فصلنامه مطالعات دفاعی استراتژیک
سال بیست و یکم، شماره ۹۲، تابستان ۱۴۰۲
مقاله چهارم، از صفحه ۶۹ تا ۹۲

مقاله پژوهشی: الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء

محمدرضا موحدی صفت[۱]، محمد سپهری[۲]، خداداد هلیلی[۳]، عادل فرزانه[۴]

دریافت مقاله: ۱۴۰۱/۱۲/۰۹ **پذیرش مقاله: ۱۰ /۱۴۰۲/۰۲**

چکیده

امروزه با پیشرفت‌های بشر در زمینه دانش و فناوری، شاهد تحولات شگرف در حوزه‌های مختلف به‌ویژه در حوزه دفاعی هستیم. با بهره‌گیری مناسب و به‌موقع از فناوری‌های نوین از جمله فناوری اینترنت اشیاء در دفاع هوشمند، تا حدود زیادی می‌توان امور متنوع نظامی را بادقت بیشتر و پویاتری پیاده‌سازی نموده تا بحث هوشمندی تجهیزات محقق گردد. با به‌کارگیری اینترنت اشیاء در فرماندهی و کنترل هوشمند، آماد هوشمند، ترابری هوشمند، پایش محیطی، آموزش و شبیه‌سازی و... می‌توان به قابلیت‌های دفاعی نوین و اثربخش و درواقع به دفاعی هوشمند در برابر تهدیدات نوین و هوشمند دست یافت. پژوهش حاضر با عنوان «ارائه الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء» و با روش توصیفی - تحلیلی و رویکرد آمیخته (کمی و کیفی) انجام شده است. در این تحقیق، از نظرات ۷۰ نفر از فرماندهان، مدیران و کارشناسان حوزه علوم دفاعی راهبردی و سایبری کشور در قالب پرسشنامه استفاده شده است. بر اساس پژوهش انجام شده و با استفاده از نظر خبرگان شش مفهوم زیرساخت و تجهیزات، سرویس و خدمات، ساختار و سازمان، دانش و اطلاعات، امنیت و مدیریت و حکمرانی به مثابه ابعاد اساسی دفاع هوشمند مبتنی بر اینترنت اشیاء و ۴۰ مؤلفه ارائه گردیده است.

واژگان کلیدی: دفاع، دفاع هوشمند، اینترنت اشیاء

[۱] استادیار دانشگاه عالی دفاع ملی
[۲] استادیار دانشگاه پدافند هوائی خاتم الانبیاء (صل‌الله‌علیه‌وآله‌وسلم)
[۳] استادیار دانشگاه هوائی شهید ستاری
[۴] دکتری علوم دفاعی راهبردی دانشگاه عالی دفاع ملی(نویسنده مسئول) adelfarzaneh313@gmail.com

مقدمه

اهمیت دفاع هوشمند در کنار مفاهیم جدیدی همچون «قدرت هوشمند»، «تهدیدات هوشمند» «جنگ هوشمند» و «ارتش هوشمند» بیشتر نمایان می‌گردد. در اجلاس شیکاگو (ژوئن ۲۰۱۲ میلادی) کشورهای عضو ناتو بر روی رویکرد جدید راهبردی که بر اساس ارزیابی‌های جدید و به‌روز شده از محیط امنیتی و الهام از مفاد مفهوم نوین راهبردی حاصل شده بود، توافق نموده و راهبرد «دفاع هوشمند» را محور اصلی این رویکرد جدید به‌عنوان یکی از راهبردهای دفاعی ناتو برای دهه آینده اعلام نمودند.

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 اشیاء، 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 اشیاء متشکل از حسگرها، سیستم شناسایی و ردیابی خودکار، ارتباطات بی‌سیم، دسترسی به شبکه و سیستم‌های توزیع‌شده می‌باشد. اهمیت ایجاد تحول در راهبردهای دفاعی و تغییرات اساسی در سبک‌های نظامی و دفاعی بر کسی پوشیده نیست. در ساختار دفاعی و نظامی سازمان‌های نظامی در سال‌های اخیر تحولات روبه رشدی به وجود آمده است؛ ولی چیزی که مسلم است این تحولات و ساختار دفاعی می‌بایست علاوه بر کسب آمادگی جهت مقابله با دشمنان منطقه‌ای، در برابر تهدیدات دشمنان فرامنطقه‌ای نیز آماده مقابله باشد. اینترنت اشیاء یک ایده جهانی برای اتصال همه اشیاء به یکدیگر است. ظهور اینترنت اشیاء 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 اشیاء نظامی[1] که درواقع مُدل 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.

در صورت بهره‌برداری مؤثر از این فناوری در مراکز فرماندهی و کنترل هوشمند[2] که نقش به سزایی در مدیریت صحنه نبرد به عهده داشته و محور اصلی در جنگ‌های آینده خواهد بود، بر عناصر زمینی، هوایی، دریایی و پدافندی موجود در صحنه نبرد میدانی و بازیگران شرکت‌کننده در صحنه جنگ ازجمله تجهیزات جنگی و تسلیحات زمینی، سایت‌ها و مواضع موشکی، هواپیماهای

1 MIoT: Military Internet of Things
2 Smart Command and Control

باسرنشین و بدون سرنشین، شناورهای سطحی و زیرسطحی و... اشرافیت کامل خواهد داشت. به‌کارگیری اینترنت اشیاء در کنترل سلاح (سامانه کنترل آتش[1])، پایش محیط[2]، تسلیحات هوشمند[3]، مدیریت صحنه نبرد[4]، سنجش مشارکتی در میدان نبرد[5]، سامانه آماد و زنجیره تأمین هوشمند، پایش سلامت و بهداشت[6]، آموزش و شبیه‌سازی، مدیریت هوشمند ناوگان خودرویی، یک سازمان نظامی را قادر می‌کند تا به قابلیت‌های دفاعی نوین و اثربخش و درواقع به دفاعی هوشمند دست پیدا نماید.

ازآنجایی‌که تاکنون الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء به‌صورت علمی تدوین و ارائه نشده است در نتیجه هدف از این تحقیق ارائه الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء و سؤال تحقیق به این صورت است که ابعاد، مؤلفه‌ها و شاخص‌های دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء کدام‌اند و چه روابطی بین آنها وجود دارد؟

مبانی نظری

الف– پیشینه‌شناسی

تحقیقی با عنوان «طرح راهبردی کاربست مفهوم اینترنت اشیاء در حوزه نظامی» توسط رسول رمضانی دهقی انجام شده است که نویسنده در نتیجه‌گیری تحقیق خود چنین آورده است: اینترنت اشیاء در حوزه نظامی به اتصال و ارتباط گسترده تجهیزات و دارایی‌های فیزیکی و کارکنان نظامی از طریق یک شبکه اینترنت نظامی و با بهره‌گیری از ابزارهای موجود در فناوری‌های اینترنتی (شناسه‌های فرکانس رادیویی، حسگرها، ابزارهای برقراری ارتباط ماشین با ماشین و غیره) اشاره دارد به نحوی که تعامل و همکاری این اشیاء و افراد به ارتقاء بهره‌وری در بخش‌های مختلف سازمان نظامی منجر شود. بر اساس تجزیه و تحلیل نقاط قوت و ضعف محیط داخلی و فرصت‌ها و تهدیدهای به دست آمده از محیط خارجی مبتنی بر ماتریس سوات، تعداد ۱۰ راهبرد به دست آمد. (رمضانی دهقی، ۱۳۹۹)

تحقیق دیگری با عنوان «همگرایی اینترنت اشیاء نظامی و پزشکی و چالش‌های امنیتی» توسط منصور فرزین‌فرد و محمدرضا کریمی قهرودی انجام شده است. در نتایج این مقاله آمده است:

---

[1] Fire control system
[2] Surveilance
[3] Smart weapons
[4] Battlefield monitor
[5] Collaborative sensing
[6] Health monitoring

کاربرد اینترنت اشیا در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی بخش نظامی محسوب می‌گردد. با توجه به اهمیت سلامتی و جان نیروهای نظامی در صحنه نبرد ظهور اینترنت اشیاء پزشکی جهت تکمیل سامانه‌های نظارتی فرماندهی و کنترل امری اجتناب‌ناپذیر خواهد بود. این امر با تجهیز سربازان به حسگرهای هوشمند، پارامترهای فیزیولوژیکی بدن از قبیل دمای بدن، ضربان قلب، فشار خون، سطح قند، نبض، سیگنال‌های قلبی و مغزی و غیره جمع آوری وارسال داده‌ها جهت رصد و پایش به مرکز فرماندهی و کنترل سلامت میسر می-گردد. همگرایی اینترنت اشیاء نظامی با اینترنت اشیاء پزشکی در صحنه نبرد، قابلیت‌های جدید و ارتقا یافته ای را ایجاد می‌نماید و می‌تواند هم‌افزایی و بهره‌وری در صحنه نبرد را به ارمغان آورده و اثربخشی اقدامات و یکپارچگی در سامانه‌های فرماندهی و کنترل را افزایش دهد. (فرزین‌فرد و همکار، ۱۳۹۹)

در تحقیق دیگری که توسط خسرو حسن‌لو با عنوان «نظریهٔ دفاع هوشمند در سپهر اندیشه‌های دفاعی» انجام گردیده است، نویسنده در پژوهش خود به این نتایج رسیده است: دفاع هوشمند تلفیقی از قدرت‌های سخت نظامی و اقتصاد و نرم فرهنگی، معنوی و... است. دفاع معنوی دفاعی حقیقی است و این دفاع ناشی از اعتقاد، ایمان و صبر و استقامت است. دفاع در ابعاد ظاهری و مادی بدون توجه به بعد باطنی شامل (عقلانی و معنوی) امکان‌پذیر نیست. دفاع در همه ابعاد (ظاهری، عقلانی و معنوی) نیازمند به‌کارگیری هم‌زمان قوای مادی، عقلانی و معنوی است. دفاعی که فاقد هر یک از این ابعاد باشد. تک‌وجهی، فروگذار، ناکارآمد و فاقد ذکاوت و اثربخشی لازم خواهد بود. (حسن‌لو، ۱۳۹۵)

ب- مفهوم‌شناسی

مفهوم الگو: الگو نمونه‌ای اقتباس شده از مسائل عینی و واقعی است که روابط بین متغیرها را نشان می‌دهد و پیش‌بینی را ساده می‌کند. (الوانی، به نقل از همان)

مدل و الگو یک نمونه ساده شده از واقعیت است. تمام الگوها انتزاعی و خیالی هستند و برخی از عوامل در آنها وارد می‌شوند و برخی دیگر خارج نگه‌داشته می‌شوند. الگوها و مدل‌ها می‌توانند شامل تصویرهای ذهنی، نمایش‌های گرافیکی، نمایش‌های بیانی و یا نمایش‌های ریاضی از واقعیت باشند. پس الگوها و مدل‌ها ضمن تفاوت‌های نسبت به یکدیگر، اشاره ضمنی به تصویر ایستای واقعیت می‌کنند. (لطفیان، به نقل از همان) الگو در این تحقیق عبارت است از ابعاد، مؤلفه و شاخص‌هایی که بتواند دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء را نشان دهد.

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، ۱۳٤٥: ٥٦٢) 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 پادکـنش در برابر آسیب‌های منافع، امنیت و یا هستی موجودات زنده است.

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) 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 تجمیع 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، فرانظامی، 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 آگاهی‌محور، شناخت محور، تأثیر محور، غیرعامل و ناهمگون) است. تلفیقی کارآمد از رویکردهای ناهمگونی، تأثیر محوری، شناخت محوری، غیرعامل بودن، مجازی بودن به‌گونه‌ای 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 گرانیگاه‌ها (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)

شکل (۱): مفهوم دفاع هوشمند

دفاع هوشمند، دفاعی همه‌جانبه، پویا، یادگیرنده، اثربخش، پایدار، انعطاف‌پذیر، آگاه به وضعیت صحنه نبرد، مبتنی بر خلاقیت و تصمیم‌گیری هوشمندانه و با بهره‌گیری صحیح و به‌موقع از منابع و ابزارهای قدرت به دنبال مقابله با هرگونه تهاجم و چالش کنش‌گران می‌باشد. (تعریف محقق ساخته)

پیشرفت‌های فناوری، باعث ایجاد تغییرات اساسی در سازمانها، راهبردها و تدابیر امنیتی و دفاعی شده است. فناوری‌های نوین، باعث توزیع و انتشار آگاهی‌ها شده، سرعت تبادل اطلاعات را افزایش داده است 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 حوزه‌های فرماندهی و کنترل که مسئول مدیریت و هدایت عملیات نظامی را بر عهده دارد، تأثیرات عمیقی برجای گذاشته است. (آژانس دفاعی اروپا، ۲۰۲۱)

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.آژانس دفاعی اروپا (EDA)[1] در سال ۲۰۲۱ فناوری-های نوین مرتبط با دفاع هوشمند با عنوان «۱۰ نوآوری دفاعی در آینده» برابر شکل ۲-۲ اعلام نموده است. (همان)

شکل (۲): فناوری‌های نوین در دفاع هوشمند (آژانس دفاعی اروپا، ۲۰۲۱)

[1]- EUROPEAN DEFENCE AJENCY

اینترنت اشیاء: اینترنت اشیاء یک فناوری نوظهور 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، اینترنت اشیاء را به‌عنوان یکی از شش فناوری دارای پتانسیل تأثیرگذاری بر منافع ایالات متحده تا سال ۲۰۲۵ معرفی نموده است. (نظری، ۱۴۰۰: ٤) 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 & etc،2018)

فناوری اینترنت اشیاء تحولات عظیمی در زندگی روزمره بشر ایجاد کرده است. اتصال «هرجا»، «هرشیء» در «هرزمان» 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. (نظری، ۱٤۰۰: ۱٤)

اینترنت اشیاء نظامی[1]: 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. شناسایی، 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 باارزش است؛ بنابراین مهم

[1] . MIOT (Militery Internet Of Things)

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)

در عصر حاضر علی‌رغم چالش‌های فراوان مربوط به پذیرش اینترنت اشیاء در حوزه نظامی، پتانسیل بالای اینترنت اشیاء برای روزآمدسازی جنگ‌افزارها، استفاده از داده‌ها و خودکارسازی جهت حفظ جان سربازان و از طرف دیگر کاهش هزینه‌ها و افزایش کارایی پذیرش این فناوری را به امری جذاب برای سازمان‌های دفاعی و نظامی مبدل ساخته است. علی‌هذا به‌موازات حوزه‌های عملیاتی و اطلاعاتی اینترنت اشیاء با کاهش هزینه‌ها، مدیریت موجودی‌ها، مدیریت تعمیر و نگهداری تجهیزات و... می‌تواند در بهبود فرایندهای حوزه پشتیبانی سازمان‌های نظامی رونق اساسی ایفا نماید. (باقری‌منش و همکاران، ۱۳۹۸: ٤)

مدیریت آماد نظامی[1] مبتنی بر اینترنت اشیاء: 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 به‌منظور ارتقاء فرایندهای اینترنت اشیاء و انسان است. در برخی از ارتش‌ها از فناوری‌ها برای ردیابی، حمل‌ونقل و فناوری برچسب شناسایی فرکانس رادیویی زیرساختی در پس‌زمینه استفاده شده است. (مینایی بیدگلی، ۱۳۹۷)

تجهیزات و تسلیحات هوشمند[2]: اینترنت اشیاء راه جدیدی را برای استقرار گسترده دستگاه‌های هوشمند ارائه می‌دهد، مانند ماشین‌های ناهمگن، حسگرها و محرک‌ها. دستگاه‌ها می‌توانند از طریق ارتباطات فراگیر، داده‌ها را مبادله کرده و از اطلاعات یکدیگر استفاده کنند که این امکان را برای اینترنت اشیاء فراهم می‌کند که درجه بالایی از آگاهی موقعیتی را داشته باشد. کارایی رزمی، هماهنگی و تصمیم‌سازی در میدان نبرد برای ارتش مدرن بستگی زیادی به توانایی آگاهی از وضعیت واقعی از طریق به‌کارگیری قابلیت‌های اینترنت اشیاء در میدان نبرد و انتشار پیوسته اطلاعات رزمی دارد. اینترنت اشیاء در زمینه جنگ‌های مدرن کاربرد امیدوارکننده‌ای دارد. فناوری اینترنت اشیاء که برای ارتباط بین تجهیزات رزمی و سایر منابع میدان جنگ استفاده می‌شود،

---

[1] . logistic managment
[2] . smart equipments and weapens

اینترنت اشیاء میدان نبرد نامیده می‌شود. جمع‌آوری داده‌ها و انتشار اطلاعات در زمان واقعی به اتصال شبکه متکی است، این مسئله در میدان نبرد بسیار حیاتی است که بتوانیم از پتانسیل کامل اینترنت اشیاء میدان نبرد خود استفاده کنیم. (Yuan et al., 2020)

بکارگیری اینترنت اشیاء در 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 به‌طوری‌که 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 موقعیت-یاب جهانی[1] برای مکان فعلی پهپاد است و براین‌اساس داده‌های همه پهپاد توسط واحد کنترل، کنترل می‌شود و در پایگاه داده ذخیره می‌شود. ماژول ارتباطی[2] برای برقراری ارتباط از طریق اینترنت با پهپادهای دیگر و همچنین منطقه کنترل استفاده می‌شود. از پهپاد به‌غیراز برنامه‌های نظامی، می‌توان به‌عنوان وسیله‌ای برای کار چندمنظوره استفاده کرد. (Utsav, 2021)

اینترنت اشیاء در سامانه‌های کنترل آتش[3]: سیستم‌های کاملاً خودکار در ارتش در منطقه آتش متمرکز شده‌اند. این سیستم‌ها از داده‌های حسگر برای واکنش سریع و ارائه دقت دقیق استفاده می‌کنند. به‌عنوان‌مثال، سیستم رزمی آگیس[4] 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 «ای ان اسپای»[5] می‌تواند مهمات هدایت شده را تا ۱۰۰ هدف در یک‌زمان کاملاً خودکار شناسایی، ردیابی و هدایت کند. ارتش برای استفاده از پهپادها برای درگیرشدن با اهداف ارزشمند سرمایه‌گذاری می‌کند. خلبانان ایستگاه‌های زمینی از دوربین‌ها و

---

1. GPS
2. GSM (Global System for Mobile communications)
3. fire control system
4. Aegis
5. AN/SPY

دیگر حسگرهای موجود در کابین خلبان به‌صورت 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» [1]، اهداف را شناسایی کرده و می‌توانند با موشک‌های هلفایر [2] 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. (Denise & William, 2019: 16)

آموزش و شبیه‌سازی (عوامل انسانی)[3]: فناوری اینترنت اشیاء را می‌توان حتی در طول آموزش نظامی به کار برد. موقعیت‌هایی مختلف رزمی را می‌توان با واقعیت مجازی مدل‌سازی کرد. موقعیت‌ها و وضعیت فیزیولوژیکی سربازان توسط سنسورها در طول آموزش نظامی تشخیص داده می‌شود. داده‌های تصویری و صوتی به‌دست‌آمده را می‌توان بعداً در هر زمان ارزیابی کرد. یکی از سیستم‌های شبیه‌سازی که توسط چندین ارتش از جمله ارتش آمریکا و نیروهای دفاعی مجارستان استفاده می‌شود میلس [4] است. این می‌تواند موقعیت‌های واقعی مبارزه مانند بازی معروف برچسب لیزری را شبیه‌سازی کند. سنسورهای متصل به لباس سرباز نور لیزر را تشخیص می‌دهند، تشخیص‌ها را شمارش می‌کنند و یک سیگنال صوتی را ارائه می‌دهند. نسخه جدیدتر میلس پیچیده‌تر است و می‌تواند وضعیت جنگی را با سلاح‌های ترکیبی شبیه‌سازی کند. (Bognar, 2018: 6)

پایش سلامت و بهداشت[5]: حسگرهای مختلف نقش مهمی در نظارت بر سلامت هرکدام از سربازان در میدان نبرد ایفا می‌کنند. سربازان مجهز به کلاه ایمنی مخصوص با سنسورهای کنترل یکپارچه برای تشخیص ضربه مغزی و سایر آسیب‌های مغزی هستند. وسایل کوچک و هوشمند نظارت بر سلامت و مراقبت‌های بهداشتی بیشتر و بیشتر در شرایط جنگی استفاده می‌شوند؛ بنابراین خدمات اولیه و مراقبت‌های بهداشتی را می‌توان بدون هیچ‌گونه پرسنلی برای سربازان ارائه کرد. به طور مثال دستگاه تمپاس پرو [6] مستقر در ارتش آمریکا، انگلیس و نروژ یک سیستم پیشرفته است که

---

1. Distributed Common Ground System (DCGS)
2. Hellfire
3. personal
4. MILES – Multiple Integrated Laser Engagement
5. health minitoring
6. Tempus Pro

می‌تواند سیگنال‌های مجازی به‌منظور جلوگیری از آسیب به سربازان را کنترل کند. (Bognar, 2018: 5)

نقش اینترنت اشیاء در نبردها: از طریق ترکیب دستگاه های مختلف هوشمند و اینترنت برای ایجاد یک مقیاس بزرگی از شبکه، اینترنت اشیاء به تبادل اطلاعات و ارتباطات بین دستگاه‌ها در زمان واقعی می‌پردازد. انتظار می‌رود فناوری اینترنت اشیاء نقش اساسی در بهبود مبارزه داشته باشد اثربخشی و توانایی آگاهی از وضعیت ارتش‌ها، ارتباط متقابل بین نبرد تجهیزات و دیگر منابع میدان جنگ به‌عنوان اینترنت اشیاء میدان جنگ[1] نامیده می‌شود. به اشتراک‌گذاری داده‌ها در زمان واقعی میدان نبرد و تصمیم‌گیری مشارکتی بین فرماندهان بستگی به ارتباط بین واحدهای مختلف رزمی در شبکه دارد. (Yuan et al., 2020)

اینترنت اشیاء در میدان جنگ یک فناوری نوآورانه است که شامل شبکه حسگرها، پوشیدنی‌ها و دستگاه‌های مرتبط می‌باشد. اینترنت اشیاء به ایجاد یک نیروی جنگی منسجم و افزایش کارآیی عملیاتی سیستم‌های نظامی در میدان نبرد کمک شایانی می‌کند. به‌عنوان مثال برای استفاده از محاسبات ابری و لبه و اتصال رزمندگان به فناوری هوشمند مانند زره، رادیو، سلاح و سایر اشیاء بکارگیری می‌شود. اینترنت اشیاء در نبردهای هوشمند واقعیت در حال ظهور در جنگ‌های آینده است. اینترنت اشیاء 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 حسگرها و ناظران انسانی تولید می‌شود. (۲) حوزه اطلاعاتی که داده ها در آن منتقل و ذخیره می‌شوند. و (۳) حوزه شناختی، که در آن داده‌ها پردازش و تجزیه و تحلیل شده است. سه حوزه جنگ شبکه‌محور، مفهوم مدرن اینترنت اشیاء را به طور کامل منعکس می‌کند. ترکیبی از حسگرها و دستگاه‌های تعبیه شده، اتصال به اینترنت، فناوری پایگاه داده و تجزیه و تحلیل نرم‌افزار. عملیات نظامی مدرن با فناوری پیچیده، بسیار پویا و چند بعدی به هم پیوسته انجام می‌شود تا وابستگی به جنگجویان انسانی را کاهش دهد. در آینده اینترنت اشیاء میدان نبرد، جنگنده‌های انسانی را به فناوری‌های هوشمند مانند زره، سلاح، رادیو و سایر اشیاء متصل می‌کند. (Lin et al., 2020)

[1]. IOBT

فرماندهی و کنترل هوشمند: استفاده از فناوری اینترنت اشیاء در مورد سیستم‌های مراکز فرماندهی و کنترل از مزایای بالاتری برخوردار است. سیستم‌های مراکز فرماندهی و کنترل از چندین میلیون حسگر در سیستم‌عامل‌های مختلف برای اطمینان از آگاهی موقعیتی توسعه‌یافته استفاده می‌کنند. شبکه بسیار پیچیده و گسترده شامل چندین میلیون حسگر (سنسورها در سیستم‌عامل‌های مختلف مانند هواپیماهای بدون سرنشین، رادارها، دوربین‌های فیلم‌برداری، سنسورهای مادون‌قرمز، سنسورهای زمینی بدون مراقبت، دستگاه‌های قابل‌حمل) داده‌های واقعی را برای نیروهای رزمی و تصمیم‌گیرندگان ارائه می‌دهد. این داده‌ها را 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 به‌سلامت 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 اشیاء به اتاق کنترل منتقل می‌شوند. در سال‌های اخیر رقابت تسلیحاتی شدیدی برای توسعه سیستم‌های نظامی و دفاعی به‌خصوص در حوزه فرماندهی و کنترل در میان کشورها به راه افتاده است.

باید توجه داشت که سلطه عمل اطلاعاتی اهمیتی بالاتر از تجهیز نظامی دارد به طوری که ممکن است فرصت ورود به مرحله اقدام عملی و نظامی را محقق سازد. این مسئله لزوم رویکردی متفاوت و راهبردی را برای پیش‌بینی اقدامات در کنار توجه به امنیت تجهیزات خریداری شده مشخص می‌سازد. به‌کارگیری حلقه OODA در فرماندهی و کنترل یکی از راهکارهای مناسب در چرخه مشاهده تا اقدام است که فرمانده را در مدیریت راهبردی عملیات کمک می‌کند. برخی از اقدامات مهم به‌کارگیری این روش در جدول زیر آمده است:

جدول (۱): اقدامات مهم در فرماندهی و کنترل با توجه به مراحل چهارگانه حلقه OODA

مرحله	اقدامات لازم
مشاهده[1]	جمع آوری از طریق حسگرها و اینترنت اشیاء
	پیش پردازش
	اعتبارسنجی
	تلخیص و دسته بندی
	گزارش‌دهی براساس حیطه بندی
	کنترل حسگرها از طریق اینترنت اشیاء
هم‌محورشدن[2]	ارزیابی وضعیت
	استنتاج وضعیت موجود از طریق قیاس
	دیتا فیوژن
	عملیات یادگیری
	تجزیه و تحلیل از طریق داده‌کاوی اطلاعات
	تفسیر وقایع و جریان‌ها
تصمیم[3]	تصمیم‌سازی مبتنی بر مدیریت دانش
	اولویت‌گذاری راه‌کارها
	طرح‌ریزی راه‌کارهای مختلف
	پیش‌بینی آینده
	درک و قضاوت انسانی
اجرا[4]	هدایت نیروها
	ایجاد داشبوردهای اطلاعاتی برای فرمانده
	ایجاد سامانه‌های خبره فرماندهی
	سامانه‌های پشتیبان تصمیم

امنیت اینترنت اشیاء: بزرگ‌ترین نگرانی پس از ورود اشیاء در خانه‌ها، سازمان‌ها و شرکت‌های خصوصی، مبحث حریم خصوصی و امنیت اطلاعات می‌باشد. این موضوع با تشدید خبرهای سرقت اطلاعات از کاربران توسط هکرها گسترش و توسعه اینترنت اشیاء را به چالش کشیده

1. Observation
2. Orientation
3. Decision
4. Action

است. نگرانی از عدم امنیت داده‌ها در کلیه سطوح مدل اینترنت اشیاء به‌عنوان داغ‌ترین مبحث تحقیقاتی مطرح می‌باشد. در حوزه نظامی حفظ حریم خصوصی رزمندگان و نیز کنترل دسترسی از اهمیت ویژه‌ای برخوردار است؛ بنابراین برای ایجاد امنیت اینترنت اشیاء در حوزه نظامی عدم انکار، جامعیت، دسترس پذیری، احراز هویت، حریم‌خصوصی، کنترل دسترسی و محرمانگی مدنظر قرار گرفته است. (رمضانی دهقی، ۱۳۹۹)

شکل (۳): ابعاد امنیت اینترنت اشیاء

در مبحث نظامی و مخصوصاً صحنه نبرد، به دلیل حساسیت به مراتب بالاتر، بایستی تمهیدات بیشتری جهت محرمانگی اتخاذ گردد، منتهی همواره بایستی توازن بین امنیت و هزینه صرف شده برای این امنیت را در نظر داشت، به خصوص اینکه دستگاه‌های بیسیم و حسگرهای مورد استفاده، توان ذخیره‌سازی انرژی محدودی دارند و مخصوصاً تجهیزاتی که روی نیروی پیاده و سربازها نصب می‌شود، برای به دلیل سبکی و راحتی سرباز، ساده و کم وزن (وزن، پردازش، حجم) طراحی می‌شوند؛ لذا نیاز است توازنی بین سطحی از امنیت و محرمانگی که مورد نیاز است و توان پردازشی و انرژی ایجاد گردد.

دفاع سایبری: اقداماتی که معمولا درون فضای سایبر وزارت دفاع برای امن سازی، عملیاتی سازی و دفاع از شبکه اطلاعاتی وزارت دفاع در برابر تهدیدات خاص انجام می‌گیرد. اهداف دفاع سایبری شامل اقداماتی جهت جلوگیری، آشکارسازی، تشخیص، مقابله و کاهش تاثیرات تهدیدات می‌باشد. (FM 3-12, 2017, 1-9) امنیت در پارادایم فضای سایبری تابع دو عنصر کلیدی انسان و فضای سایبر است. مساله اول انسان، ویژگی‌ها و قابلیت‌هایش است. مساله دوم، ابعاد، قابلیت‌ها و مبانی شکل گیری فضای سایبری است. کنش و تعامل کنشگران، این دو عامل، موجب شکل‌گیری فضای

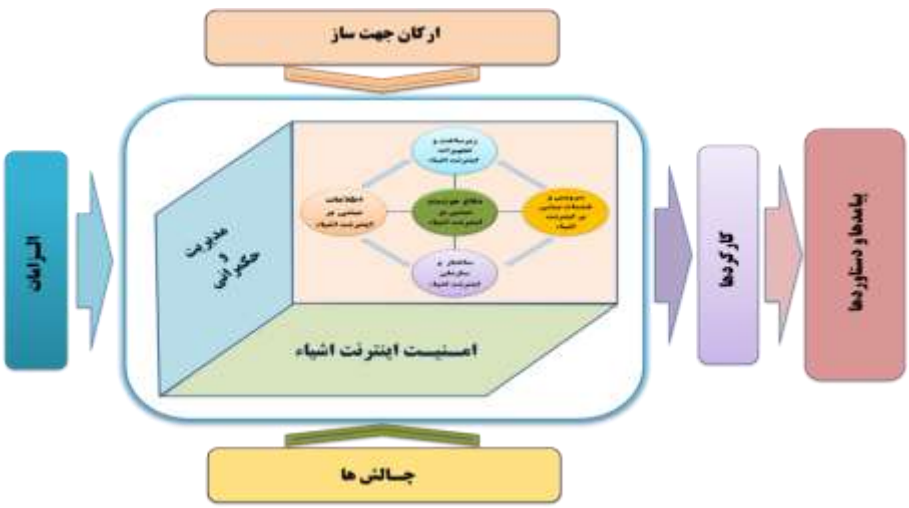
تهدیدزایی شده که ابعاد گسترده و متنوعی را در حوزه امنیت شکل می‌دهد. فضای سایبر به علت ماهیت و کارکرد خود فضایی تهدیدزا را خلق می‌نماید.مم

تکنولوژی‌های سایبر با دارا بودن عملکردهای بسیار مشخص نظامی می‌توانند به طورمستقیم بر میدان نبرد تاثیرگذار باشند.

بخش نظامی هر کشوری برای آموزش و تجهیز نیروها، سیستم‌های جنگ افزاری، ماهواره‌ها و شبکه‌های ارتباطی یا داده‌پردازی اطلاعات، به تکنولوژی‌های سایبری وابسته است. در واقع می-توان گفت: فضای اطلاعاتی و سایبری به همان نسبت که می‌تواند فرصت‌های بسیار زیادی را برای نیروهای نظامی هر کشور به وجود آورد، به همان میزان نیز می‌تواند تهدیدهای بزرگی را برای این بخش به وجود آورد. (سالاری و همکاران، ۱۳۹۹)

الگوی مفهومی تحقیق (مدل مفهومی)

دفاع هوشمند مبتنی بر اینترنت اشیاء به عنوان یک مفهوم کلیدی در این تحقیق محسوب می‌شود. بر این مبنا، برای مدل‌سازی، ابتدا عناصر و متغیرهای مرتبط با این مفهوم شناسایی شده و سپس با تعیین روابط میان این مقوله‌ها، یک مدل مفهومی کلان برای دفاع هوشمند مبتنی بر اینترنت اشیاء ارائه می‌شود.



شکل (۳): مدل مفهومی تحقیق

روش‌شناسی تحقیق

این تحقیق به صورت آمیخته و با روش‌های توصیفی - تحلیلی و مـوردی - زمینـه‌ای انـجام می-شود. از این جهت توصیفی - تحلیلی است که برای گردآوری اطلاعاتی که مدون نشده به کار می-رود و با این روش، توصیف عینی، واقعی و منظم موضوعات انجام می‌گردد. از این جهت موردی - زمینه‌ای است که در این مقاله، مطالعه عمیق روی نمونه‌هایی از یک پدیده در محیط واقعی صورت می‌گیرد.

نوع پژوهش در زمینهٔ شناخت الگوی راهبردی دفاع هوشمند، توسعه‌ای خواهد بود. از طرف دیگر پژوهش حاضر در پی هوشمندی دفاع یک سازمان نظامی است؛ بنابراین پژوهش از این منظر کاربردی محسوب گردیده و درمجموع توسعه‌ای - کاربردی خواهد بود. برای گردآوری اطلاعات از روش کتابخانه علمی و تخصصی، سایت‌های معتبر اینترنتی، همچنین روش میدانی شامل مصاحبه با خبرگان حوزه دفاعی و سایبری و تنظیم پرسشنامه استفاده شد. برای تحلیل داده‌های بخش کمی (داده‌های حاصل از پرسشنامه) نیز از روش‌های آمار توصیفی و استنباطی ازجمله معادلات ساختاری، تحلیل واریانس، ضریب همبستگی استفاده شده است. به منظور اخذ نظر خبرگان، مصاحبه عمیق با روش اشباع نظری با جامعه آماری ۷ نفر صورت پذیرفت. با توجه به جامعه آماری ۷۰ نفره پرسشنامه به صورت تمام شمار به ۷۰ نفر از خبرگان ارسال شد؛ بنابراین حجم نمونه با حجم جامعه برابر است. پرسشنامه به لحاظ روایی ظاهری و محتوا به تأیید جمعی از اساتید رسانده شد و به لحاظ پایایی با استفاده از نرم‌افزار SPSS آلفای کرونباخ پرسشنامه ۰,۸۶ برآورد شد که پایایی قابل قبولی محسوب می‌شود.

تجزیه و تحلیل داده‌ها و یافته‌های تحقیق

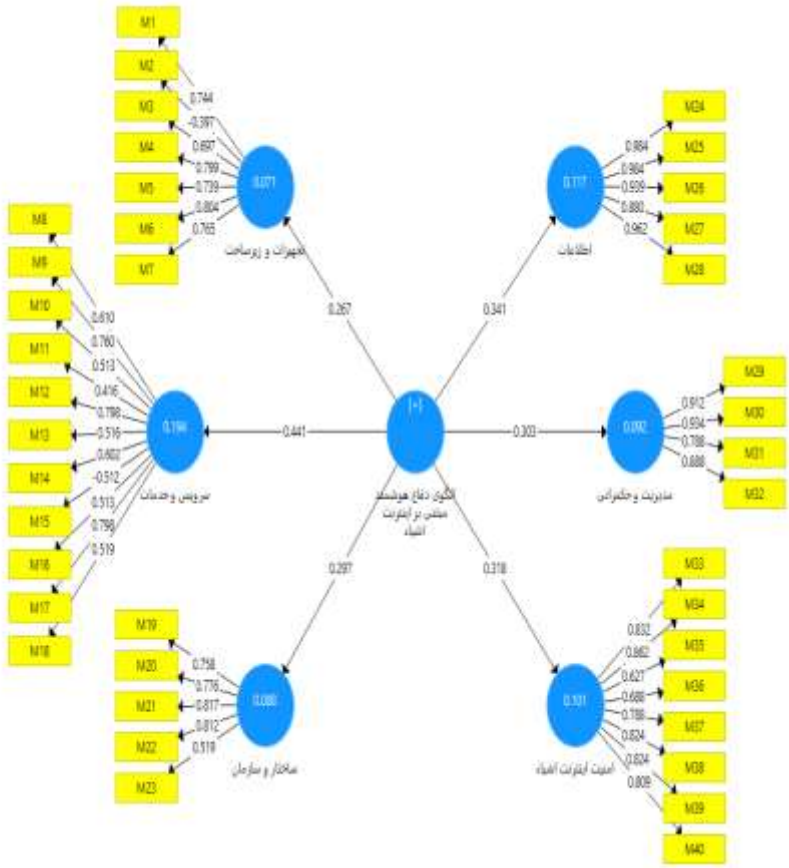
از آنجا که هدف اصلی در این تحقیق، دستیابی به الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء است، لذا جهت حصول به هدف اصلی تحقیق، می‌بایست احصاء ابعاد (مضامین فراگیر)، مؤلفه‌ها (مضامین سازمان دهنده) و شاخص‌ها مد نظر قرار گیرد. به‌منظور احصاء ابعاد و مؤلفه‌های دفاع هوشمند، مبتنی بر اینترنت اشیاء در مرحله اول با مطالعه اکتشافی و تفکر دقیق و مستمر در مبانی نظری و ادبیات تحقیق در فصل دوم و مصاحبه با خبرگان نسبت به استخراج مضامین پایه اقدام شده است. در مرحله بعد از هم‌پوشانی، ترکیب و تلخیص مضامین پایه، مضامین سازمان دهنده یعنی مؤلفه‌ها و مضامین فراگیر یعنی ابعاد دفاع هوشمند مبتنی بر اینترنت اشیاء استخراج

شده است. به منظور شناسایی سایر عواملی که ممکن است در فرایند مطالعه و تحقیق مغفول مانده باشند از مصاحبه با صاحب نظران در حوزه‌های مرتبط با دفاع هوشمند و فناوری‌های نوین استفاده شد. پس از انجام مراحل گفته شده و بهره‌گیری از نظرات خبرگان مرتبط و صاحب‌نظران در این حوزه، در نهایت تعداد ٦ بعد (مضامین فراگیر) و تعداد ٤٠ مؤلفه (مضامین سازمان دهنده) مرتبط با ابعاد مورد نظر احصاء گردید که در جدول (۲) نشان داده شده است.

جدول ۲: ابعاد و مؤلفه‌های دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء

مفهوم	ابعاد	مؤلفه‌ها
دفاع هوشمند مبتنی بر اینترنت اشیاء	زیرساخت و تجهیزات مبتنی بر اینترنت اشیاء	مراکز داده، مراکز سوئیچینگ، شبکه‌های ارتباطی، مخابراتی و رایانه‌ای، شبکه فیبرنوری امن و پایدار، تسلیحات و تجهیزات هوشمند، سامانه‌های سلاح هوشمند و فرمان‌پذیر، انواع حساسه‌ها، پروتکل‌ها و پلتفرم‌های بومی، ربات‌های هوشمند، سیستم‌های تصمیم‌گیری هوشمند
	سرویس و خدمات اینترنت اشیاء	سرویس‌های یادگیری ماشینی، سرویس‌های هوشمند پشتیبان سیستم، سرویس پایش، شناسایی و مراقبت، جنگ الکترونیک هوشمند (زمین‌پایه، هواپایه و دریاپایه)، عملیات آفند و پدافند هوشمند، سرویس‌های پیش‌بینی و کنترل، زنجیره تأمین و لجستیک هوشمند، آگاهی وضعیتی هوشمند، سرویس‌های بدون سرنشین، پایش هوشمند سلامت و بهداشت، هوش مصنوعی در تحلیل داده
	ساختار و سازمان	نیروی انسانی کارآمد، ساختار سازمانی فناور پایه، آموزش کاربران، پذیرش اینترنت اشیاء از طرف فرماندهان و کارکنان، دانش و مهارت کاربران،
	دانش و اطلاعات	یکپارچگی اطلاعات، داده‌کاوی و تحلیل اطلاعات، جمع‌آوری و ذخیره اطلاعات، پردازش اطلاعات، دقت اطلاعات، سرعت ارسال اطلاعات، مدیریت دانش، جنگ شناختی
	مدیریت و حکمرانی	فرماندهی و کنترل صحنه نبرد، رگولاتوری و حقوق و قوانین، قوانین و مقررات کشوری در حوزه سایبر، ارزیابی و کنترل هوشمند، قوانین و مقررات سازمان‌های نظامی کشورها در حوزه سایبر
	امنیت اینترنت اشیاء	محرمانگی، یکپارچگی و جامعیت، دسترس‌پذیری، کنترل دسترسی، احراز هویت، حریم خصوصی، اعتماد، عدم انکار، دفاع سایبری

محاسبه ضرایب بار عاملی، یکی از روش‌های ارزیابی پایایی ابزار اندازه‌گیری است که میزان همبستگی شاخص‌های یک سازه با آن را مشخص می‌سازد. پس از رسم مدل برای هر کدام از ابعاد دفاع هوشمند مبتنی بر اینترنت اشیاء، ضرایب بار عاملی مربوط به مؤلـفه‌ها به دسـت می‌آید. پس از اجرای نرم‌افزار در صورتی که ضرایب بار عاملی به دست آمده برای هر شاخص کمتر از ۰/٤ باشند، این مؤلفه قابل حذف است. در مرحله بعد، الگوی کلی تحقیق شامل ابعاد و مولفه‌های تأثیرگذار بر ارتقاء دفاع هوشمند، مبتنی بر اینترنت اشیاء ترسیم شد و با اجرای دستور Algorithm PLS ضرایب بار عاملی الگو برای ابعاد و مولفه‌ها به دست آمد در شکل شماره (٤) این مسئله نشان داده شده است.



شکل ۲: ضرایب بار عاملی مؤلفه‌های الگو

سنجش پایایی: برای سنجش پایایی مدل، بارهای عاملی آلفای کرونباخ و پایایی ترکیبی اندازه-گیری می‌شود. معیار قابل قبول برای آلفای کرونباخ که نشان‌دهنده پایایی مدل اندازه‌گیری خواهد بود، حداقل مقدار ۰/۷ می‌باشد. علاوه بر ضریب آلفای کرونباخ جهت بررسی پایایی متغیرها از شاخص جدیدتری به نام ضریب پایایی ترکیبی استفاده شده است. در صورتی که مقدار پایایی ترکیبی برای هر سازه بیشتر از ۰/۷ شود، علیرغم وجود ضرایب آلفای کرونباخ کمتر از آن، پایداری درونی مدل اندازه‌گیری مناسب استنباط می‌شود.

جدول (۳): آزمون‌های پایایی مدل

ابعاد	تعداد گویه	آلفای کرونباخ[1]	همبستگی اسپیرمن[2]	پایایی ترکیبی[3]	پایایی اشتراکی[4]
زیرساخت و تجهیزات	٦	۰,۸٦۱	۰,۸۷۷	۰,۸۹۵	۰,۵۸۸
سرویس و خدمات	۱۱	۰,۷٦۳	۰,۸٤۸	۰,۸۳۰	۰,۵۸٦
ساختار و سازمان	۵	۰,۷۹۷	۰,۸۲۷	۰,۸۵۹	۰,۵۵۵
دانش و اطلاعات	۵	۰,۹۷۳	۰,۹۸۰	۰,۹۷۹	۰,۹۰۳
مدیریت و حکمرانی	٤	۰,۹۱۲	۰,۹٦۹	۰,۹۳۳	۰,۷۷۸
امنیت	۸	۰,۹۱۱	۰,۹۲۷	۰,۹۲۷	۰,٦۱۷

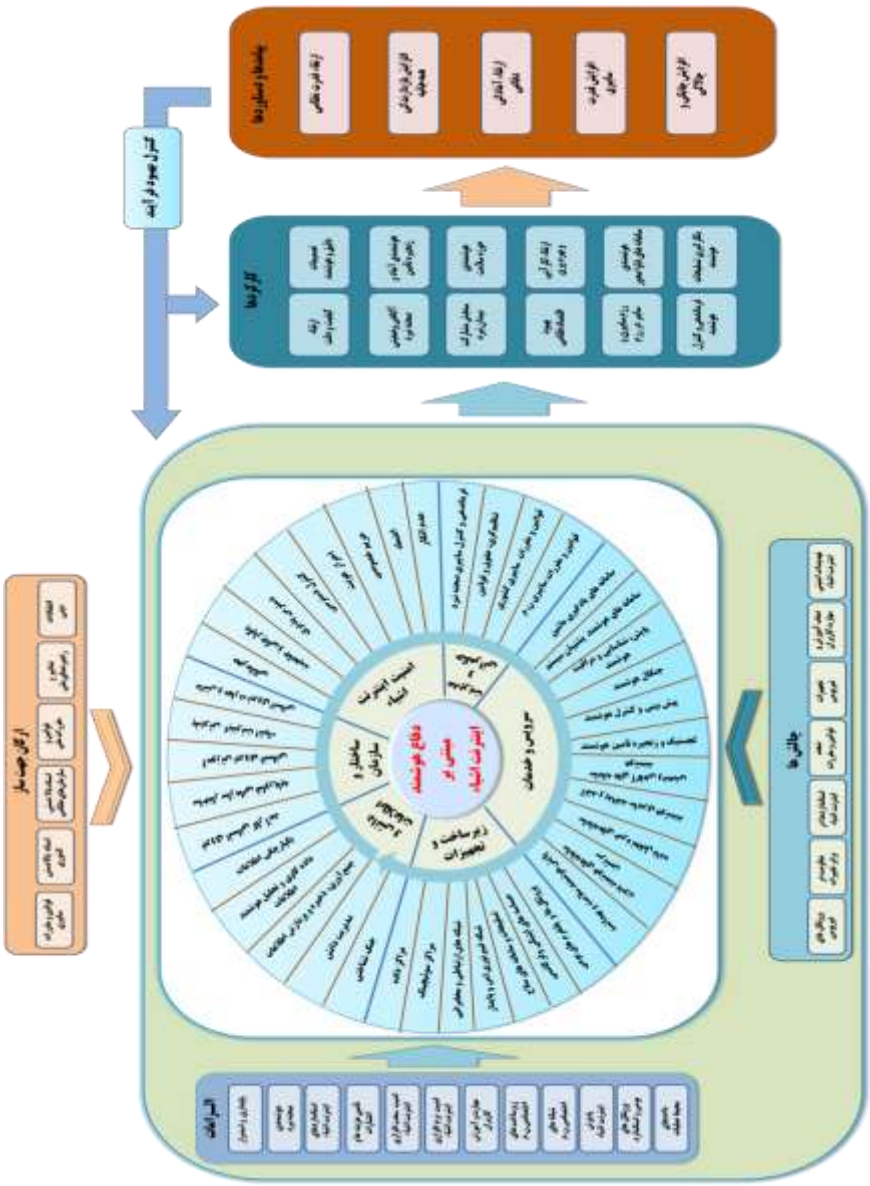
نتیجه‌گیری و پیشنهاد

الف: نتیجه‌گیری

از منظر راهبردی برای دستیابی به الگوی دفاع هوشمند مبتنی بر اینترنت اشیاء باید تمامی عوامل تأثیرگذار را مد نظر قرار داد. چرا که این عوامل هر کدام می‌توانند در دفاع هوشمند مبتنی بر اینترنت اشیاء نقشی مؤثر ایفا نمایند. در این رساله، چیستی، چگونگی و چرایی دفاع هوشمند مبتنی بر اینترنت اشیاء و همچنین ابعاد و مؤلفه‌های دفاع هوشمند مبتنی بر اینترنت اشیاء در جواب به سؤال تحقیق به تفصیل مورد بررسی قرار گرفت که شامل تعداد ٦ بعد و ٤٠ مؤلفه است. الگوی نهایی در شکل (۵) ارائه شده است. در الگوی ارائه شده، ابعاد دفاع هوشمند مبتنی بر اینترنت اشیاء در هسته مرکزی به صورت مدل خورشیدی قرار دارند و مؤلفه‌های مربوط به هر کدام از این ابعاد در پیرامون ابعاد جای گرفته‌اند. عوامل تأثیرگذار شامل ارکان جهت‌ساز، الزامات اینترنت اشیاء و چالش‌های اینترنت اشیاء که

1 . Cronbach's Alpha
2 . Rho-A
3. Composite Reliability
4. Average Variance Extracted (AVE)

در واقع به عنوان ورودی‌های هسته مرکزی قرار دارند. قسمت خروجی الگو شامل کارکردها، پیامدها و دستاوردها است.



شکل ٤: ارائه الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء

عوامل محیطی تأثیرگذار: از عوامل بیرونی تاثیرگذار بر دفاع هوشمند مبتنی بر اینترنت اشیاء که به عنوان عوامل مداخله‌گر بوده و حوزه‌ها، ابعاد و معیارهای آن را تحت تاثیر قرار می‌دهند، شامل سه مقوله ارکان جهت‌ساز جمهوری اسلامی ایران، الزامات و چالش‌ها است. در واقع ارکان جهت‌ساز، آیات و احادیث، تدابیر و بیانات مقام معظم رهبری(مدظله‌العالی)، قوانین، مقررات و چارچوب‌های موجود را نشان می‌دهد. الزامات در این عوامل مداخله‌گر، بسترهای مورد نیاز، نیازمندی‌های اعتباری و انسانی و استانداردهای امنیتی و فناوری لازم را در جهت نیل به دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء نشان می‌دهد. چالش‌ها عامل مداخله‌گری است که موانع و مشکلات پیش‌رو را از جنبه‌ها و زوایای مختلف که در فرایند پیاده‌سازی و اجرای الگوی هوشمندسازی دفاع قرار دارند، در این مدل به تصویر کشیده و آنها را نشان می‌دهد. همان‌طور که گسترش فناوری‌های نوظهور ابعاد گوناگون اجتماعی را تحت‌تأثیر قرار می‌دهد، به تبع آن مسائل و چالش‌های بسیاری را پیش روی حاکمیت‌ها می‌گذارد که نیازمند پژوهش‌های محققان در حوزه‌های گوناگون اجتماعی، به‌ویژه خط مشی‌گذاری است. این فناوری به مثابهٔ یکی از روندهای مهم فناوری اطلاعات و ارتباطات در سال‌های آتی، گستره‌ای از این گونه مسائل را نیز با خود به همراه دارد. مواجههٔ فعالانه با این فناوری نیازمند فراهم شدن زیرساخت‌های علمی و پژوهشی برای خط‌مشی‌گذاری است که مقدمهٔ آن مشخص شدن دستورکارها و حوزه‌های پژوهشی برای محققان این حوزه است.

یکی از چالش‌های عمده‌ای که باید به منظور وارد کردن اشیاء به جهان واقعی برطرف شود، «چالش امنیت» است. تهدیداتی که می‌تواند بر نهادهای اینترنت اشیاء تأثیر گذارد، متعدد هستند؛ مانند حملات با هدف کانال‌های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیاء که در آن نهادگی ناهمگن متعدد واقع در زمینه‌های مختلف، می‌تواند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی‌های بیشتر طراحی و بکارگیری مکانیزم های امنیتی کارآمد، سازگار و مقیاس‌پذیر را می‌طلبد.

در جدول زیر عوامل مرتبط و اثرگذار در مفهوم دفاع هوشمند مبتنی بر اینترنت اشیاء نشان داده شده است.

جدول ٤: عوامل مرتبط و اثرگذار در دفاع هوشمند مبتنی بر اینترنت اشیاء

مفهوم اصلی تحقیق	عوامل مرتبط و اثرگذار در مفهوم اصلی
دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء	ابعاد (امنیت، مدیریت و حکمرانی، زیرساخت و تجهیزات، سرویس و خدمات، ساختار و سازمان، اطلاعات)
	ارکان جهت‌ساز
	الزامات
	چالش‌ها

کارکردهای دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء در حوزه‌ها و زمینه‌های مختلف تأثیرگذار در صحنه میدان نبرد، از جمله در هوشمندی مراکز فرماندهی و کنترل، هوشمندی آماد و زنجیره تأمین، هوشمندی سامانه‌های کنترل آتش، پایش سلامت هوشمند و سنجش مشارکتی در میدان نبرد، می‌بایست در خروجی مدل مفهومی در نظر گرفته شود. پیامدها و دستاوردهای هوشمند شدن مقوله دفاع مبتنی بر فناوری اینترنت اشیاء، از خروجی‌های دیگر مدل لحاظ می‌گردد. افزایش اقتدار دفاعی، افزایش قدرت دفاعی، ارتقاء توان و آمادگی رزمی و... از دستاوردها و نتایج حاصل از پیاده‌سازی نتایج مستخرجه رساله حاضر و پیامدهای هوشمندی دفاع می‌تواند محقق گردد که این موارد در مدل مفهومی لحاظ گردیده است.

اثربخشی فرایند هوشمند شدن دفاع مبتنی بر فناوری اینترنت اشیاء، زمانی مفهوم خود را خواهد داشت که تمامی ابعاد مؤثر در میدان نبرد، کارکرد هوشمندانه‌ای داشته و در چرخه هوشمندانه‌ای به نقش خود در عملیات صحنه نبرد میدانی بپردازند. اگر بخواهیم تصمیمات اتخاذ شده در سامانه فرماندهی و کنترل مبتنی بر هوشمندی و برگرفته از تجزیه و تحلیل اطلاعات ارسال شده از کلیه حسگرهای متصل به پردازش‌گر مرکزی باشند لازم است کلیه اجزاء تأثیرگذار در این فرایند به صورت هوشمندانه فعال حضور داشته باشند. با در نظر گرفتن ابعاد و مؤلفه‌های احصاء شده در فرایند دفاع هوشمند مبتنی بر اینترنت اشیاء و همچنین عوامل تأثیرگذار در این چرخه مانند ارکان جهت‌ساز، الزامات و چالش‌ها در جهت دستیابی به کارکردهای این فرایند بوده و در صورت دستیابی به کارکردهای مورد نظر است که این فرایند به اهداف خود نائل گردیده است. اگر کارکردهای مطلوب و مورد نظر در خروجی مدل مفهومی بدست بیاید، در آن صورت پیامدها و دستاوردهای مطلوب و مد نظر در این چرخه احصاء خواهند شد.

ب- پیشنهادها

۱. در خصوص تدوین راهبردها و یا ارائه الگوی راهبردی دفاع هوشمند در هر کدام از حوزه‌های زمین‌پایه، هواپایه، دریاپایه، فضاپایه و سایبرپایه، پژوهش‌های جامعی صورت پذیرد.
۲. پژوهشی در خصوص ارائه الگوی راهبردی آماد و زنجیره تأمین هوشمند مبتنی بر اینترنت اشیاء انجام گردد.
۳. پژوهشی با موضوع ارائه الگوی دفاع هوشمند مبتنی بر فناوری‌های حاکمیت گریز انجام گیرد.

فهرست منابع:

- قرآن کریم، ترجمه و تفسیر آیت الله مکارم شیرازی
- حضرت امام‌خمینی (رحمت الله علیه)، صحیفه نور، ج۱۶وج۲۲، تهران، موسسه تنظیم و نشر آثار امام (رحمت الله علیه)
- حضرت امام خامنه‌ای (مدظله العالی)، مجموعه بیانات، قابل دسترسی در: www.khamenei.ir

الف– منابع فارسی

- 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 کاربست مفهوم اینترنت اشیاء در حوزه نظامی (مطالعه موردی قرارگاه پدافند هوایی خاتم‌الانبیاء (ص) آجا، دانشگاه عالی دفاع ملی
- زیبنده، 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
- محمد علی‌زاده، 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

ب – منابع انگلیسی

- 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

پ– سایت‌ها:

قیصری، محمد، هنرمند، مریم، وحدت، داود، (۱۳۹۹)، کاربرد فناوری اینترنتی از اشیاء در توسعه مدیریت لجستیک، - www.IOTiran.com