
فصلنامه علمی آماد و فناوری دفاعی، سال پنجم، شماره شانزدهم، زمستان ۱۴۰۱

مؤلفه‌ها و شاخص‌های زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر دفاع هوشمند نیروهای مسلح

علی اصغر بیک بیلندی^۱

تاریخ دریافت: ۱۴۰۱/۰۹/۲۰

تاریخ پذیرش: ۱۴۰۱/۱۰/۲۱

چکیده

اهمیت دفاع هوشمند در کنار مفاهیم جدیدی همچون «قدرت هوشمند» «تهدیدات هوشمند» «جنگ هوشمند» و «ارتش هوشمند» بیشتر نمایان می‌گردد. با بهره‌گیری مناسب و به‌موقع از فناوری‌های نوین از جمله فناوری اینترنت اشیاء در حوزه نظامی و دفاعی، تا حدود زیادی می‌توان پیاده‌سازی و مدیریت در این حوزه را با دقت بیشتر و پویاتری انجام داد. با به‌کارگیری اینترنت اشیاء در فرماندهی و کنترل هوشمند، آماد هوشمند، ترابری هوشمند، پایش محیطی، آموزش و شبیه‌سازی، ایجاد سیستم‌های کنترل آتش یکپارچه در زمین، هوا و دریا، تسلیحات هوشمند، مدیریت صحنه نبرد، سنجش مشارکتی در میدان نبرد، مدیریت امکانات و... می‌توان به قابلیت‌های دفاعی نوین و اثربخش و در واقع به دفاع هوشمند در نیروهای مسلح در برابر تهدیدات نوین و هوشمند دست یافت. زیرساخت و تجهیزات یکی از ابعاد مهم مقوله دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء است. پژوهش حاضر با عنوان «مؤلفه‌ها و شاخص‌های زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح» با روش توصیفی - تحلیلی و با رویکرد آمیخته (کمی و کیفی) انجام شده است. در این تحقیق، از نظرات ۷۰ نفر از افراد خبره در حوزه علوم دفاعی راهبردی و سایبری کشور در قالب

^۱ عضو هیئت علمی دانشگاه عالی دفاع ملی

پرسشنامه استفاده شده است. بر اساس پژوهش انجام شده، ۵ مؤلفه و ۲۷ شاخص احصاء شده و مورد تجزیه و تحلیل قرار گرفتند.

واژه‌های کلیدی: دفاع، دفاع هوشمند، اینترنت اشياء، زیرساخت و تجهیزات

۱- مقدمه

فناوری‌های نوین، باعث ایجاد تغییرات اساسی در سازمانها، راهبردها و تدابیر امنیتی و دفاعی شده است. فناوری‌های پیشرفته جدید، باعث توزیع و انتشار آگاهی‌ها شده، سرعت تبادل اطلاعات را افزایش داده و با پشت سر گذاشتن مرزهای قدیمی، افق جدیدی را در عملکرد نیروهای نظامی و تحول در حوزه دفاعی و هوشمندی سامانه‌های نظامی گشوده است. این تحولات فناورانه در حوزه‌های فرماندهی و کنترل که مسئولیت مدیریت و هدایت عملیات‌های نظامی را بر عهده دارد، تأثیرات عمیقی برجای گذاشته است. بر این اساس ارتش‌های دنیا و سازمان‌های دفاعی همواره درصدد استفاده از فناوری‌های نوین و پیشرفته به منظور ارتقاء سطح تجهیزات و سامانه‌های دفاعی و هوشمند نمودن این سامانه‌ها جهت مقابله با تهدیدات هوشمند و نوین بوده است. هوش مصنوعی، اینترنت اشياء، کلان‌داده، بلاک‌چین، رایانش ابری، رباتیک و سامانه‌های بدون سرنشین از جمله فناوری‌های نوین و پیشرفته هستند که توانسته‌اند تحولات شگرفی را در حوزه‌های امنیتی و دفاعی ایجاد کنند. اینترنت اشياء متشکل از حسگرها، سیستم شناسایی و ردیابی خودکار، ارتباطات بی‌سیم، دسترسی به شبکه و سیستم‌های توزیع شده می‌باشد. همگرایی اینترنت و اشياء هوشمندی که بتوانند به برقراری ارتباط و تعامل با یکدیگر بپردازند، اینترنت اشياء را تعریف می‌کند. این الگوی جدید به‌عنوان یکی از مهم‌ترین عوامل در صنعت فناوری اطلاعات و ارتباطات در سال‌های آینده تشخیص داده شده است. (میراندی و همکارانش، ۲۰۱۲) تحولات انجام شده در ساختار دفاعی و نظامی نیروهای مسلح در راستای

هوشمندتر شدن دفاع، در سال‌های اخیر روند روبه رشدی داشته است؛ ولی چیزی که مسلم است این ساختار دفاعی می‌بایست علاوه بر کسب آمادگی جهت مقابله با دشمنان منطقه‌ای، در برابر تهدیدات دشمنان فرامنطقه‌ای نیز آماده مقابله باشد. اینترنت اشیا یک ایده جهانی برای اتصال همه اشیاء به یکدیگر است. ظهور اینترنت اشیا منجر به اتصال فراگیر انسان، خدمات، حسگرها و اشیاء در حوزه‌های انرژی، سلامت، حمل‌ونقل، تولید، صنایع هوایی و نیز صنایع نظامی و دفاعی شده است. اینترنت اشیا نظامی^۱ که در واقع مدل جدیدتر مفهوم جنگ شبکه محور است، می‌تواند زیرساخت فیزیکی نظامی و زیرساخت اطلاعات را به طور عمیقی باهم بیامیزد و قابلیت اتصال اشیاء نظامی را به یکدیگر فراهم نماید.

به‌کارگیری اینترنت اشیا در کنترل سلاح (سامانه کنترل آتش^۲)، پایش محیط^۳، تسلیحات هوشمند^۴، مدیریت صحنه نبرده، سنجش مشارکتی در میدان نبرد^۵، سامانه آآمد و زنجیره تأمین هوشمند، پایش سلامت و بهداشت^۶، آموزش و شبیه‌سازی، مدیریت هوشمند ناوگان خودرویی، نیروهای مسلح جمهوری اسلامی ایران را قادر می‌کند تا به قابلیت‌های دفاعی نوین و اثربخش و در واقع به دفاعی هوشمند دست پیدا نماید. محققین در این پژوهش بنا دارند مؤلفه‌ها و شاخص‌های بعد زیرساخت و تجهیزات اینترنت اشیا مؤثر بر هوشمندی دفاع نیروهای مسلح را استحصال نموده و مورد تجزیه و تحلیل قرار دهند. لذا هدف تحقیق عبارت است از؛ تعیین مؤلفه‌ها و شاخص‌های زیرساخت و تجهیزات اینترنت اشیا مؤثر بر دفاع هوشمند نیروهای مسلح که متناظر با این هدف سوال تحقیق طراحی شده است.

1 MIoT: Military Internet of Things

2 Fire control system

3 Surveillance

4 Smart weapons

5 Battlefield monitor

6 Collaborative sensing

7 Health monitoring

دفاع هوشمند نیروهای مسلح

۲- مبانی نظری و ادبیات تحقیق

- مفهوم‌شناسی

تعریف دفاع:

دفاع، ایستادگی در برابر دشمن، بازداشتن (بازدارندگی) و پس زدن دشمن (دفع و رفع تهدید) می‌باشد. (وکیلی، ۱۳۸۸: ۲۰۵) دفاع و مدافعه کردن، مستحکم کردن، حمایت کردن، استحکامات. (آریان‌پور کاشانی، ۱۳۴۵: ۵۶۲) دفاع، مجموعه‌ای از اقدامات کنشی، واکنشی و همچنین پادکنش در برابر آسیب‌های منافع، امنیت و یا هستی موجودات زنده است. (حسن‌لو، ۱۳۹۷: ۲۵۵) دفاع، مجموعه‌ای از اقدامات کنشی، واکنشی و همچنین پادکنش در برابر آسیب‌های منافع، امنیت و یا هستی موجودات زنده است.

مفهوم دفاع هوشمند:

واژه هوشمند و هوشمندی در زبان فارسی با مفاهیم باهوش، فراست، خداوند هوش، عقل، دانایی، بصیرت، هوشیاری، صاحب هوش، عاقل، بخرد و زرنگ در نظر گرفته شده است. (فرهنگ دهخدا، عمید و معین)

اصطلاح هوشمندی، با داده، اطلاعات و دانش ارتباط نزدیکی دارد و اغلب در پس آنها بیان می‌شود. (نامداریان و همکار، ۱۳۹۸: ۸۷) دفاع هوشمند، مفهومی است که کشورهای متحد را برای همکاری در توسعه، تأمین و حفظ و نگهداری امکانات و توانایی‌های نظامی به منظور پاسخگویی به مسائل امنیتی فعلی که در سند «مفهوم جدید راهبردی» ناتو تصریح شده است، تشویق و راهنمایی می‌نماید؛ بنابراین «دفاع هوشمند» ناتو به معنای تجمیع و به اشتراک‌گذاری امکانات و توانمندی‌ها، تعیین اولویت‌ها و هماهنگی تلاش‌ها است. سایت رسمی ناتو، دفاع هوشمند را این‌گونه تعریف نموده است: «دفاع

هوشمند» یک شیوه تفکر جدید درباره ایجاد توانمندی‌های دفاعی نوین برای آینده کشورهای عضو ناتو می‌باشد. دفاع هوشمند یک فرهنگ جدیدی از همکاری است که کشورهای عضو را به همکاری و مشارکت در توسعه، تأمین و حفظ و نگهداری توانمندی‌های نظامی و برعهده گرفتن وظایف و مسئولیت‌های محوری آنها در چارچوب مفهوم جدید راهبردی ناتو تشویق می‌نماید و آن به معنای تجمع و به اشتراک‌گذاری، اولویت‌بندی و هماهنگی تلاش‌ها و اقدامات می‌باشد. (سایت ناتو، ۲۰۲۱)

تعریف جامع و مانع از دفاع هوشمند باید شامل همه نگرش‌های (ماهیتی، ساختاری، رفتاری، فرایندی و کارکردی) آن باشد. (حسن لو، ۱۳۹۷)

الف- تعریف ماهیتی: دفاع هوشمند دارای سرشتی همه‌جانبه یا فراگیر (فرا حوزه‌ای، فرا محیطی، فرا نظامی، همچنین چند حوزه‌ای، چندبُعدی، چندسویه و چند ساحتی) است. (همان)

ب- تعریف ساختاری: دفاع هوشمند مجموعه‌ای ساختاریافته از سازمان‌ها، سامانه‌ها، شبکه‌های هوشمند واقعی و مجازی همراه با ابزار و ادوات هوشمند است. (همان)

پ- تعریف رفتاری: دفاع هوشمند، رهیافت دفاعی انتخاب به هنگام، تصمیم سریع، هم‌زمان و هم‌افزای قدرت هوشمند (نیرو و توان سخت، نرم، نیمه‌سخت یا پوشش تمام طیفی قدرت) و کاربرد بهینه و دقیق آن در برابر چالش‌های هوشمند و پیچیده می‌باشد. دفاع هوشمند همگرایی رهیافتی از انواع دفاع (دانش و آگاهی محور، شناخت محور، تأثیر محور، غیرعامل و ناهمگون) است. تلفیقی کارآمد از رویکردهای ناهمگونی، تأثیر محوری، شناخت محوری، غیرعامل بودن، مجازی بودن به گونه‌ای که از کاستی‌های هر رویکرد بکاهد. (همان)

ت- تعریف کارکردی: دفاع هوشمند دارای کارکردهای درونی (خودآگاهی، خودمانایی، خوداتکایی، خودتنظیمی، خودارزیابی و آینده‌اندیشی) و کارکردهای بیرونی (محیط‌آگاهی، رقیب‌آگاهی، تهدید‌آگاهی، آینده‌آگاهی) است که منجر به واکنش‌های هوشمندانه، اثربخش و بازدارنده خواهد شد. از دیگر کارکردهای آن تبدیل تهدیدات به فرصت است. (همان)

ث- تعریف فرایندی: دفاع هوشمند، حاصل همگرا کردن آسیب‌های دشمن با ضربه به گرانگاه‌ها (مراکز ثقل) به‌ویژه مراکز ثقل شناختی آن می‌باشد که موجب بی‌ثباتی و بی‌تعادلی دشمن شده و دستیابی به بیشترین تأثیر و نفوذ راهبردی را سرعت می‌بخشد. (همان) دفاع هوشمند عبارت است از

مفهوم‌سازی، اختصاصی‌سازی، ایجاد فرهنگ و چارچوب جدید امنیتی، نگاه به آینده به‌منظور درگیری با حداقل هزینه‌ها و سرمایه انسانی. (محمدعلی زاده و باقری، ۱۳۹۷: ۵)

کارکرد فناوری‌ها در جنگ‌های آینده عبارت خواهند بود از الف) سرعت؛ سرعت در عملیات‌های آینده یکی از مهم‌ترین فاکتورهای پیروز در جنگ محسوب می‌شود ب) اطلاعات و ارتباط؛ یکی دیگر از کارکردهای فناوری در جنگ‌های آینده توسعه و سرعت ردوبدل کردن اطلاعات و پردازش آنها و ارتباط بین سطوح فرماندهی جهت تصمیم‌گیر درست و به موقع خواهد بود. ج) دقت، فناوری‌های هوشمند آینده نقش مهمی در دقت تسلیحات نظامی در زدن هدف خواهند داشت. بنابراین خطای سلاح‌ها در زدن هدف تقریباً نزدیک به صفر خواهد شد. د) فاصله؛ در عملیات‌های آینده، فناوری‌ها کمک می‌کنند که فاصله کمترین اهمیت را داشته باشد و هر هدفی از هر مسافتی قابل اثبات باشد. (کازرونی، ۱۳۹۹)

تعریف اینترنت اشیاء:

اینترنت اشیاء، فناوری مدرنی است که در آن برای هر شی، قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترنت، فراهم می‌شود. در این فناوری، اشیاء قادرند از محیط اطراف خود داده‌های مفیدی را از طریق حسگرهای مختلف جمع‌آوری و برای پردازش و اتخاذ تصمیمات لازم به یک سیستم مرکزی منتقل کنند.

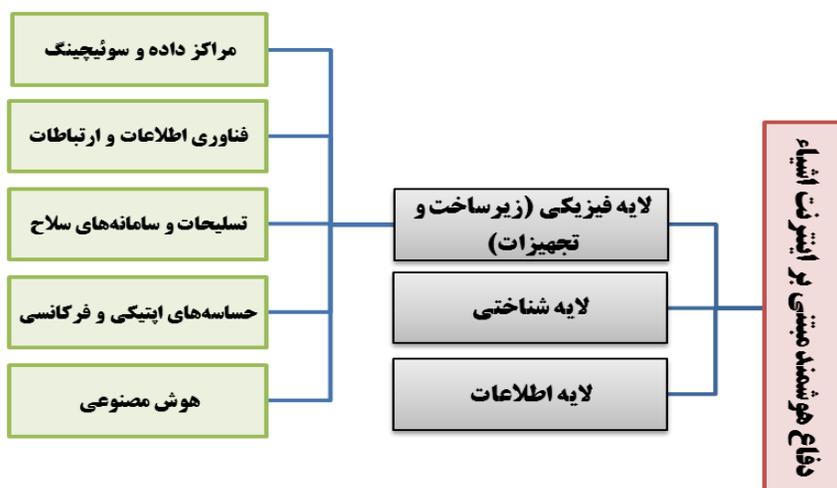
چارچوب نظری تحقیق^۱:

چارچوب نظری به مجموعه‌ای از مفروضات بنیادی لازم برای محدود و معین کردن موضوع یا مضمون یک علم یا یک نظریه گفته می‌شود و به عبارتی دیگر مبنایی است که پژوهشگر بر اساس آن درباره روابط بین عواملی که در ایجاد مساله مهم تشخیص داده شده‌اند نظریه‌پردازی می‌کند. در این تحقیق عواملی که دفاع هوشمند را شکل می‌دهند بر مبنای نظر مارتین لیبیک^۲ و مدل سه‌لایه‌ای فضای

1 - Teorical framework

2 - Martin libicki

سایبری ایشان شامل لایه فیزیکی (زیرساخت و تجهیزات)، لایه نحوی (شناختی) و لایه منطق (اطلاعات) مورد بررسی قرار می‌گیرد. بنابراین ابعاد دفاع هوشمند مبتنی بر اینترنت اشیا طبق نظریه فوق شناسایی شده و در گام بعدی محققین بر اساس بررسی پیشینه‌های تحقیق، ادبیات مرتبط، هم-پوشانی مطالعات کتابخانه‌ای و نظر خبرگان، مؤلفه‌ها و شاخص‌های لایه فیزیکی (زیرساخت و تجهیزات) را احصاء می‌نمایند. بنابراین چارچوب نظری این پژوهش برابر با شکل شماره (۱) می‌باشد.



شکل شماره ۱: چارچوب نظری

مطالعات کتابخانه‌ای و میدانی تحقیق متناسب با چارچوب نظری تحقیق

الف) مطالعات کتابخانه‌ای

- اینترنت اشیاء

اینترنت اشیاء یک الگوی جدید فناوری بوده و به‌عنوان شبکه‌ای جهانی از ماشین‌ها و دستگاه‌هایی است که توانایی تعامل با یکدیگر را دارند. اینترنت اشیاء به‌عنوان یکی از مهم‌ترین محورهای فناوری آینده شناخته شده و توجه قابل‌ملاحظه‌ای از صنعت را به خود اختصاص داده است. به همین دلیل، شورای ملی اطلاعات آمریکا در سال ۲۰۰۸، اینترنت اشیاء را به‌عنوان یکی از شش فناوری دارای پتانسیل تأثیرگذاری بر منافع ایالات متحده تا سال ۲۰۲۵ معرفی نموده است. (نظری، ۱۴۰۰: ۴)

اینترنت اشیاء فناوری نوظهوری است که در آن برای هر موجودیت امکان ارسال و دریافت داده از طریق شبکه‌های ارتباطی مختلف فراهم می‌گردد. اشیاء به هر چیزی گفته می‌شود که قابلیت جمع‌آوری داده‌ها، کنترل شدن و یا ارتباط از راه دور را داشته باشد. اینترنت اشیاء به بسیاری از کسب‌وکارها نفوذ می‌کند و ابزار ساده‌ای برای جمع‌آوری و تجزیه‌وتحلیل داده‌های سیستم فنی برای شناسایی و بهینه‌سازی عملکرد بسیاری از اشیاء در زندگی خصوصی و کاری ما فراهم می‌کند. (Ploennigs & 2018, etc)

فناوری اینترنت اشیاء تحولات عظیمی در زندگی روزمره بشر ایجاد کرده است. در عصر اینترنت اشیاء، فرستنده‌ها و گیرنده‌ها به اکثر فعالیت‌های روزمره گره‌خورده است. اتصال هر جا، هر کس، هر شیء در هر زمان ایجاد شده و مسیر زندگی را فوق‌العاده تغییر داده است. شهرهای هوشمند و برنامه‌ریزی شهری تأثیر مستقیم و اصلی روی پیشرفت جوامع دارد و باعث افزایش قدرت تصمیم‌گیری جوامع با ایجاد یک تصمیم‌گیری هوشمند و مؤثر و در زمان مناسب می‌شود. افزایش قابل‌توجه دستگاه‌های متصل شهری سبب رشد سریع داده‌ها و اطلاعات شده است که توجه بسیاری از پژوهشگران و دانشمندان را در حوزه‌های مختلف پژوهشی جلب کرده است. شهرهای هوشمند و برنامه‌ریزی شهری تأثیر مستقیم و اصلی روی پیشرفت جوامع دارد و با ایجاد یک تصمیم‌گیری هوشمند، مؤثر، و در زمان مناسب باعث افزایش قدرت تصمیم‌گیری جوامع می‌شود. اینترنت اشیاء به‌عنوان چشم اندازی بزرگ از دنیای اینترنت و چارچوبی برای دستگاه‌ها و حسگرها برای ارتباط ایمن

در محیط شهر هوشمند را فراهم کرده است و به اشتراک‌گذاری اطلاعات در سرتاسر شهر هوشمند را برای مدیریت شهری بهتر ممکن ساخته است. (نظری، ۱۴۰۰: ۱۴)

- اینترنت اشیاء نظامی^۱

با وجود چالش‌های مربوط به پذیرش اینترنت اشیاء در حوزه نظامی، پتانسیل بالایی برای روزآمدسازی جنگ‌افزارها، استفاده از داده‌ها و خودکارسازی جهت حفظ جان سربازان و از طرف دیگر کاهش هزینه‌ها و افزایش کارایی وجود دارد. شنا سایی، کنترل و نظارت نیروها و جنگ‌افزارها از مهم‌ترین کاربردهای اینترنت اشیاء در حوزه نظامی است. (بدری، ۱۳۹۸: ۵)

اینترنت اشیاء به‌عنوان یک ارتباط سریع و بهتر بسیار سریع رشد می‌کند. استفاده از اینترنت اشیاء در کاربردهای نظامی به یک ضرورت تبدیل شده است. امروز جهان با افزایش فعالیت‌های ضد نظامی و تهدیدی برای ملت‌ها مواجه می‌شود. زندگی رزمندگان بارزش است؛ بنابراین مهم است که از زندگی آنها محافظت شود. ما می‌توانیم کنترل مهمات نظامی به‌عنوان یک بخش مهم و جدایی‌ناپذیر فعالیت‌های نظامی را از طریق فناوری اینترنت اشیاء انجام دهیم. (Vishal Gotarane, 2019: 1)

از آنجایی که کاربری اینترنت اشیاء در امور نظامی اهری نوظهور و در حال پیشرفت است، ارزیابی برنامه‌های فعلی نظامی و تجاری اینترنت اشیاء برای تعیین و ظایف تحقیقاتی مرتبط لازم به نظر می‌رسد. مهم‌ترین مزیت سامانه‌های اینترنت اشیاء در دسترس بودن تجهیزات و زیرساخت‌ها برای پیاده‌سازی طرح‌های عملیاتی است. (مینایی بیدگلی، ۱۳۹۷)

مدیریت آآمد نظامی^۲:

اینترنت اشیاء نظامی می‌تواند در لجستیک نظامی حمایت‌های اسلحه‌ها، نظارت بر محیط برای حمایت از تمام قابلیت سامانه (مبتنی بر اطلاعات) استفاده شود. به‌عنوان مثال اطلاعات جمع‌آوری شده توسط دستگاه‌های اینترنت اشیاء نظامی از شرایط محیطی، شرایط اسلحه‌ها و نیروهای خودی می‌تواند امکان نظارت بهتر بر محیط جنگ و همچنین ارسال نیروهای پشتیبانی برای جایگزینی اسلحه‌ها و نیروهای تلف شده را در برداشته باشد. (دوستی مطلق، ۱۴۰۰)

^۱ . MIOT (Military Internet Of Things)

^۲ . logistic managment

مدیریت آماد حوزه‌ای است که در آن معمولاً چندین حسگر در سطوح پایین در وزارت دفاع آمریکا استفاده شده است. اگرچه استفاده کنونی همچنان محدود به محیط‌های کنترل شده با دخالت زیرساخت‌ها در سناریوهای جنگی به منظور ارتقاء فرایندهای اینترنت اشیاء و انسان است. در برخی از ارتش‌ها از فناوری‌ها برای ردیابی، حمل و نقل و فناوری برجسب شناسایی فرکانس رادیویی زیرساختی در پس‌زمینه استفاده شده است. برای مثال، برجسب‌های مدیریت موجودی‌ها بین مراکز تدارکات و آمادگاه استفاده شده است. از کاربردهای عملی دیگری که برای بحث آماد و تأمین عملاً به کار گرفته شده است، نظارت و مدیریت ناوگان و تدارکات انفرادی است اینترنت اشیاء در صورتی که در ارتش فراگیر شود، امکان انتقال و گسترش زنجیره تأمین تا خود منطقه عملیاتی، وسایل نقلیه و حتی تا سطح سربازان را فراهم می‌کند. با استفاده از خودروهای هوشمند وضعیت کلی خودرو، میزان سوخت موجود، قطعات و اجزای آن را از راه دور می‌توان کنترل کرد و پیش از اتمام لوازم‌ذکی موردنیاز درخواست تأمین مجدد را ارسال نمود. همچنین با کمک سیستم‌های مشابه و با اشتراک‌گذاری اطلاعات امکان عرضه اقلام مهم در همان واحد بدون نیاز به پرس‌وجو فراهم می‌شود. سنسورهای متصل به اینترنت اشیاء می‌توانند علاوه بر نظارت بر علائم فرسودگی، صدور هشدار تعمیر و نگهداری، به طور بالقوه باعث کاهش موارد منجر به حادثه شوند. (مینایی بیدگلی، ۱۳۹۷)

پهپاد هوشمند

از کاربردهای دیگر اینترنت اشیاء، استفاده از آن در یک شبکه پهپاد (وسیله نقلیه بدون سرنشین) مبتنی بر کاربردهای نظامی است. در این مدل، مجموعه‌ای از چندین شبکه پهپاد را برای نظارت بر منطقه جغرافیایی و همچنین نظارت بر آنها برای اهداف امنیتی اختصاص می‌دهند. سیستم پیشنهادی همچنین دارای عملکرد رادار است. تنظیمات منحصربه‌فرد آنتن بر اساس مفهوم هدایت پرتو طراحی شده است به طوری که در چندین زاویه پرتو برای تشخیص سیگنال‌های ناخواسته تشکیل می‌شود. هر پهپاد به یکدیگر متصل است و از طریق اینترنت اشیاء کل شبکه از واحد کنترل، کنترل می‌شود. هر پهپاد دارای یک ماژول موقعیت‌یاب جهانی^۱ برای مکان فعلی پهپاد است و براین اساس داده‌های همه پهپاد توسط

^۱ . GPS

واحد کنترل، کنترل می‌شود و در پایگاه داده ذخیره می‌شود. مازول ارتباطی^۱ برای برقراری ارتباط از طریق اینترنت با پهپادهای دیگر و همچنین منطقه کنترل استفاده می‌شود. از پهپاد به غیر از برنامه‌های نظامی، می‌توان به عنوان وسیله‌ای برای کار چندمنظوره استفاده کرد. (Utsav, 2021)

سامانه‌های کنترل آتش^۲

سیستم‌های کاملاً خودکار در ارتش در منطقه آتش متمرکز شده‌اند. این سیستم‌ها از داده‌های حسگر برای واکنش سریع و ارائه دقت دقیق استفاده می‌کنند. به عنوان مثال، سیستم رزمی آگیس^۳ نیروی دریایی آمریکا، یک سیستم کنترل آتش یکپارچه برای کشتی‌های سطحی، دارای قابلیت‌های کنترل آتش کاملاً خودکار است. آگیس، فرماندهی و کنترل و همچنین کنترل تسلیحات را برای مجموعه کامل سلاح‌های کشتی‌های سطحی ایالات متحده، از توپخانه کشتی و اژدر گرفته تا موشک‌های کروز هدایت‌شونده تا سلاح‌های ضد موشک فراهم می‌کند. سیستم راداری AN/SPY می‌تواند مهمات هدایت شده را تا ۱۰۰ هدف در یک‌زمان کاملاً خودکار شناسایی، ردیابی و هدایت کند. ارتش برای استفاده از پهپادها برای درگیر شدن با اهداف ارزشمند سرمایه‌گذاری می‌کند. خلبانان ایستگاه‌های زمینی از دوربین‌ها و دیگر حسگرهای موجود در کابین خلبان به صورت کنترل شده برای پرواز هواپیما استفاده می‌کنند و گویی در کابین خلبان هستند. خلبانان با استفاده از ترکیبی از سنسورهای موجود در هواپیما و اطلاعات دریافتی از «سیستم توزیع مشترک زمینی»^۴، اهداف را شناسایی کرده و می‌توانند با موشک‌های هلفایر^۵ درگیر شوند، با استفاده از یک تعیین‌کننده لیزر، هدف خود را رنگ‌آمیزی می‌کنند و به سر جستجوگر موشک اجازه می‌دهد با دقت به هدف برخورد کند. مهمات نیز می‌تواند به شبکه متصل شود و به سلاح‌های هوشمند اجازه می‌دهد اهداف متحرک را ردیابی کرده یا در پرواز هدایت شوند. نمونه بارز آن موشک^۶ تامهاوک است، مهم‌ترین سلاح ضربه‌ای نیروی دریایی. نوع جدیدتر^۷ دارای یک پیوند ماهواره‌ای دوطرفه است که به موشک اجازه می‌دهد تا در حین پرواز به هدف جدید

1 . GSM

2 . fire control system

3 . Aegis

4 . Distributed Common Ground System (DCGS)

5 . Hellfire

6 . Tomahawk Land Attack Missile (TLAM)

7 . TLAM IV

هدایت شود یا بر فراز منطقه موردنظر بچرخد و فیلم را از دوربین آن به فرماندهان ارسال کند و به آنها اجازه دهد تا اهداف جدید را تعیین کنند و آسیب ناشی از حملات دیگر را ارزیابی کنند. همچنین می‌توان به موشک دستور داد که به هر هدف از پیش برنامه‌ریزی شده حمله کند یا مختصات جدید برای حمله ارائه دهد. (Denise & William, 2019: 16)

سنجش مشارکتی در میدان نبرد^۱

اینترنت اشياء در میدان جنگ یک فناوری نوآورانه است که شامل شبکه‌های سگرها، پوشیدنی‌ها و دستگاه‌های مرتبط می‌باشد. اینترنت اشياء به ایجاد یک نیروی جنگی منسجم و افزایش کارایی عملیاتی سیستم‌های نظامی در میدان نبرد کمک شایانی می‌کند. به عنوان مثال برای استفاده از محاسبات ابری و لبه و اتصال رزمندگان به فناوری هوشمند مانند زره، رادار، سلاح و سایر اشياء. اینترنت اشياء در نبرد های هوشمند واقعیت در حال ظهور در جنگ‌های آینده است. اینترنت اشياء برای ارتش تازگی ندارد. در دهه ۱۹۹۰، رهبران نظامی چشم‌اندازی را برای چگونگی تغییر شبکه‌ها و داده‌ها در نحوه جنگ ایجاد کردند. این مفهوم پایه و اساس "جنگ شبکه محور" را تشکیل داد. آنها مدلی از جنگ را بر اساس ادغام سه حوزه توصیف کردند: (۱) حوزه فیزیکی، جایی که وقایع رخ داده و عملیات انجام شده است داده‌هایی از سگرها و ناظران انسانی تولید می‌شود. (۲) حوزه اطلاعاتی که داده‌ها در آن منتقل و ذخیره می‌شوند. و (۳) حوزه شناختی، که در آن داده‌ها پردازش و تجزیه و تحلیل شده است. سه حوزه جنگ شبکه محور، مفهوم مدرن اینترنت اشياء را به طور کامل منعکس می‌کند ترکیبی از سگرها و دستگاه‌های تعبیه شده، اتصال به اینترنت، فناوری پایگاه داده و تجزیه و تحلیل نرم افزار. جنگ شبکه محور استفاده از فناوری های اینترنت اشياء در مأموریت های نظامی را حتی قبل از معرفی مفهوم اینترنت اشياء توضیح داد. دو ادعای فنی قانع کننده باعث توسعه سریع فناوری اینترنت اشياء می‌شود: هوش ماشینی و ارتباطات شبکه‌ای. اگر تجهیزات باهوش تر باشند، همه چیز کارآمدتر و موفق تر است و زمانی که بتوانند با یکدیگر ارتباط برقرار کنند این کارآمدی حتی بیشتر نیز خواهد شد. این منطبق

^۱ . collaborative sensing

یک سان در مورد همه اجسامی که در جهان رز می نظامی زندگی می کنند صدق می کند. عملیات نظامی مدرن با فناوری پیچیده، بسیار پویا و چند بعدی به هم پیوسته انجام می شود تا وابستگی به جنگجویان انسانی را کاهش دهد. در آینده اینترنت اشیا میدان نبرد، جنگنده های انسانی را به فناوری های هوشمند مانند زره، سلاح، رادار و سایر اشیا متصل می کند. (Lin et al., 2020)

پایش محیط^۱

امروزه اکثر کشورها از افزایش تروریسم فرامرزی، نفوذ و تهاجم مرزی شبه نظامیان مسلح و مهاجرت غیرقانونی رنج می برند. نظارت و حفاظت از مرزهای ملی در برابر این گونه تهدیدها مهم ترین مسئله برای هر کشوری بوده است. کشورهایی مانند هند دارای مرز ملی چند هزار کیلومتری هستند که با هفت کشور مشترک است. نظارت دستی بر چنین مرز بزرگی از نظر نیروی انسانی و مالی، هزینه بر می شود بیشتر قسمت های مرز کشورها با نرده های سیم خاردار محافظت می شود. با این حال، استقرار سیم خاردار در هر قسمت از چنین مرز وسیعی به دلیل توپوگرافی یا آب و هوای نامناسب امکان پذیر نیست. فناوری مدرن نظارت نیاز به زمان دارد. فناوری هایی مانند دیوار لیزری، سنسورهای حرارتی، حسگرهای تشخیص تونل، وسایل نقلیه هوایی بدون سرنشین در حال حاضر مدنظر است. به دلیل شرایط محیطی خصمانه در برخی از مناطق مرزی، انواع مختلف سیستم های نظارتی مورد نیاز است. (Priyank, 2021: 3 & Vijay)

فرماندهی و کنترل هوشمند

استفاده از فناوری اینترنت اشیا در مورد سیستم های مراکز فرماندهی و کنترل از مزایای بالاتری برخوردار است. سیستم های مراکز فرماندهی و کنترل از چندین میلیون حسگر در سیستم عامل های مختلف برای اطمینان از آگاهی موقعیتی توسعه یافته استفاده می کنند. شبکه بسیار پیچیده و گسترده شامل چندین میلیون حسگر (سنسورها در سیستم عامل های مختلف مانند هواپیماهای بدون سرنشین، رادارها، دوربین های فیلم برداری، سنسورهای مادون قرمز، سنسورهای زمینی بدون مراقبت، دستگاه های قابل حمل) داده های واقعی را برای نیروهای رزمی و تصمیم گیرندگان ارائه می دهد. این داده ها را

^۱ . surveillance

می‌توان برای تصویری مشترک از پشتیبانی از تصمیم‌گیری توسط فرماندهان، هماهنگی و کنترل بهتر در منطقه عملیاتی یکپارچه و استفاده کرد. در جریان درگیری‌ها و عملیات جستجوی نظامی، سربازان زخمی شده و گاهاً تلفات می‌یابند. ایستگاه پایگاه ارتش برای یافتن سربازان به یک کامپیوتر برای سیستم موقعیت‌یابی جهانی، یک ایستگاه پایه بی‌سیم برای تعیین معیارهای مربوط به سلامت برای سربازان و یک گیرنده بی‌سیم برای انتقال بی‌سیم داده‌ها برای یافتن و ارائه نظارت بر سلامتی برای سربازان نیاز دارد. هنگام ازدست‌رفتن منطقه نبرد، ایستگاه پایه باید فرد را راهنمایی کند. با ایستگاه پایه می‌توان به مکان فعلی سربازان در دستگاه دسترسی پیدا کرد. برای ردیابی سلامت و وضعیت فعلی از طریق سیستم موقعیت‌یابی جهانی، دستگاه پیشنهادی را می‌توان بر روی بدن سرباز سوار کرد. این داده‌ها از طریق اینترنت اشياء به اتاق کنترل منتقل می‌شوند. سیستم پیشنهادی همچنین شامل سیستم تشخیص است که از سنسورهای فرکانسی اضطراری استفاده می‌کند؛ بنابراین از این سیستم برای اجرای یک رویکرد کم‌هزینه برای نجات جان انسان‌های گران‌بها در میدان جنگ استفاده می‌شود.

(Vijay, 2020)

رباتیک در دفاع^۱

اتکای روزافزون نظامیان به رباتیک و سیستم‌های خودمختار (RAS)^۲ قرار است نحوه مبارزه با جنگ‌ها را به روش‌های اساسی تغییر دهد. پلتفرم‌های خودمختار که از سربازان انسانی پشتیبانی می‌کنند در حال حاضر در میدان هستند، بارهای سنگین را حمل می‌کنند، وسایل را به عقب و جلو می‌برند، به عنوان ایستگاه‌های شارژ باتری عمل می‌کنند و برای تخلیه پزشکی پشتیبانی می‌کنند. اگرچه اینها تنها بارزترین نمونه‌ها هستند. رباتیک و خودمختاری همچنین مستلزم رابط‌های انسان و ماشین مانند اسکلت‌های بیرونی هستند که اکنون قدرت، استقامت و آگاهی موقعیتی سربازان را افزایش می‌دهند. علاوه بر این، سرعت تصاعدی تحقیقات رباتیک در شبیه‌سازی رفتار انسان می‌تواند نهایتاً نیاز به استقرار انسان‌ها در خط مقدم را کاهش دهد یا به طور کامل حذف کند. این به طور کامل آستانه

1 . Robotics in defence

2 . Robotics and autonomous systems

مداخله نظامی را تغییر می‌دهد، زیرا قیمت سیاسی تلفات سربازان دیگر عاملی نخواهد بود. (دتراتی، ۲۰۲۱)

رباتیک و سیستم‌های خودمختار (RAS) در حال حاضر به طور گسترده در بسیاری از حوزه‌های عمرانی مورد استفاده قرار می‌گیرند، به ویژه از آنجایی که پیشرفت تکنولوژی آنها را ارزان‌تر و حجیم‌تر می‌کند و در عین حال انعطاف‌پذیرتر و تعامل با آنها را آسان‌تر می‌کند. به این ترتیب، ربات‌ها و سیستم‌های چند رباتی (یا ازدحام) (MRS)^۱ همچنین پتانسیل این را دارند که در آینده قابل پیش‌بینی، نقش مخربی را در عملیات نظامی ایفا کنند، به این معنا که به انجام وظایفی که امروزه بسیار خطرناک تلقی می‌شوند، اجازه می‌دهند برای انسان پیچیده یا حتی غیرممکن است. (همان)

تجهیزات و تسلیحات هوشمند^۲

وزارت دفاع ایالات متحده آمریکا پروژه‌های آغاز نموده است که فناوری‌های بسیار لازم برای جنگنده‌های نظامی و همچنین حتی موارد غیرنظامی را پیاده‌سازی می‌کند. برنامه‌های موبایل مجزا از طریق سرویس‌ها و آژانس‌های انفرادی و با استفاده از پلتفرم‌ها، پروتکل‌ها و ملزومات متفاوت توسعه داده می‌شوند. این برنامه‌ها تحت نظر افسر ارشد اطلاعات با یک کارگروه هماهنگ شده و می‌توانند اطلاعات را میان خود به اشتراک گذاشته و در مواقع موردنیاز بهترین واکنش و عمل را انجام دهند. بیش از یک دهه است که مبحث تحرک و سیار بودن تاکتیکی در حوزه نظامی توسعه داده شده است. برنامه جنگجوی زمینی که قبلاً به انجام رسیده است، چندین سال زمان صرف توسعه دستگاه‌های ایمن اندرویدی برای پیاده‌نظام و با استفاده از یک نسخه اختصاصی از سیستم‌عامل اندروید نموده است. این دستگاه‌ها که نسخه‌های اصلاح‌شده گوشی‌های هوشمند می‌باشند به رادیوی تفنگ‌دار با قابلیت اتصال داده متصل می‌شوند و هدفشان اتصال سربازان میدان نبرد به امکانات و برنامه‌هایی همچون نقشه‌های سه‌بعدی، ردیابی نیروها، ترجمه زبان‌ها و پروفایل اهداف ارزشمند می‌باشد. (Denise & William, 2019: 16)

1 . multi-robots systems

2 . smart equipments and weapons

از نگاه مطالعات اینترنت اشیاء، شهر هوشمند به صورت محیط شهری است که حسگرها و عامل‌های فراگیر در آن تعبیه شده و این تجهیزات به ارائه خدمات هم به شهروندان و هم به مدیریت شهری می‌پردازند. در محیط‌های بست‌های که دسترسی سیستم‌های اطلاعاتی موجود محدود است، زیرساخت‌های اینترنت اشیاء دسترس، در صورت وجود می‌توانند در جهت اجرای عملیات نظامی مورد استفاده قرار گیرند. به‌عنوان مثال از سنسورهای محیطی می‌توان در تشخیص وجود مواد شیمیایی خطرناک بهره برد یا با استفاده از حسگرهای نظارت رفتار انسانی برای تشخیص وجود فعالیت‌های مشکوک افراد در محیط عملیات استفاده کرد. بهره‌برداری از اطلاعات فراهم شده توسط زیرساخت‌های موجود در محیط ممکن است علاوه بر مزایایی که فراهم می‌کند خطرآفرین باشد. از جمله این خطرات می‌توان از خرابکاری در تجهیزات و یا نشر اطلاعات غلط و گمراه‌کننده نام برد. (مینایی بیدگلی، ۱۳۹۷: ۵)

سامانه‌های کنترل آتش^۱

سیستم‌های کاملاً خودکار در ارتش در منطقه آتش متمرکز شده‌اند. این سیستم‌ها از داده‌های حسگر برای واکنش سریع و ارائه دقت دقیق استفاده می‌کنند. به‌عنوان مثال، سیستم رزمی آگیس^۲ نیروی دریایی آمریکا، یک سیستم کنترل آتش یکپارچه برای کشتی‌های سطحی، دارای قابلیت‌های کنترل آتش کاملاً خودکار است. آگیس، فرماندهی و کنترل و همچنین کنترل تسلیحات را برای مجموعه کامل سلاح‌های کشتی‌های سطحی ایالات متحده، از توپخانه کشتی و اژدر گرفته تا موشک‌های کروز هدایت‌شونده تا سلاح‌های ضد موشک فراهم می‌کند. سیستم راداری AN/SPY می‌تواند مهمات هدایت شده را تا ۱۰۰ هدف در یک‌زمان کاملاً خودکار شناسایی، ردیابی و هدایت کند. ارتش برای استفاده از پهپادها برای درگیر شدن با اهداف ارزشمند سرمایه‌گذاری می‌کند. خلبانان ایستگاه‌های زمینی از دوربین‌ها و دیگر حسگرهای موجود در کابین خلبان به صورت کنترل شده برای پرواز هواپیما استفاده می‌کنند و گویی

^۱ . fire control system

^۲ . Aegis

در کابین خلبان هستند. خلبانان با استفاده از ترکیبی از سنسورهای موجود در هواپیما و اطلاعات دریافتی از «سیستم توزیع مشترک زمینی»^۱، اهداف را شناسایی کرده و می‌توانند با موشک‌های هلفایر^۲ درگیر شوند، با استفاده از یک تعیین‌کننده لیزر، هدف خود را رنگ‌آمیزی می‌کنند و به سر جستجوگر موشک اجازه می‌دهد با دقت به هدف برخورد کند. مهمات نیز می‌تواند به شبکه متصل شود و به سلاح‌های هوشمند اجازه می‌دهد اهداف متحرک را ردیابی کرده یا در پرواز هدایت شوند. نمونه بارز آن موشک^۳ تامهاوک است، مهم‌ترین سلاح ضربه‌ای نیروی دریایی. نوع جدیدتر^۴ دارای یک پیوند ماهواره‌ای دوطرفه است که به موشک اجازه می‌دهد تا در حین پرواز به هدف جدید هدایت شود یا بر فراز منطقه موردنظر بچرخد و فیلم را از دوربین آن به فرماندهان ارسال کند و به آنها اجازه دهد تا اهداف جدید را تعیین کنند و آسیب ناشی از حملات دیگر را ارزیابی کنند. همچنین می‌توان به موشک دستور داد که به هر هدف از پیش برنامه‌ریزی شده حمله کند یا مختصات جدید برای حمله ارائه دهد. (Denise & William, 2019: 16)

دفاع مبتنی بر هوش مصنوعی (هوش مصنوعی نظامی)

به نظر می‌رسد که سمبل دوران فراصنعتی و نماد فرآورده‌های بی‌همتای قرن آینده «هوش مصنوعی» است. هوش مصنوعی را کوشش‌هایی تعریف می‌کنند که در پی ساختن نظام‌های رایانه‌ای (سخت‌افزار و نرم‌افزار) است که رفتاری انسان‌وار داشته باشند. چنین نظام‌هایی توان یادگیری زبان‌های طبیعی، انجام وظیفه‌های انسانی به صورت آدمواره (ربات) و رقابت با خبرگی و توان تصمیم‌گیری انسان را دارند. (حاج قاسم و همکاران، ۱۴۰۰: ۲) همان‌طور که پروفیسور استیون هاوکینگ^۵ گفت: "ظهور هوش مصنوعی قدرتمند، بهترین یا بدترین چیزی خواهد بود که برای بشریت اتفاق افتاده است. (Bistron, 2021: 14) به گفته رییس‌جمهور روسیه (ولادیمیر پوتین) «هر کسی که در آینده رهبر این حوزه شود بر همه جهان حاکم خواهد شد». (سازمند، ۱۳۹۸: ۱۸) هوش مصنوعی می‌تواند قابلیت-

1 . Distributed Common Ground System (DCGS)

2 . Hellfire

3 . Tomahawk Land Attack Missile (TLAM)

4 . TLAM IV

5 . Stephen Hawking

های تحرک یگان نظامی را از طریق تشخیص هدف^۱، سیستم‌های سلاح خودکار^۲، ابزارهای حمایتی و برنامه‌ریزی^۳، بهبود بخشید. این فناوری در همه زمینه‌های نظامی (زمین، دریا، هوا، فضا، اطلاعات) و در تمام سطوح دفاعی (سیاسی، راهبردی، عملیاتی و تاکتیکی) کاربرد دارد. هوش مصنوعی و ارتباط آن با شبکه جهانی اینترنت، هسته اصلی فناوری اطلاعات در بخش دفاعی تلقی می‌شود. به همین دلیل موضوعی تحت عنوان حاکمیت هوش مصنوعی مطرح شده است که بر متغیرهایی همانند پویایی‌های رقابت نظامی، نابرابری‌های اجتماعی و اقتصادی، آگاهی‌های عامه مردم و پیش تمرکز کرده است. (Perry & Uuk, 2019)

کاربردهای نوین هوش مصنوعی از داده‌کاوی، رباتیک و پردازش زبان طبیعی فراتر رفته و حیطه‌هایی همانند مراقبت نظامی، شناسایی، ارزیابی تهدید، مین‌گذاری زیر آب، امنیت سایبری، آنالیز هوشمند، فرماندهی و کنترل، و آموزش دربرمی‌گیرد. (Svenmarck et al, 2018)

داده‌ها در خصوص سطح سرمایه‌گذاری در زمینه هوش مصنوعی در منطقه محدود است. مطابق با آمار مکنزی^۴ شرکت‌ها بین ۲۰ تا ۳۰ میلیارد دلار در سال ۲۰۱۶ در این حوزه در جهان سرمایه‌گذاری کرده‌اند. غول‌های فناوری مانند علی‌بابا، آمازون، بایدو، فیس بوک و گوگل تا امروز بیش از سه چهارم کل سرمایه‌گذاری را در حوزه هوش مصنوعی انجام داده‌اند. (ESCAP, 2018: 3)

(ب) مطالعات میدانی

برای جمع‌آوری داده‌های تحقیق، علاوه بر جمع‌آوری به روش کتابخانه‌ای، از روش میدانی با ابزار مصاحبه نیز بهره گرفته شد. لذا جمع‌بندی مصاحبه با صاحب‌نظران در خصوص مؤلفه‌ها و شاخص‌های اثرگذار در رابطه با موضوع تحقیق به شرح ذیل عبارتند از:

- 1 . Target detection
2. Autonomous weapon systems
- 3 . planning and support tools
- 4 . Mackinsey

(۱) مؤلفه‌ها

- مراکز فرماندهی و کنترل هوشمند
- مراکز داده
- مراکز سوئیچینگ
- فناوری اطلاعات و ارتباطات
- هوش مصنوعی
- تسلیحات و سامانه‌های هوشمند
- شبکه‌های حسگری اپتیکی و فرکانسی

(۲) شاخص‌ها

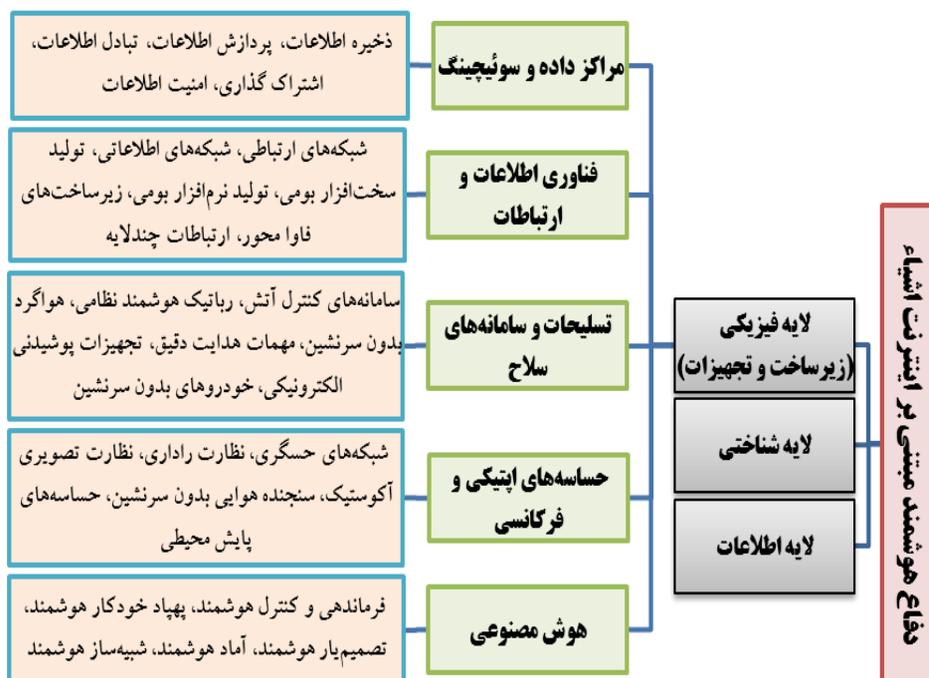
- میزان امنیت و پایداری زیرساخت‌های دفاعی
- میزان بکارگیری فناوری‌های مرتبط با مباحث الکترونیکی و فضای الکترومغناطیس
- شبکه‌های ارتباطی و مخابراتی جهت تبادل و پردازش اطلاعات
- میزان هوشمندسازی سلاح‌ها و تجهیزات زمینی، دریایی و هوایی
- تعداد سامانه‌ها و تسلیحات در رابطه با کنترل آتش هوشمند در صحنه نبرد میدانی
- میزان بکارگیری فناوری‌های مرتبط با هوش مصنوعی و یادگیری ماشینی
- نحوه امنیت مطلوب در تبادل اطلاعات
- روش برقراری ارتباطات چندلایه
- نوع تجهیزات و متعلقات همراه با سرباز (سربازان هوشمند آینده)
- تجهیزات و ریزساخت‌های مرتبط با مدیریت صحنه نبرد
- نحوه پردازش اطلاعات، ذخیره اطلاعات و پردازش اطلاعات
- روش اشتراک‌گذاری اطلاعات مابین عناصر موجود در صحنه نبرد
- نحوه ایجاد و برقراری شبکه‌های حسگری و بهره‌برداری از این شبکه‌ها در هوشمندی دفاع
- میزان بهره‌برداری مناسب و به‌موقع از شبکه‌های ارتباطی و اطلاعاتی
- میزان تولید سخت‌افزارها و نرم‌افزارهای بومی

- میزان بهره‌برداری از رباتیک هوشمند نظامی در ارتقاء توانمندی‌های دفاعی
- میزان بهره‌گیری از فناوری‌های نوین در هوشمندی آماد دفاعی
- تعداد استفاده از خودروهای بدون سرنشین در نبرد

چارچوب مفهومی:

چارچوب مفهومی نوعی نمودار سازی برای متغیرهای است که از چارچوب نظری تحقیق استخراج شده است. (بیک، ۱۳۹۵: ۲۷۳) چارچوب مفهومی باید ۱- پاسخ به سؤالات تحقیق را به‌طور اجمال از نگاه محقق بیان کند، ۲- روابط بین متغیرهای تحقیق را مشخص کند. ۳- قابلیت سنجش در پرسشنامه‌های تحقیق را داشته باشد. (همان)

از آنجایی که محققین در این تحقیق به دنبال کشف مؤلفه و شاخص‌های زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح می‌باشند؛ لذا پس از بررسی ادبیات نظری، اسناد و مدارک و نظر خبرگان مؤلفه‌ها استخراج و شاکله چارچوب نظری تحقیق شکل گرفت. در مرحله بعد محقق متناسب با چارچوب نظری تحقیق محیط‌شناسی را انجام داده و زمانی که با کمبود ادبیات و اسناد و مدارک مواجه شد با مصاحبه با افراد متخصص علوم دفاعی راهبردی و علوم سایبری، این نقیصه را برطرف تا سرانجام شاخص‌های تحقیق مطابق با شکل شماره (۲) احصاء گردید.

شکل شماره (۲): چارچوب مفهومی^۱

۳- روش تحقیق

این پژوهش کاربردی با روش‌های توصیفی - تحلیلی و زمینه‌ای - موردی به انجام رسیده است. نوع پژوهش توسعه‌ای بوده و از طرف دیگر پژوهش حاضر در پی یافتن مؤلفه‌ها و شاخص‌های زیرساخت و تجهیزات اینترنت اشیا مؤثر بر هوشمندی دفاع نیروهای مسلح است؛ بنابراین پژوهش از این منظر کاربردی محسوب گردیده و در مجموع توسعه‌ای - کاربردی است. برای گردآوری اطلاعات از روش کتابخانه علمی و تخصصی، سایت‌های معتبر اینترنتی، همچنین روش میدانی شامل مصاحبه با خبرگان و تنظیم پرسشنامه استفاده شد. جامعه آماری تحقیق از افرادی است که دارای تجارب و سوابق مطالعاتی و

تحقیقاتی در حوزه‌های علوم دفاعی راهبردی و سایبری برخوردارند که با برآورد صورت گرفته ۷۰ نفر می‌باشند که به صورت تمام شمار به آن‌ها مراجعه شده است. تجزیه و تحلیل اطلاعات با به کارگیری آمارهای توصیفی و استنباطی بوده و تحلیل آماری یافته‌های تحقیق، آزمون روائی و همچنین آزمون-های پایایی با استفاده از نرم افزار Smart PLS انجام گردید.

۴- تجزیه و تحلیل یافته‌های تحقیق

سؤال تحقیق: مؤلفه‌ها و شاخص‌های زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر دفاع هوشمند نیروهای مسلح کدامند؟

جدول شماره (۱): تجزیه و تحلیل داده‌های تحقیق

P Values	شاخص‌ها	بار عاملی	مؤلفه‌ها (مضامین سازمان دهنده)	ضریب مسیر	بعد (مضمون فراگیر)
۰/۰۰۰	ذخیره اطلاعات	۰/۷۸۶	مراکز داده و سوئیچینگ	۰/۷۶۸	زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاعی نیروهای مسلح
	پردازش اطلاعات	۰/۷۴۶			
	تبادل اطلاعات	۰/۸۰۰			
	اشتراک گذاری	۰/۷۲۱			
	امنیت اطلاعات	۰/۷۵۹			
۰/۰۰۰	شبکه‌های ارتباطی	۰/۸۸۴	فناوری اطلاعات و ارتباطات	۰/۶۷۹	
	شبکه‌های اطلاعاتی	۰/۷۶۸			
	تولید سخت افزار بومی	۰/۷۷۵			
	تولید نرم افزار بومی	۰/۷۱۰			
	زیرساخت‌های فاوا محور	۰/۷۵۶			
	ارتباطات چندلایه	۰/۸۷۱			

۰/۰۰۰	سامانه‌های کنترل آتش	۰/۷۷۷	تسلیحات و سامانه‌های سلاح	۰/۷۳۰
	رباتیک هوشمند نظامی	۰/۷۹۶		
	هواگرد بدون سرنشین	۰/۷۸۶		
	مهمات هدایت دقیق	۰/۹۰۰		
	تجهیزات پوشیدنی الکترونیکی	۰/۷۲۱		
	خودروهای بدون سرنشین	۰/۷۵۹		
۰/۰۰۰	شبکه‌های حسگری	۰/۷۶۵	حساسه‌های اپتیک و فرکانسی	۰/۸۱۳
	نظارت راداری	۰/۸۱۶		
	نظارت تصویری آکوستیک	۰/۸۱۱		
	سنجنده هوایی بدون سرنشین	۰/۹۲۰		
	حساسه‌های پایش محیطی	۰/۹۸۴		
۰/۰۰۰	فرماندهی و کنترل هوشمند	۰/۸۸۴	هوش مصنوعی	۰/۷۸۴
	پهپاد خودکار هوشمند	۰/۸۴۰		
	تصمیم‌یار هوشمند	۰/۹۸۰		
	آآمد هوشمند	۰/۹۶۲		
	شبیه‌ساز هوشمند	۰/۸۹۷		

جدول بالا بیانگر آن است که:

۱. مؤلفه مراکز داده و سوئیچینگ: با ضریب مسیر $0/768$ بر بعد زیرساخت و تجهیزات اینترنت اشياء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر بوده و با توجه به مقدار P Values که $0/000$ می‌باشد، این مسیر با اطمینان $0/99$ معنادار می‌باشد. همچنین این مؤلفه توسط پنج شاخص تبیین شده که بار عاملی هر کدام از شاخص‌ها بیشتر از 0.7 بوده و لذا هر یک از شاخص‌ها از قدرت تبیین خوبی برای این مؤلفه برخوردارند.

۲. مؤلفه فناوری اطلاعات و ارتباطات: با ضریب مسیر $0/679$ بر بعد زیرساخت و تجهیزات اینترنت اشياء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر بوده و با توجه به مقدار P Values که $0/000$ می‌باشد، این مسیر با اطمینان $0/99$ معنادار می‌باشد. همچنین این مؤلفه توسط شش شاخص تبیین شده که بار عاملی هر کدام از شاخص‌ها بیشتر از 0.7 بوده و لذا هر یک از شاخص‌ها از قدرت تبیین خوبی برای این مؤلفه برخوردارند.

۳. مؤلفه تسلیحات و سامانه‌های سلاح: با ضریب مسیر $0/730$ بر بعد زیرساخت و تجهیزات اینترنت اشياء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر بوده و با توجه به مقدار P Values که $0/000$ می‌باشد، این مسیر با اطمینان $0/99$ معنادار می‌باشد. همچنین این مؤلفه توسط شش شاخص تبیین شده که بار عاملی هر کدام از شاخص‌ها بیشتر از 0.7 بوده و لذا هر یک از شاخص‌ها از قدرت تبیین خوبی برای این مؤلفه برخوردارند.

۴. مؤلفه حساسه‌های اپتیکی و فرکانسی: با ضریب مسیر $0/813$ بر بعد زیرساخت و تجهیزات اینترنت اشياء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر بوده و با توجه به مقدار P Values که $0/000$ می‌باشد، این مسیر با اطمینان $0/99$ معنادار می‌باشد. همچنین این مؤلفه توسط شش شاخص تبیین شده که بار عاملی هر کدام از شاخص‌ها بیشتر از 0.7 بوده و لذا هر یک از شاخص‌ها از قدرت تبیین خوبی برای این مؤلفه برخوردارند.

۵. مؤلفه هوش مصنوعی: با ضریب مسیر $0/784$ بر بعد زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر بوده و با توجه به مقدار P Values که $0/000$ می باشد، این مسیر با اطمینان $0/99$ معنادار می باشد. همچنین این مؤلفه توسط شش شاخص تبیین شده که بار عاملی هر کدام از شاخص ها بیشتر از $0/7$ بوده و لذا هر یک از شاخص ها از قدرت تبیین خوبی برای این مؤلفه برخوردارند.

۵- نتیجه گیری

نتیجه تجزیه و تحلیل داده های تحقیق برای پاسخ به سؤال تحقیق (مؤلفه ها و شاخص های زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح کدامند؟) به شرح ذیل است:

– مؤلفه مراکز داده و سوئیچینگ: این مؤلفه با ضریب مسیر $0/768$ و سطح اطمینان 99% بر بعد زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر و معنادار است. همچنین این مؤلفه توسط ۵ شاخص سنجیده می شود که بار عاملی هر کدام از شاخص ها بیشتر از $0/7$ بوده و لذا هر کدام از شاخص ها از قدرت سنجش خوبی برای این مؤلفه برخوردارند. این ۵ شاخص عبارت است از:

✓ ذخیره اطلاعات

✓ پردازش اطلاعات

✓ تبادل اطلاعات

✓ اشتراک گذاری

✓ امنیت اطلاعات

– مؤلفه فناوری اطلاعات و ارتباطات: این مؤلفه با ضریب مسیر $0/679$ و سطح اطمینان 99% بر بعد زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر و معنادار است. همچنین این مؤلفه توسط ۶ شاخص سنجیده می شود که بار عاملی هر کدام از شاخص ها

بیشتر از ۰.۷ بوده و لذا هر کدام از شاخص‌ها از قدرت سنجش خوبی برای این مؤلفه برخوردارند. این ۶ شاخص عبارت است از:

- ✓ شبکه‌های ارتباطی
- ✓ شبکه‌های اطلاعاتی
- ✓ تولید سخت‌افزار بومی
- ✓ تولید نرم‌افزار بومی
- ✓ زیرساخت‌های فاوا محور
- ✓ ارتباطات چندلایه

– مؤلفه تسلیحات و سامانه‌های سلاح: این مؤلفه با ضریب مسیر ۰/۷۳۰ و سطح اطمینان ۹۹٪ بر بعد زیرساخت و تجهیزات اینترنت اشیا مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر و معنادار است. همچنین این مؤلفه توسط ۶ شاخص سنجیده می‌شود که بار عاملی هر کدام از شاخص‌ها بیشتر از ۰.۷ بوده و لذا هر کدام از شاخص‌ها از قدرت سنجش خوبی برای این مؤلفه برخوردارند. این ۶ شاخص عبارت است از:

- ✓ سامانه‌های کنترل آتش
- ✓ رباتیک هوشمند نظامی
- ✓ هواگرد بدون سرنشین
- ✓ مهمات هدایت دقیق
- ✓ تجهیزات پوشیدنی الکترونیکی
- ✓ خودروهای بدون سرنشین

– مؤلفه حساسه‌های اپتیکی و فرکانسی: این مؤلفه با ضریب مسیر ۰/۸۱۳ و سطح اطمینان ۹۹٪ بر بعد زیرساخت و تجهیزات اینترنت اشیا مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر و معنادار است. همچنین این مؤلفه توسط ۵ شاخص سنجیده می‌شود که بار عاملی هر کدام از شاخص‌ها

بیشتر از ۰.۷ بوده و لذا هر کدام از شاخص‌ها از قدرت سنجش خوبی برای این مؤلفه برخوردارند. این ۵ شاخص عبارت است از:

- ✓ شبکه‌های حسگری
- ✓ نظارت راداری
- ✓ نظارت تصویری آکوستیک
- ✓ سنجنده هوایی بدون سرنشین
- ✓ حساسه‌های پایش محیطی

– مؤلفه هوش مصنوعی: این مؤلفه با ضریب مسیر ۰/۷۸۴ و سطح اطمینان ۹۹٪ بر بعد زیرساخت و تجهیزات اینترنت اشیاء مؤثر بر هوشمندی دفاع نیروهای مسلح مؤثر و معنادار است. همچنین این مؤلفه توسط ۵ شاخص سنجنده می‌شود که بار عاملی هر کدام از شاخص‌ها بیشتر از ۰.۷ بوده و لذا هر کدام از شاخص‌ها از قدرت سنجش خوبی برای این مؤلفه برخوردارند. این ۵ شاخص عبارت است از:

- ✓ فرماندهی و کنترل هوشمند
- ✓ پهپاد خودکار هوشمند
- ✓ تصمیم‌یار هوشمند
- ✓ آآمد هوشمند
- ✓ شبیه‌ساز هوشمند

منابع و مأخذ:

- قرآن کریم، ترجمه و تفسیر آیت الله مکارم شیرازی
- حضرت امام خمینی (رحمت الله علیه)، صحیفه نور، ج ۱۶ و ج ۲۲، تهران، موسسه تنظیم و نشر آثار امام (رحمت الله علیه)
- حضرت امام خامنه‌ای (مدظله العالی)، مجموعه بیانات، قابل دسترسی در: www.khamenei.ir
- باقری‌منش، محمد، غلامی، محمود، کاویانی، حسن، امکان‌سنجی پیاده‌سازی فناوری اینترنت اشیاء در آماد یک سازمان دفاعی، نشریه علوم و فنون نظامی، شماره ۴۸
- نظری، اسفندیار (۱۴۰۰)، کاربرد اینترنت اشیاء در توسعه مدیریت شهری، فصلنامه پژوهش‌های نوین علوم جغرافیایی، معماری و شهرسازی، شماره سی‌ام
- دهقی، رسول (۱۳۹۹)، رساله: طرح راهبردی کاربردی مفهوم اینترنت اشیاء در حوزه نظامی (مطالعه موردی قرارگاه پدافند هوایی خاتم‌الانبیاء (ص) آجا، دانشگاه عالی دفاع ملی
- زبینه، حسین (۱۳۹۹)، دستور کار پژوهش در مورد خط‌مشی در حوزه حکمرانی اینترنت اشیاء، فصلنامه سیاست‌نامه علم و فناوری، دوره ۱۰، شماره ۳
- شهبازی، محمد، جهانیان، مجتبی، سیفی، علی (۱۳۹۸)، امنیت اینترنت اشیاء، هفتمین کنفرانس ملی علوم، مهندسی و فناوری اطلاعات
- قیصری، محمد، هنرمند، مریم، وحدت، داود، (۱۳۹۹)، کاربرد فناوری اینترنتی از اشیاء در توسعه مدیریت لجستیک، www.IOTiran.com
- کازرونی، حنیف (۱۳۹۹) مطالعه علوم فناوریهای دفاعی - امنیتی آینده و بررسی همگرایی آنان، فصلنامه آماد و فناوری دفاعی - سال سوم شماره هفتم، مرکز تحقیقات راهبردی دفاعی، دانشگاه عالی دفاع ملی
- محمدعلی‌زاده، اکبر، باقری، حسین (۱۳۹۷)، دفاع هوشمند؛ مفهوم جدید در راهبرد امنیتی ناتو تا سال ۲۰۲۰، فصلنامه مطالعات بین‌رشته‌ای دانش راهبردی، سال هشتم، شماره ۳۰
- بدری، رامین (۱۳۹۸)، کاربردها و چالش‌های مورد بحث در اینترنت اشیاء، کنفرانس بین‌المللی پیشرفت‌های اخیر در علوم اطلاعات، مهندسی و فناوری

- Bognar Eszter Katalin, possibilities and security challenges of using iot for military purposes, 2018, www.researchgate.net
- Lin Zhu, Suryadipta Majumdar, Chinwe Ekenna (2020), An invisible warfare with the internet of battlefield things: A literature review, <https://doi.org/10.1002/hbe2.231>
- Madhiarasan, M. Design and development of IoT based solar powered versatile moving robot for military application. Int J Syst Assur Eng Manag 12, 437–450 (2021). <https://doi.org/10.1007/s13198-021-01089-9>
- Ploennigs, Joern John Cohn, and Andy Stanford-Clark, IBM(2018) IEEE Internet of Things Magazine • September 2018

