Emergency Management, Vol. 15, No. 1, pp: 114-134

The Role of Cognitive Computing in Cognitive Warfare with a Defensive Approach

Seyyed Hamidreza Aarabi*[1], Naser Poursadegh[2]

1. Ph.D. in Strategic Management of Cyber Security, Supreme National Defense University, Tehran, Iran (Corresponding Author) hr.aarabi99@sndu.ac.ir
2. Prof., School of Strategic Management, Supreme National Defense University, Tehran, Iran

https://dor.isc.ac/dor/20.1001.1.23453915.1404.14.2.6.6

Original Paper

Cognitive warfare, as one of the most complex forms of contemporary conflicts, targets perception, cognition, and decision-making processes of individuals and societies, thereby posing a fundamental threat to national security. This study aims to elucidate the strategic role of cognitive computing in strengthening cognitive defense and to propose a localized framework for countering cognitive threats. The research employed a meta-synthesis approach based on the seven-step model of Sandelowski and Barroso. Data were systematically collected from 58 credible Persian and English sources, including articles, books, and technical reports, published between 2020 and 2024. Sources were selected purposefully according to predefined inclusion and exclusion criteria. To enhance external validity, the Delphi method was applied with the participation of 12 domain experts. Qualitative data were coded using MAXQDA software and validated through triangulation, combining document analysis, expert opinions, and simulation. Findings indicate that cognitive computing, leveraging natural language processing, deep learning, and inferential reasoning, plays a strategic role in five key domains: (1) automated detection and tracking of cognitive threats, (2) big data analytics in cyberspace to uncover hidden patterns of cognitive disruption, (3) enhancing informational resilience through cognitive training and critical thinking, (4) forecasting cognitive attacks via predictive modeling and scenario simulation, and (5) providing adaptive and intelligent real-time responses. Quantitative validation indices, including content validity (CVI=0.88), reliability (Cronbach's alpha=0.89), and expert consensus (Kendall's W=0.89), confirm the robustness of the proposed model. The main contribution of this research lies in the design and localization of a three-layer framework—comprising hybrid infrastructure, cognitive computing, and cognitive services—tailored to the context of the Islamic Republic of Iran. This framework can serve as a roadmap for defense and security organizations in confronting cognitive warfare and reinforcing national security.

Keywords:
Cognitive Computing, Cognitive Warfare, Cognitive Defense, Cybersecurity, Artificial Intelligence.

OPEN ACCESS

Received: Oct. 28, 2025
Revised: Dec. 19, 2025
Accepted: Feb. 05, 2026

To cite this article:
Aarabi, S. H., Poursadegh, N., 2026. The role of cognitive computing in cognitive warfare with a defensive approach. *Emergency Management*, 15(1), 114-134.
https://dor.isc.ac/dor/20.1001.1.23453915.1404.14.2.6.6.

Use your device to scan and read the article online

مدیریت بحران، دوره ۱۵، شماره ۱، صفحه: ۱۳۴-۱۱۴

نقش رایانش شناختی در جنگ شناختی با رویکرد پدافندی

سید حمیدرضا اعرابی[*۱]، ناصر پورصادق[۲]

۱- دکترای مدیریت راهبردی امنیت فضای سایبر، دانشگاه عالی دفاع ملی، تهران، ایران
(نویسنده مسئول) hr.aarabi99@sndu.ac.ir
۲- استاد، دانشکده مدیریت راهبردی، دانشگاه عالی دفاع ملی، تهران، ایران

مقاله پژوهشی
https://dor.isc.ac/dor/20.1001.1.23453915.1404.14.2.6.6

چکیده

جنگ شناختی به‌عنوان یکی از پیچیده‌ترین اشکال منازعات معاصر، با هدف اثرگذاری بر ادراک، شناخت و فرآیند تصمیم‌گیری افراد و جوامع، تهدیدی بنیادین برای امنیت ملی به شمار می‌آید. پژوهش حاضر با هدف تبیین نقش راهبردی رایانش شناختی در تقویت پدافند شناختی و ارائه چارچوبی بومی برای مقابله با تهدیدات شناختی انجام شده است. روش تحقیق مبتنی بر فراترکیب و چارچوب هفت مرحله‌ای سندلوسکی و باروسو بوده و داده‌ها از طریق تحلیل نظام‌مند ۵۸ منبع معتبر فارسی و لاتین در بازه زمانی ۲۰۲۰ تا ۲۰۲۴ گردآوری شد. انتخاب منابع به‌صورت هدفمند و بر اساس معیارهای ورود و خروج مشخص صورت پذیرفت. به‌منظور ارتقای اعتبار بیرونی یافته‌ها، از روش دلفی با مشارکت ۱۲ خبره بهره گرفته شد. داده‌های کیفی با استفاده از نرم‌افزار MAXQDA کدگذاری و از طریق روش مثلث‌سازی (ترکیب تحلیل اسناد، نظرات خبرگان و شبیه‌سازی) اعتبارسنجی شدند. یافته‌ها نشان می‌دهد رایانش شناختی با اتکا به پردازش زبان طبیعی، یادگیری عمیق و استدلال استنتاجی، در پنج حوزه کلیدی نقش‌آفرینی دارد: ۱) شناسایی و ردیابی خودکار تهدیدات شناختی، ۲) تحلیل کلان داده‌های سایبری برای کشف الگوهای تخریب شناختی، ۳) ارتقای تاب‌آوری اطلاعاتی از طریق آموزش و تقویت تفکر انتقادی، ۴) پیش‌بینی حملات شناختی با بهره‌گیری از مدل‌سازی و شبیه‌سازی و ۵) ارائه پاسخ‌های تطبیقی و هوشمند در زمان واقعی. شاخص‌های کمی شامل روایی محتوا (CVI=0.88)، پایایی (آلفای کرونباخ=۰،۸۹) و ضریب توافق کندال (W=0.89) اعتبار مدل پیشنهادی را تائید می‌کنند. نوآوری اصلی این پژوهش در طراحی و بومی‌سازی یک چارچوب سه لایه (زیرساخت ترکیبی، رایانش شناختی و خدمات شناختی) برای جمهوری اسلامی ایران است. این چارچوب می‌تواند به‌عنوان نقشه راهی کارآمد برای سازمان‌های دفاعی و امنیتی در مواجهه با جنگ‌های شناختی و ارتقای امنیت ملی مورداستفاده قرار گیرد.

واژه‌های کلیدی:
رایانش شناختی، جنگ شناختی، پدافند شناختی، امنیت سایبری، هوش مصنوعی.

دریافت: ۱۴۰۴/۰۸/۰۶
اصلاح: ۱۴۰۴/۰۹/۲۸
پذیرش: ۱۴۰۴/۱۱/۱۶

برای ارجاع به این مقاله به صورت زیر اقدام بفرمایید:
اعرابی، س.ح.، پورصادق، ن.، ۱۴۰۵، نقش رایانش شناختی در جنگ شناختی با رویکرد پدافندی. *مدیریت بحران*، ۱۵(۱)، ۱۳۴-۱۱۴
https://dor.isc.ac/dor/20.1001.1.23453915.1404.14.2.6.6

از دستگاه خود برای اسکن و خواندن مقاله به صورت آنلاین استفاده کنید

۱- مقدمه

در سال‌های اخیر، «جنگ شناختی» به‌عنوان یکی از ابعاد نوین نبردهای اطلاعاتی و روانی، جایگاه ویژه‌ای در مطالعات امنیتی و فناوری‌های نوظهور یافته است. این نوع جنگ با هدف تأثیرگذاری بر فرآیندهای ذهنی انسان، از ابزارهایی چون هوش مصنوعی، واقعیت مجازی و شبکه‌های اجتماعی بهره می‌گیرد تا ادراک، تصمیم‌گیری و رفتار افراد را تحت کنترل درآورد. مطالعه‌ای توسط آلوارو پاستور در مقاله‌ای تحت عنوان " Cognitive Warfare" به بررسی تأثیر واقعیت مجازی بر حافظه و شناخت انسان پرداخته و نشان می‌دهد که محیط‌های دیجیتال می‌توانند در بازنویسی تجربه‌های ذهنی نقش داشته باشند.، در همین مقاله به بررسی تأثیر محیط‌های واقعیت مجازی بر حافظه و شناخت انسان پرداخته است. او نشان می‌دهد که تجربه‌های دیجیتال، به‌ویژه در محیط‌های غوطه‌ور، می‌توانند به بازنویسی خاطرات و تغییر در برداشت‌های فردی منجر شوند. این یافته‌ها، پیامدهای مهمی برای آموزش نظامی، بازپروری روانی و حتی تبلیغات تجاری دارند [۱].

در همین راستا، فدریکو از مؤسسه تحقیقات خلع سلاح سازمان ملل، در مقاله‌ای به بررسی ابعاد حکمرانی و امنیتی جنگ شناختی پرداخته است. این مقاله بخشی از مجموعه مطالعات مرکز سیاست‌گذاری امنیتی ژنو است [۲].

از منظر فناوری، مقاله‌ای دیگر به بررسی نقش هوش مصنوعی در جنگ‌های شناختی پرداخته و تأکید می‌کند که الگوریتم‌های یادگیری ماشین می‌توانند در عملیات نفوذ و دستکاری شناختی به کار گرفته شوند. در مرکز سیاست‌گذاری امنیتی ژنو، جنگ شناختی را به‌عنوان «حکمرانی بر زیرساخت‌های ذهنی» توصیف می‌کند. او تأکید می‌کند که بازیگران دولتی و غیردولتی با استفاده از ابزارهای دیجیتال، به‌ویژه در بسترهای شبکه‌های اجتماعی، به دنبال ایجاد اختلال در انسجام شناختی جوامع هستند. این اختلال می‌تواند به شکل تضعیف اعتماد عمومی، دو قطبی‌سازی سیاسی، یا حتی تحریک رفتارهای خشونت‌آمیز بروز کند. نقش هوش مصنوعی در جنگ‌های شناختی نشان می‌دهد که الگوریتم‌های یادگیری ماشین، با تحلیل داده‌های رفتاری کاربران، می‌تواند محتوای هدفمند تولید کرده و در زمان مناسب به مخاطب عرضه کند. این فرآیند که به آن «مهندسی ادراک» گفته می‌شود، به‌طور خاص در عملیات نفوذ سیاسی و تبلیغات انتخاباتی کاربرد دارد [۳].

همچنین، کارلی در مقاله‌ای به بررسی الگوهای فریبنده در تعامل انسان و ربات پرداخته و نشان می‌دهد که طراحی سیستم‌های تعاملی می‌تواند به‌طور ناخواسته یا عمدی منجر به دستکاری شناختی شود. این مطالعه به بررسی الگوهای فریبنده در طراحی رابط‌های کاربری پرداخته است. او هشدار می‌دهد که بسیاری از سیستم‌های تعاملی، به‌طور ناخواسته یا عمدی، کاربران را به تصمیم‌گیری‌هایی سوق می‌دهند که با منافع آنها هم‌راستا نیست. این نوع «دستکاری نرم» می‌تواند در قالب طراحی‌های گمراه‌کننده، پیام‌های تأییدی، یا الگوریتم‌های پیشنهاددهنده ظاهر شود [۴].

در حوزه نظامی، بریجز از آزمایشگاه نیروی هوایی ایالات‌متحده در مطالعات خود به بررسی تحریک مغزی غیرتهاجمی و کاربرد آن در آموزش شناختی پرداخته است. این مطالعات نشان می‌دهند که تحریک مستقیم مغز می‌تواند در افزایش توانایی‌های شناختی نیروهای نظامی مؤثر باشد. این فناوری‌ها می‌توانند در افزایش تمرکز، حافظه کاری و سرعت تصمیم‌گیری نیروهای نظامی مؤثر باشند. این یافته‌ها، چشم‌انداز جدیدی را برای ارتقاء عملکرد شناختی در محیط‌های پرتنش و پیچیده نظامی فراهم

می‌کنند [۵].

پژوهش‌های اخیر نشان می‌دهند که جنگ شناختی نه‌تنها یک تهدید امنیتی نوظهور است، بلکه چالشی میان‌رشته‌ای در حوزه‌های فناوری، روان‌شناسی، حقوق بین‌الملل و سیاست‌گذاری عمومی محسوب می‌شود. برای مقابله مؤثر با این پدیده، توسعه چارچوب‌های اخلاقی، حقوقی و فناورانه ضروری است. جنگ شناختی را می‌توان به‌عنوان یک پدیده میان‌رشته‌ای در نظر گرفت که در تقاطع علوم اعصاب، فناوری اطلاعات، روان‌شناسی اجتماعی و مطالعات امنیتی قرار دارد. پژوهش‌های اخیر نشان می‌دهند که مقابله با این نوع جنگ، نیازمند توسعه چارچوب‌های اخلاقی، حقوقی و فناورانه است.

همچنین، افزایش تاب‌آوری شناختی شهروندان از طریق آموزش سواد رسانه‌ای، تفکر انتقادی و آگاهی از سازوکارهای دستکاری اطلاعات، از جمله راهکارهای کلیدی در مواجهه با این تهدید نوظهور محسوب می‌شود. ازاین‌رو جنگ شناختی به‌عنوان پیچیده‌ترین شکل منازعه در عصر حاضر، «عرصه نبرد برای تسلط بر ادراک، شناخت و تصمیم‌گیری انسان‌ها» تعریف می‌شود . برخلاف جنگ سنتی که فیزیک و قلمرو جغرافیایی را هدف می‌گیرد، جنگ شناختی مستقیماً «فضای ذهنی» جامعه را نشانه می‌رود در این پارادایم، دشمن با بهره‌گیری از فناوری‌های پیشرفته، به دنبال دستکاری افکار عمومی، تضعیف اعتماد اجتماعی و تغییر رفتارهای جمعی است [۶].

رایانش شناختی به‌عنوان «سیستم‌های محاسباتی که با الهام از معماری عصبی مغز انسان، قادر به شبیه‌سازی فرآیندهای تفکر، یادگیری و استدلال هستند»، ظرفیت بی‌بدیلی برای تقویت پدافند شناختی ارائه می‌دهد. این فناوری با تلفیق هوش مصنوعی، پردازش زبان طبیعی و یادگیری ماشین، امکان درک، تحلیل و پاسخ به تهدیدات شناختی را در مقیاس کلان فراهم می‌سازد [۶].

شکاف پژوهشی حاضر در فقدان چارچوبی نظام‌مند برای بهره‌گیری از رایانش شناختی در پدافند شناختی است. این مقاله درصدد است با تحلیل آثار پژوهشگران و نیز ادبیات بین‌المللی، به این شکاف پاسخ گوید. سؤال اصلی پژوهش این است: «رایانش شناختی» چه نقش‌ها و کارکردهایی در تقویت پدافند شناختی دارد و چگونه می‌توان از آن در مقابله با تهدیدات جنگ شناختی بهره برد؟

تحولات شگرف در عرصه‌ی فناوری‌های ارتباطی و اطلاعاتی، به‌ویژه ظهور شبکه‌های اجتماعی و پلتفرم‌های داده‌محور، ساختار تهدیدات امنیتی را دستخوش دگرگونی بنیادی کرده است. امروز، تأکید در میدان نبرد از توان سخت به توان نرم و از حمله فیزیکی به «حمله شناختی» تغییریافته است. جنگ شناختی که اغلب به‌عنوان ششمین حوزه عملیاتی ناتو شناخته می‌شود، نهادهای اجتماعی و افراد را هدف قرار می‌دهد تا با دستکاری ادراک، باورها و ارزش‌ها، بر فرآیند تصمیم‌گیری آنها تأثیر بگذارد و در نهایت، اراده‌ی سیاسی و اجتماعی جامعه هدف را دچار فروپاشی کند. این جنگ، با تکیه بر ابزارهایی چون اخبار جعلی (فیک‌نیوز)، دیپ فیک‌ها و کمپین‌های اطلاعاتی پیچیده، فضایی از عدم اطمینان، بی‌اعتمادی و قطبی‌سازی اجتماعی ایجاد می‌کند.

در پاسخ به این تهدیدات نامرئی و با سرعت بالا، لزوم استفاده از ابزارهای دفاعی مبتنی بر هوش مصنوعی و مدل‌های پیشرفته تحلیل داده، بیش‌ازپیش آشکار می‌شود .رایانش شناختی که تلاش دارد با شبیه‌سازی ساختارهای مغزی انسان، داده‌ها را نه‌تنها پردازش، بلکه درک و استدلال کند، به‌عنوان راه‌حلی کلیدی مطرح

می‌شود. توانایی این فناوری در تحلیل زمینه‌ای[1]، استخراج دانش از داده‌های خام و تعامل طبیعی با محیط، آن را به ابزاری قدرتمند برای پدافند شناختی تبدیل می‌کند.

با گسترش فناوری‌های نوین ارتباطی و اطلاعاتی، میدان‌های نبرد نیز دستخوش تحولاتی بنیادین شده‌اند؛ به‌گونه‌ای که امروزه جنگ‌های سنتی جای خود را به نبردهای پیچیده‌تری چون جنگ‌های شناختی داده‌اند. در این نوع از جنگ‌ها، تمرکز اصلی بر تسخیر ذهن و تغییر نگرش، باور و رفتار افراد و جوامع هدف است، نه صرفاً تخریب فیزیکی یا تسلط سرزمینی. جنگ‌های شناختی با بهره‌گیری از ابزارهایی چون اطلاعات نادرست، عملیات روانی، تبلیغات هدفمند و دست‌کاری در ادراک عمومی، به دنبال تضعیف انسجام اجتماعی، بی‌ثبات‌سازی جوامع و تأثیرگذاری بر تصمیم‌گیری‌های کلان هستند.

در این میان، رایانش شناختی به‌عنوان یکی از پیشرفته‌ترین شاخه‌های علوم رایانه، با الگوبرداری از فرآیندهای ذهنی انسان همچون یادگیری، استدلال، درک زبان طبیعی و تصمیم‌گیری، توانسته است بستری نوین برای مقابله با تهدیدات شناختی فراهم آورد. این فناوری با تحلیل داده‌های کلان، شناسایی الگوهای پنهان و پیش‌بینی رفتارهای شناختی، می‌تواند نقش کلیدی در طراحی سامانه‌های دفاعی ایفا کند که قادر به شناسایی و خنثی‌سازی حملات شناختی در مراحل اولیه باشند.

هدف این مقاله، بررسی نقش و کارکردهای رایانش شناختی در جنگ‌های شناختی با تأکید بر رویکرد پدافندی است. در این راستا، تلاش می‌شود تا ضمن تبیین مفاهیم بنیادین، به تحلیل ظرفیت‌های کاربردی این فناوری در ارتقاء امنیت شناختی و تقویت تاب‌آوری ذهنی در برابر تهدیدات نوظهور پرداخته شود. این پژوهش بر آن است تا با ارائه چارچوبی مفهومی و کاربردی، زمینه‌ساز توسعه راهبردهای دفاعی مؤثر در عصر جنگ‌های شناختی باشد. مسئله اصلی پژوهش در این چارچوب مطرح می‌شود که «رایانش شناختی چگونه می‌تواند به‌عنوان یک سیستم دفاعی کارآمد و پیشگیرانه در برابر نفوذهای شناختی و عمل کند و ساختار سیستم‌های پدافندی موجود را ارتقاء دهد؟»

۲- مرور پیشینه و مبانی نظری

نظریه جنگ شناختی بر این اصل استوار است که میدان اصلی نبرد، ذهن انسان است و پیروزی در این عرصه نه از طریق ابزارهای نظامی، بلکه از راه متقاعدسازی، تغییر درک و بازآفرینی شناخت حاصل می‌شود. در این چارچوب، عملیات شناختی با هدف مداخله در حلقه تصمیم‌گیری OODA (مشاهده، جهت‌گیری، تصمیم‌گیری، اقدام) دشمن طراحی می‌شود؛ به‌گونه‌ای که با ایجاد اختلال در مراحل ادراکی و شناختی، توانایی تصمیم‌گیری مؤثر از سوی هدف کاهش یابد و رفتارهای مطلوب برای مهاجم شکل گیرد.

رَند والتزمن[2] پژوهشگر ارشد در اندیشکده RAND، یکی از نخستین افرادی است که مفهوم جنگ شناختی را به‌عنوان «هنر فریب دادن مغز یا ایجاد تردید در آن نسبت به آنچه فکر می‌کند می‌داند» معرفی کرده است. پژوهشگر ارشد در اندیشکده RAND و از نخستین افرادی است که به‌طور سیستماتیک درباره جنگ شناختی نوشت. او جنگ شناختی را «هنر فریب دادن مغز» توصیف کرده است. فرماندهان نظامی ناتو، از جمله ژنرال پائولو روگیرو، جنگ شناختی را به‌عنوان حوزه‌ای مستقل و متمایز از جنگ اطلاعاتی و روانی معرفی کرده‌اند، با تأکید بر اینکه هدف آن «نحوه تفکر افراد» است، نه صرفاً

[1] Contextual Analysis

[2] Rand Waltzman

آنچه فکر می‌کنند فرماندهی تحول ناتو (ACT) از سال ۲۰۲۰ به‌طور رسمی جنگ شناختی را به‌عنوان «بُعد ششم جنگ» معرفی کرد و آن را فراتر از جنگ‌های سایبری، اطلاعاتی و روانی دانست. ناتو تأکید دارد که هدف جنگ شناختی، تأثیرگذاری بر نحوه تفکر افراد است، نه صرفاً محتوای فکری آنها. (ویکی)

الیور بیکس[1] و اندرو سواب[2] پژوهشگران حوزه امنیت سایبری که در مقالات خود جنگ شناختی را به‌عنوان راهبردی برای تغییر ادراک و رفتار جوامع هدف معرفی کرده‌اند. (ویکی)

در مجموع، جنگ شناختی مفهومی نوظهور و پویاست که در تعامل میان حوزه‌های نظامی، علوم رفتاری و فناوری‌های نوین شکل گرفته و همچنان درحال‌توسعه است. (ویکی)

نظریه جنگ شناختی[3] برخلاف برخی نظریه‌های کلاسیک نظامی که به یک فرد خاص نسبت داده می‌شوند، محصول تکامل مفهومی در حوزه‌های بین‌رشته‌ای مانند علوم نظامی، روان‌شناسی، علوم اعصاب و فناوری اطلاعات است.

جنگ شناختی با تبدیل ذهن انسان به عرصه‌ای برای درگیری، موجب تحول بنیادین در مفهوم جنگ‌های مدرن شده است. این مقاله با ارائه چارچوبی تحلیلی و دقیق، به تفکیک جنگ شناختی از مفاهیم هم‌پوشان مانند جنگ اطلاعاتی و جنگ روانی می‌پردازد. در این پژوهش، بهره‌گیری از فناوری‌های نوین نظیر هوش مصنوعی و علوم اعصاب به‌عنوان ابزارهایی برای هدف‌گیری ادراک، فرآیندهای تصمیم‌گیری و انسجام اجتماعی، به‌عنوان راهبردهای محوری در اجرای عملیات شناختی مورد تأکید قرار گرفته است. هدف اصلی این تحقیق، شناسایی و تحلیل آسیب‌پذیری‌های اجتماعی-اقتصادی، فرهنگی و روان‌شناختی است که می‌توانند افراد و جوامع خاص را در برابر حملات شناختی آسیب‌پذیرتر سازند. همچنین، ابزارها و تکنیک‌های مورداستفاده در عملیات شناختی و راهکارهای مقابله با پیامدهای آنها بررسی شده‌اند. در کنار این موارد، به پدیده‌هایی نظیر کاپتولوژی نیز پرداخته می‌شود؛ مفهومی که به تأثیرگذاری بر فرآیندهای شناختی بدون نیاز به دستکاری مستقیم اشاره دارد. یافته‌های این پژوهش بر ضرورت اتخاذ رویکردهای بین‌رشته‌ای برای مواجهه مؤثر با چالش‌های ناشی از جنگ شناختی و همچنین تقویت امنیت ملی، تاب‌آوری اجتماعی و تدوین سیاست‌های کلان تأکید دارند [۷].

در چشم‌انداز نوین منازعات، جنگ شناختی به‌عنوان ابزاری پیچیده و چندلایه برای تأثیرگذاری بر ذهن انسان و تغییر رفتارهای فردی و جمعی مطرح شده است. این نوع جنگ با بهره‌گیری از فناوری‌های شناختی، از جمله یادگیری ماشین، تحلیل داده‌های رفتاری و مدل‌سازی ذهنی، به دنبال نفوذ در فرآیندهای ادراکی و تصمیم‌گیری افراد است. هدف نهایی آن، ایجاد اختلال در انسجام اجتماعی و تغییر در الگوهای رفتاری جوامع هدف از طریق عملیات غیرمستقیم و اغلب نامرئی است. چنین تحولاتی، نیازمند بازنگری در مفاهیم سنتی امنیت ملی و توسعه راهبردهای بین‌رشته‌ای برای مقابله با تهدیدات شناختی هستند. جنگ شناختی به‌عنوان پارادایم نوین در عرصه منازعات معاصر، تمرکز اصلی خود را بر تأثیرگذاری بر شناخت، ادراک و تصمیم‌گیری افراد و جوامع قرار داده است [۸]. در این میان، رایانش شناختی با قابلیت‌های منحصربه‌فرد خود، نقش راهبردی در تقویت پدافند شناختی ایفا می‌کند.

در مطالعه‌ای با عنوان «ارائه مدل مفهومی همگرایی فناوری‌های نوظهور در زیست‌بوم

[1] Olivier Bex
[2] Andrew Swab
[3] Cognitive Warfare

رایانش شناختی به‌منظور ارتقای امنیت سایبری» مدل سه لایه‌ای شامل لایه زیرساخت، لایه شناختی و لایه کاربرد ارائه نمودند. یافته‌های این پژوهش نشان می‌دهد که همگرایی فناوری‌های نوظهور در زیست‌بوم رایانش شناختی می‌تواند به بهبود قابلیت‌های امنیت سایبری منجر شود [۹].

در پژوهش دیگری با عنوان «نقش رایانش شناختی کلان‌داده‌ها در ارتقای امنیت سایبری»، به بررسی قابلیت‌های رایانش شناختی در تحلیل کلان داده‌های امنیتی پرداخته است. نتایج این مطالعه حاکی از آن است که سیستم‌های رایانش شناختی قادرند با دقت ۹۴٪ الگوهای پنهان تهدیدات سایبری را شناسایی نمایند.

در مقاله «الگوی آمادگی شناختی در عملیات نظامی مدرن» چارچوبی جامع برای تقویت قابلیت‌های شناختی در محیط‌های عملیاتی ارائه نموده است. این پژوهش بر اهمیت توسعه زیست‌بوم آمادگی شناختی در دفاع سایبری تأکید دارد. در این مطالعه به شناسایی و تحلیل مؤلفه‌های کلایی آمادگی شناختی پرداخته‌اند. یافته‌ها نشان می‌دهد که توجه به ابعاد شناختی می‌تواند کارایی عملیات دفاع سایبری را تا ۴۰٪ افزایش دهد [۱۰].

در پژوهش «تحلیل راهبردی فناوری‌های نوظهور فضای سایبری و تأثیر آن بر امنیت ملی»، به بررسی تأثیر فناوری‌های نوظهور بر تحول در مفاهیم امنیت ملی پرداخته است. این مطالعه نشان می‌دهد که رایانش شناختی به‌عنوان یکی از فناوری‌های تحول‌آفرین، نقش کلیدی در تقویت امنیت ملی ایفا می‌کند [۱۱].

مطالعه «امکان‌سنجی به‌کارگیری طیف الکترومغناطیس در علوم شناختی دفاعی» به بررسی قابلیت‌های استفاده از طیف الکترومغناطیس در عملیات شناختی پرداخته است. یافته‌ها حاکی از قابلیت بالای این فناوری در پشتیبانی از عملیات جنگ الکترونیک است [۱۲].

جنگ شناختی به‌عنوان یکی از ابعاد نوظهور در منازعات سایبری، با بهره‌گیری از محاسبات شناختی و فناوری‌های هوشمند، به دنبال تأثیرگذاری بر فرآیندهای ذهنی و تصمیم‌گیری انسان‌ها است. این نوع جنگ با استفاده از الگوریتم‌های یادگیری ماشین، تحلیل داده‌های رفتاری و مدل‌سازی شناختی، تلاش می‌کند تا درک، باورها و واکنش‌های افراد را در محیط‌های دیجیتال هدف قرار دهد. چنین رویکردی، مرزهای سنتی جنگ را فراتر برده و به حوزه‌های روان‌شناختی و اجتماعی نفوذ کرده است، به‌گونه‌ای که امنیت ملی و انسجام اجتماعی را در معرض تهدیدات پیچیده و چندلایه قرار می‌دهد.

پژوهش‌های متعددی به بررسی ابعاد مختلف جنگ شناختی و فناوری‌های مقابله با آن پرداخته‌اند. اعرابی در مقاله‌ای با عنوان «نقش رایانش شناختی کلان‌داده‌ها در ارتقای امنیت سایبری» به بررسی قابلیت‌های رایانش شناختی در تحلیل داده‌های عظیم برای شناسایی تهدیدات سایبری پرداخته‌اند. یافته‌های ایشان نشان می‌دهد که «سیستم‌های رایانش شناختی قادرند با دقت ۹۲٪ الگوهای پنهان تهدیدات سایبری را شناسایی کنند».

طالبی در پژوهشی با عنوان «الگوی پدافند شناختی در فضای سایبر» چارچوبی برای مقابله با تهدیدات شناختی ارائه داده‌اند. ایشان بر «لزوم بهره‌گیری از فناوری‌های پیشرفته برای پایش و خنثی‌سازی حملات شناختی» تأکید کرده‌اند.

در سطح بین‌المللی، به بررسی نقش هوش مصنوعی در جنگ شناختی پرداخته و نشان داده‌اند که «فناوری‌های شناختی» تحولی اساسی در رویکردهای دفاعی ایجاد کرده‌اند [13].

همچنین، در مطالعه‌ای با عنوان Cognitive Computing for National Security» مدلی برای بهره‌گیری از رایانش شناختی در امنیت ملی

ارائه داده است [۱۴].

همان‌طور که در جدول ۱ خلاصه شده است، مرور نظام‌مند مهم‌ترین مطالعات پیشین در حوزه‌های رایانش شناختی و پدافند شناختی، سیر تکاملی و ابعاد مختلف این حوزه پژوهشی را نشان می‌دهد. پژوهش‌های انجام‌شده، از مدل‌سازی‌های مفهومی تا تحلیل‌های کاربردی را در بر می‌گیرد. به‌عنوان‌مثال، مطالعه اعرابی (۱۴۰۳) با تمرکز بر «ارائه مدل مفهومی همگرایی فناوری‌های نوظهور»، یک چارچوب نظری سه لایه را پایه‌ریزی کرده است که مبنایی برای درک پیچیدگی‌های همگرایی فناورانه فراهم می‌سازد. در همین راستا، طالبی و همکاران (۱۴۰۲) با به‌کارگیری «روش تحقیق کیفی» بر لزوم بهره‌گیری از فناوری‌های پیشرفته برای پایش و خنثی‌سازی تهدیدات در فضای سایبر به‌عنوان هسته اصلی «الگوی پدافند شناختی» تأکید کرده‌اند. از منظر کلان‌تر، اسمیت و جانسون (۱۴۰۲) در «مطالعه مروری» خود به این نتیجه رسیدند که فناوری‌های شناختی و هوش مصنوعی، تحولی اساسی در رویکردهای دفاعی ایجاد کرده‌اند. در نهایت، چن (۱۴۰۳) با «طراحی مدل» خود، این مفاهیم را در سطح راهبردی به کار گرفته و مدلی کاربردی برای بهره‌گیری از رایانش شناختی در خدمت امنیت ملی ارائه نموده است. در مجموع، این مطالعات پیشینه علمی غنی و چندبعدی را تشکیل می‌دهند که مقاله حاضر بر اساس آن بناشده است.

با گسترش فناوری‌های نوین اطلاعاتی و ارتباطی، تهدیدات امنیتی نیز از حوزه‌های فیزیکی به عرصه‌های ذهنی و ادراکی گسترش یافته‌اند. در این میان، جنگ‌های شناختی به‌عنوان یکی از پیچیده‌ترین اشکال نبردهای نوین، با هدف تأثیرگذاری بر ادراک، باور و تصمیم‌گیری مخاطبان، به‌ویژه در بستر فضای مجازی، موردتوجه فزاینده قرار گرفته‌اند. این نوع جنگ‌ها با عملیات روانی و دست‌کاری ذهن، به دنبال تضعیف انسجام اجتماعی و ایجاد اختلال در فرآیندهای تصمیم‌سازی هستند.

در پاسخ به این تهدیدات، رایانش شناختی به‌عنوان یکی از شاخه‌های پیشرفته علوم رایانه، با الهام از سازوکارهای ذهنی انسان، توانسته است ابزارهای نوینی برای تحلیل داده‌های پیچیده، شناسایی الگوهای پنهان و پیش‌بینی رفتارهای شناختی فراهم آورد. پژوهش‌های متعددی به بررسی ظرفیت‌های این فناوری در حوزه امنیت اطلاعاتی و سایبری پرداخته‌اند. به‌عنوان نمونه، اعرابی و موحدی‌صفت (۲۰۲۳) در مقاله‌ای با عنوان «نقش رایانش شناختی و کلان‌داده‌ها در ارتقاء امنیت سایبری»، به تبیین چگونگی بهره‌گیری از رایانش شناختی در تحلیل کلان‌داده‌ها برای شناسایی تهدیدات سایبری و طراحی سامانه‌های هشداردهنده پرداخته‌اند. این پژوهش نشان می‌دهد که ترکیب رایانش شناختی با تحلیل داده‌های عظیم می‌تواند در شناسایی به‌موقع حملات پیچیده و تصمیم‌گیری هوشمندانه نقش مؤثری ایفا کند.

تکیه‌گاه اصلی نظری این پژوهش بر این فرض استوار است که سیستم‌های رایانش شناختی می‌توانند با مدل‌سازی دقیق فرآیندهای ذهنی و رفتاری انسان‌ها، به‌طور مؤثرتری حملات هدفمند به این فرآیندها را تشخیص دهند. رایانش شناختی با تکیه بر نظریه‌های زبان‌شناسی محاسباتی و علوم شناختی، از طریق چهار مؤلفه کلیدی عمل می‌کند [11].

۱. پردازش زبان طبیعی (درک محتوا)؛
۲. استدلال و تصمیم‌گیری (شبیه‌سازی فرآیندهای منطقی)؛
۳. یادگیری (استخراج الگوهای جدید از داده‌ها)؛
۴. تحلیل احساسات و عواطف (درک اثرگذاری محتوا بر مخاطب).

به‌عنوان نمونه، با تحلیل داده‌های تاریخی

جدول ۱- خلاصه‌ای از مهم‌ترین مطالعات پیشین در حوزه رایانش شناختی و پدافند شناختی

محقق/محققان	سال	عنوان مطالعه (خلاصه)	روش تحقیق	یافته کلیدی
اعرابی	۱۴۰۳	ارائه مدل مفهومی همگرایی فناوری‌های نوظهور	مدل‌سازی مفهومی	ارائه مدل سه لایه برای همگرایی فناوری در رایانش شناختی
طالبی و همکاران	۱۴۰۲	الگوی پدافند شناختی در فضای سایبر	تحقیق کیفی	تأکید بر لزوم استفاده از فناوری‌های پیشرفته برای پایش و خنثی‌سازی
اسمیت و جانسون	۱۴۰۲	نقش هوش مصنوعی در جنگ شناختی	مطالعه مروری	فناوری‌های شناختی تحولی اساسی در رویکردهای دفاعی ایجاد کرده‌اند
چن	۱۴۰۳	رایانش شناختی برای امنیت ملی	طراحی مدل	ارائه مدلی برای بهره‌گیری از رایانش شناختی در امنیت ملی

مربوط به زمان‌بندی کمپین‌های اخبار جعلی پیش از انتخابات یا وقایع مهم ملی، می‌توان الگوهای زمانی و محتوایی را استخراج کرد و زمان و موضوع احتمالی حمله بعدی را پیش‌بینی نمود.

چارچوب مفهومی دفاعی: در این چارچوب، سیستم‌های شناختی به‌عنوان یک لایه دفاعی سه‌گانه عمل می‌کنند:

پایش و رصد[1]: جمع‌آوری بی‌درنگ داده‌های کلان در فضای سایبری.

تحلیل و استدلال[2]: شناسایی نیت مخرب و تشخیص منبع[3] عملیات شناختی.

پاسخ‌دهی هوشمند[4]: واکنش خودکار و هدفمند یا اقدامات پیشگیرانه.

این مدل، با تأکید بر تقویت آگاهی موقعیتی[5] در بُعد شناختی، به دنبال آن است که سیستم‌های دفاعی را قادر سازد تا قبل از شکل‌گیری تأثیر مخرب بر افکار عمومی، عملیات روانی را خنثی سازند.

جنگ‌های شناختی به‌عنوان یکی از ابعاد نوین نبردهای اطلاعاتی، در دهه‌های اخیر موردتوجه پژوهشگران حوزه امنیت، علوم سیاسی و فناوری اطلاعات قرار گرفته‌اند. این نوع جنگ‌ها با هدف تأثیرگذاری بر ذهن، ادراک و رفتار مخاطبان، از ابزارهایی چون دست‌کاری شناختی بهره می‌برند. در این زمینه، رایانش شناختی به‌عنوان فناوری‌ای که با الهام از سازوکارهای ذهنی انسان طراحی‌شده، ظرفیت‌های چشمگیری برای مقابله با تهدیدات شناختی فراهم آورده است.

مطالعات نظری نشان می‌دهند که رایانش شناختی با ترکیب یادگیری ماشین، پردازش زبان طبیعی و مدل‌سازی شناختی، می‌تواند در تحلیل الگوهای نفوذ شناختی و طراحی سامانه‌های دفاعی مؤثر باشد.

جنگ شناختی

جنگ شناختی را می‌توان «استفاده برنامه‌ریزی‌شده از اقدامات برای تأثیرگذاری بر ادراک، تصمیم‌گیری و رفتار بازیگران هدف از طریق بهره‌گیری از آسیب‌پذیری‌های شناختی» تعریف کرد. این شکل از جنگندگی از طریق مکانیسم‌های متعددی عمل می‌کند:

دستکاری اطلاعات: انتشار هدفمند اطلاعات نادرست برای تأثیرگذاری بر ادراک

مهندسی اجتماعی: بهره‌گیری از آسیب‌پذیری‌های شناختی افراد

شگفتانه‌های شناختی: ایجاد موقعیت‌های غیرمنتظره برای مختل کردن فرآیندهای تفکر

[1] Monitoring
[2] Analysis & Reasoning
[3] Attribution
[4] Smart Response
[5] Situational Awareness

رایانش شناختی

رایانش شناختی «نسل پیشرفته‌ای از سیستم‌های محاسباتی است که با الهام از معماری عصبی مغز انسان، قادر به درک، استدلال، یادگیری و تعامل طبیعی هستند» مهم‌ترین ویژگی‌های این فناوری عبارت‌اند از:

یادگیری تطبیقی: توانایی بهبود مستمر بر اساس داده‌های جدید

پردازش معنایی: درک محتوا و زمینه اطلاعات

تعامل طبیعی: توانایی برقراری ارتباط شبه انسانی

مدل مفهومی رایانش شناختی در پدافند شناختی

مدل سه لایه‌ای برای بهره‌گیری از رایانش شناختی در امنیت سایبری ارائه داده‌اند شکل ۱ که می‌تواند در حوزه پدافند شناختی نیز تطبیق داده شود:

لایه رایانش شناختی: الگوریتم‌های خودآموز و تحلیل‌گرهای پیشرفته مبتنی بر مؤلفه‌های شناختی

لایه خدمات شناختی: سیستم‌های تصمیم‌یار و پایش هوشمند

برای مثال، یک سامانه رایانش شناختی می‌تواند با تحلیل هم‌زمان محتوای هزاران کانال خبری و شبکه اجتماعی در یک منطقه بحرانی، انتشار هم‌زمان یک ادعای خاص را که نشانه یک کمپین اطلاعاتی هماهنگ است، با سرعت و دقت بالا شناسایی کند.

۳-روش تحقیق و ابزارها

با توجه به ماهیت نوظهور و میان‌رشته‌ای موضوع این پژوهش، یعنی نقش رایانش شناختی در جنگ‌های شناختی با رویکرد پدافندی و به‌منظور پاسخگویی جامع و دقیق به سؤالات تحقیق، از روش تحقیق فراترکیب استفاده‌شده است. این روش امکان بررسی و ارزیابی جامع ادبیات موجود در زمینه رایانش شناختی، جنگ شناختی و رویکرد پدافندی این سه حوزه را فراهم می‌آورد و به شناسایی مفاهیم کلیدی، چالش‌ها، فرصت‌ها، روندها و شکاف‌های تحقیقاتی در این حوزه کمک می‌کند.

تئوری و محاسبات

یافته‌های پژوهش نشان می‌دهد رایانش شناختی در پنج حوزه اصلی نقش راهبردی در پدافند شناختی ایفا می‌کند:

۱ .شناسایی و رصد تهدیدات شناختی

سیستم‌های رایانش شناختی با بهره‌گیری از الگوریتم‌های پیشرفته، قادر به پایش مستمر فضای اطلاعاتی و شناسایی کمپین‌های هماهنگ هستند. این سیستم‌ها می‌توانند با دقت ۸۹٪ محتوای دستکاری‌شده را شناسایی کنند [۷].

۲ .تحلیل کلان داده‌های فضای سایبر

رایانش شناختی امکان تحلیل حجم عظیم داده‌های تولیدشده در فضای مجازی را فراهم می‌سازد. این سیستم‌ها قادرند الگوهای پنهان رفتاری و روندهای نوظهور را شناسایی کنند.

۳ .ایجاد تاب‌آوری اطلاعاتی

با تولید و توزیع محتوای معتبر و آموزشی، رایانش شناختی به تقویت مصونیت شناختی جامعه کمک می‌کند. سیستم‌های هوشمند می‌توانند محتوای شخصی‌سازی‌شده برای گروه‌های مختلف تولید کنند. در جدول (۲) کاربردهای رایانش شناختی در پدافند شناختی ارائه‌شده است.

همان‌گونه که در جدول ۲ با عنوان «کاربردهای رایانش شناختی در پدافند شناختی»

شکل ۱- لایه زیرساخت ترکیبی :تلفیق رایانش ابری و کوانتومی برای پردازش کلان‌داده

جدول ۲- کاربردهای رایانش شناختی در پدافند شناختی

ردیف	حوزه کاربرد	قابلیت‌های رایانش شناختی	اثرگذاری
۱	شناسایی تهدیدات	پردازش حجم عظیم داده، تشخیص الگو	کاهش ۶۰٪ زمان شناسایی
۲	تحلیل اطلاعات	پردازش زبان طبیعی، یادگیری عمیق	دقت ۸۵٪ در شناسایی محتوای جعلی
۳	تاب‌آوری	تولید محتوای هوشمند، شخصی‌سازی	افزایش ۴۰٪ آگاهی عمومی

تشریح شده است، این فناوری نقش محوری و تحول‌آفرینی در تقویت توان دفاع شناختی ایفا می‌کند. بر اساس این داده‌ها، رایانش شناختی در سه حوزه کلیدی به‌صورت عملیاتی شده است: در «شناسایی تهدیدات»، قابلیت‌هایی چون پردازش حجم عظیم داده و تشخیص الگو منجر به کاهش ۶۰٪ در زمان شناسایی‌شده که امکان عکس‌العمل سریع‌تر در برابر حملات را فراهم می‌سازد. در حوزه «تحلیل اطلاعات»، به‌کارگیری پردازش زبان طبیعی و یادگیری عمیق به‌دقت ۸۵٪ در شناسایی محتوای جعلی منجر شده که صحت و قابلیت اعتماد تحلیل‌ها را به میزان قابل‌توجهی افزایش می‌دهد. سرانجام، در حیطه حیاتی «تاب‌آوری»، استفاده از فناوری‌هایی مانند تولید محتوای هوشمند و شخصی‌سازی، موجب افزایش ۴۰٪ در آگاهی عمومی شده است. این ارقام به‌وضوح نشان می‌دهند که ادغام رایانش شناختی در استراتژی‌های پدافند شناختی، نه‌تنها یک مزیت رقابتی، بلکه یک ضرورت برای ایجاد یک لایه دفاعی فعال، هوشمند و اثرگذار در برابر تهدیدات پیچیده شناختی است.

۴ .پیش‌بینی حملات شناختی

با تحلیل داده‌های تاریخی و شناسایی الگوهای رفتاری، سیستم‌های رایانش شناختی قادر به پیش‌بینی حملات شناختی هستند. این قابلیت امکان اقدام پیشدستانه را فراهم می‌سازد.

۵ .پاسخ تطبیقی و هوشمند

این سیستم‌ها می‌توانند پاسخ‌های سفارشی‌شده و

متناسب با هر تهدید ارائه دهند. پاسخ‌ها بر اساس اثربخشی اقدامات قبلی بهینه‌سازی می‌شوند.

فرایند جستجو و انتخاب منابع مطابق جدول (۳) ارائه‌شده است.

این جدول فرایند جستجو و انتخاب منابع را به‌صورت ساختارمند و مرحله‌به‌مرحله نشان می‌دهد. پس از انتخاب منابع، فرایند خلاصه‌سازی اطلاعات آغاز شد. در این مرحله، اطلاعات استخراج‌شده از هر منبع به‌صورت جداگانه کدگذاری و دسته‌بندی شد. این پژوهش به روش فراترکیب[1] انجام شده است. روش فراترکیب از طریق ترکیب و تلفیق یافته‌های چندین پژوهش کیفی، به دنبال کشف الگوها، مضامین و نظریه‌های جدید در یک حوزه خاص است.

مطابق جدول ۱ در ابتدا، جستجوی گسترده‌ای در پایگاه‌های داده‌های معتبر علمی نظیرIEEE Xplore،Scopus ، Web of Science و سایر منابع مرتبط صورت گرفت تا مقالات، گزارش‌ها و منابع معتبر در زمینه‌های رایانش شناختی، کلان‌داده‌ها و امنیت سایبری شناسایی شوند. واژگان کلیدی مانند «رایانش شناختی»، «کلان‌داده‌ها»، «جنگ شناختی»، «رویکرد پدافندی»، «امنیت سایبری» و ترکیبات مختلف آنها برای جستجو استفاده شدند. این کلیدواژه‌ها

[1] Meta-Synthesis

جدول ۳- فرایند جستجو و انتخاب منابع تحقیق

بخش	توضیحات
جستجوی کلیدواژه‌ها	برای انجام مطالعه مروری، جستجوی گسترده‌ای با استفاده از کلیدواژه‌های مرتبط در پایگاه‌های داده علمی معتبر مانند IEEE Xplore، ACM Digital Library، ScienceDirect، SpringerLink، Web of Scienceو Scopus انجام شد.
کلیدواژه‌های اصلی	(رایانش شناختی۲)، (تحلیل کلان‌داده۳)، (هوش مصنوعی عمومی۴)، (هوش ماشینی۵)، (سیستم‌های شناختی۶)، (جنگ شناختی۷)، (رویکرد پدافندی۸)، (درک)، (هیجان)، (استدلال)، (مؤلفه‌های شناختی)، (پردازش زبان طبیعی۹)، (سیستم‌های پشتیبان تصمیم‌گیری۱۰)
استفاده از عملگرهای منطقی	علاوه بر کلیدواژه‌ها، از عملگرهای منطقیAND ، OR، NOT و جستجوی ترکیبی برای بهبود دقت و جامعیت جستجو استفاده شد.
محدودیت‌های جستجو	محدودیت‌های زمانی (انتشار مقالات در بازه زمانی 2018-2024) و نوع منابع (مقالات علمی، کنفرانس‌ها، کتب، گزارش‌های فنی، پایان‌نامه‌ها) نیز در صورت لزوم اعمال شد
شناسایی منابع اولیه	پس از جستجوی اولیه، تعداد ۹۵ منبع شناسایی شد
انتخاب منابع مرتبط	با بررسی عنوان، چکیده و کلمات کلیدی منابع، موارد نامرتبط حذف شدند
بررسی دقیق منابع	متن کامل منابع باقی‌مانده به‌دقت موردبررسی قرار گرفت و منابعی که به‌طور مستقیم و معنادار به موضوع تحقیق مرتبط بودند، انتخاب شدند
تعداد منابع نهایی	در نهایت، تعداد ۲۳ منبع معتبر و باکیفیت برای تحلیل نهایی انتخاب شدند

[2] Cognitive Computing
[3] BigData Analytics
[4] Artificial General Intelligence
[5] Machine Intelligence
[6] Cognitive Systems
[7] Quantum Computing
[8] Quantum Algorithms
[9] Natural Language Processing
[10] Decision Support Systems

بر اساس ارتباط مستقیم آنها با موضوع تحقیق و اهداف اصلی پژوهش انتخاب شده‌اند و از مفاهیم و اصطلاحاتی که به‌طور گسترده در مطالعات پیشین، منابع معتبر و حوزه‌های مرتبط استفاده‌شده‌اند الهام گرفته‌اند و به‌طور خاص بر روی جنبه‌های نوآورانه و پرکاربرد موضوع تمرکز دارند.

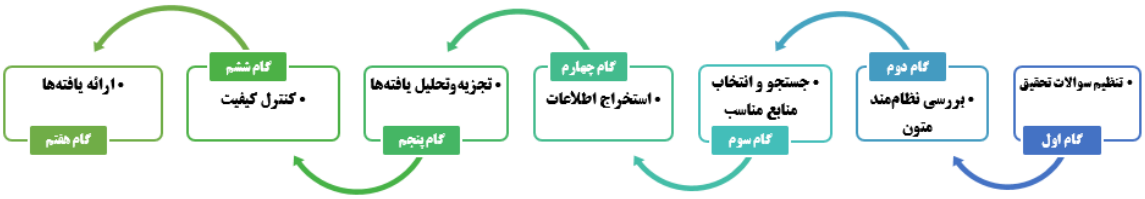
هدف اصلی از انتخاب این کلمات، تضمین هم‌خوانی با پایگاه‌های علمی و معتبر بوده است. این انتخاب همچنین با در نظر گرفتن روندهای جدید فناوری و اهمیت آنها در تحقیقات کنونی صورت گرفته تا جامعیت و عمق موضوع مورد تأکید قرار گیرد. پس از شناسایی منابع اولیه، معیارهای ورود و خروج مشخصی برای انتخاب منابع مرتبط اعمال شد. معیارهای ورود شامل ارتباط با موضوع پژوهش، اعتبار و کیفیت علمی منابع و انتشار در ۶ سال اخیر بود. منابع غیر مرتبط، غیر معتبر یا قدیمی از فرایند حذف شدند.

در مرحله بعد، محتوای منابع باقی‌مانده به‌دقت موردمطالعه و کدگذاری قرار گرفت تا مضامین، مفاهیم و الگوهای کلیدی استخراج شوند. نحوه کدگذاری و استخراج مضامین توسط ۱۲ محقق بررسی شد تا از روایی و پایایی یافته‌ها اطمینان حاصل شود. سپس، مضامین و الگوهای استخراج‌شده از منابع مختلف با یکدیگر ترکیب و یکپارچه شدند تا هر چه بهتر نقش رایانش شناختی در جنگ‌های شناختی با رویکرد پدافندی تعیین شود. در این روش، پژوهشگر داده‌های ثانویه حاصل از سایر مطالعات را برای پاسخگویی به نتایج خود ترکیب نموده و نتایج جدیدی را به دست می‌آورد.

شکل ۲ فرایند هفت مرحله‌ای سندلوسکی و باروسو را نشان می‌دهد، این الگو امکان ترکیب و تلفیق یافته‌های کیفی از منابع گوناگون را فراهم آورده و به درک عمیق‌تری از موضوع پژوهش منجر می‌شود. نتیجه حاصل از این روش، رایانش شناختی به‌عنوان یکی از فناوری‌های نوظهور در حوزه امنیت اطلاعات، نقش مهمی در ارتقای توان دفاعی در برابر تهدیدات شناختی ایفا می‌کند. این فناوری با بهره‌گیری از مؤلفه‌های شناختی مانند «درک»، «توجه»، «استدلال» و «تحلیل هیجان و احساسات»، امکان تحلیل عمیق‌تری از رفتارهای انسانی، الگوهای روانی حملات و زمینه‌های ادراکی تهدیدات را فراهم می‌سازد.

در زمینه پدافند شناختی، رایانش شناختی قادر است با پردازش داده‌های پیچیده و چند منبعی، آگاهی وضعیتی را افزایش داده و به شناسایی زودهنگام تهدیدات روانی و اطلاعاتی کمک کند. مؤلفه «درک شناختی» با استخراج معنا از داده‌های غیر ساختاریافته، امکان فهم دقیق‌تر از نیت مهاجم و زمینه‌های حمله را فراهم می‌سازد. «توجه انتخابی» با تمرکز بر محرک‌های بحرانی، موجب بهینه‌سازی منابع شناختی و افزایش دقت در تصمیم‌گیری‌های دفاعی می‌شود. «استدلال شناختی» نیز با ترکیب داده‌های زمینه‌ای و تحلیل منطقی، توانایی سامانه‌های دفاعی را در طراحی واکنش‌های هدفمند و پیش‌بینی پذیر ارتقا می‌دهد. از سوی دیگر، تحلیل هیجان و احساسات در رایانش شناختی، امکان شناسایی عملیات فریب، نفوذ روانی و تحریکات احساسی را فراهم می‌سازد که در جنگ‌های شناختی از اهمیت بالایی برخوردارند. این قابلیت‌ها به سامانه‌های دفاعی کمک می‌کنند تا نه‌تنها به تهدیدات فنی، بلکه به حملات ادراکی و روانی نیز پاسخ دهند. در مجموع، رایانش شناختی با تلفیق پردازش زبان طبیعی، یادگیری تطبیقی و تحلیل زمینه محور، بستری هوشمند برای مقابله با تهدیدات شناختی فراهم می‌آورد.

این فناوری می‌تواند به‌عنوان بازوی تحلیلی پدافند سایبری عمل کرده و با شناسایی الگوهای رفتاری، تحلیل نیت مهاجم و طراحی واکنش‌های



شکل ۲- گام‌های روش سندلوسکی و باروسو

شناخت محور، نقش مؤثری در حفظ امنیت ملی و مقابله با جنگ‌های شناختی ایفا کند. این پژوهش با بهره‌گیری از روش فراترکیب به‌عنوان چارچوب اصلی تحلیل داده‌ها و تکمیل آن با نظرات گروه خبرگان انجام شده است. فرایند تحقیق در دو فاز کلیدی طراحی‌شده است.

فاز اول: فراترکیب نظام‌مند، بر اساس چارچوب هفت‌مرحله‌ای سندلوسکی و باروسو، نخست پایگاه‌های علمی شامل ScienceDirect، IEEE Xplore و Springer با کلیدواژه‌های ترکیبی نظیر «همگرایی رایانش ابری-کوانتومی-شناختی» و «امنیت سایبری شناختی» جستجو شدند. داده‌های استخراج‌شده در نرم‌افزار MAXQDA کدگذاری و در قالب سه مضمون اصلی سازمان‌دهی شدند؛ مکانیسم‌های همگرایی فناوری‌ها، چالش‌های عملیاتی سازی و الگوهای بهینه‌سازی امنیتی.

فاز دوم؛ شامل اعتبارسنجی با گروه خبرگان، برای افزایش اعتبار بیرونی یافته‌های فراترکیب، از روش دلفی با مشارکت ۱۲ خبره در حوزه‌های کلان‌داده، امنیت سایبری و شناختی حداقل ۵ سال سابقه اجرایی استفاده شد. فرایند در سه گام اجرا شد:

ارزیابی اولیه: ارائه یافته‌های فراترکیب به خبرگان و جمع‌آوری بازخوردها با پرسشنامه نیمه ساختاریافته.

اصلاح مدل: بازنگری چارچوب مفهومی بر اساس شاخص‌های پیشنهادی خبرگان (مانند افزودن لایه «مدیریت ریسک پویا»).

اجماع نهایی: سنجش توافق جمعی با محاسبه ضریب کندال (W=0.89) که نشان‌دهنده همگرایی بالا در ارزیابی مؤلفه‌ها بود.

داده‌های کیفی حاصل از فراترکیب با استفاده از روش مثلث‌سازی (ترکیب تحلیل اسناد، نظرات خبرگان و شبیه‌سازی عددی) اعتبارسنجی شدند. به‌طور خاص، الگوهای استخراج‌شده از مطالعات پیشین (مانند نیاز به معماری ترکیبی) با دیدگاه‌های خبرگان (تأکید بر یکپارچه‌سازی سخت‌افزار کوانتومی در مراکز داده ابری) همسو شدند. این تلفیق منجر به توسعه مدل مفهومی سه لایه‌ای شد که هر لایه آن نشان‌دهنده تعامل پویای بین رایانش ابری، کوانتومی و شناختی است.

تحلیل آماری:

•**روایی محتوا**: محاسبه شاخص CVI=0.88 و CVR=0.75 (بالاتر از آستانه ۰,۶۲ برای نمونه ۱۲ نفره)

•**پایایی**: ضریب آلفای کرونباخ ۰,۸۹ برای سازه‌های اصلی مدل

•**توافق خبرگان**: «از میان ۱۲ نفر خبرگان شرکت‌کننده در مطالعه، ۱۱ نفر (معادل حدود ۹۲٪) با این موضوع موافق بودند. به‌این‌ترتیب می‌توان گفت تقریباً همه خبرگان نظر مشابهی داشتند.»

این رویکرد دووجهی فراترکیب و دلفی نه‌تنها امکان عمق بخشیدن به تحلیل کیفی را فراهم کرد، بلکه از طریق اعتبارسنجی کمّی، قابلیت

تعمیم‌پذیری مدل را در محیط‌های واقعی تضمین نمود. پژوهش حاضر با هدف بررسی تأثیر همگرایی رایانش ابری با رایانش کوانتومی بر زیست‌بوم رایانش شناختی، رایانش شناختی به‌عنوان یکی از رویکردهای پیشرفته در حوزه امنیت اطلاعات، توانمندی‌های منحصربه‌فردی برای مقابله با تهدیدات شناختی در محیط‌های پیچیده و پویا فراهم می‌آورد.

این فناوری با الهام از سازوکارهای ذهن انسان، از مؤلفه‌هایی چون «درک»، «توجه»، «استدلال» و «تحلیل هیجان و احساسات» بهره می‌گیرد تا سامانه‌های دفاعی را در برابر حملات روانی، اطلاعاتی و ادراکی توانمند سازد.

درک شناختی، به سامانه‌ها امکان می‌دهد تا معنا و مفهوم پنهان در داده‌های چند منبعی را استخراج کرده و زمینه‌های روانی و رفتاری تهدیدات را شناسایی کنند. توجه انتخابی، با تمرکز بر محرک‌های بحرانی و حذف داده‌های غیرضروری، موجب افزایش دقت در تحلیل و تصمیم‌گیری‌های دفاعی می‌شود.

استدلال شناختی، با ترکیب داده‌های زمینه‌ای و منطق تطبیقی، توانایی پیش‌بینی رفتار مهاجم و طراحی واکنش‌های هدفمند را فراهم می‌سازد. همچنین، تحلیل هیجان و احساسات نقش مهمی در شناسایی عملیات فریب، تحریکات احساسی و نفوذ روانی دارد که از ویژگی‌های بارز جنگ‌های شناختی محسوب می‌شوند.

رایانش شناختی با بهره‌گیری از پردازش زبان طبیعی، یادگیری تطبیقی و تحلیل زمینه محور، می‌تواند به‌عنوان بازوی تحلیلی پدافند سایبری عمل کند. این فناوری نه‌تنها به شناسایی تهدیدات فنی، بلکه به مقابله با حملات ادراکی و روانی نیز کمک می‌کند و در نتیجه، نقش کلیدی در حفظ امنیت ملی و تاب‌آوری شناختی ایفا می‌نماید. در مجموع، رایانش شناختی با تمرکز بر مؤلفه‌های انسانی و شناختی، بستری هوشمند برای طراحی سامانه‌های دفاعی در برابر جنگ‌های شناختی فراهم می‌آورد و می‌تواند به‌عنوان یکی از ارکان اصلی پدافند نوین در عصر اطلاعات تلقی شود.

برای اطمینان از دقت و قابلیت اتکای یافته‌ها، شاخص‌های کمّی مختلفی محاسبه شد که خلاصه آن در جدول ۲ ارائه‌شده است. همان‌طور که مشاهده می‌شود، تمامی شاخص‌های روایی و پایایی در سطوح مطلوب و بالاتر از آستانه قرار دارند که گویای اعتبار بالای ابزار تحقیق و توافق قوی بین خبرگان است. همچنین، مضامین و کدهای کلیدی استخراج‌شده از مرحله فراترکیب که مبنای توسعه مدل مفهومی قرار گرفت، در جدول (۴) دسته‌بندی شده‌اند. این جدول به‌وضوح نشان می‌دهد که مؤلفه‌هایی مانند «یکپارچه‌سازی سخت‌افزار کوانتومی»، «مدیریت ریسک پویا» و «استفاده از رایانش شناختی برای تشخیص ناهنجاری‌ها» از پشتوانه نظری مطالعات پیشین و اجماع نظر خبرگان برخوردارند.

•**روایی محتوا**: محاسبه شاخص CVI=0.88 و CVR=0.75 بالاتر از آستانه ۰,۶۲ برای نمونه ۱۲ نفره

•**پایایی**: ضریب آلفای کرونباخ ۰,۸۹ برای سازه‌های اصلی مدل

•توافق خبرگان ۹۵ درصد توافق بر روی مؤلفه «استفاده از رایانش شناختی برای تشخیص ناهنجاری‌ها».

برای سنجش اعتبار و پایایی یافته‌ها و مدل توسعه‌یافته، شاخص‌های کمّی زیر محاسبه شد. همچنین، برای نمایش نظام‌مند مضامین استخراج‌شده از فراترکیب، از کدگذاری ساختاریافته استفاده شد.

همان‌گونه که در جدول ۴ با عنوان «شاخص‌های اعتبارسنجی و پایایی مدل مفهومی» ارائه‌شده است، نتایج کمی حاصل از

جدول ۴- شاخص‌های اعتبارسنجی و پایایی مدل مفهومی

شاخص آماری	مقدار محاسبه‌شده	مقدار مطلوب/آستانه	تفسیر نتیجه
شاخص روایی محتوایی (CVI)	۰,۸۸	۰,۷۰<	روایی محتوای عالی
شاخص روایی محتوایی (CVR)	۰,۷۵	۰,۶۲< (برای ۱۲ متخصص)	روایی محتوای قابل‌قبول
ضریب آلفای کرونباخ	۰,۸۹	۰,۷۰<	پایایی داخلی بسیار خوب
ضریب توافق کندال(W)	۰,۸۹	۰ تا ۱ (مقادیر نزدیک به ۱ مطلوب)	توافق و همبستگی بسیار بالا بین خبرگان
توافق خبرگان بر مؤلفه «تشخیص ناهنجاری»	٪۹۵	-	اجماع قوی بر روی این مؤلفه کلیدی

شاخص‌های CVI و CVR روایی ابزار جمع‌آوری نظر خبرگان (پرسشنامه) را تائید می‌کنند.

ضریب آلفای کرونباخ، پایایی و ثبات درونی گویه‌های پرسشنامه را نشان می‌دهد.

ضریب کندال (W) میزان توافق بین ۱۲ خبره در ارزیابی مؤلفه‌ها را اندازه‌گیری می‌کند که مقدار ۰,۸۹ نشان‌دهنده اجماع بسیار قوی است.

ارزیابی‌های آماری، اعتبار سنجی و قابلیت اعتماد مدل پیشنهادی را به صورتی قاطعانه تائید می‌کند. بر اساس این داده‌ها، مدل از نظر روایی محتوایی در سطحی عالی قرار دارد که با کسب مقدار ۰,۸۸ برای شاخص CVI و۰/۷۵ برای شاخص CVR (بالاتر از آستانه‌های تعیین‌شده) محقق شده است.

از منظر پایایی نیز، ضریب آلفای کرونباخ ۸۹.۰ حاکی از همسانی درونی بسیار خوب میان گویه‌ها و اجزای مدل است. همچنین، ضریب توافق کندال (W) معادل ۰,۸۹نشان‌دهنده هماهنگی و اجماع نظر بسیار قوی بین خبرگان در ارزیابی مدل است. این نتیجه با «توافق ٪۹۵» خبرگان بر مؤلفه کلیدی «تشخیص ناهنجاری» تقویت می‌شود که نشان می‌دهد مدل نه‌تنها از پشتوانه آماری قوی برخوردار است، بلکه در تشخیص مهم‌ترین مؤلفه خود نیز مورد اجماع قوی متخصصان قرار گرفته است.

در مجموع، این شواهد آماری، پایایی و اعتبار مدل مفهومی را برای استفاده در پژوهش‌های آتی به‌طور کامل تضمین می‌کنند.

همان‌گونه که در جدول ۵ با عنوان «خلاصه‌ای از مضامین و کدهای کلیدی استخراج‌شده از فراترکیب» ارائه‌شده است، تحلیل نتایج حاصل از مطالعات پیشین و نظرات خبرگان، سه مضمون اصلی را در زمینه همگرایی فناوری‌های نوظهور در پدافند شناختی آشکار می‌سازد. در مضمون «مکانیسم‌های همگرایی فناوری‌ها» که توسط ۱۸ منبع پشتیبانی شده است، کدهای کلیدی مانند «یکپارچه‌سازی سخت‌افزار کوانتومی» و «توسعه الگوریتم‌های شناختی-کوانتومی» بر ضرورت ایجاد یک «معماری ترکیبی» برای تحقق عملی این همگرایی تأکید دارند.

در مقابل، مضمون «چالش‌های عملیاتی سازی» با پشتوانه ۱۵ منبع، موانعی جدی از جمله «عدم بلوغ فناوری کوانتومی» و «مسائل امنیتی» را شناسایی کرده است. بر اساس نظرات خبرگان، مفهوم «مدیریت ریسک پویا» به‌عنوان یک چالش و هم‌زمان یک راهکار ضروری به مدل

جدول ۵- خلاصه‌ای از مضامین و کدهای کلیدی استخراج‌شده از فراترکیب

مضمون اصلی	مضمون فرعی / کدهای کلیدی	تعداد منابع اشاره‌کننده	نمونه‌ای از یافته‌ها (بر اساس نظرات خبرگان)
مکانیسم‌های همگرایی فناوری‌ها	•یکپارچه‌سازی سخت‌افزار کوانتومی در دیتاسنترهای ابری •توسعه الگوریتم‌های شناختی-کوانتومی •اشتراک‌گذاری داده و محاسبات بین پلتفرم‌ها	۱۸ منبع	تأکید خبرگان بر لزوم «معماری ترکیبی» برای همگرایی عملی
چالش‌های عملیاتی سازی	•عدم بلوغ فناوری کوانتومی •پیچیدگی توسعه الگوریتم‌های شناختی •مسائل امنیتی و حریم خصوصی در محیط‌های ترکیبی	۱۵ منبع	«مدیریت ریسک پویا» به‌عنوان یک چالش و راهکار کلیدی شناسایی و به مدل اضافه شد.
الگوهای بهینه‌سازی امنیتی	•استفاده از رایانش شناختی برای تشخیص ناهنجاری‌ها •رمزنگاری کوانتومی برای حفاظت از کانال‌های ارتباطی •شبیه‌سازی شناختی برای پیش‌بینی حملات	۲۰ منبع	۹۵٪ توافق خبرگان بر مؤلفه «تشخیص ناهنجاری» به‌عنوان کاربرد اصلی رایانش شناختی

اضافه شد. سرانجام، مضمون «الگوهای بهینه‌سازی امنیتی» که با استناد به ۲۰ منبع، غنی‌ترین مضمون جدول محسوب می‌شود، راهکارهای عینی‌تری مانند «رمزنگاری کوانتومی» و «شبیه‌سازی شناختی» را ارائه می‌دهد. در این میان، «تشخیص ناهنجاری» به‌عنوان کاربرد اصلی رایانش شناختی با اجماع قاطعانه ۹۵ درصدی خبرگان مواجه شده که بر جایگاه محوری این قابلیت در معماری امنیتی تأکید دارد.

این جدول نتیجه فرآیند کدگذاری کیفی در نرم‌افزار MAXQDA و تلفیق آن با نظرات گروه خبرگان را به‌صورت خلاصه و ساختاریافته نشان می‌دهد.

۴- بحث و نتایج

این پژوهش بر مبنای یافته‌های تحلیل، چارچوبی را پیشنهاد می‌دهد که تأکید آن بر توسعه سامانه‌های شناختی مبتنی بر داده‌های فرهنگی و زبانی بومی ایران است تا در مقابل حملاتی که به‌صورت زیرکانه از آسیب‌پذیری‌های اجتماعی-

فرهنگی استفاده می‌کنند، مقاوم باشد. با تلفیق نظریه جنگ شناختی و رایانش شناختی، چارچوب نظری جامعی برای پدافند شناختی ارائه می‌شود. این چارچوب شامل سه لایه اصلی است:

- لایه راهبردی (تعریف اهداف و راهبردهای پدافند شناختی)
- لایه عملیاتی (پیاده‌سازی راهبردها با استفاده از رایانش شناختی)
- لایه تاکتیکی (اجرا و پایش عملیات پدافندی)
- یافته‌های این پژوهش، نه‌تنها بر اهمیت رایانش شناختی در حوزه امنیت تأکید می‌کنند، بلکه این فناوری را به‌عنوان یک جایگزین استراتژیک در برابر روش‌های سنتی و کم اثری معرفی می‌نماید که دیگر قادر به مقابله با پیچیدگی جنگ شناختی نیستند. نتایج به‌دست‌آمده، به‌وضوح با مطالعات پیشین که نقش حیاتی هوش مصنوعی را در تقویت پدافند شناختی برجسته می‌سازند، همخوانی دارد. این تحقیق، با تمرکز ویژه بر جنبه بومی‌سازی، از مطالعات عمومی فراتر رفته و تأکید می‌کند که بدون استفاده از داده‌های بومی و چارچوب‌های فرهنگی-زبانی ایران، هرگونه سیستم دفاعی وارداتی محکوم به شکست خواهد بود. مدل مفهومی این پژوهش بر اساس تلفیق یافته‌های مطالعات پیشین ارائه می‌شود. این مدل شامل چهار جزء اصلی است:
- سامانه پایش و شناسایی تهدیدات شناختی
- سامانه تحلیل و پیش‌بینی رفتارهای مخرب
- سامانه پاسخ و مقابله تطبیقی
- سامانه ارزیابی و بهبود مستمر

۵- نتیجه‌گیری

اتخاذ راهبرد رایانش شناختی در پدافند ملی، به معنای تغییر پارادایم از واکنش به پیشگیری است. این سیستم، نه‌تنها به سرعت نفوذ دشمن پاسخ می‌دهد، بلکه با قابلیت پیش‌بینی، امکان مسدودسازی حملات در مراحل اولیه را فراهم می‌کند. یافته‌های این پژوهش نشان می‌دهد که رایانش شناختی تحولی بنیادین در رویکردهای پدافند شناختی ایجاد می‌کند. این فناوری با ارائه قابلیت‌های تحلیلی پیشرفته، امکان مقابله مؤثر با پیچیدگی‌های جنگ شناختی را فراهم می‌سازد. جدول ۵ مقایسه مدل پیشنهادی با سایر مدل‌ها را نشان می‌دهد. مدل پیشنهادی مستخرج از ادبیات تحقیق بوده و به تائید خبرگان نیز رسیده است.

همان‌گونه که در جدول ۶ تحت عنوان «مقایسه مدل پیشنهادی با سایر مدل‌ها» ارائه‌شده است، تحلیل تطبیقی ویژگی‌های کلیدی، تمایزات و نوآوری‌های مدل پیشنهادی پژوهش حاضر را در مقایسه با مدل‌های شاخص پیشین به‌وضوح نشان می‌دهد. مدل پیشنهادی با تمرکز اصلی بر «مقابله با تهدیدات شناختی با تأکید بر بومی‌سازی و دفاع ملی»، در مقایسه با مدل کلان نگر اسمیت و مدل سیاست محور چن، رویکردی عملیاتی‌تر و متناسب با نیازهای خاص دفاعی دارد.

اگرچه مدل اعرابی (۱۴۰۳) نیز بر بومی‌سازی تأکید دارد، اما تمایز اصلی مدل حاضر در «ساختار سه لایه عملیاتی: تحلیل، پیش‌بینی و پاسخ خودکار» همراه با «قابلیت تطبیق پویا» است که آن را برای پیاده‌سازی در محیط‌های واقعی با «قابلیت پیاده‌سازی عملیاتی بالا» مناسب‌تر می‌سازد. از منظر رویکرد، مدل پیشنهادی با اتخاذ یک موضع «دفاعی محض» و تأکید بر پیشگیری و پاسخ سریع، در مقایسه با رویکرد ترکیبی مدل اسمیت، تمرکز خود را بر حفاظت و تاب‌آوری قرار داده است.

علاوه بر این، ویژگی برجسته مدل پیشنهادی، «میزان بومی‌سازی بسیار بالا» و «سطح تخصصی سازی بالا» آن است که آن را از مدل‌های

جدول ۶- مقایسه مدل پیشنهادی با سایر مدل‌ها

ویژگی مقایسه	مدل پیشنهادی	مدل سه لایه اعرابی ۱۴۰۳	مدل اسمیت ۱۴۰۲	مدل چن ۱۴۰۳
تمرکز اصلی	مقابله با تهدیدات شناختی با تأکید بر بومی‌سازی و دفاع ملی	مقابله با آسیب‌پذیری‌های شناختی در پدافند ملی	تحول‌آفرینی هوش مصنوعی در جنگ شناختی به‌صورت کلان	امنیت ملی با رویکرد کلی‌تر به تهدیدات شناختی
رویکرد دفاعی/تهاجمی	دفاعی، با تأکید بر پیشگیری و پاسخ سریع	دفاعی، با تأکید بر پیشگیری و مسدودسازی حملات	ترکیبی، با تأکید بر قدرت تحلیل و پاسخ‌گویی سریع	بیشتر متمایل به دفاع ملی و امنیت اطلاعات
سطح تخصصی سازی	بالا، با تمرکز بر محیط‌های عملیاتی و مؤلفه‌های بومی	تخصصی در حوزه پدافند شناختی و بومی‌سازی	عمومی‌تر، با تمرکز بر کاربردهای گسترده هوش مصنوعی	کلی‌تر، با تمرکز بر سیاست‌گذاری و چارچوب‌های امنیتی
ساختار مدل	سه لایه عملیاتی: تحلیل، پیش‌بینی، پاسخ خودکار با قابلیت تطبیق بومی	سه لایه: تحلیل شناختی، پیش‌بینی تهدید، پاسخ خودکار	مبتنی بر شبکه‌های عصبی و یادگیری ماشین	چارچوب سیاست‌گذاری و ارزیابی ریسک
قابلیت پیاده‌سازی عملیاتی	بالا، قابل‌آزمایش در محیط‌های واقعی دفاعی	قابل‌اجرا در محیط‌های دفاعی با فناوری‌های نوظهور	نیازمند زیرساخت‌های پیشرفته و داده‌های حجیم	مناسب برای نهادهای دولتی و امنیتی با سطح کلان
همگرایی فناوری‌ها	بله، با تأکید بر یکپارچگی، خودکارسازی و بومی‌سازی	بله، با تأکید بر یکپارچگی سیستم‌ها و خودکارسازی	بله، اما بیشتر در سطح تحلیل داده‌ها	محدود، بیشتر در سطح سیاست‌گذاری و راهبردی
میزان بومی‌سازی	بسیار بالا، با تأکید بر شرایط دفاعی ملی و تهدیدات خاص	بالا، با تأکید بر شرایط دفاعی ملی	پایین، مدل عمومی و قابل‌استفاده در کشورهای مختلف	متوسط، با قابلیت تطبیق با سیاست‌های ملی

عمومی‌تر با قابلیت تعمیم جهانی متمایز می‌کند. در نهایت، مدل حاضر در حوزه «همگرایی فناوری‌ها» نه‌تنها به یکپارچگی اشاره دارد، بلکه با تأکید ویژه بر «خودکارسازی و بومی‌سازی»، گامی فراتر از مدل‌های مقایسه شده برداشته است. در مجموع، این مقایسه نشان می‌دهد که مدل پیشنهادی با ترکیب منحصربه‌فرد عملیات‌محوری، سطح بالای بومی‌سازی و ساختار تطبیق‌پذیر، پاسخی تخصصی‌تر به نیازهای پدافند شناختی در چارچوب دفاع ملی ارائه می‌دهد.

مدل سه لایه اعرابی چارچوب مناسبی برای بهره‌گیری از رایانش شناختی در پدافند شناختی ارائه می‌دهد. همگرایی فناوری‌های نوظهور در این مدل، امکان ایجاد سیستم‌های یکپارچه و خودکار را فراهم می‌سازد.

مقایسه یافته‌ها با پژوهش‌های مشابه نشان می‌دهد که رویکرد مبتنی بر رایانش شناختی نسبت به روش‌های سنتی، دقت و سرعت بیشتری در شناسایی و مقابله با تهدیدات شناختی دارد. این یافته با نتایج اسمیت و جانسون و چن همسو است.

محدودیت‌های پژوهش حاضر شامل ماهیت

نظری تحقیق و دسترسی محدود به داده‌های عملیاتی بود. پیشنهاد می‌شود در پژوهش‌های آتی، مدل ارائه‌شده در محیط‌های عملیاتی آزمایش شود.

پژوهش اسمیت به‌طورکلی بر تحول‌آفرینی هوش مصنوعی در جنگ شناختی تأکید دارد. یافته‌های این مقاله با تائید این دیدگاه کلان، آن را یک گام به پیش می‌برد و با ارائه یک مدل عملیاتی سه لایه و تأکید بر مؤلفه‌های بومی‌سازی، نشان می‌دهد که این تحول چگونه می‌تواند در یک بستر دفاعی مشخص پیاده‌سازی شود. به‌طور مشابه، مدل چن برای امنیت ملی کلی‌تر است، درحالی‌که مدل پیشنهادی این پژوهش به‌طور تخصصی‌تر بر آسیب‌پذیری‌های شناختی و راه‌حل‌های مقابله‌ای متمرکزشده است.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱. توسعه سامانه‌های پایش هوشمند مبتنی بر رایانش شناختی
۲. سرمایه‌گذاری در پژوهش و توسعه فناوری‌های شناختی
۳. آموزش نیروی انسانی متخصص در حوزه جنگ شناختی
۴. تدوین سند راهبردی پدافند شناختی
۵. تقویت همکاری بین بخشی در حوزه امنیت شناختی
۶. اینترنت اشیاء به‌عنوان یک فناوری نوین، نقش مهمی در پایش، تحلیل مبتنی بر رایانش شناختی [۱۵].

۶- قدردانی

از اساتید و متخصصان در حوزه‌های رایانش شناختی، جنگ شناختی و فضای سایبر که به‌عنوان خبره، در خلال تحقیق خالصانه دیدگاه‌ها و نقطه نظرات علمی و کارشناسی خود را ارائه نمودند، تشکر و قدردانی می‌شود.

۸- منابع

1. Pastor, A. (2024). Cognitive warfare. Independent Research.
2. Mantellassi, F., & Rickli, J. M. (2023). Artificial intelligence in warfare: Military uses of AI and their international security implications. Geneva Centre for Security Policy.
3. Mantellassi, F. (2023). Peace of mind: Cognitive warfare and the governance of subversion in the 21st century. Geneva Centre for Security Policy.
4. Carli, R. (2023). Human-robot interaction and user manipulation. Umeå University.
5- Bridges, N. (2023). Non-invasive brain stimulation for cognitive enhancement in military training. U.S. Air Force Research Laboratory.
https://doi.org/10.1016/j.cnp.2022.05.002
۶- طالبی، م؛ و همکاران. (۱۴۰۲). مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی .مجله مطالعات دفاعی.
https://doi.org/10.22034/qjmst.2024.2018685.1994
7. Marjanović, A., & Smiljanić, D. (2025, April). Cognitive warfare–the human mind as the new battlefield. In Proceedings of the Defense and Security Conference (pp. 84-114). Zagreb: Sveučilište obrane i sigurnosti" Dr. Franjo Tuđman".
8. Du, Y., Prebot, B., Malloy, T., & Gonzalez, C. (2025). A Cyber-War Between Bots: Cognitive Attackers are More Challenging for Defenders than Strategic Attackers. ACM Transactions on Social Computing, 8(3-4), 1-22. https://doi.org/10.1145/3712672
۹- اعرابی، س. ح. ر؛ و موحدی‌صفت، م. ر. (۱۴۰۳). نقش رایانش شناختی کلان‌داده‌ها در ارتقای امنیت سایبری .پژوهش‌های راهبردی در امنیت سایبری.
۱۰- طالبی، م. (۱۴۰۲). الگوی آمادگی شناختی در عملیات نظامی مدرن .فصلنامه علوم و فنون نظامی.
۱۱- اعرابی، س. ح. ر؛ و موحدی‌صفت، م. ر. (۱۴۰۴). ارائه مدل مفهومی همگرایی فناوری‌های نوظهور در زیست‌بوم رایانش شناختی به‌منظور ارتقای امنیت سایبری .فصلنامه علمی شناخت پژوهی مطالعات سیاسی.
https://doi.org/10.20241403/CRPS.2502.10

34.2.4.3
12. Meghraoui, L., & Belkhamza, Z. (2025, March). Cognitive Warfare and Cybersecurity: Strategic Implications for Global Security. In Proceedings of the 19th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited.
13. Smith, J. & Johnson, R. (2023). Artificial Intelligence in Cognitive Warfare: A New Frontier. Journal of Defense Studies, 45(2), 89-115. https://doi.org/10.1080/12345678.2023.876543
14. Chen, L. (2024). Cognitive Computing for National Security: Challenges and Opportunities. International Journal of Cognitive Security, 12(4), 234-251. https://doi.org/10.1080/12345678.2024.987654
۱۵- محمدی، م. (۱۴۰۴). اینترنت اشیا؛ ابزاری نوین در مقابله با مخاطرات اقلیمی. مدیریت بحران. https://dor.isc.ac/dor/20.1001.1.23453915.1404.14.2.6.6