Supreme National Defense University Quarterly Journal of Defense Logistics and Technology

https://amfad.sndu.ac.ir E-ISSN: 2980-8073

Vol. 8, Special Issue, Issue. 28, Winter 2025 **Received:** 2025/08/03 **Accepted:** 2025/11/08

Research paper

Conceptual Model of the Application Emerging Technologies in Signals Intelligence with a Cybersecurity Approach

Mehdi Teymoori
Ph.D. student, Supreme National Defense University, Tehran, Iran (Corresponding Author)
Email: mehraeen786@gmail.com.
Sina Keyhanian
Assistant Professor, Supreme National Defense University, Tehran, Iran
Mohammad Sepehri
Assistant Professor, Khatam Al-Anbiya Air Defense University, Tehran, Iran
Mehran Keshtkar
Associate Professor, Supreme National Defense University, Tehran, Iran

Abstract

In the current era, defense organizations face numerous challenges in the field of signal intelligence, one of the solutions to which is the adoption of emerging technologies, particularly artificial intelligence. This research has endeavored to innovatively analyze the most practical emerging technologies in this domain from a cybersecurity perspective. The study follows an applied-development approach with a qualitative descriptive methodology. For data collection, a systematic literature review approach was employed, followed by snowball sampling to conduct semi-structured interviews with ten experts who were experienced officials in the field of signal intelligence until theoretical saturation was achieved. Finally, through thematic analysis, an indigenous research model was designed. The findings indicate that the most practical technologies in signal intelligence are artificial intelligence/machine learning, cloud computing, quantum computing, natural language processing, robotics, and 5G. Additionally, the most critical cybersecurity requirements encompass four layers: hardware security, software security, information security, and communication security against cyber vulnerabilities and threats. The details of each of these categories are elaborated in the paper.

Keywords: Signals Intelligence (SIGINT), Emerging Technologies, Artificial Intelligence (AI), Cybersecurity

سال هشتم ویژه‌نامه (پیاپی ۲۸)، زمستان ۱۴۰۴، صص. ۱۳۳-۱۷۸
تاریخ دریافت: ۱۴۰۴/۰۵/۱۲ ـ تاریخ پذیرش: ۱۴۰۴/۰۸/۱۷

مقاله پژوهشی

مدل مفهومی کاربست فناوری‌های نوظهور در اطلاعات سیگنالی با رویکرد امنیت سایبری

مهدی تیموری
دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، تهران، ایران (نویسنده مسئول)
Email: mehraeen786@gmail.com

سینا کیهانیان
استادیار دانشگاه عالی دفاع ملی، تهران، ایران

محمد سپهری
استادیار دانشگاه پدافند هوایی خاتم‌الانبیا (ص)، تهران، ایران

مهران کشتکار
دانشیار دانشگاه عالی دفاع ملی، تهران، ایران

چکیده

در عصر حاضر، سازمان‌های دفاعی با مشکلات عدیده‌ای در حوزه اطلاعات سیگنالی مواجه هستند که یکی از راه‌های حل چالش‌های پیش‌رو، به‌کارگیری فناوری‌های نوظهور به‌ویژه هوش مصنوعی است. در این پژوهش تلاش گردیده تا با نگاهی نوآورانه کاربردی‌ترین فناوری‌های نوظهور در این حوزه با رویکرد امنیت سایبری مورد تحلیل قرار گیرد. هدف پژوهش کاربردی-توسعه‌ای بوده و روش آن توصیفی با رویکرد کیفی است. به‌منظور گردآوری داده‌ها از رویکرد مرور ادبیات سیستماتیک استفاده‌شده است و در ادامه، با روش نمونه‌گیری گلوله برفی با ده نفر از خبرگانی که از مسئولین باتجربه در حوزه اطلاعات سیگنالی بودند مصاحبه نیمه‌ساختاریافته تا اشباع نظری انجام شد. در نهایت با تحلیل مضمون مدل بومی پژوهش طراحی گردید. نتایج پژوهش نشان می‌دهد کاربردی‌ترین فناوری‌ها در حوزه اطلاعات سیگنالی فناوری‌های هوش مصنوعی و یادگیری ماشینی، رایانش ابری، رایانش کوانتومی، پردازش زبان طبیعی، رباتیک و 5G بوده و نیز مهم‌ترین الزامات امنیت سایبری شامل چهار لایه امنیت سخت‌افزار، امنیت نرم‌افزار، امنیت اطلاعات و امنیت ارتباطات در برابر آسیب‌پذیری‌ها و تهدیدات سایبری است که به جزییات هر یک از مقولات فوق در مقاله پرداخته‌شده است.

کلیدواژه‌ها: اطلاعات سیگنالی، فناوری‌های نوظهور، هوش مصنوعی، امنیت سایبری

20.1001.1.28212606.1404.8.5.4.7 https://amfad.sndu.ac.ir/ E-ISSN: 2980-8073

مقدمه و بیان مسئله

در عصر حاضر، فناوری‌های نوظهور به‌طور فزاینده‌ای در حال ایجاد تغییر و تحول شگرف در زیرساخت‌ها، تجهیزات و فرایندهای حوزه‌های مختلف دفاعی هستند. با بهره‌گیری مناسب و به‌موقع از فناوری‌های نوین در حوزه نظامی و دفاعی، تا حدود زیادی می‌توان پیاده‌سازی و مدیریت در این حوزه را با دقت بیشتر و پویاتری انجام داد (بیک بیلندی، ۱۴۰۱). ازجمله این حوزه‌ها، «اطلاعات سیگنالی»[1] است. این اطلاعات از سیگنال‌های منتشره از طیف امواج الکترومغناطیس در بخش ارتباطی و الکترونیکی کسب و پس از جمع‌آوری، پردازش، تجزیه‌وتحلیل و انتشار، به‌صورت گزارش اطلاعاتی به‌دست می‌آید (شاه‌رضایی، ۱۴۰۲). اطلاعات سیگنالی به‌منظور اشراف اطلاعاتی، آگاهی وضعیتی از صحنه نبرد، تهدیدشناسی و رفتارشناسی کشورهای دوست، رقیب و دشمن به‌کار رفته و برای مقاصد راهبردی، عملیاتی و تاکتیکی نیروهای مسلح بسیار کاربردی است به‌گونه‌ای که حتی سازمان‌های غیردفاعی نیز به‌منظور تصمیم‌گیری‌های بهینه در حوزه کاری خود از این اطلاعات بهره‌برداری می‌کنند.

با پیشرفت فناوری‌های نوظهور، نقش اطلاعات سیگنالی در تحلیل داده‌ها نیز افزایش یافته و ادغام روزافزون اطلاعات سیگنالی با دیگر حوزه‌های اطلاعاتی، تصمیم‌سازی جامع‌تر و دقیق‌تری را ممکن می‌سازد. در آینده، انتظار می‌رود که اطلاعات سیگنالی نقش پررنگ‌تری در حوزه‌هایی مانند امنیت سایبری، مقابله با تروریسم و جنگ الکترونیکی ایفا کند؛ جایی که توانایی تحلیل سریع و پاسخ فوری به تهدیدات حیاتی است (The Role of SIGINT, 2024).

به‌منظور ارتقای قابلیت‌های عملیاتی و بهبود کارایی و اثربخشی در چرخه فعلی اطلاعات سیگنالی ازجمله افزایش قابل‌توجه سرعت و دقت حسگرهای پیشرفته، جمع‌آوری، پردازش و تحلیل و رمزگشایی داده‌های حجیم و پیچیده و انتشار بلادرنگ، به‌کارگیری فناوری‌های نوظهور ازجمله هوش مصنوعی و رایانش کوانتومی بسیار راهگشا خواهد بود. با نوآوری‌های فناورانه، امکان سفارشی‌سازی و انعطاف‌پذیری بیشتر و متناسب با نیازهای عملیات اطلاعاتی

1. Signals Intelligence

خاص ممکن می‌شود. ازاین‌رو، با توجه به پیشرفت فناوری ارتباطات و اطلاعات، سازمان‌های دفاعی برای حفظ برتری و اشراف اطلاعاتی خود ناگزیر به بهره‌برداری از فرصت‌های فناوری‌های نوظهور به‌ویژه هوش مصنوعی به‌منظور ارتقای سطح تجهیزات، هوشمند نمودن زیرساخت‌ها، سامانه‌ها و فرایندهای اطلاعات سیگنالی هستند.

با توجه به پیشرفت علم و فناوری در کلیه حوزه‌ها، روند ظهور و بروز تهدیدات به شکل و فرم جدید در قالب تهدیدات نوپدید، به‌ویژه تهدیدات نوپدید دفاعی ظهور می‌نمایند (شاملو، ۱۴۰۳). ازجمله راه‌کارهای کشف و شناسایی این تهدیدات اطلاعات سیگنالی است که در سالیان اخیر در این حوزه چالش‌های مختلفی در زمینه‌های عملیاتی، فنی و تجهیزاتی، نیروی انسانی و ... مشاهده می‌گردد. کشورها در برابر رهگیری اطلاعات سیگنالی خود توسط دیگران نسبت به گذشته آگاه‌تر و خبره‌تر شده‌اند و این مهم، کار را برای سازمان‌های اطلاعاتی سخت‌تر کرده است. همچنین، تغییرات گسترده محیطی و پیشرفت روزافزون فناوری و درنتیجه تولید و انتشار اطلاعات با سرعت بالا و رمزنگاری پیچیده و چندلایه از طریق ارتباطات الکترونیکی و ارتباطی از منابع متنوع، باعث ایجاد حجم انبوهی از داده و اطلاعات شده که علاوه بر چالش‌های ذخیره‌سازی، نیازمند به‌روزرسانی مستمر ابزارها و روش‌های جمع‌آوری، پردازش، رمزگشایی و تجزیه‌وتحلیل آن‌ها است که برای سازمان‌های دفاعی بسیار هزینه‌بر است.

فعالیت در زمینه اطلاعات سیگنالی نیازمند دانش علمی پیشرفته، یادگیری مداوم و صرف سال‌ها کسب تجربه در محیط به‌صورت بی‌وقفه و شبانه‌روزی است. متخصص حوزه اطلاعات سیگنالی بایستی در کوتاه‌ترین زمان پس از تجزیه‌وتحلیل اطلاعات رهگیری شده تصمیم‌گیری نماید که درحال‌حاضر با توجه به حجم انبوه داده‌ها با روش‌های دستی و سنتی قادر به انجام مأموریت خود نخواهد بود. چراکه آگاهی وضعیتی از صحنه نبرد باید در کمترین زمان ممکن همراه با دقیق‌ترین اطلاعات در اختیار فرماندهان و تصمیم‌گیرندگان سازمان‌های ذی‌نفع قرار گیرد. عدم اشراف در علوم پیشرفته مورد نیاز و به‌روز فناوری

اطلاعات و ارتباطات، خستگی ناشی از وظایف تکراری روزانه، عدم تمرکز و خطای ناشی از آن از دیگر چالش‌های پیش‌رو است.

از سوی دیگر، با توجه به رشد روز افزون فناوری اطلاعات و ارتباطات در حوزه «رقمی»[1] و نقش محوری داده‌ها و بهره‌برداری از فناوری‌های نوظهور وابستگی حوزه اطلاعات سیگنالی به فضای سایبر بیشتر از گذشته خواهد شد و در نتیجه، با مخاطرات و چالش‌های جدید روبه‌رو خواهد گردید. در زمینه امنیت سایبری در حوزه اطلاعات سیگنالی نیز افزایش آسیب‌پذیری‌ها و تهدیدات سایبری ازجمله دسترسی غیرمجاز، حملات بدافزاری و نقض داده‌ها متصور بوده که در نتیجه نیاز به رعایت الزامات امنیت سایبری دارایی‌های مشهود و نامشهود سایبری برای حفظ تداوم عملکرد، حفاظت از سامانه‌ها، تجهیزات و حفظ یکپارچگی، محرمانگی و دسترسی داده‌ها است. از این‌رو، ضرورت دارد با رویکرد امنیت سایبری و رعایت الزامات امنیتی در برابر آسیب‌پذیری‌ها و تهدیدات سایبری متصور، حفظ تداوم عملکرد و حفاظت از سامانه‌ها و تجهیزات سایبری حوزه اطلاعات سیگنالی موردتوجه قرار گیرد.

با توجه به مسائل مطرح‌شده، سازمان‌های دفاعی جهت افزایش توان رزم خود و جلوگیری از عقب‌ماندگی در حوزه اطلاعات سیگنالی نیازمند به‌کارگیری فناوری‌های نوظهور هستند. تا بتوانند ضمن افزایش دقت، سرعت، کارایی و اثربخشی در تصمیم‌سازی و تصمیم‌گیری بهتر و بهینه‌سازی منابع و عملکرد، کاهش خطا و هزینه‌های نیروی انسانی کارکردی موفقیت‌آمیز داشته باشند. همچنین امنیت سایبری نیز در حوزه اطلاعات سیگنالی ضروری است. ازاین‌رو، جهت بررسی موارد پیش‌گفته، این پژوهش به دنبال ارائه مدلی در خصوص چگونگی به‌کارگیری فناوری‌های نوظهور در حوزه اطلاعات سیگنالی با رویکرد امنیت سایبری است.

1. Digital

۱. پیشینهٔ پژوهش

ترسلی و همکاران (۱۴۰۳) در پژوهشی با عنوان «کاربرد هوش مصنوعی در بهبود فرایند جمع‌آوری و تحلیل اطلاعات» نشان داده‌اند که برای پردازش و تحلیل کلان‌داده‌ها و دستیابی به اشراف اطلاعاتی، سازمان‌های مرتبط، باید قابلیت‌های هوش مصنوعی را در تمام اجزای چرخه اطلاعات به‌صورت یکپارچه پیاده‌سازی نماید. این کاربرد با خودکارسازی و کاهش نقش کاربران و زمان در کل چرخه اطلاعات، ضمن ایجاد فرصت‌های نوآورانه، قدرت پیش‌بینی و تصمیم‌گیری را برای تصمیم‌سازان افزایش می‌دهد. جامعه اطلاعاتی باید قابلیت‌های مبتنی بر هوش مصنوعی را در تمام اجزاء چرخه اطلاعات به‌صورت یکپارچه، به‌عنوان بخشی از چشم‌انداز آینده هوشمند، پیاده‌سازی کند تا با خودکارسازی و کاهش نقش کاربران در کل چرخه اطلاعات، زمان انجام چرخه را به‌طور قابل‌توجهی ساعت‌ها تا روزها کاهش دهد.

رستمی (۱۴۰۱) در مطالعه دیگری با عنوان «شناسایی و معرفی ظرفیت‌های کاربردی هوش مصنوعی در توسعه مضمون‌های راهبردی در سازمان‌های نظامی» با ارائه الگویی کاربردهای فناوری هوش مصنوعی در حوزه نظامی را بدین شرح احصا کرده است: ۱. پلتفرم جنگ‌افزارها؛ ۲. امنیت سایبری؛ ۳. لجستیک و حمل‌ونقل؛ ۴. سلامت میدان نبرد؛ ۵. شبیه‌سازی و آموزش؛ ۶. برنامه‌ریزی و تخصیص منابع؛ ۷. آگاهی محیطی و رصد تهدید؛ ۸. پردازش اطلاعات.

شاد دل (۱۴۰۲) در پژوهش خود «آینده مدیریت و تصمیم‌گیری با استقرار سامانه‌های هوش مصنوعی» نشان داده که فواید استفاده از هوش مصنوعی در زمینه مدیریت و تصمیم‌گیری عبارت است از: تسریع در جمع‌آوری داده‌های حجیم و پیچیده، تواناسازی سازمان‌ها به اتخاذ تصمیماتی آگاهانه، خودکارسازی فرایندهای تصمیم‌گیری معمول و ... .

خزایی و همکاران (۱۴۰۳) در مطالعه‌ای با عنوان «ارائه مدل ارتقای قدرت عملیاتی تهاجم هوایی بر پایه حوزه‌های اثرگذار علوم و فناوری کوانتومی» تأثیر علوم و فناوری کوانتومی را در سه حوزه عمده: ۱. رایانه‌های کوانتومی، رایانش و شبیه‌سازی کوانتومی، ۲. ارتباطات و

شبکه‌های کوانتومی و ۳. سنجش کوانتومی مورد تجزیه‌وتحلیل قرار داده‌اند. نتایج آن‌ها نشان‌دهنده تبیین سه حوزه هم‌پوشانی گسترده فناوری کوانتومی نظامی در میان کشورهای پیشرو در سطح جهان بوده که مرتبط با مؤلفه عملیاتی تهاجم قدرت هوایی هستند و همچنین شامل تدوین دستاوردهای قابل پیش‌بینی فناوری کوانتومی و تأثیرات آن در حوزه عملیاتی تهاجم هوایی نهاجا است.

(Ahmed, 2022) در مطالعه‌ای با عنوان «ادغام یادگیری ماشینی در فرایند اطلاعات نظامی: مطالعه رویکردهای آینده‌نگرانه به سمت همکاری انسان و ماشین» نشان می‌دهد که تحلیل و ادغام داده می‌توانند در چهارچوب چهار مرحله ۱. منابع جمع‌آوری داده‌ها؛ ۲. ذخیره‌سازی و پردازش؛ ۳. ادغام و پروفایل‌سازی و ۴. اشتراک داده‌ها؛ با استفاده از شبکه ابری نظامی و اینترنت اشیا انجام شود. همچنین، در سطح سازمان‌ها و واحدهای جمع‌آوری اطلاعات عملیاتی و تاکتیکی و در سطح تحلیل‌های اطلاعاتی مختلف، مراحل جمع‌آوری و تحلیل داده‌ها می‌توانند از طریق ادغام سیستم‌های مبتنی بر هوش مصنوعی خودکار شوند و کارایی عملیات اطلاعاتی را بهبود بخشند.

(Ish et.al, 2021) در مطالعه‌ای با عنوان «ارزیابی اثربخشی سیستم‌های هوش مصنوعی در تحلیل اطلاعات» با «شناسایی معیارها»[1] (یا به‌عبارت‌دیگر، «شاخص‌های عملکرد»[2]) برای سیستم‌های هوش مصنوعی که با مأموریت اطلاعاتی سازگار باشند تمرکز کرده و به توسعه یک روش‌شناسی برای ارزیابی تأثیری که یک سیستم هوش مصنوعی بر مأموریت اطلاعاتی خواهد داشت می‌پردازند و آن تأثیرات را به ویژگی‌های خود سیستم نسبت می‌دهند.

در پژوهشی با عنوان «تعیین اولویت برای به‌کارگیری فناوری هوش مصنوعی در حوزه‌های اطلاعات نظامی» توسط (Cho et.al, 2020)، نتیجه‌گیری شده که با توجه به پنج مرحله گردش اطلاعات (طرح‌ریزی، جمع‌آوری، پردازش، تجزیه‌وتحلیل و انتشار) در سرویس‌های اطلاعات نظامی، «مرحله پردازش» دارای بالاترین اولویت در به‌کارگیری فناوری

1. Identifying metrics
2. Measures of performance

هوش مصنوعی در حوزه‌های اطلاعاتی است. مرحله پردازش از نظر در دسترس بودن و خوانایی داده‌ها نسبت به سایر مراحل رتبه بالاتر و الزامات روشن و ساده‌ای داشت.

(Cornelis, 2023) در مقاله خود «رمزگشایی از پیوند کوانتومی–سیگینت: بررسی جامع اطلاعات سیگنالی در عصر رایانش کوانتومی» به بررسی و تحول قریب‌الوقوع اطلاعات سیگنالی تحت تأثیر رایانش کوانتومی پرداخته است. بررسی‌های محقق نشان می‌دهد که سازوکارهای اطلاعات سیگنالی توسط الگوریتم‌های کوانتومی با ایجاد اشکال جدید ارتباطات امن و روش‌های نوین تحلیل داده ممکن است به خطر بیفتند یا منسوخ شوند و این مهم نیازمند بازنگری راهبردی و بنیادین در شیوهٔ انجام عملیات اطلاعات سیگنالی است.

با بررسی و جمع‌بندی مطالعات انجام‌شده مشابه بر روی موضوع پژوهش حاضر، مشاهده می‌شود که بر روی کاربرد فناوری‌های نوظهور به‌ویژه هوش مصنوعی در حوزه کلی اطلاعات پژوهش‌هایی صورت گرفته ولی مطالعه‌ای به‌صورت ویژه بر روی کاربرد انواع فناوری‌های نوظهور در حوزه تخصصی سیگینت با رویکرد امنیت سایبری انجام‌نشده است. ازاین‌رو، مهم‌ترین نوآوری این مقاله همین مورد است که در ادامه به آن پرداخته خواهد شد.

۲. مفهوم‌شناسی

۲-۱. اطلاعات سیگنالی

اطلاعات سیگنالی (سیگینت) دسته‌ای از اطلاعات بوده که به‌طور جداگانه یا ترکیبی از اطلاعات ارتباطی (کامینت)[1]، اطلاعات الکترونیکی (الینت)[2] و اطلاعات سیگنال‌های ابزار خارجی (فیسینت)[3] تعریف می‌شود. به‌بیان‌دیگر، سیگینت به اطلاعات شنود شده از ارتباطات، سیگنال‌های الکترونیکی راداری و یا سیگنال‌های ابزار خارجی اشاره دارد.

براساس جمع‌آوری و تحلیل سیگنال‌های مورد نظر، هدف نهایی عملیات سیگینت، ارائه اطلاعات حیاتی رهگیری شده از سیگنال‌های هدف به تصمیم‌گیران و مصرف‌کنندگان

1. Communications Intelligence (COMINT)
2. Electronic Intelligence (ELINT)
3. Foreign Instrumentation signals intelligence (FISINT)

اطلاعات در تمامی سطوح است. تحلیلگران، محصولات و گزارش‌های سیگینت را با سایر منابع اطلاعاتی تلفیق کرده تا درک بهتری از محیط به دست آورند (Boudreaux, 2023).

اطلاعات ارتباطی (کامینت) از ارتباطات الکترومغناطیسی و سیستم‌های ارتباطی توسط افرادی غیر از گیرندگان یا کاربران موردنظر به‌دست می‌آید. چنین اطلاعاتی ممکن است به شکل کلامی از طریق دریافت پیام‌های رادیویی پخش‌شده، رهگیری ارتباطات «نقطه‌به‌نقطه»[1] مانند تلفن‌ها و لینک‌های رله رادیویی، یا به‌صورت داده از طریق رهگیری لینک‌های «داده پخش‌شده»[2] یا نقطه‌به‌نقطه جمع‌آوری شود.

اطلاعات الکترونیکی (الینت) از ارزیابی فنی انتشارات الکترومغناطیسی غیرارتباطی، مانند انتشارات تولیدشده توسط رادارها و سیستم‌های هدایت موشک، به‌دست می‌آید. همچنین شامل لیزرها، دستگاه‌های مادون‌قرمز و هر تجهیزات دیگری که انتشاراتی در طیف الکترومغناطیسی دارند شامل می‌شود. با مقایسه اطلاعات پارامترهای انتشار رهگیری‌شده با مشخصات تجهیزات موجود در پایگاه‌های داده، می‌توان اطلاعات ارزشمندی درباره تجهیزات و اپراتور آن‌ها به‌دست آورد (Joint Doctrine, 2023).

۲-۲. چرخه فرایند اطلاعات

در مراجع و نشریات منتشره معمولاً فرایند اطلاعات را در مراحل مختلف چهار تا شش مرحله‌ای تعریف می‌کنند. در این پژوهش چرخه اطلاعاتی شامل شش مرحله ۱. برنامه‌ریزی و هدایت؛ ۲. جمع‌آوری؛ ۳. پردازش و بهره‌برداری؛ ۴. تجزیه‌وتحلیل و تولید؛ ۵. انتشار و یکپارچگی و ۶. ارزیابی و بازخورد تعریف می‌شود. این مراحل را در شکل (۱) می‌توان مشاهده کرد:

1. Point-to-point
2. Broadcast

شکل ۱: چرخه فرایند اطلاعات سیگنالی (Boudreaux, 2023)

۲-۳. چالش‌های حوزهٔ اطلاعات سیگنالی

با رشد نمایی اطلاعات در عصر حاضر، حفظ پوشش سیستم سیگینت در سطح جهان دشوارتر شده و از طرفی چالش‌های متعددی در حوزه‌های فنی، راهبردی، فنی، فناوری‌های نوظهور، جغرافیایی و محیطی، عوامل انسانی و تجهیزات و سامانه‌ها پیشِ‌روی اطلاعات سیگنالی است. طیِ مطالعات انجام‌شده در این پژوهش از منابع مختلف کتابخانه‌ای برخی از این چالش‌ها احصا شده و با دسته‌بندی آن‌ها به‌صورت عمده و زیرچالش، مطابق جدول (۱) تشریح می‌شود:

جدول ۱: چالش‌های حوزه اطلاعات سیگنالی

چالش عمده	زیرچالش	منابع
راهبردی	❖ افزایش خبرگی کشورها و بازیگران غیردولتی متخاصم در مقابله با روش‌های سنتی سیگینت ❖ ادغام اطلاعات سیگنالی با سایر شکل‌های اطلاعات مانند انسانی و جغرافیایی ❖ زمان‌بر بودن و نیاز به منابع مالی زیاد (پرهزینه‌ترین رشته اطلاعاتی) ❖ اشتراک‌گذاری اطلاعات، اتصال میان بخش‌ها و سازمان‌های مختلف اطلاعاتی	(Hayden, 2014) (The Intelligence Community, 1996).

چالش عمده	زیرچالش	منابع
	❖ عدم گزارش داده‌ها و اطلاعاتی که به نظر سازمان سیگینت دارای ارزش اطلاعاتی نیست	
فنی	❖ افزایش میزان و پیچیدگی رمزنگاری ❖ به‌روزرسانی مستمر ابزارها و تکنیک‌ها جهت جمع‌آوری اطلاعات ❖ ذخیره‌سازی و پردازش حجم عظیم داده‌ها ❖ گسترش کانال‌های ارتباطی رمزگذاری شده ❖ ایجاد الگوهای پیچیده تداخل با انواع مدولاسیون‌ها و روش‌های متنوع انتقال ❖ فیلتر کردن حجم عظیم داده‌ها و استخراج اطلاعات از لایه‌های فرم‌بندی، تسهیم، فشرده‌سازی و پروتکل‌های انتقال ❖ رمزگشایی فرمت‌های مختلف سیگنال ❖ تکامل مداوم سیستم‌های ذخیره‌سازی داده و تحلیل بلادرنگ ❖ سیستم‌ها و روش‌های پیشرفته جهت مدیریت، ذخیره‌سازی و تحلیل حجم انبوه اطلاعات ❖ یکپارچه‌سازی داده‌های مختلف برای ارزیابی ❖ امنیت داده‌ها و اطلاعات حساس ❖ کشف اهداف در حالتی که سیستم راداری آن‌ها خاموش باشد.	
فناوری‌های نوظهور	❖ سوگیری الگوریتمی و امنیت داده‌ها با ادغام فناوری‌های پیشرفته مانند هوش مصنوعی و یادگیری ماشینی ❖ رایانش کوانتومی برای روش‌های رمزگذاری موجود، امنیت سایبری و حفاظت از اطلاعات حساس ❖ ارتباطات کوانتومی با ماهواره‌های کوانتومی و عدم توانایی رمزشکنی توسط سامانه‌های سیگینت ❖ افزایش حجم سیگنال‌ها با گسترش اینترنت اشیا و 5G ❖ تشخیص تهدید در حوزه سایبری	(Jagannath et.al, 2019)
جغرافیایی و محیطی	❖ عدم بازدهی مناسب با وجود ویژگی‌های طبیعی و عوارض زمین مانند کوه‌ها، جنگل‌های انبوه و ساختارهای شهری ❖ شرایط جوی مانند باران شدید، مه یا طوفان‌های شن ❖ مکان‌های دورافتاده یا ناامن	(گودرزی، ۱۳۹۲) و (شاه‌رضائی، ۱۴۰۱)
عوامل انسانی	❖ وابسته به نیروی انسانی متخصص و تحلیلگران ماهر و باتجربه ❖ دانش علمی بالا و دوره‌های تخصصی گسترده ❖ آموزش محدود و ناکافی ❖ اضافه‌بار شناختی (اشتباهات احتمالی در تفسیر و تصمیم‌گیری)	

چالش عمده	زیرچالش	منابع
	❖ عدم ارتباط و همکاری بین‌رشته و حوزه‌های مختلف	
تجهیزات و سامانه‌ها	❖ تحریم تجهیزات و سامانه‌های سیگینت توسط استکبار جهانی ❖ تعمیر و نگهداری سامانه‌های پیشرفته و پیچیده سیگینت ❖ به‌روزرسانی مداوم سامانه‌های سیگینت ❖ لزوم حداقل ۲ سامانه سیگینت به‌منظور مکان‌یابی اهداف ❖ هزینه زیاد مکان‌یابی، خرید، استقرار و راه‌اندازی تجهیزات سیگینت ❖ تعدد و تنوع نوع و مدل سامانه‌ها و تجهیزات با تأمین آن‌ها از داخل و خارج کشور	

۲-۴. به‌کارگیری فناوری هوش مصنوعی و یادگیری ماشینی در اطلاعات سیگنالی

روش‌های سنتی اطلاعات سیگنالی به‌شدت متکی بر تخصص انسانی و الگوریتم‌های مشخص برای شناسایی الگوها در سیگنال‌های رهگیری شده بودند. این سیستم‌ها اغلب در پردازش داده‌های مقیاس بزرگ یا شناسایی تهدیدات ناپیدا و در حال تکامل به‌صورت بلادرنگ با محدودیت‌هایی مواجه هستند.

هوش مصنوعی و به‌ویژه یادگیری ماشینی و یادگیری عمیق، پیشرفت‌های قابل‌توجهی در سیستم‌های اطلاعات سیگنالی ایجاد کرده است. با یادگیری از داده‌های تاریخی، مدل‌های هوش مصنوعی می‌توانند تهدیدات احتمالی را پیش‌بینی کرده و خود را با انواع جدید سیگنال‌ها تطبیق دهند. علاوه بر این، هوش مصنوعی قادر است وظایف پیچیده‌ای مانند طبقه‌بندی سیگنال‌ها، استخراج ویژگی‌ها و شناسایی ناهنجاری‌ها را به‌صورت خودکار انجام دهد.

سیستم‌های اطلاعات سیگنالی مبتنی بر هوش مصنوعی به‌طور گسترده‌ای برای نظارت بر ارتباطات شبکه‌ای به‌منظور شناسایی تهدیدات سایبری مورد استفاده قرار می‌گیرند. این سیستم‌ها ترافیک شبکه را تجزیه‌وتحلیل کرده و الگوهای غیرعادی را که ممکن است نشانه نفوذ، بدافزار یا جاسوسی سایبری باشند، شناسایی می‌کنند. شناسایی تهدیدات در محیط‌های نظامی به‌شدت به اطلاعات سیگنالی وابسته است تا ارتباطات دشمن، سیگنال‌های راداری و

سایر انتقالات الکترونیکی را رهگیری کند. سیستم‌های مبتنی بر هوش مصنوعی امکان شناسایی سریع فعالیت‌های خصمانه را فراهم کرده و به اجرای اقدامات متقابل کمک می‌کنند. اطلاعات سیگنالی مبتنی بر هوش مصنوعی به‌طور فزاینده‌ای در امنیت مرزی مورد استفاده قرار می‌گیرد تا انتقالات غیرمجاز از پهپادها، رادیوها یا شبکه‌های تلفن همراه را شناسایی کند. با خودکارسازی تجزیه‌وتحلیل سیگنال‌ها، فرماندهان می‌توانند تهدیدات امنیتی بالقوه را به‌سرعت شناسایی کرده و به آن‌ها واکنش مناسب نشان دهند (Kumari, 2024).

۲-۵. نقش فناوری‌های هوش مصنوعی در سازمان‌های اطلاعات سیگنالی و مراکز تحقیقاتی

آژانس امنیت ملی آمریکا: ازجمله اقدامات آژانس امنیت ملی آمریکا، اختراع، توسعه و به‌کارگیری پیشرفت‌ها در علم و فناوری‌های نوظهور جهت ارتقای مأموریت‌های اطلاعات سیگنالی و امنیت سایبری، قابلیت‌های اطلاعاتی و امنیت ملی ایالات متحده است و به‌عنوان یک آژانس پشتیبانی رزمی وزارت دفاع و عضو جامعه اطلاعاتی، هدف آن توسعه تکنیک‌ها و فناوری‌های جدید و نوآورانه برای پشتیبانی و فعال کردن مأموریت‌های اطلاعات سیگنالی و امنیت سایبری است. تحقیقات بنیادی آژانس در فناوری‌های زبان انسان و بینایی رایانه، تجزیه‌وتحلیل گراف در مقیاس بزرگ، تا تیم‌سازی انسان و ماشین با عوامل هوش مصنوعی را در برمی‌گیرد (Research Overview, 2025). این آژانس در حجم وسیعی از داده‌های اطلاعاتی سیگنالی که جمع‌آوری می‌کند برای درک بهتر و دیدن الگوها، غربالگری الگوهای ترافیک وب غیرمتعارف یا سایر داده‌هایی که می‌تواند حمله را به تصویر بکشد، از هوش مصنوعی استفاده می‌کند. انتظار این آژانس این است که هوش مصنوعی بار تحلیلگران را کاهش داده و ترجمه ماشین آنی و تشخیص گفتار به تحلیلگران کمک کند تا انواع مختلف داده‌های جمع‌آوری‌شده را بررسی، اطلاعات را تأیید و به نتایج محکم‌تری برسند (Tucker, 2020).

«آژانس اطلاعات سیگنالی بریتانیا»[1]: از نظر این آژانس افزایش استفاده از هوش مصنوعی برای انجام مأموریت خود در حفظ امنیت کشور اساسی است. هوش مصنوعی برای بهبود کارایی و اثربخشی و توانایی ما در مدیریت حجم و پیچیدگی فزاینده داده‌ها و توسعه قابلیت‌های لازم برای مقابله با تهدیدات مجهز به هوش مصنوعی توسط بازیگران مخرب حیاتی خواهد بود.

در آژانس، هوش مصنوعی برای توانمندسازی انسان‌ها در اتخاذ تصمیمات بهتر به‌کار گرفته‌شده و تلاش‌های ما بر توسعه سیستم‌های «هوش افزوده»[2] متمرکز خواهد بود، به‌طوری‌که هوش مصنوعی برای جمع‌آوری اطلاعات از منابع مرتبط و برجسته کردن داده‌های مهم برای بررسی تحلیلگران ما با هدف حمایت از فرایند تصمیم‌گیری مورد استفاده قرار می‌گیرد (Fleming, 2021).

مراکز تحقیقاتی: از نظر «اندیشکده دفاعی و امنیتی بریتانیا»[3] هوش مصنوعی پتانسیل بهبود بسیاری از جنبه‌های کار اطلاعاتی دارد. بهره‌برداری کامل از این فرصت‌ها مستلزم ایجاد فرایندهای استاندارد برای توسعه، آزمایش و ارزیابی ابزارهای جدید هوش مصنوعی در زمینه عملیاتی است. اولین مزیت استفاده از هوش مصنوعی برای جامعه اطلاعاتی بریتانیا توانایی خودکارسازی فرایندهای سازمانی، اداری و مدیریت داده‌ها خواهد بود وظایف تکراری که بخش قابل‌توجهی از حجم کاری سازمان را تشکیل می‌دهند. تحلیل اطلاعات با کمک هوش مصنوعی می‌تواند مزایای قابل‌توجهی در استخراج بینش از مجموعه داده‌های غیرساختاریافته و متنوع ارائه دهد و به‌این‌ترتیب کارایی جریان کار اطلاعاتی را بهبود داده و به کاهش میزان داده‌ها و محتوایی که باید توسط کارکنان بررسی شود، کمک کند. نمونه‌های تحلیل اطلاعات با کمک هوش مصنوعی به‌طور کلی به سه دسته تقسیم می‌شوند (Babuta, 2020):

- «خودکارسازی شناختی»[4] پردازش حسی انسانی به‌ویژه پردازش زبان طبیعی (NLP) و تحلیل صوتی–تصویری؛

1. Government Communications Headquarters (GCHQ)
2. Augmented intelligence (AuI)
3. Royal United Services Institute (RUSI)
4. Cognitive automation

- ❖ فیلتر کردن، علامت‌گذاری و اولویت‌بندی داده‌های به‌دست آمده از طریق جمع‌آوری انبوه، به‌عنوان بخشی از یک جریان کار تحلیلی تعامل انسان و ماشین؛
- ❖ تجزیه‌وتحلیل رفتاری برای استخراج بینش‌ها، کشف موضوعی خاص و پیش‌بینی اهداف طرف‌های مقابل.

استفاده مؤثر از تبدیل گفتار به متن می‌تواند به‌طور چشمگیری منابع انسانی مورد نیاز برای پردازش داده‌های صوتی (مانند محتوای رهگیری شده) را کاهش دهد. ترجمه ماشین نیز مزایای آشکاری را ارائه می‌دهد، چه برای متن رونویسی شده و چه به‌طور مستقیم برای داده‌های صوتی. علاوه بر این، شناسایی گوینده می‌تواند حجم زیادی از داده‌های صوتی را به‌طور مؤثرتری قابل جستجو کند. برای استخراج اطلاعات از داده‌های انبوه، هوش مصنوعی احتمالاً زمانی مفیدترین خواهد بود که به‌عنوان بخشی از یک جریان کار تحلیلی «تیم انسان–ماشین» تعاملی به کار گرفته شود (Babuta, 2020). فناوری‌های هوش مصنوعی و یادگیری ماشینی اغلب به‌عنوان آینده اطلاعات نیروی دریایی در نظر گرفته می‌شوند. به‌طور مشخص، این فناوری‌ها نه‌تنها سرعت تحلیل را افزایش می‌دهند، بلکه کیفیت بینش‌های به‌دست‌آمده از مجموعه داده‌های بزرگ را نیز عمیق‌تر می‌کنند. می‌توان به‌راحتی کاربردهای متعددی از هوش مصنوعی و یادگیری ماشینی را در اطلاعات نیروی دریایی در سطوح تاکتیکی، عملیاتی و راهبردی تصور کرد: شناسایی اولیه تهدیدها و هدایت عملیات بعدی از طریق اطلاعات سیگنالی یا اطلاعات الکترونیکی (الینت)، پیش‌بینی حرکات دشمن در جنگ ضد زیردریایی و بسیاری موارد دیگر (Dorton and Harper, 2021).

هوش مصنوعی نقش مهمی در تجزیه‌وتحلیل اطلاعات سیگنالی و شفافیت زیر مجموعه داده‌های اطلاعاتی بزرگ ایفا می‌کند. هوش مصنوعی و یادگیری ماشینی می‌توانند به‌طور مستقل سیگنال‌های حاوی اطلاعات دقیق و عمیق پنهان‌شده، روندها و فعالیت‌ها را شناسایی کنند. این فناوری زیرسیستم‌های پردازش سیگنال مرتبط‌تر با مأموریت را در سطح کد منبع و برای انواع سیگنال‌های پیچیده نوظهور نوید می‌دهد. همچنین، می‌تواند به اپراتور فنی و مهندس نرم‌افزار در توسعه ابزارهای جدیدی کمک کنند که طیف گسترده‌ای از شرایط در

حال تغییر را پیش‌بینی کرده و با آن سازگار شوند (Turner, 2024). سیستم‌های هوش مصنوعی نظامی می‌توانند داده‌های بیشتر و به‌طور مؤثرتر نسبت به سیستم‌های سنتی پردازش کنند. با توجه به قابلیت‌های رایانشی و تصمیم‌گیری ذاتی، هوش مصنوعی همچنین خودکنترلی، خودتنظیمی و خودگردانی سیستم‌های رزمی را افزایش می‌دهد (Rashid, 2023).

۲-۶. محصولات شرکت‌های سازنده سامانه اطلاعات سیگنالی با استفاده از فناوری هوش مصنوعی

درحال‌حاضر، شرکت‌های سازنده سامانه‌های اطلاعات سیگنالی (شامل سامانه‌های الینت و کامینت) در دنیا از فناوری‌های نوظهور به‌ویژه هوش مصنوعی استفاده بسیاری می‌کنند. طی جستجو در وب‌سایت‌ها، نشریات و کاتالوگ‌های منتشره توسط شرکت‌های سازنده عمده این سامانه‌ها در دنیا، مواردی گردآوری‌شده که در جدول (۲) به‌طور خلاصه اشاره می‌شود:

جدول ۲: برخی از محصولات شرکت‌های سازنده سیگنت مبتنی بر هوش مصنوعی

نام شرکت	محصول
شرکت «هنسولت»[1] صنایع دفاعی اروپا	سامانه «کالاترون انتگرال»[2] این شرکت با طراحی کاملاً رقمی، کارکرد چندین سیستم کامینت و الینت را به‌طور هم‌زمان دارد. این سیستم از الگوریتم‌های هوش مصنوعی برای شناسایی الگوهای تهدید جدید از میان حجم عظیمی از داده‌های خام جمع‌آوری‌شده استفاده می‌کند و طی مأموریت، ترتیب «الکترونیک میدان نبرد»[3] (EOB) را نمایش می‌دهد (Belz, 2025).
شرکت جنرال دینامیک	نرم‌افزار «سیگنال آی»[4] تشخیص، جداسازی و طبقه‌بندی سیگنال‌های «فرکانس رادیویی»[5] را با استفاده از فناوری پیشرفته یادگیری ماشینی خودکار می‌کند. داده‌های فرکانس رادیویی رهگیری شده را دریافت، سیگنال‌های موجود را شناسایی و ایزوله می‌کند. هر سیگنال را براساس نوع مدولاسیون طبقه‌بندی و سیگنال‌ها و ابرداده‌های شناسایی‌شده را برای بهره‌برداری بیشتر گزارش می‌دهد (Automatic Spectrum Situational, 2020).

1. HENSOLDT
2. Kalaetron Integral
3. Electronic Order of Battlefield
4. SignalEye
5. RF

نام شرکت	محصول
شرکت «بی‌آی‌ایی سیستمز»[1]	فناوری «چیمرا»[2] این شرکت مخفف «ادغام سخت‌افزار قابل‌کنترل برای سازگاری در زمان واقعی با یادگیری ماشینی» بوده و یک پلتفرم سخت‌افزاری قابل تنظیم مجدد است. این سیستم برای غربال کردن طیف فزاینده «فرکانس رادیویی»[3] شلوغ در میدان جنگ مناسب است
شرکت لاکهید مارتین	یک سیستم اطلاعات هوشمند، نظارت و شناسایی (ISR) خودکار را برای بهبود اثربخشی عملیاتی جنگنده در محیط‌های ارتباطی منع شده، ارائه کرده است. از طریق یک پاد توسعه‌یافته شرکت در یک جنگنده F-16 و با بهره‌گیری از قدرت هوش مصنوعی، این سیستم ISR خودکار می‌تواند موقعیت هدف را شناسایی کرده و تشخیص دهد، به‌طور خودکار به سمت هدف هدایت شود و تصویری را برای تأیید هدف در یک محیط شبیه‌سازی‌شده و بدون ارتباطات ضبط کند
شرکت «رود اند شوارتز»[4]	سیستم R&S®CA210DNG، یک آشکارساز سیگنال در باند فرکانسی HF مبتنی بر یادگیری عمیق با هوش مصنوعی یکپارچه برای کامینت خودکار است. که از فناوری هوش مصنوعی نسل بعدی برای گسترش قابلیت‌های نرم‌افزار پردازش خودکار و تحلیل سیگنال استفاده می‌کند. این سیستم به‌طور خودکار بیشتر وظایف تکراری کامینت را انجام می‌دهد تا تحلیلگران بتوانند بر روی کارهای مهم اطلاعاتی تمرکز کنند (Rohde & Schwarz meets current, 2023)
شرکت ان.آی	با استفاده از ترکیبی از سخت‌افزار پهن باند و پردازنده‌های قدرتمند، «رادیوهای تعریف‌شده نرم‌افزاری»[5] سکویی ایدئال برای کاربردهای اطلاعات سیگنالی ارائه کرده است. با استفاده از تکنیک‌های هوش مصنوعی و یادگیری عمیق می‌توانند یک سیستم را برای شناسایی سیگنال‌ها سریع‌تر از الگوریتم‌های کدنویسی شده دستی آموزش دهند. این سیستم‌ها می‌توانند شناسایی، طبقه‌بندی و عملکرد کلی سیگنال را در محیط‌های RF پیچیده و رقابتی افزایش دهند (Artificial Intelligence in Software-Defined, 202).
شرکت «ساب»[6]	سامانه کامینت شرکت ساب، تعادل مناسبی بین نظارت خودکار و کنترل شده توسط اپراتور برقرار کرده و امکان نظارت با استفاده از حسگرهای خودکار شبکه‌ای را در هر پلتفرم متحرک یا ثابت فراهم می‌آورد. هدف به‌دست آوردن تصویری از طیف کامل رادیویی است. همه سیگنال‌ها در باند درخواستی شناسایی، مکان‌یابی،

1. BAE Systems
2. Chimera
3. RF
4. Rohde & Schwarz
5. Software defined radios
6. Saab

نام شرکت	محصول
	طبقه‌بندی، دمدولاسیون و رمزگشایی می‌شوند. هر جا که ممکن باشد، این کارها به‌صورت خودکار انجام می‌شوند.
شرکت «وویجراسپیس»[1]	سیستم‌های اطلاعات سیگنالی این شرکت می‌توانند اطلاعات «بلادرنگ»[2] را در موقعیت‌های پیچیده فراهم می‌کند. از الگوریتم‌های تحلیلی یادگیری ماشینی و فناوری پیشرفته تجسم داده‌ها استفاده می‌شود. سیستم چندکاربره و چند پلتفرمی «تالیکس»[3] برای برنامه‌ریزی وظایف، جمع‌آوری، پردازش، بهره‌برداری و توزیع (TCPED) است که از چرخه‌های مأموریتی اطلاعات ارتباطی (کامینت) و اطلاعات الکترونیکی (الینت) پشتیبانی می‌کند. رویکرد این شرکت در استفاده از سیستم‌های «معماری باز»[4] (OA) با بهره‌گیری از چهارچوب‌های نرم‌افزاری باز و استانداردهای فناوری است. این رویکرد مزایای چشمگیری دارد: استقرار سریع، یکنواختی در سیستم‌های متعدد و کاهش هزینه‌های توسعه و استقرار. رویکرد معماری باز در راستای توسعه چابک بوده که منجر به تسریع در تحویل و تسهیل در ادغام فناوری‌های جدید می‌شود. فناوری‌های معماری باز مانند «سیستم‌های مأموریتی باز»[5] (OMS)، چهارچوب‌های REDHAWK/TOA و RAPTORX و استانداردهایی مانند «معماری سیستم‌های باز حسگر»[6] (SOSA)، «معماری RF باز ماژولار»[7] (MORA) و «رویکرد سیستم‌های باز ماژولار»[8] (MOSA) است (Signals Intelligence, 2025).

۲-۷. به‌کارگیری سایر فناوری‌های نوظهور در اطلاعات سیگنالی

سازمان‌های اطلاعاتی و شرکت‌های فعال در حوزه سیگنت به‌جز فناوری هوش مصنوعی از سایر فناوری‌های نوظهور دیگر مانند فناوری‌های رایانش ابری، رایانش کوانتومی بهره‌برداری می‌کنند. در این رابطه طی مطالعات صورت گرفته مواردی به‌شرح جدول (۳) آورده شده است:

1. Voyager Space
2. Real-time
3. TALIX
4. Open architecture
5. Open Mission Systems
6. Sensor Open Systems Architecture
7. Modular Open RF Architecture
8. Modular Open Systems Approach

جدول ۳: به‌کارگیری فناوری‌های نوظهور در سیگینت

فناوری	توضیح
فناوری پردازش زبان طبیعی	فناوری «گفتار به متن»[1]، ترجمه، پردازش زبان طبیعی و تجزیه‌وتحلیل شبکه سیستم جهت استخراج بینش معنادار از حجم عظیم داده‌ها استفاده می‌شود تا نیاز تحلیلگران را به تسلط بر زبان‌های خارجی را کاهش دهد (Kumari, 2024). تحلیلگران اطلاعاتی با پردازش زبان طبیعی می‌توانند انبوهی از متن و اطلاعات که در مقابلشان قرار دارد را با دقت و سرعت بیشتر پردازش و تجزیه‌وتحلیل کرده و نیز پردازش میلیاردها کلمه در ثانیه «غربال، مرتب‌سازی، ترجمه و درک همه این داده‌ها» را خودکار کند آژانس امنیت ملی آمریکا در ۱۰ سال گذشته بر توسعه پردازش زبان طبیعی و بینایی رایانه‌ای جهت فهم زبان انسان توسط رایانه متمرکز بوده است تا با استفاده از قابلیت‌هایی مانند رونویسی ماشینی، ترجمه ماشینی و غیره مأموریت اصلی خود را انجام دهد. همچنین، فرایند «اولویت‌بندی و دسته‌بندی»[2] امنیت سایبری این آژانس یکی از حوزه‌های تمرکزی است که تحت تأثیر پردازش زبان طبیعی قرارگرفته است (Artificial Intelligence, 2021).
رایانش ابری	یک سرویس ابر رزمی-تاکتیکی کاملاً کاربردی، کاملاً مجازی و خودترمیم‌شونده، پایه و اساس سیستم‌های اطلاعاتی نسل بعدی است. انتقال اطلاعات به یک زیرساخت ابری رزمی، مزایای عملیاتی عظیمی را به‌صورت بلادرنگ برای عملیات مشترک فراهم می‌کند. نسل بعدی سیستم‌های اطلاعاتی باید مبتنی بر سرورهای شبکه پیشرفته باشند تا هم دسترسی بالا را فراهم کنند و هم رویکردهای جدیدی را برای کنترل و تأمین سیستم‌های شبکه با ارائه کامل «مجازی‌سازی عملکرد شبکه»[3] (NFV) فعال کنند (The Internet of Things, 2015).
	شرکت «نورث گرومن»[4]، یک معماری اطلاعات سیگنالی نسل بعدی به‌نام «سیج»[5] طراحی کرده است. سیج یک معماری باز مبتنی بر ابر، پلتفرم-آگنوستیک شامل فرستنده-گیرنده و میکروسرویس‌ها است که به‌عنوان یک حسگر جامع عمل می‌کند. سیج گیرنده‌ها-فرستنده‌های جدید توسعه‌یافته دارای قدرت رایانشی بسیار بیشتری هستند که به نیروهای نظامی امکان جمع‌آوری طیف وسیع‌تری از سیگنال‌های پیشرفته دشمن را می‌دهد (Signals Intelligence Global Market Report, 2025).

1. Speech to Text (STT)
2. Triage
3. Network function virtualization
4. Northrop Grumman
5. SAGE

فناوری	توضیح
	آمازون وب سرویسز (AWS) در سال ۲۰۲۲ قراردادی به ارزش ۱۰ میلیارد دلار با آژانس امنیت ملی آمریکا منعقد کرده است. این قرارداد با نام رمز «وحشی و طوفانی»[1] شناخته می‌شود. که شامل خدمات ابری است و از برنامه ابتکار رایانش ترکیبی (رایانش با ترکیبی از رایانه‌های کوانتومی و کلاسیک) پشتیبانی می‌کند. آمازون وب سرویسز به‌عنوان ارائه‌دهنده خدمات ابری به انتقال داده‌ها و اطلاعات نظارتی آژانس در سطح جهان از سرورهای داخلی به ابر کمک خواهد کرد (موسسه تحقیقاتی و تحلیلی Futurum) (Kramer, 2022).
	«خدمات وب آمازون»[2] با طیف گسترده‌ای از خدمات و محصولات ابری ایمن و مقیاس‌پذیر و با بالاترین حفاظت از جامعه اطلاعاتی ایالات متحده پشتیبانی کرده و کمک می‌کند تا قابلیت‌های جدید را کشف و فناوری‌های نوظهوری مانند هوش مصنوعی و یادگیری ماشینی را برای بهبود موفقیت در مأموریت پیاده‌سازی کنند و باعث حفظ مزیت فناوری کشور شود. این شرکت اخیراً دومین منطقه فوق سری به‌نام AWS Top Secret-West برای اجرای اقدامات کاری در سطح طبقه‌بندی امنیتی فوق سری ایالات متحده راه‌اندازی کرده است (Cloud Computing, 2025).
رایانش کوانتومی	رایانش کوانتومی با الگوریتم‌هایی مانند «شور»[3] فرصتی برای سیگینت است زیرا می‌تواند تکنیک‌های رمزنگاری را که برای دهه‌ها بستر ارتباطات امن بوده‌اند، بشکند و با حل مسائل پیچیده و با سرعت‌هایی که تاکنون غیرقابل‌تصور بود، می‌تواند راه‌های جدیدی را در تجزیه‌وتحلیل داده‌ها و جمع‌آوری اطلاعات باز کند.
فناوری 5G	در «فرماندهی و کنترل مشترک در تمام حوزه‌ها»[4] (JADC2) وزارت دفاع آمریکا تشریح شده که هدف آن اتصال حسگرهای تمام شاخه‌های نظامی (نیروی هوایی، نیروی زمینی، نیروی دریایی، سپاه تفنگداران دریایی و نیروی فضایی) به یک شبکه یکپارچه با استفاده از فناوری 5G است. قابلیت‌های آن، یکپارچگی در توسعه قابلیت‌ها، سیستم‌های انعطاف‌پذیر در محیط‌های مختل‌شده، اشتراک‌گذاری اطلاعات به‌صورت امن و چابک میان نیروها، شبکه‌ای متصل و قابل تعامل از حسگرها و مقیاس‌پذیر براساس نیازها و تقاضاهای آینده است (Hoehn, 2022)؛ (Cantrell, 2023).

1. Wild and Stormy
2. Amazon Web Services
3. Shor
4. Joint All-Domain Command and Control

فناوری	توضیح
رباتیک	پروژه «همگرایی»[1] در نیروی زمینی آمریکا با هدف ادغام هوش مصنوعی، رباتیک و خودمختاری طراحی‌شده تا آگاهی از موقعیت در میدان نبرد را بهبود داده، حسگرها را به سلاح‌ها متصل کرده و زمان‌بندی تصمیم‌گیری را تسریع بخشد (Cantrell, 2023).

۲-۸. رویکرد امنیت سایبری در حوزه سیگینت

الف. سرمایه‌های سایبری در سیگینت

سرمایه سایبری، هر موجودیت مشهود یا نامشهود برخوردار از ارزش برای یک سازمان است که ماشین‌آلات، تجهیزات و نرم‌افزار به‌عنوان مصادیق سرمایه مشهود و خدمات مبتنی بر شبکه، اطلاعات سازمانی، اعتبار، مهارت و دانش به‌عنوان مصادیق دارایی نامشهود است (Ross et.al, 2021). در تعریفی دیگر، بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم‌افزارها، اطلاعات و حتی افراد که در فرایند تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور نقش مستقیم و تعیین‌کننده داشته باشند، سرمایه سایبری نامیده می‌شود (سند راهبردی پدافند سایبری کشور، ۱۳۹۴). سازمان‌هایی که در حوزه اطلاعات سیگنالی فعالیت دارند در ایستگاه‌ها و مراکز جمع‌آوری و پردازش اطلاعات منطقه‌ای خود دارای انواع سامانه‌ها و تجهیزات متنوعی از الینت، کامینت، جهت‌یاب (جهت پردازش و ذخیره‌سازی انواع داده و اطلاعات) و ارتباطی و نیز انواع نرم‌افزارها و سیستم‌های عامل و اطلاعات و داده هستند که همه آن‌ها جزو سرمایه سایبری آن سازمان محسوب می‌شوند.

در جدول (۴) انواع سرمایه‌های سایبری در حوزه سیگینت مشاهده می‌شود:

جدول ۴: انواع سرمایه‌های سایبری سیگینت

نوع سرمایه	شرح
سخت‌افزار	انواع سامانه‌های الینت، کامینت، جهت‌یاب و ...
	تجهیزات فاوایی ازجمله سرور، سوئیچ، مودم و ...

1. Convergence

نوع سرمایه	شرح
نرم‌افزار	نرم‌افزارهای کاربردی سامانه‌ها و تجهیزات
	نرم‌افزارهای رایانه‌ای ازجمله انواع سیستم‌های عامل
داده و اطلاعات	داده و اطلاعاتی که در چرخه سیگینت جمع‌آوری، پردازش، تجزیه‌وتحلیل و منتشر می‌شوند.
کاربران	کلیه نفراتی که با نرم‌افزارها و سخت‌افزارهای چرخه سیگینت کار می‌کنند

ب. آسیب‌پذیری‌های سرمایه‌های سایبری سیگینت

به ضعف در یک سیستم اطلاعاتی، رویه‌های امنیتی سیستم، کنترل‌های داخلی یا پیاده‌سازی که می‌تواند توسط یک منبع تهدید مورد بهره‌برداری یا تحریک قرار گیرد آسیب‌پذیری گفته می‌شود. آسیب‌پذیری یک ویژگی داخلی سرمایه سایبری است و برای ترمیم یا رفع آن، باید از کنترل‌های امنیتی استفاده نمود (Ross, 2018).

به‌طور سالیانه آسیب‌پذیری‌های عمده امنیت سایبری توسط مراکز مختلف در دنیا معرفی می‌شوند. شرکت امنیت سایبری «بایت‌هاید»[1] ده نوع آسیب‌پذیری کلی در سال ۲۰۲۴ را بدین‌صورت برشمرده است (Top 10 Application, 2024): ۱. کنترل دسترسی ناقص؛ ۲. نقص رمزنگاری؛ ۳. تزریق کد یا دستور غیرمجاز؛ ۴. طراحی ناامن؛ ۵. پیکربندی نادرست امنیتی؛ ۶. قطعات آسیب‌پذیر و قدیمی؛ ۷. نقص‌های شناسایی و احراز هویت؛ ۸. نقص‌های یکپارچگی نرم‌افزار و داده؛ ۹. نقص‌های ثبت و نظارت امنیتی و ۱۰. جعل درخواست از سمت سرور.

در این رابطه، برخی از مهم‌ترین آسیب‌پذیری‌های سایبری حوزه سیگینت را می‌توان چنین مطرح نمود:

- ❖ آسیب‌پذیری‌هایی که در مراحل طراحی، ساخت و تولید سامانه اعم از تولید سخت‌افزار و نرم‌افزارها ایجاد شده‌اند و با عنوان نقص‌ها یا نقاط ضعف سامانه‌های سیگینت شناخته می‌شود؛
- ❖ آسیب‌پذیری‌های سهوی که در اثر بروز خطا یا اشتباه به وجود می‌آید.

1. Bytehide

- ❖ آسیب‌پذیری‌های ناشی از بهره‌برداری نادرست و یا عدم آگاهی کاربر نسبت به امکانات و قابلیت‌های سامانه و نرم‌افزارهای کاربردی آن؛
- ❖ آسیب‌پذیری‌هایی که از ارتباط ناامن شبکه ارتباطی سیگینت به وجود می‌آیند؛
- ❖ آسیب‌پذیری‌های عمدی با نیّت بدخواهانه که با هدف بهره‌برداری بعدی ایجاد می‌شوند.

پ. تهدیدات سایبری سیگینت

هر سرمایه سایبری، از یک یا چند آسیب‌پذیری سایبری برخوردار است و توسط یک یا چند تهدید امنیتی نیز مورد تهدید قرار می‌گیرد. تهدید سایبری به هرگونه پیشامد یا رویداد با پتانسیل ضربه متخاصمانه به عملیات سازمان، سرمایه‌ها، افراد، سازمان‌های دیگر یا کشور، با استفاده از یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء یا تغییر اطلاعات و یا ممانعت از سرویس گفته می‌شود (Dodson et.al, 2020) و نیز عامل داخلی یا بیرونی، که قابلیت و یا نیّت نقض خط‌مشی امنیتی یک سرمایه سایبری و یا ضربه به مؤلفه‌های امنیتی آن سرمایه را داشته باشد (خالقی دخت، ۱۴۰۰).

هفت تهدید اصلی امنیت سایبری توسط موسسه «انیسا»[1] در سال ۲۰۲۴ شناسایی‌شده بدین شرح است: ۱. باج‌افزار؛ ۲. بدافزار؛ ۳. مهندسی اجتماعی؛ ۴. تهدیدات علیه داده‌ها؛ ۵. تهدیدات علیه دسترس‌پذیری: انکار سرویس؛ ۶. دستکاری و مداخله در اطلاعات؛ ۷. حملات زنجیره تأمین (Lella, 2024).

در حوزه اطلاعات سیگنالی نیز می‌توان برخی تهدیدات سایبری را بدین شرح اشاره کرد:

۱. حمله به سامانه‌ها و تجهیزات سیگینت: این حملات ممکن است شامل تخریب و دستکاری نرم‌افزارهای کاربری سامانه‌ها و تجهیزات یا ایجاد اختلال در ارتباطات باشد.

۲. نفوذ به شبکه‌های ارتباطی سیگینت: هکرها ممکن است با نفوذ به شبکه‌های ارتباطی سیگینت به اطلاعات حساس دسترسی پیدا کرده، آن‌ها سرقت کرده یا تغییر دهند.

1. ENISA

۳. حملات جعل: حملات سایبری می‌توانند به‌منظور جعل یا فریب در اطلاعات سیگنالی صورت گیرند، به‌ویژه در شرایطی که اطلاعات تقلبی ارسال شوند و فرایند تجزیه‌وتحلیل اطلاعات را گمراه کنند.

۴. نشت اطلاعات: درصورتی‌که اطلاعات جمع‌آوری‌شده به‌طور غیرمجاز منتشر شوند یا به دست دشمنان یا گروه‌های غیرمجاز برسد، می‌تواند باعث بروز تهدیدات جدی در زمینه نظامی و امنیت ملی شود.

ت. الزامات امنیت سایبری سیگینت

به توانایی محافظت از یک سرمایه سایبری ازجمله پیشگیری از آسیب، حفاظت و بازیابی رایانه‌ها، سیستم‌ها و خدمات ارتباطات الکترونیکی، ارتباطات سیم‌دار و ارتباطات الکترونیکی، ازجمله اطلاعاتی که در آن‌ها موجود است، به‌منظور تضمین در دسترس بودن، یکپارچگی، احراز هویت، محرمانگی و عدم انکار آن «امنیت سایبری» گفته می‌شود (Bartock, 2021).

خالقی دخت (۱۴۰۰) الزامات امنیت سایبری را به‌صورت کلی تشریح نموده که در این پژوهش، محقق با استفاده از آن مطالب این الزامات را در حوزه سیگینت به شرح زیر بازتعریف می‌نماید:

۱. الزامات امنیت سخت‌افزار: در هنگام طراحی و معماری سامانه‌های سیگینت باید استانداردهای امنیت سخت‌افزار توسط شرکت‌های سازنده ازجمله محرمانگی تراشه‌های ذخیره‌ساز و پردازشی بکار رفته رعایت شود. همچنین، برای کنترل دسترسی به سامانه‌ها و تجهیزات نیاز است از تأیید هویت چندعاملی سخت‌افزاری استفاده‌شده و امنیت فیزیکی سخت‌افزار شامل دسترسی فیزیکی محدود، نگهداری در محیط‌های کنترل‌شده از نظر دما و رطوبت مدنظر باید باشد.

۲. الزامات امنیت نرم‌افزار: نرم‌افزارهای مورد استفاده در سیگینت شامل نرم‌افزارهای رایانه‌ای ازجمله سیستم‌عامل و نرم‌افزارهای کاربردی ویژه سامانه‌های سیگینت برای جمع‌آوری و پردازش اطلاعات است. امنیت نرم‌افزارها شامل دو بخش است. بخش اول

امنیت خود نرم‌افزارها است که باید توسط تولیدکننده آن تأمین شود و بخش دوم، امنیت نصب، پیکربندی و بهره‌برداری از نرم‌افزارها است که بر عهده کاربر سامانه است و باعث می‌شود تنظیمات یا بهره‌برداری به‌گونه‌ای انجام شود که امکان سوءاستفاده از برنامه توسط هکر محلی یا از راه‌دور، امکان‌پذیر نباشد.

استفاده از چهارچوب‌های امن کدنویسی مطابق با استانداردها، به‌روزرسانی‌های امنیتی، تست نفوذ، روش‌های احراز هویت قوی، بررسی نقش‌ها و مجوزهای دسترسی، ثبت و نظارت دسترسی به اطلاعات، حفاظت از یکپارچگی داده‌ها ضرورت دارد.

۳. الزامات امنیت اطلاعات: اطلاعات مهم‌ترین و با ارزش‌ترین بخش از دارایی سازمان است. محرمانگی، صحت و دسترس‌پذیری اطلاعات باید تأمین شود. هرگونه دسترسی به اطلاعات باید پس از احراز هویت و با اعمال مکانیسم‌های کنترل دسترسی انجام گیرد تا امکان انکار عملکرد از بین برود.

طبقه‌بندی اطلاعات سیگنالی براساس حساسیت (عادی، محرمانه، خیلی محرمانه و ...)، اعمال اصل حداقل دسترسی و اصل نیاز به دانستن برای محدود کردن دسترسی کاربران، ذخیره‌سازی اطلاعات حساس در محیط‌های ایزوله و با کنترل دسترسی قوی، تعریف خط‌مشی‌های مدیریت چرخه حیات اطلاعات برای تعیین زمان نگهداری و حذف اطلاعات حساس، اطمینان از انهدام فیزیکی رسانه‌های ذخیره‌سازی حاوی داده‌های حساس پس از پایان عمر مفید آن‌ها، استفاده از روش‌های حذف امن داده‌ها برای جلوگیری از بازیابی اطلاعات، پشتیبان‌گیری منظم از اطلاعات حساس جزو الزامات امنیت سایبری اطلاعات سیگنالی هستند.

۴. الزامات امنیت ارتباطات: ارتباطات در حوزه اطلاعات سیگنالی شامل انتقال داده‌های حساس در محیط‌های مختلف (شبکه‌های باسیم، بی‌سیم، ماهواره‌ای و رادیویی) است. به دلیل ماهیت حساس این اطلاعات، الزامات امنیتی ویژه‌ای برای محافظت از محرمانگی، یکپارچگی و در دسترس بودن ارتباطات باید رعایت شود.

استفاده از پروتکل‌های امنیتی پیشرفته و الگوریتم‌های رمزنگاری قوی برای انتقال اطلاعات و اطمینان از به‌روز بودن آن‌ها برای محافظت در برابر شنود و دستکاری، پیاده‌سازی یک سیستم مدیریت کلید امن برای تولید، توزیع و ذخیره کلیدهای رمزنگاری، ثبت تمام فعالیت‌های مربوط به ارتباطات، احراز هویت متقابل برای اطمینان از صحت فرستنده و گیرنده اطلاعات، پیکربندی صحیح تجهیزات شبکه‌ای، رعایت استانداردهای بین‌المللی امنیت شبکه‌ها و کنترل‌های امنیت سایبری ارتباطات می‌تواند در امنیت سایبری ارتباطات در حوزه سیگینت مؤثر باشند.

۳. روش‌شناسی پژوهش

از آن‌جایی‌که در این پژوهش به‌منظور چیستی و چگونگی وضع موجود بررسی و واقعیت‌ها و شرایط و چالش‌های موجود توصیف‌شده، روش پژوهش توصیفی و رویکرد پژوهش کیفی است. به‌طوری‌که در بخش مبانی نظری در مرحله اول با روش گردآوری داده‌ها از رویکرد «مرور ادبیات سیستماتیک»[1] جهت استخراج مدل اولیه استفاده‌شده است، بدین منظور، از طریق مطالعات کتابخانه‌ای با روشی نظام‌مند در پایگاه‌های علمی مختلف منابع موجود با کلیدواژه‌های مدنظر شناسایی، طبقه‌بندی و تلخیص شده و در صورت مغایرت با ادبیات موردنیاز پژوهش حذف شدند.

سپس با مبنا قرار دادن یافته‌های مرحله اول، مرحله دوم با روش نمونه‌گیری «گلوله برفی»[2] و طراحی سؤالات از پیش تعیین‌شده، مصاحبه‌های نیمه ساختاریافته با ده نفر از خبرگانی که از مسئولین باتجربه در حوزه اطلاعات سیگنالی و امنیت سایبری بودند، انجام و سپس با تحلیل مضمون مقولات اصلی از میان پاسخ‌ها استخراج شد. همچنین برای اطمینان از مناسب‌بودن مراحل و منطق روش پژوهش در پایان مصاحبه‌ها، در خصوص ارزیابی و میزان کارآمدی روش پژوهش از کلیه خبرگان پرسش شد، ارزیابی‌های انجام‌شده نشان داد که رویکرد به‌کاررفته با توجه به تناسب روش مورد تأیید است.

1. Systematic Literature Review (SLR)
2. Snowball

در ابتدای مصاحبه از مصاحبه‌شوندگان سؤال‌های مربوط به سن، سابقه‌کاری، میزان تحصیلات و تخصص در سازمان‌های نظامی پرسیده شد که نتایج به شرح جدول (۵) است:

جدول ۵: مشخصات مصاحبه‌شوندگان

سن	۴۵-۵۰	۵۰-۵۵	>۵۵
	۴	۵	۱
سابقه کار	۲۵-۳۰	۳۰-۳۵	>۳۰
	۲	۵	۳
میزان تحصیلات	کارشناسی ارشد		دکترا
	۷		۳
تخصص	اطلاعات سیگنالی		امنیت سایبری
	۸		۲

۴. تجزیه‌وتحلیل یافته‌ها

در این بخش به‌منظور تکمیل نتایج حاصل از مبانی نظری پژوهش با ده نفر از صاحب‌نظران حوزه اطلاعات سیگنالی مصاحبه و از آن‌ها خواسته شد تا در خصوص به‌کارگیری از فناوری‌های نوظهور در حوزه اطلاعات سیگنالی نظر خود را مطرح نمایند. خلاصه مطالب حاصل از مصاحبه‌ها در جدول (۶) تشریح شده است:

جدول ۶: نظرات خبرگان در خصوص به‌کارگیری فناوری‌های نوظهور در سیگینت

شماره خبره	خلاصه نظرات خبرگان	فناوری‌های مورد استفاده
P1	- فرایند خودکارسازی عملیات جمع‌آوری اطلاعات سیگنالی- نیروی انسانی ایده‌ها، تفکرات و خلاقیت‌ها را از طریق یاددهی ماشین به سیستم هوشمند تزریق نموده تا سیستم هوشمند جمع‌آوری اطلاعات سیگنالی را برابر تفکرات نیروی انسانی انجام دهد - تکمیل داده‌ها، پیش‌بینی روندها و بهبود فرایند با استفاده از الگوریتم‌های هوش مصنوعی، اینترنت اشیا	- خودکارسازی عملیات جمع‌آوری اطلاعات سیگنالی - الگوریتم‌های هوش مصنوعی - اینترنت اشیا - کلان داده‌ها

شماره خبره	خلاصه نظرات خبرگان	فناوری‌های مورد استفاده
	و اتصال دستگاه‌ها به شبکه برای جمع‌آوری اطلاعات به‌صورت بلادرنگ - کلان داده‌ها (Big Data) برای مدیریت و تحلیل حجم وسیعی از داده‌ها برای استخراج اطلاعات مفید - پردازش ابری برای ذخیره‌سازی و پردازش داده‌ها-ایجاد شبکه‌های ارتباطی پرسرعت، پایدار و امن برای پشتیبانی از فناوری‌های هوشمند - این فضا امکان دسترسی به منابع رایانشی بزرگ و تحلیل داده‌های حجیم را فراهم می‌کند.	- پردازش ابری برای ذخیره‌سازی و پردازش داده‌ها - شبکه‌های ارتباطی پرسرعت، پایدار و امن
P2	- بهره‌مندی از پردازش با هوش مصنوعی با نظارت عامل انسانی و مبتنی بر رویه‌ها و دستورالعمل‌های جاری - زیرساخت و رویه‌های ارتباطی امن و پایدار - سامانه‌های جمع‌آوری اطلاعات با قابلیت دیجیتال - نرم‌افزارهای پردازش، تحلیل و انتشار هوشمند	- پردازش با هوش مصنوعی - زیرساخت و رویه‌های ارتباطی امن و پایدار - سامانه‌های جمع‌آوری اطلاعات با قابلیت دیجیتال - نرم‌افزارهای پردازش، تحلیل و انتشار هوشمند
P3	- استفاده از ابزارها و تکنیک‌های پیشرفته مانند هوش مصنوعی، اینترنت اشیا و داده‌های بزرگ برای جمع‌آوری و تجزیه‌وتحلیل و استفاده از اطلاعات - شبکه‌های ارتباطی پیشرفته امن و پایدار و مراکز داده قوی - استفاده از سنسورهای جمع‌آوری اطلاعات و سامانه‌های اطلاعاتی برای جمع‌آوری داده‌های خام از منابع مختلف - استفاده از پایگاه‌های داده و سیستم‌های مدیریت داده برای ذخیره‌سازی و سازمان‌دهی داده‌های جمع‌آوری شده-استفاده از تکنیک‌های تحلیل داده و هوش	- تکنیک‌های پیشرفته مانند هوش مصنوعی، اینترنت اشیا و داده‌های بزرگ - شبکه‌های ارتباطی پیشرفته امن و پایدار و مراکز داده قوی

شماره خبره	خلاصه نظرات خبرگان	فناوری‌های مورد استفاده
	مصنوعی برای استخراج الگوها و اطلاعات مفید از داده‌های خام - تصمیم‌گیری هوشمند: استفاده از نتایج تحلیل داده‌ها برای پشتیبانی از فرایندهای تصمیم‌گیری و بهبود کارایی و اثربخشی سازمان و مصرف‌کنندگان	
P4	- هوشمندسازی سیگینت با استفاده از داده‌های ورودی آن و یادگیری ماشینی جهت انجام یک فعالیت ویژه توسط الگوریتم‌های هوش مصنوعی - پردازشگرهای متناسب با عملکرد مورد انتظار، اینترنت اشیا - سخت‌افزارها و نرم‌افزارها جهت استفاده از سامانه‌های هوش مصنوعی	- هوشمندسازی سیگینت با استفاده از داده‌های ورودی آن و یادگیری ماشینی - الگوریتم‌های هوش مصنوعی - اینترنت اشیا
P5	- انتشار به‌موقع: با بهره‌گیری از شبکه‌های ارتباطی با حجم دیتای ارسالی مناسب و ایجاد سرویس‌های ابری و فراهم نمودن زمینه‌های مناسب در بهره‌گیری از لایه‌های ارتباطی چندگانه با امنیت سایبری مناسب - جمع‌آوری و پردازش هوشمند - سامانه‌های تلفیق و یکپارچه‌ساز اطلاعات (تجزیه‌وتحلیل هوشمند) - ایجاد بانک‌های اطلاعاتی جهت فراخوانی اطلاعات (ابر خصوصی سیگینت) - واحدسازی (یکسان‌سازی) اطلاعات - شبکه‌های ارتباطی امن و پایدار جهت تلفیق و یکپارچه سازی و انتشار به‌موقع اطلاعات	- سرویس‌های ابری - لایه‌های ارتباطی چندگانه با امنیت سایبری مناسب - جمع‌آوری و پردازش هوشمند - ابر خصوصی سیگینت - شبکه‌های ارتباطی امن و پایدار
P6	- بهره‌گیری از ابزارهای هوش مصنوعی، داده‌کاوی و سیستم‌های اطلاعاتی پیشرفته برای افزایش کارایی و دقت در شناسایی تهدیدات - فناوری‌های نوین ارتباطی و بی‌سیم: استفاده از فناوری‌ها برای جمع‌آوری و انتقال داده‌ها به‌صورت سریع و دقیق	- هوش مصنوعی و یادگیری ماشینی، داده‌کاوی - فناوری‌های نوین ارتباطی و بی‌سیم

شماره خبره	خلاصه نظرات خبرگان	فناوری‌های مورد استفاده
	- سیستم‌های مانیتورینگ هوشمند: ابزارهایی که شرایط محیطی و سیگنالی را به‌صورت لحظه‌ای پایش کرده و اطلاعات را برای تحلیل ارسال می‌کنند - داده‌کاوی و تحلیل داده‌ها: استفاده از الگوریتم‌های پیشرفته برای استخراج اطلاعات مفید از حجم عظیمی از داده‌های سیگنالی - هوش مصنوعی و یادگیری ماشینی: این فناوری‌ها می‌توانند در شناسایی الگوهای تهدید و پیش‌بینی رفتارهای دشمن نقش کلیدی داشته باشند	- سیستم‌های مانیتورینگ هوشمند
P7	- هشداردِهی با هوش مصنوعی در جهت تولید علائم و هشدار - فناوری‌های پیشرفته مانند پردازنده‌های سیگنال دیجیتال (DSP) و هوش مصنوعی می‌توانند سیگنال‌ها را با سرعت و دقت بیشتری پردازش کنند - با فناوری‌هایی مانند رمزنگاری کوانتومی و بلاکچین، می‌توان داده‌های حساس را به‌طور ایمن‌تر ذخیره و انتقال داد زیرا این فناوری‌ها در برابر تهدیدات سایبری پیشرفته‌تر مقاومت بیشتری دارند	- هشداردهی با هوش مصنوعی - پردازنده‌های سیگنال دیجیتال (DSP) - رمزنگاری کوانتومی و بلاکچین
P8	- فناوری‌های هوش مصنوعی و یادگیری ماشینی می‌توانند به تحلیل داده‌های سیگنالی به‌صورت خودکار کمک کرده و با شناسایی الگوهای پیچیده در داده‌ها، پیش‌بینی‌های دقیقی ارائه دهند - رایانش کوانتومی می‌تواند قدرت پردازش داده‌ها را به‌طور چشم‌گیری افزایش دهد - تحلیل کلان داده نیز می‌تواند به استخراج الگوها و اطلاعات ارزشمند از حجم بزرگی از داده‌های سیگنالی کمک کند.	- فناوری‌های هوش مصنوعی و یادگیری ماشینی - رایانش کوانتومی - تحلیل کلان داده
P9	- هوش مصنوعی می‌تواند حجم عظیم داده‌های سیگنالی را با دقت و سرعت بالا تحلیل کند و شناسایی	- هوش مصنوعی - پردازش زبان طبیعی - رباتیک

شماره خبره	خلاصه نظرات خبرگان	فناوری‌های مورد استفاده
	سیگنال‌های جدید و نامشخص که ممکن است از دید اپراتور انسانی پنهان بمانند - با استفاده از پردازش زبان طبیعی و رباتیک می‌توان بسیاری از فرایندهای تکراری و زمان‌بر در سیگینت را خودکار کرد. این موضوع باعث صرفه‌جویی در زمان و منابع انسانی می‌شود.	
P10	- جستجو، جمع‌آوری و تحلیل سیگنال‌ها به کمک هوش مصنوعی بسیار سریع‌تر نسبت به کاربر انسانی انجام می‌شود - پردازش ابری امکان مقیاس‌پذیری بالا را فراهم کرده و می‌تواند به پردازش حجم بالای سیگنال‌ها کمک کند - الگوریتم‌های یادگیری عمیق می‌توانند در پردازش و تحلیل سیگنال‌ها مانند فیلتر کردن نویز و کلاسترینگ خیلی کارآمد هستند- با استفاده از قابلیت‌های رایانش کوانتومی، پردازش سیگنال‌ها با سرعت چند برابر صورت می‌گیرد - با پردازش لبه (Edge Computing) بار پردازشی سیستم‌ها کاهش می‌یابد- فناوری‌های 5G و ارتباطات بی‌سیم پیشرفته باعث افزایش نرخ انتقال داده و کاهش تأخیر در انتشار اطلاعات جمع‌آوری‌شده می‌شوند.	- استفاده از هوش مصنوعی - رایانش ابری - الگوریتم‌های یادگیری عمیق - قابلیت‌های رایانش کوانتومی - پردازش لبه - فناوری 5G

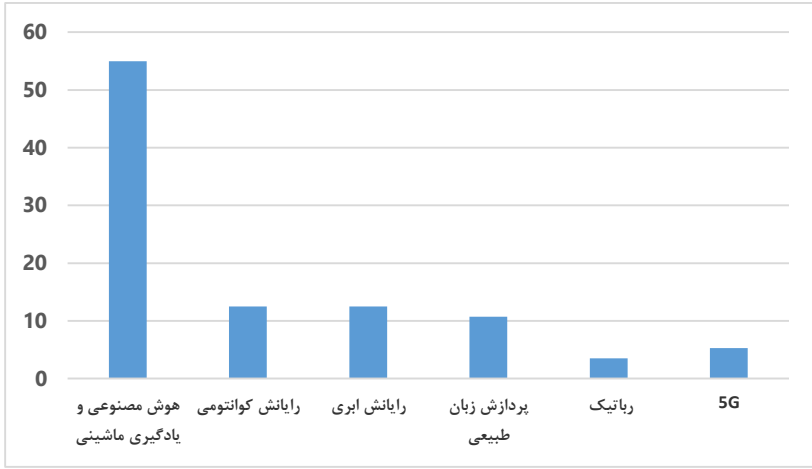
با تحلیل مضمون مصاحبه با صاحب‌نظران مشاهده می‌شود که تأکید آن‌ها برای استفاده از فناوری‌های نوظهور در حوزه سیگینت چنین است: فناوری‌های هوش مصنوعی و یادگیری ماشینی، اینترنت اشیا، تحلیل کلان داده‌ها، پردازش ابری برای ذخیره‌سازی و پردازش داده‌ها، فناوری‌های نوین ارتباطی و بی‌سیم و شبکه‌های ارتباطی پرسرعت، فناوری 5G، سیستم‌های

مانیتورینگ هوشمند، رمزنگاری کوانتومی و بلاکچین، رایانش کوانتومی، اتوماسیون فرایندهای رباتیک و پردازش لبه.

براساس یافته‌های پژوهش و با تقاطع‌گیری نتایج حاصله از منابع پژوهش ازجمله مقالات، اسناد و مدارک وب‌سایت‌های سازمان‌های اطلاعاتی دنیا و شرکت‌های سازنده سامانه‌های اطلاعات سیگنالی با پاسخ‌های خبرگان، می‌توان چنین تحلیل کرد که فناوری‌های زیادی در این حوزه مورد استفاده قرار می‌گیرند ولی در یک جمع‌بندی کلی می‌توان مهم‌ترین و کاربردی‌ترین فناوری‌های نوظهور در حوزه سیگینت را چنین برشمرد: هوش مصنوعی و یادگیری ماشینی، پردازش ابری، رایانش کوانتومی، پردازش زبان طبیعی، فناوری 5G و رباتیک که در ادامه تحلیل کمی آن‌ها مشاهده می‌شود:

جدول ۷: فراوانی فناوری‌های نوظهور کاربردی در اطلاعات سیگنالی حاصل از یافته‌های پژوهش

ردیف	فناوری نوظهور	فراوانی در اسناد و مدارک	فراوانی در مصاحبه با خبرگان	فراوانی کل	درصد فراوانی کل
۱	هوش مصنوعی و یادگیری ماشینی	۲۲	۹	۳۱	۵۵
۲	رایانش کوانتومی	۴	۳	۷	۱۲/۵
۳	رایانش ابری	۴	۳	۷	۱۲/۵
۴	پردازش زبان طبیعی	۵	۱	۶	۱۰/۷
۵	رباتیک	۱	۱	۲	۳/۵
۶	5G	۲	۱	۳	۵/۳
جمع کل				۵۶	



شکل ۲: نمودار فراوانی فناوری‌های نوظهور کاربردی در اطلاعات سیگنالی حاصل از یافته‌های پژوهش

همان‌طور که در جدول (۷) و شکل (۲) دیده می‌شود هوش مصنوعی و یادگیری ماشینی با ۳۱ بار میزان اشاره (۵۵٪ از کل تأکیدها) بالاترین کاربرد را در میان فناوری‌های نوظهور در حوزه سیگنت داشته و فناوری‌های رایانش کوانتومی و رایانش ابری هرکدام با ۷ بار میزان اشاره (۱۲/۵٪) و پردازش زبان طبیعی با ۶ اشاره (۱۰/۷٪) اهمیت کاربردی میانی و رباتیک با ۲ بار تکرار (۳/۵٪) و 5G با ۳ بار تکرار (۵/۳٪) تأکید کمتری را داشته‌اند.

در ادامه مصاحبه از خبرگان در خصوص الزامات امنیت سایبری در حوزه سیگنت سؤال شد که خلاصه مطالب در جدول (۸) آورده شده است:

جدول ۸: نظرات خبرگان در خصوص الزامات امنیت سایبری در حوزه سیگنت

ردیف	خلاصه نظرات خبرگان	مقولات اصلی
P1	امنیت سایبری و تضمین امنیت داده‌ها در برابر تهدیدات سایبری و عملیات هکرها در زیرساخت‌های فناوری اطلاعات و انتشار و ارسال اطلاعات	تضمین امنیت داده‌ها در زیرساخت‌های فناوری اطلاعات و ارتباطات
P2	الزامات امنیت سایبری شامل چند جنبه مهم ازجمله جلوگیری از دسترسی غیرمجاز به اطلاعات رهگیری شده، امنیت ارتباطات و پیروی از استانداردهای امنیتی است.	جلوگیری از دسترسی غیرمجاز به اطلاعات و امنیت ارتباطات پیروی از استانداردهای امنیتی

ردیف	خلاصه نظرات خبرگان	مقولات اصلی
P3	الزامات امنیت سایبری شامل مجموعه‌ای از اصول و اقدامات بوده که به حفاظت از داده‌ها و سیستم‌های اطلاعات سیگنالی کمک می‌کند. ازجمله استفاده از روش‌های رمزگذاری برای محافظت از داده‌ها در حین انتقال و ذخیره‌سازی، محدود کردن دسترسی‌ها، روش‌های احراز هویت قوی و افزایش آگاهی کارکنان است.	مجموعه‌ای از اصول و اقدامات رمزگذاری برای محافظت از داده‌ها؛ محدود کردن دسترسی‌ها؛ احراز هویت قوی و افزایش آگاهی کارکنان
P4	شناسایی و رفع آسیب‌پذیری‌های موجود در نرم‌افزارها و سخت‌افزارهای مرتبط با سامانه‌های اطلاعات سیگنالی و اطمینان از این‌که فقط افراد مجاز به داده‌ها و سیستم‌ها دسترسی دارند	شناسایی و رفع آسیب‌پذیری‌های نرم‌افزارها و سخت‌افزارها؛ دسترسی افراد مجاز به داده‌ها و سیستم‌ها
P5	امنیت سایبری در حوزه اطلاعات سیگنالی از اهمیت بالایی برخوردار است، زیرا این حوزه با داده‌های حساس و حیاتی سروکار دارد که ممکن است هدف حملات سایبری قرار گیرد. برای تضمین امنیت در این حوزه، رعایت الزامات و اقدامات امنیتی ضروری است.	حساسیت بالای داده‌ها و اطلاعات سیگنالی؛ رعایت الزامات و اقدامات امنیتی
P6	تضمین امنیت داده‌های سیگنالی با روش‌های رمزنگاری داده‌ها در برابر تهدیدات سایبری و نشت اطلاعات. همچنین به‌صورت دوره‌ای تجهیزات را ارزیابی امنیتی کرد.	رمزنگاری داده‌ها و ارزیابی امنیتی تجهیزات
P7	با فناوری‌هایی مانند رمزنگاری کوانتومی و بلاکچین، می‌توان داده‌های حساس را به‌طور ایمن‌تر ذخیره و انتقال داد زیرا این فناوری‌ها در برابر تهدیدات سایبری پیشرفته‌تر مقاومت بیشتری دارند	رمزنگاری کوانتومی و بلاکچین در انتقال اطلاعات
P8	باید با پیروی از استانداردها و مقررات و تأمین امنیت فیزیکی تجهیزات و زیرساخت‌های مرتبط با اطلاعات سیگنالی مراقب تهدیدات و حملات سایبری بود.	پیروی از استانداردها و مقررات تأمین امنیت فیزیکی تجهیزات و زیرساخت‌ها
P9	باید چالش‌های امنیت سایبری را مدنظر قرار داده و مخاطرات سامانه‌های اطلاعات سیگنالی را شناسایی، ارزیابی و کاهش داد.	یافتن چالش‌های امنیت سایبری؛ شناسایی، ارزیابی و کاهش مخاطرات سامانه‌های اطلاعات سیگنالی

ردیف	خلاصه نظرات خبرگان	مقولات اصلی
P10	باید به امنیت داده‌ها توجه داشت و مجموعه‌ای از استانداردها و مقررات برای حفاظت از اطلاعات سیگنالی و جلوگیری از دسترسی غیرمجاز به آن‌ها تدوین کرد؛ حفاظت از اطلاعات سیگنالی در برابر حملات سایبری با کنترل دسترسی و رمزنگاری پیشرفته بهبود می‌یابد.	تدوین استانداردها و مقررات برای حفاظت از اطلاعات و جلوگیری از دسترسی غیرمجاز کنترل دسترسی و رمزنگاری پیشرفته

نظرات مصاحبه‌شوندگان در خصوص الزامات امنیت سایبری در حوزه سیگینت براساس تحلیل محتوا در چهار دسته کلی زیر طبقه‌بندی‌شده است:

امنیت سخت‌افزار: تدوین و پیروی از استانداردها و مقررات امنیتی، کنترل و محدود کردن دسترسی افراد به داده‌ها و سیستم‌ها، ارزیابی امنیتی تجهیزات، شناسایی و رفع آسیب‌پذیری‌های سخت‌افزارها، تأمین امنیت فیزیکی تجهیزات و زیرساخت‌ها، ارزیابی و کاهش مخاطرات سامانه‌های اطلاعات سیگنالی

امنیت نرم‌افزار: شناسایی و رفع آسیب‌پذیری‌های نرم‌افزارها

امنیت اطلاعات: تضمین امنیت داده‌ها، جلوگیری از دسترسی غیرمجاز به اطلاعات، رمزگذاری پیشرفته برای محافظت از داده‌ها، احراز هویت قوی، امنیت داده‌های سیگنالی در برابر تهدیدات و حملات سایبری.

امنیت ارتباطات: رمزنگاری کوانتومی و زنجیره بلوکی در انتقال اطلاعات

در نهایت، با بهره‌برداری و جمع‌بندی از یافته‌های به‌دست‌آمده مدل مفهومی پژوهش به شرح شکل (۳) توسط محقق طراحی‌شده است:

شکل ۳: مدل مفهومی کاربست فناوری‌های نوظهور در اطلاعات سیگنالی با رویکرد امنیت سایبری (منبع: یافته‌های پژوهش)

همان‌طور که ملاحظه می‌شود، مدل مفهومی ترسیم‌شده در شکل (۳) از لایه‌های مختلفی تشکیل گردیده، ابتدا چرخه اطلاعات سیگنالی با ذکر مراحل جزئی و فنی بیشتر نسبت به فرایندهای معمول در اسناد و مدارک تشریح شده و در لایه بعد فناوری‌های نوظهور پرکاربرد و مورد استفاده در این چرخه شامل: فناوری‌های هوش مصنوعی و یادگیری ماشینی، رایانش کوانتومی، رایانش ابری، پردازش زبان طبیعی، رباتیک و 5G آمده است. در لایه بعد مؤلفه‌های امنیت سایبری حوزه اطلاعات سیگنالی شامل محرمانگی، صحت، دسترس‌پذیری، کنترل دسترسی و عدم انکار تشریح شده و در لایه آخر الزامات امنیت سایبری برای کاربست فناوری‌های نوظهور شامل امنیت سخت‌افزار، امنیت نرم‌افزار، امنیت اطلاعات و امنیت ارتباطات دیده می‌شود. همچنین مؤلفه‌های اثرگذار بر روی امنیت سایبری حوزه اطلاعات سیگنالی شامل دو دسته اصلی آسیب‌پذیری‌ها و تهدیدات سایبری اطلاعات سیگنالی ذکر شده که در بخش بعد در خصوص این لایه‌ها توضیح بیشتری ارائه شده است.

نتیجه‌گیری و پیشنهاد

در این مقاله تلاش گردید با نگاهی نو به حوزه اطلاعات سیگنالی پرداخته شود. در بخش مبانی نظری ابتدا با بررسی صورت گرفته چالش‌های این حوزه ارائه گردید که می‌توان بخش عمده‌ای از این چالش‌ها را با به‌کارگیری فناوری‌های نوظهور به‌ویژه فناوری هوش مصنوعی کاهش داد. سپس با جستجوی کتابخانه‌ای شرکت‌های سازنده سامانه‌ها و تجهیزات اطلاعات سیگنالی در دنیا شناسایی‌شده و محصولاتی که در آن‌ها از فناوری‌های نوظهور استفاده کرده‌اند و نیز سازمان‌های اطلاعات سیگنالی و مراکز تحقیقاتی که در این زمینه اقدامات زیادی انجام داده و یا اعلام نظر نموده‌اند تشریح شد. همچنین به‌دلیل وجود سرمایه‌های سایبری بسیار در حوزه اطلاعات سیگنالی؛ نگاه به مقوله امنیت سایبری نیز ضرورت دارد که در ادامه به آسیب‌پذیری‌ها، تهدیدات و الزامات امنیت سایبری این حوزه نیز پرداخته شد. در بخش تجزیه‌وتحلیل، به‌منظور تکمیل یافته‌های پژوهش در بخش مبانی نظری، با تعداد ده نفر از صاحب‌نظران در این حوزه مصاحبه شد. در نهایت با روش کیفی تحلیل مضمون از اسناد، مدارک، مقالات و متن مصاحبه‌ها، مدل مفهومی طراحی گردید.

مدل مفهومی طراحی‌شده از چندلایه تشکیل‌شده است. ابتدا چرخه سیگینت تشریح گردیده، با این تفاوت که چرخه‌های مرسوم در ادبیات این حوزه شامل مراحل عمده برنامه‌ریزی، جمع‌آوری، پردازش، تجزیه‌وتحلیل و انتشار هستند؛ ولی در این پژوهش جهت عینیت بیشتر کاربرد فناوری‌های نوظهور؛ اجزای بیشتر و جزئی‌تر از مراحل اطلاعات سیگنالی ازجمله مراحل «طبقه‌بندی»[1]، «خوشه‌بندی»[2]، «دمدولاسیون»[3]، «رمزشکنی»[4]، «جهت‌یابی»[5]، ذخیره‌سازی، «رونویسی»[6] و «ادغام»[7] نیز اضافه شده‌اند.

1. Classification
2. Clustering
3. Demodulation
4. Decryption
5. Direction Finding
6. Transcription
7. Fusion

لازم به توضیح است که با توجه مأموریت‌های کاری مختلف در دو بخش اصلی سیگینت شامل الینت و کامینت مراحل فوق و ترتیب انجام آن‌ها می‌تواند متفاوت است.

در لایه بعد مدل؛ کاربردی‌ترین فناوری‌های نوظهور در این حوزه که حاصل از یافته‌های پژوهش بوده مشاهده می‌شود که توضیح آن‌ها بدین شرح است:

- ❖ فناوری هوش مصنوعی و یادگیری ماشینی: برای مراحل جستجو، جمع‌آوری، خوشه‌بندی، دمدولاسیون، پردازش، رمزشکنی، جهت‌یابی، ادغام و تجزیه‌وتحلیل؛
- ❖ فناوری رایانش کوانتومی: مانند فناوری هوش مصنوعی و یادگیری ماشینی در مراحل فوق به‌ویژه در بخش مهم رمزشکنی اطلاعات سیگنالی می‌توان بهره‌برداری کرد؛
- ❖ فناوری رایانش ابری: برای مراحل ذخیره‌سازی و پردازش داده‌ها؛
- ❖ فناوری پردازش زبان طبیعی: برای مرحله رونویسی (تبدیل گفتار به متن و ترجمه زبان)؛
- ❖ فناوری رباتیک: در بخش جستجو و جمع‌آوری و پردازش اطلاعات؛
- ❖ فناوری 5G: برای انتشار و اشتراک‌گذاری پرسرعت و با حجم بالای اطلاعات در شبکه ارتباطی.

بدون تردید این فناوری‌ها و یا نیز سایر فناوری‌های نوظهور می‌توانند کاربردهای متنوع دیگری در حوزه اطلاعات سیگنالی داشته باشند. همچنین، ازآنجایی‌که اطلاعات سیگنالی دارای سرمایه‌های سایبری متعددی است، در لایه بعد نیاز است تا الزامات سایبری نیز لحاظ گردد. ابتدا مؤلفه‌های امنیت سایبری ازجمله محرمانگی، صحت، دسترس‌پذیری، کنترل دسترس‌پذیری و عدم انکار داده‌ها آورده شده و در لایه بعد الزامات امنیت سایبری در چهار بخش شامل امنیت سخت‌افزار، امنیت نرم‌افزار، امینت اطلاعات و امنیت ارتباطات تشریح شده است. دو عامل اثرگذار در امنیت سایبری شامل آسیب‌پذیری‌ها و تهدیدات سایبری است که برخی از مهم‌ترین آن‌ها مشاهده می‌گردد. آسیب سایبری سیگنت می‌تواند شامل ناشی از مراحل طراحی و معماری، ساخت و تولید سامانه‌ها و تجهیزات، بهره‌برداری سهوی و اشتباه توسط کاربران و یا با نیت بدخواهانه و عمدی، ارتباطات بدون امنیت، کنترل

دسترسی ناقص، نقص رمزنگاری، نقص احراز هویت و نقص ثبت و نظارت باشد و در نهایت عمده تهدیدات سایبری سیگینت می‌تواند مواردی چون باج‌افزار، بدافزار، دسترسی غیرمجاز، دستکاری و مداخله در اطلاعات و حملات زنجیره تأمین باشند.

در مدل فوق سعی گردید با دیدگاهی نوآورانه کاربرد فناوری‌های نوظهور در حوزه اطلاعات سیگنالی با رویکرد امنیت سایبری تشریح شود که می‌تواند علاوه بر سازمان‌های با مأموریت اطلاعات سیگنالی، برای سایر سازمان‌های نظامی که در سایر حوزه‌های اطلاعاتی فعالیت می‌کنند مفید واقع شود.

به‌دلیل حساسیت بالای حوزه اطلاعات سیگنالی اسناد، مدارک، مقالات و کتب بسیار کمی جهت مطالعات کتابخانه‌ای و تعداد کمی از صاحب‌نظران در دسترس بوده که این امر باعث ایجاد محدودیت در جمع‌آوری و تحلیل مبانی نظری و بخش تجزیه‌وتحلیل پژوهش حاضر گردیده بود.

پیشنهادهای پژوهش

- ✓ سازمان‌های فعال در حوزه اطلاعات سیگنالی نیروهای مسلح کشور با کمک صنعت دفاعی، شرکت‌های فناور و دانش‌بنیان و نیز دانشگاه‌های کشور به‌منظور به‌کارگیری از فناوری‌های احصا شده در این مقاله به مطالعه و تحقیقات گسترده پرداخته تا منجر به طراحی و تولید تجهیزات پیشرفته و به‌روز گردد و پاسخ‌گوی نیازمندی‌های اطلاعات سیگنالی این سازمان‌ها در انجام بهینه مأموریت خود باشند.
- ✓ با توجه به اهمیت و ضرورت رعایت الزامات امنیت سایبری در به‌کارگیری فناوری‌های نوظهور، پیشنهاد می‌شود در کلیه مراحل از طراحی اولیه تا ساخت و تولید و پیاده‌سازی نهایی زیرساخت‌های فناورانه و تجهیزات اطلاعات سیگنالی، الزامات امنیت سایبری مدنظر طراحان، سازندگان و نیروهای بهره‌بردار قرار گیرد.

- ✓ پیشنهاد می‌گردد جهت شناخت و آگاهی بیشتر آسیب‌پذیری‌ها و تهدیدات امنیت سایبری در حوزه اطلاعات سیگنالی، کارگاه‌های آگاه‌سازی و آموزش‌های کوتاه‌مدت برای مسئولان و کارکنان مرتبط با این حوزه در سطح نیروهای مسلح برگزار گردد.

فهرست منابع

- بیک بیلندی، علی‌اصغر (۱۴۰۱). ***مؤلفه‌ها و شاخص‌های زیرساخت و تجهیزات اینترنت اشیا مؤثر بر دفاع هوشمند نیروهای مسلح***. فصلنامه آماد و فناوری دفاعی، ۵(۴)، ۱۰۷-۱۳۶.
- ترسلی، احمدرضا؛ محمدی منفرد، حسن؛ موحدی صفت، محمدرضا (۱۴۰۳). ***کاربرد هوش مصنوعی در بهبود فرایند جمع‌آوری و تحلیل اطلاعات***. مطالعات بین‌رشته‌ای دانش راهبردی، ۱۴(۵۶)، ۳۰۳-۲۷۷.
- خالقی دخت، محمود (۱۴۰۰). ***مباحث تخصصی پدافند سایبری***، انتشارات سبک نو، تهران.
- خزاعی، رضا؛ حبیبی، نیک‌بخش؛ دوستی مطلق، سیدنصیب الله؛ زروندی، جواد (۱۴۰۳). ***ارائه مدل ارتقای قدرت عملیاتی تهاجم هوایی بر پایه حوزه‌های اثرگذار علوم و فناوری کوانتومی***. فصلنامه آماد و فناوری دفاعی، ۷(۳)، ۱۱-۴۰.
- رستمی، محسن (۱۴۰۱). ***شناسایی و معرفی ظرفیت‌های کاربردی هوش مصنوعی در توسعه مضمون‌های راهبردی در سازمان‌های نظامی***. راهبرد دفاعی، ۲۰(۷۸)، ۳۴-۷۴.
- شاددل، امیرحسین (۱۴۰۲). ***آینده مدیریت و تصمیم‌گیری با استقرار سامانه‌های هوش مصنوعی***، فصلنامه آینده‌پژوهی راهبردی، ۲(۵)، ۱۲۱-۱۳۸.
- شاملو، رضا (۱۴۰۳). ***واکاوی تهدیدات هوایی نوپدید و راهکارهای مقابله با آن (مطالعه موردی: ریز پرنده‌ها)***. فصلنامه آماد و فناوری دفاعی، ۷(۲)، ۱۵۵-۱۹۰.
- شاه‌رضائی، محمّدحسن (۱۴۰۱)، ***نقش اطلاعات سیگنالی در ۸ سال دفاع مقدس***، همایش ملی جایگاه علم و فناوری در دفاع مقدس، تهران.
- گودرزی، علی (۱۳۹۲). ***عملیات اطلاعات سیگنالی***. تهران: انتشارات مرکز آموزشی پژوهشی شهید صیاد شیرازی، ص ۲۱.
- مظلوم، جلیل؛ بیگدلی، حمید (۱۴۰۱). ***شبکه عصبی عمیق ترکیبی بهینه ادغام‌شده با انتخاب ویژگی برای سامانه تشخیص نفوذ در حملات سایبری***. پدافند الکترونیکی و سایبری، ۱۰(۴)، ۴۱-۵۱.
- نصیرزاده، عزیز؛ شاه‌رضائی، محمدحسن (۱۳۹۱). ***میدان نبرد دیجیتال***، مرکز انتشارات آموزشی و پژوهشی شهید صیاد شیرازی، تهران.

References

- Ahmed, N. U. (2022). Integrating machine learning in military intelligence process: study of futuristic approaches towards human-machine collaboration. NDC e-journal, 2(1), 59-89.
- Artificial Intelligence in Software-Defined SIGINT Systems. (2024). available at: https://www.ni.com/en/solutions/aerospace-defense/radar-electronic-warfare-sigint/artificial-intelligence-in-software-defined-sigint-systems.html
- Artificial Intelligence: Next Frontier is Cybersecurity. (2021). available at: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2702241/artificial-intelligence-next-frontier-is-cybersecurity/
- Automatic Spectrum Situational Awareness through Machine Learning. (2020). available at: https://gdmissionsystems.com/-/media/General-Dynamics/Cyber-and-Electronic-Warfare-Systems/PDF/Data-Sheets/cyber-signaleye-datasheet.ashx?la=en&hash=EB2E9C736E2943B8D3F8874D90777E92B4C56119
- Babuta, A., Oswald, M., & Janjeva, A. (2020). Artificial intelligence and UK national security: policy considerations.
- Bartock, M., Brule, J., Li-Baboud, Y. S., Lightman, S., McCarthy, J., ... & Suloway, T. (2021). Foundational PNT Profile: Applying the Cyber Security Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services. US Department of Commerce, National Institute of Standards and Technology.
- Belz, L. (2019). HENSOLDT's 'Kalaetron Integral' – the Future of Signals Intelligence.
- Boudreaux, L. (2023). Signals Intelligence, MCRP 2-10A.1. US Marine Corps.
- Cantrell, T. L. (2023). JADC2 Culture at the Operational Level of War. Air & Space Operations Review, 2(1).
- Cloud Computing for U.S. Intelligence Community. (2025). Available at: https://aws.amazon.com/federal/us-intelligence-community/
- Cho, S., Shin, W., Kim, N., Jeong, J., & In, H. P. (2020). Priority Determination to Apply Artificial Intelligence Technology in Military Intelligence Areas. Electronics, 9(12), 2187.
- Cornelis Jan G, (2023). Unraveling the Quantum-SIGINT Nexus: A Comprehensive Examination of Signals Intelligence in the Age of Quantum Computing. available at: https://www.linkedin.com/pulse/unraveling-quantum-sigint-nexus-comprehensive-signals-groeneveld/
- Dodson, D. and etc. (2021). Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD).
- Dorton, S. L., & Harper, S. (2021). Trustable AI: A critical challenge for naval intelligence. Center for International and Maritime Security (CIMSEC).
- Fleming, J. (2021). Pioneering a New National Security The Ethics of Artificial Intelligence. Government Communications Headquarters, a British intelligence and security organization.

- Hayden, M. V. (2014). Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence. Notre Dame JL Ethics & Pub. Pol'y, VOL19, 1.
- Hoehn, J. R. (2022). Joint All-Domain Command and Control (JADC2).
- Ish, D., Ettinger, J., & Ferris, C. (2021). Evaluating the effectiveness of artificial intelligence systems in intelligence analysis. RAND Corporation.
- Jagannath, J., Polosky, N., Jagannath, A., Restuccia, F., & Melodia, T. (2019). Machine learning for wireless communications in the Internet of Things: A comprehensive survey. Ad Hoc Networks, 93, 101913.
- Joint Doctrine Publication 2-00 Intelligence. (2023). Counter-intelligence and Security Support to joint Operations. available at: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf
- Kramer, S. (2022). Amazon Web Services Re-Awarded $10 Billion 'Wild and Stormy' NSA Contract After Microsoft Dispute.
- Kumari, N. (2024). Al-Based Signal Intelligence for Real-Time Threat Detection. Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146, 10(3), 1-8.
- Lella, I and etc. (2024). ENISA THREAT LANDSCAPE 2024. European Union Agency for Cybersecurity (ENISA).
- The Intelligence Community in the 21st Century. (1996). available at: https://www.govinfo.gov/content/pkg/GPO-IC21/html/GPO-IC21-5.html
- The Internet of Things for the intelligence community. (2015). available at: https://militaryembedded.com/ai/big-data/the-internet-things-the-intelligence-community
- The Role of SIGINT in Data Analytics: Bridging Intelligence & Insight. (2024). available at: https://www.elementx.biz/post/the-role-of-sigint-in-data-analytics-bridging-intelligence-and-insight#:~:text=Real%2DTime%20Intelligence,battlefield%20or%20in%20cybersecurity%20operations.
- Tucker, P. (2020). Spies Like AI: The Future of Artificial Intelligence for the US Intelligence Community. Defense One.
- Rashid, A. B., Kausik, A. K., Al Hassan Sunny, A., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. International Journal of Intelligent Systems, 2023(1), 8676366.
- Research Overview. (2025). available at: https://www.nsa.gov/Research/Overview/
- Rohde & Schwarz meets current and future COMINT challenges head on. (2023). available at: https://www.rohde-schwarz.com/fr/a-propos-de/actualites-et-presse/all-news/rohde- schwarz-meets-current-and-future-comint-challenges-head-on-page-de-details-des-communiques-de-presse_229356-1364846.html
- Ross, R. S. (2018). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. J., & McQuaid, R. M. (2021). Nist special publication 800-160, volume 2 revision 1: Developing cyber-resilient

systems: a systems security engineering approach. In National Institute of Standards and Technology (US) (No. NIST SP 800-160, Vol. 2, Rev. 1.

- Signals Intelligence. (2025). available at: https://voyagertechnologies.com/defense-natsec/signals-intelligence/
- Signals Intelligence Global Market Report. (2025). available at: https://www.thebusinessresearchcompany.com/report/signals-intelligence-sigint-global-market-report
- Top 10 Application Security Vulnerabilities in 2024. (2024). available at: https://www.bytehide.com/blog/top-10-application-security-vulnerabilities-in-2024
- Turner, Paul D. (2024). “SIGINT, TSCM and AI.” available at: https://www.intersecmag.co.uk/sigint-tscm-and-ai/