Supreme National Defense University Quarterly of Defense Strategy

https://ds.sndu.ac.ir E-ISSN: 2980-8464

Vol. 24, No. 1, Issue. 93, Spring 2026 **Received:** 2025/09/30 **Accepted:** 2026/02/08

Research paper

Examining and Analyzing the Defense and Security Roles of Artificial Intelligence in the 12-Day Imposed War Waged by the United States and the Israeli Regime Against the Islamic Republic of Iran

Mohammadreza Hassani Ahanghar
Professor, Faculty of Artificial Intelligence and Cognitive Sciences, Imam Hossein Comprehensive University, Tehran, Iran
Mohammad Hossein Alipour
Assistant Professor, Imam Hossein Comprehensive University, Tehran, Iran (Corresponding Author).
Email: mhalipor@ihu.ac.ir
Alireza Rahnama
Faculty of Management and Strategic Planning, Imam Hossein Comprehensive University, Tehran, Iran
Ramin Dalir
Researcher, Imam Hossein Comprehensive University, Tehran, Iran

Abstract

The 12-day imposed war waged by the United States and the Israeli regime against the Islamic Republic of Iran in June 2025 represents a significant example of the transformation of hybrid warfare in the age of artificial intelligence. This study aims to analyze the role of artificial intelligence in the defense and security dimensions of this conflict and to elucidate its effects on the intelligence, decision-making, and action cycle. In terms of purpose, the study is applied and policy-oriented; in terms of approach, it is qualitative; and in terms of analytical method, it employs framework analysis. Data were collected through documentary research and field observation and were examined, validated, and supplemented with input from 12 defense and security experts. The analytical framework is based on four dimensions: intelligence, operations, defense, and cyber operations. The findings indicate that, in this war, artificial intelligence functioned not as an isolated tool but as an integrated architecture encompassing data, algorithms, command and control, and operational platforms. Through the compression of the intelligence cycle, rapid targeting—with an 87% success rate in identifying high-value targets—shortening the kill chain to as little as 60 seconds, the intelligent enhancement of air and missile defense, and the reinforcement of cyber operations, artificial intelligence increased the speed and precision of the combat cycle. The study concludes that strategic advantage in future warfare will depend less on possessing any single technology than on the capacity to integrate data, decision-making, and action.

Keywords: Command and Control, Hybrid Warfare, 12-Day War, Autonomous Systems, Artificial Intelligence

فصلنامه راهبرد دفاعی

سال بیست و چهارم، شماره یکم (پیاپی ۹۳)، بهار ۱۴۰۵، صص.۹۵-۱۳۸
تاریخ دریافت: ۱۴۰۴/۰۷/۰۸ ـ تاریخ پذیرش: ۱۴۰۴/۱۱/۱۹

مقاله پژوهشی

بررسی و تحلیل نقش‌های دفاعی-امنیتی هوش مصنوعی در جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران

محمدرضا حسنی آهنگر
استاد دانشکده هوش مصنوعی و علوم شناختی، دانشگاه جامع امام حسین (ع)، تهران، ایران
محمدحسین علیپور
استادیار دانشگاه جامع امام حسین (ع)، تهران، ایران (نویسنده مسئول)
Email: mhalipor@ihu.ac.ir
علیرضا رهنما
دانشکده مدیریت و برنامه‌ریزی راهبردی، دانشگاه جامع امام حسین (ع)، تهران، ایران
رامین دلیر
پژوهشگر دانشگاه جامع امام حسین (ع)، تهران، ایران

چکیده

جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران در ژوئن ۲۰۲۵، یکی از نمونه‌های مهم تحول جنگ ترکیبی در عصر هوش مصنوعی است. هدف این پژوهش، تحلیل نقش‌آفرینی هوش مصنوعی در ابعاد دفاعی-امنیتی این نبرد و تبیین اثر آن بر چرخه اطلاعات، تصمیم و اقدام است. پژوهش از نظر هدف، کاربردی و سیاست‌پژوهانه، از نظر رویکرد، کیفی و از حیث روش تحلیل، مبتنی بر تحلیل چهارچوبی است. داده‌ها با استفاده از مطالعه اسنادی و مشاهده میدانی گردآوری و با بهره‌گیری از نظر ۱۲ خبره دفاعی-امنیتی بررسی، صحت‌سنجی و تکمیل شده‌اند. چهارچوب تحلیلی پژوهش بر چهار محور اطلاعاتی، عملیاتی، دفاعی و سایبری استوار است. یافته‌ها نشان می‌دهد هوش مصنوعی در این جنگ نه در قالب یک ابزار منفرد، بلکه به‌مانند معماری یکپارچه داده، الگوریتم، فرماندهی و کنترل و سکوهای عملیاتی عمل کرده و از طریق فشرده‌سازی مدار اطلاعات، هدف‌یابی سریع و ۸۷ درصدی اهداف ارزشمند، کوتاه‌سازی زنجیره کشتار تا ۶۰ ثانیه، هوشمندسازی پدافند و تقویت عملیات سایبری، سرعت و دقت چرخه نبرد را افزایش داده است. نتیجه پژوهش نشان می‌دهد مزیت راهبردی در جنگ‌های آینده، بیش از آنکه تابع برخورداری از یک فناوری خاص باشد، به توان یکپارچه‌سازی داده، تصمیم و اقدام وابسته است.

کلیدواژه‌ها: فرماندهی و کنترل، جنگ ترکیبی، جنگ ۱۲ روزه، سامانه‌های خودمختار، هوش مصنوعی

صحت مطالب بر عهده نویسنده مقاله است و بیانگر دیدگاه دانشگاه عالی دفاع ملی نیست.

مقدمه

تجاوز و حمله رژیم صهیونیستی به جمهوری اسلامی ایران در ژوئن ۲۰۲۵، صرفاً یک عملیات نظامی محدود نبود؛ بلکه نمونه‌ای برجسته از «جنگ ترکیبی»[1] بود که در آن سطوح مختلف اطلاعاتی، عملیاتی، دفاعی، سایبری و رسانه‌ای درهم‌تنیده شدند. این جنگ ازآن‌جهت اهمیت دارد که در آن، فناوری‌های نوظهور، به‌ویژه «هوش مصنوعی»[2]، در پیوند با شبکه‌های اطلاعاتی، سامانه‌های «فرماندهی و کنترل»[3]، «جنگ سایبری»[4]، «عملیات شناختی»[5] و ابزارهای خودمختار به‌کار گرفته شدند و شکل جدیدی از تعامل میان داده، تصمیم و اقدام را در میدان نبرد پدید آوردند (Jensen, 2025; Shah, 2025). اهمیت این جنگ ازجمله در پیوند عملیات پهپادی، شبکه‌های اطلاعاتی و ابزارهای تحلیل مبتنی بر هوش مصنوعی با عملیات نظامی آشکار می‌شود؛ در گزارش منتشرشده درباره عملیات آغازین ژوئن ۲۰۲۵ نیز به استفاده از پهپادهای خودمختار و قابلیت‌های اطلاعاتی و شناساییِ متکی بر هوش مصنوعی اشاره شده است (Jensen, 2025).

در این رخداد، رژیم صهیونیستی از اصل غافل‌گیری در آغاز حمله بهره گرفت و هم‌زمان تلاش کرد با ترکیب توان اطلاعاتی، شبکه نفوذ، قابلیت‌های فناورانه، پشتیبانی تسلیحاتی و پوشش رسانه‌ای، ضربه نخست را به مؤلفه‌های فرماندهی، کنترل، پدافند، توان موشکی و زیرساخت‌های حساس جمهوری اسلامی ایران وارد کند. با وجود این، جنگ پس از ۱۲ روز به مرحله آتش‌بس رسید و همین امر نشان داد که تحلیل این رخداد نباید صرفاً در سطح توصیف نظامی باقی بماند. اهمیت این تحلیل از آن روست که هیچ تضمینی برای عدم تکرار یا گسترش درگیری‌های مشابه وجود ندارد و آمادگی برای نبردهای آینده نیازمند شناخت دقیق قابلیت‌ها، آسیب‌پذیری‌ها و الگوهای عملیاتی طرف مقابل است (رهبر معظم انقلاب، ۱۴۰۴).

1. Hybrid Warfare
2. Artificial Intelligence (AI)
3. Command and Control (C2)
4. Cyber Warfare
5. Cognitive Operations

از منظر دفاعی–امنیتی، جنگ ۱۲ روزه واجد شگفتی‌سازهای متعددی بود. بخشی از این شگفتی‌ها به ترکیب جنگ سخت با جنگ سایبری، عملیات روانی، شبکه نفوذ انسانی، داده‌کاوی اطلاعاتی، پهپادهای خودمختار، سامانه‌های تصمیم‌یار و پدافند هوشمند مربوط می‌شود (Jensen, 2025; Shah, 2025). بااین‌حال، یکی از مهم‌ترین ابعاد این جنگ، ورود برجسته‌تر هوش مصنوعی به زنجیره اطلاعات، تصمیم و اقدام بود؛ تا جایی که می‌توان آن را جنگ ترکیبی متکی بر هوش مصنوعی نامید. این کاربرد، به‌ویژه از سوی رژیم صهیونیستی، پیش‌تر در برخی عملیات محدود پس از ۷ اکتبر، به‌خصوص در غزه، نیز گزارش شده بود (Andersin,2025).

هوش مصنوعی در اینجا صرفاً به معنای استفاده از یک نرم‌افزار یا ابزار فنی نبود، بلکه به‌مانند لایه‌ای پیونددهنده میان داده‌های خام، تحلیل ماشینی، اولویت‌بندی اهداف، تصمیم‌سازی عملیاتی، اجرای حمله، دفاع ضدموشکی و عملیات سایبری عمل کرد. در ادبیات جدید جنگ‌های داده‌محور نیز بر همین نکته تأکید می‌شود که هوش مصنوعی، «کلان‌داده»[1] و «خودکارسازی»[2]، نقش انسان را در بخشی از زنجیره‌های تصمیم به سمت نظارت، ارزیابی و تأیید نهایی سوق داده‌اند (Shahvaroughi Farahani & Ghasemi, 2024). در مطالعات پیش از جنگ ۱۲ روزه نیز نشان داده شده است که هوش مصنوعی و داده‌های چندمنبعی می‌توانند فرایند شناسایی و اولویت‌بندی اهداف نظامی را تسریع کنند (King, 2024).

در ادبیات دفاعی جدید، هوش مصنوعی نه‌فقط به‌عنوان فناوری مستقل، بلکه به‌عنوان عامل تغییر در ماهیت جنگ، فرماندهی و کنترل، هدف‌یابی، شناسایی تهدید، تصمیم‌گیری سریع، عملیات خودمختار و دفاع هوشمند شناخته می‌شود. در چنین الگویی، برتری نظامی به توان گردآوری داده، پردازش سریع، «همجوشی اطلاعات»[3]، تولید «تصویر عملیاتی مشترک»[4]، «تصمیم‌گیری بلادرنگ»[5] و تبدیل داده به اقدام مؤثر بستگی دارد.

1. Big Data
2. Automation
3. Information/Data Fusion
4. Common Operational Picture (COP)
5. Real-time Decision-making

رستمی پردازش اطلاعات، امنیت سایبری، آگاهی محیطی، رصد تهدید و پلتفرم جنگ‌افزارها را از حوزه‌های اصلی کاربرد این فناوری در سازمان‌های نظامی می‌داند (رستمی، ۱۴۰۱: ۵۸).

پژوهش حاضر با تمرکز بر ابعاد دفاعی–امنیتی جنگ ۱۲ روزه، در پی آن است که نقش‌های اصلی هوش مصنوعی را در این جنگ صورت‌بندی کند و نشان دهد این فناوری چگونه بر چرخه اطلاعات – تصمیم – اقدام اثر گذاشته است. برای این منظور، مقاله از چهارچوبی چهارمحوری شامل نقش اطلاعاتی، عملیاتی، دفاعی و سایبری استفاده می‌کند.

۱. کلیات

۱-۱. بیان مسئله

تحول فناوری‌های نوظهور، به‌ویژه هوش مصنوعی، کلان‌داده، «یادگیری ماشین»[1]، «سامانه‌های خودمختار»[2]، جنگ سایبری و فرماندهی و کنترل هوشمند، موجب شده است که ماهیت جنگ‌های معاصر از الگوی صرفاً سخت‌افزارمحور فاصله بگیرد و به سمت جنگ داده‌محور و شبکه‌محور حرکت کند. توسعه حسگرها، سامانه‌های جنگ الکترونیک، رادارها، جنگنده‌ها، هواپیماهای بدون سرنشین و جنگ‌افزارهای هوشمند، حجم، سرعت و تنوع داده‌های میدان نبرد را به‌شدت افزایش داده است (عظیمی‌زاده و همکاران، ۱۴۰۴: ۱۳).

جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران، همچون برخی جنگ‌های اخیر ازجمله اوکراین و غزه، محیط آشکار بروز ابعاد دفاعی ـ امنیتی هوش مصنوعی بود. بااین‌حال، وجود امکان مشاهده مستقیم میدانی و مستندسازی بخشی از رخدادها در ایران، این جنگ را به موردی مهم برای بررسی نقش هوش مصنوعی در چرخه اطلاعات، تصمیم و اقدام تبدیل کرده است. صورت‌بندی‌های موجود حاکی از آن است که انتخاب و اولویت‌بندی بخشی از اهداف، بر انباشت بلندمدت داده‌های اطلاعاتی و پردازش ماشینی آن‌ها تکیه داشته است (King, 2024).

1. Machine Learning
2. Autonomous Systems

مسئله اصلی پژوهش آن است که اگر نقش هوش مصنوعی صرفاً در حد چند ابزار جداگانه دیده شود، فهم راهبردی از جنگ ۱۲ روزه ناقص خواهد ماند. پژوهش‌های داخلی، نخست، کم‌تر به نقش هوش مصنوعی در حوزه دفاعی–امنیتی پرداخته‌اند و دوم، در موارد محدود موجود نیز بیشتر بر یکی از مراحل چرخه اطلاعات یا فرماندهی و کنترل تمرکز کرده‌اند. این در حالی است که اهمیت اصلی هوش مصنوعی در این نبرد، نه در یک سامانه یا یک مرحله منفرد، بلکه در معماری یکپارچه «داده – الگوریتم – فرماندهی و کنترل – سکوهای عملیاتی» نهفته است. ازاین‌رو، مسئله این تحقیق، نبود صورت‌بندی منسجم و قابل ردیابی از نقش‌های دفاعی–امنیتی هوش مصنوعی در جنگ ۱۲ روزه و اثر آن بر چرخه اطلاعات، تصمیم و اقدام است.

۱-۲. اهمیت و ضرورت تحقیق

اهمیت و ضرورت این تحقیق را می‌توان در چند محور زیر تبیین کرد:

۱. جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران، یکی از نمونه‌های مهم ورود آشکارتر هوش مصنوعی به منازعه مستقیم میان قدرت‌های منطقه‌ای و فرامنطقه‌ای است (Fitz-Gerald & Hennebry, 2025). در این جنگ، هوش مصنوعی صرفاً ابزار پردازش داده نبود، بلکه در پیوند با سامانه‌های فرماندهی و کنترل، سکوهای عملیاتی، پدافند هوشمند، جنگ سایبری و عملیات شناختی عمل کرد؛ بنابراین تحلیل آن برای شناخت معماری جدید قدرت نظامی ضروری است.

۲. از منظر کاربردی، جمهوری اسلامی ایران در حوزه‌های موشکی، پهپادی و پدافندی از ظرفیت‌های مهمی برخوردار است، اما تداوم بازدارندگی مؤثر در برابر تهدیدهای نوظهور، مستلزم شناخت دقیق نقش داده، هوش مصنوعی، شبکه حسگرها، فرماندهی و کنترل هوشمند و سامانه‌های تصمیم‌یار است. در جنگ‌های داده‌محور، یکپارچگی شبکه حسگرها و اتصال آن به سامانه‌های تحلیل و تصمیم‌یار، یکی از نقاط تمرکز اصلی در ارتقای توان دفاعی است (Baeza et al., 2025). تقویت یکپارچگی سامانه‌های «فرماندهی، کنترل، ارتباطات،

رایانه، اطلاعات، مراقبت و شناسایی»[1] و تعبیه هوش مصنوعی در زنجیره‌های اطلاعاتی و رزمی، از ضرورت‌های آمادگی برای نبردهای آینده است.

۳. ضرورت دیگر تحقیق، به مخاطرات اخلاقی، حقوقی و عملیاتی کاربرد هوش مصنوعی مربوط است. بهره‌گیری از هوش مصنوعی در جنگ، افزون بر ظرفیت‌های عملیاتی، با خطرهایی مانند خطای الگوریتمی، سوگیری داده، کاهش نقش انسان در تصمیم مرگبار، ابهام مسئولیت و دشواری کنترل همراه است (Hendrycks et al., 2025). در ادبیات حکمرانی هوش مصنوعی نیز بر ضرورت کنترل، پاسخ‌گویی و تنظیم قواعد استفاده از سامانه‌های هوشمند در محیط‌های پُرخطر تأکید شده است (Wasi et al., 2025). نگرانی درباره پیامدها و مخاطرات فراگیر هوش مصنوعی در ادبیات عمومی این فناوری نیز مطرح شده است (Shahvaroughi Farahani & Ghasemi, 2024).

۱-۳. پیشینه تحقیق

رستمی (۱۴۰۱) در مقاله «شناسایی و معرفی ظرفیت‌های کاربردی هوش مصنوعی در توسعه مضمون‌های راهبردی در سازمان‌های نظامی»، کاربردهای هوش مصنوعی را در حوزه‌هایی مانند پلتفرم جنگ‌افزارها، امنیت سایبری، لجستیک، سلامت میدان نبرد، شبیه‌سازی، برنامه‌ریزی، آگاهی محیطی و پردازش اطلاعات دسته‌بندی کرده است (رستمی، ۱۴۰۱: ۴۶). گرچه در این پژوهش، پردازش اطلاعات، امنیت سایبری، آگاهی محیطی و پلتفرم جنگ‌افزارها از مصادیق مهم کاربرد هوش مصنوعی در حوزه نظامی معرفی شده‌اند (رستمی، ۱۴۰۱: ۵۸)؛ اما جایگاه هوش مصنوعی در ساخت نظام یکپارچه دفاعی–امنیتی بررسی نشده است.

اسماعیلی و میارعباسی (۱۴۰۳) در مقاله «بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی–امنیتی جمهوری اسلامی ایران»، کاربردهای علوم و فناوری‌های شناختی را در حوزه دفاعی–امنیتی بررسی کرده و در پیوند با آن، به نقش ابزارهایی مانند

1. C4ISR; Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

هوش مصنوعی، یادگیری ماشین، تحلیل داده و تعامل انسان و ماشین در تشخیص تهدید، مدیریت مخاطرات و پردازش داده‌های حجیم پرداخته‌اند (اسماعیلی و میارعباسی، ۱۴۰۳: ۴۳–۴۵). آنان همچنین گردآوری اطلاعات، تشخیص تهدید، سامانه‌های فرماندهی و کنترل پیشرفته و امنیت سایبری را از کاربردهای مهم این حوزه معرفی کرده‌اند (اسماعیلی و میارعباسی، ۱۴۰۳: ۶۳–۶۴)؛ اما به‌دلیل تدوین مقاله در بازهٔ زمانی پیش از وقوع جنگ اخیر، به کاربردهای عینی و ملموس این حوزه ناظر به جنگ ۱۲ روزه و متناسب با محیط امنیتی جمهوری اسلامی ایران نپرداخته‌اند.

عظیمی‌زاده، سپهری، هلیلی و نقوی (۱۴۰۴) در مقاله «طراحی الگوی فرماندهی و کنترل هوشمند ارتش جمهوری اسلامی ایران مبتنی بر کلان‌داده»، نشان داده‌اند که الگوی فرماندهی و کنترل هوشمند مبتنی بر کلان‌داده می‌تواند با گردآوری، پردازش، تحلیل و بهره‌برداری از داده‌های میدان نبرد، سرعت و دقت تصمیم‌گیری را افزایش دهد (عظیمی‌زاده و همکاران، ۱۴۰۴: ۱۳–۱۴). پژوهش یادشده بر طراحی الگوی فرماندهی و کنترل متمرکز است؛ ازاین‌رو، تحلیل نقش هوش مصنوعی در سایر ابعاد دفاعی–امنیتی، ازجمله شناسایی، عملیات تهاجمی، پدافند و عملیات سایبری، در کانون آن قرار ندارد.

«سابادفولدی»[1] (2021) در مقاله‌ای مروری درباره فرصت‌ها و چالش‌های کاربرد هوش مصنوعی در حوزه نظامی، هوش مصنوعی را از مؤلفه‌های اثرگذار بر تحول جنگ‌های آینده و افزایش سرعت تصمیم‌سازی نظامی می‌داند. این پژوهش برای فهم جایگاه عمومی هوش مصنوعی در تحول نظامی و تصمیم‌سازی دفاعی قابل استفاده است، اما به سامانه‌های خاص رژیم صهیونیستی یا رخداد مشخص جنگ ۱۲ روزه نمی‌پردازد (Szabadföldi, 2021).

«پوپا»[2] (2022) بر پیوند فناوری‌های نوظهور با سازمان رزم، دکترین و زیرساخت‌های فرماندهی و کنترل تأکید می‌کند و نشان می‌دهد که تغییرات فناورانه، فرایند تصمیم‌گیری و کارایی ساختارهای نظامی را تحت تأثیر قرار می‌دهد. این پژوهش نیز از نظر توجه به نسبت فناوری و فرماندهی و کنترل با موضوع مقالهٔ حاضر هم‌پوشانی دارد؛ اما چهارچوب مشخصی

1. Szabadföldi
2. Popa

برای تحلیل معماری یکپارچه داده، تصمیم و اقدام در یک جنگ معاصر ارائه نمی‌کند (Popa, 2022).

براین‌اساس، می‌توان چنین نتیجه گرفت که پژوهش‌های موجود کم‌تر به تحلیل نقش‌آفرینی هوش مصنوعی در یک رخداد جنگی مشخص و معاصر، یعنی جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران، پرداخته‌اند. نوآوری مقالهٔ حاضر در آن است که نقش هوش مصنوعی را در قالب چهار نقش اطلاعاتی، عملیاتی، دفاعی و سایبری، به‌عنوان یک نظام و معماری یکپارچه بررسی می‌کند و نشان می‌دهد این نقش‌ها چگونه چرخه اطلاعات، تصمیم و اقدام را متحول ساخته‌اند. به بیان دیگر، در بسیاری از پژوهش‌های پیشین بر کلیات تأثیر هوش مصنوعی بر حوزه دفاعی–امنیتی یا جنگ‌های آینده تأکید شده و در برخی موارد نیز صرفاً به یک یا چند جزء، مانند سامانه کنترل هوشمند یا سامانه تحلیل، توجه شده است؛ درحالی‌که پژوهش حاضر با بررسی وقایع جنگ تحمیلی ۱۲ روزه، نوع نقش‌آفرینی هوش مصنوعی را در قالب معماری یکپارچه، فرایندی صریح، شفاف و قابل ارزیابی کرده است.

۱-۴. هدف‌های تحقیق

۱-۴-۱. هدف اصلی

تبیین نقش‌های دفاعی–امنیتی هوش مصنوعی در جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران و تحلیل اثر آن بر چرخه اطلاعات، تصمیم و اقدام.

۱-۴-۲. هدف‌های فرعی

۱. شناسایی نقش هوش مصنوعی در فشرده‌سازی مدار اطلاعاتی و هدف‌یابی سریع در جنگ ۱۲ روزه؛
۲. تحلیل نقش هوش مصنوعی در خودمختارسازی و هوشمندسازی عملیات تهاجمی؛
۳. بررسی نقش هوش مصنوعی در هوشمندسازی پدافند هوایی، ضدموشکی و ضدپهپادی؛

۴. تبیین نقش هوش مصنوعی در تقویت عملیات سایبری و جنگ دیجیتال؛
۵. استخراج دلالت‌های راهبردی و سیاستی برای ارتقای تاب‌آوری دفاعی-امنیتی جمهوری اسلامی ایران در برابر جنگ‌های آینده مبتنی بر هوش مصنوعی.

۱-۵. سؤال‌های تحقیق

۱-۵-۱. سؤال اصلی

هوش مصنوعی در جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران، از منظر دفاعی-امنیتی چه نقش‌هایی ایفا کرده و چگونه چرخه اطلاعات، تصمیم و اقدام را متحول ساخته است؟

۱-۵-۲. سؤال‌های فرعی

۱. هوش مصنوعی در حوزه اطلاعاتی و هدف‌یابی جنگ ۱۲ روزه چه نقشی داشته است؟
۲. هوش مصنوعی چگونه در خودمختارسازی و هوشمندسازی عملیات تهاجمی نقش‌آفرینی کرده است؟
۳. هوش مصنوعی چه نقشی در هوشمندسازی پدافند هوایی، ضدموشکی و ضدپهپادی داشته است؟
۴. هوش مصنوعی چگونه عملیات سایبری و کنش‌های مکمل در فضای دیجیتال را تقویت کرده است؟
۵. نقش‌آفرینی هوش مصنوعی در این جنگ چه دلالت‌هایی برای سیاست‌گذاری دفاعی-امنیتی جمهوری اسلامی ایران در برابر جنگ‌های آینده دارد؟

۲. ادبیات و مبانی نظری تحقیق

۲-۱. هوش مصنوعی نظامی و جنگ داده‌محور

ورود هوش مصنوعی، کلان‌داده و خودکارسازی به حوزه نظامی، جنگ را از الگوی سخت‌افزارمحور به سمت «جنگ داده‌محور»[1] و تصمیم‌محور سوق داده است. در این الگو، داده‌های میدانی، حسگری، ارتباطی، تصویری، سیگنالی، رفتاری و سایبری به ماده خام تصمیم‌گیری نظامی تبدیل می‌شوند و نقش انسان در برخی زنجیره‌های تصمیم، به نظارت و تأیید نهایی گرایش می‌یابد؛ زیرا گستردگی، پراکندگی و تنوع داده‌ها موجب شده است تحلیل این حجم از داده‌ها در زمان مورد نیاز، تنها با توان انسانی ممکن نباشد. به همین دلیل، جنگ‌های آینده فقط در زمین، دریا و هوا تعریف نمی‌شوند و حوزه‌های اطلاعاتی، سایبری، جنگ الکترونیک، عملیات شناختی و فضا، با محوریت ابزارهای گردآوری و تحلیل فناورانه، به اجزای «میدان نبرد چنددامنه‌ای»[2] تبدیل می‌شوند (Shahvaroughi Farahani & Ghasemi, 2024).

جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران را می‌توان از منظر جنگ داده‌محور بررسی کرد؛ در ادبیات پیش از این جنگ نیز ضرورت حفاظت از غیرنظامیان در میدان نبرد دیجیتال و داده‌محور مطرح شده بود (Gerald & Hennebry-Fitz, 2025). مطالعات پیش از این جنگ همچنین نشان داده‌اند که انباشت داده‌های اطلاعاتی و پردازش ماشینی می‌تواند انتخاب و اولویت‌بندی اهداف را تسریع کند؛ این مطالعات به‌تنهایی شاهد مستقیمی درباره عملیات ژوئن ۲۰۲۵ نیستند (King, 2024). پیش از آن نیز استفاده رژیم صهیونیستی از سامانه‌های هوش مصنوعی در عملیات محدود پس از ۷ اکتبر، به‌ویژه در غزه، گزارش شده بود (Andersin, 2025).

1. Data-driven Warfare
2. Multi-domain Operations

۲-۲. فرماندهی و کنترل هوشمند، کلان‌داده و چرخه تصمیم

فرماندهی و کنترل در جنگ‌های جدید، بیش از گذشته به داده، شبکه، سرعت پردازش و تصویر عملیاتی مشترک وابسته شده است. در الگوی فرماندهی و کنترل هوشمند، داده‌های میدان جنگ در سه لایه تولید، پردازش و بهره‌برداری سازمان‌دهی می‌شوند و خروجی آن‌ها در قالب هشدار، تصویر عملیاتی، توصیه تصمیم، اولویت‌بندی هدف یا تخصیص منابع در اختیار فرماندهان و سامانه‌های عملیاتی قرار می‌گیرد (عظیمی‌زاده و همکاران، ۱۴۰۴). این فرایند با نقش‌آفرینی هوش مصنوعی در چرخه «مشاهده، جهت‌یابی، تصمیم و اقدام»[1]، به فرماندهان کمک می‌کند تا با تسریع مراحل مشاهده، جهت‌یابی و تصمیم، اقدام را زودتر از دشمن اجرا کنند. در این مقاله، «اطلاعات- تصمیم- اقدام» صورت فشرده و عملیاتی چرخه مشاهده، جهت‌یابی، تصمیم و اقدام است؛ به این معنا که مشاهده و جهت‌یابی در مؤلفه «اطلاعات» جمع می‌شوند و این صورت‌بندی جایگزین چرخه چهارمرحله‌ای OODA نیست.

در جنگ ۱۲ روزه، اهمیت چرخه داده-تصمیم-اقدام در هدف‌یابی سریع، هماهنگ‌سازی سکوها، دفاع ضدموشکی و عملیات سایبری آشکار شد. در گزارش‌ها و اسناد عمومی درباره الگوی هدف‌یابی هوشمند رژیم صهیونیستی، از سامانه‌هایی مانند «گاسپل»[2]، «لاوندر»[3]، «کیمیاگر»[4]، «جنی»[5] و «عمق حکمت»[6] به‌عنوان ابزارهای داده‌محور برای سازمان‌دهی، پردازش و تحلیل لایه‌های مختلف اطلاعاتی و کمک به شناسایی یا پیشنهاد اهداف یاد شده است (Rehak & Woodcock, 2026). این سامانه‌ها در اسناد مورد تحلیل، به‌عنوان ابزارهای تحلیل داده، هدف‌سازی و تصمیم‌یاری میدانی، ازجمله تولید سناریوهای حمله، مدیریت آتش و تخصیص مهمات، مطرح شده‌اند و کارکرد آن‌ها از جست‌وجوی سریع در انبوه داده‌های اطلاعاتی تا رتبه‌بندی اهداف و تولید توصیه‌های تاکتیکی را در برمی‌گیرد. این

1. Observe, Orient, Decide, Act (OODA)
2. Habsora / The Gospel
3. Lavender
4. Alchemist
5. Genie
6. Depth of Wisdom

گزارش‌ها برای توضیح سازوکار تحلیل داده و پیشنهاد هدف سودمندند، اما به‌تنهایی کاربرد همان سامانه‌ها یا همان شیوه تأیید هدف را در جنگ ۱۲ روزه علیه ایران اثبات نمی‌کنند.

بااین‌حال، دسترسی عمومی به جزئیات فنی، پیکربندی و شیوه عملیاتی این سامانه‌ها محدود است؛ بنابراین در این پژوهش، کارکرد آن‌ها در سطح تحلیلی و بر پایه منابع آشکار بررسی می‌شود و نه به‌عنوان داوری قطعی درباره جزئیات محرمانه عملکرد آن‌ها (Rehak & Woodcock, 2026; Wilson & Donnelly, 2026).

۲-۳. جنگ ترکیبی، جنگ شناختی و جنگ سایبری

جنگ ترکیبی در معنای عام، الگویی از منازعه است که در آن ابزارهای نظامی، اطلاعاتی، سایبری، رسانه‌ای، اقتصادی، روانی، شناختی و دیپلماتیک به‌صورت هم‌زمان و مکمل به‌کار گرفته می‌شوند. بااین‌حال، پژوهش حاضر در پی تحلیل همه ابعاد جنگ ترکیبی نیست و با توجه به هدف دفاعی–امنیتی مقاله، تعریف عملیاتی آن را به چهار حوزه اطلاعاتی، عملیاتی–نظامی، دفاعی–پدافندی و سایبری محدود می‌کند؛ بنابراین، مؤلفه‌های اقتصادی، دیپلماتیک و رسانه‌ای، هرچند در فهم کلان جنگ ترکیبی اهمیت دارند، در این پژوهش زمینه‌های مکمل تلقی شده و وارد چهارچوب اصلی یافته‌ها نشده‌اند. برهمین‌اساس، جنگ ۱۲ روزه از منظر اثر هوش مصنوعی بر چرخه اطلاعات، تصمیم و اقدام در چهار محور اطلاعاتی، عملیاتی، دفاعی و سایبری بررسی می‌شود.

۲-۳-۱. جنگ شناختی

جنگ شناختی ناظر به اثرگذاری بر ذهن، ادراک، توجه، قضاوت، تصمیم و رفتار انسان‌هاست. در این نوع جنگ، هدف اصلی نه تخریب مستقیم زیرساخت دیجیتال، بلکه تغییر درک بازیگران، تضعیف اعتماد، ایجاد خطای محاسباتی و اثرگذاری بر تصمیم فردی و جمعی است. ابزارهای آن می‌تواند رسانه، شبکه اجتماعی، روایت‌سازی، عملیات روانی، داده‌کاوی رفتاری و پیام‌رسانی هدفمند باشد. در محیط دفاعی–امنیتی، علوم و فناوری‌های شناختی

می‌توانند در تشخیص تهدید، تحلیل رفتار دشمن، تعامل انسان و ماشین و مقابله با عملیات روانی نقش‌آفرینی کنند (اسماعیلی و میارعباسی، ۱۴۰۳: ۴۳-۴۵).

۲-۳-۲. امنیت سایبری و جنگ سایبری

امنیت سایبری و جنگ سایبری ناظر به حفاظت، نفوذ، اختلال یا تخریب در سامانه‌ها، شبکه‌ها، داده‌ها و زیرساخت‌های دیجیتال است. ازاین‌رو، موضوع اصلی آن ذهن و ادراک انسان نیست، بلکه شبکه، داده، نرم‌افزار، سخت‌افزار، زیرساخت ارتباطی و سامانه‌های فرماندهی و کنترل است. البته عملیات سایبری می‌تواند زمینه‌ساز یا تقویت‌کننده عملیات شناختی باشد؛ برای مثال نفوذ، سرقت داده، اختلال در خدمات یا انتشار هدفمند اطلاعات می‌تواند آثار روانی و ادراکی ایجاد کند؛ اما این هم‌پوشانی ابزاری به معنای یکی بودن دو مفهوم نیست.

تجربه‌هایی مانند «استاکس‌نت»[1] نشان داد که جنگ سایبری می‌تواند بدون درگیری فیزیکی مستقیم، اختلالات معناداری در زیرساخت‌های حساس ایجاد کند. حفاظت از زیرساخت‌های دفاع موشکی در برابر تهدیدهای سایبری و توجه به امنیت نرم‌افزار و سامانه‌های برنامه‌نویسی، بخشی از الزامات پدافند سایبری است (عباسی و همکاران، ۱۳۹۶؛ کشوری و همکاران، ۱۳۹۶: ۲۳-۳۴). در جنگ ۱۲ روزه، نقش سایبری عمدتاً مکمل میدان اصلی نبرد بود؛ بااین‌حال، هوش مصنوعی می‌تواند سرعت شناسایی آسیب‌پذیری، خودکارسازی حملات، شخصی‌سازی فیشینگ، تحلیل رفتار شبکه و دفاع سایبری را افزایش دهد (Wasi et al., 2025)؛ بنابراین، در چهارچوب این پژوهش، نقش شناختی به اثرگذاری بر ادراک و تصمیم انسان‌ها مربوط است؛ اما نقش سایبری به نفوذ، اختلال، حفاظت و خودکارسازی کنش در زیرساخت‌ها و شبکه‌های دیجیتال مربوط می‌شود.

۲-۴. چهارچوب تحلیلی تحقیق

براساس مبانی نظری و پیشینه، چهارچوب تحلیلی تحقیق در چهار حوزه اطلاعاتی، عملیاتی، دفاعی و سایبری سازمان‌دهی شد که منطبق با سؤال‌های تحقیق است. نقش اطلاعاتی، ناظر

1. Stuxnet

به فشرده‌سازی مدار اطلاعات، ادغام داده‌های چندمنبعی، اتصال سرنخ‌های پراکنده و رتبه‌بندی اهداف است. نقش عملیاتی به خودمختارسازی عملیات تهاجمی، هماهنگ‌سازی پهپادها، تخصیص سکوها و کاهش زمان زنجیره کشتار مربوط می‌شود. نقش دفاعی نیز شامل هوشمندسازی پدافند هوایی، ضدموشکی و ضدپهپادی از طریق تشخیص هدف، پیش‌بینی مسیر، همجوشی داده‌های حسگری و اولویت‌بندی مصرف رهگیرهاست. نقش سایبری نیز به مقیاس‌دهی حملات، خودکارسازی نفوذ، تحلیل رفتار شبکه و دفاع سایبری مربوط می‌شود؛ در این حوزه، مدل‌سازی توپولوژی شبکه، شناسایی مسیرهای حمله و تصمیم‌گیری پویا برای انتخاب راهبرد دفاعی، از محورهای اصلی به‌کارگیری هوش مصنوعی در دفاع سایبری است (Wang et al., 2025).

براساس این چهارچوب، هوش مصنوعی در جنگ ۱۲ روزه نه به‌عنوان یک فناوری منفرد، بلکه به‌مانند معماری یکپارچه «داده ـ الگوریتم ـ فرماندهی و کنترل ـ سکوهای عملیاتی» عمل کرده است. نوآوری مقاله در تبیین نسبت فرایندی و ناهم‌وزن این چهار نقش در معماری یکپارچه داده، تصمیم و اقدام است؛ چهارچوبی که می‌تواند برای سیاست‌گذاری دفاعی، حکمرانی داده، تاب‌آوری فرماندهی و کنترل، یکپارچگی شبکه حسگرها و تنظیم قواعد تعامل انسان و ماشین به‌کار رود. در کاربردهای پُرخطر هوش مصنوعی نیز ملاحظات کنترل و پاسخ‌گویی اهمیت ویژه‌ای دارد (Hendrycks et al., 2025).

۲-۵. روش‌شناسی تحقیق

این پژوهش از نظر هدف، کاربردی و سیاست‌پژوهانه، از نظر رویکرد، کیفی و از حیث روش تحلیل، مبتنی بر «تحلیل چهارچوبی»[1] است و با هدف تبیین نقش‌آفرینی هوش مصنوعی در جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران و استخراج دلالت‌های راهبردی آن انجام شده است. ازآنجاکه خروجی مورد انتظار پژوهش، تحلیلی قابل‌ردگیری و مناسب برای تصمیم‌سازی دفاعی–امنیتی است، تحلیل چهارچوبی به‌عنوان

1. Framework Analysis

راهبرد اصلی تحلیل داده‌ها انتخاب شد. این روش برای پژوهش‌های کاربردی و سیاستی مناسب است؛ زیرا داده‌های چندمنبعی را در قالب مقوله‌های روشن، ماتریس تحلیلی و مسیر استدلالی قابل پیگیری سازمان‌دهی می‌کند (Ritchie & Spencer, 1994: 173-194).

بر مبنای «پیاز پژوهش ساندرز»[1]، این مطالعه در سطح فلسفی بر «پارادایم عمل‌گرایی»[2] استوار است. در این پارادایم، معیار اصلی انتخاب روش‌ها، کارآمدی آن‌ها در پاسخ‌گویی به مسئله و تولید دانش قابل استفاده برای تصمیم‌سازی است (Saunders et al., 2019: 144-147). انتخاب روش‌شناختی پژوهش، تک‌روشی کیفی است و داده‌ها از طریق تحلیل اسنادی کیفی پردازش شدند؛ زیرا رویکرد کیفی امکان فهم زمینه‌ای، تفسیر نظام‌مند و استخراج مقوله‌های معنادار از متون را فراهم می‌کند (Creswell & Poth, 2018).

۲-۵-۱. قلمرو، جامعه و نمونه پژوهش

قلمرو موضوعی پژوهش، نقش‌آفرینی هوش مصنوعی در ابعاد دفاعی–امنیتی جنگ ۱۲ روزه در چهار محور اطلاعاتی، عملیاتی، دفاعی و سایبری است. قلمرو زمانی، رخداد جنگ ۱۲ روزه در ژوئن ۲۰۲۵ و متون و اسناد مرتبط با آن است. قلمرو مکانی، فضای عملیاتی مرتبط با جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران است. با توجه به ماهیت اسنادی و رخدادمحور تحقیق، قلمرو سازمانی به یک سازمان مشخص محدود نیست و ساختارها و نهادهای دفاعی–امنیتی مرتبط با طرف‌های درگیر و موضوع پژوهش را در برمی‌گیرد. جامعه اسنادی پژوهش شامل متون تحلیلی، گزارش‌ها، یادداشت‌ها، مقاله‌های علمی و داده‌های آشکار مرتبط با جنگ ۱۲ روزه و نقش هوش مصنوعی در آن بود. واحد تحلیل، گزاره‌ها و شواهدی بود که درباره یکی از ابعاد نقش‌آفرینی هوش مصنوعی در چهار محور اطلاعاتی، عملیاتی، دفاعی و سایبری اطلاعات معنادار ارائه می‌کردند. معیار ورود اسناد، ارتباط با جنگ ۱۲ روزه یا نقش هوش مصنوعی، برخورداری از محتوای تحلیلی و قابلیت انتساب به یکی از محورهای پژوهش بود. با مراجعه به بیش از ۳۰ منبع علمی و

1. Saunders' Research Onion
2. Pragmatism

رسانه‌ای، بیش از ۵۰ سند اولیه گردآوری و بررسی شد. اسناد فاقد ارتباط مستقیم، فاقد اعتبار تحلیلی، تکراری یا غیرقابل طبقه‌بندی کنار گذاشته شدند و در نهایت ۳۵ منبع مرتبط، مبنای تحلیل قرار گرفتند. جامعه خبرگانی پژوهش نیز شامل متخصصان دارای سابقه علمی یا اجرایی مرتبط با حوزه دفاعی–امنیتی بود که از میان آنان ۱۲ خبره با روش نمونه‌گیری هدفمند و منطق قضاوتی انتخاب شدند. مشخصات این خبرگان در جدول (۱)، ارائه شده است.

۲-۵-۲. روش گردآوری داده‌ها

داده‌های اصلی پژوهش از طریق مطالعه کتابخانه‌ای و اسنادی منابع علمی، گزارش‌های تحلیلی و داده‌های آشکار مرتبط با جنگ گردآوری شدند. گروه کانونی خبرگانی و دریافت بازخوردهای تکمیلی نیز برای اعتبارسنجی یافته‌ها و نه به‌عنوان منبع مستقل تولید داده اصلی پژوهش به‌کار رفت؛ بنابراین، داده‌های اصلی پژوهش از طریق پرسش‌نامه یا مصاحبه ساختاریافته گردآوری نشده‌اند و مشارکت خبرگان در مرحله بازبینی و اعتبارسنجی کدها، مقوله‌ها و یافته‌های استخراج‌شده صورت گرفته است. برای سازمان‌دِهی اسناد، کدگذاری داده‌ها، تشکیل مقوله‌ها و تنظیم ماتریس‌های تحلیلی از «نرم‌افزار تحلیل داده‌های کیفی»[1] استفاده شد. افزون بر مطالعه اسنادی، بخشی از داده‌ها از طریق مشاهده میدانی مستقیم رخدادها و پیامدهای قابل‌مشاهده جنگ ۱۲ روزه در ایران گردآوری و برای تکمیل و تطبیق شواهد اسنادی مورد استفاده قرار گرفت.

۲-۵-۳. چهارچوب و فرایند تحلیل

«چهارچوب اولیه»[2] پژوهش بر چهار محور تحلیلی سازمان‌دِهی شد: نقش اطلاعاتی، شامل فشرده‌سازی مدار اطلاعات و هدف‌یابی سریع؛ نقش عملیاتی، شامل خودمختارسازی عملیات تهاجمی و کوتاه‌سازی «زنجیره کشتار»[3]؛ نقش دفاعی، شامل هوشمندسازی پدافند هوایی،

1. MAXQDA 2020
2. A Priori Framework
3. Kill Chain

ضدموشکی و ضدپهپادی؛ و نقش سایبری، شامل تقویت عملیات سایبری، فیشینگ، اختلال و عملیات روانی دیجیتال. فرایند تحلیل داده‌ها با استفاده از نرم‌افزار تحلیل داده‌های کیفی و مطابق گام‌های کلاسیک تحلیل چهارچوبی شامل «آشنایی با داده‌ها»[1]، «صورت‌بندی چهارچوب تحلیلی»[2]، «کدگذاری»[3]، «جدول‌بندی»[4] و «نگاشت و تفسیر»[5] انجام شد. کدگذاری به‌صورت ترکیبی صورت گرفت؛ بخشی از کدها قیاسی بودند، مانند همجوشی داده، کاهش زنجیره کشتار، «خودکارسازی تصمیم»[6] و اختلال کوتاه‌مدت ناشی از حملات «منع خدمت توزیع‌شده»[7]؛ و بخشی دیگر به‌صورت استقرایی از داده‌ها استخراج شدند، مانند پیوند «اطلاعات انسانی»[8] با هوش مصنوعی در فرایند هدف‌یابی و مخاطرات اخلاقی–حقوقی اتوماسیون مرگبار. استفاده هم‌زمان از چهارچوب اولیه و مفاهیم نوظهور، امکان ترکیب انسجام نظری و حساسیت به داده‌های تجربی را فراهم می‌کند (Srivastava & Thomson, 2009: 72-79).

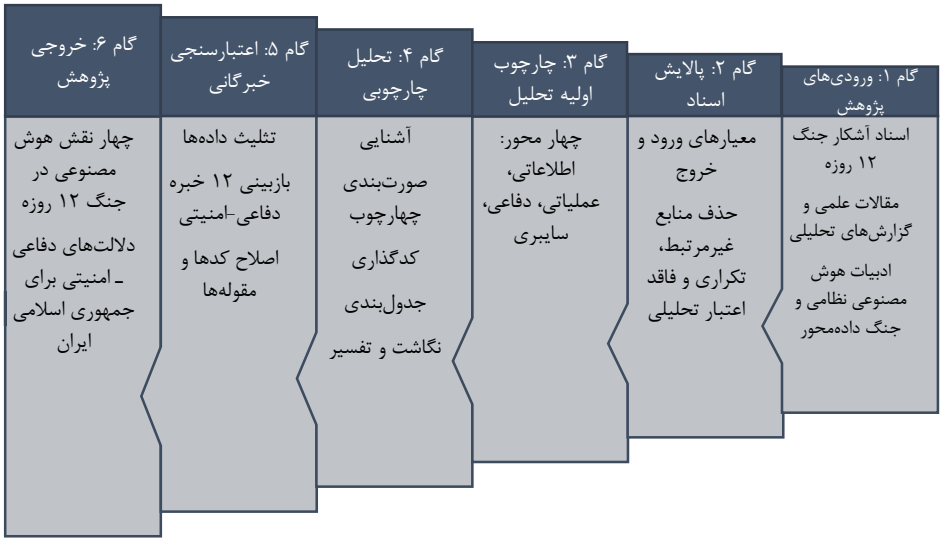
۲-۵-۴. اعتبارسنجی یافته‌ها

برای افزایش اعتبار و اعتمادپذیری یافته‌ها، از تثلیث داده‌ها، بازبینی خبرگانی و حفظ مسیر تبدیل داده خام به کد و مقوله استفاده شد. مشارکت خبرگان به‌صورت هدفمند و با منطق نمونه‌گیری قضاوتی انجام گرفت؛ به این معنا که افراد براساس سابقه علمی یا اجرایی مرتبط با حوزه دفاعی–امنیتی، آشنایی تخصصی با یکی از محورهای هوش مصنوعی، اطلاعات و امنیت، پدافند، فنی–سایبری یا تحلیل راهبردی و توان اظهارنظر درباره اعتبار کدها و مقوله‌های استخراج‌شده انتخاب شدند. این شیوه با منطق نمونه‌گیری هدفمند در پژوهش‌های کیفی سازگار است؛ زیرا در چنین پژوهش‌هایی، ملاک اصلی غنای اطلاعاتی و ارتباط مستقیم مشارکت‌کنندگان با مسئله تحقیق است (Patton, 2015; Creswell & Poth, 2018).

1. Familiarization
2. Identifying a Thematic Framework
3. Indexing/Coding
4. Charting
5. Mapping and Interpretation
6. Decision Automation
7. Distributed Denial of Service (DDoS)
8. Human Intelligence (HUMINT)

تعامل با خبرگان در قالب گروه کانونی خبرگانی و دریافت بازخوردهای تکمیلی انجام شد. خلاصه یافته‌ها، ماتریس کدها و مقوله‌ها و چهارچوب چهارمحوری پژوهش در اختیار ۱۲ خبره قرار گرفت و از آنان خواسته شد درباره کفایت شواهد، تناسب کدها با داده‌ها، تمایز مقوله‌ها، جامعیت محورهای تحلیلی و دلالت‌های سیاستی اظهارنظر کنند. محورهای بحث شامل دقت مفهومی کدها، نسبت مقوله‌ها با داده‌های خام، هم‌پوشانی یا تمایز محورهای چهارگانه و امکان‌پذیری پیشنهادهای سیاستی بود. مرحله نگاشت و تفسیر نیز برای عبور از توصیف داده‌ها به سمت تبیین الگوها و استخراج دلالت‌های کاربردی به‌کار رفت (Gale et al., 2013: 6-8).

مبنای پذیرش یا رد نظرات اصلاحی، بازگشت به داده‌های خام، سازگاری با چهارچوب تحلیلی، قابلیت استناد به منابع آشکار و کمک به افزایش دقت مفهومی بود. پیشنهادهایی پذیرفته شدند که به روشن‌تر شدن کدها، ادغام یا تفکیک مقوله‌ها، اصلاح عنوان محورها یا تقویت دلالت‌های سیاستی کمک می‌کردند. پیشنهادهای خارج از قلمرو پژوهش، مبتنی بر داده‌های طبقه‌بندی‌شده یا غیرقابل استناد، یا بازخوردهای صرفاً تأییدی که اثری بر ساختار تحلیل نداشتند، در متن نهایی اعمال نشدند. در موارد اختلاف‌نظر، داده‌های اولیه و شواهد اسنادی بازبینی و تصمیم نهایی براساس توافق غالب خبرگان و سازگاری با شواهد اتخاذ شد. از میان ۱۲ بازخورد دریافت‌شده، بازخوردهای ۱۰ نفر، معادل ۸۳/۳ درصد، به اصلاح کدها، مقوله‌ها یا نحوه صورت‌بندی یافته‌ها منجر شد و بازخوردهای ۲ نفر، معادل ۱۶/۷ درصد، عمدتاً تأییدی یا تکمیلی بود و تغییر محتوایی مستقیم در چهارچوب نهایی ایجاد نکرد. این فرایند برای افزایش اعتبار، اعتمادپذیری و تأییدپذیری یافته‌ها انجام شد (Lincoln & Guba, 1985; Gale et al., 2013).



شکل ۱: الگوی مفهومی فرایند روش‌شناسی پژوهش

جدول ۱: مشخصات خبرگان مشارکت‌کننده در اعتبارسنجی کیفی یافته‌ها

ردیف	جایگاه	عضویت	تخصص
۱	معاون دانشگاه	عضو هیئت‌علمی	مدیریت راهبردی
۲	رئیس دانشکده	عضو هیئت‌علمی	هوش مصنوعی
۳	رئیس دانشکده	عضو هیئت‌علمی	علوم دفاعی
۴	رئیس دانشکده	عضو هیئت‌علمی	فنی سایبری
۵	رئیس پژوهشکده	عضو هیئت‌علمی	اطلاعات و امنیت
۶	عضو قرارگاه جنگ	عضو هیئت‌علمی	هوش مصنوعی
۷	عضو قرارگاه جنگ	عضو هیئت‌علمی	فنی سایبری
۸	عضو قرارگاه جنگ	عضو هیئت‌علمی	اطلاعات و امنیت
۹	عضو قرارگاه جنگ	پژوهشگر	اطلاعات و امنیت
۱۰	عضو قرارگاه جنگ	پژوهشگر	تاب‌آوری اجتماعی
۱۱	عضو قرارگاه جنگ	پژوهشگر و دانشجوی دکتری	هوش مصنوعی
۱۲	عضو قرارگاه جنگ	پژوهشگر و دانشجوی دکتری	تحلیل سیستماتیک

۳. یافته‌های تحقیق و تجزیه‌وتحلیل آن‌ها

با توجه به مبانی نظری و داده‌های گردآوری‌شده، نقش‌های دفاعی–امنیتی هوش مصنوعی در جنگ ۱۲ روزه در چهار محور اطلاعاتی، عملیاتی، دفاعی و سایبری دسته‌بندی شدند. این چهار محور به‌صورت قیاسی و براساس سؤال‌های تحقیق و چهارچوب نظری تعیین شدند و سپس با خوانش رفت‌وبرگشتی اسناد، کدهای توصیفی و تفسیری مانند همجوشی داده‌های چندمنبعی، امتیازدهی تهدید، خودکارسازی تصمیم، فشرده‌سازی زنجیره کشتار، هوش ازدحامی، تیم‌سازی انسان–ماشین، پیش‌بینی مسیر، بهینه‌سازی رهگیر، مقیاس‌دهی حملات سایبری و اختلال کوتاه‌مدت استخراج شدند. در ادامه، کدهای هم‌معنا و مرتبط در قالب زیرمقوله‌ها تجمیع و نسبت آن‌ها با چهار محور اصلی نگاشت شد. جدول (۲)، مسیر فشرده تبدیل شواهد اسنادی به کد، زیرمقوله و مقوله نهایی را نشان می‌دهد.

جدول ۲: نمونه ماتریس فشرده کدگذاری، جدول‌بندی و نگاشت شواهد در تحلیل چهارچوبی

ردیف	شواهد مستخرج از اسناد	کدهای اولیه	زیرمقوله تفسیری	محور نهایی	منبع
۱	تجمیع هم‌زمان داده‌های شنودی، تصویری، ماهواره‌ای، مالی، رفتاری و اطلاعات انسانی، جست‌وجوی خودکار در بانک‌های اطلاعاتی، اتصال سرنخ‌های پراکنده توسط سامانه‌هایی مانند گاسپل و کارخانه آتش	همجوشی داده‌های چندمنبعی، غربالگری خودکار، کشف الگو، پیوند اطلاعات انسانی و تحلیل ماشینی	ایجاد تصویر اطلاعاتی یکپارچه و تبدیل داده خام به سرنخ هدف‌ساز	نقش اطلاعاتی	گزارش‌های استخراج‌شده از: CSIS، Al Jazeera، The Times of Israel، Military.com، Red Analysis
۲	امتیازدهی افراد و شبکه‌ها، رتبه‌بندی اهداف، تولید فهرست اهداف اولویت‌دار، پردازش حجم بالای داده و کاهش زمان شناسایی	امتیازدهی تهدید، اولویت‌بندی هدف، تولید بانک اهداف پویا، اتوماسیون	فشرده‌سازی مدار اطلاعات و هدف‌یابی سریع	نقش اطلاعاتی	گزارش‌های استخراج‌شده از: واحد ۸۲۰۰، INSS، The Guardian،

ردیف	شواهد مستخرج از اسناد	کدهای اولیه	زیرمقوله تفسیری	محور نهایی	منبع
	تا اقدام، گزارش شناسایی ۸۷ درصد اهداف ارزشمند و زنجیره کشتار ۶۰ ثانیه‌ای	تصمیم، فشرده‌سازی زنجیره کشتار			Magazine، Responsible Statecraft، The Jerusalem Post، CSIS
۳	دریافت داده‌های زنده از پهپادها، هواپیماها و حسگرهای زمینی، ارائه تصویر عملیاتی مشترک، پیشنهاد مسیر امن، حمله نقطه‌ای، عقب‌نشینی یا درخواست پشتیبانی توسط کیمیاگر و جمینی، تخصیص سکو، مهمات و زمان حمله	تصمیم‌یاری بلادرنگ، فرماندهی و کنترل هوشمند، تخصیص سکو و سلاح، پیشنهاد تاکتیکی، هماهنگی چندسکویی	اتصال خروجی اطلاعاتی به تصمیم و اقدام عملیاتی	نقش عملیاتی	گزارش‌های استخراج‌شده از: The Jerusalem Post، CSIS، The JINSA، Times of Israel، Military.com
۴	به‌کارگیری پهپادهای پیش‌مستقر و خودمختار، عملیات جمعی و اشباع راداری، هماهنگی پهپادهای شناسایی با جنگنده‌های اف-۳۵، شناسایی و قفل هدف توسط ماشین و تأیید نهایی انسان، اجرای حملات نقطه‌ای علیه اهداف ارزشمند	خودمختاری عملیاتی، هوش ازدحامی، تیم‌سازی انسان ـ ماشین، هماهنگی پهپاد و جنگنده، اتوماسیون مرگبار	خودمختارسازی و هوشمندسازی عملیات تهاجمی	نقش عملیاتی	گزارش‌های استخراج‌شده از: CSIS، The Times of Israel، Ynet، The Jerusalem Post، Euronews، DroneLife
۵	استفاده از یادگیری ماشین برای تشخیص و طبقه‌بندی تهدید، حذف هشدارهای کاذب،	تشخیص خودکار هدف، تفکیک هدف واقعی و کاذب،	کاهش زمان واکنش و افزایش کارایی تصمیم دفاعی	نقش دفاعی	گزارش‌های استخراج‌شده از: The Jerusalem

ردیف	شواهد مستخرج از اسناد	کدهای اولیه	زیرمقوله تفسیری	محور نهایی	منبع
	پیش‌بینی مسیر و نقطه برخورد و تخصیص انتخابی رهگیر در سامانه‌های گنبد آهنین، پیکان و فلاخن داوود	پیش‌بینی مسیر، اولویت‌بندی تهدید، بهینه‌سازی مصرف رهگیر			Post، Forbes، Defense Newsو وزارت امور خارجه اسرائیل
۶	تلفیق داده‌های راداری، الکترواپتیکی، حرارتی، صوتی و ماهواره‌ای، اتصال شبکه‌های حسگری و رادارهای همکار، شناسایی و مقابله هوشمند با پهپادها توسط درون دوم و درون گارد	همجوشی چندحسگری، شبکه حسگر هوشمند، AioT، ردیابی پیوسته، دفاع ضدپهپادی	پدافند هوشمند مبتنی بر پیش‌بینی و ادغام داده	نقش دفاعی	گزارش‌های استخراج‌شده از: The Times of Israel، The Jerusalem Post، Red Analysisو Defense News
۷	حملات منع سرویس توزیع‌شده، نفوذ به خدمات مالی و رمزارزی، اختلال در خدمات برخط، شخصی‌سازی فیشینگ، کشف آسیب‌پذیری و امکان خودکارسازی ابزارهای نفوذ و عملیات روانی	مقیاس‌دهی حمله، خودکارسازی نفوذ، فیشینگ هوشمند، اختلال خدمات، نفوذ مالی، عملیات روانی دیجیتال	تقویت ظرفیت و مقیاس عملیات سایبری	نقش سایبری	گزارش‌های استخراج‌شده از: Trends Research، Atlantic Council، The Economic Timesو The Times of Israel
۸	تداوم حملات فیزیکی دو طرف با وجود عملیات سایبری، موقتی‌بودن بخش عمده اختلال‌ها، ناتوانی حملات سایبری در توقف شلیک موشک‌ها	اختلال کوتاه‌مدت، اثر روانی، عدم تعیین‌کنندگی مستقل، گسست سایبر و	نقش مکمل و مشروط عملیات سایبری	نقش سایبری	گزارش‌های استخراج‌شده از: Trends Research، Atlantic Council،

ردیف	شواهد مستخرج از اسناد	کدهای اولیه	زیرمقوله تفسیری	محور نهایی	منبع
	یا تغییر قاطع نتیجه جنگ، وابستگی اثربخشی سایبری به پیوند آن با عملیات فیزیکی	میدان فیزیکی، نقش تقویتی			The Economic Times و The Times of Israel

همان‌گونه که جدول نشان می‌دهد، محورهای نهایی بر پایه نام سامانه‌ها یا حوزه‌های فنی شکل نگرفته‌اند، بلکه براساس سازوکار غالب نقش‌آفرینی هوش مصنوعی سازمان‌دهی شده‌اند. در ادامه، سازوکار و آثار عملیاتی-راهبردی هر یک از این نقش‌ها تبیین می‌شود.

۳-۱. نقش اطلاعاتی: فشرده‌سازی مدار اطلاعات و هدف‌یابی سریع

یافته‌ها نشان می‌دهد تمرکز بر ادغام مراحل مدار اطلاعاتی و کوتاه کردن زمان تحلیل حجم عظیم داده‌ها، مهم‌ترین نقش هوش مصنوعی در این جنگ بوده است. سامانه گاسپل در این سطح، با جست‌وجو و تحلیل هم‌زمان بانک‌های اطلاعاتی، از شنود مکالمات و رهگیری بی‌سیم تا تصاویر ماهواره‌ای، به شناسایی سریع الگوهای مشکوک کمک کرد. در این الگو، سرنخ‌های پراکنده‌ای که به‌تنهایی ارزش عملیاتی محدودی دارند، با تقاطع حجم بالایی از داده‌ها به نشانه‌های هدف‌ساز تبدیل می‌شوند. در گزارش‌های مربوط به جنگ غزه، گاسپل به‌عنوان نمونه‌ای از سامانه‌های پیشنهاد هدف بر پایه داده معرفی شده است (Abraham,2023). سامانه لاوندر نیز برای شناسایی افراد هدف و رتبه‌بندی تهدید به‌کار گرفته شد و با تحلیل داده‌های مالی، ارتباطی و رفتاری، خروجی خود را به شکل فهرست اهداف اولویت‌دار در اختیار ساختارهای عملیاتی قرار می‌داد. لاوندر برای امتیازدهی و پیشنهاد افراد هدف گزارش شده است. در این فرایند، عامل انسانی عمدتاً نقش تأییدکننده نهایی را داشت که از یک‌سو سرعت شناسایی و اقدام را افزایش می‌داد و از سوی دیگر، خطر اتکای بیش از حد به خروجی الگوریتم را برجسته می‌کرد. در گزارش مربوط به غزه، تأیید انسانی در برخی موارد بسیار کوتاه و شکلی توصیف شده است؛ بنابراین، قرار داشتن انسان در انتهای فرایند به‌تنهایی

به معنای نظارت مؤثر بر تصمیم الگوریتمی نیست (Abraham, 2024). درمجموع، هوش مصنوعی در حوزه اطلاعات و شناسایی نقش یک ضرب‌کننده نیرو را ایفا کرد و ترکیب تحلیل ماشینی با شبکه نفوذ انسانی و داده‌های چندمنبعی، به کوتاه‌شدن چرخه شناسایی تا انهدام، افزایش ظرفیت ضربه نخست و تقویت غافل‌گیری تاکتیکی انجامید.

۳-۲. نقش عملیاتی: خودمختارسازی عملیات تهاجمی

دومین نقش مهم هوش مصنوعی در جنگ ۱۲ روزه، خودمختارسازی و هوشمندسازی بخشی از عملیات تهاجمی بود. هدف رژیم صهیونیستی در آغاز جنگ، فلج‌کردن حداکثری توان دفاعی، پدافندی و فرماندهی ایران در ضربه نخست بود و تحقق آن به‌سرعت، دقت، هماهنگی و غافل‌گیری نیاز داشت. در این سطح، استفاده از سلاح‌های هوشمند، پهپادهای خودمختار، مهمات نقطه‌زن و ترکیب انسان و ماشین در عملیات تهاجمی اهمیت ویژه‌ای پیدا کرد.

یکی از زیرمحورهای این نقش، استفاده از پهپادهای خودمختار و مهمات نقطه‌زن از داخل یا نزدیک محیط عملیاتی ایران بود. در این الگو، نفوذ انسانی، استقرار پنهان تجهیزات، تحلیل مسیر، انتخاب زمان حمله، هماهنگی چندسکویی و اجرای سریع عملیات با یکدیگر ترکیب می‌شوند. پهپادهای کوچک نیز در صورت عملکرد جمعی و هماهنگ می‌توانند رادارها را اشباع کرده و مسیر را برای موج‌های بعدی حمله باز کنند؛ سازوکاری که بر منطق «هوش ازدحامی»[1] استوار است.

زیرمحور دیگر، تلفیق جنگنده‌های سرنشین‌دار و پهپادهای رزمی بود. در چنین الگویی، پهپادهای شناسایی تصاویر زنده و وضعیت پدافند را منتقل می‌کنند و سامانه‌های هوش مصنوعی با پردازش داده‌ها، مسیر امن، سطح تهدید، زمان حمله و نوع سلاح مناسب را پیشنهاد می‌دهند. این الگو از منظر نظری با ادبیات عمومی «تیم‌سازی انسان و ماشین»[2] و کاربرد هوش مصنوعی در پشتیبانی تصمیم نظامی هم‌خوان است؛ الگویی که سرعت واکنش

1. Swarm Intelligence
2. Human-Machine Teaming

را افزایش می‌دهد و نقش انسان را به ارزیابی و تأیید تصمیم نزدیک می‌کند (Szabadföldi, 2021).

در سطح عملیات نقطه‌ای علیه اهداف ارزشمند نیز، هوش مصنوعی می‌تواند با تحلیل داده‌های تصویری، ارتباطی، رفتاری و مکانی، احتمال حضور هدف را ارزیابی و زمان مناسب حمله را پیشنهاد کند. جمع‌بندی این محور نشان می‌دهد هوش مصنوعی در سطح عملیاتی، موجب کوتاه‌سازی زنجیره کشتار، افزایش دقت و هماهنگی حمله، تقویت غافل‌گیری تاکتیکی و کاهش ریسک نیروهای خودی شده است. بااین‌حال، حرکت به سمت «خودکارسازی مرگبار»[1]، پرسش‌های مهمی درباره کنترل انسانی، مسئولیت تصمیم و خطای الگوریتمی ایجاد می‌کند (Hendrycks et al., 2025).

۳-۳. نقش دفاعی: هوشمندسازی پدافند هوایی، ضد موشکی و ضدپهپادی

نقش سوم هوش مصنوعی در جنگ ۱۲ روزه، هوشمندسازی پدافند هوایی، ضدموشکی و ضدپهپادی بود. رژیم صهیونیستی در سال‌های گذشته بر هوشمندسازی سپرهای دفاع موشکی خود سرمایه‌گذاری کرده و لایه‌هایی مانند «گنبد آهنین»[2]، «پیکان»[3] و «فلاخن داوود»[4] را با ارتقاهای نرم‌افزاری و تحلیلی همراه ساخته است. در این سامانه‌ها، هوش مصنوعی در تشخیص و طبقه‌بندی هدف، تفکیک اهداف واقعی از کاذب، پیش‌بینی مسیر و ادغام داده‌های راداری و حسگری نقش دارد.

کارکرد اصلی هوش مصنوعی در این محور، کاهش زمان واکنش و بهینه‌سازی مصرف منابع رهگیری است. مدل‌های پیش‌بینی مسیر، نقطه برخورد احتمالی موشک را برآورد می‌کنند و به سامانه دفاعی امکان می‌دهند رهگیرها را بر تهدیدهای واقعاً خطرناک متمرکز کند. همچنین همجوشی داده‌های رادارها، حسگرهای الکترواپتیکی، داده‌های ماهواره‌ای و هشدارهای هم‌پیمانان، تصویر دقیق‌تری از مسیر و سطح تهدید فراهم می‌سازد.

1. Lethal Automation
2. Iron Dome
3. Arrow
4. David’s Sling

در حوزه ضدپهپادی نیز سامانه‌هایی مانند «درون دوم»[1] و «درون گارد»[2] با ترکیب رادار، حسگرهای اپتیکی و صوتی و تحلیل هوشمند، الگوی حرکت پهپادها را تشخیص داده و با اختلال در سامانه «موقعیت‌یابی جهانی»[3]، جنگ الکترونیک یا ابزارهای سخت‌کُش با آن‌ها مقابله می‌کنند؛ بنابراین، الگوی کلان این محور را می‌توان «مزیت دفاعی مبتنی بر پیش‌بینی و ادغام داده» دانست؛ هرچند شلیک اشباع، موشک‌های مانورپذیر و محدودیت منابع رهگیری همچنان از چالش‌های اصلی پدافند هوشمند به شمار می‌روند.

۳-۴. نقش سایبری: تقویت عملیات سایبری و کنش‌های مکمل

پیش‌بینی می‌شد در جنگ تمام‌عیار میان ایران و رژیم صهیونیستی، جبهه سایبری نقشی هم‌تراز جبهه فیزیکی ایفا کند؛ اما بررسی‌ها نشان می‌دهد بعد سایبری جنگ ۱۲ روزه، برخلاف انتظار، محدود بود. فعالیت‌هایی از نفوذ و خرابکاری سایبری تا عملیات روانی در فضای مجازی مشاهده شد؛ اما هیچ‌یک ضربه‌ای تعیین‌کننده وارد نکردند و بیشتر نقشی مکمل، اختلالی یا تبلیغاتی داشتند و شواهد بررسی‌شده از تغییر قاطع نتیجه نظامی جنگ بر اثر این عملیات حکایت ندارند (Shah, 2025).

در این جنگ، موجی از حملات نفوذگرانه و حملات «منع خدمت توزیع‌شده»[4] علیه وب‌سایت‌ها و خدمات برخط دو طرف مشاهده شد. نفوذ به خدمات مالی و رمزارزی، پیام‌سازی راهبردی و عملیات روانی دیجیتال نیز بخشی از صحنه سایبری جنگ را تشکیل داد. با وجود این، این حملات تعیین‌کننده سرنوشت جنگ نبودند و موشک‌ها، پدافند و عملیات فیزیکی، محور اصلی میدان باقی ماندند.

هوش مصنوعی در حوزه سایبری می‌تواند از طریق شخصی‌سازی حملات «فریب‌کارانه»[5]، خودکارسازی بدافزارها، تحلیل رفتار شبکه، کشف آسیب‌پذیری‌ها و مقیاس‌دهی عملیات سایبری نقش‌آفرینی کند. همچنین مدل‌سازی ساختار شبکه، شناسایی مسیرهای حمله و

1. Drone Dome
2. Drone Guard
3. Global Positioning System (GPS)
4. Distributed Denial of Service (DDoS)
5. Phishing

انتخاب پویای راهبردهای دفاعی، از ظرفیت‌های هوش مصنوعی در دفاع سایبری است (Wang et al., 2025)؛ بنابراین، هرچند عملیات سایبری جنگ ۱۲ روزه اختلال و خسارت غیرنظامی ایجاد کرد، شواهد موجود برای انتساب همه این رویدادها به هوش مصنوعی یا اثبات تغییر قاطع نتیجه نظامی بر اثر آن‌ها کافی نیست؛ بااین‌حال، ظرفیت هوش مصنوعی برای افزایش مقیاس و سرعت کنش‌های سایبری در آینده جدی است (Shah, 2025; Wang et al., 2025). شرط تعیین‌کنندگی این نقش، ایجاد پیوند عملیاتی میان عملیات سایبری و میدان فیزیکی است؛ در غیر این صورت، نقش آن عمدتاً در سطح اختلال، فرسایش و پیام‌سازی باقی می‌ماند.

۳-۵. جمع‌بندی تحلیلی یافته‌ها

در سطح تجمیعی، چهار محور فوق یک الگوی مشترک را نشان می‌دهند: هوش مصنوعی در این جنگ عمدتاً نقش شتاب‌دهنده و ضرب‌کننده قوا را ایفا کرده است. این نقش از طریق ادغام داده و تولید هدف، کوتاه‌سازی زنجیره کشتار و خودکارسازی اقدام، بهینه‌سازی تصمیم دفاعی بر پایه پیش‌بینی و همجوشی داده، و تقویت کنش‌های سایبری بروز یافته است.

جدول ۳: سیر نقش‌آفرینی هوش مصنوعی در جنگ ۱۲ روزه از داده تا اثر

مراحل دفاعی-امنیتی	نقش غالب	مؤلفه محوری	داده‌های ورودی	سازوکار نقش‌آفرینی	خروجی‌های فوری	اثر عملیاتی و راهبردی
۱. انباشت داده و دسترسی	نقش ۱	تأمین داده خام، دسترسی میدانی	داده سیگنالی، تصویری، مالی، ارتباطی، رفتاری، میدانی، شبکه نفوذ انسانی	ایجاد بستر داده چندمنبعی قابل اتکا برای تحلیل ماشینی و هدف سازی	بانک داده چندمنبعی، دسترسی‌های فوری به سطوح تحلیل‌گران	افزایش ظرفیت هدف سازی، زمینه‌سازی غافل‌گیری اولیه
۲. پردازش، همجوشی، هدف سازی	نقش ۱	جست وجوی هم‌زمان،	شنود، رهگیری بی‌سیم،	کاوش هم‌زمان چندمنبعی و کشف الگو در	فهرست اهداف اولویت‌دار، مکان‌یابی و	کوتاه سازی چرخه شناسایی تا

مراحل دفاعی- امنیتی	نقش غالب	مؤلفه محوری	داده‌های ورودی	سازوکار نقش‌آفرینی	خروجی‌های فوری	اثر عملیاتی و راهبردی
		اتصال سرنخ‌ها، رتبه‌بندی اهداف	ماهواره، داده مالی و ارتباطی	زمان کوتاه توسط گاسپل و امتیازدهی تهدید و رتبه‌بندی افراد، شبکه‌ها و انسان‌ها توسط لاوندر	زمان‌بندی، شناسایی موفق حدود ۸۷ درصد اهداف ارزشمند	انهدام، تقویت ضربه نخست
۳. تصمیم یاری، تخصیص اقدام	نقش ۱ و ۲	برنامه‌ریزی حمله، تخصیص سکو، تخصیص سلاح	اهداف اولویت‌دار، داده به روز، محدودیت‌های زمانی	تبدیل خروجی هوش مصنوعی به بسته اقدام عملیاتی. طرح زنجیره کشتار ۶۰ ثانیه‌ای. پردازش روزانه ۱۰۰ ترابایت، تولید صدها هدف با دقت بالای ۹۰ درصد	برنامه حمله زمان‌بندی شده، تخصیص سریع و هوشمند سلاح و مهمات	افزایش «آهنگ عملیات»[1]، کاهش فرصت واکنش، نابودی اهداف ارزشمند در ساعات اولیه
۴. اقدام تهاجمی	نقش ۲	پهپاد خودمختار از درون، تلفیق جنگنده، پهپاد، ترور،	پهپاد قاچاق شده، مسیر نفوذ، داده زنده پهپادی، اطلاعات انسانی	ازدحام پهپادی برای اشباع رادار و ایجاد حفره پدافندی. بهینه‌سازی مسیر، هماهنگی خودمختار	ایجاد حفره پدافندی، حملات دقیق هم‌زمان، ترور، انهدام اهداف ارزشمند	کوتاه‌سازی زنجیره کشتار، افزایش دقت و غافل‌گیری، کاهش ریسک

1. Tempo

مراحل دفاعی- امنیتی	نقش غالب	مؤلفه محوری	داده‌های ورودی	سازوکار نقش‌آفرینی	خروجی‌های فوری	اثر عملیاتی و راهبردی
		انهدام نقطه‌ای		(هوش ازدحامی)؛ فرماندهی و کنترل هوشمند برای تقسیم نقش، پیشنهاد مسیر امن، کمک به قفل هدف؛ تلفیق اطلاعات انسانی و تحلیل بلادرنگ برای تأیید حضور هدف و زمان حمله و رساندن ۴۳ درصد عملیات به مرحله کاملاً خودکار (اتوماسیون مرگبار)		نیروهای خودی
۵. دفاع هوشمند و مدیریت رهگیری	نقش ۳	تشخیص، پیش‌بینی مسیر، همجوشی داده، حسگرهای	رادارها، اپتیک، صوت، هشدار ماهواره، داده هم پیمان	بینایی ماشین برای تفکیک تهدید واقعی. پیش‌بینی نقطه برخورد برای اولویت‌بندی. همجوشی	کاهش زمان واکنش، تخصیص بهینه مهمات رهگیر، انهدام یا انحراف بخشی از پهپادها	مزیت دفاعی مبتنی بر پیش‌بینی و ادغام داده، کاهش خسارت نسبت به

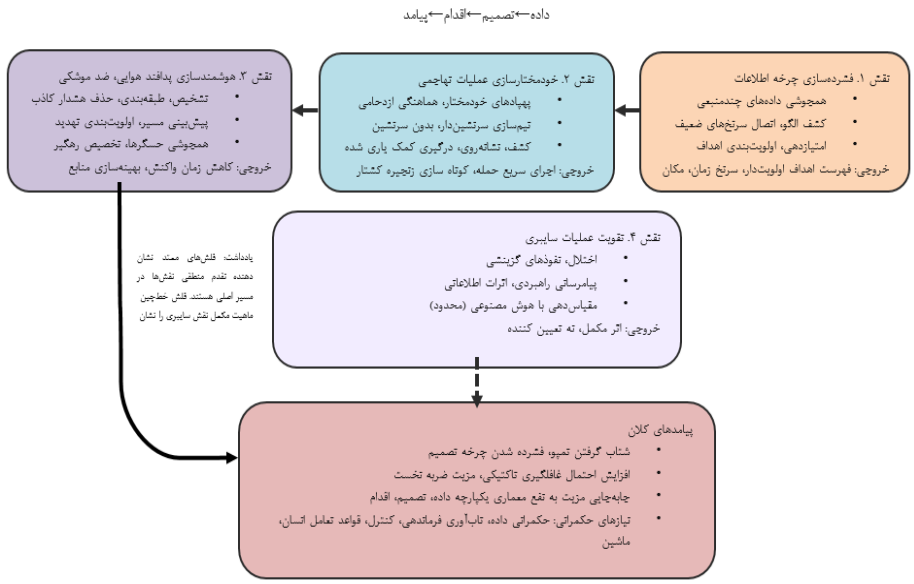
مراحل دفاعی- امنیتی	نقش غالب	مؤلفه محوری	داده‌های ورودی	سازوکار نقش‌آفرینی	خروجی‌های فوری	اثر عملیاتی و راهبردی
		متصل، ضدپهپادی		چندحسگر. هاب هوش مصنوعی در «ماتسپن»[1] برای غربال هشدار. شبکه اینترنت اشیا و اشتراک داده پیکان و رادارهای همکار. ضدپهپادی با درون دوم و درون گارد		حالت بدون هوش مصنوعی، باقی ماندن چالش اشباع و موشک‌های مانورپذیر
۶. سایبر مکمل	نقش ۴	اختلال، نفوذ مالی، جنگ روانی، تقویت مقیاس با هوش مصنوعی	وب سایت‌ها، خدمات آنلاین، بانک، رمزارز، شبکه اجتماعی	حملات عمدتاً DdoS و حضور گسترده گروه‌ها. نفوذهای شاخص به خدمات مالی و رمزارزی با اثر اختلالی روانی. نقش تقویتی در فیشینگ، عملیات روانی و خودکارسازی ابزارها	اختلال موقت، پیام سازی راهبردی	اثر مکمل و ظرفیت شگفتی‌سازی در جنگ آینده

1. Matspen

مراحل دفاعی- امنیتی	نقش غالب	مؤلفه محوری	داده‌های ورودی	سازوکار نقش‌آفرینی	خروجی‌های فوری	اثر عملیاتی و راهبردی
۷. اثر نهایی راهبردی	نقش‌های ۱ تا ۳	جمع‌بندی بین محوری	برتری داده، الگوریتم، فرماندهی و کنترل، حسگرها، خودمختاری عملیاتی	فشرده‌سازی زمان تصمیم و اقدام، تغییر آهنگ عملیات، تقویت ضربه نخست از مسیر تولید هدف سریع و اجرای هماهنگ	بازتعریف موازنه در سطح معماری داده‌محور	جابه‌جایی موازنه به نفع طرف دارای معماری یکپارچه داده، تصمیم و اقدام

این سازوکارها نشان می‌دهند مزیت اصلی هوش مصنوعی نه در یک فناوری منفرد، بلکه در معماری داده – الگوریتم – فرماندهی و کنترل – سکوهای عملیاتی و توان تبدیل داده به اقدام در زمان کوتاه نهفته است. از این منظر، هوش مصنوعی یک عرصه مستقل جنگ نیست، بلکه بستری است که ابزارهای اطلاعاتی، امنیتی، دفاعی و عملیاتی را تقویت و دگرگون می‌کند.

در این راستا نسبت چهار محور نقش‌آفرینی هوش مصنوعی در جنگ ۱۲ روزه را می‌توان در شکل(۲)، خلاصه و جمع‌بندی نمود.



شکل ۲: جمع‌بندی چهار محور یافته‌ها

۴. نتیجه‌گیری و پیشنهاد

۴-۱. پاسخ به سؤال‌های تحقیق

مسیر استنتاج پاسخ‌ها در جدول (۲)، قابل ردیابی است. کدهایی مانند «همجوشی داده‌های چندمنبعی»، «امتیازدهی تهدید»، «خودکارسازی تصمیم»، «فشرده‌سازی زنجیره کشتار»، «هوش ازدحامی»، «تیم‌سازی انسان–ماشین»، «پیش‌بینی مسیر»، «بهینه‌سازی مصرف رهگیر» و «اختلال کوتاه‌مدت»، پس از تجمیع در زیرمقوله‌های تفسیری، به چهار نقش نهایی نگاشت شدند. جدول (۳)، نیز نسبت این نقش‌ها را در فرایند تبدیل داده خام به اثر عملیاتی و راهبردی نشان می‌دهد.

۴-۱-۱. هوش مصنوعی در حوزه اطلاعاتی و هدف‌یابی جنگ ۱۲ روزه چه نقشی داشته است؟

تحلیل شواهد مربوط به سؤال فرعی نخست نشان داد که مهم‌ترین نقش اطلاعاتی هوش مصنوعی، کاهش زمان و افزایش ظرفیت تبدیل داده‌های پراکنده به سرنخ‌ها و اهداف قابل

اقدام بوده است. در جدول (۲)، شواهد مربوط به تجمیع داده‌های شنودی، ماهواره‌ای، تصویری، مالی، رفتاری و اطلاعات انسانی، زیرکدهای «همجوشی داده‌های چندمنبعی»، «غربالگری خودکار» و «کشف الگو» سازمان‌دهی شدند و به زیرمقوله «ایجاد تصویر اطلاعاتی یکپارچه و تبدیل داده خام به سرنخ هدف‌ساز» انجامیدند.

در سطح بعد، کدهای «امتیازدهی تهدید»، «اولویت‌بندی هدف»، «تولید بانک اهداف پویا» و «خودکارسازی تصمیم» نشان دادند که سامانه‌هایی مانند گاسپل و لاوندر تنها ابزار ذخیره یا بازیابی اطلاعات نبودند، بلکه در رتبه‌بندی اهداف و تولید فهرست‌های اولویت‌دار نقش داشتند؛ بنابراین، هوش مصنوعی با اتصال سرنخ‌های پراکنده، کاوش هم‌زمان داده‌های چندمنبعی و اولویت‌بندی اهداف، مدار اطلاعاتی را فشرده و فاصله میان شناسایی و هدف‌سازی را کاهش داده است. بااین‌حال، این نتیجه به معنای استقلال کامل الگوریتم‌ها از داده‌های پیشینی و شبکه اطلاعات انسانی نیست؛ بلکه کارایی آن‌ها به کیفیت داده، دسترسی میدانی و اتصال خروجی تحلیلی به ساختار فرماندهی وابسته بوده است.

۴-۱-۲. هوش مصنوعی چگونه در خودمختارسازی و هوشمندسازی عملیات تهاجمی نقش‌آفرینی کرده است؟

شواهد مرتبط با سؤال فرعی دوم در دو زیرمقوله اصلی سازمان‌دهی شدند. زیرمقوله نخست، «اتصال خروجی اطلاعاتی به تصمیم و اقدام عملیاتی» بود که از کدهایی مانند «تصمیم‌یاری بلادرنگ»، «فرماندهی و کنترل هوشمند»، «تخصیص سکو و سلاح»، «پیشنهاد تاکتیکی» و «هماهنگی چندسکویی» شکل گرفت. این مجموعه نشان می‌دهد خروجی سامانه‌های اطلاعاتی در قالب بسته‌های عملیاتی، مسیرهای پیشنهادی، تخصیص مهمات و زمان‌بندی حمله به یگان‌های رزمی منتقل شده است.

زیرمقوله دوم، «خودمختارسازی عملیات تهاجمی» بود که کدهای «هوش ازدحامی»، «هماهنگی پهپاد و جنگنده»، «تیم‌سازی انسان-ماشین» و «خودکارسازی مرگبار» را دربرگرفت. براین‌اساس، نقش هوش مصنوعی در عملیات تهاجمی تنها جایگزینی انسان با ماشین نبود؛ بلکه تقسیم کار میان حسگرها، سامانه‌های تحلیل، پهپادها، جنگنده‌ها و عامل

انسانی را بازآرایی کرد. نتیجه این بازآرایی، کاهش فاصله میان کشف و درگیری، افزایش هماهنگی چندسکویی و فراهم‌شدن امکان اجرای هم‌زمان حملات نقطه‌ای بود. درعینِ‌حال، باقی‌ماندن انسان در مرحله تأیید نهایی، لزوماً به معنای کنترل انسانی مؤثر نیست و می‌تواند در برخی موارد به تأییدی شکلی و متکی بر خروجی الگوریتم تبدیل شود.

۴-۱-۳. هوش مصنوعی چه نقشی در هوشمندسازی پدافند هوایی، ضدموشکی و ضدپهپادی داشته است؟

در پاسخ به سؤال فرعی سوم، شواهد اسنادی در دو دسته مکمل قرار گرفتند. دسته نخست به کدهای «تشخیص خودکار هدف»، «تفکیک هدف واقعی از کاذب»، «پیش‌بینی مسیر»، «اولویت‌بندی تهدید» و «بهینه‌سازی مصرف رهگیر» مربوط بود. این کدها نشان می‌دهند که هوش مصنوعی در کاهش هشدارهای کاذب، تخمین مسیر و نقطه احتمالی برخورد و تصمیم‌گیری درباره تخصیص رهگیر نقش داشته است.

دسته دوم شامل «همجوشی چندحسگری»، «شبکه حسگر هوشمند»، «ردیابی پیوسته» و «دفاع ضدپهپادی» بود. ترکیب داده‌های راداری، الکترواپتیکی، صوتی، حرارتی و ماهواره‌ای، امکان ایجاد تصویری منسجم‌تر از تهدید را فراهم می‌کرد؛ بنابراین، نقش دفاعی هوش مصنوعی را می‌توان «مزیت دفاعی مبتنی بر پیش‌بینی و ادغام داده» دانست. این مزیت مطلق نبوده و با محدودیت‌هایی مانند شلیک اشباع، موشک‌های مانورپذیر، ظرفیت محدود رهگیرها و امکان فریب حسگرها مواجه است. ازاین‌رو، هوشمندسازی پدافند به معنای حذف آسیب‌پذیری دفاعی نیست، بلکه به معنای افزایش سرعت و کیفیت تخصیص منابع دفاعی است.

۴-۱-۴. هوش مصنوعی چگونه عملیات سایبری و کنش‌های مکمل در فضای دیجیتال را تقویت کرده است؟

تحلیل سؤال فرعی چهارم نشان داد که باید میان «افزایش ظرفیت عملیات سایبری» و «تعیین‌کنندگی راهبردی آن» تمایز گذاشت. کدهایی مانند «مقیاس‌دهی حمله»، «خودکارسازی

نفوذ»، «فیشینگ هوشمند»، «نفوذ مالی» و «عملیات روانی دیجیتال»، از ظرفیت هوش مصنوعی برای افزایش سرعت، حجم و شخصی‌سازی کنش‌های سایبری حکایت دارند.

بااین‌حال، کدهای «اختلال کوتاه‌مدت»، «اثر روانی»، «عدم تعیین‌کنندگی مستقل» و «گسست سایبر و میدان فیزیکی» نشان دادند که بخش عمده عملیات سایبری مشاهده‌شده نتوانسته است جریان اصلی عملیات نظامی را متوقف یا نتیجه جنگ را به‌طور قاطع تغییر دهد. ازاین‌رو، پاسخ به سؤال چهارم آن است که هوش مصنوعی ظرفیت عملیاتی و مقیاس کنش‌های سایبری را افزایش داده، اما اثر این نقش در جنگ ۱۲ روزه عمدتاً مکمل، محدود و مشروط به پیوند آن با عملیات فیزیکی بوده است.

۴-۱-۵. نقش‌آفرینی هوش مصنوعی در این جنگ چه دلالت‌هایی برای سیاست‌گذاری دفاعی-امنیتی ج.ا. ایران در برابر جنگ‌های آینده دارد؟

در پاسخ به سؤال پنجم، نخستین دلالت آن است که واحد مناسب برنامه‌ریزی دفاعی، یک سامانه منفرد هوش مصنوعی نیست، بلکه معماری یکپارچه‌ای است که داده، حسگر، الگوریتم، فرماندهی و کنترل و سکوی عملیاتی را به یکدیگر متصل می‌کند. برخورداری از پهپاد، موشک، رادار یا نرم‌افزار هوشمند، بدون امکان تبادل داده و تبدیل سریع تحلیل به اقدام، مزیت پایدار ایجاد نمی‌کند.

دلالت دوم، تبدیل «زمان» به یکی از متغیرهای محوری قدرت دفاعی است. یافته‌ها نشان دادند که مزیت اصلی هوش مصنوعی در بسیاری از موارد نه تولید قابلیتی کاملاً جدید، بلکه کاهش زمان گردآوری، تحلیل، تصمیم‌گیری، تخصیص و اجرا بوده است؛ بنابراین، شکاف راهبردی می‌تواند نه‌فقط از کمبود تجهیزات، بلکه از کندی گردش داده و تصمیم ناشی شود.

دلالت سوم، ضرورت توجه هم‌زمان به اثربخشی و تاب‌آوری است. هرچه چرخه تصمیم به داده‌ها و الگوریتم‌ها وابسته‌تر شود، مخاطراتی مانند آلودگی داده، فریب الگوریتم، اختلال ارتباطی، تمرکز فرماندهی، خطای خودکار و اتکای بیش از حد به خروجی ماشین نیز افزایش می‌یابد. درنتیجه، سیاست دفاعی باید توسعه توانمندی هوشمند را با تاب‌آوری فرماندهی و

کنترل، حفاظت داده، امکان عملکرد در شرایط قطع ارتباط و قواعد روشن تعامل انسان و ماشین همراه سازد.

۴-۱-۶. هوش مصنوعی در جنگ تحمیلی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه ج. ا. ایران، از منظر دفاعی-امنیتی چه نقش‌هایی ایفا کرده و چگونه چرخه اطلاعات، تصمیم و اقدام را متحول ساخته است؟

در پاسخ به سؤال اصلی تحقیق، برآیند تحلیل چهارچوبی نشان داد که نقش‌آفرینی هوش مصنوعی را نمی‌توان به کاربرد چند سامانه یا ابزار منفرد تقلیل داد؛ بلکه این فناوری در قالب معماری به‌هم‌پیوسته‌ای از داده، الگوریتم، فرماندهی و کنترل و سکوهای عملیاتی عمل کرده است. چهار نقش اطلاعاتی، عملیاتی، دفاعی و سایبری، اجزای این معماری را تشکیل می‌دهند، اما وزن و جایگاه آن‌ها یکسان نیست. سه نقش نخست در امتداد زنجیره اصلی «داده ـ تصمیم ـ اقدام» قرار دارند، درحالی‌که نقش سایبری در جنگ مورد مطالعه عمدتاً ماهیتی مکمل و تقویتی داشته است.

براین‌اساس، دلالت اصلی پژوهش آن است که رقابت آینده تنها بر سر برخورداری از «هوش مصنوعی بیشتر» نیست، بلکه بر سر ایجاد معماری قابل‌اعتمادتر، سریع‌تر و تاب‌آورتر برای تبدیل داده به تصمیم و اقدام خواهد بود.

۵. نتیجه‌گیری و پیشنهاد

یافته‌های این پژوهش، نتایج مطالعات پیشین درباره نقش هوش مصنوعی در پردازش سریع اطلاعات، تشخیص تهدید، تصمیم‌یاری و خودکارسازی عملیات نظامی را تأیید می‌کند، ولی از رویکرد فهرست کردن کاربردها و سامانه‌های منفرد فراتر رفته است. برخلاف پژوهش‌های گذشته که هر یک بر حوزه‌هایی مانند پردازش اطلاعات، فرماندهی و کنترل، امنیت سایبری یا سکوهای هوشمند تمرکز کرده‌اند، نتایج این تحقیق نشان می‌دهد اثر راهبردی هوش مصنوعی زمانی شکل می‌گیرد که داده‌های چندمنبعی، الگوریتم‌های تحلیلی، فرماندهی و کنترل و سکوهای عملیاتی در یک معماری به‌هم‌پیوسته قرار گیرند؛ بنابراین تولید یا

اولویت‌بندی هدف به‌تنهایی مزیت عملیاتی ایجاد نمی‌کند، بلکه این مزیت هنگامی حاصل می‌شود که خروجی تحلیل ماشینی به تصمیم، تخصیص سلاح و اجرای هماهنگ عملیات متصل شود.

این سازوکار را می‌توان براساس چرخه «مشاهده، جهت‌یابی، تصمیم و اقدام» تبیین کرد. نقش اطلاعاتی هوش مصنوعی با گسترش مشاهده و تسریع جهت‌یابی، داده‌های پراکنده را به تصویر عملیاتی و هدف تبدیل می‌کند؛ نقش عملیاتی، فاصله میان تصمیم و اقدام را از طریق تصمیم‌یاری، تخصیص سکو، هماهنگی انسان-ماشین و خودمختاری کاهش می‌دهد؛ و نقش دفاعی، چرخه تشخیص، پیش‌بینی، اولویت‌بندی و رهگیری را فشرده می‌سازد؛ بنابراین نتیجه اصلی پژوهش آن است که هوش مصنوعی در این جنگ مانند معماری فشرده‌ساز چرخه تصمیم عمل کرده و مزیت آن نه در سرعت یک سامانه، بلکه در کاهش فاصله و اصطکاک میان مراحل چرخه تصمیم بوده است.

نوآوری پژوهش، ارائه صرف یک دسته‌بندی چهارمحوری نیست، بلکه صورت‌بندی یک مدل تحلیلی فرایندی و ناهم‌وزن است که نقش‌های اطلاعاتی، عملیاتی، دفاعی و سایبری را براساس جایگاه آن‌ها در چرخه تصمیم تبیین می‌کند و واحد تحلیل را از «سامانه منفرد» به «معماری یکپارچه داده-تصمیم-اقدام» انتقال می‌دهد. براین‌اساس، برخورداری از هوش مصنوعی شرط لازم، اما ناکافی برای برتری است و مزیت پایدار به‌سرعت، یکپارچگی، تاب‌آوری و قابلیت کنترل این معماری وابسته خواهد بود.

۵-۱. پیشنهادهای پژوهش

پیشنهادهای این بخش، صورت اجرایی دلالت‌های تحلیلی استخراج‌شده در پاسخ به سؤال پنجم‌اند. دلالت‌های مذکور ضرورت حرکت از رویکرد سامانه‌محور به معماری یکپارچه داده ـ تصمیم ـ اقدام، کاهش زمان چرخه تصمیم و افزایش تاب‌آوری زیرساخت‌های هوشمند را نشان دادند. بر این مبنا، پیشنهادهای زیر در دو دسته ارائه می‌شوند.

الف. پیشنهادهایی به فرماندهان و مدیران

۱. طراحی و استقرار آزمایشی زنجیره یکپارچه داده ـ تصمیم ـ اقدام توسط ستاد کل نیروهای مسلح با مشارکت وزارت دفاع و سازمان‌های اطلاعاتی نیروهای مسلح؛
۲. ایجاد معماری توزیع‌شده و تاب‌آور فرماندهی و کنترل همراه با مسیرهای ارتباطی جایگزین و قابلیت بازیابی سریع، توسط ستاد کل نیروهای مسلح و سازمان پدافند غیرعامل؛
۳. توسعه شبکه چندحسگری، همجوشی بلادرنگ داده‌ها و تخصیص هوشمند رهگیرها توسط قرارگاه خاتم‌الانبیا با پشتیبانی وزارت دفاع و نیروی هوافضای سپاه؛
۴. تدوین و ابلاغ چهارچوب ممیزی الگوریتم، ثبت مسیر تصمیم و حفظ کنترل معنادار انسان در سامانه‌های هوش مصنوعی رزمی توسط ستاد کل نیروهای مسلح و وزارت دفاع؛
۵. راه‌اندازی برنامه پژوهشی-آزمایشی مقابله با فریب حسگرها، آلودگی داده و حملات خصمانه به الگوریتم‌ها در مراکز پژوهشی و دانشگاه‌های دفاعی تحت هدایت وزارت دفاع و ستاد کل نیروهای مسلح.

ب. پیشنهادهایی به پژوهشگران برای تحقیقات آینده

۱. بررسی تطبیقی نقش هوش مصنوعی در جنگ ۱۲ روزه با جنگ‌های دیگر مانند اوکراین و غزه، برای سنجش میزان تعمیم‌پذیری الگوی چهارمحوری پژوهش؛
۲. مطالعه دقیق‌تر درباره نسبت کنترل انسانی، اتوماسیون مرگبار و مسئولیت حقوقی در سامانه‌های هوش مصنوعی رزمی؛
۳. بررسی آسیب‌پذیری‌های داده‌ای، فریب الگوریتمی، آلودگی داده و حملات خصمانه به شبکه‌های حسگری و سامانه‌های تصمیم‌یار دفاعی.

۵-۲. محدودیت‌های پژوهش

۱. محدودیت جدی در داده‌های مرتبط با نقش‌های دفاعی–امنیتی هوش مصنوعی در دنیا و نزدیک بودن زمان واقعه جنگ ۱۲ روزه، موجب محدودیت در منابع قابل استفاده شد؛

۲. به‌دلیل تازه بودن رخداد جنگ ۱۲ روزه، هنوز پژوهش‌های علمی کافی درباره ابعاد دفاعی–امنیتی هوش مصنوعی در این جنگ شکل نگرفته است؛

۳. وجود داده‌های طبقه‌بندی‌دار و عدم امکان ارائه همه مستندات مسیر سپری‌شده در تحلیل داده‌ها، از مهم‌ترین محدودیت‌ها در عرضه نتایج پژوهش حاضر است؛

۴. ازاین‌رو، یافته‌های پژوهش باید در چهارچوب داده‌های آشکار، اسناد قابل دسترس و نظر خبرگان تلقی شود.

فهرست منابع

رهبر معظم انقلاب (۱۴۰۴). سخنرانی تلویزیونی خطاب به ملت ایران در ۱۴۰۴/۰۹/۰۶.

نورمحمدی، مرتضی؛ تقی‌پور جاوی، تیرداد (۱۴۰۴). ***تأثیر هوش مصنوعی بر ماهیت جنگ‌های آینده***. فصلنامه محیط‌شناسی راهبردی ج.ا.ایران، ۹ (۱).

عباسی، مصطفی؛ کشوری، سامان؛ کشوری، عبدالرحمن؛ حسنی آهنگر، محمدرضا (۱۳۹۶). ***تهدیدشناسی امنیت فضای سایبری حوزه دفاع موشکی در پسا برجام***. فصلنامه پژوهش‌های حفاظتی امنیتی، ۶ (۲۲).

کشوری، سامان؛ حسنی آهنگر، محمدرضا؛ کشوری، ساناز (۱۳۹۶). ***استفاده از روش برنامه‌نویسی پدافندی جهت افزایش امنیت نرم‌افزار در زبان C#***. پدافند غیرعامل، ۸ (۳).

رستمی، محسن (۱۴۰۱). ***شناسایی و معرفی ظرفیت‌های کاربردی هوش مصنوعی در توسعه مضمون‌های راهبردی در سازمان‌های نظامی***. فصلنامه علمی راهبرد دفاعی، سال ۲۰، شماره ۷۸.

اسماعیلی، حمید؛ میارعباسی، ابوذر (۱۴۰۳). ***بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی-امنیتی جمهوری اسلامی ایران***. فصلنامه علمی راهبرد دفاعی، سال ۲۲، شماره ۸۶.

عظیمی‌زاده، حمید؛ سپهری، محمد؛ هلیلی، خداداد؛ نقوی، احد (۱۴۰۴). ***طراحی الگوی فرماندهی و کنترل هوشمند ارتش جمهوری اسلامی ایران مبتنی بر کلان‌داده***. فصلنامه علمی راهبرد دفاعی، سال ۲۳، شماره دوم، پیاپی ۹۰.

References

Srivastava, A., & Thomson, S. B(2009) amework analysis: A qualitative methodologyFr

Abraham, Y. (2023, November 30). 'A mass assassination factory': Inside Israel's calculated bombing of Gaza. +972 Magazine.

Abraham, Y. (2024, April 3). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. +972 Magazine.

Al Jazeera. (2025, June 23). How extensive are Israel's intelligence operations inside Iran? Al Jazeera.

Alam, F. (2025, June 29). How AI shaped the Iran-Israel 12-day war. The Daily Star.

Frankel, J., & Mednick, S. (2025, June 17). How Israel used spies, smuggled drones and AI to stun and hobble Iran. The Times of Israel.

Gosselin-Malo, E. (2025, February 20). Iron Dome unsuitable as missile shield for US or Europe, officials say. Defense News.

Israel Ministry of Defense. (2025, July 1). Israel MOD concludes evaluation of advanced systems performance in Operation Rising Lion.

Jensen, B. (2025, June 13). Ungentlemanly robots: Israel's Operation Rising Lion and the new way of war. Center for Strategic and International Studies.

Mahamad, A. (2025, July 3). The shadow war: How Israel's Mossad infiltrated Iran's security apparatus. IranWire.

McKernan, B., & Davies, H. (2024, April 3). 'The machine did it coldly': Israel used AI to identify 37,000 Hamas targets. The Guardian.

McNabb, M. (2025, June 23). The silent invasion: How Israel's small drones infiltrated Iran. DroneLife.

Motamedi, M. (2025, June 26). How Israel launched attacks from inside Iran to sow chaos during war. Al Jazeera.

Roblin, S. (2025, June 30). How did Israel's air defenses fare against Iran's ballistic missiles? Forbes.

Satter, R. (2025, January 31). Meta's WhatsApp says spyware company Paragon targeted users in two dozen countries. Reuters.

Sexton, M. (2025, August 25). AI and the evolution of asymmetric cyber warfare: Insights from the 2025 Israel-Iran conflict. TRENDS Research & Advisory.

Shah, N. (2025, July 30). What the Israel-Iran conflict revealed about wartime cyber operations. Atlantic Council.

Vasques, E. (2025, June 13). Israel's Mossad mounted high-tech covert operation to strike targets deep inside Iran, sources say. Euronews.

Wald, C., Fox, M., Ashley, R., Misztal, B., Cicurel, A., Tobin, Y., Brody, J., Havdala, S., & Gabber, R. (2025, November 20). Operation Rising Lion: Insights from Israel's 12-day war against Iran. Jewish Institute for National Security of America.

The Times of Israel. (2025, June 13). Mossad set up drone base in Iran, UAVs took out missile launchers overnight. The Times of Israel.

Military.com. (2025, June 17). Israel's spy agency used AI and smuggled-in drones to prepare attack on Iran. Military.com.