نقش هوش مصنوعی در آینده دفاع» نشان می‌دهد که هوش مصنوعی به عنوان محرک نوآوری‌های نظامی، توان رزمی، سرعت تصمیم‌گیری و دقت عملیات‌ها را افزایش می‌دهد و در آینده، بازتعریف مفاهیم قدرت و بازدارندگی را ضروری می‌سازد. مقاله بر نیاز به هماهنگی بین تحقیق و توسعه، آموزش نیروها و سیاست‌های ملی تأکید می‌کند. مارکوئیز (۲۰۲۴) در تحقیق خود با عنوان «مزایا و چالش‌های هوش مصنوعی نظامی در حوزه دفاع» نشان می‌دهد که هوش مصنوعی توانمندی‌هایی همچون بهبود تصمیم‌گیری، کاهش ریسک انسانی و تحلیل داده‌های پیچیده را فراهم می‌کند، اما همزمان با چالش‌هایی مانند مسائل امنیتی، اخلاقی و وابستگی فناورانه همراه است که نیازمند مدیریت دقیق و سیاست‌گذاری مناسب است. ایمام (۲۰۲۱) در تحقیق خود با عنوان «نقش هوش مصنوعی در راهبرد دفاعی: پیامدها برای امنیت جهانی و ملی»، به تحلیل تأثیر هوش مصنوعی بر طراحی و اجرای سیاست‌های دفاعی می‌پردازد و نشان می‌دهد که این فناوری توانایی تغییر توازن قدرت، بهبود پاسخ‌دهی نظامی و بازتعریف تهدیدات را دارد، در حالی که ایجاد چارچوب‌های قانونی و سیاست‌گذاری برای مدیریت پیامدهای فناورانه ضروری است.

۲. روش شناسی تحقیق

به طور کلی روش های تحقیق در علوم رفتاری را می توان با توجه به دو ملاک هدف تحقیق و نحوه گردآوری داده ها، طبقه بندی نمود. این پژوهش از نظر هدف کاربردی و از لحاظ روش توصیفی از نوع همبستگی می باشد. این پژوهش توصیفی است، زیرا هدف آن توصیف عینی، واقعی و منظم حوادث، رویدادها و موضوعات مرتبط با حیطه پژوهش است. تحقیق توصیفی تحقیقی است که هدف آنها توصیف شرایط یا پدیده های مورد بررسی است. این تحقیق از جمله تحقیقات کاربردی بوده که برای کاربردهای هوش مصنوعی طراحی شده است. از لحاظ عدم دسترسی به آزمایشگاه نیز در زمره تحقیقات توصیفی می باشد. از حیث ماهیت تحقیق نیز منجمله تحقیقات ارزیابی بشمار می رود. اطلاعات و داده های مورد نیاز در این تحقیق به روش کتابخانه ای که اطلاعات مورد نیاز جهت تدوین مبانی نظری تحقیق که مرحله مهمی از یک کار تحقیقاتی را شامل می شود، با مراجعه به مراکز مختلف دانشگاهی، تحقیقاتی و با مطالعه نشریات معتبر علمی داخلی و خارجی و مجموعه مقالات موجود و گزارشات و نتایج مطالعات طرحها و پروژه ها و سوابق تحقیقات صورت گرفته مورد بازبینی قرار خواهد گرفت. همچنین با استفاده از شبکه اینترنت و مراجعه به سایتهای مرتبط مطالب مورد نظر استخراج و استفاده

خواهد شد. جهت تجزیه تحلیل اطلاعات از تکنیک تحلیل محتوا و فرایند تحلیل سلسله مراتبی استفاده شده است.

۳. تجزیه و تحلیل داده ها

ازآنجاکه هدف این پژوهش کاربردهای هوش مصنوعی در تحول استراتژی های نظامی و امنیتی است، تجزیه‌وتحلیل یافته های این فصل بصورت تجزیه و تحلیل یافته های کیفی انجام می‌شود. در واقع متغیرهای مورد نیاز مدل پژوهش از مصاحبه ها استخراج شده و روابط بین آنها تعیین می‌گردد. در راستای تحلیل داده‌ها، ابتدا روایی پژوهش مطابق روش لینکلن و گوبا (۱۹۸۰) و پایایی پژوهش براساس روش توافق درونی بررسی شده، سپس آمار توصیفی مصاحبه شوندگان ارائه گردیده و سپس به تحلیل داده‌ها، جهت استخراج کدها و مقوله‌ها و روابط بین آنها در نرم افزار مکس کیودا پرداخته شده است. در پژوهش حاضر جهت بررسی روایی پژوهش از روش لینکلن و گوبا (۱۹۸۰) که بر اساس چهار عنصر قابلیت انتقال، قابلیت اعتبار، قابلیت اعتماد و قابلیت تایید شکل گرفته و روایی ابزار را تایید نمود، استفاده گردید.

جدول (۱) روایی پژوهش طبق روش لینکلن و گوبا (۱۹۸۰)

شاخص	فرایند
قابلیت انتقال[1]	نظرسنجی از خبرگانی که در تحقیق حاضر شرکت نداشتند.
قابلیت اعتبار[2]	صرف زمان کافی برای پژوهش و تایید داده‌های مصاحبه توسط مصاحبه شوندگان.
قابلیت تایید[3]	مستندسازی و رعایت همه گامهای طی شده در پژوهش و مستندات در فرایندهای پژوهش.
قابلیت اعتماد[4]	ثبت تمام جزئیات و یادداشت همه موارد در مرحله مصاحبه و انجام آن.

جهت ارزیابی پایایی پژوهش از دو نفر که خارج از موضوع پژوهش بودند، پس از توضیحات و آموزشهای لازم درخواست شد که ۵ مورد از مصاحبه‌ها را کدگذاری نمایند تا بتوان میزان پایایی را اندازه گیری و مقایسه نمود.

[1] Transferability
[2] Credibility
[3] Confirmation
[4] Reliability

جدول (۲) پایایی پژوهش با روش میزان اتفاق درونی

مصاحبه	تعداد کد استخراج شده از مصاحبه	تعداد توافقات	درصد اتفاق نظر یا پایایی آزمون
مصاحبه ۱	۴۳	۳۷	۸۶.۰۵٪
مصاحبه ۴	۵۱	۴۲	۸۲.۴٪
مصاحبه ۵	۳۷	۳۰	۸۱.۱٪
مصاحبه ۹	۳۴	۲۵	۷۳.۵۳٪
مصاحبه ۱۱	۲۸	۲۳	۸۲.۱٪

همانطور که در جدول بالا مشاهده می‌شود، میزان توافق درونی برای ۵ مصاحبه بالاتر از ۷۰ درصد می‌باشد که نشان دهنده پایایی قابل قبول برای مصاحبه‌های انجام شده و کدهای استخراجی توسط محقق می‌باشد. به منظور استخراج متغیرهای مورد نیاز مدل پژوهش در حل مسائل حوزه کاری خبرگان، روش‌های متعددی به کار گرفته می‌شود. این روش ها می توانند به طرق گوناگون دسته بندی شوند. یک طریقه رایج، دسته بندی این روش ها بر اساس نحوه دریافت دانش از خبره است. بر این اساس دو دسته ی استخراج مستقیم و استخراج غیرمستقیم دانش مطرح می گردد. روش های مستقیم، به طور مستقیم به درخواست توضیح از خبره در رابطه با چگونگی انجام کار می پردازند. شرط لازم برای اینکه این روش ها به موفقیت دست یابند این است که خبره به اندازه کافی توانایی و رضایت برای به اشتراک گذاری دانش خود داشته باشد. در این روش اطلاعات به سهولت توسط خبره بیان می شوند، البته به غیر از مواردی که خبره به قدری فعالیت مورد نظر را تکرار کرده است که اطلاعات راجع به آن برای خبره بدیهی به نظر می رسند. روش‌های غیرمستقیم به منظور دست یابی به اطلاعاتی به کار گرفته می شوند که به راحتی توسط خبره قابل بیان نیستند. البته دسته بندی روش ها علاوه بر نحوه تعامل با خبره، بر اساس نوع اطلاعاتی که به دست می دهند نیز صورت می گیرد، که در این بخش به آنها اشاره خواهد شد. در این پژوهش از روش مستقیم استفاده شده است و پس از انجام مصاحبه برای درک و استخراج متغیرهای مورد نیاز پژوهش این مفاهیم ابتدا کدگذاری باز، سپس مقوله بندی شده و در نهایت کدگذاری محوری جهت استخراج الگوی پژوهش انجام شده است. با بررسی داده‌های مصاحبه، استخراج سایر

مفاهیم نیز به همین ترتیب صورت گرفته است. این فرایند در جدول زیر به طور کامل نشان داده شده است.

جدول (۴) فرایند کدگذاری باز مصاحبه با خبرگان

کد	کاربرد
A1	تحلیل کلان‌داده‌های اطلاعاتی
A2	پیش‌بینی تهدیدات امنیتی
A3	تشخیص الگوهای رفتاری دشمن
A4	تحلیل شبکه‌های تروریستی
A5	پایش هوشمند مرزها
A6	تشخیص نفوذ سایبری
A7	دفاع خودکار در برابر حملات سایبری
A8	تحلیل بدافزارها
A9	پشتیبانی تصمیم‌گیری فرماندهان
A10	شبیه‌سازی سناریوهای امنیتی
A11	بهینه‌سازی تخصیص منابع دفاعی
A12	تحلیل ریسک راهبردی
A13	پردازش تصویر ماهواره‌ای
A14	تشخیص اشیای تهدیدآمیز
A15	پایش هوشمند پهپادی
A16	تحلیل ویدئویی بلادرنگ
A17	لجستیک هوشمند نظامی
A18	پیش‌بینی خرابی تجهیزات
A19	مدیریت زنجیره تأمین دفاعی
A20	نگهداری پیش‌بینانه
A21	آموزش تطبیقی نیروها
A22	شبیه‌سازهای آموزشی هوشمند
A23	تحلیل عملکرد رزمی
A24	بهینه‌سازی دکترین آموزشی
A25	عملیات روانی مبتنی بر داده
A26	تحلیل افکار عمومی و رسانه

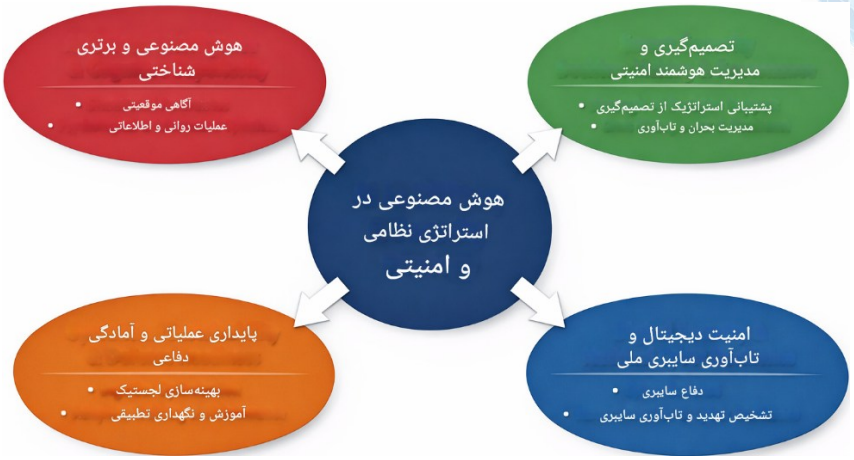
A27	تشخیص اخبار جعلی
A28	جنگ شناختی دیجیتال
A29	مدیریت بحران هوشمند
A30	پیش‌بینی پیامدهای امنیتی
A31	پشتیبانی تصمیم‌گیری کلان
A32	ارزیابی تاب‌آوری ملی

جدول (۵) مرحله دوم: تلفیق کاربرد اصلی

کد کاربرد اصلی	عنوان کاربرد اصلی	کدهای تلفیق‌شده
B1	هوشمندی اطلاعاتی و تحلیل تهدید	A1, A2, A3, A4
B2	امنیت و دفاع سایبری هوشمند	A6, A7, A8
B3	پایش و شناسایی هوشمند محیطی	A5, A13, A14, A15, A16
B4	تصمیم‌گیری راهبردی مبتنی بر AI	A9, A10, A12, A31
B5	بهینه‌سازی منابع و لجستیک دفاعی	A11, A17, A19
B6	نگهداری و پایداری تجهیزات	A18, A20
B7	آموزش و توانمندسازی تطبیقی	A21, A22, A23, A24
B8	مدیریت عملیات شناختی و روانی	A25, A26, A28
B9	مقابله با جنگ اطلاعاتی	A27
B10	مدیریت بحران و پاسخ هوشمند	A29, A30
B11	تحلیل تاب‌آوری و امنیت ملی	A32
B12	پشتیبانی کلان‌راهبردی امنیتی	A12, A31

جدول (۶) مرحله سوم: سطح کلان راهبردی

کد	کاربرد نهایی	کدهای کاربردهای اصلی
C1	برتری اطلاعاتی و شناختی مبتنی بر هوش مصنوعی	B1, B3, B8, B9
C2	تصمیم‌گیری و حکمرانی امنیتی هوشمند	B4, B10, B11, B12
C3	پایداری عملیاتی و آمادگی دفاعی هوشمند	B5, B6, B7
C4	امنیت دیجیتال و تاب‌آوری سایبری ملی	B2



نمودار (۲) شبکه مفاهیم ومضمون های نهایی

تحقق کفایت نظری

فرایند جمع آوری داده ها تا جایی ادامه پیدا می کند که محقق در داده ها به مرز اشباع برسد و مفاهیم مرتبط با پدیده مورد نظر که توسط مصاحبه شوندگان مختلف مطرح می شوند تکراری شده و مطلب جدیدی به مدل اضافه نشود. جدول زیر چگونگی تحقق این معیار در پژوهش حاضر را نشان می دهد:

جدول (۶) چگونگی تحقق کفایت نظری

مصاحبه	فراوانی کدهای باز	تعداد مفاهیم	تکمیل مفاهیم قبلی	ظهور مقولات جدید	تکمیل مقولات قبلی
برتری اطلاعاتی و شناختی مبتنی بر هوش مصنوعی	۸۳	۴۵	-	۱۱	
تصمیم‌گیری و حکمرانی امنیتی هوشمند	۶۲	۶۱	۱۶	۳	۲
پایداری عملیاتی و آمادگی دفاعی هوشمند	۶۹	۶۷	۶		۱
امنیت دیجیتال و تاب‌آوری سایبری ملی	۴۸	۶۹	۲		

در ادامه جهت رتبه بندی از تکنیک فرایند تحلیل سلسله مراتبی فازی استفاده شده که نتایج آن در ادامه آورده شده است: پس از آنکه جدول مقایسات زوجی با اعداد مثلثی فازی تشکیل شد، با استفاده از روش EA، نسبت بزرگی شاخصها نسبت به هم محاسبه شده و بر اساس آن نیز وزن غیر بهنجار(w′)هر

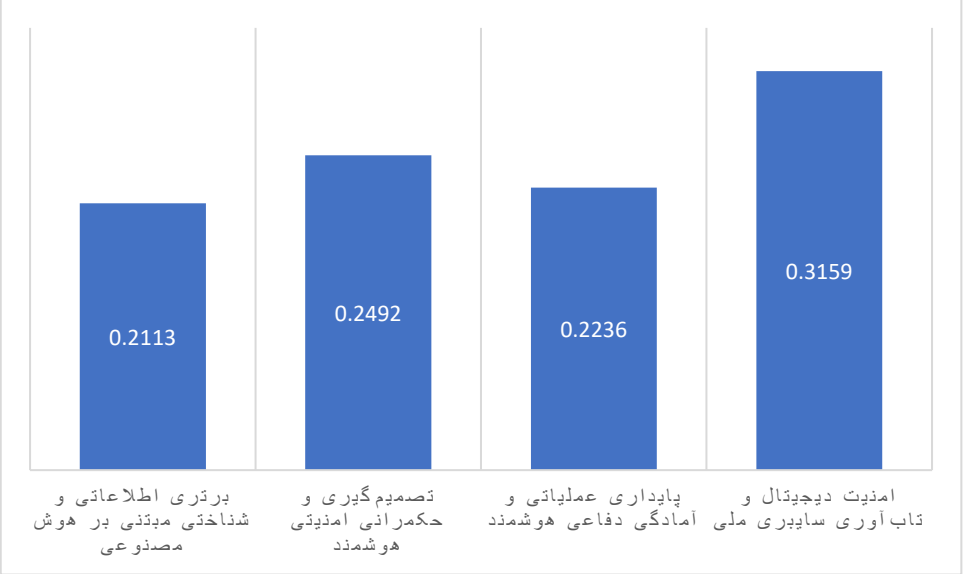
شاخص بدست آمده است. اوزان غیر بهنجار، هنجار شده و اوزان بهنجار (W) حاصل شده است. نحوه انجام محاسبات در زیر آمده است :

جدول (۷) ماتریس تصمیم فازی

							L	M	U
S1	17.000	25.000	33.000	0.007	0.008	0.012	0.118	0.212	0.393
S2	21.000	29.000	37.000	0.007	0.008	0.012	0.146	0.246	0.440
S3	19.000	27.000	33.000	0.007	0.008	0.012	0.132	0.229	0.393
S4	27.000	37.000	41.000	0.007	0.008	0.012	0.188	0.314	0.488

جدول (۸) نتایج اوزان شاخص

	w1	w2	w3	w4
w	0.2113	0.2492	0.2236	0.3159



نمودار (۳) اولویت بندی متغیرهای شاخص های منتخب

جدول (۹) اولویت بندی متغیرهای اصلی

ردیف	معیار	وزن	اولویت
۱	برتری اطلاعاتی و شناختی مبتنی بر هوش مصنوعی	0.2113	۴
۲	تصمیم‌گیری و حکمرانی امنیتی هوشمند	0.2492	۲

۳	پایداری عملیاتی و آمادگی دفاعی هوشمند	0.2236	۳
۴	امنیت دیجیتال و تاب‌آوری سایبری ملی	0.3159	۱

با توجه به جدول (۹) ملاحظه می گردد با توجه به وزن اصلی بدست آمده بترتیب شاخص های امنیت دیجیتال و تاب‌آوری سایبری ملی، تصمیم‌گیری و حکمرانی امنیتی هوشمند، پایداری عملیاتی و آمادگی دفاعی هوشمند و برتری اطلاعاتی و شناختی مبتنی بر هوش مصنوعی از بیشترین و کمترین اهمیت در گروه برخوردار هستند.

تحلیل یافته‌های این پژوهش نشان می‌دهد که هوش مصنوعی دیگر صرفاً یک فناوری پشتیبان در حوزه دفاعی محسوب نمی‌شود، بلکه به یکی از عوامل بنیادین در بازتعریف استراتژی‌های دفاعی و راهبردی تبدیل شده است. فرآیند تحلیل داده‌های حاصل از مصاحبه با خبرگان نشان داد که کاربردهای شناسایی‌شده در ابتدا به‌صورت مجموعه‌ای از فعالیت‌های پراکنده و تخصصی ظاهر می‌شوند، اما با تلفیق مفهومی، قابلیت‌های کلان‌تری را شکل می‌دهند که بر ابعاد مختلف قدرت دفاعی و امنیت ملی اثرگذار هستند. این موضوع بیانگر آن است که ارزش راهبردی هوش مصنوعی نه در تعداد کاربردهای آن، بلکه در میزان هم‌افزایی میان این کاربردها و تبدیل آن‌ها به قابلیت‌های یکپارچه نهفته است.

یکی از مهم‌ترین یافته‌های پژوهش، شکل‌گیری مفهوم برتری اطلاعاتی و شناختی به‌عنوان نخستین بعد راهبردی بود. این یافته نشان می‌دهد که هوش مصنوعی با افزایش سرعت جمع‌آوری، پردازش و تحلیل حجم عظیمی از داده‌های چندمنظوره، امکان دستیابی به آگاهی موقعیتی دقیق‌تر، پیش‌بینی تهدیدها و تحلیل رفتار بازیگران را فراهم می‌کند. در محیط امنیتی امروز که سرعت تغییرات بسیار بالا است، برخورداری از چنین قابلیتی می‌تواند فاصله زمانی میان شناسایی تهدید و واکنش مؤثر را به میزان قابل توجهی کاهش دهد و برتری تصمیم‌گیری را برای سازمان‌های دفاعی ایجاد کند.

دومین یافته اساسی پژوهش، نقش هوش مصنوعی در تصمیم‌گیری و حکمرانی هوشمند است. تحلیل مصاحبه‌ها نشان داد که هوش مصنوعی تنها ابزار ارائه پیشنهاد به فرماندهان نیست، بلکه می‌تواند با تحلیل هم‌زمان داده‌های اطلاعاتی، عملیاتی، اقتصادی و سایبری، کیفیت تصمیمات راهبردی را ارتقا داده و از خطاهای ناشی از محدودیت‌های شناختی انسان بکاهد. در نتیجه، تحول در فرآیندهای تصمیم‌گیری دفاعی بیش از آنکه ناشی از جایگزینی انسان باشد، حاصل همکاری میان انسان و سامانه‌های هوشمند است؛ همکاری‌ای که سرعت، دقت و قابلیت پیش‌بینی را افزایش می‌دهد. یافته دیگر پژوهش، اهمیت

پایداری عملیاتی و آمادگی دفاعی است. نتایج نشان می‌دهد که هوش مصنوعی با بهینه‌سازی مدیریت منابع، پیش‌بینی خرابی تجهیزات، بهبود زنجیره تأمین نظامی، مدیریت عملیات و افزایش انعطاف‌پذیری سازمان‌های دفاعی، نقش مهمی در حفظ آمادگی مستمر نیروهای مسلح ایفا می‌کند. این یافته بیانگر آن است که هوش مصنوعی تنها در میدان نبرد کاربرد ندارد، بلکه در تمامی مراحل برنامه‌ریزی، آموزش، پشتیبانی، نگهداری تجهیزات و مدیریت بحران نیز می‌تواند موجب افزایش کارایی و کاهش هزینه‌های عملیاتی شود.

چهارمین یافته پژوهش به امنیت دیجیتال و تاب‌آوری سایبری مربوط می‌شود. تحلیل داده‌ها نشان داد که گسترش وابستگی سامانه‌های دفاعی به زیرساخت‌های دیجیتال، همزمان سطح آسیب‌پذیری آن‌ها را نیز افزایش داده است. در چنین شرایطی، هوش مصنوعی با قابلیت شناسایی سریع تهدیدات، کشف رفتارهای غیرعادی، پاسخ خودکار به حملات سایبری و پیش‌بینی آسیب‌پذیری‌ها، به یکی از ارکان اصلی دفاع سایبری تبدیل شده است. این یافته نشان می‌دهد که آینده امنیت ملی بیش از گذشته به توانایی کشورها در مدیریت هوشمند فضای سایبری وابسته خواهد بود. در ارتباط با مسئله اصلی پژوهش، یافته‌ها نشان می‌دهد که تحول استراتژی‌های دفاعی صرفاً حاصل ورود فناوری‌های جدید نیست، بلکه نتیجه تعامل میان فناوری، ساختارهای سازمانی، حکمرانی، سرمایه انسانی و مدیریت دانش است. بنابراین، استفاده موفق از هوش مصنوعی مستلزم ایجاد زیرساخت‌های داده، توسعه نیروی انسانی متخصص، تدوین مقررات حقوقی و اخلاقی، ارتقای امنیت اطلاعات و بازنگری در دکترین‌های دفاعی است. در غیر این صورت، حتی پیشرفته‌ترین سامانه‌های هوش مصنوعی نیز نمی‌توانند به مزیت راهبردی پایدار تبدیل شوند.

از منظر نظری، یافته‌های این پژوهش شکاف موجود در ادبیات را تا حد زیادی برطرف می‌کند. برخلاف بسیاری از مطالعات پیشین که هر یک تنها به بخشی از کاربردهای هوش مصنوعی پرداخته‌اند، این پژوهش با استفاده از یک فرآیند سه‌مرحله‌ای شامل شناسایی کاربردهای اولیه، تلفیق آن‌ها در قالب قابلیت‌های کلیدی و استخراج ابعاد راهبردی، چارچوبی منسجم برای تبیین نقش هوش مصنوعی در تحول استراتژی‌های دفاعی ارائه می‌دهد. این چارچوب نشان می‌دهد که کاربردهای عملیاتی، قابلیت‌های سازمانی و پیامدهای راهبردی در یک زنجیره منطقی به یکدیگر متصل هستند و تنها در صورت تعامل میان این سطوح است که هوش مصنوعی می‌تواند موجب تحول واقعی در نظام دفاعی شود. در مجموع، تجزیه و تحلیل یافته‌ها نشان می‌دهد که پاسخ مسئله اصلی پژوهش مثبت است؛ بدین معنا که هوش

مصنوعی از طریق ایجاد برتری اطلاعاتی و شناختی، ارتقای تصمیم‌گیری و حکمرانی هوشمند، افزایش پایداری عملیاتی و تقویت امنیت دیجیتال و تاب‌آوری سایبری، قادر است تحول بنیادینی در استراتژی‌های دفاعی و راهبردی ایجاد کند. با این حال، تحقق این ظرفیت مستلزم اتخاذ رویکردی یکپارچه، فرابخشی و بلندمدت است که در آن توسعه فناوری، حکمرانی داده، الزامات حقوقی و اخلاقی و توانمندسازی منابع انسانی به‌صورت هم‌زمان مورد توجه قرار گیرند. این نتیجه نشان می‌دهد که آینده برتری دفاعی کشورها بیش از آنکه به حجم تجهیزات نظامی وابسته باشد، به توانایی آن‌ها در بهره‌گیری هوشمندانه، یکپارچه و راهبردی از ظرفیت‌های هوش مصنوعی بستگی خواهد داشت.

نتیجه گیری

پژوهش حاضر با هدف تبیین نقش و جایگاه هوش مصنوعی در تحول استراتژی‌های نظامی و امنیتی، تلاشی نظام‌مند برای عبور از نگاه‌های پراکنده، موردی و فناورمحور به سوی یک چارچوب یکپارچه، چندسطحی و راهبردی انجام داده است. برخلاف بسیاری از مطالعات پیشین که صرفاً به معرفی مصادیق فنی یا بررسی پیامدهای کوتاه‌مدت فناوری‌های هوش مصنوعی در حوزه دفاعی بسنده کرده‌اند، این مقاله با بهره‌گیری از رویکرد کدگذاری مفهومی و تلفیق تدریجی کاربردها، نشان می‌دهد که هوش مصنوعی نه یک ابزار منفرد، بلکه یک «توانمندساز تحول‌آفرین» در بازتعریف منطق امنیت، تصمیم‌گیری و حکمرانی دفاعی در سطوح مختلف است. از این منظر، نتایج پژوهش حاضر بر این نکته تأکید دارد که ارزش واقعی هوش مصنوعی در حوزه نظامی–امنیتی، نه در سطح کاربردهای منفرد، بلکه در هم‌افزایی راهبردی میان قابلیت‌های اطلاعاتی، شناختی، عملیاتی و نهادی آن نهفته است.

در سطح نخست تحلیل، شناسایی و کدگذاری ۳۲ کاربرد مجزای هوش مصنوعی، تصویری جامع از گستره نفوذ این فناوری در ابعاد مختلف نظامی و امنیتی ارائه می‌دهد. این کاربردها از تحلیل کلان‌داده‌های اطلاعاتی و پیش‌بینی تهدیدات گرفته تا مدیریت بحران، جنگ شناختی، لجستیک هوشمند و آموزش تطبیقی نیروها را دربرمی‌گیرد. تنوع و پراکندگی این کاربردها نشان می‌دهد که هوش مصنوعی به‌طور هم‌زمان در سطوح تاکتیکی، عملیاتی و راهبردی ایفای نقش می‌کند و مرزهای سنتی میان این سطوح را تا حد زیادی درهم می‌شکند. یکی از یافته‌های کلیدی این مرحله آن است که بسیاری از این کاربردها به‌صورت منفرد معنا و اثرگذاری محدودی دارند و تنها در چارچوب شبکه‌ای از قابلیت‌های مکمل می‌توانند به تحول واقعی در استراتژی‌های امنیتی منجر شوند.

در گام دوم، تلفیق ۳۲ کاربرد اولیه در قالب ۱۲ کاربرد اصلی، امکان عبور از سطح «کاربردمحوری» به سطح «قابلیت‌محوری» را فراهم می‌سازد. این سطح از تحلیل نشان می‌دهد که هوش مصنوعی چگونه می‌تواند قابلیت‌هایی نظیر هوشمندی اطلاعاتی، تصمیم‌گیری راهبردی، پایداری عملیاتی، امنیت سایبری، عملیات شناختی و تاب‌آوری ملی را به‌طور ساختاری تقویت کند. یافته‌های این بخش حاکی از آن است که تحول واقعی در استراتژی‌های نظامی و امنیتی زمانی رخ می‌دهد که سازمان‌های دفاعی بتوانند این قابلیت‌های دوازده‌گانه را به‌صورت هم‌راستا با اهداف کلان امنیت ملی توسعه دهند. به بیان دیگر، هوش مصنوعی زمانی به مزیت راهبردی تبدیل می‌شود که از سطح ابزارهای مجزا فراتر رفته و در معماری تصمیم‌گیری و حکمرانی امنیتی نهادینه شود.

در مرحله نهایی تحلیل، تلفیق ۱۲ کاربرد اصلی در قالب ۴ کاربرد نهایی کلان، تصویری روشن از مسیر تحول دکترین‌های امنیتی در عصر هوش مصنوعی ترسیم می‌کند. این چهار کاربرد نهایی—شامل برتری اطلاعاتی و شناختی، تصمیم‌گیری و حکمرانی امنیتی هوشمند، پایداری عملیاتی و آمادگی دفاعی، و امنیت دیجیتال و تاب‌آوری سایبری—نشان می‌دهند که هوش مصنوعی در نهایت منجر به شکل‌گیری یک الگوی جدید از قدرت امنیتی می‌شود که ماهیتی شبکه‌ای، داده‌محور، پیش‌نگر و تطبیقی دارد. در این الگو، برتری نظامی دیگر صرفاً تابع توان سخت‌افزاری یا برتری عددی نیست، بلکه به توانایی در تولید، تحلیل و به‌کارگیری هوشمندانه اطلاعات و دانش در زمان مناسب وابسته است.

یکی از مهم‌ترین نتایج نظری این پژوهش، تأکید بر گذار از «امنیت واکنشی» به «امنیت پیش‌نگر» در پرتو هوش مصنوعی است. یافته‌ها نشان می‌دهند که با تلفیق قابلیت‌های پیش‌بینی، شبیه‌سازی و تحلیل بلادرنگ، امکان شناسایی تهدیدات پیش از تحقق عینی آن‌ها به‌طور قابل‌توجهی افزایش می‌یابد. این تحول، پیامدهای عمیقی برای استراتژی‌های بازدارندگی، مدیریت بحران و تخصیص منابع دفاعی دارد و می‌تواند منجر به کاهش هزینه‌های انسانی، اقتصادی و سیاسی در مواجهه با تهدیدات پیچیده و چندبعدی شود. از این منظر، هوش مصنوعی نه‌تنها کارایی عملیاتی را افزایش می‌دهد، بلکه منطق تصمیم‌گیری امنیتی را نیز دگرگون می‌سازد.

در بعد شناختی و اطلاعاتی، نتایج پژوهش نشان می‌دهد که هوش مصنوعی نقش محوری در شکل‌دهی به «میدان نبرد شناختی» ایفا می‌کند. تلفیق کاربردهای مرتبط با تحلیل افکار عمومی، تشخیص اخبار جعلی و عملیات شناختی، بیانگر آن است که آینده امنیت ملی بیش از هر زمان دیگری به مدیریت ادراک، معنا و روایت وابسته خواهد بود. در این چارچوب، برتری اطلاعاتی صرفاً به دسترسی به داده

محدود نمی‌شود، بلکه به توانایی تفسیر، اولویت‌بندی و تبدیل داده به دانش راهبردی بستگی دارد. این یافته، ضرورت بازنگری در دکترین‌های سنتی امنیتی و توجه جدی به ابعاد نرم، شناختی و اجتماعی امنیت را برجسته می‌سازد.

در حوزه حکمرانی امنیتی، پژوهش حاضر نشان می‌دهد که هوش مصنوعی می‌تواند به‌عنوان یک زیرساخت تصمیم‌سازی کلان عمل کند، به‌گونه‌ای که انسجام میان سطوح مختلف تصمیم‌گیری—از تاکتیکی تا ملی—افزایش یابد. با این حال، نتایج همچنین بر این نکته تأکید دارند که تحقق چنین ظرفیتی مستلزم وجود چارچوب‌های نهادی، حقوقی و اخلاقی مناسب است. بدون حکمرانی هوشمندانه، استفاده گسترده از هوش مصنوعی در حوزه نظامی و امنیتی می‌تواند به چالش‌هایی نظیر تمرکز بیش از حد قدرت تصمیم‌گیری، کاهش شفافیت و افزایش ریسک خطاهای سیستمی منجر شود. بنابراین، یکی از پیامدهای کلیدی این پژوهش، ضرورت هم‌زمانی توسعه فناورانه با توسعه نهادی و سیاستی است.

از منظر عملی و سیاست‌گذاری، یافته‌های مقاله نشان می‌دهد که کشورها برای بهره‌برداری مؤثر از هوش مصنوعی در حوزه امنیتی، باید رویکردی مرحله‌ای و سیستماتیک اتخاذ کنند. تمرکز صرف بر خرید یا توسعه فناوری‌های پیشرفته بدون توجه به تلفیق آن‌ها در معماری کلان امنیت ملی، نه‌تنها مزیت راهبردی ایجاد نمی‌کند، بلکه می‌تواند منجر به اتلاف منابع و افزایش آسیب‌پذیری شود. در مقابل، رویکرد مبتنی بر قابلیت‌های تلفیقی—همان‌گونه که در مدل چهارسطحی این پژوهش ارائه شده—می‌تواند به‌عنوان نقشه راهی برای تحول تدریجی و پایدار استراتژی‌های نظامی و امنیتی مورد استفاده قرار گیرد. در نهایت، این پژوهش با ارائه یک چارچوب مفهومی جامع و چندسطحی، زمینه را برای تحقیقات آتی فراهم می‌سازد. پژوهش‌های آینده می‌توانند با بهره‌گیری از روش‌های کمی، مدل‌سازی ساختاری یا مطالعات تطبیقی بین‌کشوری، به آزمون تجربی روابط میان کاربردهای شناسایی‌شده بپردازند و اعتبار مدل پیشنهادی را در بسترهای مختلف ژئوپلیتیکی بررسی کنند. همچنین، بررسی پیامدهای اخلاقی، حقوقی و اجتماعی به‌کارگیری هوش مصنوعی در حوزه نظامی و امنیتی می‌تواند به غنای نظری و عملی این حوزه بیفزاید. به‌طور کلی، نتایج این مقاله نشان می‌دهد که هوش مصنوعی نه‌تنها آینده جنگ و امنیت، بلکه آینده تفکر راهبردی در حوزه دفاع و امنیت ملی را نیز به‌طور بنیادین بازتعریف می‌کند.

محدودیت‌های تحقیق

با وجود تلاش برای طراحی و اجرای یک چارچوب منسجم و روشمند، پژوهش حاضر همانند سایر مطالعات کیفی مبتنی بر مصاحبه، با مجموعه‌ای از محدودیت‌های اجتناب‌ناپذیر مواجه بوده است.

نخست، ماهیت کیفی تحقیق و اتکای آن به مصاحبه‌های عمیق با خبرگان سبب می‌شود که یافته‌ها بیش از آنکه قابلیت تعمیم آماری داشته باشند، واجد تعمیم‌پذیری تحلیلی و مفهومی باشند؛ به این معنا که نتایج پژوهش بیشتر در قالب الگوها، مفاهیم و روابط نظری قابل استفاده‌اند تا پیش‌بینی‌های کمّی دقیق. دوم، محدودیت دسترسی به خبرگان دارای تجربه مستقیم و عمیق در حوزه‌های هم‌پوشان هوش مصنوعی، امنیت و استراتژی نظامی، دامنه تنوع دیدگاه‌ها را تا حدی محدود کرده است؛ به‌ویژه آنکه در حوزه‌های امنیتی، ملاحظات محرمانگی و حساسیت اطلاعاتی می‌تواند بر میزان شفافیت پاسخ‌ها و عمق برخی اظهارنظرها اثرگذار باشد. سوم، نتایج مصاحبه‌ها به‌طور طبیعی تحت تأثیر برداشت‌های ذهنی، تجربیات حرفه‌ای و چارچوب‌های فکری مصاحبه‌شوندگان قرار دارد و اگرچه با استفاده از تکنیک‌های کدگذاری نظام‌مند و بازبینی مکرر داده‌ها تلاش شده است این سوگیری‌ها کنترل شود، اما حذف کامل آن‌ها امکان‌پذیر نیست. افزون بر این، پویایی بالای فناوری‌های هوش مصنوعی و تغییر سریع محیط‌های امنیتی موجب می‌شود که برخی از یافته‌ها در بازه‌های زمانی میان‌مدت نیازمند بازنگری و به‌روزرسانی باشند. در نهایت، تمرکز پژوهش بر سطح راهبردی و مفهومی، اگرچه مزیت نظری محسوب می‌شود، اما موجب شده است که بررسی‌های جزئی‌تر در سطح فنی یا عملیاتی خارج از دامنه تحقیق قرار گیرد که این امر خود به‌عنوان یکی دیگر از محدودیت‌های مطالعه قابل ذکر است.

پیشنهادات کاربردی برگرفته از نتایج تحقیق

بر اساس یافته‌های این پژوهش، مجموعه‌ای از پیشنهادات کاربردی در سطح سیاست‌گذاری، سازمانی و راهبردی قابل ارائه است. نخست، پیشنهاد می‌شود نهادهای نظامی و امنیتی به‌جای تمرکز پراکنده بر پروژه‌های منفرد هوش مصنوعی، رویکردی مبتنی بر توسعه قابلیت‌های تلفیقی اتخاذ کنند و سرمایه‌گذاری‌ها را در راستای ایجاد هم‌افزایی میان حوزه‌های اطلاعاتی، شناختی، سایبری و تصمیم‌گیری کلان هدایت نمایند. دوم، نتایج تحقیق نشان می‌دهد که استقرار موفق هوش مصنوعی در حوزه امنیتی مستلزم ایجاد ساختارهای حکمرانی داده، چارچوب‌های اخلاقی و سازوکارهای نظارتی شفاف است؛ ازاین‌رو پیشنهاد می‌شود سیاست‌گذاران هم‌زمان با توسعه فناوری، به تدوین مقررات و استانداردهای نهادی متناسب با مخاطرات و پیچیدگی‌های این حوزه بپردازند. سوم، با توجه به نقش کلیدی هوش مصنوعی در تصمیم‌سازی راهبردی، توصیه می‌شود آموزش و توانمندسازی مدیران و فرماندهان در زمینه سواد داده، تحلیل الگوریتمی و درک محدودیت‌های سیستم‌های هوشمند به‌عنوان یک اولویت راهبردی دنبال شود. همچنین، نتایج پژوهش بر اهمیت تقویت زیرساخت‌های بومی داده و کاهش

وابستگی به منابع خارجی در حوزه‌های حساس امنیتی تأکید دارد؛ امری که می‌تواند تاب‌آوری ملی و استقلال راهبردی را افزایش دهد. در نهایت، پیشنهاد می‌شود از مدل مفهومی ارائه‌شده در این تحقیق به‌عنوان یک نقشه راه تحلیلی برای ارزیابی وضعیت موجود و طراحی برنامه‌های تحول دیجیتال در سازمان‌های امنیتی و دفاعی استفاده شود.

سهم دانش‌افزایی پژوهش

پژوهش حاضر از منظر دانش‌افزایی، چندین سهم نظری و مفهومی قابل‌توجه را به ادبیات مطالعات امنیتی و هوش مصنوعی اضافه می‌کند. نخست، این تحقیق با عبور از رویکردهای توصیفی و موردی، یک چارچوب مفهومی چندسطحی و کدگذاری‌شده ارائه می‌دهد که امکان تحلیل نظام‌مند نقش هوش مصنوعی در تحول استراتژی‌های نظامی و امنیتی را فراهم می‌سازد. این چارچوب با تلفیق تدریجی کاربردهای خرد در قالب قابلیت‌های کلان، شکاف موجود میان سطح عملیاتی فناوری و سطح راهبردی تصمیم‌گیری را پر می‌کند. دوم، پژوهش حاضر با تأکید بر ابعاد شناختی، حکمرانی و تاب‌آوری، نگاه غالب فناورمحور در ادبیات موجود را به چالش کشیده و نشان می‌دهد که هوش مصنوعی بیش از آنکه یک ابزار تکنیکی باشد، یک پدیده تحول‌آفرین نهادی و معرفتی است. سوم، استفاده از روش تحقیق کیفی مبتنی بر مصاحبه‌های خبرگانی در این حوزه، به غنای ادبیات کمک کرده و بینش‌هایی عمیق و زمینه‌مند ارائه می‌دهد که کمتر در مطالعات کمّی قابل دستیابی است. در نهایت، مدل ارائه‌شده در این پژوهش می‌تواند به‌عنوان مبنایی برای مطالعات آتی، توسعه مدل‌های کمّی، آزمون‌های تجربی و پژوهش‌های تطبیقی در سطوح ملی و بین‌المللی مورد استفاده قرار گیرد و بدین‌ترتیب به توسعه نظریه‌پردازی در حوزه امنیت و هوش مصنوعی کمک کند.

References

Abbas, T., Ali, W., Khan, I., & Saleem, S. (2024). Revolutionizing warfare: The role of artificial intelligence in the future of defense. The Regional Tribune, 3, 192-200. https://doi.org/10.63062/trt/V24.032

Akrami, T. (2024). Investigating the role of technology in the military competition of great powers. Strategic Report of the Research Center of the Islamic Consultative Assembly, Political Studies Office.
Allahvysian, J., Farhang, S., Razavi, S.R. & Rabii Far, K. (2024). Investigating the Role of Artificial Intelligence in Developing Command and Control Strategies in Cognitive Warfare. https://civilica.com/doc/2174603(In Persian).
Anderson, P. (2023). Command and control systems in modern warfare. Oxford University Press.
Ansari-Mohiyari, A., Ansari-Mohiyari, A. & Hosseini, Z.S. (2024). The Impact of Artificial Intelligence on Warfare and the Rules of International Law with Emphasis on Nahj al-Balagha. Third International Congress on Nahj al-Balagha as a Path of Salvation (Nahj al-Balagha and Dignified Living). https://civilica.com/doc/2136698(In Persian).
Azimi Zadeh, H., Sepehri, M., Helili, K. & Naqavi, A. (2025). Designing an Intelligent Command and Control Model for the Islamic Republic of Iran's Army Based on Big Data. https://civilica.com/doc/2373137(In Persian).
Babuta, A., Oswald, M., & Janjeva, A. (2020). Artificial intelligence and UK national security: Policy considerations. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/ai_national_security_final_web_version.pdf
Betul Yucer, E. (2023). How US sanctions are fueling China’s ambition for chip self-reliance. TRT World. https://www.trtworld.com/magazine/how-us-sanctions-are-fueling-chinas-ambition-for-chip-self-reliance-18215263
Boulanin, V. (Ed.). (2016). The impact of artificial intelligence on strategic stability and nuclear risk: Volume I. SIPRI. https://www.sipri.org/publications/2016/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i
Bousquet, A. J. (2022). The scientific way of warfare: Order and chaos on the battlefields of modernity. Oxford University Press.
Bradford, A. (2023). The battle for technological supremacy: The US–China tech war. In Digital empires: The global battle to regulate technology. Oxford University Press.
Brandt, J., Kreps, S., Meserole, C., Singh, P., & Sisson, M. W. (2022). Succeeding in the AI competition with China: A strategy for action. The Brookings Institution.
Brown, L., & Taylor, M. (2024). Machine learning applications in defense strategy. Springer.
China Daily. (2024). Global AI competition is a marathon, not a sprint. https://www.chinadaily.com.cn/a/202403/21/WS65fb72d0a31082fc043bdd37.html
Csernatoni, R. (2024). Charting the geopolitics and European governance of artificial intelligence. Carnegie Europe.
Csernatoni, R., Broeders, D., Andersen, L. H., et al. (2025). Myth, power, and agency: Rethinking artificial intelligence, geopolitics, and war. Minds & Machines, 35(1), 37. https://doi.org/10.1007/s11023-025-09741-0
Dehghanian, M., Romina, A., Hafez-Nia, M.R. & Qadri-Hajat, M. (2025). Analysis and Examination of the Impact of Artificial Intelligence on the Strategic Depth of Countries. Security Horizons Quarterly, 18(67), 229-265. (In Persian).

Ding, J. (2022). The U.S.-China AI race: Where do both countries stand? The National Committee on United States-China Relations.
Esmaeili, H. & Meyarabbasi, A. (2024). Examining Cognitive Capabilities and Technologies for Defensive-Security Applications in the Islamic Republic of Iran. Defense Strategy, 22(86).(In Persian).
Faghani, R., & Ghoreshi Mohammadi, F. S. (2025). The use of artificial intelligence in military weapons: From the perspective of humanitarian law principles and Islamic jurisprudence. Interdisciplinary Studies in Society, Law, and Politics, 4(3), 1-9. https://doi.org/10.61838/kman.isslp.4.3.25
Fang, T., & Hwang, T. (2023). The rise of techno-nationalism. Open Technology Institute.
Finn, E., & Sinha, U. (2023). China is using AI to ramp up spying, US says. NewsNation. https://www.newsnationnow.com/world/china/china-ai-spying-fbi/
Franke, U., & Torreblanca, J. I. (2021). Geo-tech politics: Why technology shapes European power. European Council on Foreign Relations.
Frizon, G. (2022). Modern military drones. New technologies in military tactics project. Center for Special Operations Instruction. https://www.researchgate.net/publication/365144498_Modern_Military_Drones
Ghavami-Pour Sarshekeh, M. & Mahmoudi, A. (2024). The Impact of Artificial Intelligence-Based Smart Warfare Strategies on National, Regional and Global Security Studies. https://civilica.com/doc/2275583(In Persian).
Harris, J., Patel, R., & Wong, D. (2024). Intelligence, surveillance, and reconnaissance in the age of AI. Routledge.
Imam, I. (2021). Role of artificial intelligence in defence strategy: Implications for global and national security. Strategic Studies, 41(1), 19-40. https://doi.org/10.53532/ss.041.01.0058
JahanDideh, A. & Mirfakhraei, S.H. (2024). The Application of Artificial Intelligence in the Military Sector; A Case Study: The United States and China. International Studies Quarterly, 21(2), 295-313. doi: 10.22034/isj.2024.397508.2018(In Persian).
Johnson, E., & Miller, S. (2024). Autonomous weapon systems and the future of warfare. Cambridge University Press.
Kaur, N., & Singh, R. (2024). Explainable artificial intelligence: Transparency in military applications.
Khusrawi, M.R., Sabzevari, E.H., Karimi, A. & Roozbehani, Y. (2025). The Use of Artificial Intelligence in Military Simulation and Training. https://civilica.com/doc/2265193(In Persian).
Mahdavi Kiya, M. (2025). Examining the Capabilities of Artificial Intelligence for Defensive-Security Applications of the Islamic Republic of Iran. National Conference on Innovations in Human Sciences and Social Sciences. (In Persian).
Nazari, M. (2024). Artificial Intelligence and Fundamental Transformation in Security-Defense Policy Making. Public Policy Quarterly, 10(3). (In Persian).
PirMohammadi, S., Hedayati Shahidani, M. & Niakoui, S.A. (2024). Techno-Geopolitics and the Changing Global Traditional Patterns in Digital Technologies; A Strategic Perspective for Iran. Foreign Relations Quarterly, 16(4), 89-116. doi: 10.22034/fr.2025.470234.1558(In Persian).

Rostami, M. (2022). Identification and Introduction of Practical Capacities of Artificial Intelligence in the Development of Strategic Themes in Military Organizations. Defense Strategy, 20(78), 34-74. (In Persian).
Ryazi, V. & Biabani, A. (2024). The Pattern of New Technological Threats of the Ground Forces of the Islamic Republic of Iran. Military Management Quarterly, 24(96), 58-77. doi: 10.22034/iamu.2024.2030517.3064(In Persian).
Simbar, R., Shashti, S. & Sedighi-Roudsari, R. (2025). Analysis of the Role of Artificial Intelligence in Defensive Strategy and Its Implications for National and Global Security (Case Studies: China, Russia, and the USA). Political Studies Cognition, (), e231714. doi: 10.20241403/CRPS.2508.1056.4.7.1(In Persian).
Taghipour Javi, H. (2025). The Impact of Artificial Intelligence on the Nature of Future Wars. Defense Strategy Quarterly, 23(2). (In Persian).