Quarterly Journal Defensive Future Studies
IRI Military Command and Staff University www.dfsc.ir Online ISSN: 2645-7172 Print ISSN: 2588-428x

Applying Artificial Intelligence in the execution of Electronic Warfare Operations of the Islamic Republic of Iran Army

alireza mohamadi[1] ✉ | **Morteza Talebi** [2] | **ali panahi** [3]

1. Instructor of Defense Management, IRI Military Command and Staff University, Tehran, Iran. Email: a.mohamadi33@casu.ac.ir
2. Assistant Professor of Strategic Management, IRI Military Command and Staff University, Tehran, Iran. Email: Pyan9288@gmail.com
3. Instructor of Defense Management, IRI Military Command and Staff University, Tehran, Iran. Email: alipanahi14@yahoo.com

Article Info

Article type:
Research Article

Article history:

Received:
2024-10-28
Received in revised form:
2024-12-27
Accepted :
2025-1-12
Published online:
2025-5-22

Keywords:
Artificial Intelligence, execution, Electronic Warfare Operations

ABSTRACT

Objective: This study aims to clarify how artificial intelligence can be applied in electronic warfare operations by the Islamic Republic of Iran Army, considering the requirements and characteristics of future warfare.

Methodology: This applied research utilized a descriptive approach. The study's population included senior officers in the Islamic Republic of Iran Army, all holding at least a master's degree and possessing over twenty years of experience in fields such as telecommunications, electronic warfare, electronics, computer science, and other relevant areas. Additionally, perspectives from eight experts in the field were included.

Findings: The prioritization results reveal that using artificial intelligence to identify vulnerabilities in targeted systems is of the utmost importance. This is followed by the application of fuzzy systems and genetic algorithms in signal processing, which ranks second. The third priority is the use of intelligent design algorithms for gathering information on jammers and decoys.

Conclusion: The findings suggest that artificial intelligence can significantly enhance the effectiveness of electronic warfare operations conducted by the Islamic Republic of Iran Army. Key strategies for addressing future warfare challenges include focusing on vulnerability detection of target systems, utilizing advanced algorithms for signal processing, and collecting intelligence on threats.

Cite this article: Mohamadi, A. , Talebi, M. and Panahi, A. (2025). Applying Artificial Intelligence in the execution of Electronic Warfare Operations of the Islamic Republic of Iran Army. *Defensive Future Studies*, *10*(36), 137-166.

DOI: 10.22034/dfsr.2024.2044300.1844

Publisher: IRI Military Command and Staff University

Extended Abstract

Introduction:

The capabilities of artificial intelligence (AI) are currently at various stages of development and application. As AI technology continues to grow and enter the military sector, it is fundamentally transforming military operations. Recent advancements indicate that this emerging technology will have a significant and potentially transformative impact on the military power of any nation. AI can play a crucial role in various aspects of electronic warfare through algorithms that enhance capabilities, such as processing radar signals to identify and classify different types of transmitters, detecting the nature of jamming operations and their characteristics, and developing effective anti-jamming strategies.

Additionally, AI techniques can enable a range of systems to operate independently and decisively. Given that electronic warfare has become a key component of the battlefield, mastering the electromagnetic spectrum and information systems with the help of AI can lead to absolute dominance in military engagements. Moreover, AI can enhance the effectiveness of the electronic battlefield. The adverse effects of human error in complex operations are minimized because AI can quickly rectify its mistakes. When unexpected confrontations or unplanned scenarios arise, AI-driven systems can adapt swiftly to changing conditions.

Methodology:

The research conducted in this study is of an applied nature. The researcher collected factual information, distinct from subjective interpretations of phenomena, and identified and examined the relevant factors and current situation without any personal bias or inference. Based on the findings, the study explores how to utilize artificial intelligence in the execution of electronic warfare operations for the Islamic Republic of Iran's Army in the context of future conflicts. Therefore, the research method employed is descriptive.

Results:

In future conflicts, it is essential to plan for the utilization of all artificial intelligence tools at every level for attack, support, and electronic protection. The findings show that 89.45% of the surveyed population (an absolute majority) believes that artificial intelligence can be effectively used in various

aspects of electronic warfare operations, including electronic attack, electronic support, and electronic protection, with an average agreement score of 4.36. Based on the analysis of documents and interviews with research experts, the use of artificial intelligence in the electronic warfare operations of the Islamic Republic of Iran Army encompasses three main components: electronic attack, electronic support, and electronic protection. The results of the qualitative analysis derived from the document studies and expert interviews are as follows.

Indicators Calculated in the Electronic Attack Component:

- Application of machine learning algorithms and neural networks for automatic responses to electronic attacks.
- Utilization of artificial intelligence systems to determine the optimal timing and frequency for maximizing disruption and interference in enemy communications while minimizing power consumption.
- Employment of artificial neural networks to diagnose and identify types of disturbances, along with providing solutions for these disruptions.
- Use of artificial intelligence to uncover vulnerabilities in targeted systems.
- Implementation of artificial intelligence algorithms to design more accurate deceptive signals.
- Application of intelligent voice processing for creating fake communications and imitation deception.

Indicators Calculated in the Electronic Support Component:

- Utilizing Artificial Intelligence for Intelligent Information Analysis to create a Threat Bank and facilitate Intelligent Threat Pattern Detection.
- Employing artificial intelligence and machine learning capabilities to visualize the evolving situation and enhance situational awareness (understanding, visualizing, and predicting) through a comprehensive understanding of the electronic arrangement of the battlefield.
- Implementing artificial intelligence and machine learning algorithms to manage and analyze large amounts of data collected during electronic warfare in real time.
- Using the collected data model to predict attacks and propose suitable defensive and offensive solutions.
- Applying artificial intelligence and machine learning algorithms to detect and classify enemy signals.
- Leveraging Artificial Intelligence in Electromagnetic Spectrum Sensing.

- Applying intelligent design algorithms to gather information about disruptors and deceptive individuals.
- Utilizing Fuzzy Systems and Genetic Algorithms in Signal Processing.
- Implementing Natural Language Processing to analyze textual information from various sources.
- Employing artificial intelligence in data mining to integrate the collected data and signals.

Indicators Included in the Electronic Protection Component:

- Utilizing expert systems with deep learning for both positive and negative intelligent control.
- Employing expert systems and deep learning to prioritize and allocate frequencies.
- Implementing cognitive radiotherapy to establish a secure platform.
- Applying smart algorithms to thwart enemy deception operations.
- Leveraging deep learning algorithms for data analysis in cryptography.
- Using AI to intelligently implement, develop, and enhance anti-interference methods and disruptor detection.

The application of artificial intelligence (AI) in identifying vulnerabilities in attacked systems, along with the use of fuzzy systems and genetic algorithms in signal processing, plays a crucial role in modern electronic warfare. Additionally, intelligent design algorithms can be employed to gather information on disruptors and deceivers. These are the most significant ways AI is expected to be utilized in electronic warfare operations in future conflicts.

Discussion and Conclusion:

The integration of artificial intelligence (AI) in military operations, particularly in emerging conflicts, is becoming increasingly unavoidable. This is especially true for electronic warfare operations, where AI must be considered in all scenarios. In the near future, understanding and analyzing the electromagnetic spectrum without the aid of artificial intelligence will be extremely challenging, and electronic warfare operations may face significant setbacks as a result. Based on analysis prioritization, the use of artificial intelligence to identify vulnerabilities in targeted systems is the top priority. This is followed by the application of fuzzy systems and genetic algorithms for signal processing. Additionally, the use of intelligent design algorithms to gather information from jammers and decoys ranks as the third priority in future warfare scenarios.

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: ۲۵۸۸-۴۲۸X شاپای الکترونیکی: ۲۶۴۵-۷۱۲۳ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد آجا

به‌کارگیری هوش مصنوعی در اجرای عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران

علیرضا محمدی [۱]✉ | مرتضی طالبی [۲] | علی پناهی [۲]

۱. مربی مدیریت‌دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران، رایانامه: a.mohamadi33@casu.ac.ir
۲. استادیار مدیریت راهبردی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: Pyan9288@gmail.com
۳. مربی مدیریت‌دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران، رایانامه: alipanahi14@yahoo.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:
تاریخ دریافت:
۱۴۰۳/۰۸/۰۷
تاریخ بازنگری:
۱۴۰۳/۱۰/۰۷
تاریخ پذیرش:
۱۴۰۳/۱۰/۲۳
تاریخ انتشار:
۱۴۰۴/۰۳/۰۱

کلیدواژه‌ها:
هوش‌مصنوعی، اجرا، عملیات جنگ الکترونیک

چکیده

هدف: تبیین چگونگی به‌کارگیری هوش مصنوعی در اجرای عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران مبتنی بر الزامات و ویژگی‌های جنگ‌های آینده، هدف اصلی این مطالعه بوده است.

روش‌شناسی: این پژوهش از نوع کاربردی و با رویکرد توصیفی انجام شده است. جامعه آماری شامل افسران ارشد و بالاتر ارتش جمهوری اسلامی ایران با حداقل مدرک کارشناسی ارشد و بیش از بیست سال سابقه خدمت در حوزه‌های مرتبط با موضوع تحقیق است. همچنین از نظرات هشت نفر از متخصصان این حوزه استفاده شده است.

یافته‌ها: نتایج اولویت‌بندی مؤلفه‌ها نشان می‌دهد که به‌کارگیری هوش مصنوعی در تشخیص نقاط ضعف سیستم‌های مورد حمله، بالاترین اولویت را دارد. پس از آن، استفاده از سیستم‌های فازی و الگوریتم‌های ژنتیک در پردازش سیگنال در جایگاه دوم قرار می‌گیرد. همچنین، به‌کارگیری الگوریتم‌های طراحی هوشمند در جمع‌آوری اطلاعات اخلالگران و فریب‌دهنده‌ها، در اولویت سوم قرار دارد.

نتیجه‌گیری: بر اساس یافته‌های پژوهش، هوش مصنوعی می‌تواند نقش بسیار مؤثری در ارتقای اثربخشی عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران ایفا کند. تمرکز بر تشخیص نقاط ضعف سیستم‌های هدف، بهره‌گیری از الگوریتم‌های پیشرفته در پردازش سیگنال و جمع‌آوری اطلاعات از تهدیدات، از مهم‌ترین راهبردها برای مواجهه با چالش‌های جنگ‌های آینده محسوب می‌شود.

استناد: محمدی, علیرضا , طالبی, مرتضی و پناهی, علی . (۱۴۰۴). به‌کارگیری هوش مصنوعی در اجرا عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران. *آینده‌پژوهی دفاعی*، ۱۰(۳۶): ۱۶۶-۱۳۷.
DOI: 10.22034/dfsr.2024.2044300.1844

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

همراه با رشد فناوری اطلاعات و ارتباطات چهره جنگ‌های نظامی در دنیا نیز تغییر کرده و انواع جدیدی از جنگ‌ها پا به عرصه وجود گذاشته است. نیروهای نظامیِ مدرن به طرز چشمگیری به انواع مختلفی از فناوری‌های پیچیده و پیوسته در حال تحول برای به دست آوردن دست برتر با بهره‌گیری از تجهیزات الکترونیکی وابسته هستند. امروزه در هر سرزمینی توجه ویژه‌ای به گسترش و توسعه دانش طراحی و تولید دستگاه‌ها و مجموعه‌های وابسته به جنگ الکترونیک می‌شود، چراکه این حوزه دانشی به‌عنوان لبه فناوری در نظر گرفته می‌شود. فناوری‌های کلیدی مانند میکروالکترونیک، نانو فناوری و هوش مصنوعی در حال پیش بردن جوامع کنونی هستند که نقش عامل انسانی کم‌رنگ‌تر شود (نقی بیرانوند، ۱۴۰۱).

قابلیت‌های متفاوت و پیشرفته هوش مصنوعی در حال حاضر در مراحل مختلف توسعه و استفاده قرار دارند و با رشد فناوری هوش مصنوعی و ورود آن به حوزه نظامی، باعث تغییر شکل عملکرد نظامیان شده است. این امر به‌طور فراوانی جنگ‌ها و عملیات نظامی را در آینده دگرگون می‌کند به‌طوری‌که تحولات اخیر در هوش مصنوعی نشان می‌دهد که این فناوری در حال ظهور یک تأثیر قطعی و بالقوه دگرگون ساز بر قدرت نظامی در هر کشوری خواهد داشت (امیر جاوید، ۱۳۹۸).

سیستم‌های جنگ الکترونیک امروزی متکی به پایگاه داده تهدیدهای شناخته‌شده با اقدامات متقابل از پیش تعیین‌شده هستند که این موارد می‌تواند توانایی آن‌ها را در انطباق سریع و پاسخ به تهدیدات پیشرفته جدید محدود کند. به‌زودی، این سیستم‌ها ممکن است به‌طور فزاینده‌ای وظیفه جدا کردن سیگنال‌های ناشناخته دشمن را در محیط‌های الکترومغناطیسی متراکم داشته باشند و با اقدامات مقابله‌ای الکترونیکی سریع به آن‌ها پاسخ دهند. این روش، قدرت پردازش و حافظه سیستم قابل‌توجهی نیاز دارد. علاوه بر این، ایجاد و نگهداری پایگاه داده تهدید پرهزینه و زمان‌بر است و ظهور مداوم رادارهای پیشرفته مشکل را تشدید می‌کند. قابلیت‌های متفاوت و پیشرفته هوش مصنوعی در حال حاضر در مراحل مختلف توسعه و استفاده قرار دارند و با رشد فناوری هوش مصنوعی و ورود آن به حوزه نظامی، باعث تغییر شکل عملکرد نظامیان شده است. (Haigh,2020)

در عملیات جنگ الکترونیک به دلیل وابستگی تمام سیستم‌های نه‌گانه جنگ مانند فرماندهی و کنترل، اطلاعات و... به طیف الکترومغناطیس، عدم قطعیت در مراحل مختلف به‌شدت در حال افزایش است. باتوجه‌به این مطالب، اجرا عملیات جنگ الکترونیک با رویکرد سنتی مقدور نیست، به‌طوری‌که امکان فهم، درک، تجسم محیط عملیات جنگ الکترونیک، ایجاد آگاهی وضعیتی و تصمیم‌گیری را با چالش روبه‌رو کرده است. ازاین‌رو فرماندهان در جنگ‌های مدرن و پسامدرن با مسائل متعدد عملیات جنگ الکترونیک نظیر ناشناخته بودن ماهیت، کارکرد و ابعاد جنگ الکترونیک شناختی و مسائل عملیاتی، فنی و مدیریتی روبرو خواهند بود.

باتوجه‌به مطلب بیان‌شده فرایند عملیات جنگ الکترونیک در چهار مرحله شامل طرح‌ریزی، آماده‌سازی، اجرا و ارزیابی تعریف می‌شود (FM 3-36,2012).

در این تحقیق به تبیین چگونگی به‌کارگیری هوش مصنوعی در مرحله سوم یعنی اجرا عملیات جنگ الکترونیک در ارتش جمهوری اسلامی ایران پرداخته‌شده است که محقق در تلاش است با احصاء مؤلفه‌های آن به تشریح این مهم بپردازد.

سؤال اصلی پژوهش حاضر:

به‌کارگیری هوش مصنوعی در اجرا عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران چگونه باید باشد؟

و سؤالات فرعی پژوهش به شرح زیر مطرح می‌گردند:

۱) به‌کارگیری هوش مصنوعی در حمله الکترونیکِ عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران مبتنی بر جنگ‌های آینده چگونه باید باشد؟

۲) به‌کارگیری هوش مصنوعی در پشتیبانی الکترونیکِ عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران مبتنی بر جنگ‌های آینده چگونه باید باشد؟

۳) به‌کارگیری هوش مصنوعی در حفاظت الکترونیکِ عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران مبتنی بر جنگ‌های آینده چگونه باید باشد؟

مبانی نظری و پیشینه‌های پژوهش

پیشینه‌های پژوهش

پیشینه پژوهش نشان می‌دهد که هوش مصنوعی به‌عنوان یکی از فناوری‌های نوین، نقش مهمی در بهبود عملکرد دستگاه‌های نظامی ایفا می‌کند. در پایان‌نامه کارشناسی ارشد میر امیر پور موسوی (۱۴۰۱) با عنوان «کاربرد هوش مصنوعی در دستگاه‌های نظامی»

بررسی‌شده است که هوش مصنوعی با بهره‌گیری از سیستم‌های خبره، یادگیری ماشینی و بیگ دیتا می‌تواند سرعت، دقت و هوشمندی پدافند را افزایش دهد. این پژوهش نشان می‌دهد که با هوشمندتر و سریع‌تر شدن جنگ‌افزارها، فناوری پدافند نیازمند سیستم‌های تشخیص‌دهنده و عوامل هوشمند است تا پیش از بروز هرگونه مخاطره، اقدامات پیشگیرانه انجام شود.

در پژوهش دیگری توسط علی پناهی (۱۳۹۸) تحت عنوان «بررسی میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر فرایند تصمیم‌گیری عملیات جنگال در نبرد ناهمتراز» تأکید شده است که کسب اطلاعات الکترونیکی از صحنه نبرد، اطلاعات فنی سامانه‌ها و تجهیزات جنگ الکترونیک دشمن و سامانه‌های هدف، نقش مهمی در ارتقا و بهبود فرایند تصمیم‌گیری عملیات جنگال دارد. این امر به‌ویژه در نبردهای ناهمتراز که پیچیدگی‌های خاص خود را دارد، بسیار حیاتی است.

همچنین در چهاردهمین کنفرانس ملی مهندسی برق، کامپیوتر و مکانیک (۱۴۰۱)، مسلم نقی بیرانوند و محمدهادی مزیدی در پژوهشی با عنوان «به‌کارگیری هوش مصنوعی در سیستم‌های جنگ الکترونیک» بیان کردند که استفاده از هوش مصنوعی می‌تواند اجرای عملیات جنگ الکترونیک را به صورت مستقل و خودکفا تسهیل کند، آگاهی موقعیتی را افزایش دهد و به تصمیم‌گیری قابلیت اطمینان و اعتماد ببخشد. آن‌ها توضیح دادند که یک سیستم جنگ الکترونیک مبتنی بر هوش مصنوعی قادر است رادار متخاصم را به‌طور مؤثر شناسایی کرده، میزان تهدید آن را ارزیابی نموده و سپس استراتژی مقابله‌ای مناسبی را برای خنثی‌سازی تهدید طراحی و اجرا کند.

نوآوری پژوهش حاضر با عنوان در این است که این مطالعه به‌طور جامع و سیستماتیک به نحوه ادغام هوش مصنوعی در عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران می‌پردازد، به‌ویژه با تمرکز بر جنگ‌های آینده و چالش‌های نوظهور در این حوزه. این پژوهش با تحلیل دقیق و اولویت‌بندی مؤلفه‌های مختلف، نقش کلیدی هوش مصنوعی را در تشخیص نقاط ضعف سیستم‌های هدف، پردازش سیگنال‌های پیچیده با استفاده از الگوریتم‌های فازی و ژنتیک، و جمع‌آوری هوشمندانه اطلاعات از اخلالگران و فریب‌دهنده‌ها برجسته می‌کند. این رویکرد نوین، راهکاری عملی و استراتژیک برای ارتقای توانمندی‌های جنگ الکترونیک ارتش جمهوری اسلامی ایران ارائه می‌دهد و درنتیجه، موجب افزایش اثربخشی و پایداری عملیات در مواجهه با تهدیدات پیچیده و پیشرفته آینده می‌شود.

جنگ الکترونیک: به‌کارگیری طیف الکترومغناطیس برای کاهش عملکرد یا خراب کردن قابلیت رزمی دشمن، شامل پایین آوردن توانایی یا ممانعت از استفاده دشمن از طیف الکترومغناطیسی و نیز پایین آوردن عملکرد تجهیزات، کارکنان و امکانات دشمن و در مقابل، محافظت از توانایی رزمی خودی که می‌تواند در برابر اقدام الکترونیکی دشمن آسیب‌پذیر باشد (عفیفی و همکاران، ۱۳۸۵).

هوش مصنوعی: هوش مصنوعی به سامانه طراحی‌شده توسط انسان گفته می‌شود که برای حل یا مسئله پیچیده، محیط آن را به‌درستی درک کرده و با تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده، دانش موردنیاز را استخراج نموده و با تصمیم‌گیری در مورد بهترین اقدامات، به یک هدف از قبل مشخص‌شده در مسئله می‌رسد (نقشه راه توسعه ملی هوش مصنوعی، ۱۴۰۱).

داده‌کاوی: داده‌کاوی به ساده‌سازی و خلاصه کردن داده‌ها در چارچوبی که برای ما قابل‌درک باشد می‌پردازد و به ما اجازه می‌دهد تا با مشاهده الگوها به استنتاج چیزهای مفید از مجموعه داده‌ها نائل شویم. درهرحال کاربردهای خاص داده‌کاوی محدود به داده‌ها و قدرت ابزارهای محاسباتی قابل‌دسترس هست، و همچنین باید متناسب با نیازها و اهداف باشند (جهان‌گشته، ۱۴۰۱).

یادگیری ماشین: یادگیری ماشین به طراحی ماشین‌هایی پرداخته می‌شود که با استفاده از مثال‌های داده‌شده به آن‌ها و تجربیات خودشان، می‌آموزند (نقشه راه توسعه ملی هوش مصنوعی، ۱۴۰۱).

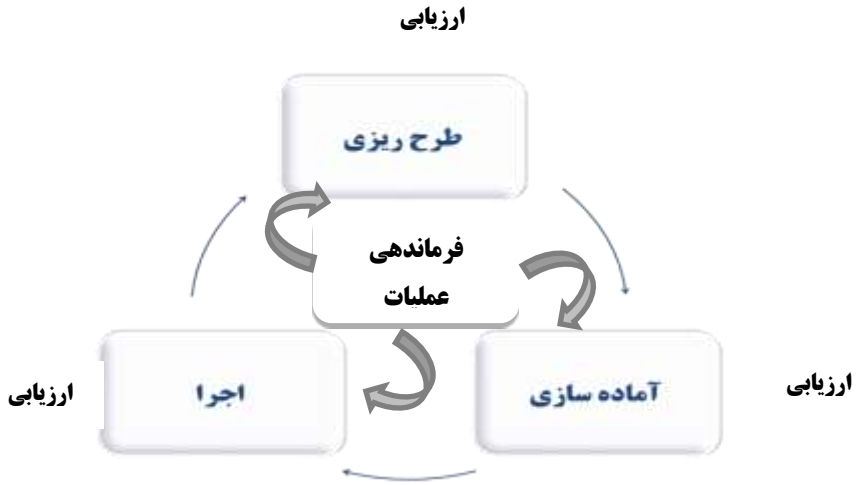
پردازش زبان طبیعی: به فرایند درک و استخراج خودکار مفاهیم بیان‌شده در یا متن که به زبان طبیعی گفتاری و نوشتاری آورده شده است، پردازش زبان طبیعی گفته می‌شود (نقشه راه توسعه ملی هوش مصنوعی، ۱۴۰۱).

منطق فازی: مجموعه ثابتِ متداولی را که از طریق توابع همواندی باقابلیت ردگیریِ تغییرات محدود در ورودی‌ها شکل‌گرفته، با روش طبقه‌بندی آماری ترکیب می‌کند (نقی بیرانوند، ۱۴۰۱).

شبکه‌ها عصبی مصنوعی: شبکه‌های عصبی یک روش یادگیری ماشین است و شبکه‌های عصبی را می‌توان مدل‌های الکترونیکی از ساختار عصبی مغز انسان نامید (بیگدلی، ۱۴۰۰).

کلیات فرایند عملیات جنگ الکترونیک:

فرایند عملیات جنگ الکترونیک دارای سه مرحله طرح‌ریزی، آماده‌سازی، اجرا بوده که در تمام فرایند عملیات، اقدامات مرتبط با ارزیابی انجام می‌شود که توسط فرمانده راهبری و نظارت می‌گردد. این اقدامات ممکن است به‌طور متوالی و یا بی‌وقفه در طول یک عملیات انجام‌پذیرند و در صورت لزوم تکرار شده و با یکدیگر تداخل داشته باشند. افسر جنگ الکترونیک به‌طور فعال در فرایند عملیات درگیر است. طرح‌ریزی، آماده‌سازی اجرا و ارزیابی جنگ الکترونیک مستلزم دانش مهارت و تخصص جمعی عناصر ذی‌ربط در مورد عملیات اطلاعات مدیریت طیف الکترومغناطیس و فرماندهی مأموریت است. افسر جنگ الکترونیک از تلاش‌های به‌عمل‌آمده در راستای اجرای مأموریت‌های محوله اطمینان می‌یابد و اقدامات پشتیبانی از عملیات جنگ الکترونیک و اهداف فرمانده را هماهنگ می‌سازد (اسدالله زاده، ۱۴۰۱).



شکل شماره (۱) فرایند عملیات جنگ الکترونیک

نقش هوش مصنوعی در جنگ الکترونیک:

اهمیت جنگ الکترونیک در قالب یک سیستم فرماندهی و کنترل نظامیِ مدرن به‌سرعت در حال رشد و توسعه است و از طرفی تأکید فراوانی بر ایجاد ارتباط بین تمامی سطوح دارد. تعبیه الگوریتم هوش مصنوعی در یک سیستم جنگ الکترونیک سبب می‌شود که سیستم مذکور قابلیت اجرای مأموریت خود در قالب یک سیستم مستقل و خودکافی

به‌گونه‌ای مؤثر را داشته باشد. هوش مصنوعی را می‌توان در حوزه‌های مختلف نظامی مانند: انتخاب سیستم‌ها، سامانه‌ها، تسلیحات و نحوه به‌کارگیری آن‌ها، پشتیبانی هوشمند، تجزیه‌وتحلیل تهدید، تفسیر و واکاوی داده‌ها و اطلاعات گردآوری‌شده، تدارکات و... به کاربرد. کاربردهای نظامیِ هوش مصنوعی در دودسته کلی تقسیم می‌شوند: سامانه‌ها و سیستم‌های جنگ الکترونیک وابسته به هوش مصنوعی که بر «سطح عملیاتی» در یک میدان تقابلی در صحنه نبرد تأثیر داشته و سیستم‌هایی با تأثیر مستقیم بر «سطح راهبردی». هوش مصنوعی می‌تواند در سطح عملیاتی میدان نبرد در دستیابی به اهداف تاکتیکی، طرح‌ریزی و اجرا، حذف عدم اطمینان و ایجاد آمادگی مؤثر بسیار حائز اهمیت باشد و از طرفی در سطح راهبردی نیز بر نحوه سازمان‌دهی نظم نبرد، مأموریت‌های محوله به نیروهای عمل‌کننده، استراتژی‌های جنگی، تصمیم‌گیری در مورد مقیاس و وسعت میدان نبرد، به اشتراک‌گذاری اطلاعات و تفسیر آن‌ها، دامنه و ماهیت جنگ، پیامد استقرار و جانمایی دارایی‌ها و تجهیزات خاص و... نظارت مستقیم و تأثیرگذار داشته باشد (SHARMA,2020).

سامانه جنگ الکترونیکِ مبتنی بر هوش مصنوعی:

هوش مصنوعی در عملیات جنگ الکترونیک می‌تواند به نیروهای خودی کمک شایانی جهت مقابله با اقدامات دشمن و اختلال در خطوط و شبکه‌های ارتباطی آن‌ها ازجمله سامانه موقعیت‌یاب جهانی، سیگنال‌های ماهواره‌ای و... نماید. هوش مصنوعی می‌تواند ظرفیت دانشی و اثربخشی جنگ الکترونیک برای اجرای هدفمند یک عملیات چند دامنه‌ای را بهبود بخشد. داده‌های دریافتی به ترتیب اولویت سریع و دقیق رتبه‌بندی شده و بنابراین سیگنال‌هایی با درجه اهمیت کمتر حذف می‌شوند. همچنین در پردازش حجم زیادی از داده‌ها نیز کاربرد داشته و درنتیجه تشخیص الگو و استخراج اطلاعات معنی‌دار با درجه اعتبار بالاتری صورت خواهد پذیرفت (SHARMA,2020).

اجرا:

ستاد طرح‌ریزی عملیات را در مرحله اجرای جنگ الکترونیک، با درک شرایط صحنه نبرد و با به‌کارگیری توان رزم عملی کرده و تصمیمات اجرایی و تطبیقی را اتخاذ می‌کند. افسران با صدور تدابیر و دستورات فرمانده باعث تجمیع مساعی در پیشبرد اهداف عملیاتی می‌شوند. در حین اجرا، افسر جنگ الکترونیک و مرکز هماهنگی عملیات جنگ

الکترونیک اقدامات زیر را انجام می‌دهند:

الف) انجام‌وظیفه به‌عنوان افسر تخصصی و مشاور جنگ الکترونیک برای فرمانده

ب) تدوین و به‌روزرسانی برآورد وضعیت جنگ الکترونیک برای عملیات جنگ الکترونیک

پ) نظارت بر عملیات جنگ الکترونیک و پیشنهاد تغییرات و با اصلاحات موردنیاز دستورات در حین اجرا

ت) تجدیدنظر و پیشنهاد تغییر در نیازمندی‌های اطلاعاتی فرمانده بر اساس شرایط صحنه نبرد

ث) تجدیدنظر و پیشنهاد تغییرات جهت رویه‌ها و اقدامات کنترل و نظارت مرتبط با جنگ الکترونیک

ج)ارتباط مستمر و مستقیم با گروه‌های آتش و عملیات سایبر الکترونیک (سایبر در رزم) جهت اطمینان از یکپارچگی و رفع ناسازگاری عملیات جنگ الکترونیک

چ) دریافت تجزیه‌وتحلیل و هماهنگی تقاضاها برای تجهیزات جنگ الکترونیک در حین اجرای عملیات

ح) دریافت و تجزیه‌وتحلیل تقاضاهای پشتیبانی فوری جنگ الکترونیک برای سرکوب پدافند هوایی یا جنگ الکترونیک

خ)هماهنگی با بخش نظارت و کنترل هوایی مراقبت پرواز در تمامی مراحل سرکوب پدافند هوایی با مأموریت‌های جنگ الکترونیک دشمن (FM 3-36,2012).

حمله الکترونیک:

حمله الکترونیکی به‌عنوان یکی از زیر بخش‌های جنگ الکترونیک متضمن استفاده از انرژی الکترومغناطیس، انرژی تابشی یا تسلیحات ضد تشعشع در حمله به افراد، تأسیسات یا تجهیزات است که باهدف تنزل خنثی‌سازی یا انهدام توان رزمی دشمن صورت گرفته و نوعی اجرای آتش محسوب می‌شود.

حمله الکترونیکی شامل مراحل زیر است:

۱- روش‌هایی در جلوگیری با کاهش استفاده مؤثر دشمن از طیف الکترومغناطیس مانند عملیات اخلال و فریب الکترومغناطیسی

۲-به‌کارگیری تسلیحاتی که انرژی الکترومغناطیس با تابشی (لیزر، تسلیحات فرکانس رادیویی و پرتوهای حاوی ذرات باردار) را به‌عنوان سازوکار انهدامی خود مورداستفاده قرار می‌دهند.

حمله الکترونیکی برای اجرای عملیات متقابل هر دو نوع فعالیت‌های حمله‌ای و دفاعی را در اختیار دارد:

الف) فعالیت‌های تهاجمی حمله الکترونیکی به‌طورمعمول از سوی نیروهای خودی شکل‌گرفته و هدایت می‌شوند. برای مثال ایجاد اخلال روی سامانه‌های راداری یا سامانه فرماندهی و کنترل دشمن استفاده از موشک‌های ضد تشعشع در سرکوب دفاع هوایی دشمن، استفاده از روش‌های قریب الکترونیکی در مغشوش نمودن سامانه‌های اطلاعاتی، شناسایی و مراقبت و استفاده از تسلیحات انرژی تابشی در نانوان ساختن تجهیزات و سلب توانایی دشمن.

ب) فعالیت‌های دفاعی حمله الکترونیکی از طیف الکترومغناطیس برای حفاظت از کارکنان تأسیسات توانمندی‌ها و تجهیزات استفاده می‌کنند. برای مثال می‌توان به روش‌های دفاع از خود و حفاظت از نیروها مانند استفاده از وسایل مصرفی (گلوله‌های حرارتی موسوم به فلیر و دام‌های فعال اخلال‌گرها دام‌های کششی سامانه‌های ضد فروسرخ انرژی تابشی و مقابله با سامانه‌های انفجاری دست‌ساز کنترل رادیویی) اشاره نمود.

اقدامات حمله الکترونیکیِ جنگ الکترونیک دشمن از طریق انتشار و انتقال انرژی الکترومغناطیسی است. در این حوزه با دو فاکتور اصلی و اساسی سروکار داریم؛ جمینگِ نویزی و جمینگِ فریب. جمینگ مانع از انجام عملیات متداول رادار در اندازه‌گیری موقعیت و سرعت هدف می‌شود، درحالی‌که تکنیک‌های فریب سبب ایجاد موقعیت و سرعت نادرست و ساخت یک هدف جعلی می‌شوند.

به‌طورکلی عملیات فریب در حوزه الکترونیکی را می‌توان در چهار دسته کلی زیر تعریف نمود(Waghray, 2018) :

۱-تولید اهداف جعلی۲-فریب برد ۳- فریب سرعت۴- فریب زاویه

تولید اهداف جعلی: این نوع فریب نوعی از پارازیت مؤثر است که در برابر رادارهای هشدار اولیه، ره‌گیر و رادارهای ره‌گیری کنترل زمینی می‌تواند مورداستفاده قرار گیرد. در این نوع فریب با تولید تعداد زیادی اکوی جعلی هدف مشابه با اکوی اصلی هدف به دنبال گیج کردن رادار دشمن و اپراتور هستیم.

فریب در برد: در این تکنیک، به دنبال ایجاد فریب در تشخیص برد توسط سامانه راداری و یا سامانه هدایت خودکار موشک هستیم. روش کار به این صورت است که در ابتدا گیت برد سامانه راداری دریافت و بر اساس الگوهای از پیش مشخص‌شده به آن‌یک تأخیر

زمانیِ منطقی اضافه‌شده و سپس باز انتشار داده می‌شود، نتیجه به این صورت خواهد بود که به علت وجود اختلاف بین مدارهای زمانی، فاصله واقعی تا هدف اشتباه برآورد شده و نهایتاً اطلاعات غلط نمایش داده خواهد شد.

فریب در سرعت: رادارِ موج پیوسته و پالس داپلر اهداف را بر اساس سرعت یا فرکانس جابه‌جایی داپلر ردگیری می‌کند. در این تکنیک فریب، اطلاعاتِ ردگیری سرعت با تولید اهدافی با سرعت مشابه هدف اصلی جایگزین می‌شوند، این کار از طریق ربایش گیت سرعت، نویزداپلرو نویز داپلر باند باریک صورت می‌پذیرد.

فریب در زاویه: در این تکنیک، تمرکز ما بر روی توانایی رادار ردیاب برای استخراج زاویه صحیح و اطلاعات ارتفاع یک هدف است؛ بنابراین، رادار اطلاعات نادرست در مورد موقعیت زاویه‌ای هدف را درنهایت به دست خواهد آورد.

پشتیبانی الکترونیک:

فعالیت‌هایی است که توسط یا تحت کنترل مستقیم یک فرمانده عملیاتی با اهداف جستجو، ره‌گیری، شناسایی و تعیین موقعیت منابع انرژی الکترومغناطیسی دشمن، به‌منظور تشخیص فوری تهدید، هدف‌گیری، طراحی و اجرای عملیات بعدی انجام می‌شود. (فرح بخت، ۱۳۹۸)

اولین گام در هر سیستم جنگ الکترونیک هوشمند، پشتیبانی الکترونیک است تا درک بهتری از طیف رادیویی حاصل شود. پشتیبانی الکترونیک که به‌عنوان ارزیابی وضعیت در جامعه هوش مصنوعی شناخته می‌شود، تعیین می‌کند که چه کسی از طیف استفاده می‌کند، کجا و چه زمانی از آن استفاده می‌کند و آیا الگوهایی وجود دارد که مورد سوءاستفاده قرار گیرد (Haigh,2021).

تعریف آگاهی از وضعیت طیف (SSA)[1] به‌عنوان «وسیله‌ای برای جمع‌آوری اطلاعات متفاوت در مورداستفاده از طیف و پردازش این اطلاعات برای تولید یک تصویر طیف آمیخته است.» SSA داده‌های طیف موردنیاز برای جنگ الکترونیک را جمع‌آوری، سازمان‌دهی و پردازش می‌کند. علاوه بر تجزیه‌وتحلیل قبل و بعد از مأموریت، SSA باید در زمان واقعی و خیلی سریع، با توجه به نیازهای تصمیم‌گیرنده رخ دهد.

1 - Space Situational Awareness

برای رسیدگی به فرستنده‌ها و دشمنان جدید، قابلیت‌های هوش مصنوعی و ML می‌توانند SSA[1] را در هر سطح بهبود بخشند. یک سیستم جنگ الکترونیک کامل باید SSAچندوجهی داشته باشد. سیستم‌های SSA آینده را می‌توان با مدل‌های یادگیری عمیق برای تولید ویژگی‌های پنهان، مدل‌های ML[2] کلاسیک برای به‌روزرسانی‌های پذیرش و مدل‌های هیبریدی برای جبران داده‌های محدود آموزش داد. علاوه بر این، SSAمجبور نیست تنها به داده‌های RF[3] تکیه کند، می‌توان آن را با داده‌های غیر RF مانند ویدئو و تصاویر ثابت، اپتیک فضای آزاد یا منبع‌باز، تاکتیکی یا اطلاعات عملیاتی ترکیب کرد.

حفاظت الکترونیک:

اقداماتی که برای حفاظت از اشخاص، امکانات یا تجهیزات در مقابل تأثیرات استفاده دوستانه یا دشمن از طیف الکترومغناطیس که قابلیت‌های جنگی خودی را کاهش، خنثی یا تخریب می‌کند. (فرحبخت،۱۳۹۸)

حفاظت الکترونیکی شامل روش‌هایی در اطمینان از استفاده نیروهای خودی از طیف الکترومغناطیس است که مواردی مانند چالاکی فرکانس در یک سامانه رادیویی با تنوع در فرکانس تکرار پالس یک رادار را در برمی‌گیرد. حفاظت الکترونیکی نباید با روش دفاع از خود اشتباه شود. استفاده از منطق حذف فلیر در یک موشک فروسرخ که باهدف خنثی نمودن اثر فلیر دشمن صورت می‌گیرد. نوعی روش حفاظت الکترونیکی محسوب می‌شود. در این حالت عدم پذیرش فلیر خارج کردن آن از چرخه ره‌گیری هدف تضمینی برای استفاده نیروهای خودی از طیف الکترومغناطیس در ردیابی هدف است که (باوجود اقدام دشمن در به‌کارگیری روش‌های دفاعی حمله الکترونیکی دفاع از خود مانند فلیر) در جلوگیری یا کاهش استفاده نیروهای خودی از طیف الکترومغناطیس صورت می‌گیرد. درحالی‌که اقدام‌های دفاعی حمله الکترونیکی و حفاظت الکترونیکی هر دو درصدد حفاظت از کارکنان، تأسیسات امکانات و تجهیزات نیروهای خودی هستند. حفاظت الکترونیکی، روش‌هایی حفاظتی خود را روی آثار حمله‌ای جنگ الکترونیک خودی یا دشمن متمرکز نموده که در این حالت روش دفاعی حمله الکترونیکی به‌طور عمده به

۱- آگاهی از وضعیت طیف (SSA)

۲-یادگیری ماشین

۳ -فرکانس رادیویی

حفاظت در برابر حمله‌های مرگبار ناشی از فعالیت طیف الکترومغناطیس دشمن ادامه می‌دهد. این امر با جلوگیری از استفاده دشمن در بهره‌برداری از طیف الکترومغناطیس در هدایت تسلیحات وی انجام می‌گیرد (ال شارپ، ۱۳۹۴).

سامانه جنگ الکترونیکِ مبتنی بر هوش مصنوعی:

هوش مصنوعی در عملیات جنگ الکترونیک می‌تواند به نیروهای خودی کمک شایانی جهت مقابله با اقدامات دشمن و اختلال در خطوط و شبکه‌های ارتباطی آن‌ها ازجمله سامانه موقعیت‌یاب جهانی، سیگنال‌های ماهواره‌ای و... نماید. هوش مصنوعی می‌تواند ظرفیت دانشی و اثربخشی جنگ الکترونیک برای اجرای هدفمند یک عملیات چند دامنه‌ای را بهبود بخشد. داده‌های دریافتی به ترتیب اولویت سریع و دقیق رتبه‌بندی شده و بنابراین سیگنال‌هایی با درجه اهمیت کمتر حذف می‌شوند. همچنین در پردازش حجم زیادی از داده‌ها نیز کاربرد داشته و درنتیجه تشخیص الگو و استخراج اطلاعات معنی‌دار با درجه اعتبار بالاتری صورت خواهد پذیرفت(SHARMAT, 2020) .

به‌طورکلی، اگر از ی یادگیری عمیق/ یادگیری ماشین[1] مبتنی بر سیستم هوش مصنوعی در بلوک جنگ الکترونیک استفاده شود، نقش آن ارائه یک پیش‌بینی از وضعیت در حال تغییر خواهد بود. جدول شماره یک نشان می‌دهد که چگونه تکنیک‌های هوش مصنوعی در طرح‌های کاربردی مختلف در تمام زیرمجموعه‌های EW نتایج امیدوارکننده‌ای در اختیار قرار می‌دهد. چرا به‌کارگیری هوش مصنوعی در کنار جنگ الکترونیک ضروری و الزام‌آور است؟ از دلایل اصلی ارجحیت استفاده از سیستم‌های جنگ الکترونیک مبتنی بر هوش مصنوعی شامل قابلیت‌های تأثیرگذار در تصمیم‌گیری، مدیریت حجم زیادی از داده‌هایِ گردآوری‌شده، تجزیه‌وتحلیل آنی و ارائه اطلاعات با درنظرگرفتن جزئیات، آگاهی موقعیتی، تجسم صحنه در حال تحول و ایجاد پاسخ‌ها و واکنش‌های مناسب در کمترین زمان ممکن است. علاوه بر این، سیستم‌ها و تجهیزات الکترونیکی، مخابراتی، کامپیوتری و... که از قابلیت‌های هوش مصنوعی استفاده می‌کنند، به دلیل محاسبات ذاتی‌شان، قابلیت تصمیم‌گیری و تصمیم‌سازی، خودکنترلی، خودتنظیمی و فعال شامل تخریب اثربخشی پشتیبانی جنگ الکترونیک دشمن از طریق انتشار و انتقال انرژی الکترومغناطیسی است (T. Singh, 2020).

[1] Deep learning/Machine learning

«استفاده از هوش مصنوعی، اجرای عملیات جنگ الکترونیک را به‌صورت مستقل و خودکافی تسهیل می‌کند، آگاهی موقعیتی را افزایش داده و به تصمیم‌گیری قابلیت اطمینان و اعتماد می‌بخشد» (نوروزی، ۱۴۰۲).

جدول شماره (۱) دقت اثربخشی هوش مصنوعی در جنگ الکترونیک(SHARMA, 2020)

دقت صحت اثربخشی	حوزه‌های جنگ الکترونیک	کاربرد تکنیک‌های هوش مصنوعی
۹۶.۱٪	ES	CNN بر اساس نوع تشخیص مدولاسیون PRI
٪۹۹.۸	ES	CNN، SAE براساس سامانه تشخیص سیگنال رادار
٪۸۴	ES	شبکه عصبی بر اساس طبقه‌بندی و تشخیص انتشاردهنده سیگنال راداری
٪۹۴.۵	ES	تفکیک‌کننده ترکیبی شامل CNN و ENN جهت تشخیص شکل موج راداری
٪۹۵.۲	EA	ANN-GA بر اساس سیستم آشکارساز جمینگ فریب
٪۹۸.۳۴	EA	SVM اساس مدل انتخاب نوع جمینگ
٪۸۵	EA	بر اساس سامانه تشخیص پیش‌یابی اخلالگر و مشخصه‌های آن
٪۹۰	ES	الگوریتم هوش مصنوعی(ANN ، SVMو DNN)برای تشخیص پارامتر اسکن آنتن رادار
٪۱۰۰	ES	خوشه‌بندی WARDS و PNN بر اساس آشکارسازی و طبقه‌بندی سیگنال ارسالی رادار
٪۹۹	ES	N، میزان احتمال و آنتروپی تقریبی برای طبقه بندی سیگنال رادار

روش‌شناسی پژوهش

محقق به چگونگی به‌کارگیری هوش مصنوعی در اجرا عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران پرداخته است، بنابراین ازنظر نوع تحقیق کاربردی است.

نظر به اینکه محقق در این تحقیق آنچه هست را بدون هیچ‌گونه دخالت و استنتاج ذهنی گزارش نموده و نتایج عینی از موقعیت گرفته و درنهایت بر مبنای یافته‌های تحقیق به چگونگی به‌کارگیری هوش مصنوعی در اجرا عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران پرداخته است، لذا روش تحقیق توصیفی است.

تجزیه‌وتحلیل یافته‌های پژوهش:

در این تحقیق، به‌منظور پاسخ به سؤالات تعیین‌شده تحقیق، محقق مبادرت به انجام دو نوع تجزیه‌وتحلیل نموده است:

۱- تجزیه‌وتحلیل کیفی: فرآیند تجزیه‌وتحلیل کیفی با استفاده از نرم‌افزار اطلس‌تی‌ای انجام‌گرفته است، برای انجام تحلیل کیفی در نرم‌افزار اطلس‌تی‌ای، در ابتدا پیشینه تحقیق و مصاحبه‌های صورت گرفته به‌صورت مجزا با عنوان سند تفکیک گردیده و در گام اول، دسته‌بندی داده‌ها که شامل دسته‌بندی بر اساس اسناد و مدارک و مصاحبه با صاحب‌نظران و انجام پالایش، تلخیص و نمایش داده‌ها است بر مبنای کدهای باز اختصاص‌یافته به روایت‌ها صورت پذیرفته است. در گام دوم، پردازش اطلاعات شامل همگرایی داده‌ها (ترکیب)، واگرایی (تعدیل) و تقارن، که از دسته‌بندی روایت‌ها بر اساس اهداف تحقیق برای هر هدف با انجام سه مرحله ذکرشده انجام‌شده است. درنهایت در گام سوم، قضاوت و تصمیم‌گیری باتوجه به داده‌های استخراج‌شده از دسته‌بندی کدها و پس از پردازش جهت دست‌یابی و رسیدن به هدف مربوطه انجام‌گرفته است.

۲- تجزیه‌وتحلیل کمی: دیدگاه و نگرش جامعه در پاسخ به سؤالات پرسش‌نامه با استفاده از نرم‌افزار اس‌پی‌اس‌اس تحلیل گردیده است.

ازآنجاکه تحقیق درزمینه هوش مصنوعی و جنگ الکترونیک است از رویکرد ترکیبی برای تحقیق استفاده‌شده، با ۸ نفر از خبرگان که در حوزه جنگال، سایبر و هوش مصنوعی به‌صورت عملی مشغول به کار بوده و با مشکلات آن آشنایی دارند و همچنین اساتید دانشگاه، اقدام به مصاحبه گردیده است، و سپس پرسش‌نامه در میان جامعه نمونه توزیع گردید.

جامعه آماری تحقیق شامل کارکنان شاغل درزمینه جنگ الکترونیک و هوش مصنوعی دارای دانش و کار تجربی هستند انتخاب گردیده که با بررسی انجام‌شده، تعداد افراد جامعه آماری، با اعمال ضریبی، ۱۰۴ نفر و تمام شمار برآورد شده است.

ابزارهای گردآوری اطلاعات به‌صورت میدانی و کتابخانه‌ای بوده و در روش میدانی از ابزار مصاحبه و پرسش‌نامه استفاده گردیده است. در این پژوهش از آزمون آلفای کرون باخ جهت بررسی پایایی ابزار سنجش استفاده گردیده است. نتایج این آزمون در جدول زیر آورده شده است.

جدول شماره (۳) آزمون پایایی پرسش‌نامه

عنوان پرسش‌نامه	تعداد سؤال	آلفای کرون باخ
اجرا	۲۷	۰/۸۸۹

بررسی روایی و پایایی سازه‌ها

با توجه به شاخص میانگین واریانس استخراج‌شده، مقادیر بالاتر از ۰.۵ نشان‌دهنده روایی مناسب سازه موردبررسی است که با استفاده از نرم‌افزار اس‌پی‌اس‌اس محاسبه می‌گردد.

جدول شماره (۴) نتایج آزمون روایی پرسشنامه

سؤالات	نتایج	سؤالات	نتایج
۱	۰.۶۸۸	۱۵	۰.۷۸۸
۲	۰.۷۸۵	۱۶	۰.۷۹۰
۳	۰.۷۹۲	۱۷	۰.۷۹۹
۴	۰.۸۰۴	۱۸	۰.۷۳۵
۵	۰.۷۲۸	۱۹	۰.۷۸۳
۶	۰.۷۵۷	۲۰	۰.۷۱۸
۷	۰.۷۹۹	۲۱	۰.۸۰۳
۸	۰.۶۵۹	۲۲	۰.۷۱۳
۹	۰.۶۷۲	۲۳	۰.۷۵۱
۱۰	۰.۷۴۴	۲۴	۰.۸۳۳
۱۱	۰.۷۳۵	۲۵	۰.۷۱۵
۱۲	۰.۷۶۹	۲۶	۰.۸۷۶
۱۳	۰.۷۹۲	۲۷	۰.۸۴۲
۱۴	۰.۷۹۷		

با تجزیه‌وتحلیل نظرات صاحب‌نظران و اسناد و مدارک موجود، تبیین چگونگی به‌کارگیری هوش مصنوعی در اجرا عملیات جنگ الکترونیک ارتش جمهوری اسلامی ایران به شرح جدول زیر احصا گردید.

تعداد ۳۷ سند مصاحبه با صاحب‌نظران و ۳۰ سند مربوط به اسناد و مدارک کدگذاری گردید که با استفاده از نرم‌افزار اطلس‌تی‌ای نسخه ۹ تعداد ۷۱ کد اولیه با مجموع فراوانی ۱۲۳ از مصاحبه با صاحب‌نظران و مطالعه اسناد و مدارک استخراج شد.

جدول شماره (۵)کدهای استخراج‌شده هدف سوم

ردیف	کد استخراج‌شده	فراوانی	درصد فراوانی
۱	پاسخ خودکار به حملات الکترونیک با استفاده از الگوریتم‌های هوش مصنوعی یادگیری ماشین و شبکه‌های عصبی	۵	۴.۰۶
۲	سیستم‌های هوش مصنوعی با انتخاب بهترین زمان و فرکانس بیشترین اختلال و تداخل را با کمترین مصرف انرژی در ارتباطات دشمن ایجاد می‌کند	۳	۲.۴۴

۳	خودکارسازی فرایندهای حمله و تحلیل داده‌های به‌دست‌آمده	۳	۲.۴۴
۴	استفاده از شبکه‌های عصبی مصنوعی در انجام فرایند تشخیص و انتخاب نوع جمینگ تشخیص نقاط ضعف سیستم‌های موردحمله و ارائه راهکارهایی برای اختلال یا تخریب	۲	۱.۶۳
۵	استفاده از شبکه‌های عصبی مصنوعی در انجام فرایند تشخیص و انتخاب نوع جمینگ	۲	۱.۶۳
۶	تشخیص نقاط ضعف سیستم‌های موردحمله و ارائه راهکارهایی برای اختلال یا تخریب	۲	۱.۶۳
۷	طراحی سیگنال‌های فریب‌دهنده با دقت بیشتر با استفاده از سیستم‌های هوش مصنوعی	۲	۱.۶۳
۸	استفاده از پردازش صوت در فریب جعلی و تقلیدی ارتباطی	۲	۱.۶۳
۹	الگوریتم‌های هوشمند در عملیات فریب	۲	۱.۶۳
۱۰	شناسایی الگوهای مشترک حملات	۳	۲.۴۴
۱۱	بینایی ماشین و پردازش تصویر در حمله الکترونیکی	۱	۰.۸۱
۱۲	هوش مصنوعی در بهبود امنیت عملیات حمله	۱	۰.۸۱
۱۳	سناریوهای مختلف حمله را شبیه‌سازی کرده و اثرات آن را پیش‌بینی می‌کند	۱	۰.۸۱
۱۴	تشخیص خودکار اثرات حمله	۱	۰.۸۱
۱۵	انتخاب اقدام بهینه برای حمله با درنظرگرفتن بیشترین خسارت به دشمن با کمترین منابع	۱	۰.۸۱
۱۶	پیش‌بینی حملات با استفاده از الگو و داده‌های جمع‌آوری‌شده و ارائه راه‌حل حمله‌ای مناسب	۳	۲.۴۴
۱۷	به‌کارگیری هوش مصنوعی در سامانه‌های اخلال در موقعیت‌یاب جهانی و سیگنال‌های ماهواره‌ای	۱	۰.۸۱
۱۸	استفاده از یادگیری عمیق در برآورد تکنیک‌های مناسب اختلال در برابر سیگنال‌های تهدید بدون استفاده از کتابخانه	۱	۰.۸۱
۱۹	تشخیص هوشمند الگوی تهدیدات	۶	۴.۸۸
۲۰	تجسم صحنه در حال تحول و آگاهی موقعیتی با درک صحیح از نظم الکترونیکی میدان نبرد با استفاده از قابلیت‌های هوش مصنوعی و یادگیری ماشین	۴	۳.۲۵
۲۱	مدیریت و تجزیه‌وتحلیل حجم عظیمی از داده‌های گردآوری‌شده در جنگ الکترونیک با استفاده از هوش مصنوعی و الگوریتم‌های یادگیری ماشین در زمان واقعی	۴	۳.۲۵
۲۲	تجزیه‌وتحلیل هوشمند در قالب یک بانک تهدید	۳	۲.۴۴
۲۳	با الگوی داده‌های جمع‌آوری‌شده می‌توان حملات را پیش‌بینی به راه‌حل دفاعی و حمله مناسب پیشنهاد داد	۳	۲.۴۴
۲۴	تشخیص و طبقه‌بندی سیگنال‌های دشمن با استفاده از هوش مصنوعی و الگوریتم‌های یادگیری ماشین	۳	۲.۴۴
۲۵	سنجش طیف الکترومغناطیس با استفاده از هوش مصنوعی	۲	۱.۶۳
۲۶	تجزیه‌وتحلیل بلادرنگ ارتباطات دشمن	۲	۱.۶۳
۲۶	الگوریتم‌های طراحی است هوش مصنوعی در جمع‌آوری اطلاعات اخلالگران و فریب‌دهنده‌ها	۲	
۲۸	سیستم‌های فازی و الگوریتم‌های ژنتیک در پردازش سیگنال‌های رادار	۲	۱.۶۳
۲۹	تحلیل اطلاعات متنی با استفاده از پردازش زبان طبیعی از منابع مختلف	۲	۱.۶۳
۳۰	استخراج عملکرد عملیات پشتیبانی الکترونیک و خودکارسازی تمامی فرایند پشتیبانی الکترونیک	۲	۱.۶۳
۳۱	تحلیل داده‌های اخذشده با استفاده از الگوریتم‌های تشخیص الگو و روندهای جدید و تجزیه‌وتحلیل داده‌های رمز شده	۲	۱.۶۳
۳۲	تجزیه‌وتحلیل هوشمند داده‌های سنجش برای ارتباطات و اداره فضای سیگنالی	۲	۱.۶۳
۳۳	تفسیر و واکاوی داده‌ها و اطلاعات گردآوری‌شده با استفاده از هوش مصنوعی	۲	۱.۶۳
۳۴	داده‌کاوی و همجوشی داده‌ها به‌منظور تلفیق داده‌ها و سیگنال‌های به‌دست‌آمده	۲	۱.۶۳

۳۵	تشخیص انواع عملیات اختلال و مشخصه‌های آن و شناسایی و طبقه‌بندی انواع فرستنده‌ها	۲	۱.۶۳
۳۶	ارائه خورد از میزان موفقیت‌آمیز بودن عملیات حمله الکترونیکی	۱	۰.۸۱
۳۷	نقاط ضعف شبکه‌های دشمن و استفاده از آن‌ها برای نفوذ و اختلال	۱	۰.۸۱
۳۸	استخراج پارامترهای مهم با استفاده از بانک اطلاعات تهدید	۱	۰.۸۱
۳۹	طبقه‌بندی هوشمند جمینگ راداری	۱	۰.۸۱
۴۰	شبکه‌های عصبی عمیق و انتساب آن به داده‌های کتابخانه تهدید	۱	۰.۸۱
۴۱	تحلیل متن و پردازشی طبیعی در جمع‌آوری اطلاعات مفید	۱	۰.۸۱
۴۲	تجزیه‌وتحلیل هوشمند داده‌ها در عملیات شنود با استفاده از هوش مصنوعی	۱	۰.۸۱
۴۳	سیستم‌های هوش مصنوعی می‌توانند الگوهای مشهود را در داده‌ها شناسایی کرده و هشدارهای لازم را ارائه دهند	۱	۰.۸۱
۴۴	سیستم‌های هوش مصنوعی می‌توانند الگوهای مشهود را در داده‌ها شناسایی کرده و هشدارهای لازم را ارائه دهند	۱	۰.۸۱
۴۵	استفاده از هوش مصنوعی برای شناسایی تهدیدات الکترونیکی و حملات سایبری	۱	۰.۸۱
۴۶	استخراج اطلاعات مفید با استفاده از الگوریتم‌ها و شبکه‌های عصبی	۱	۰.۸۱
۴۷	کنترل هوشمند فضای الکترومغناطیس با استفاده از یادگیری ماشین	۲	۱.۶۳
۴۸	تحلیل هوشمند ترافیک شبکه	۱	۰.۸۱
۴۹	رتبه‌بندی داده‌های دریافتی به ترتیب اولویت	۱	۰.۸۱
۵۰	بهره‌گیری از تکنیک‌های پیشرفته تحلیل داده	۱	۰.۸۱
۵۱	خودکار کردن فرایند جمع‌آوری اطلاعات	۱	۰.۸۱
۵۲	تجزیه‌وتحلیل هوشمند داده‌ها در عملیات جهت‌یابی و استفاده از هوش مصنوعی	۱	۰.۸۱
۵۳	کنترل هوشمند مثبت و منفی با به‌کارگیری سامانه‌های خبره مجهز به یادگیری عمیق	۲	۱.۶۳
۵۴	به‌کارگیری سامانه‌های خبره و یادگیری عمیق در اولویت‌بندی فرکانس‌ها	۲	۱.۶۳
۵۵	رادیو شناختی برای ایجاد بستر امن با به‌کارگیری هوش مصنوعی	۲	۱.۶۳
۵۶	استفاده از الگوریتم‌های هوشمند برای جلوگیری از عملیات فریب دشمن و سایت‌یابی با درنظرگرفتن ملاحظات حفاظت الکترونیکی	۲	۱.۶۳
۵۷	جلوگیری از حملات مخرب با استفاده از سیستم‌های شناختی	۱	۰.۸۱
۵۸	به‌کارگیری شبکه‌های عصبی فازی در تشخیص حملات	۱	۰.۸۱
۵۹	به‌کارگیری روش‌های یادگیری عمیق در شناسایی حملات	۱	۰.۸۱
۶۰	اجرای هوشمند توسعه و بهبود روش‌های ضداختلال و آشکارسازی اخلال‌گرها و عملیات رمزنگاری	۲	۱.۶۳
۶۱	تکنیک‌های یادگیری تقویتی عمیق جهت توسعه الگوریتم‌های ضداختلال در یک رادار	۱	۰.۸۱
۶۲	تشخیص جمینگ چف با تکنیک‌های سیگنال در برابر نویز هوش مصنوعی	۱	۰.۸۱
۶۳	امنیت داده‌ها	۱	۰.۸۱
۶۴	بهبود رمزنگاری	۱	۰.۸۱
۶۵	تحلیل و ارزیابی آسیب‌پذیری‌ها و خودکارسازی اقدامات دفاعی با به‌کارگیری هوش مصنوعی	۱	۰.۸۱
۶۶	تغییر شکل موج تهدیدات از طریق نرم‌افزار	۱	۰.۸۱
۶۷	مقاوم‌سازی در برابر حملات الکترونیکی با استفاده از هوش مصنوعی	۱	۰.۸۱
۶۸	استفاده از سیستم‌ها را تحلیل و رفتارهای مشکوک و بدخواهانه را شناسایی می‌کند	۱	۰.۸۱
۶۹	بهبود امنیت سامانه‌های راداری و ارتباطی	۱	۰.۸۱
۷۰	ارائه راه‌حل‌های دفاعی مناسب	۱	۰.۸۱
۷۱	بهبود سیستم‌های امنیتی تشخیص حمله	۱	۰.۸۱

از نظرات ۸ نفر از خبرگان حوزه جنگ الکترونیک و هوش مصنوعی در زمینه محتوای موردنظر استفاده شد.

ابتدا اهداف پژوهش برای خبرگان توضیح داده شد و تعاریف عملیاتی مربوط به محتوای سؤالات بیان گردید. سپس از آن‌ها خواسته شد تا هریک از گزاره‌ها را بر اساس طیف سه‌بخشی لیکرت طبقه‌بندی کنند:

- گویه ضروری است
- گویه مفید است؛ ولی ضروری نیست
- گویه ضرورتی ندارد

پس از گردآوری دیدگاه خبرگان با استفاده از رابطه زیر CVR را محاسبه گردید:

$$\mathrm{CVR}=\frac{Ne-N/2}{\mathrm{N}/2}$$

N:تعداد کل خبرگان=۸

Ne:تعداد خبرگانی که گزینه ضروری را انتخاب کرده‌اند=۷

لذا باتوجه‌به اینکه برابر جدول لاوشه، نسبت روایی فوق ۰.۷۵ هست روایی محتوایی گزاره‌های زیر تأیید گردید:

- ✓ پاسخ خودکار به حملات الکترونیک با استفاده از الگوریتم‌های هوش مصنوعی یادگیری ماشین و شبکه‌های عصبی.
- ✓ سیستم‌های هوش مصنوعی با انتخاب بهترین زمان و فرکانس بیشترین اختلال و تداخل را با کمترین مصرف انرژی در ارتباطات دشمن ایجاد می‌کند.
- ✓ استفاده از شبکه‌های عصبی مصنوعی در انجام فرایند تشخیص و انتخاب نوع جمینگ تشخیص نقاط ضعف سیستم‌های موردحمله و ارائه راهکارهایی برای اختلال یا تخریب.
- ✓ تشخیص نقاط ضعف سیستم‌های موردحمله و ارائه راهکارهایی برای اختلال یا تخریب.
- ✓ طراحی سیگنال‌های فریب‌دهنده با دقت بیشتر با استفاده از سیستم‌های هوش مصنوعی.

- ✓ استفاده از پردازش صوت در فریب جعلی و تقلیدی ارتباطی.
- ✓ تشخیص هوشمند الگوی تهدیدات.
- ✓ تجسم صحنه در حال تحول و آگاهی موقعیتی با درک صحیح از نظم الکترونیکی میدان نبرد با استفاده از قابلیت‌های هوش مصنوعی و یادگیری ماشین.
- ✓ تشخیص و طبقه‌بندی سیگنال‌های دشمن با استفاده از هوش مصنوعی و الگوریتم‌های یادگیری ماشین.
- ✓ سنجش طیف الکترومغناطیس با استفاده از هوش مصنوعی.
- ✓ الگوریتم‌های طراحی است هوش مصنوعی در جمع‌آوری اطلاعات اخلالگران و فریب‌دهنده‌ها و اجرای عملیات رمزنگاری.
- ✓ سیستم‌های فازی و الگوریتم‌های ژنتیک در پردازش سیگنال‌های رادار.
- ✓ تحلیل اطلاعات متنی با استفاده از پردازش زبان طبیعی از منابع مختلف.
- ✓ استخراج عملکرد عملیات پشتیبانی الکترونیک و خودکارسازی تمامی فرایند پشتیبانی الکترونیک.
- ✓ تجزیه‌وتحلیل هوشمند داده‌های سنجش برای ارتباطات و اداره فضای سیگنالی.
- ✓ داده‌کاوی و همجوشی داده‌ها به‌منظور تلفیق داده‌ها و سیگنال‌های به‌دست‌آمده.
- ✓ کنترل هوشمند مثبت و منفی با به‌کارگیری سامانه‌های خبره مجهز به یادگیری عمیق.
- ✓ به‌کارگیری سامانه‌های خبره و یادگیری عمیق در اولویت‌بندی فرکانس‌ها.
- ✓ رادیو شناختی برای ایجاد بستر امن با به‌کارگیری هوش مصنوعی.
- ✓ استفاده از الگوریتم‌های هوشمند برای جلوگیری از عملیات فریب دشمن و سایت‌یابی با درنظرگرفتن ملاحظات حفاظت الکترونیکی.

شاخص روایی محتوایی یا CVI[1] نیز برای سنجش روایی گزاره‌های فوق استفاده شد.

[1] - Content Validity Index

جدول شماره (۶) آماره آزمون

سؤال	شاخص‌ها	میانگین	واریانس	اولویت	فاصله اطمینان		آماره آزمون
					حد بالا	حد پایین	
۱	الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی را می‌توان در پاسخ خودکار به حملات الکترونیک به کار گرفت.	۴.۴۵	۰.۵۸۰	۵	۴.۶۲	۴.۲۸	۱.۰۵۷
۲	سیستم‌های هوش مصنوعی را می‌توان در انتخاب بهترین زمان و فرکانس جهت ایجاد بیشترین اختلال و تداخل با کمترین مصرف توان در ارتباطات دشمن به کار گرفت.	۴.۱۸	۰.۹۸۲	۲۶	۴.۴۰	۳.۹۵	۱.۶۷۰-
۳	شبکه‌های عصبی مصنوعی را می‌توان در انجام فرایند تشخیص و انتخاب نوع اختلال و ارائه راهکارهایی برای اختلال یا تخریب استفاده کرد.	۴.۳۵	۰.۷۶۲	۱۷	۴.۵۴	۴.۱۶	۰.۱۰۲-
۴	هوش مصنوعی را می‌توان در تشخیص نقاط ضعف سیستم‌های موردحمله به کار گرفت.	۴.۴۹	۰.۵۳۱	۱	۴.۶۵	۴.۳۳	۱.۵۶۴
۵	الگوریتم‌های هوش مصنوعی را می‌توان در طراحی سیگنال‌های فریب‌دهنده با دقت بیشتر به کار گرفت.	۴.۳۸	۰.۵۹۲	۱۳	۴.۵۵	۴.۲۰	۰.۱۷۴
۶	پردازش هوشمند صوت را می‌توان در فریب جعلی و تقلیدی ارتباطی به کار گرفت.	۴.۳۱	۰.۷۲۴	۱۹	۴.۵۰	۴.۱۲	۰.۴۹۹-
۷	هوش مصنوعی را می‌توان در تجزیه‌وتحلیل هوشمند اطلاعات جهت تشکیل یک بانک تهدید و تشخیص هوشمند الگوی تهدیدات به کار گرفت.	۴.۴۴	۰.۵۵۳	۷	۴.۶۰	۴.۲۷	۰.۹۳۲
۸	قابلیت‌های هوش مصنوعی و یادگیری ماشین را می‌توان در تجسم صحنه در حال تحول و آگاهی موقعیتی (درک، فهم، تجسم و پیش‌بینی) با درک صحیح از ترتیب الکترونیکی میدان نبرد به کار گرفت.	۴.۳۶	۰.۵۶۳	۱۵	۴.۵۳	۴.۲۰	۰.۰۳۰
۹	هوش مصنوعی و الگوریتم‌های یادگیری ماشین را می‌توان در مدیریت و تجزیه‌وتحلیل حجم عظیمی از داده‌های گردآوری‌شده در جنگ الکترونیک در زمان واقعی به کار گرفت.	۴.۴۰	۰.۵۴۷	۹	۴.۵۶	۴.۲۴	۰.۴۸۴
۱۰	الگوی داده‌های جمع‌آوری‌شده را می‌توان در پیش‌بینی حملات، پیشنهاد یک راه‌حل دفاعی و حمله مناسب به کار گرفت.	۴.۳۱	۰.۶۸۲	۲۱	۴.۶۵	۴.۲۸	۱.۱۱۰
۱۱	هوش مصنوعی و الگوریتم‌های یادگیری ماشین را می‌توان در تشخیص و طبقه‌بندی سیگنال‌های دشمن به کار گرفت.	۴.۳۶	۰.۶۶۴	۱۴	۴.۵۴	۴۴.۱۸	۰.۰۲۷
۱۲	هوش مصنوعی را می‌توان در سنجش طیف الکترومغناطیس به کار گرفت.	۴.۴۵	۰.۶۸۱	۴	۴.۶۳	۴.۲۷	۰.۹۷۵
۱۳	الگوریتم‌های طراحی هوشمند را می‌توان در جمع‌آوری اطلاعات اخلالگران و فریب‌دهنده‌ها به کار گرفت.	۴.۴۵	۰.۶۰۵	۳	۴.۶۲	۴.۲۸	۱.۰۳۵
۱۴	سیستم‌های فازی و الگوریتم‌های ژنتیک را می‌توان در پردازش سیگنال به کار گرفت.	۴.۴۷	۰.۵۳۱	۲	۴.۶۴	۴.۳۱	۱.۴۱۲

۱۵	پردازش زبان طبیعی را می‌توان در تحلیل اطلاعات متنی از منابع مختلف به کار گرفت.	۴.۳۱	۰.۸۵۰	۲۰	۴.۵۲	۴.۱۱	۰.۴۶۱-
۱۶	هوش مصنوعی را می‌توان در استخراج عملکرد عملیات پشتیبانی الکترونیک و خودکارسازی تمامی فرایند پشتیبانی الکترونیک به کار گرفت.	۴.۳۸	۰.۷۱۸	۱۲	۴.۵۶	۴.۱۹	۰.۱۵۸
۱۷	الگوریتم‌های تشخیص الگو و روندهای جدید را می‌توان در تحلیل داده‌های اخذشده به کار گرفت.	۴.۲۴	۰.۸۶۷	۲۵	۴.۴۴	۴.۰۳	۱.۱۷۷-
۱۸	تجزیه‌وتحلیل هوشمند داده‌های سنجش را می‌توان برای ارتباطات و اداره فضای سیگنالی به کار گرفت.	۴.۳۵	۰.۷۳۷	۱۶	۴.۵۴	۴.۱۶	۰.۱۰۴-
۱۹	هوش مصنوعی را می‌توان در داده‌کاوی به‌منظور تلفیق داده‌ها و سیگنال‌های به‌دست‌آمده به کار گرفت.	۴.۳۸	۰.۵۹۲	۱۱	۴.۵۵	۴.۲۰	۰.۱۷۴
۲۰	الگوریتم‌های یادگیری عمیق را می‌توان در تجزیه‌وتحلیل داده‌های رمز شده به کار گرفت.	۴.۴۵	۰.۶۵۶	۶	۴.۶۳	۴.۲۷	۰.۹۹۴
۲۱	سامانه‌های خبره مجهز به یادگیری عمیق را می‌توان در کنترل هوشمند مثبت و منفی به کار گرفت.	۴.۳۱	۰.۹۷۷	۲۲	۴.۵۳	۴.۰۹	۰.۴۳۰-
۲۲	سامانه‌های خبره و یادگیری عمیق را می‌توان در اولویت‌بندی و تخصیص فرکانس‌ها به کار گرفت.	۴.۳۰	۰.۸۹۶	۲۳	۴.۵۱	۴.۰۹	۰.۵۷۶-
۲۳	رادیو شناختی را می‌توان برای ایجاد یک بستر امن به کار گرفت.	۴.۳۰	۰.۸۴۶	۲۴	۴.۵۰	۴.۱۰	۰.۵۸۴-
۲۴	الگوریتم‌های هوشمند را می‌توان برای جلوگیری از عملیات فریب دشمن به کار گرفت.	۴.۳۹	۰.۸۲۳	۱۰	۴.۵۹	۴.۱۹	۰.۲۷۱
۲۵	الگوریتم‌های یادگیری عمیق را می‌توان در تجزیه‌وتحلیل داده‌ها جهت رمزنگاری به کار گرفت.	۴.۰۹	۱.۰۱۸	۲۷	۴.۳۱	۳.۸۶	۲.۴۱۶-
۲۶	هوش مصنوعی را می‌توان در اجرای هوشمند توسعه و بهبود روش‌های ضداختلال و آشکارسازی اخلال‌گرها به کار گرفت.	۴.۴۱	۰.۶۵۰	۸	۴.۵۹	۴.۲۳	۰.۵۸۲
۲۷	هوش مصنوعی را می‌توان در سایت‌یابی، با درنظرگرفتن ملاحظات مربوط به اختفا و پوشش الکترونیکی به کار گرفت.	۴.۳۱	۰.۶۵۹	۱۹	۴.۶۱	۴.۲۵	۰.۷۷۱

۱-۸۹.۴۵ درصد افراد جامعه نمونه (اکثریت مطلق) معتقدند که می‌توان هوش مصنوعی را در اجرا (حمله الکترونیک، پشتیبانی الکترونیک و حفاظت الکترونیک) عملیات جنگ الکترونیک ارتش مبتنی بر جنگ‌های آینده به‌کارگرفت.

۲-با توجه به اولویت‌بندی انجام‌گرفته بر اساس ضرایب تعیین، در کلیه مؤلفه‌ها، به‌کارگیری هوش مصنوعی در تشخیص نقاط ضعف سیستم‌های موردحمله، از بالاترین اولویت برخوردار بوده و بعدازآن به‌کارگیری سیستم‌های فازی و الگوریتم‌های ژنتیک در پردازش سیگنال، در اولویت دوم قرارگرفته است. همچنین به‌کارگیری الگوریتم‌های طراحی هوشمند در جمع‌آوری اطلاعات اخلالگران و فریب‌دهنده‌ها، در اولویت سوم قرار دارد.

نتیجه‌گیری و ارائه پیشنهادها

در جنگ‌های پیش رو برنامه‌ریزی در جهت استفاده از همه ابزارهای هوش مصنوعی در تمامی سطوح آن در حمله، پشتیبانی و حفاظت الکترونیک لازم و ضروری است.
نتایج حاصله بیانگر این واقعیت است که ۸۹.۴۵ درصد افراد جامعه نمونه (اکثریت مطلق) با میانگین۴.۳۶معتقدند که می‌توان هوش مصنوعی را در اجرا (حمله الکترونیک، پشتیبانی الکترونیک و حفاظت الکترونیک)، عملیات جنگ الکترونیک به‌کارگیری.
به‌کارگیری هوش مصنوعی در تشخیص نقاط ضعف سیستم‌های موردحمله، به‌کارگیری سیستم‌های فازی و الگوریتم‌های ژنتیک در پردازش سیگنال، به‌کارگیری الگوریتم‌های طراحی هوشمند در جمع‌آوری اطلاعات اخلالگران و فریب‌دهنده‌ها، مهم‌ترین موارد استفاده هوش مصنوعی در اجرای عملیات جنگ الکترونیک در جنگ‌های آینده است.
پیشنهاد می‌گردد پژوهشی در خصوص ارائه مدل به‌کارگیری هوش مصنوعی در سایر حوزه‌های عملیات جنگال صورت پذیرد.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

- سرمایه‌گذاری هدفمند بر توسعه و ادغام هوش مصنوعی در عملیات جنگ الکترونیک
- ایجاد زیرساخت داده و آموزش تخصصی برای بهره‌برداری از الگوریتم‌های پیشرفته
- تدوین راهبردهای تطبیقی و انعطاف‌پذیر برای مواجهه با تهدیدات نوین

قدردانی

از کلیه فرماندهان، استادان، اندیشمندان و پژوهشگرانی که در خلال تحقیق خالصانه دیدگاه‌ها و نظرات علمی خود را ارائه کردند، تشکر و قدردانی می‌شود.

تضاد منافع

بدین‌وسیله تیم پژوهش تصریح می‌نمایند که هیچ‌گونه تضاد منافعی در خصوص مطالعه حاضر وجود ندارد.

منابع:

- اسدالله زاده، محمد، طرح‌ریزی عملیات جنگ الکترونیک، دانشگاه فرماندهی و ستاد آجا،۱۴۰۱
- ال شارپ، والتر، رهنامه جنگ الکترونیک مشترک آمریکا، ترجمه علیرضا جواهری، مؤسسه آموزشی و تحقیقاتی صنایع دفاع، ۱۳۹۴
- امیرجاوید، شبنم، آینده جنگ و هوش مصنوعی، انتشارات پشتیبان، ۱۳۹۸
- بیگدلی، حمید ؛ پرتوی، محمدتقی، اصول و مبانی هوش مصنوعی با رویکرد نظامی، انتشارات دافوس، ۱۴۰۰
- پناهی، علی، بررسی میزان تأثیر تهدیدات الکترونیکی نیروهای خودی بر فرایند تصمیم‌گیری عملیات جنگال در نبرد ناهمتراز، علوم و فنون نظامی، ۱۳۹۸ (DOI: 10.22034/qjmst.2020.38956/)
- پورابی، شارما، سامانه‌های جنگ الکترونیک به کمک هوش مصنوعی، روندهای اخیر و برنامه‌های در حال تکامل، IEEE، ۲۰۲۰
- پورموسوی، میرامیر، کاربرد هوش مصنوعی در سیستم‌های نظامی، پایان‌نامه کارشناسی‌ارشد، دانشگاه خوارزمی، شهریور ۱۴۰۱
- جی راسل، استیوارت؛ نورویگ، پیتر، مترجم، حاج رسولی‌ها، حسین، هوش مصنوعی راهبردی نوین، نیاز دانش، ۱۳۹۱
- رضایی، محسن؛ رشید، غلامعلی، پوردستان، احمدرضا، مؤلفه‌ها و ویژگی‌های فرماندهی و کنترل هوشمند در صحنه نبرد، فصلنامه علوم و فنون نظامی، ۱۳۹۹ (DOI:10.22034/qjmst.2021.243882)
- سجادی اصیل، وحید، عملیات حمله و دفاع الکترونیکی و سایبری، انتشارات دافوس، ۱۴۰۱
- شرفی‌نژاد، سیّدرضا؛ رضوی‌زاده، محمودرضا، شناسایی تهدیدهای نوین جنگ الکترونیک در حوزه دریایی باتکیه‌بر هوش مصنوعی و داده‌کاوی، دوفصلنامه مهندسی شناورهای تندرو، مرداد،۱۴۰۲ (URL: https://journals.ihu.ac.ir/article_209029)
- صابری، علی، علوم‌شناختی در هوش مصنوعی، کنفرانس ملی رویکردهای نوین علوم‌انسانی در قرن ۲۱، آذر ۱۳۹۶
- عباسی، مهناز؛ عباسی، حمیدرضا، مروری بر فناوری هوش مصنوعی، چالش‌ها و کاربردهای نظامی نوپدید آن، هشتمین همایش ملی علوم و مهندسی دفاعی، تهران، دانشگاه افسری و تربیت پاسداری امام حسین (ع)، ۱۴۰۰ (URL: https://civilica.com/doc/1577137)
- فرحبخت، احمدرضا؛ دهقانی، مهدی، همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی، فصلنامه امنیت ملی، سال نهم، شماره ۳۱، ۱۳۹۸ (URL: https://ns.sndu.ac.ir/article_481)
- قلی‌زاده، مهدی، کاربردها و چالش‌های فناوری هوش مصنوعی در حوزه نظامی، هفتمین کنفرانس ملی مطالعات مدیریت در علوم‌انسانی، ۱۴۰۰ (URL: https://civilica.com/doc/1475550)

- مسلمی، حسین ؛ خنجری، حسین، مدیریت عملیات جنگ الکترونیک و سایبری، دانشگاه فرماندهی و ستاد آجا، ۱۳۹۶
- مسلمی، حسین؛ بیات، عیسی، هوش مصنوعی فرصت‌ها، چالش‌ها و تهدیدها آن در سازمان‌های نظامی، انتشارات دافوس، ۱۴۰۳
- ناصری، علی، روند تکامل جنگ الکترونیک و تقسیمات آن، فصلنامه فرآماد، شماره ۱۴۰۲،۲۳ (URL: https://scmj.ihu.ac.ir/article_205299)
- نقشه راه توسعه ملی هوش مصنوعی، پژوهشگاه ارتباطات و فناوری اطلاعات، مهر ۱۴۰۱
- نقی‌بیرانوند، مسلم؛ مزید، محمدهادی، به‌کارگیری هوش مصنوعی در سیستم‌های جنگ الکترونیک، چهاردهمین کنفرانس ملی مهندسی برق، کامپیوتر و مکانیک، اردیبهشت ۱۴۰۱ (URL: https://civilica.com/doc/1458071/)
- نوروزی، عرفانه؛ بیرانوند، آریا، تأثیر هوش مصنوعی در ارتقا توانمندی‌های زیر سامانه‌های الکترونیکی، مخابراتی و سایبری در بستر جنگ الکترونیک، مجله نخبگان علوم و مهندسی، جلد ۸، شماره ۵، سال ۱۴۰۲ (URL: https://www.sid.ir/paper/1113805/fa)

- Abbasi, M., & Abbasi, H. (2021). A review of artificial intelligence technology, its emerging military challenges, and applications. *8th National Conference on Defense Science and Engineering*, Imam Hossein Military and Revolutionary Guard Training University, Tehran, Iran. (In Persian). URL: https://civilica.com/doc/1577137
- Amir Javid, S. (2019). *The future of war and artificial intelligence*. Poshtiban Publications. (In Persian
- Department of the Army. (n.d.). *Army Doctrine Publication (ADP 5-0)*.
- Department of the Army. (2012). *Army Doctrine Reference Publication (ADRP 3-90)*.
- Department of the Army. (2018). *Army Doctrine Reference Publication (ADRP 2-0) (FM 2-0)*.
- Asadollahzadeh, M. (2022). *Electronic warfare operations planning*. AJA Command and Staff University. (In Persian).
- Bigdeli, H., & Partovi, M. T. (2021). *Principles and foundations of artificial intelligence with a military approach*. AJA Command and Staff University Publications. (In Persian).
- Farahbakht, A., & Dehghani, M. (2019). The convergence of electronic warfare and cyber warfare and the requirements for its implementation in military organizations. *National Security Quarterly, 9*(31). (In Persian). URL: https://ns.sndu.ac.ir/article_481
- Department of the Army. (2017). *FM 3-12: Cyberspace and electronic warfare operations*.
- Department of the Army. (2012, November 9). *FM 3-36*. Washington, DC.

- Department of the Army. (2005, January). *FM 5-0: Army planning and orders production.*
- Gholizadeh, M. (2021). Applications and challenges of artificial intelligence technology in the military field. *7th National Conference on Management Studies in Humanities*. (In Persian). URL: https://civilica.com/doc/1475550
- James, J. (2021). *Artificial intelligence and the future of warfare: The USA, China, and strategic stability*.
- Andrusenko, K. Z., & Andrusenko, J. (2021). *Cognitive electronic warfare: An artificial intelligence approach*. Library of Congress Cataloging-in-Publication Data.
- Lee, D., & Yoon, S. N. (2021). Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges. *International Journal of Environmental Research and Public Health, 18*(4), 1438. DOI:10.3390/ijerph18041438
- Sharp, L. W. (2015). *U.S. joint electronic warfare guideline* (A. Javaheri, Trans.). Defense Industries Research and Training Institute. (In Persian).
- Moslemi, H., & Khanjari, H. (2017). Electronic and cyber warfare operations management. AJA Command and Staff University. (In Persian).
- Naghibeyranvand, M., & Mazidi, M. H. (2022, May). Application of artificial intelligence in electronic warfare systems. In the 14th National Conference on Electrical, Computer, and Mechanical Engineering. URL: https://civilica.com/doc/1458071
- Naseri, A. (2023). The evolution of electronic warfare and its classifications. Faramaad Quarterly, (23), Article 1402. URL: https://scmj.ihu.ac.ir/article_205299
- Norouzi, E., & Beiranvand, A. (2023). The impact of artificial intelligence on improving the capabilities of electronic, telecommunication, and cyber subsystems in the context of electronic warfare. *Journal of Elite Science and Engineering, 8*(5). (In Persian). URL: https://www.sid.ir/paper/1113805/fa
- Schmitt, N. (2019). Autonomous weapon systems and international humanitarian law: A reply to the critics. *Harvard Law School*.
- Popenici, S. A., & Kerr, S. (2017). Exploring the impact of artificial intelligence on teaching and learning in higher education. *Research and Practice in Technology Enhanced Learning, 12*(1). DOI: 10.1186/s41039-017-0062-8
- Panahi, A. (2019). Investigating the impact of electronic threats from insider forces on the decision-making process of jungle operations in asymmetric warfare. *Military Science and Technology*. (In Persian). DOI: /10.22034/qjmst.2020.38956
- Pourmousavi, M. (2022). *Application of artificial intelligence in military systems* (Master's thesis). Kharazmi University. (In Persian).

- Rezaei, M., Rashid, G., & Pourdastan, A. (2020). Components and characteristics of intelligent command and control on the battlefield. *Military Science and Technology Quarterly*. (In Persian). DOI:10.22034/qjmst.2021.243882
- Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science, 10*(5). DOI:10.22161/ijaers.105.8
- Saberi, A. (2017). Cognitive sciences in artificial intelligence. *National Conference on New Approaches to Humanities in the 21st Century*. (In Persian).
- Sajjadi Asil, V. (2022). *Electronic and cyber attack and defense operations*. Dafoos Publications. (In Persian).
- Sharafinejad, S. R., & Razavizadeh, M. (2023). Identifying new threats of electronic warfare in the maritime field based on artificial intelligence and data mining. *Journal of High Speed Vessel Engineering*. (In Persian). URL: https://journals.ihu.ac.ir/article_209029
- Sharma, P., & Kumar Sarma, K. (2020). Artificial intelligence-aided electronic warfare systems: Recent trends and evolving applications. *IEEE*, December 2020. https://doi.org/10.1109/ICCCNT49239.2020.9225419
- Singh, T., & Gulhane, A. (2018, January 6). 8 key military applications for artificial intelligence in 2018. MarketResearch.com Blog. URL: https://blog.marketresearch.com
- Waghray, N. (2018, December). Electronic warfare: The next step in national security. Radar & Control Systems Dept, Military College of Electronics & Mechanical Engineering, Secunderabad. DOI:10.1109/INDCON.2011.6139348
- Yang, Z. (2020). Modelling and simulation of cognitive electronic attack under the condition of system of systems combat. *Defence Science Journal, 70*(3), 261-268. https://doi.org/10.14429/dsj.70.15139
- Zhang, YuLong & Dai, Zijie & Zhang, LongFei & Wang, ZhengYi & Chen, Li & Zhou, YuZhen. (2020). Application of Artificial Intelligence in Military: From Projects View. 113-116. DOI:10.1109/BigDIA51454.2020.00026