فصلنامه تهدیدپژوهی
سال اول، شماره دوم
تابستان ۱۴۰۲

مرکز مطالعات و پژوهش‌های اطلاعاتی

صص: ۱۰۱ – ۷۱

جنگ الکترونیک شناختی مولفه‌ای جدید در جنگ‌های امروزی

محمدحسن شاه‌رضایی [۱]

دریافت: ۱۴۰۲/۰۱/۱۲ پذیرش: ۱۴۰۲/۰۳/۲۰

چکیده

با پیچیدگی روزافزون محیط الکترومغناطیسی و توسعه هوشمند رادارها، عملیات اختلال الکترونیکی یا به عبارتی جنگ الکترونیک جهت انجام پارازیت، برخلاف رادار، نیاز فوری به بهبود توانایی خود در تشخیص اهداف تهدید و تصمیم‌گیری در مورد نوع پارازیت دارد. امروزه تجهیزات فرکانس رادیویی قابل برنامه‌ریزی و دیجیتال که با نام رادیو نرم‌افزاری شناخته می شوند، روند رو به رشدی دارند. بر همین اساس رادارها می‌توانند به سرعت شکل موج را تغییر دهند و هویت و مشخصه منحصر به فردی را ایجاد کنند. در نتیجه در محیط‌های فرکانسی متراکم و رقابتی، کار فرستنده‌های دشمن برای موقعیت‌یابی، شناسایی، مسدود کردن و مغشوش کردن سخت‌تر و سخت‌تر می‌شود. از طرفی گستردگی و تنوع حملات در حوزه الکترومغناطیس، با پیشرفت رادارها و ابزارهای شناختی، سامانه‌های جنگ الکترونیک سنتی را با چالشی اساسی مواجه کرده است. وقوع حملات جدید و ناشناخته باعث ناکارآمدی سامانه‌های سنتی جنگ الکترونیک در مواجهه با این حملات شده است. در این مقاله که به روش توصیفی – تحلیلی گردآوری شده محقق به‌دنبال پاسخ به این سئوال است که جنگ الکترونیک شناختی به چه میزان می‌تواند حملات جدید و ناشناخته را شناسایی و به آن‌ها پاسخ دهد؟ یافته‌های پژوهش بیانگر این است که جنگ الکترونیک شناختی با ترکیب روش‌های سنتی و هوش مصنوعی در قالب یک سامانه کامل و منسجم، می‌تواند حملات جدید و ناشناخته را شناسایی کرده و واکنش مناسب را در صحنه نبرد اتخاذ کند.

واژگان کلیدی: جنگ الکترونیک شناختی، معماری جنگ الکترونیک شناختی، رادار شناختی، هوش مصنوعی

استناد: شاه‌رضایی، محمدحسن (۱۴۰۲). جنگ الکترونیک شناختی مولفه‌ای جدید در جنگ‌های امروزی. *فصلنامه علمی تهدیدپژوهی ۱(۲) ۱۰۱-۷۱.*

---

۱ . دانشجوی دکترای روابط بین‌الملل، دانشگاه آزاد اسلامی، واحد اصفهان(خوراسگان).
mohamadhasanshah1347@gmail.com

Center for Intelligence Studies and Research

Quarterly Journal of Threat Studies
Volume 1, Issue2
Summer 2023

PP 71 - 101

Cognitive Electronic Warfare: A New Component in Modern Warfare

Mohammad Hassan Shahrezaee[1]

Received: 2023/06/10 **Accept:2023/05/15**

Abstract

With the increasing complexity of the electromagnetic environment and the intelligent development of radars, electronic jamming operations, or in other words, electronic warfare for jamming, unlike radar, urgently need to improve their ability to detect threat targets and decide on the type of jamming. Today, programmable, digital radio frequency equipment, known as software-defined radio, is on the rise. Accordingly, radars can quickly change the waveform and create a unique identity and characteristic. As a result, in dense and competitive frequency environments, the work of enemy transmitters to locate, identify, block, and confuse becomes more and more difficult. On the other hand, the breadth and diversity of attacks in the electromagnetic domain, with the advancement of radars and cognitive tools, has presented traditional electronic warfare systems with a fundamental challenge.The occurrence of new and unknown attacks has made traditional electronic warfare systems ineffective in dealing with these attacks. In this article, which was compiled using a descriptive-analytical method, the researcher seeks to answer the question of to what extent cognitive electronic warfare can identify and respond to new and unknown attacks? The research findings indicate that cognitive electronic warfare, by combining traditional methods and artificial intelligence in the form of a complete and coherent system, can identify new and unknown attacks and adopt the appropriate response on the battlefield.

Keywords: Cognitive Electronic Warfare, Cognitive Electronic Warfare Architecture, Cognitive Radar, Artificial Intelligence

Citation: Shahrezaei, Mohammad Hassan (1402). Cognitive Electronic Warfare: A New Component in Modern Wars. *Quarterly Journal of Threat Research. 1(2).71-101*.

---

1. PhD student in International Relations, Islamic Azad University, Isfahan Branch (Khorasgan). mohamadhasanshah1347@gmail.com

مقدمه

پدیده جنگ اصولاً همراه دائمی بشر در طول تاریخ بوده و از دیرباز زندگی او را با مخاطرات گوناگونی مواجه نموده ا ست. از دوران با ستان و از زمان جنگ‌های ایرانیان، مصـــریان، یونانیان و چینی‌ها تا به امروز، بشـــر مشـــغول مطالعه جنگ و ویژگی‌های آن بوده ا ست. در این را ستا همواره جوامعی پیروز و غالب شده‌اند که توانسته‌اند بر ا ساس فرهنگ راهبردی، محیط و ماهیت تهدیدها و قابلیت‌های در د سترس، اولاً تهدیدات را شنا سایی نموده و ثانیاً ت صویری جامع و دقیق از جنگ زمان خود ترســـیم کنند و بر اســـاس آن، فناوری، دکترین و ســـازمان‌های رزمی‌اشـــان را توســـعه دهند. ســـرتاســـر تاریخ جنگ بیانگر مواردی اســـت که قدرت‌های بزرگ گاه با عدم درک صـــحیح از شـــکل تغییر یافته جنگ در زمان خود و به‌رغم برتری در عده و عُده به شک ست تن داده‌اند و چه ب سیار حریفان ضـــعیف‌تری که با وجود قلت کمی و کیفی توان رزمی، صـــرفاً با شـــناخت دقیق ویژگی‌های نوظهورجنگ به پیروزی رسیده یا حداقل مانع از انهدام خود شده‌اند. از جمله جنگ‌های نوین که امروزه به‌عنوان یکی از رویکردهای مطرح در زمینه جنگ تکاملی مطرح است، جنگ الکترونیک شناختی[1] است.

برای درک مقوله جنگ الکترونیک شـــناختی لازم اســـت در ابتدا جنگ شـــناختی تبیین گردد. پایه و مبنای جنگ شناختی، علوم شناختی است. علم شناختی مطالعه میان ر شته‌ای با مو ضوع ذهن و هوش ا ست که حوزه‌های فل سفه، روان شنا سی، هوش م صنوعی، علوم اع صاب، زبان شنا سی و ان سان شنا سی را دربر می‌گیرد. جنگ شناختی یک جنگ پیچیده و چند لایه در جهان معا صر ا ست که به‌عنوان مولفه مهم امنیت ملی در نزاع میان کشورها و گروه‌های مخالف تبدیل شده است. با این وجود، هنوز یک شـــناخت کلی و واحد از این مفهوم در نزد واضـــعان و

1.Cognitive Electronic Warfare

کاربران وجود ندارد. ایجاد یک شناخت همه جانبه از جنگ شناختی، مستلزم یک نقشه راه یا نگاه آینده نگرانه و دست‌یابی به دانش گسترده از علوم مفید نظیر جامعه شناسی، روان شناسی، انسان شناسی، اقتصاد و به‌ویژه الکترونیک است. در این زمینه برخی از کشورها، از جمله کشورهای غربی با توجه به نقش، جایگاه و اهمیت فزاینده جنگ شناختی، با تاسیس موسسه‌های ویژه وابسته به دولت، آن را به‌عنوان ابزاری کارآمد و تاثیرگذار در جهت نیل به اهداف خود تعریف کرده‌اند.

از طرف دیگر جنگ الکترونیک یا جنگال اصطلاحی نظامی و بیانگر کاربرد الکترونیک و امواج الکترومغناطیس در نبردها است و شامل ارتباطات راداری و رادیویی، ایجاد اختلال در ارتباطات راداری و رادیویی دشمن و شنود گفتگوهای دشمن است. از این‌رو با ارائه فناوری رادیو شناختی، هوشمندسازی جنگ الکترونیک می‌تواند بسیار مفید با شد. به همین دلیل در سال‌های اخیر محققان با به‌کار بردن روش‌های هوش مصنوعی و یادگیری ماشین در تلاش برای ارائه فناوری‌های جنگ الکترونیک شناختی هستند.

جنگ الکترونیک شناختی، باید بتواند در عین نداشتن ذره‌ای شناخت از سامانه‌های دشمن، وارد محیط شود، سامانه‌ها را شناسایی کرده و حتی اقدامات متقابل مورد نیاز را به سرعت پیاده‌سازی کند. شناخت در این محیط شامل استفاده از آموزش ماشین برای ساخت سامانه‌های هوشمندتر است. این سامانه‌ها باید بتوانند سامانه‌های مقابل را تحریک کرده و با توجه به واکنش آن‌ها، ضمن تحمل کمترین آسیب به‌طور خودکار آموزش ببینند و به سرعت راهکار مقابله را کشف کنند. در همین راستا محققان وزارت دفاع آمریکا در حال آزمایش فناوری های شناختی جنگ الکترونیکی هستند که در طول یک دهه آینده، سامانه‌های دشمن را به‌طور مستقل شناسایی کرده و بدون هیچ برنامه‌ریزی قبلی به مبارزه با آن‌ها بپردازند. بر همین ا ساس آژانس تحقیقاتی دفاعی آمریکا (دارپا)

در برخی پروژه‌های خود از هوش مصنوعی برای سامانه‌های جنگ الکترونیک استفاده کرده است. به‌عنوان نمونه پروژه اقدامات راداری انطباقی (ARC)[1] و یادگیری رفتاری برای جنگ الکترونیک انطباقی از سامانه‌های جنگ الکترونیک هوشمند استفاده کرده‌اند.

پیشینه و سوابق پژوهش

با توجه به این که جنگ الکترونیک شناختی از پارادیم جنگ های نوظهور به شمارمی‌رود، از این‌رو در این خصوص تا کنون کتب، مقاله یا پژوهش چندانی به رشته تحریر در نیامده است. اما از جمله آثار محدودی که در این زمینه منتشر شده می‌توان به موارد ذیل اشاره نمود:

پژوهشکده اویونیک دانشگاه صنعتی اصفهان (۱۳۹۷)، در مقاله‌ای با عنوان "جنگ الکترونیک شناختی" آورده است: دیجیتالی شدن سامانه‌های راداری باعث شده است روش‌های جمینگ و ضد جمینگ پیشرفت‌های زیادی داشته باشند. در زمان فعلی دیگر تکیه بر آگاهی از اطلاعات قدیمی از یک سامانه راداری برای مقابله با آن کفایت نمی‌کند. به‌عبارت دیگر رادارها می‌توانند با سرعت بالا بسیاری از ویژگی‌های خود را تغییر داده و برای دشمن خود کاملا ناشناخته باشند. در چنین محیطی سامانه‌های جنگ الکترونیکی شناختی می‌توانند راهکاری مناسب برای مقابله با رادارها باشند. فناوری‌های یادگیری ماشین و هوش مصنوعی کلید اصلی برای ساخت یک سامانه جنگ الکترونیک شناختی است.

رجبی و خالقی بیزکی(۱۴۰۰)، در پژوهشی با عنوان" معماری پیشنهادی جنگ الکترونیک شناختی مبتنی بر رادارهای شناختی و سیستم شناختی انسان"

1.Adaptive Radar Countermeasures

آورده‌اند: گستردگی و تنوع حملات در حوزه الکترومغناطیس، با پیشرفت رادارها و ابزارهای شناختی، سامانه‌های جنگ الکترونیک سنتی را باچالشی اساسی روبر کرده است. امروزه وقوع حملات جدید و ناشناخته باعث ناکارآمدی سامانه‌های سنتی جنگ الکترونیک درمواجه با این حملات شده است. جنگ الکترونیک شناختی با ترکیب روش‌های سنتی و هوش مصنوعی در قالب یک سامانه، می‌تواند حملات جدید و ناشناخته را شناسایی کرده و واکنش مناسب را در صحنه نبرد اتخاذ کند.

هیگ و آندروسنکو[1] (۲۰۲۱) در کتابی با عنوان "جنگ الکترونیک شناختی رویکردی با هوش مصنوعی" آورده‌اند: جنگ الکترونیک شناختی یکی از پیشرفت‌های حیاتی است که آینده نبردها را تعیین می‌کند. کاربرد هوش مصنوعی در این مقوله پیشرفتی بزرگ محسوب می‌شود. در دنیای دیجیتال سامانه‌های جنگ الکترونیک بایستی قادر باشند به سیگنال‌های ناشناس پاسخگو باشند و اقدام مناسب را انجام دهند و این همان ترکیب هوش مصنوعی با روش‌های سنتی جنگ الکترونیک است.

چارچوب نظری پژوهش

بدون شک یکی از مهم‌ترین دستاوردهای هر رشته علمی یا موضوعات مطالعاتی را دستاوردهای نظری آن تشکیل می‌دهد. اصطلاح جنگ شناختی با پشینه انتزاعی طی چند سال اخیر بسیار مورد توجه واقع شده است این جنگ مطابق با الگوی معرفی شده از سوی جیمز جوردانو[2]، است. جیمز جوردانو متخصص علوم

1.Haigh & Andrusenko
2. James Jordano

اعصاب، مغز انسان را میدان جنگ قرن بیست ویکم توصیف نموده است. جنگ شناختی نشانگر همگرایی همه عناصری است که از زمان ظهور این اصطلاح در دهه۱۹۹۰، تحت تاثیر مفهوم جنگ اطلاعات مورد بی‌توجهی قرارگرفته بود، با این حال سازمان‌های موضوعی که اکنون درگیر این مفهوم بحث برانگیز هستند، دریافته‌اند که جنگ شناختی مفهومی بزرگتر است. جنگ شناختی در حقیقت نوعی جنگ اطلاعاتی است که به آن ابعاد دیگری نیز اضافه شده و همچنان در حال اضافه شدن هست و آگاهی در این زمینه مستمراً در حال افزایش است و در نتیجه این احتمال مطرح است که سازمان‌های نظامی و امنیتی که بر اساس قواعد جنگ اقدام می‌کردند ممکن است گرفتار بازی اشتباه شده باشند(حاجی زاده، ۱۴۰۱: ۱۰۵).

جنگ اطلاعاتی در اوائل دهه ۱۹۹۰ با توجه به تغییر عملیات جنگی فرسایشی به عملیات مبتنی بر تاثیر و زیرساخت‌های دیجیتالیزه شده و شبکه‌ای که اساس جنگ‌های معاصر را رقم می‌زند، مورد توجه واقع شد. این حوزه مجموعه تلاش‌ها در زمینه اطلاعات، نظارت و شناسایی، جنگ الکترونیک، عملیات روانشناختی و عملیات سایبری را مورد بررسی قرار داد که به‌طور کلی نیاز به رقابت و بهره‌گیری از کنترل جریان اطلاعات را افزایش می‌دهد. در زمان حاضر فناوری‌های نوین و روش‌های گوناگون تفکر در مورد تصمیم‌گیری به سمت ایجاد مفهوم جنگ شناختی همگرا شده‌اند(محمدی نجم، ۱۳۹۵: ۵).

وینستون چرچیل[1] (نخست وزیر بریتانیا در زمان جنگ جهانی دوم) در ارتباط با این حوزه، گفته معروفی دارد. او می‌گوید: «امپراطوری‌های آینده، امپراطوری‌های ذهن هستند». در حقیقت آینده مورد نظر او هم اکنون فرا رسیده است، رویه‌های

1.Winston Churchill

جاری دلالت می‌کنند که ما به دوره جدیدی از فناوری‌ها، امکانات و تجهیزاتی وارد شدیم که زمینه را برای تحقق تسلط بر ذهن فراهم کرده است.

کارکرد جنگ شـــناختی در فضـــای نفوذ به اذهان افراد در جهت دســـتکاری‌های ذهنی، دگردیســـی نگرش، تغییر و تســـلط بر مدل تحلیل اطلاعات در افراد، اثرگذاری بر تصمیم‌گیری‌ها و اقدامات افراد، پیش‌بینی کنش‌های رقیب، مدیریت هیجانات، احساسات و تمایلات، مدل سازی ریاضی فرایندهای ذهنی، استفاده حداکثری از پتانسیل هوش مصنوعی و فناوری‌های نوین و سایر اقدامات در این عرصه از جمله جنگ الکترونیک شناختی، از اهدافی است که در این زمینه مورد توجه است.

این که جیمز جوردانو مغز انسان را میدان جنگ قرن بیست ویکم توصیف نموده و یا وینســـتون چرچیل امپراطوری‌های آینده را امپراطوری‌های ذهن می‌پندارد بیانگر بلوغ تکاملی این پارادایم جنگی در عصـــر حاضـــر اســـت که حوزه‌های متعددی را درگیر خود ســـاخته اســـت. از جمله حوزه‌های این جنگ می‌توان به ورود آن در حوزه الکترونیک پرداخت. این در واقع به نوعی ورود به جنگ الکترونیک شـــناختی را تداعی می‌کند. جنگ الکترونیک شـــناختی اســـتفاده از سامانه‌های شناختی که معمولاً به‌عنوان هوش مصنوعی یا یادگیری ماشین شناخته می‌شـــود اســـت. این جنگ برای ارتقاء توســـعه و عملیات فن‌آوری‌های جنگ الکترونیک برای جامعه دفاعی اســـت. زیرا ســـامانه‌های شـــناختی می‌توانند حس کنند، بیاموزند، اســـتدلال کنند و به‌طور طبیعی با افراد و محیط‌ها تعامل برقرار کرده و توسعه و اجرای فناوری‌های شناسایی، سرکوب و خنثی سازی تهدیدات جنگ الکترونیک نسل بعد را تسریع نمایند.

تعاریف و مفاهیم

الف) جنگ الکترونیک

استفاده از طیف الکترومغناطیسی برای کاهش عملکرد یا خراب کردن قابلیت رزمی دشمن(شامل پایین آوردن توانایی یا ممانعت از استفاده دشمن از طیف الکترومغناطیسی و نیز کاهش عملکرد تجهیزات، کارکنان و امکانات دشمن)؛ و درمقابل محافظت از توانایی رزمی خودی شامل محافظت از طیف الکترومغناطیسی مورد استفاده نیروهای خودی و نیز تجهیزات، کارکنان و امکانات خودی که می‌توانند در برابر حمله از طریق طیف الکترومغناطیسی آسیب‌پذیر باشند را جنگ الکترونیک می‌نامند(عفیفی، کریم زاده و نظافتی، ۱۵:۱۳۸۵).

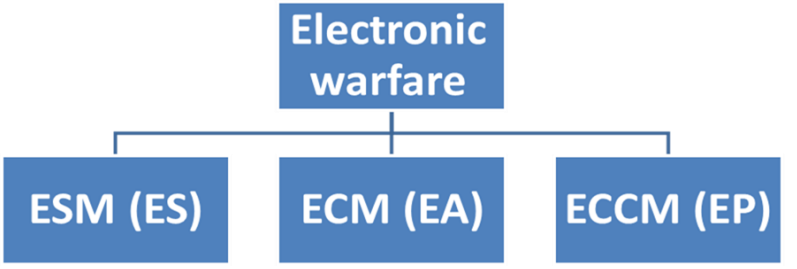
یا جنگ الکترونیک سلسله اعمالی است که از انرژی نهفته در طیف الکترومغناطیس برای شناسایی، بهره‌برداری اطلاعاتی، کاهش یا جلوگیری از استفاده موثر دشمن از طیف الکترومغناطی خود و تداوم استفاده نیروهای خودی از طیف صورت می‌گیرد. جنگ الکترونیک از سه بخش عمده شامل تهاجم الکترونیکی، حفاظت الکترونیکی و پشتیبانی الکترونیکی تشکیل شده است (سنگرگیر و جواهری،۳۳۵:۱۳۹۱).

ب- بخش‌های مختلف جنگ الکترونیک

جنگ الکترونیک معمولاً به دو بخش مخابراتی و غیرمخابراتی یا به عبارتی ارتباطی و غیرارتباطی تقسیم می‌شود؛ بخش مخابراتی معمولاً دارای قدمتی به اندازه خود مخابرات الکترونیک است و معمولاً در میدان جنگ به منابع مخابراتی که در باندهای HF (محدوده فرکانسی ۳ تا ۳۰ مگاهرتز) تا SHF (محدوده فرکانسی ۳ تا ۳۰ گیگاهرتز) کار می‌کنند اطلاق می‌گردد. بخش غیرمخابراتی از

زمان بکارگیری رادارها و سامانه‌های ناوبری در جنگ جهانی دوم توسعه پیدا کرد. این بخش نیزدر محدوده باندهای فرکانس راداری صورت می‌گیرد.

همانطور که در شکل زیر نشان داده شده سه تقسیم‌بندی اصلی برای جنگ الکترونیک وجود دارد که هر دو بخش مخابراتی و غیرمخابراتی را پوشش می‌دهد(گودرزی و شاه‌رضایی، ۱۴۰۱: ۱۲).



شکل ۱) تقسیم‌بندی جنگ الکترونیک

اقدامات پشتیبانی جنگ الکترونیکی که در گذشته به (ESM)[1] معروف بود بخشی از اقدامات جنگ الکترونیک شامل فعالیت‌های تاکتیکی و یا تحت کنترل مستقیم فرمانده عملیات برای جستجو، رهگیری، شناسایی و تعیین موقعیت منابع انرژی الکترومغناطیسی دشمن را به‌منظور شناسایی بلادرنگ تهدید دربر می‌گیرد که البته اقدام اساسی در این خصوص جهت تهیه آرایش الکترونیکی میدان نبرد یا (EOB) توسط سامانه‌های اطلاعات سیگنالی انجام می‌گیرد.

اقدامات ضد الکترونیکی(ECM)[2] : بخشی از جنگ الکترونیک که استفاده.از انرژی الکترومغناطیسی برای حمله به پرسنل، تجهیزات و یا امکانات به‌منظور

1-Electronic Support Measure
2-Electronic Counter Measure

کاهش عملکرد یا تخریب توان رزمی دشـمن را در بر می‌گیرد. شـایداین شـائبه به‌وجود آید که چگونه اقدامات ضد الکترونیکی حمله به افراد ا ست؟ در پا سخ باید اذعان نمود پس از شـنود اطلاعات ارتباطی و غیرارتباطی و انجام حمله الکترونیکی قربانی آن می‌تواند شـامل افراد و تجهیزات باشـد زیرا به‌نوعی ارتباطات فرد مورد نظر مورد اختلال واقع می‌گردد.

اقدامات ضد ضدالکترونیکی(ECCM)[1] : این بخش شامل فعالیت‌هایی ا ست که برای حفاظت پرسنل، امکانات و تجهیزات در برابر تمام دستگاه جنگال خودی و دشـمن که باعث تنزل عملکرد، خنثی شـدن یا خراب شـدن تجهیزات رزمی نیروهای خودی می‌شوند.

البته در تقسـیم بندی دیگر جنگ الکترونیک را می‌توان به به شـرح زیر تقسـیم بندی کرد:

پشتیبانی الکترونیکی(ES)[2]

تهاجم الکترونیکی(EA)[3]

حفاظت الکترونیکی(EP)[4]

بخش‌های ES و EA یعنی بخش‌های (پشـتیبانی و تهاجم الکترونیکی) از موارد آفندی است که برای حمله به دشمن تنظیم شده و فرآیندهای جستجو، رهگیری، جهت‌یابی، تجزیه و تحلیل و درگیری با سامانه‌های الکترونیک د شمن به صورت اختلال، فریب و خنثی‌سازی را دربر می‌گیرد.

1-Electronic Counter-Counter Measure
2-Electronic Support
3-Electronic Attack
4 -Electronic Protection

بخشEP یا حفاظت الکترونیکی گرایشی کاملاً دفاعی است و استفاده نیروهای خودی از طیف الکترومغناطیسی را در برابر جنگال آفندی دشمن محافظت می‌کند. EP به تمام کاربران تجهیزات الکترونیکی مربوط می‌شود و کارهایی مانند امنیت انتشار و امنیت مخابرات را دربر می‌گیرد (گودرزی و شاهر ضایی، ۱۴۰۱: ۱۳).

پ) جنگ شناختی[1] چیست؟

همواره بشر در هر زمان و هر سرزمینی درگیر انواع جنگ و نزاع همچون جنگ نرم، جنگ سخت و جنگ‌های قومی و قبیله‌ای، جنگ سرد و بسیاری دیگر از اقسام جنگ‌ها بوده و هست. امروز اما دشمن‌ها و نیروهای ضد یکدیگر در تلاشند با استفاده دشمنی در قالب جنگ شناختی با یکدیگر مبارزه کنند و بدون ردپایی از خود رقیب را از صحنه به در کنند.

اما جنگ شناختی چیست؟ اصطلاح جنگ شناختی نیازمند برخی فاکتورهاست. تشریح و تفسیر در متن امنیت ملی، بصورت فرآیند اطلاعات غلط برای فرسودگی روانشناختی گیرنده‌های اطلاعات به‌طور گسترده تعریف شده است. اثرات این جنگ از طریق منابع اطلاعاتی مانند رسانه‌های اجتماعی، شبکه اینترنت به‌طور استراتژیک گسترش می‌یابد. جنگ شناختی، هنگامی که به‌طور موثر تمرین می‌شود، دارای ماهیت موذیانه‌ای است و درک و واکنش معمولی ما نسبت به حوادث را مختل می‌کند(پایدار، ۲۰۲۰: ۳).

حال این سوال مطرح است که چگونه دشمنان با استفاده از این نوع جنگ یکدیگر را تحت تاثیر قرار می‌دهند و به رقبای خود آسیب وارد می‌کنند؟ چگونه

5-Cognitive warfare

قدرت‌ها بدون دخالت محسوس خود این جنگ را به راه می‌اندازند؟ این جنگ وحشتناک دارای چه تسلیحات و چه اهدافی است؟

ت) تسلیحات و اهداف جنگ شناختی

حتماً اطرافتان کسانی را دارید که دچار تزلزل در افکار و جهت‌های خود شده‌اند. این افراد قبلاً نسبت به خاک و وطن خود تعصب و حس وفاداری بی‌حدی داشته‌اند. ولی امروز نسبت به حکومت و ساختار کشور خود تردید دارند و یا با بدبینی و ظن از آن حرف می‌زنند. این تغییر جریان تفکری ناگهانی نبوده است. اگر شما هم درگیر این تغییرات و تردیدها شده‌اید مطمئن باشید گلوله‌ها و ترکش‌های جنگ شناختی به شما و اطرافیانتان هم برخورد کرده است. شاید تصور کنید این همان جنگ نرم است اما جنگ شناختی با جنگ نرم متفاوت است. گرچه ممکن است جنگ شناختی شباهتی به جنگ نرم داشته باشد، اما در این جنگ دیگر خبری از تلاش دشمن بر تضعیف باورها و افکار افراد یک سرزمین با استفاده از اعتقادات نیست. بلکه از رسانه‌های جدیدتر و فضاهای مجازی برای تحت تاثیر قرار دادن افراد جامعه استفاده می‌کند، بدون این‌که خود را نشان دهد. مانند حشره‌ای که ساختار چوب را از داخل از بین می‌برد اما از خارج چیزی مشهود نیست، قربانی خود را تحت تأثیر قرار می‌دهد.

به‌طور کلی در جنگ شناختی دشمن از سلاح‌هایی همچون اعتماد زدایی، ناامیدسازی جامعه، ناکارآمد نشان دادن حاکمیت، از بین بردن مشروعیت‌های جامعه و زیر سوال بردن اعتبار نظام و حاکمیت در راس یک کشور استفاده می‌کند(همان: ۵)

اما هدف جنگ شناختی چیست؟ بدون شک هدف و مقصود همه جنگ‌ها نابودی دشمن با هر روشی که بهتر و موثرتر باشد است. اما اهداف اصلی این

جنگ از بین بردن اعتماد جامعه نسبت به حاکمیت، نابود کردن نیروهای اجتماعی و سرمایه‌های کاری کشور است.

جنگ الکترونیک شناختی

جنگ الکترونیک شناختی استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشین (ML)[1] برای بهبود قابلیت‌های جنگ الکترونیک است. این مقوله می‌تواند طیف وسیعی از کاربردها را شامل شود، از خودکارسازی تصمیم‌گیری در مورد جنگ الکترونیک گرفته تا شناسایی و طبقه‌بندی سیگنال‌های الکترونیکی و پیش‌بینی تاکتیک‌های جنگ الکترونیک دشمن. یکی از نمونه‌هایی از این‌که چگونه می‌توان از فناوری شناختی در جنگ الکترونیک استفاده کرد، توسعه سامانه‌های جنگ الکترونیک هوشمند است که می‌توانند محیط‌های متغیر و تاکتیک‌های دشمن را بیاموزند و سازگار شوند. این سامانه‌ها می‌توانند از هوش مصنوعی برای تجزیه و تحلیل داده‌های حسگرهای الکترونیکی و سایر منابع برای شناسایی، ردیابی و طبقه بندی سیگنال های الکترونیکی و پیش‌بینی رفتار سامانه‌های جنگ الکترونیک دشمن استفاده کنند. اساساً، جنگ الکترونیک شناختی یک زمینه نوظهور است که هدف آن افزایش قابلیت‌های سامانه‌های جنگ الکترونیک از طریق استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشینی است(BIS Research, 2023: 1).

جنگ الکترونیک شناختی برای ارتقاء توسعه و عملیات فن‌آوری‌های جنگ الکترونیک در جامعه دفاعی اقدام به استفاده هوش مصنوعی در جنگ الکترونیک می‌کند. هوش مصنوعی سامانه‌های جنگ الکترونیک را قادر می سازد تا سریع‌تر و مؤثرتر به شرایط میدان نبرد با ساطع‌کننده‌های پیچیده و جدید پاسخ دهند. این

1- Machine Learning

جنگ، تکنیک های ارزیابی موقعیت مبتنی بر هوش مصنوعی برای اقدامات پشتیبانی الکترونیکی، تکنیک‌های تصمیم‌گیری برای حفاظت الکترونیکی، حمله الکترونیکی و مدیریت نبرد الکترونیکی، از جمله بهینه سازی، معاوضه‌های زمانی و هماهنگی توزیع شده را دربرمی‌گیرد (Haigh,2021, 1).

در سال‌های اخیر محققان با به‌کار بردن روش‌های هوش مصنوعی و یادگیری ماشین در تلاش برای ارائه فناوری‌های جنگ الکترونیک شناختی هستند. جنگ الکترونیک شناختی، باید بتواند در عین نداشتن ذره‌ای شناخت از سامانه‌های دشمن، وارد محیط شود، سامانه‌ها را شناسایی کند و حتی اقدامات متقابل مورد نیاز را به سرعت پیاده‌سازی کند. شناخت در این محیط شامل استفاده از آموزش ماشین برای ساخت سامانه‌های هوشمندتر است. این سامانه‌ها باید بتوانند سامانه‌های مقابل را تحریک کرده و با توجه به واکنش آن‌ها، ضمن تحمل کمترین آسیب به‌طور خودکار آموزش ببینند و به سرعت راهکار مقابله را کشف کنند (پژوهشکده اویونیک دانشگاه صنعتی اصفهان، ۱۳۹۷:۲).

البته ارتش ایالت متحده اغلب در استفاده از هوش مصنوعی در میدان جنگ احتیاط می‌کند. زیرا ممکن است تصمیم‌گیری در آن شرایط عواقب ناگواری داشته باشد. این در صورتی است که مدیران دارپا معتقدند که جنگ الکترونیک در فناوری‌های شناختی نقش مهمی دارد. از نظر آن‌ها میدان جنگ الکترونیک می‌تواند محیطی برای بهبود قابلیت‌های هوش مصنوعی باشد. از طرفی اثرات مخرب ناشی از تصمیم‌گیری سامانه‌های جنگ الکترونیک هوشمند بسیار پایین است زیرا به سرعت اشتباهات خود را تصحیح می‌کنند.

به ادعای مقامات نظامی آمریکا، در صورت تصمیم‌گیری نادرست از سوی سیستم هوشمند، از یک نیروی انسانی برای جبران اشتباه استفاده می شود؛ اما آقای تیلمن این‌چنین استدلال می‌کند: «سامانه‌های شناختی جنگ الکترونیک

می‌توانند کاملاً مستقل باشند. در یک مقطع، شما می‌توانید از یک انسان استفاده کنید. در ابتدا ارتش سامانه‌های راداری و ارتباطی دشمن را بررسی می‌کند تا بتواند حرکت متقابلی انجام دهد و سپس فناوری‌های جنگ الکترونیک را برای شناسایی و مسدود کردن سامانه‌های دشمن برنامه‌ریزی می‌کند. وقتی سامانه‌های راداری و ارتباطی توسط سخت‌افزار آنالوگ تعریف می‌شوند، این مسئله به‌مراتب حساس‌تر خواهد بود؛ اما بسیاری از نیروهای ارتش اکنون سامانه‌هایشان را با هسته دیجیتال توسعه می‌دهند و به این معناست که داشتن یک کتابچه راهنمای سخت‌افزاری واقعاً کار درستی به‌نظر نمی‌رسد زیرا آن‌چه در نهایت در میدان جنگ دیده می‌شود ممکن است واقعاً چیزی نباشد که برای آن برنامه‌ریزی صورت گرفته است. سامانه‌های جنگ الکترونیکی می‌توانند با شرایط غیرمنتظره خود را سازگار کنند».

استفاده از سامانه‌های شناختی در توسعه جنگ الکترونیک به محققان دفاعی کمک می‌کند تا الگوها را شناسایی کرده و فرضیه‌هایی را ایجاد کنند که می‌تواند منجر به پیشرفت‌های گسترده در سامانه‌های متعدد شود، در حالی که این سامانه‌ها پاسخ‌های قطعی برای مسائل را نمی‌دانند، اما می‌توانند حجم وسیعی از داده‌ها را از طیف وسیعی از منابع پیچیده تفسیر کنند تا فرضیه‌های مستدلی را برای بررسی ارائه کنند.

فن‌آوری یادگیری ماشین چیست؟

مطالعات نشان داده که سیستم یادگیری ماشین عملکرد بهتری نسبت به رویکردهای سنتی در هر میزان سیگنال به نویز دارد. از این‌رو سیستم‌های یادگیری ماشین می‌توانند ویژگی‌های اضافه و اطلاعات خارج از طیف RF را برای کمک به درک بهتر ما از محیط سیگنال بیفزایند. از این‌رو یک سیستم شناختی قادر به یادگیری به صورت بلادرنگ است. چنین سیستمی می‌تواند آنچه را که می‌بیند

(سیگنال‌هایی که دریافت می‌کند) یا آنچه را که می‌فرستند را بر اساس تجربه‌های کسب شده تغییر دهد. طبق گفته دارپا این قابلیت تصمیم‌گیری را می‌توان یک پیشرفت عمده نسبت به سامانه‌های RF سنتی که در آن فرکانس‌ها و جهت‌های فضایی صرف نظر از محیط عملیاتی اغلب دریک دنباله پیوسته اسکن می شوند، محسوب کرد. سامانه‌های سنتی درک کمی از آنچه که در طیف اتفاق می‌افتد دارند. همچنین سیگنال‌های تهدید ممکن است در یک ناحیه یا باند فرکانسی غیرمعمول باشند؛ اما از برنامه یادگیری ماشین انتظار می‌رود که سیگنال‌های غیر منتظره را نیز شناسایی کند(پژوهشکده اویونیک دانشگاه صنعتی اصفهان، ۱۳۹۷:۵).

سامانه‌های RF امروزی از استدلال‌های مبتنی بر قواعدی که مشابه نسل اول سامانه‌های هوش مصنوعی هستند، استفاده می‌کنند. جان تامپسون مدیر سامانه های عملیاتی شرکت نورثروپ‌گرومن می‌گوید: «برای مثال اکثریت سامانه‌های اقدامات پشتیبانی جنگ الکترونیک (ESM)[1] از جداول جستجو استفاده می‌کنند. به این صورت که داده‌ها جمع‌آوری شده وارد هواپیما می شوند و نرم‌افزار سیگنال ورودی را با پاسخ مناسب مرتبط می‌کند. اما افزایش دیجیتال سازی قابلیت‌های رادار، نیاز به سامانه‌های جنگ الکترونیک شناختی و انطباقی را مستلزم کرده است». آقای تامپسون در ادامه می‌گوید: «نیروهای نظامی دیگر نمی‌توانند برای مدت طولانی تنها به پایگاه داده‌های تهدید از پیش تعریف شده برای تشخیص، شناسایی، موقعیت‌یابی و واکنش به موقع متکی باشند، زیرا فناوری‌های امروزه قادرند شکل موج تهدیدها را از طریق نرم‌افزار و بدون نیاز به سخت‌افزار تغییر دهند. در چنین شرایطی سیستم‌های شناختی کلید موفقیت عملیات‌های آینده هستند»(همان: ۸)

1-Electronic support measurements.

یکی از اهداف برنامه سیستم‌های یادگیری ماشین آگاهی طیفی است. در واقع یادگیری ماشین نیازمند شناخت طیف رادیویی یا رادیو شناختی است.

رادیو شناختی چیست؟

زمانی که در رابطه با رادیو شناختی صحبت می‌کنیم در واقع در مورد توانایی درک محیط اطراف شامل تشخیص خودکار سیگنال‌های خودی از سیگنال‌های دشمن، تشخیص تهدیدات جنگ الکترونیک و سپس عملیات انتقال به فرکانس‌های مختلف برای جلوگیری از حمله الکترونیکی صحبت می‌کنیم. اغلب چنین عملیاتی را با اصطلاح «رادیو انطباقی» نامگذاری می‌کنند. در واقع رادیو شناختی یک فناوری مفید است که پیشرفت قابل توجهی در زمینه استفاده مؤثر از طیف فرکانسی به ارمغان می‌آورد. طراحی این فناوری به گونه‌ای است که با تغییر پارامترهای رادیویی، از طیف فرکانسی موجود استفاده بهینه را می‌برد(پژوهشکده اویونیک دانشگاه صنعتی اصفهان، ۱۳۹۷: ۷).

طی سال‌های اخیر، علایق تحقیقاتی رو به رشدی در توسعه قابلیت‌های شناختی در سامانه‌های مختلف الکترونیک پا به عرصه وجود گذاشته‌اند. میتولا و مگوایر[1] برای اولین بار مفهوم رادیو شناختی را در سال ۱۹۹۹معرفی نمودند(Mitola and Maguire, 1999: 2). در سال ۲۰۰۶، هایکین ایده رادار شناختی، که یک سیستم پویا است را پیشنهاد کرد که شکل موج ارسالی را بر اساس محیط عملیاتی انطباق و بهینه‌سازی می‌کند(Haykin, 2006: 5).

یکی از مهمترین اهداف رادیو شناختی، قابلیت دسترسی به طیف است. با توجه به بررسی‌های انجام شده، بخش عمده‌ای از هر باند فرکانسی که به کاربران اختصاص داده می‌شود، بدون استفاده باقی می‌ماند. رادیو شناختی این توانایی را

1-Mitola and Maguire

دارد که از بخش‌های بدون ا ستفاده طیف که به حفره‌های طیف معروف ه ستند، ا ستفاده کند. بنابراین، رادیو شناختی یک فناوری مخابرات بی سیم هو شمند ا ست که از محیط بیرونی خود آگاه ا ست و با توجه به آن، پارامترهای عملیاتی خود از قبیل توان ارسالی، فرکانس حامل و روش مدولاسیون را تنظیم می‌کند تا بتواند هر زمان و در هر مکان که احتیاج شد، مخابره قابل اطمینانی داشته باشد. از آنجایی که این مساله نوعی استدلال و یادگیری است، می‌توان برای هوشمندسازی آن از الگوریتم‌های یادگیری ماشین استفاده کرد.

از آنجا که د شمن همیشه سعی دارد ارتباطات را از بین ببرد، رادیو شناختی باید یک قدم جلوتر از د شمن با شد و همیشه در طول زمان بهبود یابد. به دلیل این‌که سامانه‌های شناختی می‌توانند سریعتر از انسان‌ها واکنش نشان دهند، بنابراین برای جلوگیری از حملات مخرب و بازیابی لینک ارتباطات با حداقل زمان خرابی، یک قدم جلوتر از هر دشمن بالقوه است. در سامانه‌های جنگ الکترونیک شناختی نیز همین رویکرد وجود دارد، به‌طوری‌که سامانه جنگ الکترونیک هو شمندتر و با سرعت بیشتر با تهدیدات و تداخل تطبیق می شود (پژوهشکده اویونیک دانشگاه صنعتی اصفهان، ۱۳۹۹: ۹).

از این‌رو یک سامانه شناختی قادر به یادگیری به صورت بلادرنگ ا ست. چنین سامانه‌ای می‌تواند آن‌چه را که می‌بیند (سیگنال‌هایی که دریافت می‌کند) یا آن‌چه را که می‌فر ستند بر ا ساس تجربه‌های کسب شده تغییر دهد. طبق گفته دارپا این قابلیت تصمیم‌گیری را می‌توان یک پیشرفت عمده نسبت به سامانه‌های فرکانس رادیویی سنتی که در آن فرکانس‌ها و جهت‌های فضایی صرف نظر از محیط عملیاتی اغلب دریک دنباله پیو سته ا سکن می شوند، مح سوب کرد. سامانه‌های سنتی درک کمی از آنچه که در طیف اتفاق می‌افتد دارند. همچنین سیگنال‌های

تهدید ممکن ا ست در یک ناحیه یا باند فرکانسی غیرمعمول با شند؛ اما از برنامه یادگیری ماشین انتظار می‌رود که سیگنال‌های غیر منتظره را نیز شناسایی کند.

سامانه‌هایفرکانس رادیویی امروزی از استدلال‌های مبتنی بر قواعدی که مشابه نسل اول سامانه‌های هوش مصنوعی هستند، استفاده می‌کنند. جان تامپسون مدیر سامانه های عملیاتی شرکت نورثروپ‌گرومن می‌گوید: «برای مثال اکثریت سامانه‌های اقدامات پشتیبانی جنگ الکترونیک(ESM)[1] از جداول جستجو استفاده می‌کنند. به این صورت که داده‌ها جمع‌آوری شده وارد هواپیما می‌شوند و نرم‌افزار سیگنال ورودی را با پاسخ مناسب مرتبط می‌کند. اما افزایش دیجیتال سازی قابلیت‌های رادار، نیاز به سامانه‌های جنگ الکترونیک شناختی و انطباقی را مستلزم کرده است پژوهشکده اویونیک دانشگاه صنعتی اصفهان، ۱۳۹۷: ۱۰).

آقای تامپسون اضافه کرد: «نیروهای نظامی دیگر نمی‌توانند برای مدت طولانی تنها به پایگاه داده‌های تهدید از پیش تعریف شده برای تشخیص، شناسایی، موقعیت‌یابی و واکنش به موقع متکی باشند، زیرا فناوری‌های امروزه قادرند شکل موج تهدیدها را از طریق نرم‌افزار و بدون نیاز به سخت‌افزار مجدد تغییر دهند. در چنین شرایطی سامانه‌های شناختی کلید موفقیت عملیات‌های آینده هستند.

توسعه الگوریتم‌های یادگیری ماشین

شرکت نورثروپ گرومن با همکاری نیروی دریایی آمریکا در حال توسعه الگوریتم‌های یادگیری ماشین برای دنبال کردن حمله الکترونیکی علیه هواپیمای جنگ الکترونیک EA-18G Growler است. این برنامه که تا سال ۲۰۲۵ اجرایی

1-Electronic Support Measures

خواهد شد، قابلیت‌های جنگ الکترونیک را در برابر رادارهای دشمن یا رادارهای ناشناخته انطباقی و هوشمند تقویت خواهد کرد.

یک نسخه توسعه یافته از پروژه نورثروپ گرومن، مفهوم عملیات تجمعی پرنده‌های بدون سرنشین است که با اصطلاح Remedy کدگذاری شده است. این پرنده‌های بدون سرنشین داخل یک کپسول در زیر هواپیما قرار می‌گیرند و به‌عنوان حسگرهای نزدیک عمل می‌کنند. از این‌رو داده‌های بیشتری برای نگرش شناختی فراهم می‌کنند. هنگامی که کپسول از هواپیمای جنگنده رها می‌شود، تعداد زیادی پرنده بدون سرنشین کوچک از آن خارج شده و به سمت رادارهای دشمن حرکت می‌کنند. به‌دلیل سرعت کم و کوچک بودن این پرنده‌ها، رادار آن‌ها را به‌عنوان دسته‌ای از پرنده‌ها تشخیص داده و عکس‌العملی نشان نخواهد داد. از این‌رو این پرنده‌ها به هدف نزدیک شده و عملیات طیف شناختی را انجام داده و نتیجه را برای هواپیما ارسال می‌کنند. همچنین شرکت نورثروپ گرومن به‌دنبال حسگرهای مادون قرمز و RF برای این پرنده‌های بدون سرنشین کوچک است تا آگاهی موقعیتی چند بعدی را فراهم کند. نمونه دیگر این پروژه هواپیمای بدون سرنشین Dash X است که می‌تواند به تنهایی از هواپیمای جنگ الکترونیک EA-18G Growler رها شده و عملیات جمع‌آوری و ارسال سیگنال‌های رادار به هواپیما را انجام دهد.

کاربردهای جنگ الکترونیک شناختی

موفق‌ترین کاربردهای جنگ الکترونیک شناختی آن‌هایی نیستند که کاملاً به رایانه‌ها متکی باشند، بلکه آن‌هایی هستند که ورودی رایانه را با استراتژی‌ها و درک انسانی ترکیب می‌کنند. تخصیص جمع‌آوری داده‌ها، ذخیره سازی اطلاعات و محاسبات به رایانه‌ها به انسان اجازه می‌دهد تا ظرفیت بیشتری برای تمرکز خلاقیت و بینش خود بر روی راه‌حل‌های بهتر داشته باشد(BAE SYSTEMS, 2024: 3).

مدیر پردازش حسگر و استخراج شرکت BAE Systems می‌گوید: درگذشته هنگامی‌که نیروها وارد یک صحنه نبرد شده و با سیگنال‌های مختل‌کننده روبه‌رو می‌شدند، نوع سیگنال، فرکانس، طول‌موج و پهنای باند را جمع‌آوری می‌کردند و اطلاعات به آزمایشگاه منتقل می‌شد تا پس از بررسی اقدامات متقابل ارائه شود. بعد از چند ماه راه‌های مقابله در سامانه‌ها پیاده‌سازی می‌شد. اما پیشرفت نرم‌افزارها و تجهیزات رادیویی قابل‌برنامه‌ریزی مجدد، روش های قبلی را غیرممکن و بلااستفاده کرده و راه را برای گذر به نسل بعد با استفاده از یادگیری ماشین بازکرده است. شکل زیر یک حسگر قابل حملی را نشان می‌دهد که از روش پردازش شناختی برای سیگنال‌های فرکانس رادیویی در تداخلات استفاده می‌کند.

شکل ۲) حسگر قابل حمل که از روش پردازش شناختی برای شناسایی سیگنال‌های RF در زمان تداخلات استفاده می‌کند.

در حال حاضر محققان وزارت دفاع آمریکا در حال آزمایش فناوری‌های شناختی جنگ الکترونیک هستند. این فناوری‌ها در آینده می‌توانند سامانه‌های دشمن را به‌طور مستقل شناسایی کرده و بدون هیچ برنامه‌ریزی قبلی به مبارزه با آن‌ها

بپردازند. بر همین اساس آژانس تحقیقاتی دفاعی آمریکا (دارپا) در برخی پروژه‌های خود از هوش مصنوعی برای سامانه‌های جنگ الکترونیک استفاده کرده است. به‌عنوان نمونه پروژه اقدامات راداری انطباقی و یادگیری رفتاری برای جنگ الکترونیک انطباقی، از سامانه‌های جنگ الکترونیک هوشمند استفاده کرده‌اند.

به‌عنوان مثال فناوری اقدام متقابل راداری می‌تواند سامانه‌های جنگ الکترونیک هوابرد را برای اقدامات مؤثر علیه رادارهای جدید و ناشناخته به‌صورت بلادرنگ آماده کند. در واقع این فناوری در برابر یک رادار جدید یا ناشناس قادر به انجام فعالیت‌های زیر است:

- ✓ تفکیک سیگنال‌های رادارهای ناشناس در برابر دیگر سیگنال‌ها؛
- ✓ کاهش تهدید از رادارهای ناشناس؛
- ✓ ارسال سیگنال‌های متقابل و ارزیابی تاثیر آن‌ها روی رادار.

همچنین به دلیل این‌که معماری این فناوری باز است، اجازه ورود، اصلاح و حذف ماژول‌های نرم‌افزاری تو سط کاربر داده می شود. علاوه بر این الگوریتم‌ها و نرم‌افزارهای پردازش سیگنال در فناوری اقدامات راداری انطباقی به گونه‌ای است که برای بکارگیری آن در نیروی هوایی و صنایع دفاعی نیاز به تغییرات سخت‌افزاری کلی نیست.

از طریق فناوری « اقدامات راداری انطباقی» هواپیما می‌تواند عملیات جنگ الکترونیک مناسبی در مقابل شبکه راداری دشمن اجرا کند.

فناوری اقدامات راداری انطباقی به‌طور ویژه سامانه رادار را هدف قرار می‌دهد. در حالی که پروژه BLADE با توسعه روش‌ها و الگوریتم‌های یادگیری ماشین،

به‌سرعت تهدیدات رادیویی جدید را تشخیص داده و با ترکیب اقدامات متقابل جدید، خسارت جنگی را بر اساس مشاهدات هوایی به‌صورت دقیق ارزیابی می‌کند. هدف از طراحی این فناوری، مقابله با تهدیدات ارتباطات بی‌سیم جدید و پویا در محیط های تاکتیکی است. علاوه بر این فناوری BLADE می‌تواند سامانه‌های ارتباطی بی‌سیم را با هدف متوقف کردن پخش اطلاعات زیر نظر بگیرد (پژوهشکده اویونیک دانشگاه صنعتی اصفهان، ۱۳۹۷: ۶).

حوزه اقدامات جنگ الکترونیک و جنگ الکترونیک شناختی

توسعه جنگ الکترونیک بر سه حوزه اقدامات پشتیبانی الکترونیکی، اقدامات ضد الکترونیکی و اقدامات ضدضد الکترونیکی متمرکز شده است. طی سال‌های اخیر، تحقیقات بر روی مدل سیستم شناختی محیط جنگ الکترونیک پیشرفت زیادی داشته است. ناو و جونگ[1] مدل تهدیدی را برای تحقق یک فرآیند تصمیم‌گیری مستقل جهت تشخیص تهدید، طبقه بندی و انتخاب اقدامات متقابل جایگزین در برابر تهدیدات در تنظیمات جنگ الکترونیک معرفی کردند. (You *et al, 2019*: 4)

استفاده از فناوری‌های نوظهور به‌ویژه الگوریتم‌های شناختی و به‌کارگیری تکنیک‌های مبتنی بر شناخت، یک سیستم راداری را قادر به درک محیط عملیاتی خود نموده و با تنظیم دقیق و بر ا ساس پارامترهای فنی خود، مانند عرض پالس، فاصله تکرار پالس و فرستنده وظیفه محول شده را به نحو مطلوب انجام می‌دهد. البته مسلم است که روش‌های سنتی جنگ الکترونیک، که از قبل برنامه‌ریزی شده و بر آن تکیه می‌کنند، نمی‌تواند به‌طور موثر کارآمد باشد. بنابراین با تهدیدات راداری مدرن، نیاز است نسل بعدی سامانه‌هایجنگ الکترونیک با توانایی‌های

1-Noh and Jeong

شناختی تقویت شده تا بتوانند در پاسخ به تغییر، تصمیمات مستقل بگیرند (Xiao, 2018: 1)

برخلاف سامانه‌های رادار سنتی، توانایی‌های شناختی می‌تواند به رادار امکان تنظیم دقیق ارسال پرتو خود را بدهد، پارامترهایی مانند عرض پالس، فاصله تکرار پالس، توان و فنون فشردگی پالس موجب شده تا رادار وظیفه محوله را بنحو احسن انجام دهد. بنابراین، برای دفاع در برابر سامانه‌های رادار شناختی، شناخت، کلیدی برای سامانه جنگ الکترونیک نسل بعدی است.

پیامدهای بالقوه هوش مصنوعی و یادگیری ماشین در استراتژی‌های جنگ الکترونیک شناختی

پیامدهای بالقوه هوش مصنوعی و یادگیری ماشین در استراتژی‌های جنگ الکترونیک شناختی را می‌توان در قالب فرصت و چالش مورد بررسی قرار داد.

الف) فرصت‌های هوش مصنوعی و یادگیری ماشین

ادغام هوش مصنوعی و یادگیری ماشین در استراتژی‌های جنگ الکترونیک شناختی و جنگ‌های آینده، این پتانسیل را دارد که نحوه مبارزه با درگیری‌ها را به‌طور قابل توجهی تغییر دهد. از این‌رو برخی از فرصت‌های بالقوه آن عبارتند از:

- ✓ **سلاح‌های خودمختار**: فناوری‌های هوش مصنوعی و یادگیری ماشین را می‌توان برای توسعه سلاح‌های خودمختار مانند هواپیماهای بدون سرنشین و سایر سامانه‌های بدون سرنشین استفاده کرد. این سامانه‌ها را می‌توان طوری برنامه‌ریزی کرد که بدون دخالت انسان تصمیم‌گیری و اقداماتی انجام دهند. این می‌تواند سرعت و کارایی عملیات نظامی را افزایش دهد، اما

همچنین نگرانی‌هایی را در مورد مسئولیت‌پذیری و کنترل تسلیحات خود مختار ایجاد می‌کند.

- ✓ **جنگ سایبری**: هوش مصنوعی و یادگیری ماشین را می‌توان برای بهبود قابلیت‌های جنگ سایبری، مانند تشخیص خودکار و پاسخ به حملات سایبری، استفاده کرد. با این حال، این فناوری‌ها همچنین می‌توانند توسط دشمنان برای راه‌اندازی حملات سایبری پیچیده‌تر و موثرتر مورد استفاده قرار گیرند.
- ✓ **بهبود آگاهی موقعیتی**: هوش مصنوعی و یادگیری ماشین می‌توانند برای تجزیه و تحلیل و پردازش مقادیر زیادی از داده‌ها از منابع مختلف مانند رادار، سیگنال‌های الکترونیکی و تصاویر ماهواره‌ای استفاده شوند. این می‌تواند اطلاعات بی‌درنگ در مورد میدان نبرد را به واحدهای نظامی ارائه دهد و آن‌ها را قادر می سازد تا تصمیمات آگاهانه‌تری بگیرند و سریع‌تر به شرایط متغیر پاسخ دهند.
- ✓ **افزایش دقت**: هوش مصنوعی و یادگیری ماشین را می‌توان برای بهبود دقت سامانه‌های تسلیحاتی، مانند هدف‌گیری خودکار تجهیزات دشمن، استفاده کرد. این می‌تواند خطر آسیب‌های جانبی را کاهش دهد و اثربخشی عملیات نظامی را افزایش دهد.
- ✓ **تصمیم گیری**: هوش مصنوعی و یادگیری ماشین می‌توانند برای خودکار سازی فرآیندهای تصمیم‌گیری، مانند تجزیه و تحلیل داده‌ها و ارائه توصیه‌هایی به فرماندهان، استفاده شوند. این امر می‌تواند سرعت و کارایی تصمیم‌گیری را افزایش دهد، اما نگرانی‌هایی را در مورد پاسخگویی و شفافیت این تصمیمات نیز ایجاد می‌کند.

- ✓ **جنگ نامتقارن**[1]: استفاده از هوش مصنوعی و یادگیری ماشین در جنگ می‌تواند یک مزیت نامتقارن برای کشورهایی با فناوری پیشرفته ایجاد کند و به‌طور بالقوه آن‌ها را قادر به تسلط بر میدان نبرد کند(BIS Research, 2023: 2).

ب) چالش‌های هوش مصنوعی و یادگیری ماشینی در جنگ الکترونیک شناختی

استفاده از هوش مصنوعی و یادگیری ماشین در استراتژی‌های جنگ آینده چالش‌های متعددی را نیز از نظر نگرانی‌های اخلاقی و قانونی، مانند مسئولیت اقدامات سلاح‌های خودمختار و حفاظت از غیرنظامیان در جنگ، ایجاد می‌کند که در نظر گرفتن این چالش‌ها هنگام توسعه و اجرای این فناوری‌ها در ارتش بسیار مهم است. برخی از مهم‌ترین چالش‌های این فنآوری‌ها عبارتند از:

- ✓ **پیچیدگی**: توسعه و پیاده‌سازی الگوریتم‌های هوش مصنوعی و یادگیری ماشین برای جنگ الکترونیک شناختی می‌تواند یک کار پیچیده و چالش‌برانگیز باشد که به سطح بالایی از تخصص و دانش تخصصی نیاز دارد.
- ✓ **کیفیت داده**: کیفیت و دقت داده‌های مورد استفاده برای آموزش هوش مصنوعی و الگوریتم‌های یادگیری ماشین بسیار مهم است، اگر داده‌ها دقیق یا بی‌طرفانه نباشند، سامانه قادر به تصمیم‌گیری مناسب نخواهد بود.

1-Asymmetric warfare

- ✓ **امنیت سایبری:** خطر هک شدن یا به خطر افتادن سامانه‌های هوش مصنوعی و یادگیری ما شین وجود دارد که می‌تواند عواقب جدی برای عملیات جنگ الکترونیک داشته باشد.
- ✓ **نگرانی‌های اخلاقی:** مانند هر فناوری نظامی، نگرانی‌های اخلاقی در مورد اســتفاده از هوش مصــنوعی و یادگیری ماشــین در جنگ الکترونیک وجود دارد، مانند تصمیم‌گیری مستقل و احتمال عواقب ناخواسته.
- ✓ **خطرات اتکای بیش از حد به فناوری:** این خطر وجود دارد که ســازمان‌ها بیش از حد به هوش مصنوعی و سامانه‌های یادگیری ما شین وابسته شوند، که می‌تواند منجر به کمبود تخصص انسانی و توانایی‌های تصمیم‌گیری شود.

بنابراین، در حالی که اســتفاده از هوش مصــنوعی و یادگیری ماشــینی در جنگ الکترونیک شــناختی می‌تواند مزایای زیادی به همراه داشــته باشــد، اما آگاهی از چالش‌ها و محدودیت‌های این فناوری‌ها و بردا شتن گام‌هایی برای مقابله با آن‌ها نیز حائز اهمیت می‌باشد (BIS Research, 2023: 3).

نتیجه‌گیری

جنگ الکترونیک شــناختی نشــان دهنده تغییر قابل توجهی در نحوه انجام جنگ الکترونیک ا ست. از آنجایی که ا ستفاده از هوش مصنوعی و یادگیری ما شینی در جنگ الکترونیک همچنان در حال رشــد اســت، ادامه تحقیق و توســعه این فناوری‌ها برای تحقق کامل پتانســیل آن‌ها و رســیدگی به چالش‌هایی که ارائه می‌کنند بسیار مهم است.

گســتردگی و تنوع حملات در حوزه الکترومغناطیس، با پیشــرفت رادارها و ابزارهای شناختی، سامانه‌های جنگ الکترونیک سنتی را باچالشی ا سا سی روبر

کرد. در همین راســتا دیجیتالی شــدن ســامانه‌های راداری باعث شــده اســت روش‌های جمینگ و ضــد جمینگ پیشــرفت‌های زیادی داشــته باشــند. در حال حاضر دیگر تکیه بر آگاهی از اطلاعات قدیمی از یک سامانه راداری برای مقابله با آن کفایت نمی‌کند. به عبارت دیگر رادارها می‌توانند با سرعت بالا بسیاری از ویژگی‌های خود را تغییر داده و برای دشمن خود کاملا ناشناخته باشند. در چنین محیطی سامانه‌های جنگ الکترونیکی شناختی می‌توانند راهکاری مناسب برای مقابله با رادارها ارائه دهند. در همین رابطه فناوری‌هایی همچون یادگیری ماشین و هوش مصنوعی کلید اصلی برای ساخت یک سامانه جنگ الکترونیک شناختی به‌شمار می‌روند.

بنابراین ظهور هوش مصــنوعی و یادگیری ماشــینی در درگیری‌های مدرن، آینده جنگ الکترونیک را شــکل می‌دهد و این فن‌آوری‌ها تأثیر عمیقی بر نحوه مبارزه ما با جنگ‌ها در آینده خواهد داشت. از این‌رو جنگ الکترونیک شناختی با ترکیب روش‌های سنتی و هوش مصنوعی در قالب یک سامانه، می‌تواند حملات جدید و ناشناخته را شناسایی کرده و به میزان بسیار زیادی حملات جدید و ناشناخته را شناسایی و واکنش مناسب را در صحنه نبرد اتخاذ کند.

منابع

الف) منابع فارسی

۱- حاجی زاده، سیروس، (۱۴۰۱)، " تبیین زمینه‌ای، نظری، مفهومی و کاربردی جنگ شناختی"، دوفصلنامه بازی جنگ، سال پنجم، شماره ۱۰، صص: ۱۴۳-۱۰۳.

۲- پایدار، پانته‌آ، (۲۰۲۰)، " جنگ شناختی چیست؟" ، قابل دسترسی در: https://dataak.com/blog

۳- پژوهشکده اویونیک دانشگاه صنعتی اصفهان، (۱۳۹۷)، " جنگ الکترونیک شناختی"، دانشگاه صنعتی اصفهان.

۴- رجبی، محمد ابراهیم و خالقی بیزکی، حسین، (۱۴۰۰)، "معماری پیشنهادی جنگ الکترونیک شناختی مبتنی بر رادارهای شناختی و سیستم شناختی انسان"، هشتمین کنفرانس ملی رادار و سامانه‌های مراقبتی ایران، دانشگاه صنعتی مالک اشتر.

۵- سنگرگیر، مراد و جواهری، علی‌رضا، (۱۳۹۱)، "جنگ الکترونیک"، موسسه آموزشی و تحقیقاتی صنایع دفاع، تهران

۶- عفیفی، احمد،کریم زاده، مرتضی و نظافتی، محمدباقر، (۱۳۸۵)، "جنگ الکترونیک برای صحنه نبرد دیجیتالی"، موسسه آموزشی و تحقیقاتی صنایع دفاع، تهران.

۷- گودرزی، مهناز و شاه‌رضائی، محمدحسن، (۱۴۰۱)، " به‌کارگیری علم و فن‌آوری در جنگ الکترونیک در ارتقاء قدرت منطقه‌ای ج.ا.ایران"، اولین همایش ملی جایگاه علم و فناوری در دفاع مقدس.

۸- محمدی نجم، سیدحسین، (۱۳۹۵)، "جنگ شناختی؛ بعد پنجم جنگ"، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

ب) منابع انگلیسی

9-BAE SYSTEMS, (2024), “What is cognitive electronic warfare?”, Access in: https:// www.baesystems.com /en-us/definition.

10-BIS Research, (2023), “Cognitive Electronic Warfare: The Rise of AI and ML in Modern Conflicts”, access in: https://bisresearch.com

11-Haigh, Karen, & Andrusenko, Julia, (2021), “Cognitive Electronic Warfare An Artificial Intelligence Approach”, Artech House, Canton Street, Norwood, MA 2062.

12-J. Mitola III and G. Q. Maguire, Jr., (1999) “Cognitive radio: Making software radios more personal,” IEEE Personal Commun., vol. 6, no. 4, pp. 13–18.

13-S. Haykin, (2006), “Cognitive radar: A way of the future,” IEEE Signal Processing Magazine, vol. 23, no. 1, pp. 30-40.

14-S. Haykin, (2009) “Cognition is the key to the next generation of radar systems,” Proc. of the 13th IEEE Digital Signal Processing Workshop and 5th IEEE Signal Processing Education Workshop (DSP/SPE ’09), pp. 463–467.

15-Xiao, Qinghan, (2018), “A Conceptual Architecture of Cognitive Electronic Warfare System”, Radar Electronic Warfare Section Defense R&D Canada – Ottawa Research Centre Ottawa, Canada.

16-You, Shixun, Diao, Ming & Gao, Lipeng, (2019), “Deep Reinforcement Learning for Target Searching in Cognitive Electronic Warfare”, Published in: IEEE Access (Volume: 7).