تاریخ دریافت: ۱۴۰۰/۱۰/۰۴
تاریخ پذیرش: ۱۴۰۱/۰۹/۱۸

فصلنامه علوم و فنون نظامی
سال هجدهم، شماره ۶۱، پاییز ۱۴۰۱
صص ۸۲- ۵۵

تحلیلی برکاربرد اینترنت اشیاء در شبکه پدافند هوایی از منظر آسیب‌ها و تهدیدها

ایرج بختیاری*[۱]

نوع مقاله: پژوهشی

چکیده

روند رو به رشد فناوری و توسعه رویکرد شبکه‌ای در آینده در حوزه‌های مختلف نظامی و غیر نظامی از یک سو و اثرگذاری آن بر سامانه‌های پدافندی از سوی دیگر این مهم را مورد تاکید قرار می‌دهد که، با توجه به هوشمندی و خودکار شدن سلاح‌های نسل جدید و انجام ماموریت‌ها تحت کنترل و هدایت شبکه فرماندهی و کنترل، در راستای استفاده از شبکه‌هایی مانند IOT[2]، لازم است همواره با پایش تهدیدها و رصد فناوری‌های مورد استفاده، نسبت به رفع نقاط ضعف و ارتقاء آمادگی دفاعی اقدام نمود. حملات برق آسای هوایی با استفاده از انواع تجهیزات و سلاح‌های مدرن باعث شده، سامانه‌های پدافند هوایی تحت پوشش شبکه یکپارچه در خط مقدم درگیری و اولویت اول در مباحث دفاعی قرار گیرند. هدف اصلی پژوهش بررسی و تحلیل کاربرد اینترنت اشیاء در شبکه پدافند هوایی از منظر آسیب‌ها و تهدیدها است که با توجه به ماهیت موضوع، نوع پژوهش توسعه‌ای-کاربردی و روش آن توصیفی با رویکرد آمیخته کمی و تحلیل محتوای کیفی است. جهت احصاء عوامل محیطی از جامعه آماری شامل ۱۶ نفر از خبرگان و صاحبنظران حوزه پدافند هوایی و شبکه و آشنا به مباحث دفاعی راهبردی بصورت هدفمند جهت مصاحبه عمیق استفاده گردید. یافته‌های پژوهش مشتمل بر تعداد ۱۳ مقوله فرعی (عوامل محیط داخلی و خارجی) به عنوان چالش‌ها می‌باشد که نهایتا ۹ مقوله فرعی مرتبط با تعداد ۴ مقوله اصلی تعیین و رتبه بندی شده و در انتها پیشنهادهای مرتبط در راستای هدف پژوهش ارائه گردیده است.

واژه‌های کلیدی:

اینترنت اشیاء، فرماندهی و کنترل، چالش‌ها، شبکه پدافند هوایی.

---

[۱] استادیار مدیریت راهبردی دانشگاه پدافندهوایی خاتم الانبیا(ص)، تهران، ایران
* نویسنده مسئول: Email: eraj_baktiar@yahoo.com

[2] Internet of Things

DOI: doi.org/10.22034/qjmst.2022.545564.1639

مقدمه

امروزه شاهد رشد سریع فناوری اطلاعات و ارتباطات و ورود آن به عرصه‌ها و بخش‌های مختلف نظامی و غیرنظامی هستیم. نیازهای حیاتی امنیتی و دفاعی، به عنوان پیشرانی قوی در مطالبه فناوری های جدید و نوآوری‌ها در صنایع دفاعی به شمار می‌رود. با توجه به اهمیت بخش نظامی در ارتقای نقش کشورها در معادلات سیاسی و اقتصادی، توجه به امر نوآوری و پژوهش و توسعهٔ محصول جدید امری غیرقابل اجتناب می‌باشد (فراهانی‌فر و همکاران،۱۴۰۰ :۱۸۰). با عنایت به رویکردهای سه گانه معماری سامانه‌های فرماندهی و کنترل(عملیاتی، فنی، سیستمی)، تاثیر کاربرد IoT بر هریک از این ابعاد مهم می‌تواند در بازطراحی سامانه‌های فرماندهی و کنترل مد نظر قرار گیرد. البته کاربرد اینترنت اشیاء به طور قطع بر عناصر اصلی سامانه‌های فرماندهی و کنترل شامل؛ نیروی انسانی، تجهیزات، ارتباطات و روش‌ها و رویه‌ها، تاثیر و تاثر متقابل دارد. شبکه پدافندهوایی به عنوان یک سامانه کل[1] متشکل از زیرسامانه‌های مراکز فرماندهی و کنترل، سامانه‌های سلاح زمین و هوا پایه، سامانه‌های کشف راداری و شنود الکترونیکی و دیده‌بانی، کاربران هریک از این سامانه‌ها، سامانه‌های ارتباطی و مخابراتی، قوانین و پروتکل‌های ارتباط عناصر شبکه جهت تبادل داده‌ها با توجه به لزوم به روز بودن آن‌ها متناسب با سطح فناوری تهدیدها، لازم است از فناوری به روز و پیشرفته بهره‌مند گردد. کاربرد رایانه‌های پیشرفته جهت پردازش اطلاعات سامانه‌های کشف و تجزیه تحلیل آن جهت تصمیم سازی و تصمیم گیری در فرماندهی و کنترل یکی از جنبه‌های این الزام می‌باشد. استفاده از پهپادها و سلاح‌های دورایستا، کروز و بالستیک، حملات الکترونیکی و سایبری از جمله مهم‌ترین تهدیدها و چالش‌های پدافندهوایی می‌باشد(بختیاری، ۱۳۹۹ :۳۵). رویکرد شبکه‌ای و استفاده از هوش مصنوعی و فناوری روباتیک جهت هماهنگی و یکپارچه سازی سامانه‌های تهدید و استفاده از ماهواره‌ها و اطلاعات RS/GIS[2] در هدایت سلاح‌ها و مهمات دقیق و نقطه زن، دخالت عامل انسانی را به حداقل ممکن رسانده که یکی از دلایل مهم آن کاهش آسیب پذیری و تلفات نیروی انسانی و افزایش دقت و سرعت عمل سامانه‌های سلاح است. هوشمندسازی سامانه‌ها و بکارگیری آن‌ها تحت شبکه‌های پیشرفته زمینه کاربرد اینترنت اشیاء (نظامی) را با ویژگی‌های خاص آن فراهم نموده است بگونه‌ای که سامانه‌های سلاح نقطه زن شامل انواع مهمات و بمب‌های هوشمند، پهپادهای رزمی و موشک‌های کروز، متصل شده و تحت هدایت شبکه با استفاده از فناوری پیشرفته هوش مصنوعی و سامانه‌های هوشمند تصمیم سازی و تصمیم گیری خبره، به سهولت

[1] System of Systems
[2] Remout senssing/geographical information system

اهداف دور از دسترس و پنهان را که تحت تدابیر پدافندغیرعامل مناسبی هم قرار دارند، مورد اصابت قرار می‌دهند (فرجپور،۱۳۹۸ :۴۶). در خصوص تقویت شبکه پدافندهوایی، فرماندهی معظم کل قوا ؛ رصد و پایش روند تحول تهدیدها و آمادگی مقابله را همواره مورد تاکید قرار داده و مطالعه و بررسی در این زمینه را از بخش‌های پژوهشی مطالبه نموده‌اند. بنابراین رصد تهدیدهای فرا روی پدافند هوایی و فناوری‌های مورد استفاده در راستای انجام ماموریت که همانا دفاع نفوذناپذیر از آسمان امن کشور در برابر تهدیدهای دشمنان است؛ جهت حفظ آمادگی و مرتفع نمودن چالش‌ها می‌تواند به نوعی آینده نگری و آینده پژوهی در حوزه‌های مختلف باشد (جعفرزاده، ۱۳۹۸: ۹۱). در جنگ‌های آینده، اخلال در فعالیت‌های مراکز فرماندهی و کنترل، حساسه‌ها و سامانه‌های کشف و سامانه‌های سلاح و انهدام آن‌ها، و در یک کلام سرکوب پدافند هوایی[1] با انجام اقدامات نرم کشنده[2] و سخت کشنده[3] با تاکید بر فناوری‌های پیشرفته و سلاح‌ها و مهمات هوشمند و با رویکرد جنگ شبکه محور در دستور کار دشمن قرار دارد، لذا اتخاذ تدابیر لازم جهت مقابله متناسب با این تهدیدها با استفاده از دفاع شبکه‌ای هوشمند بسیار حائز اهمیت است. روند جنگ‌های آینده بیانگر این موضوع است که بلادرنگی، دقت و جامعیت در پاسخ به تهدیدها سرنوشت‌ساز بوده و گستردگی مکانی و جغرافیایی تهدیدها، زمان عمل یا عکس‌العمل را بسیار محدود نموده است (فرجپور، ۱۳۹۸: ۲۳). در این پژوهش برآن هستیم تا با توجه به تغییرات سریع فناوری، با رویکرد کاربرد اینترنت اشیاء در شبکه پدافند هوایی، به تحلیل محیطی این کاربرد از جنبه‌های مختلف و چالش‌های احتمالی بپردازیم.

مبانی نظری پژوهش و پیشینه‌ها

آیه ۶۰ سوره مبارکه انفال؛ کسب آمادگی دفاعی تا سر حدّ توان، پیش از رویارویی با تجاوز و تهاجم از سوی دشمنان و بازدارندگی و ارعاب آنان را مورد تاکید قرار داده است. در سند چشم انداز ۱۴۰۴کشور نیز بر ایران امن، مستقل، مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه تاکید شده، که برای دستیابی به این هدف، لازم است برنامه‌ریزی‌ها و پژوهش‌ها با کاربرد آخرین فناوری‌ها در حوزه‌های دفاعی، با دقت‌نظر و واقع‌نگری مورد توجه جدی قرار گیرند.

[1] SEAD: Suppression of Enemy Air Defence
[2] Soft kill
[3] Hard kill

مفهوم شناسی

۱) شـــبکه پدافنـد هوایی: مجموعه متشـــکل از مرکز عملیات پدافند هوایی، مراکز عملیات منطقه‌ای، مراکز کنترل و گزارش، پست‌های فرماندهی، سامانه‌های سلاح، و ارتباطات این اجزاء در راســتای انجام ماموریت پدافند هوایی که شـامل چهار مرحله؛ کشـف، شـناسـایی، رهگیری، درگیری و انهدام اهداف پرنده می‌باشد (نوروزی،۱۳۸۵ :۲۰۷).

۲) اینترنت اشـیاء: واژه اینترنت اشـیا، برای نخسـتین بار در سـال ۱۹۹۹ توسـط کوین اشـتون جهانی را توصـیف کرد که در آن هر چیزی، از جمله اشـیا بی جان، برای خود هویت دیجیتال داشـــته و به کامپیوترها اجازه دهند آن‌ها را ســـازملندهی و مدیریت کنند. اینترنت اشـــیاء دربرگیرنده تجهیزات تعبیه شده مبتنی بر IP[1] از قبیل حسگرها، لوازم و ماشین آلات، تجهیزات اتوماسیون ساختمان و... می‌باشد (تدین، ۱۳۹۴ : ۲۶).

۳) تهدیدها: فرهنگ آکسفورد تهدید را امکان به وحشت انداختن، ترساندن یا ایجاد فاجعه برای یک فرد یا جامعه و آســـیب زدن به کســـی یا چیزی و نتایج ناخوشـــایند به بار آوردن می‌داند (جعفرزاده، ۱۳۹۴: ۶۷). تهدید در برابر امنیت قرار می‌گیرد، به‌عبارتی تهدید، امنیت را به چالش کشـیده و آن را نفی می‌کند. در واقع امنیت تابع نوع، میزان و شـدت تهدید قرار دارد (حافظ‌نیا، ۱۳۸۵: ۱۳۳).

اینترنت اشیاء یک فناوری بین رشته‌ای است که به همگرایی شبکه‌ای، اجرا و نصب سخت‌افزار، معماری نرم‌افزار، فناوری‌های سنجش، مدیریت اطلاعات، تجزیه و تحلیل داده‌ها و تجسم منجر می‌شود و کلید آن، استفاده از شبکه‌های توزیع دستگاه بوده که از طریق پروتکل‌های اینترنتی و اغلب معماری‌های سرویس‌گرا[2] (شکل ۱)ارتباط برقرار می‌کنند. هر وسیله‌ای ممکن است با ارتباط از راه دور، به منظور جمع‌آوری اطلاعات یا کنترل، ارسال و اجرای فرامین، قابل استفاده باشد.

[1] Internet Protocol
[2] SOA: Service-Oriented Architectures

معماری IoT، (a) سه لایه، (b) برمبنای میان افزار، (c) برمبنای SOA، (d) پنج لایه

شکل (۱) معماری IoT

انتقال فناوری‌های اینترنت اشیاء در برنامه‌های کاربردی نظامی طبیعی است زیرا سازمان‌های نظامی به کالاهای تجاری بدون قفسه[1] برای مدیریت شناسایی فرکانس رادیویی[2] و فناوری‌های مرتبط، وابسته هستند (وایتمور و همکاران، ۲۰۱۴ :۳۶). همانگونه که پژوهش در مورد حوزه‌های پژوهشاتی نوظهور کاربرد تجاری اینترنت اشیاء با اهمیت است، ایجاد پتانسیل اینترنت اشیاء در مجموعه‌های نظامی باید محقق شود. از نگاه فرماندهی و کنترل، این حوزه‌ها، به دلیل افزایش پیچیدگی صحنه عملیات[3]، چالش‌های مهمی دارد و انتظار می‌رود در بخش حسگرهای جمع‌آوری اطلاعات، چالش امنیت و صحت اطلاعات را داشته باشیم، اما در بخش فرماندهی و فرمانپذیری مربوط به سامانه‌های عمل کننده و مجری فرامین، بحث امنیت، دقت و اعتماد پذیری یا قابلیت اطمینان، انطباق‌پذیری و نقش سامانه‌های ناظر و رصد کننده یا بازخوردگیر و در چرخه فرماندهی و کنترل؛ حسگرها، پردازش اطلاعات و فرآیند آن، ارسال فرامین و کنترل و نظارت بر اجرای آن‌ها و نیز موضوع آگاهی وضعیتی قابل تأمل است.

۴) برنامه‌ها و زمینه‌های کاربردی: از آنجایی که اینترنت اشیاء در حوزه نظامی، همچنان یک حوزه پژوهشاتی جدید می‌باشد، ارزیابی کاربرد فعلی نظامی و تجاری آن، برای شناسایی جنبه‌های پژوهشاتی مهم است که در این راستا برخی از سناریوهای قابل توجه اینترنت اشیاء ارائه می‌شود.

الف- سنجش همکاری در صحنه عملیات: دستگاه‌های اینترنت اشیاء، همراه با ارتباطات قوی و برد کوتاه، می‌توانند از روش سنجش حسگرهای دیگر، برای تکمیل روش‌های سنجش خود استفاده کنند. پس از تأیید اعتبار، می‌توان اطلاعات هر منبع را در اختیار شبکه قرار داد. خدمات

[1] COTS: Commercial-off –the Shelf
[2] RFID: radio frequency identification
[3] Scheme of operation

سنجش اینترنت اشیاء می‌تواند مزایای متعددی از جمله قرار گرفتن در معرض روندهای آماری، تشخیص ناهنجاری و سایر اشکال آنالیز داده را به همراه داشته باشد و برنامه‌ریزی مأموریت موقت را از طریق کاربرد حسگرها در انجام وظایف در ماموریت‌ها تسهیل نماید (تدین، ۱۳۹۴ : ۲۸). بکارگیری چند دستگاه در منطقه مورد نظر که هر کدام با تکیه بر سنجش مشارکتی برای تأمین نیازهای جدید یا غیرقابل پیش‌بینی، وظیفه و مأموریت خود را داشته و اتصال با یک محیط اینترنت اشیاء مشارکتی، منجر به افزایش آگاهی وضعیتی[1] و امکان ادامه و تکمیل مأموریت می‌شود. با توجه به زیرساخت اولیه اینترنت اشیاء شبکه یکپارچه می‌توان داده‌ها را از چندین عنصر جمع‌آوری و یک تصویر منسجم‌تر از منطقه و عوامل موجود ارائه داد که باعث می‌شود بخش عظیمی از مجموعه و پردازش‌ها، به صورت محلی به آگاهی وضعیتی، زمان عکس‌العمل و تصمیم‌گیری و کاهش نیازهای ارتباطات پشتیبان در چرخه اطلاعات سامانه فرماندهی و کنترل کمک نماید (رمضانی،۱۴۰۰ :۲۲۴).

ب- مدیریت لجستیک و زنجیره تأمین[2]: در برنامه‌های لجستیک نظامی، چندین حسگر با جمع‌آوری، یکپارچگی و انتشار اطلاعات که از یک هسته اینترنت اشیاء برای مواجهه با مأموریت‌های متنوع عملیاتی و جغرافیایی بهره می‌برند، مورد استفاده قرار می‌گیرد که در حال حاضر، استقرار چنین فناوری‌هایی محدود به محیط‌های امن و زیرساخت‌های گسترده با مشارکت انسانی بالا می‌باشد (وایتمور و همکاران، ۲۰۱۴). اینترنت اشیاء نظامی می‌تواند توزیع منابع و طبقات آمادی را در سطح شبکه پدافند هوایی امکان‌پذیر و برای ردیابی وضعیت سامانه‌ها و تجهیزات، از جمله وضعیت نگهداری و قطعات یدکی در هر وسیله برای تأمین مجدد اقلام با موجودی کم، استفاده گردد. حسگرهای متصل به اینترنت اشیاء، می‌توانند به طور بالقوه بر علائم فرسودگی، انتشار هشدارهای نگهداری و کاهش حوادث خرابی کامل نظارت داشته و آماد را با هشدارهای صادر شده برای تأمین مجدد نیازهای اعلام شده، تحت نظارت قرار دهند. با ایجاد روندها و رویکرد پیشگیرانه در مورد مسائل مربوط به نگهداری، آماد و مدیریت زنجیره تأمین، می‌توان برخلاف حالت واکنشی فعلی، با تجزیه و تحلیل در این سطوح، زنجیره تأمین را برای تحقق الزامات، ساده‌تر نمود.

پ- اجرای عملیات در محیط‌های بزرگ (شهر هوشمند): شهر هوشمند، محیطی از حسگرها و محرک‌های فراگیر برای ارائه خدمات نوآورانه شامل نظارت بر آلودگی، پارکینگ و ترافیک ،حمایت از امنیت و ممانعت از فعالیت‌های مجرمانه است. چنین سطوحی از کارایی در شبکه

[1] Situational Awareness
[2] Supply chain

فرماندهی و کنترل به‌عنوان ابزاری برای آگاهی وضـعیتی از صـحنه عملیات، سـودمند و برای محیط‌های غیرقابل دسـترسـی که امکان اسـتقرار تجهیزات حسـگر دشـوار باشـد، زیرسـاخت‌های اینترنت اشـیاء و شـهر هوشـمند می‌توانند به‌عنوان جانشـین عمل کرده که از کاربردهای نظامی می‌باشد (تدین، ۱۳۹۴ : ۲۸).

ت- ردیابی و سـنجش پارامترهای فردی: دسـتگاه‌های الکترونیکی شـخصـی با قابلیت عملکرد سـنجش فعال، مانند تلفن‌های هوشـمند با ردیاب جی پی اس[1] به شـکل رایانه‌های پوشـیدنی طراحی شـده‌اند که می‌توانند عملکردهایی از جمله ردیابی وضـعیت اندام را از طریق نظارت بر شـمارش قدم و ضـربان قلب انجام و با اسـتنباط وضـعیت جسـمی و روانی، حالت‌های غیرطبیعی مانند کم‌آبی، قند خون پایین یا ضربان قلب بالا را تشخیص داده و بر این اساس، هشدارهایی را برای اعضاء تیم ارسـال و با اسـکن محیط به عنوان حسـگرهای سـامانه فرماندهی و کنترل عمل نمایند.

- **فناوری‌های اینترنت اشیاء تجاری در دسترس**: سازوکاری‌های اولیه فناوری در بخش صنعت، در درجه اول جهت صـرفه‌جویی عملیاتی و بهره‌وری در بازار هدف هدایت شـده، که پیشـرفت قابل توجهی در کنترل صـنعتی، اتوماسـیون، کنترل فرآیند لجسـتیک و عملیات داشـته اسـت (تدین، ۱۳۹۴ : ۲۸). در بخش فناوری‌های اینترنت اشـیاء تجاری در دسـترسِ صـحنه عملیات، موارد برجسـته عبارت‌اند از؛ دسـتگاه‌ها، فناوری‌های ارتباطی دسـتگاه‌ها برای برقراری ارتباط با یکدیگر (و بقیه زیرسـاخت‌ها) و مدیریت مبتنی بر اَبر جهت جمع‌آوری و تجزیه و تحلیل داده‌ها که در ادامه آمده‌اند:

الف- دسـتگاه‌ها: دسـتگاه‌های اینترنت اشـیاء در حال حاضـر روی کنترل منزل، اتوماسـیون، خدمات شخصی و ارائه محتوای چندرسانه‌ای متمرکز هستند. سهم غیرقابل اغماض از دستگاه‌ها در بازار اینترنت اشیاء، طراحی شده برای محیط‌های پیچیده صنعتی اگر چه در رده کاملاً نظامی نیست، اما برای پذیرش در محیط‌های نظامی نسبتاً مناسب است (رمضانی،۱۴۰۰ :۲۲۶).

ب- ارتباطات: بسیاری از پروتکل‌های اینترنت اشیاء، یا از اسـتانداردهای بی‌سیم موجود اسـتفاده می‌کنند، یا تطبیقی با پروتکل‌های بی‌سـیم قبلی در بخش هدف هسـتند. پروتکل‌های مصـرفی عبارتند از: کن باس، سـی آی پی، اترنت، ایکس-۱۰، اینسـتون، زدویو، زیگبی، وای فای، بلوتوث و شـبکه‌های تلفن همراه[2]. بیشـتر این پروتکل‌های بی‌سـیم در باندهایی که نیازی به مجوز برای منطقه عملیاتی ندارند، کار می‌کنند. در این مرحله، مجموعه‌های تراشـه‌ای کاملاً یکپارچه، برای

---

[1] GPS

[2] Canbus, Zigbee, CIP, Ethernet, X10, Inston, Zview, Wifi, Bluetooth

بیشتر این پروتکل‌ها وجود دارد که به آسانی امکان یکپارچه‌سازی سخت‌افزار را فراهم می‌آورد (همان:۲۲۷).

پ- مدیریت اطلاعات مبتنی بر اَبر[1] : رایانش اَبری یک فناوری کلیدی توانمند برای برنامه‌های آینده اینترنت اشیاء است که به مقدار قابل‌توجهی از قدرت پردازش برای تجزیه و تحلیل نیاز دارد. با این حال، استفاده کارآمد از منابع مبتنی بر ابر برای اینترنت اشیاء نیاز به انتخاب دقیق معماری نرم‌افزارهای ارتباطات و پردازش دارد (وایتمور ، ۲۰۱۴). هر نمونه از داده‌های خام تولید شده برای تجزیه و تحلیل به ابر منتقل می‌شود که انتقال داده‌های خام از اینترنت اشیاء به ابر، فشار قابل توجهی را در زیرساخت‌های شبکه بی‌سیم ایجاد می‌کند و مرحله پردازش داده‌ها، یک روش پیچیده محاسباتی گران است که از روش‌ها و ابزارهای پیشرفته داده‌های بزرگ استفاده می‌کند. تأخیر بین زمان تولید داده و زمان دسترسی نتایج تجزیه و تحلیل، می‌تواند از اهمیت حیاتی در سناریوهای اینترنت اشیاء نظامی برخوردار باشند.

- **اینترنت اشیاء صحنه عملیات؛ الزامات و چالش‌ها**: دیدگاه‌های مختلفی برای قیاس اینترنت اشیاء تجاری با کاربردهای نظامی در خصوص موانع و محدودیت‌های متصور مطرح شده است. موانع فنی در مورد پذیرش اینترنت اشیاء نظامی شامل موارد ذیل است:

الف- زیرساخت‌های غیرمتمرکز تجزیه و تحلیل داده‌ها: برای این که کاربرد فناوری اینترنت اشیاء نظامی در محیط‌های میدان نبرد پویا، مداوم باشد انتظار می‌رود تجزیه و تحلیل داده‌ها در مقیاس بزرگ، در زمان تقریباً واقعی انجام شود. در اینجا، چالش‌های خاص نظامی از محدودیت زمانی در تجزیه و تحلیل داده‌ها، همراه با چالش‌های اتصال بالقوه ناشی می‌شود. یکی از ویژگی‌های موجود در محیط اینترنت اشیاء تجاری، اتصال همه جا و امکان اتکا به مراکز داده اَبر متمرکز است. حتی در صورت وجود شبکه‌های تلفن همراه یا بی‌سیم، زمانی که دستگاه به ایستگاه مبنا یا نقطه دسترسی می‌رسد، اتصال در همه جا گسترده و آن را برای هر دستگاه برای رسیدن به یک منبع مبتنی بر ابر، آسان می‌سازد. در نتیجه، اغلب دستگاه‌های اینترنت اشیاء بر بارگذاری اکثر داده‌ها از دستگاه‌ها به یک اَبر، که به طور معمول تحت مالکیت و یا مدیریت توسط ارائه دهنده می‌باشد، تکیه دارند. این معماری به ارائه دهنده اجازه می‌دهد تا اساساً مالکیت داده‌ها را برعهده بگیرد، آن را طبق نیاز مورد پردازش قرار داده و نتایج را به مصرف‌کننده انتقال دهد. در سطح شبکه پدافندهوایی که به شبکه‌های بی‌سیم و رادیوها تکیه دارد، هر رویکردی که نیازمند یک زیرساخت متمرکز مبتنی بر اَبر باشد به احتمال زیاد موثر نخواهد بود. شبکه‌های تاکتیکی اغلب دارای پهنای باند محدود هستند و به سرویس‌های

[1] Cloud based Information Management

مختلف مبادله داده‌های مهم مأموریت، اختصاص می‌یابد. علاوه بر این، اتصال در همه جا مانند محیط تجاری فراگیر نیست. بنابراین، یکی از چالش‌هایی که باید مورد توجه قرار گیرد، توسعه یک زیرساخت غیر متمرکز برای پشتیبانی از اینترنت اشیاء در صحنه عملیات است.

ب- کاربرد شبکه‌ای: در سناریوی نظامی تاکتیکی، زیرساخت‌های شبکه، به دلیل قطع ارتباطات مکرر، تقسیم‌بندی و نوسانات کانال رادیویی، به شدت محدود هستند. این موضوع می‌تواند به تغییر در دسترس بودن حسگر و همچنین محدودیت در استفاده از حسگرهایی که در تنظیمات تجاری، آنچنان آشکار نیستند، منجر شود که با توسعه شبکه‌های 5G و 6G قابل حل خواهدبود.

پ- قابلیت همکاری: یکی از محبوب‌ترین رویکردها برای افزایش قابلیت همکاری، استفاده از معماری‌های سرویس‌گرا[1] می‌باشد که با توجه به جنبه‌هایی از قبیل استفاده مجدد خدمات، قابلیت سازگاری با گردش‌های کاری پویا و پیکربندی سریع و مجدد، قابلیت همکاری سریع و پویا را دارند. معماری‌های سرویس‌گرا در حوزه تاکتیکی، سعی در برطرف کردن چالش‌های قابلیت همکاری ویژه برای C_4ISR را دارند و از این رو به خوبی با نیازهای قابلیت همکاری اینترنت اشیاء نظامی مطابقت دارند. در مقایسه سیستم‌های اینترنت اشیاء و به طور گسترده‌تر، معماری سرویس‌مدار، از دیدگاه نظامی و تجاری، بسیاری از چالش‌های منحصر به فرد در زیرساخت‌های نظامی برای تهدید قابلیت همکاری سیستم‌ها وجود دارند زیرا هم رایانه‌های نظامی و هم شبکه‌های حسگر، عمر کاری بیشتری نسبت به معادل‌های تجاری باید دارا باشند؛ در نتیجه نیاز بیشتری به پشتیبانی از دستگاه‌های قدیمی و پروتکل‌ها دارند. بعلاوه، استفاده از طرح‌های سخت‌افزاری متفاوت و استانداردهای داده، می‌تواند بر انسجام زیرساخت‌های نظامی اینترنت اشیاء تأثیر بگذارد و منجر به سیستم‌های مبتنی بر مدل استوپایپ[2] شود (وایتمور ، ۲۰۱۴).

ت- اعتماد و امنیت: از دیدگاه فرماندهی، بروزخرابی و اشکال در تجهیزات می‌تواند کار جمع‌آوری اطلاعات و عملیات برنامه‌ریزی‌شده را به خطر اندازد. تجهیزات نظامی می‌توانند در معرض خرابکاری و یا سازش با فعالیت‌های دشمن قرار گیرند که منجر به بروز وقفه‌های خدماتی یا انتشار اطلاعات نادرست شوند.

ث- کاربرد دستگاه و حسگر: محدودیت‌های تامین برق، یکی از مشکلات همیشگی در صحنه عملیات است. در حوزه نظامی، حسگرها و دستگاه‌ها احتمالاً با باتری یا شاید انرژی خورشیدی

[1] SOA: Service Oriented Architectures
[2] Stove pipe

کار کنند. در هر دو حالت، انتظار این است که دستگاه‌ها برای مدت زمانی طولانی یا حداقل برای مدت زمان ماموریت، دوام بیاورند. بنابراین، حسگرها و دستگاه‌ها باید در استفاده از توان خود کارآمد باشند و سیستم یا کاربر باید عاقلانه از آنها استفاده نمایند. اغلب تعویض باتری‌ها در دستگاه‌های مستقر، غیرعملی است. در مورد تجهیزات پوشیدنی، این انتظار که سربازان باتری‌های اضافه را به همراه تجهیزات خود داشته باشند، عملی نیست که این امر نشان می‌دهد سیستم باید آگاه بوده و تقاضاهای موجود بر روی این دستگاه‌ها را مدیریت کند. این انتظار که ناهنجاری لازم وسایل نظامی، محدودیت‌هایی را در قابلیت‌های عملیاتی آنها (به عنوان مثال، در اندازه سلول‌های باتری یا توانایی انتقال) اعمال کند، منطقی می‌باشد.

ج- کاربرد فناوری‌های وب معنایی: فناوری‌های وب معنایی قبلاً جهت برنامه‌های شبکه حسگر و تسهیل قابلیت همکاری داده‌ها بکار می‌رفت و برای پژوهشات و توسعه عمومی اینترنت اشیاء، مهم شناخته شده‌اند. انتظار می‌رود که برنامه‌های نظامی اینترنت اشیاء، کاربردهای مشابهی برای قابلیت‌های وب معنایی داشته باشند، که شامل پشتیبانی از یکپارچه‌سازی داده‌ها، استدلال و کشف محتوا است. با توجه به زمینه‌های چالش فنی مشخص شده، اتصال، تجزیه و تحلیل دیجیتالی و قابلیت همکاری، سه وجه از فناوری وب معنایی به عنوان قابلیت‌های مطلوب اینترنت اشیاء نظامی شامل؛ استانداردهای یکپارچگی باز، پشتیبانی استدلالی، و پشتیبانی برای مدیریت منشاء داده‌ها بشرح ذیل شناسایی شده‌اند:

۱) استانداردهای یکپارچگی باز: هدف اصلی استانداردهای یکپارچگی باز، که از طریق پشتیبانی آنتولوژی[1] (هستی‌شناسی) تعریف شده، تسهیل قابلیت همکاری میان دستگاه‌ها با اشکال مختلف توانایی و مالکیت است (شنگ[2] و همکاران،۲۰۱۳). برای کمک به تسهیل چنین قابلیت همکاری، آنتولوژی اینترنت اشیاء باید تلاش کند تا با استانداردهای جامعه موجود ادغام شود. به عنوان مثال، خصوصیاتی برای توسعه آنتولوژی شبکه حسگر معنایی تعریف کرده‌اند.

۲) پشتیبانی استدلالی: استدلال مبتنی بر آنتولوژی، نسبت به سیستم‌های مدیریت نظامی از جمله آنهایی که وظیفه‌ای با حسگرهای جفت شده برای وظایف مأموریت دارند، یک آنتولوژی را بر اساس چارچوب مأموریت‌های نظامی و معنایی[3] ارائه می‌کند که قادر است مشخصات حسگر را تعیین و ویژگی‌های مربوط به وظیفه را بیان کند. در شرایط اتصال شبکه محدود، از

[1] Ontologies
[2] Sheng
[3] MMF: Military Missions and Means Framework

چنین قابلیت استدلالی می‌توان برای ارزیابی مداوم چگونگی استفاده از منابع اینترنت اشیاء موجود، استفاده کرد.

۳) پشتیبانی برای مدیریت منشاء داده‌ها: منشاء داده‌ها به عنوان سابقه‌ای از اقدامات انجام شده برای تولید داده‌های خاص، معمولاً به عنوان یک مهم در ارزیابی کیفیت داده‌ها و قابلیت اطمینان شناخته شده است. این قابلیت می‌تواند برای تلاش‌های داده‌ای که در ارزیابی خودکار (یا نیمه خودکار) محتوا، مطلوب بوده‌اند، مفید باشد. در حال حاضر ویژگی W3CPROV [1] یک استاندارد اولیه برای نمایش منشاء دیجیتالی است که برای نشان دادن یک منشاء بر روی شبکه‌های اینترنت اشیاء توسعه یافته است.

فراتر از پیشرفت درک اساسی و مفاهیم مربوط به نظریه اطلاعات، مفاهیم مرتبه دوم مانند اعتماد، پذیرش و ارزش، نیاز به تاکید پژوهشاتی بیشتری دارند (شنگ و همکاران، ۲۰۱۳). علی‌رغم پژوهشات قابل توجه قبلی و مداوم در مورد مسائل امنیتی و حفظ حریم خصوصی در ادبیات دانشگاهی، هنوز هم جهت پاسخگویی کامل به مسأله تحقق چارچوب اعتماد جامع، پژوهشاتی لازم است که بتواند همه نیازمندی‌های اینترنت اشیاء نظامی را پشتیبانی کند (راگلین [2] و همکاران، ۲۰۱۷). بسیاری از رویکردهای مدرن که به موضوعاتی مانند اعتماد و ارزش می‌پردازند به سیاست‌ها و کنترل بین حوزه‌ای بستگی دارند. بنابراین پژوهشات اضافی باید با توجه به درجه روابط خصمانه که در محیط‌های میدان نبرد و محیطی که در آن تنوع یا عدم تنوع استانداردها زیاد باشد، هدایت، جهت‌گیری و محدود شود. برای رسیدگی به موضوع زیرساخت‌های توزیع شده برای تجزیه و تحلیل داده‌های اینترنت اشیاء، که برای سناریوهای نظامی بسیار مناسب است، پژوهش در مورد معماری‌های توزیع شده اَبر آغاز شده است، هدف پژوهشات این است که تعداد کمی از مراکز داده اَبری بزرگ، واقع در هسته شبکه که بیشتر منابع محاسباتی و ذخیره‌سازی در آن متمرکز بوده و همچنین تعداد زیادی از مراکز داده ابری کوچک در مرز بین اینترنت فعلی و اینترنت اشیاء (باسیم و وای فای)، گسترده و تکمیل شوند. این کار باعث می‌شود تا برنامه‌های کاربردی تجزیه و تحلیل داده‌ها، بتوانند از ماهیت ارتجاعی منابع مبتنی بر اَبر بهره‌مند شده و در عین حال فشار محاسبات را به اینترنت اشیاء نزدیک‌تر نمایند و از مزایای بارز آن در کاهش بارهای ارتباطی و زمان پردازش، برخوردار شوند. چندین مفهوم پژوهشاتی مانند "محاسبات اَبر"، "محاسبه لبه " و "اَبرهای اینترنت اشیاء محور"، توسط

[1] Provenance data Model W3C
[2] Roaglin

مؤسسه ارتباطات از راه دور استاندارد اروپا برای پرداختن به معماری‌های ابر توزیع شده، به منظور تجزیه و تحلیل داده‌های اینترنت اشیاء، پیشنهاد شده است.

همه داده‌های خام تولید شده توسط اینترنت اشیاء، به یک اندازه مهم نیستند و ممکن است برنامه‌هایی با تمرکز بر روی داده‌های مهم، به جای تلاش برای تجزیه و تحلیل هر بخش از داده‌های تولید شده، بهتر ارائه شوند، تمرکز بر مفاهیمی مانند کیفیت اطلاعات[1] و ارزش اطلاعات[2]. مفاهیم کیفیت و ارزش اطلاعات، ناشی از فعالیت اصلی هاوارد[3] بوده، که تلاش کرد تئوری اطلاعات شانون[4] را گسترش دهد تا هم ماهیت احتمالی عدم قطعیت‌هایی که ما را احاطه کرده‌اند و هم تأثیر اقتصادی که این عدم قطعیت‌ها خواهند داشت را در نظر بگیرد. این تلاش‌ها برای اینترنت اشیاء نظامی بسیار مهم است؛ زیرا پردازش و بهره‌برداری از اطلاعات، با توجه به ابزاری که در اختیار مصرف کننده خود قرار می‌دهد و او را در تصمیم‌گیری‌های مؤثرتر پشتیبانی می‌کند، از پتانسیل عظیمی برخوردار بوده و به طور قابل توجهی میزان منابع محاسباتی و پهنای باند مورد نیاز برای تجزیه و تحلیل و انتشار داده‌ها را کاهش می‌دهد.

علاوه بر این، سخت‌افزارهای مدرن و راه‌حل‌های محاسباتی نوظهور، برای سیستم عامل‌های اینترنت اشیاء، نیاز به معماری نرم‌افزارهای جدید دارند تا از فرصت‌های ارائه شده، به طور کامل استفاده نمایند. استفاده از سخت افزار در حال ظهور یا اینترنت اشیاء در حوزه نظامی، احتمالاً از طریق ارسال پویای مؤلفه‌های نرم‌افزاری تخصصی، که به طور عملی برای سیستم عامل‌های نوآورانه طراحی شده‌اند، می‌تواند منجر به افزایش قابل توجه در قدرت پردازش و کاهش مصرف انرژی شود. محققان، شروع به کار روی راه‌حل‌های میان افزار نموده‌اند که فقط رویکردها را در زمینه اینترنت اشیاء، کشف می‌کنند. به طور قطع نیاز به پژوهشات بیشتر، به ویژه در مباحث خاص نظامی مانند تخصیص پویای محاسبات مربوط به تجزیه و تحلیل داده‌ها (با توجه به در دسترس بودن سخت‌افزار تخصصی و مدل‌های برنامه‌نویسی مرتبط) و راه‌حل‌های ارتباطی قوی، وجود دارد.

با توسعه چهارمین فناوری صنعتی اینترنت (اینترنت اشیاء) و رایانش اَبری ، کشورهای پیشرفته از جمله ایالات متحده در حال بررسی کارایی دفاع ملی، بخش عمومی و نوآوری ملی و ایجاد زیرساخت برای محیط‌های رایانش ابری هستند. در این راستا کره جنوبی در حال تصویب قانون مربوطه و در نظر گرفتن چهارمین فناوری صنعتی در زمینه‌های مختلف است. به ویژه، این

[1] QoL: Quality of Information
[2] VoL: Value of Information
[3] Haward
[4] Shanon

برنامه در حال انطباق اَبر با سیستم فرماندهی و کنترل در بخش دفاع ملی است. با این وجود، اگر سیستم اطلاعاتی موجود با معرفی دستگاه‌های اینترنت اشیاء به سیستم رایانش اَبری تبدیل شود، نیازهای امنیتی موجود نمی توانند مشکلات مربوط به آسیب پذیری های امنیت رایانش اَبری را حل کنند. بنابراین، برای ساخت یک سیستم کنترل امن مبتنی بر اَبر، لازم است که الزامات امنیتی مربوط به رایانش اَبری اضافی را که در شرایط امنیتی موجود وجود ندارد، استخراج کرده و بر اساس آن، یک سیستم فرماندهی و کنترل ملی دفاع ملی ایجاد کرد (رمضانی، ۱۴۰۰ :۲۲۱).

همانطور که اشاره شد مانیتورینگ و جمع آوری اطلاعات آگاهی وضعیتی، صدور فرامین به نیروها و عناصر عمل کننده، لجستیک نظامی و زنجیره آماد، مدیریت توزیع منابع، امداد و نجات از جمله موارد و زمینه‌های کاربرد MIoT[1] هستند. دسته بندی ویژگی‌ها و موارد مرتبط در شکل شماره (۲) آمده است. در زمینه کاربردهای نظامی، ادغام دستگاه‌های مختلف اینترنت اشیاء در یک پلت فرم مشترک که لزوماً باید با پروتکل‌های نظامی اختصاصی، ساختار داده‌ها و سیستم‌ها تعامل داشته باشد، ضروری خواهد بود. در این شرایط، دستگاه‌ها و داده‌های اینترنت اشیاء همگن و با کنترل منشأ نخواهند بود (به عنوان مثال فروشنده منفرد / منبع / تامین کننده متعلق به آن).

[1] Military internet of things

ارتباطات/اتصال	امنیت	استانداردسازی	کاربردها	نیروی انسانی	آگاهی موقعیتی	سامانه شلیک	سیستم‌های خودکار	لجستیک	مدیریت امکانات
				ارتباطات تاکتیکی	GPS ، نقشه‌های دیجیتال	سلاح‌های حساس با هدفگیری دقیق	تشخیص و جلوگیری	تعمیر و نگهداری مبتنی بر شرایط	مدیریت انرژی
				مانیتور وضعیت فیزیولوژیکی	رهگیری/ آشکارسازی تهدید	سیستم‌های بدون سرنشین	ربات‌های سرباز	مدیریت تامین منابع	مدیریت پسماند
			دستگاه‌ها	گوشی امن	خودروهای نظامی	ناو/ کشتی	جنگنده	پرنده‌های بدون سرنشین	رایانه
			حسگرها	حسگر صوتی	لیزر	مادون قرمز/IR	تعیین موقعیت	حسگر بیولوژیک	آشکارساز هسته‌ای، شیمیایی
				آشکارساز RF	دوربین	RFID	حسگر دما	مانیتورینگ موتور	انرژی
			تحلیل‌ها	تحلیل داده بیولوژیکی			تجزیه تحلیل و پیش بینی		
			زیرساخت	سرورها		محاسبات مبتنی بر آبر DOD		سرویس‌های خصوصی آبری	

شکل(۲) ویژگی‌ها و زمینه‌های کاربرد MIoT (تدین، ۱۳۹۴)

- **کاربرد در سامانه‌های عملگر و اقدام کننده**(فرمان‌پذیری سامانه‌های اقدام کننده، سامانه‌های سلاح، سامانه‌های ارسال فرامین و کنترل)

استفاده از فناوری IoT در زمینه صدور فرامین در سامانه‌های فرماندهی و کنترل یکی از ابعاد متصور و ظرفیت‌های موجود در زمینه کاربرد این فناوری است. بعنوان مثال به کمک انواع حساسه‌های مرتبط به اینترنت اشیاء اطلاعات محیطی جمع‌آوری و پس از طی فرآیند چرخه اطلاعات در قالب آگاهی وضعیتی، تصویری جامع و بلادرنگ و مداوم برای سامانه فرماندهی و کنترل فراهم می‌نماید. پس از فرآیند تصمیم سازی و تصمیم گیری فرامین توسط شبکه یا همان اینترنت به اشیاء که همان سیستم‌های عمل کننده هستند ارسال می‌گردد و این سامانه‌ها بصورت هوشمند اقدامات مورد نظر را اجرایی و همزمان از فرآیند اقدام و نتیجه کار مراکز فرماندهی و کنترل را آگاه می‌کنند. در سامانه‌های فرماندهی و کنترل که با سیستم سلاح کار می‌کنند با وجود آگاهی وضعیتی دقیق و تصمیم سازی صحیح می‌توان با پذیرش میزانی از ریسک، فرامین را از طریق شبکه اینترنت به سامانه‌های شلیک ارسال و کیفیت فرآیند هدفگیری، شلیک و در نهایت انهدام هدف را رصد نمود. همچنین کاربرد این فناوری را در

زمینه ناوبری خودکار هوایی با استفاده از سامانه CNS/ATM[1] و استفاده از امکانات سرویس فلایت رادار ۲۴[2] می‌توان انتظار داشت (رحیمی،۱۳۹۸ :۶۵).

- **الزامات پدافند غیرعامل در معماری IoT سامانه فرماندهی و کنترل**: آنچه مسلم است در دیدگاه‌های سه گانه معماری سامانه فرماندهی و کنترل که همانا دیدگاه عملیاتی، فنی و سیستمی می‌باشند از هر منظر، کاربرد اینترنت اشیاء دارای الزامات اجرایی است که به لحاظ ایمن بودن در برابر تهدیدهای متنوع بایستی با رعایت جمیع جوانب توجه خاصی هم به الزامات پدافند غیرعامل شود. کاهش آسیب پذیری شبکه و اجزاء متصل به آن، پایدارسازی مجموعه و ارتقاء آن جهت مواجه با شرایط بحران، تداوم ماموریت و فعالیت‌های ضروری بطور ویژه بایستی در حوزه این الزامات همواره مد نظر قرار گیرد. با توجه به اهداف و کارکردهای پدافند غیرعامل که همانا افزایش بازدارندگی، کاهش آسیب پذیری زیرساخت‌ها و منابع، تداوم فعالیت‌های ضروری، ارتقاء پایداری و تسهیل مدیریت بحران در مقابل تهدیدها می‌باشد؛ کاربرد اینترنت اشیاء در سامانه‌های فرماندهی و کنترل بویژه در زیرسامانه‌ها، موضوعات امنیت در مقابل دسترسی غیر مجاز و ایجاد اختلال در دریافت، پردازش و ارسال اطلاعات (چرخه فرماندهی و کنترل) با نگاه سیستمی و در نهایت امنیت سایبری بسیار حائز اهمیت است. تهدیدهای این حوزه شامل توقف سرویس دهی، توقف زیرساخت، تخریب زیرساخت و تهدید امنیت ملی می‌باشد(فراهانی،۱۳۹۱) در عصر حاضر مدیریت زیرساخت‌های حساس توسط سیستم‌های فرماندهی و کنترل صورت می‌پذیرد. اخیرا بیشتر کشورها وابستگی زیادی به سیستم‌های سایبری و فرماندهی و کنترل پیدا نموده‌اند که با وجود مزایا و نقاط قوت، آسیب‌پذیری‌های ذاتی نیز به‌همراه دارد. در واقع تهدیدهای نوین از جمله تهدیدهای سایبری برآنند تا حصول اهداف را از طریق نابودی یا اختلال در سامانه‌های فرماندهی و کنترل پدیده‌های هوشمند محقق سازند. در حوزه‌ی نظامی در صورت اختلال در سامانه فرماندهی و کنترل، بخش عمده‌ای از امور لجستیک، ارتباطی، تجهیزاتی، تسلیحاتی، اطلاعاتی و ... غیرفعال شده یا با افت شدید کیفیت مواجه می‌شوند؛ لذا اختلال در سامانه فرماندهی و کنترل به معنی اختلال در عملکرد تمامی بخش‌های یک ارتش و ناتوانی آن خواهد بود. بنابراین علاوه بر نیاز به آموزش مفاهیم و ابعاد تهدیدهای سایبری و جنگ اطلاعات، الزامات پدافند غیرعاملی به منظور مقابله با این تهدیدها نیز ضروری می‌باشد.

[1] Communications, Navigation and Surveillance Systems for Air Traffic Management
[2] Flight radar 24

مارتین لیبیکی(۲۰۱۲)[1] هفت شـــکل مختلف جنگ اطلاعاتی را شـــامل؛ جنگ فرماندهی و کنترل، جنگ بر پایه اطلاعات که مشـــتمل بر طراحی حفاظت و ممانعت از دســـترســـی به سیستم‌هایی که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند، جنگ الکترونیک، جنگ روانی، جنگ و حمله هکرها به سـیسـتم‌های رایانه‌ای، جنگ اطلاعاتی ایجاد مانع در برابر جریان اطلاعات با هدف کسـب برتری اقتصـادی می‌داند و جنگ سـایبر را ترکیبی از همه موارد شش‌گانه بیان می‌کند .

شـبکه‌های اطلاعاتی در معرض چهار تهدید و آسـیب عمومی هسـتند؛ دسـتیابی غیر مجاز به داده‌ها، تغییر نادرست داده‌ها، جعل هویت، از کار انداختن سرویس و یا انکار آن.

حملاتی که شـبکه‌های نظامی با آن مواجه هسـتند، به مراتب گسـترده‌تر و جدی‌تر از حملاتی است که سیستم‌های غیرنظامی و تجاری را تهدید می‌کند. نیازمندی‌های امنیتی یک سـیسـتم اطلاعاتی را می‌توان بر حسـب چند مؤلفه عمده نظیر محرمانه بودن داده‌ها، جامعیت داده‌ها، در دسـترس بودن سـیسـتم و پیکربندی سـیسـتم تنظیم کرد. برآورده کردن نیازهای فوق نیازمند یک‌سری اقدامات حفاظتی و امنیتی مانند تصدیق هویت، صدور مجوز دستیابی، حسابرسی و ثبت وقایع و ممانعت از انکار عمل می‌باشـد. سـامانه فرماندهی و کنترل بر اسـاس واقعیت‌های موجود، مدلی از زیرسـاخت‌های ضـروری جهت رسـیدن اطلاعات به فرمانده ایجاد می‌نماید که برای رسـیدن به این هدف معماری‌های متفاوتی طراحی و اجرا شـده که نمونه بارز آن معماری C_4ISR[2]می‌باشـد (بختیاری،۱۳۹۱ :۴۱). از آنجایی‌که سـامانه فرماندهی و کنترل به سـطوح و فرایندهای مختلف پیچیده هوشـمند دسـترسـی دارد و آن‌ها را کنترل می‌نماید، لذا برای ایجاد اختلال در هر یک از این سطوح هوشمند، کافی است کنترل کننده آن بخش در سامانه مختل گردد. با ایجاد اختلال در ســـیســـتم فرماندهی و کنترل هدف، حداقل برای مدتی امکان تصـمیم‌گیری و اقدام متقابل از آن سـلب شـده و در بهترین حالت با صـرف منابع می‌تواند به احیای خود بپردازد. هر سـیسـتم فرماندهی و کنترل مبتنی بر اطلاعات، ارتباطات، محاسـبات و کنترل بر فرآیند آن‌ها اسـت. بر اسـاس آنکه اختلال در کدام یک از این موارد ایجاد شـود، نوع تهدید متفاوت خواهد بود. کلیات تهدیدها از طریق حذف، توقف، تحریف، ایجاد تأخیر در اجرا یا جابجایی اولویت در فرایندها و دستورات هر کدام از موارد چهارگانه حاصل می‌شود (شکوهیان راد،۱۳۹۸).

---

[1] Martin libki

[2] Command, Control, Computer, Communication, Intelligence, Surveiliance & Reconnaissance

-**حمله سایبری و سلاح سایبر:** اصولاً هرگونه نفوذ به قصد ایجاد اختلال در شبکه و سامانه‌های اطلاعاتی و امنیتی شامل؛ تلاش برای نفوذ به شبکه، تلاش برای سرقت، خرابکاری یا دستکاری و جعل اطلاعات حمله سایبری گفته می‌شود (میر رفیع، ۱۳۹۴). ابزارهای لازم برای انجام این‌گونه حملات شامل سلاح سایبر اعم از نرم افزارهای ایجاد اختلال در مراکز ذخیره داده‌ها یا منطق پردازش رایانه‌ها را در برمی‌گیرد. سلاح‌های سایبر شامل ابزارهای آفندی مانند ویروس‌های رایانه‌ای و اسب تروا، عدم دسترسی به سرویس[1]، ابزارهای دارای کاربرد دو منظوره مانند اسکنرهای تشخیص آسیب‌پذیری پورت و ابزارهای پایش شبکه و ابزارهای پدافندی مانند ضد بدافزارها، تشخیص هویت، رمزنگاری و دیواره آتش هستند. دیگر ابزارهای مورد استفاده عبارت‌اند از: سلاح‌های اختلال‌زا (جمینگ)، تزریق توان بیش از حد (اورپاورینگ)[2]، افت کیفی ارتباطات، توسط هکرها و نیروهای سایبری (اندیشکده کاوشگران آینده، ۱۳۹۸).

- تهدیدهای شبکه پدافند هوایی در دوران معاصر:

ایجاد تهدیدها در داخل محیط هوا فضای خودی باعث کاهش زمان واکنش از چند ده ثانیه تا یک دقیقه می‌شود و میزان پوشش دفاعی برای کشف تهدیدهای متناسب با طرح‌های پدافند پیرامونی را به شدت افزایش می‌دهد (Evans, R.C, 2003: 1-3). تهدیدهای متصور پدافند هوایی در سه حوزه کشف، فرماندهی و کنترل و سیستم سلاح به شرح ذیل بررسی می‌گردند:

الف)تهدیدهای مربوط به حوزه کشف:

تهدیدهای حوزه کشف بعنوان اولین مرحله اجرای ماموریت پدافند هوایی شامل؛ تهدیدهای(پرنده‌های) مخفی در ترافیک هوایی پرحجم و زمان واکنش فوق العاده کم، پهپادهای با مداومت پروازی زیاد[3]؛ پرنده‌های پنهانکار با RCS[4] کم، موشک‌های کروز، موشک‌های بالستیک، و تجهیزات نظامی متعارف دارای حجم و سرعت بالا در حمله علیه پدافند هوایی[5] می‌گردند (محمدی، ۱۳۸۸، ۱۴۰).

ب)تهدیدهای سامانه‌های فرماندهی و کنترل دفاع هوایی:

تهدیدهای این سامانه‌ها به لحاظ ماهیت از نوع سخت و نرم شامل؛ سامانه فرماندهی و کنترل فراگیر و گسترده دشمن مجهز به انواع تجهیزات رصد و شناسایی و درگیری زمین‌پایه، هواپایه و فضاپایه، توانمندی سایبرالکترونیک، ماهواره‌های شناسایی و جاسوسی، سامانه‌های ناوبری

---

[1] Denial of Service
[2] Overpowering
[3] Long endurance UAVs
[4] Radar cross section
[5] Suppression of Enemy Air Defense (SEAD)

جهانی، شبکه اطلاع‌رسانی جهانی، تحریم‌های اعمال شده بر علیه توان دفاعی کشور، هواپیماهای رادار گریز یا پنهان کار، کثرت اشیاء پرنده و حضور دشمن در قالب گروه‌های معارض در سرزمین خودی، نا امن شدن هر چه بیشتر فضای ارتباطی، توسعه حسگرهای رایانه‌ای در ابعاد نظامی، انرژی مستقیم و سلاح‌های الکترومغناطیس، موشک‌ها و بمب‌ها، انواع هواپیماهای باسرنشین و بدون سرنشین و موشک‌های بالستیک و کروز، تهدیدهای نرم شامل انواع و اقسام برنامه‌ها و نرم‌افزارها و یا پیام‌های جنگ و عملیات روانی می‌شود. تهدید سایبری و تاثیر آن بر شبکه به‌طور عمده اخلال در سامانه فرماندهی و کنترل بوده و روش مقابله؛ تهیه و تولید سامانه‌های خود-محافظتی با قابلیت کشف حملات سایبری می‌باشد (بختیاری، ۱۳۹۹ :۲۱).

پ)تهدیدهای سامانه‌های سلاح دفاع هوایی: اولین لایه دفاع هوایی هواپیماهای رهگیر گشت رزمی هوایی[1] و سامانه‌های موشکی برد بلند و ارتفاع بالا هستند. امروزه با توجه به تهدیدهای مشتمل بر انواع موشک‌های بالستیک و کروز و پرنده‌های با سرنشین و بدون سرنشین لایه اصلی در پدافند هوایی شامل موشک‌های سطح به هوای کوتاه برد ارتفاع کم، ارتفاع متوسط و ارتفاع بالا و دور برد نقشی پیشرو در مقابله با تهدیدهای این حوزه بر عهده دارند (منطقی، ۱۳۹۱: ۶۵). تهدیدهای این بخش از شبکه پدافند هوایی نیز علاوه بر تهدیدهای سخت ذکر شده، تهدیدهای نرم مانند حمله الکترونیکی[2]، حملات سایبری و حملات شبکه محور، کشف و موقعیت‌یابی توسط انواع حساسه‌های دشمن می‌گردد. از منظر سایبری هر سامانه فرماندهی و کنترل مبتنی بر مولفه‌های اطلاعات، ارتباطات، محاسبات و کنترل است که هر کدام دچار اشکال شوند عملکرد سامانه فرماندهی و کنترل مختل می‌گردد. بر مبنای اختلال در هر یک از ارکان چهارگانه فرماندهی و کنترل ایجاد نوع تهدید متفاوت خواهد بود. کلیات تهدیدها از طریق حذف، توقف، تحریف، ایجاد تأخیر در اجرا یا جابجایی اولویت در فرایندها و فرامین هر کدام از ارکان چهارگانه حاصل می‌شود (شکوهیان راد، ۱۳۹۷).

حوزه‌های تهدیدهای سایبری

- جاسوسی سایبری: با هدف؛ شنود، سرقت، نفوذ، افشاء، جمع‌آوری اطلاعات است و ابزار تهدید شامل: بدافزار، فیشینگ، هک، جعل هویت، فریب، حملات سایبری

- خرابکاری سایبری: با هدف؛ نابودی و تخریب، اختلال یا منع سرویس، دستکاری یا تغییر، درز و نشت اطلاعات. ابزار تهدید: باج افزار، بد افزار، فیشینگ، هک، جعل هویت، فریب و حملات سایبری

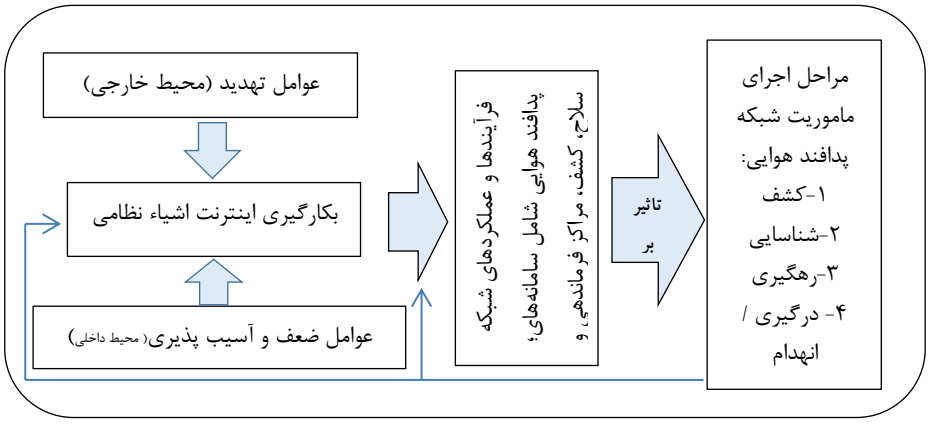
[1] CAP: Combat Air Patrol
[2] EA: Electronic Attack

- مجرمان و عوامل ناراضی: با هدف؛ سرقت، نابودی، تخریب، انکار، دستکاری یا تغییر، درز و نشت اطلاعات. ابزار تهدید: بدافزار، جعل هویت، ابزارهای ذخیره ساز

- آسیب پذیری‌های سایبری: با هدف؛ انکار، اختلال یا قطع سرویس، نابودی و تخریب، درز و نشت اطلاعات، افشا. ابزار تهدید: بدافزار، ابزارهای ذخیره ساز، رایانه‌های تک کاربره و همراه، پیکربندی و تنظیمات نامناسب شبکه، عدم کنترل، منابع انسانی فاقد صلاحیت (محمودزاده و همکار:۱۳۹۷).

مدل مفهومی پژوهش

مدل مفهومی پژوهش با رویکرد سیستمی و لحاظ ابعاد مختلف شامل عوامل بیرونی(تهدیدها و فرصت‌ها)، فرآیندها و عملکرد سامانه‌ها و بروندداد(اجرای ماموریت) بشرح زیر ارائه می‌گردد:



شکل (۳) مدل مفهومی پژوهش

پیشینه شناسی

تاج ترکمن و معدنی (۱۳۹۶) در مقاله‌ای تحت عنوان طبقه بندی موضوعات اینترنت اشیاء و درجه بندی حساسیت آن‌ها، نقش موضوعات مرتبط با اینترنت اشیاء(حسگرها، ارتباطات، فعال کننده‌ها، فضای ذخیره سازی، دستگاه‌ها، پردازش، محلی سازی و ردیابی، شناسایی و تعیین هویت) در مباحث امنیتی (محرمانگی، جامعیت، دسترس پذیری، احراز هویت و حریم خصوصی) را بررسی و میزان حساسیت هریک را مشخص نموده‌اند. اسکوبی و تدینی (۲۰۱۷) در پژوهشی با عنوان تهدیدهای امنیت سایبری اینترنت اشیاء در حوزه خدمات و برنامه‌های کاربردی، به بررسی آسیب‌پذیری‌ها و تهدیدهای امنیت سایبری اینترنت اشیاء پرداخته و با تجزیه و تحلیل آن‌ها در مقابل بازیگران تهدیدهای بالقوه، پنج نوع تهدید شامل حمله فیزیکی (تجهیزات)، حمله به نرم‌افزار، حمله به شبکه، حمله به وب و داده‌ها را معرفی نموده‌اند.

غلام نژاد و همکاران (۱۳۹۸) در مقاله‌ای با عنوان کاربردهای نظامی اینترنت اشـــیاء با تأکید بر مأموریت های نهاجا، به منظور بررسـی مسـیرهای ایجاد بسـتر لازم جهت بهره برداری از فناوری اینترنت اشـیا در مأموریت های نیروی هوایی، به پتانسـیل های انبوه فناوری های اینترنت اشـیاء، مواردی از دفاع و امنیت عمومی مبتنی بر شـــبکه تلفن همراه، که در آن می‌توان با بهره‌گیری از ویژگی‌های اینترنت اشـیا، قابلیت های بی شـماری در کنترل تجهیزات و سـامانه های دفاعی به دست آورد، اشاره نموده و نتیجه آن، پیاده سازی یک سامانه قطع و وصل کننده جریان برق با قابلیت کنترل از راه دور جهت اســـتفاده در محیط های نظامی و جنگی با اســـتفاده از رله های الکترونیکی اسـت. حسـینی (۱۳۹۵) در مقاله‌ای با عنوان اینترنت اشـیاء، چالش‌ها و راه‌کارها، به این نکته می‌رسـد که امنیت، تعداد بسـیار زیاد داده ها، عدم وجود زیر سـاخت ها، تعداد بسـیار زیاد وسـایل و تجاری سـازی از چالش های پیش رو اینترنت اشـیاء اسـت و راهکارهایی مانند رمزگذاری، اسـتفاده از پلت فرم های جدید، هوشـمند سـازی اشـیاء و پیروی ازالگوهای معماری مختلف نیز از راهکارهای مواجه با این چالش‌های می باشـــد. یزدان پناه (۱۳۹۵) در مقاله‌ای با عنوان اینترنت اشـــیاء (IoT): کاربردها، فناوری‌ها و چالش‌های مورد بحث، به بررســـی اجمالی اشـیاء و دسـتگاه‌های نامتجانس که قابلیت آدرس‌دهی و درنتیجه قابلیت کنترل پذیری دارند، از دیدگاههای مختلف پرداخته و ســـپس با معرفی کاربردهای زمینـه‌ها و حوزه های گوناگون، جدیدترین فناوری های ارائه شـده برای پیاده سـازی اینترنت اشـیاء و مهمترین چالش‌های مورد بحث را ارائه نموده اسـت. خادم دقیق و همکاران (۱۳۹۸) در مقاله‌ای الگوی فرماندهی و کنترل هوایی در جنگ‌های آینده با هدف تبیین الگو، به تبیین ابعاد و مؤلفه‌های الگوی فرماندهی و کنترل هوایی در جنگ‌های آینـده پرداختـه چهار بعـد فرمانـدهی و کنترل، مراقبت، رایانـه و ارتباطات، اطلاعات شـــناســـایی و الکترونیکی به همراه ۳۱ زیرمؤلفه، به این نتیجه رســـیده که ســامانه‌های فرماندهی و کنترل در تمامی ســطوح جنگ با ویژگی‌های اطمینان‌پذیری بیشــتر- پاسـخگویی سـریع‌تر؛ انعطاف‌پذیری مناسـب- پشـتیبانی آسـان‌تر؛ تعامل پذیری- هزینه کم‌تر؛ گرایش به مأموریت- گرایش به کاربر، موجب ایجاد شـبکه‌های مختلف(متمرکز و غیرمتمرکز) در نیروهای مسـلح گردیده تا مدیریت و فرماندهی هماهنگ را در زمان صـلح و جنگ، مقدور سـازد. این ســـامانه‌ها با بهره‌گیری از قابلیت‌ها و امکانات موجود ســـعی دارد تا در ایجاد هماهنگی، همکاری و مشـارکت در انجام فعالیت‌های آفندی و پدافندی نیروهای مسـلح، نقش موثر و تعیین کننده داشـــته باشـــد. میرمحمدیان و همکاران (۱۳۹۶) طی پژوهشـــی با عنوان راهکارهای پیشـگیری از چالش‌های اینترنت اشـیاء، چالش‌ها را شـامل داده‌های عظیم تولید شـده، نبود اسـتاندارد لازم ارتباطات اشـیاء و امنیت می‌دانند. در اینترنت اشـیاء هر دسـتگاه متصـل می‌تواند

یک درگاه احتمالی به زیرساخت اینترنت اشیاء باشد، نگرانی امنیت داده‌ها بسیار مهم است اما با ورود پیچیدگی، نقاط ضعف امنیتی و آسیب پذیری‌های احتمالی در مواردی مانند قابلیت همکاری، ترکیبات و تصمیم‌گیری‌های خودگردان خطرات احتمالی مربوط به اینترنت اشیاء سطح جدیدی به خود می‌گیرد. رمضانی و موحدی صفت (۱۴۰۰) در پژوهشی با عنوان رتبه بندی تهدیدهای اینترنت اشیاء در محیط نظامی، به این نتیجه رسیده‌اند که از میان تهدیدهای مختلف این حوزه، تهدیدهای مبتنی بر نقص امنیت فیزیکی سامانه‌ها از اهمیت بیشتری برخوردار است. بهشتی و همکاران (۱۳۹۵) در پژوهشی با عنوان اینترنت اشیاء نظامی مفهوم و چالش‌های امنیتی کاربرد IoT در حوزه‌های نظامی جزء جدانشدنی و اضطراری توسعه اطلاعاتی نظامی است. به نظر می‌رسد که به زودی شاهد شبکه‌های اینترنت اشیاء نظامی خواهیم بود که در آن نقش انسان کمرنگ‌تر می‌گردد و با توجه به دامنه کاربردهای اینترنت اشیاء نظامی و اهمیت وجودی آن‌ها، شاید بتوان گفت که بحث امنیت اصلی‌ترین چالش MIoT[1] محسوب می‌گردد، وجود یک آسیب‌پذیری در هر یک از بخش‌ها و اجزای اینترنت اشیاء نظامی می‌تواند به بروز خسارت‌های جبران ناپذیری گردد. نتایج پژوهش بختیاری (۱۳۹۹) در خصوص تهدیدهای مراکز فرماندهی و کنترل در جنگ‌های آینده موید آن است که پیشرفت فناوری نظامی در ابعاد مختلف و بویژه در زمینه سامانه‌های فرماندهی و کنترل و عدم توانمندی برخی کشورها در این رقابت سنگین، آنها را به فکر چاره‌ای دیگر وا داشته تا از طریق نفوذ به شبکه‌های ارتباطی، کشورهای دارای فناوری پیشرفته را در بکارگیری فناوری‌های پیچیده نظامی و غیر نظامی دچار مشکل کنند. جنگ سایبری در سامانه‌های ارتباطی باعث خواهد شد تا شبکه برق، شبکه کنترل ترافیک هوایی، شبکه بانکی و مالی، شبکه مخابرات و شبکه‌های رادیو تلویزیون، ماهواره و اینترنت دشمن بطور کامل فلج شده و او را درگیر ازهم گسیختگی در جامعه، تظاهرات خیابانی و بحران سیاسی کند و در صورت کاربرد مخابرات تجاری، سامانه‌های فرماندهی و کنترل نیز دچار آسیب جدی خواهد شد. جاهون‌کو و همکاران (۲۰۲۰) در پژوهشی با عنوان معماری امنیتی برای سامانه فرماندهی و کنترل (رایانش)ابری پایه[2] در محیط IoT؛ به منظور ایجاد سامانه فرماندهی و کنترل بر مبنای رایانش ابری و ایجاد معماری مربوطه، نیاز است سایر نیازمندی‌های امنیتی مرتبط با این رویکرد را که ملزومات امنیتی موجود فاقد آن‌ها است، تامین و یک معماری امنیتی همراه با یک سازه ابر پایه بسته باز[3] پیاده سازی شود.

[1] Military internet of things
[2] Cloud-Based
[3] Open- stack- based cloud platform (OpenStack)

روش‌شناسی پژوهش

پژوهش حاضر از نوع کاربردی- توسعه ای است، زیرا هدف تحلیل بکارگیری اینترنت اشیا در شبکه پدافندهوایی شناسایی و تبیین آسیب پذیری‌ها و چالش‌های است و به افزایش دانش در این زمینه کمک می نماید. جامعه آماری پژوهش شامل مجموعه مدیران، فرماندهان، خبرگان و کارشناسان نظامی در سطوح عملیاتی آشنا به حوزه این پژوهش و مباحث مرتبط هستند، بنابراین در نمونه گیری به روش هدفمند تعداد ۱۶ نفر برای مصاحبه عمیق انتخاب شد. بر این اساس پژوهش به روش تحلیل محتوا انجام شد.

مراحل اجرای پژوهش: با توجه به اینکه تحلیل محتوا روشی برای گرفتن نتایج معتبر و قابل اعتماد از داده‌های استخراج شده از متن است بنابراین دارای فرایند مشخصی است. براین اساس ابتدا با توجه به هدف پژوهش اقدام به انجام مصاحبه عمیق شد. پس از پیاده سازی و محدود کردن متن مصاحبه‌ها، واحد تحلیل و ثبت هر پیام در داخل کروشه مشخص و براساس آن مقوله‌های فرعی شکل گرفت. سپس با پالایش مقوله‌های فرعی اقدام به تعیین مقوله‌های اصلی گردید و در نهایت تهدیدها و آسیب‌پذیری‌های بکارگیری اینترنت اشیاء در شبکه پدافندهوایی با دسته بندی مورد نظر به دست آمد که در واقع چالش‌های این حوزه هستند.

تحلیل مصاحبه‌ها و داده‌های به دست آمده: در طی پژوهش با ۱۶ نفر از متخصصان و خبرگان و فرماندهان آشنا به شبکه مصاحبه انفرادی انجام شد و مقوله‌های حاصل از آن در انتهای هر واحد ثبت و در داخل کروشه قرار گرفت.

مقوله های فرعی: در این قسمت با توجه به هدف پژوهش «واحد تحلیل» انتخاب و مقوله‌های فرعی متن بر اساس آن تعیین می‌گردد. واحد تحلیل (واحد بررسی) بخش خاصی از محتواست که با توجه به هدف و متغیرهای مورد نظر مورد تحلیل قرار می‌گیرد. در این مرحله تعداد ۱۶ مقوله فرعی حاصل از تحلیل داده‌ها به دست آمد.

دسته بندی، تلخیص، پالایش مقوله های فرعی: در این مرحله مقوله‌های به دست آمده مورد ارزیابی و پالایش قرار گرفته و مقوله‌هایی انتخاب می‌شوند که با اهداف و سئوال‌های پژوهش مطابقت بیشتری داشته باشند. در این راستا، ارزیابی و پالایش از طریق حذف، اصلاح و یا ادغام مقوله‌های مشابه و تکراری صورت می‌گیرد (نصر، ۱۳۸۳). در مجموع تعداد ۱۳ مقوله فرعی از ۱۶ مقوله پالایش شده به دست آمد. جدول(۱) نشان‌دهنده مقوله‌های فرعی پالایش شده نهایی است.

جدول (۱)مقوله‌های فرعی پالایش شده بر مبنای نظر مصاحبه شوندگان

ردیف	مقوله فرعی	کد (مصاحبه شونده‌ها)
۱	چالش‌های امنیت داده‌ها و دسترسی به اطلاعات طبقه بندی شده	۱-۲-۵-۶-۷-۸-۱۴
۲	مشکلات کیفیت و امنیت ارتباطات و سامانه‌های ارسال و تبادل اطلاعات	۱-۲-۳-۵-۸-۱۱
۳	امکان نفوذ به شبکه‌ها، تهدید هکرهای وابسته به نیروهای سایبری و یا سایر هکرها	۲-۳-۵-۱۴
۴	مناسب نبودن مخابرات تجاری و نیاز به توسعه یک زیرساخت غیر متمرکز برای پشتیبانی از اینترنت اشیاء در صحنه عملیات	۴-۵-۷-۸-۱۰-۱۱-۱۴
۵	نیازمندی تامین یک معماری امنیتی همراه با یک سازه ابر پایه منبع باز	۲-۴-۵-۶-۱۱-۱۴
۶	چالش‌های صحت، دقت و اعتماد پذیری یا قابلیت اطمینان، انطباق‌پذیری اطلاعات، ارسال فرامین و کنترل و نظارت بر اجرای آن‌ها و نیز موضوع آگاهی وضعیتی	۷-۸-۹-۱۰-۱۴
۷	خرابکاری در تجهیزات یا جایگزینی تجهیزات جهت تولید اطلاعات فریبنده	۸-۱۴
۸	مسائل مربوط به قابلیت اطمینان دستگاه‌ها، تمرکز بر عدم قطعیت در فناوری‌های اینترنت اشیاء ، مدیریت اثبات و اعتماد ، سازوکارهای اعتماد و پیشرفت	۵-۷-۱۰-۱۴
۹	مشکل قطعی و اختلال ارتباطات، پردازش داده‌های خام دستگاه‌ها توسط یک اَبر محلی ، غیر متمرکز کردن منابع محاسباتی	۱-۴-۵-۱۱
۱۰	چالش‌های قابلیت همکاری ویژه شبکه C4ISR ، مشکل قابلیت همکاری سیستم‌ها در زیرساخت‌های نظامی	۱۲-۱۳
۱۱	مشکل اعتماد و امنیت، بروز خرابی در تجهیزات، اقدامات عمدی خرابکارانه، وقفه‌های خدماتی یا انتشار اطلاعات نادرست	۳-۸-۱۱-۱۴
۱۲	نیاز به پایداری منابع برق (اختصاصی) در شبکه‌های نظامی بر خلاف محیط تجاری	۱۵
۱۳	نقض حریم شخصی، آسیب‌های اتکای بیش از اندازه بر فناوری، کاهش فرصت‌های شغلی	۱۶

مقوله‌های اصلی

در این مرحله محقق به دنبال آن است تا پیوند بین مقوله‌های فرعی را از طریق توسعه(تولید) مقوله‌های اصلی و تعیین و اختصاص دادن مقوله‌های فرعی به آن‌ها مشخص نماید؛ یعنی هریک از مقوله‌های فرعی به دست آمده از مرحله قبل، صرفا در قالب یک مقوله اصلی طبقه بندی و سازماندهی شده و برای هریک از مقوله‌های اصلی نام مناسبی انتخاب می‌گردد، جهت نامگذاری مقوله‌ها سعی بر این است که براساس مفاهیم مشترک و مشابهی که از مقوله‌های فرعی به دست آمده، نامی انتخاب شود که بیشترین ارتباط منطقی را با داده‌هایی که مقوله نمایان‌گر آن است، داشته باشد (نصر، ۱۳۸۳).

جدول (۲) مقوله‌های اصلی و فرعی مرتبط

ردیف	مقوله اصلی	مقوله‌های فرعی	ویژگی‌ها و قابلیت‌ها
۱	چالش حوزه داده‌ها و اطلاعات	چالش‌های امنیت داده‌ها و دسترسی به اطلاعات طبقه بندی شده	وجود داده‌های طبقه بندی شده، پردازشگرهای ویژه، پایداری مراکز عملیات، حساسیت تجهیزات ارسال و دریافت داده‌ها(حسگرها، خطوط ارتباطی و...) قابلیت رهگیری و شنود ارتباطات، نفوذ و خرابکاری، سرقت، اختلال، فریب، مراقبت و شناسایی، تخریب
		امکان نفوذ به شبکه‌ها، تهدید هکرهای وابسته به نیروهای سایبری و یا سایر هکرها	
		نیازمندی تامین یک معماری امنیتی همراه با یک سازه ابر پایه منبع باز	
۲	چالش حوزه سرورها (خدمات) و نرم افزار	چالش‌های صحت، دقت و اعتماد پذیری یا قابلیت اطمینان، انطباق‌پذیری اطلاعات، ارسال فرامین و کنترل و نظارت بر اجرای آن‌ها و نیز موضوع آگاهی وضعیتی	ویژگی‌های مربوط به پردازشگرها و نرم افزارهای مورد نیاز پردازش و انتشار اطلاعات - صحت و دقت عملکرد و احتمال خطا و اشتباه سامانه‌ها، ویژگی امنیت سرورها
		مسائل مربوط به قابلیت اطمینان دستگاه‌ها، تمرکز بر عدم قطعیت در فناوری‌های اینترنت اشیاء، مدیریت اثبات و اعتماد، سازوکارهای اعتماد و پیشرفت	
۳	چالش‌های (سخت افزاری) شبکه و زیرساخت	مشکلات کیفیت و امنیت ارتباطات و سامانه‌های ارسال و تبادل اطلاعات	کیفیت عملکرد سامانه‌های عملگر و اقدام کننده(سامانه‌های سلاح، مراکز عملیات) تحت شبکه- ویژگی‌های زیر ساخت ارتباطات و شبکه مخابرات- الزامات نیاز به مراکز پردازش مبتنی بر ابر منبع باز
		نیاز به پایداری منابع برق (اختصاصی) در شبکه‌های نظامی بر خلاف محیط تجاری	
		مناسب نبودن مخابرات تجاری و نیاز به توسعه یک زیرساخت غیر متمرکز برای پشتیبانی از اینترنت اشیاء در صحنه عملیات	
		مشکل قطعی و اختلال ارتباطات ، پردازش داده‌های خام دستگاه‌ها توسط یک اَبر محلی، غیرمتمرکز کردن منابع محاسباتی.	
		چالش‌های قابلیت همکاری ویژه شبکه C4ISR ، مشکل قابلیت همکاری سیستم‌ها در زیرساخت‌های نظامی	
۴	چالش حوزه کاربران	خرابکاری در تجهیزات یا جایگزینی تجهیزات جهت تولید اطلاعات فریبنده	شیوه‌ها و روش‌های نفوذ انواع هکرها، ویژگی حملات سایبری، ویژگی حملات الکترونیکی، ویژگی و شرایط کارکنان و کاربران شبکه
		مشکل اعتماد و امنیت ، بروز خرابی در تجهیزات ، اقدامات عمدی خرابکارانه ، وقفه‌های خدماتی یا انتشار اطلاعات نادرست	
		نقض حریم شخصی، آسیب‌های اتکای بیش از اندازه بر فناوری، کاهش فرصت‌های شغلی	

در این گام ۹ مقوله فرعی ویرایش شده در قالب چهار مقوله اصلی شامل تهدیدها و چالش‌های مربوط به: داده‌ها و اطلاعات، سرورها(خدمات رسان‌ها) و نرم افزار، شبکه و زیرساخت، کاربران با ویژگی‌های مورد نظر انتخاب شده است. ضمنا مقوله‌های ردیف ۷ و۱۰و۱۲ و ۱۳ به دلیل روایی پایین آنها از فهرست مقوله‌ها حذف گردید.

اولویت بندی مقوله ها(فرعی): در این قسمت یافته‌های مندرج در جدول (۲) به صورت پرسشنامه پنج گزینه‌ای (طیف لیکرت) در اختیار جامعه خبره (بازبینی مجدد مصاحبه شوندگان) قرار گرفت. پاسخ‌های جمع‌آوری شده از طریق آزمون فریدمن مورد ارزیابی قرار گرفت. با توجه به مقدار آزمون مربع کای(۳۰/۰۹) و سطح معناداری (کمتر از ۰/۰۱) تفاوت بین مولفه‌های تهدید و آسیب پذیری (مقوله‌ها) از نظر مصاحبه شوندگان معنادار بود. لذا رتبه بندی بین مولفه‌ها به شرح زیر انجام شد:

جدول (۳) اولویت بندی مقوله‌ها

اولویت	عنوان	میانگین رتبه
اول	چالش‌های صحت، دقت و اعتماد پذیری یا قابلیت اطمینان، انطباق‌پذیری اطلاعات، ارسال فرامین و کنترل و نظارت بر اجرای آن‌ها و موضوع آگاهی وضعیتی	۶/۶۹
دوم	مناسب نبودن مخابرات تجاری و نیاز به توسعه یک زیرساخت غیر متمرکز برای پشتیبانی از اینترنت اشیاء در صحنه عملیات	۶/۶۶
سوم	مسائل مربوط به قابلیت اطمینان دستگاه‌ها، تمرکز بر عدم قطعیت در فناوری‌های اینترنت اشیاء، مدیریت اثبات و اعتماد، ساز وکارهای اعتماد و پیشرفت	۶/۵۹
چهارم	مشکل اعتماد و امنیت، بروز خرابی در تجهیزات، اقدامات عمدی خرابکارانه، وقفه‌های خدماتی یا انتشار اطلاعات نادرست	۶/۴۱
پنجم	چالش‌های امنیت داده‌ها و دسترسی به اطلاعات طبقه بندی شده	۶/۳۵
ششم	امکان نفوذ به شبکه‌ها، تهدید هکرهای وابسته به نیروهای سایبری و یا سایر هکرها	۶/۲۴
هفتم	مشکل قطعی و اختلال ارتباطات، پردازش داده‌های خام دستگاه‌ها توسط یک اَبر محلی، غیر متمرکز کردن منابع محاسباتی	۶/۱۸
هشتم	نیازمندی تامین یک معماری امنیتی همراه با یک سازه ابر پایه منبع باز	۶/۱۳
نهم	مشکلات کیفیت و امنیت ارتباطات و سامانه‌های ارسال و تبادل اطلاعات	۶/۰۳

نتایج جدول (۳) نشان می‌دهد که در میان مقوله‌های ذکر شده؛ چالش‌های صحت، دقت و اعتماد پذیری یا قابلیت اطمینان، انطباق‌پذیری اطلاعات، ارسال فرامین و کنترل و نظارت بر اجرای آن‌ها با میانگین رتبه (۶/۶۹) در اولویت اول و سایر چالش‌ها به ترتیب در اولویت‌های بعدی آسیب پذیری‌ها و تهدیدها قرار دارند.

نتیجه‌گیری و پیشنهادها

در بررسی چالش‌های بکارگیری اینترنت اشیاء در یک محیط نبرد تاکتیکی مانند شبکه پدافندهوایی دسترسی به دامنه‌های بین و متقابل، سنجش تنوع و ارتباط آن با تعامل انسان و ماشین حائز اهمیت است. تجهیزات مراکز فرماندهی و کنترل و سامانه‌های سلاح هوا پایه و زمین پایه تحت شبکه اینترنت اشیاء به‌صورت خودکار و هدایت از دور در راستای اجرای ماموریت پدافند هوایی بکارگرفته خواهند شد. توزیع منابع لجستیک و مدیریت زنجیره تأمین، به طور طبیعی به محیط‌های صحنه عملیات منتقل خواهند شد و تمامی عناصر شبکه تحت فرماندهی و کنترل هوشمند مبتنی بر اینترنت اشیاء نظامی قرار خواهند گرفت. با این حال، کاربرد IoT در فضاهای نبرد فیزیکی پیچیده و سایبری، به پیشرفت‌های پژوهشاتی بیشتری نیاز دارد تا بتوان چالش‌های خاص و منحصر به فردی که این محیط‌ها ارائه می‌دهند را رفع نمود. فناوری‌های اساسی مورد استفاده اینترنت اشیاء مانند شبکه‌سازی، مدیریت اطلاعات و معماری‌های رایانه‌ای، همگی از ویژگی‌های حوزه اینترنت اشیاء نظامی خواهند بود. لازم است در پرداختن به چالش‌های فنی مختلف، الزامات پدافندغیرعامل مد نظر قرار گیرد تا بتوان تاب‌آوری سامانه‌ها را در رفع ضعف‌ها و دفع تهدیدها ارتقاء بخشید. براساس آنچه بیان شد، بکارگیری MIoT تهدیدهای دیگری علاوه بر آنچه تاکنون بر سامانه‌های فرماندهی و کنترل اعمال می‌شد در پی خواهد داشت. برنامه‌ریزی اعمال تهدیدهای مبتنی بر اختلال در سامانه‌های فرماندهی و کنترل و اجزاء آن بویژه ارتباطات و بستر اینترنت اشیاء و پردازشگرها، نسبت به تهدیدهای سخت نظیر انواع مهمات، هزینه‌های بسیار کمتری را به سازنده و اعمال کننده آن تحمیل می‌نماید و همچنین به دلیل تضعیف زنجیره‌ی فرماندهی و کنترل، کاهش هماهنگی و انسجام قوای سامانه هدف (با مد نظر قرار دادن ضعف‌ها) که ناشی از اختلال در سامانه‌های فرماندهی و کنترل است، احتمال ورود به تهدیدهای دو طرفه مانند جنگ را کاهش می‌دهد، از این رو قدرت بازدارندگی را به نفع عامل تهدید افزایش می‌دهد.

پیشنهادها

براساس نتیجه‌گیری صورت گرفته و همچنین روند و سرعت پیشرفت فناوری در عرصه‌های مختلف و کاربرد آن در حوزه‌های آفندی و پدافندی در آینده، پیشنهادهای ذیل ارائه می‌گردد:

- برنامه ریزی لازم جهت کاربرد اینترنت اشیاء نظامی در شبکه پدافندهوایی در راستای حرکت به‌سوی سامانه یکپارچه خودکار و مکانیزه پدافندهوایی، از طریق فراهم سازی الزامات و شرایط استفاده از بسترهای ارتباطی موجود و همچنین تقویت آن‌ها.

- توسعه یک زیرساخت غیر متمرکز برای پشتیبانی از اینترنت اشیاء در صحنه عملیات شبکه فرماندهی و کنترل بر مبنای رایانش ابری و ایجاد معماری مربوطه و تامین سایر نیازمندی‌های امنیتی مرتبط با این رویکرد که ملزومات امنیتی موجود فاقد آن‌هاست و پیاده سازی یک معماری امنیتی همراه با یک سازه ابر پایه منبع باز.
- لزوم توجه و تاکید بر دارا بودن ویژگی و قابلیت اتصال به شبکه اینترنت اشیاء نظامی در سامانه‌های در دست طراحی و یا در حال ساخت و همچنین خریدهای تجهیزاتی در دست اقدام.

قدردانی

بدینوسیله از افرادی که نویسنده را در طی پژوهش حمایت کرده‌اند در انجام این پژوهش یاری کردند، صمیمانه تشکر می‌کنم.

منابع

- بختیاری، ایرج. (۱۳۹۹). تحلیل محیطی آینده فرماندهی و کنترل در حوزه دفاع هوافضایی، *فصلنامه فرماندهی و کنترل*. ۴ (۲): ۲۰-۱.
- تدین، محمد حسام. (۱۳۹۴). *شناسایی مراکز پژوهشاتی، چالش‌ها و راه‌حل‌ها در امنیت اینترنت اشیاء*، پژوهشکده امنیت ارتباطات و فناوری اطلاعات.
- حسینی، منصورعلی. (۱۳۹۵). *اینترنت اشیاء؛ چالش ها و راهکارها*، همایش بین المللی افق های نوین در علوم پایه و فنی و مهندسی، نمایه شده در سیویلیکا
- حیدریان، محسن و خادم دقیق، امیر هوشنگ. (۱۳۹۸). الگوی فرماندهی و کنترل هوایی در جنگ های آینده، *نشریه آینده پژوهی دفاعی*. ۴(۱۴): ۸۶-۶۱.
- رحیمی، محسن(۱۳۹۸) کاربرد CNS/ATM در شبکه پدافند هوایی، *فصلنامه فرماندهی و کنترل*، دوره شماره ۷
- رمضانی، رسول، موحدی، محمدرضا. (۱۴۰۰). رتبه بندی تهدیدهای اینترنت اشیاء در محیط نظامی، *فصلنامه امنیت ملی*.۱ (۳۹): ۲۲۸-۱۹۹.
- علی نژاد و همکاران. (۱۳۹۹). تحلیلی بر تهدیدات هوافضایی، علیه مراکز حیاتی و حساس در افق چشم انداز ۱۴۰۴ ، *فصلنامه مطالعات دفاعی استراتژیک*. ۱۸ (۸۱): ۱۵۰-۱۲۵.
- غلام‌نژاد و همکاران(۱۳۹۸)، کاربردهای نظامی اینترنت اشیاء با تأکید بر مأموریت‌های نهاجا، *فصلنامه علوم و فنون نظامی*، شماره ۴۹.
- فراهانی‌فر و همکاران. (۱۴۰۰). شناسایی و رتبه‌بندی عوامل مؤثر بر سرریز فناوری‌های دفاعی به کسب و کارهای تجاری، *فصلنامه علمی راهبرد دفاعی*. ۱۹ (۷۴): ۲۰۸-۱۷۹.

- فرجپور، عباس. (۱۳۹۸). *ارائه الگوی راهبردی بومی برای سازمان‌های شبکه‌ای در نیروهای مسلح با نگاه به جنگ‌های آینده*، دانشگاه عالی دفاع ملی.
- فیاض‌مجتهدی، محمدرضا. (۱۳۸۹). *طراحی الگوی مدیریت دستیابی به سامانه‌های عمده دفاعی در سازمان‌های صنعتی ودجا مبتنی بر عوامل اساسی موفقیت*، دانشگاه عالی دفاع ملی.
- محمودزاده، ابراهیم و اسماعیلی، کیوان. (۱۳۹۷). الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح ، *فصلنامه امنیت ملی*. ۸ (۳۰): ۲۳۷-۲۰۳.
- منطقی، مصطفی. (۱۳۸۱)، *سیستمهای تسلیحاتی مطرح در جنگهای مدرن*، موسسه آموزشی و پژوهشاتی صنایع دفاعی.
- میررفیع، سیدعلی. (۱۳۹۴). *تدوین راهبردهای پدافند غیرعامل زیرساخت‌های ارتباطی شبکه ملی اطلاعات کشور در برابر تهدیدات سایبری*، دانشگاه عالی دفاع ملی.
- میرمحمدیان و همکاران. (۱۳۹۶). *راهکارهای پیشگیری از چالش‌های اینترنت اشیاء*، پژوهش‌های نوین علوم و فناوری.
- نجفی، محمدرضا. (۱۳۹۲). *ایران و جنگ نامتقارن آینده*. تهران: هوشمند تدبیر.
- نوروزی، محمدتقی. (۱۳۸۵). *فرهنگ دفاعی - امنیتی*، تهران، انتشارات سنا
- یزدان پناه، حمیدرضا. (۱۳۹۵). *اینترنت اشیا (IoT): کاربردها، فناوریها و چالشهای مورد بحث*، کنفرانس بین المللی فناوری اطلاعات و دانش، نمایه شده در پایگاه مرکز اطلاعات علمی جهاد دانشگاهی.
- DZheng, D. E., & Carter, W. A. (2015). *Leveraging the internet of things for a more efficient and effective military*. Rowman & Littlefield.
- Evans, R. C. (2011). National Air Defense: Challenges, Solution Profiles, and Technology Needs. *The MITRE Corporation [Online]. Available: http://ww. mitre. org/work/tech-papers/tech-papers-04/04-1108/04-1108. pdf, Accessed Jun*, *30*.
- Koo, J., Oh, S. R., Lee, S. H., & Kim, Y. G. (2020). Security architecture for cloud-based command and control system in IoT environment. *Applied Sciences*, *10*(3), 1035.
- Sorenson, H. (2014), *Air Defense Opportunities and Challenges Keynote Address*, Bedford, USA, http://ftp.rta.nato.int
- Suri, N., Benincasa, G., Lenzi, R., Tortonesi, M., Stefanelli, C., & Sadler, L. (2015). Exploring value-of-information-based approaches to support effective communications in tactical networks. *IEEE Communications Magazine*, *53*(10), 39-45.
- Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information systems frontiers, 17, 261-274.

- Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things—A survey of topics and trends. Information systems frontiers, 17, 261-274.