AJA Command and Staff University

Warfare Study Quarterly

https://www.qjws.ir/ Online ISSN: 2717-1760 Print ISSN: 2717-1760

Applying Internet of Things technology in electronic warfare

Arsalan.aftabi [1]✉ |Mohamad. ghasemi tadavani [2]|Hasan. abedinzadeh[3]|Ali .panahi[4]

1.Master's student in Defense Management, AJA Command and Staff University , Tehran, Iran. E-mail: aftabiarsalan@yahoo.com

2. .Ph.D., student in Defense Management, AJA Command and Staff University Of the Islamic Republic of Iran, Tehran, Iran. E-mail: m.ghasemi@casa.Ac.ir

3.Ph.D., student in Defense Management, University of Strategic Sciences, Tehran, Iran. E-mail: abedinzadeh87@gmail.com

4.Ph.D., student in Defense Management, AJA Command and Staff University Of the Islamic Republic of Iran, Tehran, Iran. E-mail: Alipanahi14@yahoo.com

Article Info

Article type:

Research Article

Article history:

Received

08 May 2025

Received in revised form

18 May 2025

Accepted

10 June 2025

Published online

21 June 2025

Keywords:

Internet of Things,

Electronic Warfare,

Electromagnetic

Spectrum, Cyber Warfare

ABSTRACT

This study examines the application of Internet of Things (IoT) technology in enhancing the electronic warfare (EW) capabilities. The aim of the study is to explain how the Internet of Things (IoT) can be integrated into the areas of electronic support, attack, and protection to improve battlefield dominance. Using a descriptive mixed-method approach, data ۱۱was collected through library research, interviews with senior officers with ۸۵experts, and a questionnaire from relevant expertise. The findings show that the Internet of Things (IoT) significantly improves electronic warfare operations: in support, IoT sensors enable real-time data collection and analysis; in attack, it facilitates signal deception and disruption of enemy communications; and in protection, it ensures threat detection and automated responses. The results support for the use of the ٪۸۲,۴of the questionnaire indicate ٪۷۶,۴Internet of Things in the areas of support and attack, and in protection. This study emphasizes the transformative potential of the Internet of Things in modern warfare and highlights its strategic advantages in dominating the electromagnetic spectrum.

Cite this article: Arsalan.Aftabi,. Ghasemi Tadavani. Mohamad, Abedinzadeh Hasan, & Panahi,Ali. (2025). Applying Internet of Things technology in electronic warfare, Warfare Study Quarterly. 7 (21). 4-21.

. *Journal Title*, 0. DOI: http//doi.org/ 10.22034/qjws.2025.2060031.1280

 Publisher: Command and Staff University

فصلنامه علمی مطالعات جنگ
شاپای چاپی: ۱۷۶۰-۲۷۱۷ شاپای الکترونیکی: ۱۷۶۰-۲۷۱۷ https://www.qjws.ir/ دانشگاه فرماندهی و ستاد آجا

به‌کارگیری فناوری اینترنت اشیاء در جنگ الکترونیک

ارسلان آفتابی [۱] ✉ | محمد قاسمی تادوانی | حسن عابدین‌زاده [۳] | علی پناهی [۴]

۱. دانشجوی کارشناسی ارشد مدیریت دفاعی ،دانشگاه فرماندهی وستاد ارتش ج ا ایران ،تهران ، ایران رایانامه:aftabiarsalan@yahoo.com

۲. دانشجوی دکترا مدیریت دفاعی ،دانشگاه فرماندهی وستاد ارتش ج ا ایران ،تهران ، ایران رایانامه: m.ghasemi@casa.Ac.ir

۳. دانشجوی دکترا مدیریت دفاعی ،دانشگاه علوم استراتژیک ،تهران ، ایران رایانامه: abedinzadeh87@gmail.com

۴. دانشجوی دکترا مدیریت دفاعی ،دانشگاه فرماندهی وستاد ارتش ج ا ایران ،تهران ، ایران رایانامه: Alipanahi14@yahoo.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۴/۰۲/۱۸

تاریخ بازنگری:
۱۴۰۴/۰۲/۲۸

تاریخ پذیرش:
۱۴۰۴/۰۳/۲۰

تاریخ انتشار:
۱۴۰۴/۰۳/۳۱

کلیدواژه‌ها:
اینترنت اشیاء، جنگ الکترونیک، طیف الکترومغناطیسی، جنگ سایبری

چکیده

این پژوهش به بررسی کاربرد فناوری اینترنت اشیاء در ارتقای توانمندی‌های جنگ الکترونیک می‌پردازد. هدف پژوهش، تبیین چگونگی ادغام اینترنت اشیاء در حوزه‌های پشتیبانی، حمله و حفاظت الکترونیکی برای بهبود تسلط بر میدان نبرد است. با استفاده از رویکرد توصیفی با روش آمیخته، داده‌ها از طریق پژوهش کتابخانه‌ای، مصاحبه با ۱۱ متخصص و پرسشنامه از ۸۵ افسر ارشد دارای تخصص مرتبط جمع‌آوری شد. یافته‌ها نشان می‌دهد که اینترنت اشیاء به‌طور قابل‌توجهی عملیات جنگ الکترونیک را بهبود می‌بخشد: در پشتیبانی، حسگرهای اینترنت اشیاء امکان جمع‌آوری و تحلیل داده‌های بلادرنگ را فراهم می‌کنند؛ در حمله، این فناوری فریب سیگنال و اختلال در ارتباطات دشمن را تسهیل می‌کند و در حفاظت، واکنش‌های خودکار در برابر حمله را تضمین می‌نماید. نتایج پرسشنامه نشان‌دهنده حمایت ۸۲.۴ درصدی از کاربرد اینترنت اشیاء در حوزه‌های پشتیبانی و حمله و ۷۶.۴ درصد در حفاظت است. این مطالعه بر پتانسیل تحول‌آفرین اینترنت اشیاء در جنگ‌های زمینی تأکید دارد.

استناد: آفتابی، ارسلان؛ قاسمی تادوانی، محمد؛ عابدین زاده، حسن؛ و پناهی، علی (۱۴۰۴). به‌کارگیری فناوری اینترنت اشیاء جنگ الکترونیک. فصلنامه *مطالعات جنگ*. (۲۱) ۷. ۳۱-۴.

. *Journal Title*, 0. DOI: http//doi.org/ 10.22034/qjws.2025.2060031.1280

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

دسترسی راحت کاربران به اینترنت در دهه‌های اخیر، با سرعت چشمگیری درحال‌رشد است، در حدی که امروزه شاید بتوان اینترنت را به‌عنوان یک حس جدید اضافه بر حواس پنج‌گانه انسان فرض کرد. در بیان فراگیری اینترنت، می‌توان به فعالیت‌ها و اقدامات شرکت فناوری‌های اکتشاف فضایی یا اسپیس‌ایکس اشاره کرد که در دهه‌های اخیر، فعالیت‌های گسترده‌ای به‌منظور دسترسی راحت به اینترنت در سراسر جهان، انجام داده است و تاکنون صدها ماهواره اینترنتی را تحت پروژه‌ای موسوم به استارلینک در مدار قرار داده است و حتی با ظهور فناوری کوانتوم، احتمال برقراری اینترنت کوانتومی را نیز می‌توان در آینده متصور دانست. فراگیرشدن اینترنت، ظهور فناوری‌های جدید و نوظهور را نیز به دنبال داشته که از جمله آن‌ها، اینترنت اشیاء است (لک، ۱۳۹۹).

اینترنت اشیاء اولین‌بار توسط کوین اشتون در سال ۱۹۹۹ بیان شده است که طی دهه‌های اخیر انقلاب عظیمی در عرصه فناوری اطلاعات و ارتباطات به راه انداخته است. در حقیقت، اینترنت اشیاء، شبکه‌ی جهانی مبتنی بر اینترنت را تعریف می‌کند که تمامی اشیاء قابلیت اتصال به یکدیگر، تبادل اطلاعات و انجام فعالیت‌های هوشمند را خواهند داشت. تجزیه و تحلیل‌گر دیلویت نیز، این فناوری را در بین فناوری‌های دیگری مانند هوش مصنوعی، تحلیل کلان‌داده، نانوفناوری، بلاک‌چین، رباتیک پیشرفته و محاسبات کوانتوم، واقعیت افزوده، پرینتر سه‌بعدی به‌عنوان فناوری که می‌تواند بیشترین تأثیر را بر سازمان‌ها داشته باشد، معرفی کرده است (بهاتنگار [1]، ۲۰۲۰).

در میان کاربردهای متعدد اینترنت اشیاء در صنعت، ساختمان، سلامت، کشاورزی، آموزش و حمل‌ونقل، کاربردهای نظامی اینترنت اشیاء نیز بسیار حائز اهمیت است. کاربردهای نظامی این فناوری می‌تواند تأثیرات مستقیم مثبت یا منفی را در صحنه‌های نبرد به دنبال داشته باشد. ورود بحث اینترنت اشیاء و قابلیت متصل‌شدن سامانه‌های مختلف سلاح به شبکه، فرصت تسهیل کنترل سلاح‌ها توسط فرماندهان و نیز ارتقاء سرعت عمل در واکنش‌ها را پدید می‌آورد. امروزه توسعه کاربردهای نظامی فناوری اینترنت اشیاء بر روی کاربردهای در سامانه‌های فرماندهی و کنترل و کنترل آتش متمرکز شده است و همچنین

---

[1] Bhatnagar

در برخی کاربردها مانند مراقبت پزشکی، لجستیک، آموزش و شبیه‌سازی تطبیق یافته است (بهشتی، ۱۳۹۷).

از طرفی اینترنت اشیاء نیز موجب گسترش روزافزون استفاده از حسگرهای مختلف جمع‌آوری داده مانند دوربین، میکروفون، حسگر صوتی، لیزر، آشکارساز فرکانس رادیویی، اشعه مادون‌قرمز و ... در لایه دریافت، بلوتوث، وای‌فای و اینترنت نسل ۵ در لایه شبکه این فناوری و رایانه، تلفن همراه، خودروی نظامی، ناو، جنگنده و ربات‌های هوشمند در لایه کاربرد، شده است؛ بنابراین با توجه به نقش پررنگ عناصر مختلف لایه‌های فناوری اینترنت اشیاء در جنگ سایبری و الکترونیک، در این تحقیق به تبیین به‌کارگیری اینترنت اشیاء در جنگ الکترونیک نیروی زمینی ارتش جمهوری اسلامی ایران پرداخته شد.

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

۱-چارچوب مفهومی جنگ الکترونیک

جنگ الکترونیک[1] به مجموعه‌ای از اقدامات نظامی اطلاق می‌شود که از انرژی الکترومغناطیسی برای کنترل طیف الکترومغناطیسی یا حمله به دشمن استفاده می‌کنند. این حوزه به سه بخش اصلی تقسیم می‌شود: پشتیبانی الکترونیک، حمله الکترونیکی و حفاظت الکترونیکی. پشتیبانی الکترونیکی شامل شناسایی، تشخیص و مکان‌یابی منابع انتشارات الکترومغناطیسی برای پشتیبانی از عملیات نظامی است. حمله الکترونیکی از انرژی الکترومغناطیسی یا سایبری برای مختل کردن یا تخریب قابلیت‌های دشمن استفاده می‌کند، در حالی که حفاظت الکترونیکی اقداماتی را برای محافظت از سامانه‌های خودی در برابر اثرات جنگ الکترونیک دشمن در بر می‌گیرد (Joint Publication 3-13.1, 2012). این سه حوزه در کنار یکدیگر، چارچوبی جامع برای تسلط بر میدان نبرد الکترومغناطیسی فراهم می‌کنند.

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

---

[1] EW = electeronic warfare

نیروها و جنگ‌افزارها از مهمترین کاربردهای اینترنت اشیاء در حوزه نظامی است. 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 با ارزش است. 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 (موحدی و همکاران، ۱۴۰۲).

۲- اینترنت اشیاء:

اینترنت اشیاء به شبکه‌ای از اشیاء فیزیکی اطلاق می‌شود که با حسگرها، نرم‌افزارها و فناوری‌های ارتباطی مجهز شده‌اند تا داده‌ها را جمع‌آوری و تبادل کنند. این فناوری شامل دستگاه‌هایی مانند حسگرهای محیطی، تجهیزات پوشیدنی، و سامانه‌های خودکار است که از طریق پروتکل‌های ارتباطی مانند آر.اف.آی.دی، وای‌فای، بلوتوث و شبکه‌های G ۵ به یکدیگر متصل می‌شوند. معماری اینترنت اشیاء معمولاً از پنج لایه تشکیل شده است:
لایه حسگر: شامل دستگاه‌هایی مانند حسگرهای آر.اف، دوربین‌ها، حسگرهای مادون قرمز و رطوبت‌سنج‌ها که داده‌های محیطی را جمع‌آوری می‌کنند.
لایه دسترسی: امکان اتصال دستگاه‌ها را از طریق فناوری‌های بی‌سیم یا سیمی مانند وای‌فای، بلوتوث و جی.پی.اس فراهم می‌کند.
لایه شبکه: انتقال امن و قابل اعتماد داده‌ها را از طریق شبکه‌های نظامی یا تجاری مانند G ۵ تضمین می‌کند.
لایه سرویس: داده‌ها را با استفاده از فناوری‌های هوش مصنوعی و یادگیری ماشین پردازش می‌کند تا اطلاعات قابل‌اقدام تولید کند.
لایه کاربرد: داده‌های پردازش‌شده را در برنامه‌های نظامی مانند سامانه‌های فرماندهی و کنترل [1] (فرماندهی، کنترل، ارتباطات، رایانه‌ها، اطلاعات، نظارت، هدف‌گیری، اکتساب و

---

[1] C4ISTAR= Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition And Reconnaissance

شناسایی)، سامانه‌های کنترل آتش و عملیات جنگ الکترونیک ادغام می‌کند (همان منبع).

این معماری چندلایه، اینترنت اشیاء را به ابزاری قدرتمند برای کاربردهای نظامی تبدیل می‌کند، به‌ویژه در حوزه‌هایی که نیاز به جمع‌آوری داده‌های بلادرنگ، تحلیل سریع و پاسخ‌های خودکار دارند.

۳- کاربردهای اینترنت اشیاء در جنگ الکترونیک

۳-۱-پشتیبانی الکترونیکی

پشتیبانی الکترونیکی یکی از مهم‌ترین حوزه‌های جنگ الکترونیک است که بر جمع‌آوری اطلاعات از محیط الکترومغناطیسی برای پشتیبانی از تصمیم‌گیری عملیاتی تمرکز دارد. اینترنت اشیاء با استقرار شبکه‌های حسگر پیشرفته، قابلیت‌های پشتیبانی الکترونیکی را به‌طور قابل‌توجهی تقویت می‌کند. حسگرهای اینترنت اشیاء می‌توانند سیگنال‌های راداری، مخابراتی و سایر انتشارات الکترومغناطیسی را شناسایی کنند و داده‌ها را برای تحلیل به مراکز فرماندهی ارسال کنند. این داده‌ها با استفاده از الگوریتم‌های هوش مصنوعی پردازش می‌شوند تا الگوهای رفتاری دشمن، مکان سامانه‌های کلیدی و تهدیدهای بالقوه شناسایی شوند (لی و همکاران[1]، ۲۰۲۰).

یکی از مزایای کلیدی اینترنت اشیاء در پشتیبانی الکترونیکی، توانایی آن در ارائه آگاهی وضعیتی بلادرنگ است. برای مثال، حسگرهای مستقر در میدان نبرد می‌توانند تغییرات در الگوهای ارتباطی دشمن یا فعال شدن سامانه‌های راداری را تشخیص دهند و این اطلاعات را به‌سرعت به فرماندهان منتقل کنند. این قابلیت به‌ویژه در محیط‌های پیچیده‌ای که دشمن از فناوری‌های پیشرفته مانند رادارهای پنهان‌کار استفاده می‌کند، حیاتی است. علاوه بر این، اینترنت اشیاء امکان مدیریت بهینه منابع ارتباطی را فراهم می‌کند، به‌طوری که کانال‌های ارتباطی در شرایط شلوغی یا اختلال، کارایی خود را حفظ می‌کنند (بابایی، ۱۳۹۸).

---

[1] Lin Zhu, Suryadipta Majumdar, Chinwe Ekenna

۳-۲-حمله الکترونیکی

حمله الکترونیکی شامل استفاده از انرژی الکترومغناطیسی یا سایبری برای مختل کردن یا تخریب سامانه‌های دشمن است. اینترنت اشیاء در این حوزه از طریق ایجاد فریب، اختلال در ارتباطات و هدف‌گیری دقیق، نقش مهمی ایفا می‌کند. برای مثال، دستگاه‌های اینترنت اشیاء می‌توانند سیگنال‌های جعلی تولید کنند که سامانه‌های راداری یا مخابراتی دشمن را گمراه کنند. این تکنیک، که به‌عنوان فریب فعال شناخته می‌شود، می‌تواند دشمن را وادار کند تا منابع خود را به اهداف کاذب اختصاص دهد یا عملیات خود را متوقف کند (رابینسون و همکاران[1]، ۲۰۲۳).

یکی دیگر از کاربردهای اینترنت اشیاء در حمله الکترونیکی، ایجاد اختلال در شبکه‌های ارتباطی دشمن است. با شبیه‌سازی ترافیک شبکه یا ارسال سیگنال‌های پارازیت، دستگاه‌های اینترنت اشیاء می‌توانند شبکه‌های دشمن را بیش‌ازحد درگیر کنند، که منجر به کاهش کارایی عملیاتی او می‌شود. این قابلیت در جنگ‌های نامتقارن، که دشمن ممکن است به ارتباطات بی‌سیم وابسته باشد، بسیار مؤثر است. علاوه بر این، جمرهای مبتنی بر اینترنت اشیاء می‌توانند فرکانس‌های خاص را با دقت بالا هدف قرار دهند، که اثربخشی حملات الکترونیکی را افزایش می‌دهد (همان منبع).

۳-۳- حفاظت الکترونیکی

حفاظت الکترونیکی بر محافظت از سامانه‌های خودی در برابر اثرات جنگ الکترونیک دشمن تمرکز دارد. اینترنت اشیاء در این حوزه با ارائه قابلیت‌های نظارت بلادرنگ و واکنش‌های خودکار، نقش مهمی ایفا می‌کند. حسگرهای اینترنت اشیاء می‌توانند تجهیزات نظامی، مانند رادارها و سامانه‌های مخابراتی، را به‌طور مداوم نظارت کنند تا ناهنجاری‌هایی مانند تلاش‌های هک یا پارازیت را تشخیص دهند. در صورت شناسایی تهدید، سامانه‌های مبتنی بر اینترنت اشیاء می‌توانند به‌صورت خودکار اقدامات متقابلی مانند ایزوله کردن دستگاه‌های آلوده یا تغییر فرکانس‌های ارتباطی را اجرا کنند (شمیت و ونزل[2]، ۲۰۱۷).

---

[1] Robinson, C. P., et al.
[2] Schmidt, A., & Wenzel, S

یکی از مهم‌ترین ویژگی‌های اینترنت اشیاء در حفاظت الکترونیکی، استفاده از پروتکل‌های رمزنگاری پیشرفته برای محافظت از داده‌های نظامی است. این پروتکل‌ها اطمینان می‌دهند که اطلاعات حساس، حتی در صورت رهگیری، برای دشمن غیرقابل‌استفاده باقی می‌مانند. علاوه بر این، اینترنت اشیاء می‌تواند با ادغام با سامانه‌های دفاع سایبری، پاسخ‌های هماهنگ به تهدیدهای ترکیبی (سایبری و الکترومغناطیسی) را تسهیل کند. این قابلیت در برابر دشمنانی که از راهبردهای جنگ ترکیبی استفاده می‌کنند، حیاتی است (اسکین‌کالپور و پیترو[1]، ۲۰۱۹).

پیشینه پژوهش

در ایران، تحقیقات متعددی به بررسی کاربردهای نظامی اینترنت اشیاء پرداخته‌اند. پورمکاری و همکاران (۱۳۹۸) در مطالعه‌ای جامع، نقش اینترنت اشیاء را در بهبود مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران بررسی کردند. آن‌ها دریافتند که شبکه‌های حسگر اینترنت اشیاء می‌توانند با ارائه داده‌های بلادرنگ، فرآیندهای فرماندهی و کنترل را بهبود ببخشند. این مطالعه بر اهمیت ادغام اینترنت اشیاء با سامانه‌های فرماندهی و کنترل تأکید کرد و پیشنهاد کرد که این فناوری می‌تواند هماهنگی بین یگان‌های مختلف را تقویت کند.

طبی (۱۴۰۰) در پایان‌نامه کارشناسی ارشد خود، کاربرد اینترنت اشیاء را در ارتقای امنیت یگان‌های ارتش بررسی کرد. او پیشنهاد کرد که حسگرهای اینترنت اشیاء می‌توانند برای نظارت بر پایگاه‌ها و تأسیسات نظامی استفاده شوند تا تهدیدهای احتمالی مانند نفوذ یا حمله‌های سایبری به‌سرعت شناسایی شوند. این مطالعه بر اهمیت نظارت بلادرنگ و پاسخ‌های خودکار تأکید داشت، که با یافته‌های پژوهش حاضر در حوزه حفاظت الکترونیکی هم‌راستا است.

شفیعی (۱۴۰۰) در پژوهشی دیگر، راهبردهای جنگ الکترونیک در درگیری‌های معاصر را تحلیل کرد. او دریافت که فناوری‌های پیشرفته، مانند اینترنت اشیاء، برای مقابله با تهدیدهای نوظهور مانند رادارهای پنهان‌کار و سامانه‌های ارتباطی مبتنی بر ۵ Gضروری هستند. این مطالعه بر نیاز به توسعه قابلیت‌های بومی در حوزه جنگ الکترونیک تأکید

---

[1] Sciancalepore, S., & Pietro, R. D

کرد و اینترنت اشیاء را به‌عنوان یکی از فناوری‌های کلیدی برای دستیابی به این هدف معرفی نمود.

علاوه بر این، اعتضادی‌فر و گرمابدری (۱۴۰۳) در مطالعه‌ای اخیر، به بررسی طبقه‌بندی خودکار مدولاسیون درون‌پالسی ترکیبی راداری پرداختند. آن‌ها نشان دادند که فناوری‌های مبتنی بر هوش مصنوعی، که می‌توانند با اینترنت اشیاء ادغام شوند، دقت تشخیص سیگنال‌های راداری را بهبود می‌بخشند. این یافته‌ها کاربرد اینترنت اشیاء در پشتیبانی الکترونیکی را تأیید می‌کنند، به‌ویژه در زمینه تحلیل داده‌های پیچیده الکترومغناطیسی.

بابایی (۱۳۹۸) نیز در پژوهشی دیگر، مدلی برای تحلیل رفتار دشمن با استفاده از مدل‌های مخفی مارکوف مبتنی بر مشاهدات جنگ الکترونیک ارائه داد. او پیشنهاد کرد که داده‌های جمع‌آوری‌شده توسط حسگرهای پیشرفته، مانند آن‌هایی که در شبکه‌های اینترنت اشیاء استفاده می‌شوند، می‌توانند برای پیش‌بینی اقدامات دشمن مورد استفاده قرار گیرند. این مطالعه اهمیت ادغام اینترنت اشیاء با هوش مصنوعی را در پشتیبانی الکترونیکی برجسته کرد.

به‌طور کلی، پژوهش‌های داخلی نشان‌دهنده آگاهی روبه‌رشد از پتانسیل اینترنت اشیاء در کاربردهای نظامی هستند. با این حال، تمرکز خاص بر ادغام این فناوری در جنگ الکترونیک نیروی زمینی ارتش جمهوری اسلامی ایران محدود بوده است. این شکاف پژوهشی، ضرورت مطالعه حاضر را برجسته می‌کند.

در سطح بین‌المللی، کاربردهای نظامی اینترنت اشیاء به‌طور گسترده‌ای مورد مطالعه قرار گرفته‌اند. رابینسون و همکاران[1] (۲۰۲۳) در مطالعه‌ای تجربی، اثربخشی اینترنت اشیاء را در ایجاد اختلال بی‌سیم بررسی کردند. آن‌ها سیستمی به نام ایسورد[2] را توسعه دادند که از دستگاه‌های اینترنت اشیاء برای ایجاد پارازیت در شبکه‌های بی‌سیم دشمن استفاده می‌کرد. نتایج این مطالعه نشان داد که اینترنت اشیاء می‌تواند به‌طور مؤثری ارتباطات دشمن را مختل کند، که کاربرد آن را در حمله الکترونیکی تأیید می‌کند.

---

[1] Robinson, C. P., et al.

[2] eSWORD

وو و همکاران [1] (۲۰۲۳) در پژوهشی دیگر، به بررسی فریب راداری مبتنی بر اینترنت اشیاء پرداختند. آن‌ها سیستمی را پیشنهاد کردند که از دستگاه‌های اینترنت اشیاء برای تولید سیگنال‌های جعلی استفاده می‌کرد تا رادارهای دشمن را گمراه کند. این مطالعه بر توانایی اینترنت اشیاء در ایجاد اهداف کاذب تأکید داشت، که یک تاکتیک کلیدی در حمله الکترونیکی است. یافته‌های این پژوهش با نتایج مطالعه حاضر در مورد نقش اینترنت اشیاء در فریب فعال هم‌راستا است.

لیو[2] (۲۰۱۹) در مقاله‌ای در ترنسیشن مگنتیک[3]، کاربرد حسگرهای اسپین‌ترونیک را در اینترنت اشیاء بررسی کردند. آن‌ها نشان دادند که این حسگرها، که می‌توانند در شبکه‌های اینترنت اشیاء ادغام شوند، دقت تشخیص سیگنال‌های الکترومغناطیسی را بهبود می‌بخشند. این یافته‌ها کاربرد اینترنت اشیاء در پشتیبانی الکترونیکی را تأیید می‌کنند، به‌ویژه در زمینه شناسایی سیگنال‌های پیچیده.

اسکین‌کالپور و پیترو[4] (۲۰۱۹) در مطالعه‌ای دیگر، سیستمی به نام بیت‌ترنسفر[5] را برای کاهش اثرات پارازیت واکنشی در سناریوهای جنگ الکترونیک پیشنهاد کردند. آن‌ها نشان دادند که دستگاه‌های اینترنت اشیاء می‌توانند با نظارت مداوم بر محیط الکترومغناطیسی، پاسخ‌های خودکار به تهدیدهای پارازیت ارائه دهند. این مطالعه کاربرد اینترنت اشیاء در حفاظت الکترونیکی را تأیید می‌کند و بر اهمیت واکنش‌های خودکار تأکید دارد.

علاوه بر این، گوه[6] (۲۰۲۰) در کتاب اینترنت اشیاء بی‌سیم[7]، به بررسی انتشار امواج الکترومغناطیسی در شبکه‌های اینترنت اشیاء پرداخت. او استدلال کرد که فناوری‌های ارتباطی پیشرفته، مانند G۵، قابلیت اطمینان شبکه‌های اینترنت اشیاء را در محیط‌های نظامی بهبود می‌بخشند. این یافته‌ها اهمیت لایه شبکه در معماری اینترنت اشیاء را برجسته می‌کنند، که برای کاربردهای جنگ الکترونیک حیاتی است.

---

[1] Wu, Z., et al
[2] Liu, X.
[3] IEEE Transactions on Magnetics
[4] Sciancalepore, S., & Pietro, R. D
[5] Bittransfer
[6] Goh, M. W. C.
[7] Wireless Internet of Things

مک‌گوان [1] (۲۰۱۷) در مطالعه‌ای در کالج فرماندهی و ستاد ارتش ایالات متحده، به بررسی عملیات جنگ الکترونیک پرداخت. او استدلال کرد که فناوری‌های پیشرفته، مانند اینترنت اشیاء، برای مقابله با تهدیدات نوظهور در طیف الکترومغناطیسی ضروری هستند. این مطالعه بر اهمیت ادغام فناوری‌های جدید در دکترین‌های جنگ الکترونیک تأکید کرد، که با اهداف پژوهش حاضر هم‌راستا است.

وان و همکاران [2] (۲۰۱۸) در مقاله‌ای در مجله سیمتری [3]، روشی جدید برای شناسایی سیگنال‌های راداری مبتنی بر اینترنت اشیاء پیشنهاد کردند. آن‌ها نشان دادند که حسگرهای اینترنت اشیاء، هنگامی که با الگوریتم‌های طبقه‌بندی بهینه ترکیب شوند، می‌توانند دقت تشخیص سیگنال را بهبود ببخشند. این یافته‌ها کاربرد اینترنت اشیاء در پشتیبانی الکترونیکی را تأیید می‌کنند و بر اهمیت تحلیل داده‌های پیشرفته تأکید دارند. در مجموع، پژوهش‌های خارجی نشان‌دهنده پتانسیل گسترده اینترنت اشیاء در کاربردهای نظامی، به‌ویژه در جنگ الکترونیک، هستند. این مطالعات چارچوبی نظری و تجربی قوی برای پژوهش حاضر فراهم می‌کنند و کاربرد اینترنت اشیاء در پشتیبانی، حمله و حفاظت الکترونیکی را تأیید می‌کنند.

ادبیات نظری نشان می‌دهد که اینترنت اشیاء پتانسیل تحول‌آفرینی در جنگ الکترونیک دارد. در پشتیبانی الکترونیکی، این فناوری آگاهی وضعیتی و تحلیل داده‌ها را بهبود می‌بخشد؛ در حمله الکترونیکی، فریب و اختلال را تسهیل می‌کند؛ و در حفاظت الکترونیکی، واکنش‌های خودکار و امنیت سایبری را تقویت می‌کند. پژوهش‌های داخلی و خارجی، کاربردهای متنوع اینترنت اشیاء را در زمینه‌های نظامی تأیید می‌کنند، اما تمرکز خاص بر نیروی زمینی ارتش جمهوری اسلامی ایران محدود بوده است. این پژوهش با ارائه چارچوبی جامع برای ادغام اینترنت اشیاء در جنگ الکترونیک، به توسعه دانش در این حوزه کمک می‌کند.

روش تحقیق

---

[1] McGowan, J
[2] Wan, J., et al
[3] Symmetry

نوع و روش تحقیق کاربردی و توصیفی با رویکرد آمیخته است. بخش کیفی شامل پژوهش کتابخانه‌ای و مصاحبه‌های نیمه‌ساختاریافته است و بخش کمی از پرسشنامه برای اعتبارسنجی یافته‌ها بهره می‌برد. جامعه آماری شامل ۸۵ نفر از کارکنان پایور آجا با مدارک کارشناسی ارشد یا دکتری در رشته‌های الکترونیک یا علوم کامپیوتر، دارای درجه افسر ارشد و حداقل ۱۵ سال سابقه خدمت در یگان‌های جنگ الکترونیک، فناوری اطلاعات و ارتباطات یا دفاع سایبری است. روش نمونه‌گیری تصادفی طبقه‌بندی ساده برای انتخاب پاسخ‌دهندگان پرسشنامه استفاده شد. همچنین، ۱۱ متخصص به‌صورت هدفمند برای مصاحبه‌ها بر اساس تخصص آن‌ها در جنگ الکترونیک و اینترنت اشیاء انتخاب شدند.

داده‌ها از طریق موارد زیر جمع‌آوری شدند:

پژوهش کتابخانه‌ای: تحلیل اسناد، شامل دکترین‌های نظامی، مقالات علمی و گزارش‌های فنی.

مصاحبه‌ها: مصاحبه‌های نیمه‌ساختاریافته با ۱۱ متخصص، با تمرکز بر کاربرد اینترنت اشیاء در حوزه‌های جنگ الکترونیک.

پرسشنامه‌ها: توزیع‌شده میان ۸۵ پاسخ‌دهنده برای ارزیابی امکان‌پذیری و اثربخشی اینترنت اشیاء در پشتیبانی، حمله و حفاظت الکترونیکی.

۵ - نتایج

۵-۱- پشتیبانی الکترونیکی

اینترنت اشیاء پشتیبانی الکترونیکی را با استقرار حسگرها در مکان‌های مناسب برای جمع‌آوری داده‌های محیطی و الکترومغناطیسی بلادرنگ تقویت می‌کند. حسگرهای متصل از طریق آر. اف. آی. دی[1]، وای‌فای و جی.پی.اس، نظارت مداوم بر شرایط میدان نبرد را امکان‌پذیر می‌کنند. داده‌های پیش‌پردازش‌شده با استفاده از الگوریتم‌های هوش مصنوعی تحلیل می‌شوند تا رفتار دشمن پیش‌بینی و تهدیدهای شناسایی شوند. کاربردهای کلیدی شامل:

[1] RFID

تشخیص سیگنال: حسگرهای اینترنت اشیاء سیگنال‌های راداری و مخابراتی دشمن را شناسایی می‌کنند.
آگاهی وضعیتی: اشتراک‌گذاری داده‌های بلادرنگ تصمیم‌گیری فرماندهان را بهبود می‌بخشد.
مدیریت منابع: اینترنت اشیاء کانال‌های ارتباطی را بهینه‌سازی می‌کند.
نتایج پرسشنامه نشان‌دهنده حمایت ۸۲.۴ درصدی از کاربرد اینترنت اشیاء در پشتیبانی الکترونیکی است.

جدول ۱: حمایت از اینترنت اشیاء در پشتیبانی الکترونیکی

پاسخ	تعداد	درصد
کاملاً موافق	۴۴	۵۱.۸٪
موافق	۲۶	۳۰.۶٪
بی‌نظر	۸	۹.۴٪
مخالف	۳	۳.۵٪
کاملاً مخالف	۴	۴.۷٪

۵-۲- حمله الکترونیکی

در حمله الکترونیکی، اینترنت اشیاء فریب و اختلال را از طریق موارد زیر تسهیل می‌کند:
تولید سیگنال جعلی: دستگاه‌های اینترنت اشیاء سیگنال‌های فریبنده تولید می‌کنند.
اختلال در شبکه: ترافیک شبیه‌سازی‌شده شبکه‌های دشمن را بیش‌ازحد بار می‌کند.
هدف‌گیری دقیق: جمرهای مبتنی بر اینترنت اشیاء فرکانس‌های خاص را هدف قرار می‌دهند.
پاسخ‌دهندگان (۸۲.۴٪) به‌طور قوی از نقش اینترنت اشیاء در حمله الکترونیکی حمایت کردند.

جدول ۲: حمایت از اینترنت اشیاء در حمله الکترونیکی

پاسخ	تعداد	درصد
کاملاً موافق	۴۴	۵۱.۸٪
موافق	۲۶	۳۰.۶٪
بی‌نظر	۸	۹.۴٪

مخالف	۳	۳.۵٪
کاملاً مخالف	۴	۴.۷٪

۵-۳-حفاظت الکترونیکی

اینترنت اشیاء حفاظت الکترونیکی را با نظارت بلادرنگ و پاسخ‌های خودکار به تهدیدها تقویت می‌کند. کاربردهای کلیدی شامل:

تشخیص تهدید: نظارت بر سلامت تجهیزات در حوزه حفاظت جنگ الکترونیک.

اقدامات متقابل خودکار: پایش بلادرنگ وضعیت تجهیزات و تاسیسات در حوزه حفاظت جنگ الکترونیک.

ارتباطات امن: بهبود پروتکل‌های رمزنگاری و فناوری‌های امنیتی پیشرفته در حوزه حفاظت جنگ الکترونیک.

حمایت از اینترنت اشیاء در حفاظت الکترونیکی ۷۶.۴ درصد بود.

جدول ۳: حمایت از اینترنت اشیاء در حفاظت الکترونیکی

پاسخ	تعداد	درصد
کاملاً موافق	۴۱	۴۸.۲٪
موافق	۲۴	۲۸.۲٪
بی‌نظر	۸	۹.۴٪
مخالف	۶	۷.۱٪
کاملاً مخالف	۶	۷.۱٪

۶ - بحث

باید این را پذیرفت که برای عملی نمودن به‌کارگیری اینترنت اشیاء وجود زیرساخت آن بسیار مهم است ولی در حال حاضر که زیرساخت ارتباطی جنگ الکترونیک نیروی زمینی ارتش جمهوری اسلامی ایران بیشتر بصورت غیرهوشمند بوده و یکپارچه نمی‌باشد بایستی سایر هماهنگی‌ها با معاونت‌ها و قسمت‌های مختلف نیروی زمینی را جهت تحقق این هدف کاملاً انجام داد تا چنانچه مشکل زیرساختی حل شد بتوان بدون دغدغه از این فناوری استفاده نمود . یافته‌ها پتانسیل تحول‌آفرین اینترنت اشیاء در جنگ الکترونیک را نشان می‌دهند. در پشتیبانی الکترونیکی، اینترنت اشیاء آگاهی وضعیتی را بهبود می‌بخشد؛ در حمله الکترونیکی، فریب و اختلال را تسهیل می‌کند؛ و در حفاظت

الکترونیکی، امنیت سایبری را تقویت می‌کند. حمایت بالا (۸۲.۴٪ برای پشتیبانی و حمله، ۷۶.۴٪ برای حفاظت) امکان‌پذیری عملی آن را تأیید می‌کند. محدودیت‌ها شامل ماهیت تخصصی موضوع و قابلیت تعمیم محدود است. تحقیقات آینده باید ادغام اینترنت اشیاء با فناوری‌های نوظهور مانند ارتباطات کوانتومی را بررسی کند.

۷ - نتیجه‌گیری

اینترنت اشیاء یک فناوری کلیدی برای ارتقای جنگ الکترونیک نیروی زمینی ارتش جمهوری اسلامی ایران است. با امکان جمع‌آوری داده‌های بلادرنگ، فریب و حفاظت خودکار، این فناوری نیازهای جنگ مدرن را برآورده می‌کند. استقرار شبکه‌های حسگر، توسعه سامانه‌های هشدار خودکار و تقویت رمزنگاری می‌تواند راه را برای به‌کارگیری این فناوری هموار سازد. با توجه به اینکه در شرایط حال حاضر به دلیل عدم وجود زیرساخت های مورد نیاز و عدم تامین امنیت، اینترنت اشیاء در محیط رزمی و غیررزمی نیروی زمینی استفاده نشده است نمی‌توان به صورت عینی و میدانی بررسی نمود ،نتایج بیشتر براساس واقعیت های موجود و امکانات فعلی بررسی شده و تا فراهم شدن زیرساخت آن بصورت بالقوه می‌باشد. این فناوری نه‌تنها کارایی عملیات‌ها را افزایش می‌دهد، بلکه دقت و سرعت تصمیم‌گیری را نیز بهبود می‌بخشد. از فناوری اینترنت اشیاء در شناسایی اهداف با دقت بسیار بالا نیز می‌توان استفاده نمود و نباید از کاربرد آن در بهبود پروتکل‌های رمزنگاری و فناوری‌های امنیتی پیشرفته غافل شد.

قدر دانی

خداوند بزرگ را شاکرم که توفیق نگارش این مقاله را به من داد و از تمامی اساتید خودم که مرا در این نوشتار یاری نمودند کمال تشکر دارم و برای تمام کسانی که در راه پربارتر شدن دانش در این زمینه با همه محدودیت‌ها تلاش می‌کنند آرزوی موفقیت دارم.

منابع

- آدامی، دیوید. (۱۴۰۰). جنگ الکترونیک. ترجمه: محمدمهدی نایبی و علی حرمتی. تهران: مؤسسه انتشارات دانشگاه صنعتی شریف
- احمدی، لیلا. (۱۳۹۷). بررسی مکانیزم‌های دفاعی و لجستیک در اینترنت اشیاء. پنجمین کنفرانس بین‌المللی علم و مهندسی، پاریس، ص ۷.

- اسدزاده، محمد. (۱۳۹۸). طرح‌ریزی تمرینات تاکتیکی جنگ الکترونیک. انتشارات دافوس آجا، تهران.
- اصغری، غلامعلی. (۱۴۰۲). دفاع الکترونیک. چاپ سوم. تهران: انتشارات مرامخ نزاجا.
- اعتضادی‌فر، پوریا، و گرمابدری، غلامرضا. (۱۴۰۳). طبقه‌بندی خودکار مدولاسیون درون‌پالسی ترکیبی راداری. فصلنامه پژوهش‌های نوین در سامانه‌های دفاع الکترونیکی، ۳(۷)، ص ۹۵.
- اکبری، سعید، مهتابی، رضا. (۱۳۹۸). دانستنی‌های جنگ الکترونیک. تهران: دانشکده مخابرات و جنگال شهید علی امینی نزاجا.
- بابانژاد، محمدرضا، فخری، سعید. (۱۴۰۱). نقش سیستم‌های الکترواپتیک در سامانه‌های پدافند هوایی. هفتمین همایش بین‌المللی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران، صص ۹-۱۲.
- بابایی، مرتضی. (۱۳۹۸). ارائه یک مدل تحلیل رفتار دشمن با استفاده از مدل‌های مخفی مارکوف بر اساس مشاهدات جنگ الکترونیک در صحنه‌های جنگ پیچیده. فصلنامه پدافند الکترونیکی و سایبری، ۷(۱)، ص ۵۹.
- بهشتی آتشگاه. (۱۳۹۷). مفاهیم و چالش‌های امنیتی اینترنت اشیاء نظامی با محوریت مکانیزم MIoT ایالات متحده آمریکا. فصلنامه علمی-پژوهشی فرماندهی و کنترل، ص ۶۴.
- بینش، عبدالحسین. (۱۳۹۷). جنگ الکترونیک. مجله حصون، صص ۱۲۵-۱۲۹.
- پورمکاری، علیرضا، غلام‌نژاد، پژمان، و غلامی، محمود. (۱۳۹۸). کاربردهای نظامی اینترنت اشیاء با تأکید بر مأموریت نیروی هوایی ارتش جمهوری اسلامی ایران. فصلنامه علوم و فنون نظامی، صص ۴۱-۲۷.
- شفیعی، علی. (۱۴۰۰). رویکردها و فناوری‌های استفاده‌شده در جنگ الکترونیک در نبردهای معاصر. هشتمین همایش ملی علوم و مهندسی دفاعی با رویکرد تهدیدات نوپدید، صص ۶۳-۷۱.

- طبی، محمد. (۱۴۰۰). ارتقاء امنیتی یگان‌های ارتش جمهوری اسلامی ایران با بهره‌گیری از فناوری اینترنت اشیاء. پایان‌نامه کارشناسی ارشد، دانشگاه فرماندهی و ستاد آجا.
- لک، بهزاد، راهبردهای به‌کارگیری اینترنت اشیاء در مأموریت‌های پلیس آگاهی، فصلنامه پژوهش‌های مدیریت انتظامی،۱۳۹۹، ص ۷۸
- موحدی، محمدرضا، سپهری، محمد. (۱۴۰۲). الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء، فصلنامه مطالعات دفاعی استراتژیک، شماره ۹۲، صص ۶۹-۹۲
- Bhatnagar, Rishi. Internet Of Things (Iot) | The Rise Of The Connected World, Confederation Of Indian Industry 125 Years Since 1895 ,Deloitte, 2020, P: 9
- FM ۳-۱۲. (۲۰۱۷). Cyberspace and Electronic Warfare Operations. Headquarters, Department of the Army.
- FM ۳-۸۵. (۲۰۲۰). Joint Electromagnetic Spectrum Operations. Headquarters, Department of the Army.
- Gautam, V., & Shishodia, V. (۲۰۲۲). The E-Intelligence System. ArXiv. https://www.semanticscholar.org/paper/
- Goh, M. W. C. (۲۰۲۰). Electromagnetic wave propagation. Wireless Internet of Things. doi.org/۹۷۸-۱-۷۹۹۸-۲۳۸۱-۰/۱۰.۴۰۱۸.ch۰۰۵
- Joint Publication ۳-۱۳.۱. (۲۰۱۲). Electronic Warfare. U.S. Department of Defense.
- Lin Zhu, Suryadipta Majumdar, Chinwe Ekenna. (۲۰۲۰). An invisible warfare with the Internet of Battlefield Things: A literature review. Department of Educational Psychology and Methodology. DOI: ۱۰.۱۰۰۲/hbe۲.۲۳۱.
- Liu, X. (۲۰۱۹). Overview of spintronic sensors with Internet of Things for smart living. IEEE Transactions on Magnetics. DOI: ۱۰.۱۱۰۹/TMAG.۲۰۱۹.۲۹۲۷۴۵۷.
- McGowan, J. (۲۰۱۷). Electronic Warfare Operations. U.S. Army Command and General Staff College.
- Robinson, C. P., et al. (۲۰۲۳). eSWORD: Implementation of wireless jamming attacks in a real-world emulated network. ۲۰۲۳ IEEE Wireless Communications and Networking Conference (WCNC), pp. ۱-۶. https://doi.org/۱۰.۱۱۰۹/WCNC۵۵۳۸۵.۲۰۲۳.۱۰۱۱۸۶۸۷

- Schmidt, A., & Wenzel, S. (۲۰۱۷). Competence development in cybersecurity: A framework for assessing skills and knowledge. Computers & Security, ۶۸, pp. ۱-۱۲.
- Sciancalepore, S., & Pietro, R. D. (۲۰۱۹). Bittransfer: Mitigating reactive jamming in electronic warfare scenarios. IEEE Access, ۷, ۱۵۶۱۷۵-۱۵۶۱۹۰. https://doi.org/۱۰.۱۱۰۹/ACCESS.۲۰۱۹.۲۹۴۹۷۱۶
- Wan, J., et al. (۲۰۱۸). A new radar signal recognition method based on optimal classification atom and IDCQGA. Symmetry, ۱۰, ۶۵۹. https://doi.org/۱۰.۳۳۹۰/sym۱۰۱۱۰۶۵۹