AJA Command and Staff University

**Military Science and Tactics**

https://www.qjmst.ir/ Online ISSN: 4520-2676 Print ISSN: 2008-191x

# Application of Internet of Things technology in Cyber and Electronic Warfare

Ali Alinezhad[1✉] | Davod Azar[2] | Vahid Sajadi Asil[3]

1. E.W & Cyber group Master. Command and Staff University,Tehran,Iran
E-mail: A.Alinezhad@casu.ac.ir
2. Phd student of Defense Management. Command and Staff University, Tehran, Iran.
E-mail: davodaxar@yahoo.com
3. Faculty Member of AJA Command and Staff University, Tehran, Iran.
E-mail: v.d.sajadi@gmail.com

## Article Info

**Article type:**

Research Article

**Article history:**
Received

01July 2023

Received in revised form

01 September 2023

Accepted

21 September 2023

Published online

11 Desember 2023

**Keywords**: .
*Military Internet of CyberElectronic Things, warfare, Situational Awareness, Autonomous Systems, Weopens.*

## ABSTRACT

**Objective:** This research was carried out to aim of explaining the applications of Internet of Things technology in cyber and electronic warfare.

**Method:** The method of doing descriptive research is applied and with a mixed approach.Seven experts from the army's electronic, cyberspace, telecommunications and electronic warfare and familiar with Internet of Things technology were selected for interviews to theoretical saturation by purposeful sampling. The statistical population for the questionnaire included some staff of the army of the Islamic Republic of Iran with at least a bachelor's degree in in the mentioned fields. the statistical population included 100 people (using coefficients), so the census method was used to distribute the questionnaires. First, document study and interviews were used to collect data. After that, the questionnaire was used.The reliability of the questionnaire was confirmed with Cronbach's alpha. Qualitative data analysis was done using content analysis method and quantitative data was analyzed using SPSS software

**Findings:** In total, the results of the research led to the statistics of four dimensions situational awareness, autonomous systems, weapons and personnel, 10 components C4ISR, GPS, digital maps, sence and avoid systems, swarm robots, precision targeting, fire control systems, unmanned guided systems, warriors, commanders, 27 indicators.

**Conclusion:** In total, the results of the research showed that with a high level of confidence, it can be acknowledged that the applications of Internet of Things technology in cyber and electronic warfare will be prioritized in the dimensions of weapons, personnel, situational awareness and autonomous systems.

**Cite this article:** Alinezhad, A., Azar, D., & Sajadi, V. (2023). Application of Internet of Things technology in Cyber and Electronic Warfare. *Military Science and Tactics*, *19*(65), 29-68.
doi: 10.22034/qjmst.2024.556192.1738

 **Publisher:** AJA Command and Staff University
DOI: 10.22034/qjmst.2024.556192.1738

فصلنامه علمی علوم و فنون نظامی
شاپای چاپی: ۲۰۰۸-۱۹۱X شاپای الکترونیکی: ۴۵۳۰-۲۶۷۶ https://www.qjmst.ir/
دانشگاه فرماندهی و ستاد آجا

# کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک

علی علی‌نژاد[۱] ✉ | داود آذر[۲] | وحید سجادی اصیل[۳]

۱. کارشناس‌ارشد مدیریت دفاعی، دانشگاه فرماندهی‌وستاد آجا، تهران،ایران.رایانامه: A.Alinezhad@Casu.ac.ir
۲. دانشجوی دکتری مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: davodazar@yahoo.com
۳. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: v.d.sajadi@gmail.com

## اطلاعات مقاله

**نوع مقاله:**
مقالهٔ پژوهشی

**تاریخ دریافت:**
۱۴۰۲/۰۴/۱۰

**تاریخ بازنگری:**
۱۴۰۲/۰۶/۱۰

**تاریخ پذیرش:**
۱۴۰۲/۰۶/۳۰

**تاریخ انتشار:**
۱۴۰۲/۰۹/۲۰

**کلیدواژه‌ها:**
*اینترنت اشیاء نظامی، جنگ سایبر الکترونیک، آگاهی وضعیتی، سامانه‌های خودمختار، جنگ‌افزارها*

## چکیده

**هدف:** این تحقیق با هدف تبیین کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک انجام شده است.

**روش:** روش اجرای پژوهش توصیفی، از نوع کاربردی و با رویکرد آمیخته انجام شده است. جامعه آماری برای مصاحبه، شامل ۷ نفر از خبرگان در حوزه الکترونیک، سایبر، مخابرات و جنگال آجا و آشنا به فناوری اینترنت اشیاء بوده است که به روش هدفمند انتخاب و مصاحبه با ایشان تا رسیدن به اشباع نظری ادامه یافت. جامعه آماری برای پرسش‌نامه، شامل کارکنان ارتش جمهوری اسلامی ایران در طیف درجات افسر ارشد و بالاتر هستند که دارای مدرک تحصیلی کارشناسی و بالاتر در رشته‌های ذکر شده بوده است. تعداد جامعه آماری ۱۰۰ نفر (با اعمال ضریبی) است و از روش سرشماری برای توزیع پرسش‌نامه استفاده گردید. ابتدا با استفاده از ابزار مطالعه اسناد و مدارک و مصاحبه داده‌ها جمع‌آوری شد، سپس از ابزار پرسشنامه استفاده شد که پایایی آن با محاسبه آلفای کرونباخ تأیید گردید. داده‌های کیفی با روش تحلیل محتوا تجزیه‌وتحلیل شدند و از نرم‌افزار SPSS برای تجزیه‌وتحلیل داده‌های کمی استفاده گردید.

**یافته‌ها:** درمجموع نتایج تحقیق منتهی به احصاء چهار بعد آگاهی وضعیتی، سامانه‌های خودمختار، جنگ‌افزارها و کارکنان و ۱۰ مؤلفه سی۴آی‌اس‌آر، سامانه موقعیت‌یاب جهانی، نقشه‌های رقمی، سامانه‌های تشخیص و جلوگیری، ربات‌های انبوه، هدف‌گیری دقیق، سامانه‌های کنترل‌آتش، سامانه‌های هدایت‌پذیر بدون‌سرنشین، رزمندگان، فرماندهان و ۲۷ شاخص گردید.

**نتیجه‌گیری:** در مجموع نتایج تحقیق نشان داد که با سطح اطمینان بالا می‌توان اذعان داشت که کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک، به ترتیب اولویت در بعدهای جنگ‌افزارها، کارکنان، آگاهی موقعیتی و سامانه‌های خودمختار خواهد بود.

**استناد**: علی‌نژاد، علی، آذر، داود و سجادی اصیل، وحید. (۱۴۰۲). کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک. علوم و فنون نظامی، ۱۹(۶۵)، ۶۸-۲۹. doi 10.22034/qjmst.2024.556192.1738

**ناشر:** دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران



DOI:10.22034/qjmst.2024.556192.1738

**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. فراگیر شدن اینترنت، ظهور فناوری‌های جدید و نوظهور را نیز به دنبال داشته که ازجمله آن‌ها، اینترنت اشیاء[1] است (لک، ۱۳۹۹: ۷۸). اینترنت اشیاء یا اینترنت چیزها[2] که امروزه اینترنت همه‌چیز[3] نیز نام‌گذاری می‌شود، 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 (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۶۴). پایگاه اطلاعاتی استاتیستا[4]، تعداد دستگاه‌های متصل به اینترنت اشیاء تا سال ۲۰۲۵ را بیش از ۷۵ میلیارد پیش‌بینی کرده است (Wani, 2019: 4).

تمامی فناوری‌های نوظهور، ارتباط مستقیمی با امور نظامی دارند و آینده انقلاب در امور نظامی را رقم می‌زنند. این فناوری‌ها می‌توانند نه‌تنها فنون و روش‌های عملیاتی بلکه راهبردهای نظامی را هم تغییر دهند (فلسفی و صادقی، ۱۳۹۸: ۱). اینترنت اشیاء توسعه حوزه نظامی را به‌طور عمده‌ای پیش خواهد برد و به نظر می‌رسد که به‌زودی شاهد شبکه‌های اینترنت اشیاء نظامی باشیم (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۷۷). اینترنت اشیاء ایجادکننده همگرایی چند رشته مانند؛ شبکه، سخت‌افزار تعبیه‌شده، طیف رادیویی، محاسبات سیار، فناوری‌های ارتباطی، فناوری‌های نرم‌افزار، فناوری‌های حساس، بهره‌وری انرژی، مدیریت اطلاعات و تجزیه‌وتحلیل داده‌ها است (پورمکاری و همکاران، ۱۳۹۸: ۱۴۳). از طرفی با در نظر گرفتن جنگ‌های اخیر، بدون تردید می‌توان بیان نمود که جنگ سایبر[5] و جنگ الکترونیک[6] نیز در حال تبدیل‌شدن به عناصر کلیدی صحنه نبرد هستند و تسلط بر طیف الکترومغناطیسی و سامانه‌های اطلاعاتی، فرمانروایی مطلق در میدان جنگ را به ارمغان خواهد آورد. وجوه اشتراکات جنگ سایبر و جنگ الکترونیک در اصول و فرایند اجرا و همچنین تأثیرات و پیامدهای نسبتاً مشابه آن‌ها در سازمان‌های نظامی، سبب همگرایی بین این دو عرصه و عامل برتری ساز و تعیین‌کننده در نبردهای آینده خواهد بود (فرحبخت و دهقانی، ۱۳۹۸:

[1] Internet Of Objects
[2] IOT:Internet Of Things
[3] IOE: Internet of Everythings
[4] Statista
[5] Cyber Warfare
[6] Electronic Warfare

۲۰۰). با توجه به آنچه بیان گردید، کاربردهای اینترنت اشیاء در حوزه نظامی و به‌تبع آن در حوزه جنگ سایبر و الکترونیک در حال گسترش است؛ بنابراین اهمیت این تحقیق را می‌توان به شرح ذیل بیان نمود:

الف) آشنایی با کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک

ب) معرفی معماری‌های مختلف فناوری اینترنت اشیاء و لایه‌های آن شامل معرفی حسگرها و تجهیزات دریافت داده (لیزر، سونار، رادار، مادون‌قرمز، حسگر صوتی، دوربین، تعیین موقعیت، حسگر دما، تگ‌های شناسایی با امواج رادیویی، حسگرهای بیولوژیک و ...) و معرفی پروتکل‌های ارتباطی (بلوتوث، وای فای، زیگ‌بی[۱]، ارتباطات میدان نزدیک[۲]، شناسایی از طریق امواج رادیویی، زدویو[۳]، شبکه حسگر بی‌سیم و ...)، پروتکل‌های شبکه (ام‌کیوتی‌تی[۴]، سی‌اوای‌پی[۵]، دی‌دی‌اس[۶]، ای‌ام‌کیوپی[۷]) و استفاده از آن‌ها در حوزه جنگ سایبر و الکترونیک.

ت) پویایی و استفاده از علم روز، فناوری‌ها و تجهیزات به‌روز نظامی

ث) بیان توجه سازمان‌های نظامی به همگرایی جنگ سایبر و جنگ الکترونیک

در صورت عدم شناخت کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک، می‌توان به باقی ماندن مسائل و مشکلاتی به شرح ذیل اشاره نمود:

الف) عدم بهره‌برداری از فناوری‌های روز و ناکارآمدی سامانه‌های کنونی در آینده نه‌چندان دور.

ب) عدم سرعت در ارتباطات که مدیران را در تصمیم‌گیری‌های به‌موقع با مشکل مواجه می‌کند.

پ) عدم تسلط کامل بر صحنه عملیات جنگ سایبر و الکترونیک.

ت) عدم شناخت صحیح از حسگرهای روز دنیا و کاربرد آن‌ها در امور نظامی

ج) عدم توجه به همگرایی جنگ سایبر و جنگ الکترونیک در سطوح مختلف رزمی

چ) عدم آشنایی با تجهیزات به‌روز سربازان و فرماندهان درصحنه‌های نبرد سایبر و الکترونیک.

با توجه به آنچه گفته شد و با در نظر گرفتن این‌که استفاده از فناوری‌های روز دنیا ازجمله فناوری اینترنت اشیاء، یکی از راهبردهای اصلی کشورهای قدرتمند نظامی به‌ویژه کشور متخاصم آمریکا بوده و در سال‌های اخیر نیز به‌خوبی نمود پیداکرده است؛ در این تحقیق به دنبال این هستیم که جهت کسب اطلاعات دقیق، مدون و سازمان‌یافته در خصوص تبیین کاربردهای این

---

[1] ZigBee
[2] NFC: Near Filed Communication
[3] Z-Wave
[4] MQTT: Message Queue Telemetry Transport
[5] COAP: Constrained Application Protocol
[6] DDS: Data Distribution Service
[7] AMQP: Advaned Message Queuing Protocol

فناوری در جنگ سایبر و الکترونیک که از حوزه‌های اصلی صحنه‌های نبرد آینده خواهد بود، از مزایای آن‌هم بهره برده و با استفاده از آن، نقاط ضعف خودی را پوشش و نقاط قوت خودی را تقویت کنیم. در این راستا سؤال اصلی پژوهش به شرح ذیل تدوین گردید: «کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک چیست؟"

## مبانی نظری، پیشینه‌های تحقیق، چارچوب مفهومی پژوهش

در میدان نبرد آینده از اشیاء هوشمندی استفاده خواهد شد که قابلیت‌های ارتباط با یکدیگر و با نیروهای رزمی را خواهند داشت. این اشیاء با استفاده از نرم‌افزار و سخت‌افزارهای مناسب، خدمات تعیین‌کننده در میدان نبرد را در یک فضای ابری فراهم می‌آورند که با عنوان اینترنت اشیاء شناخته می‌شوند (گروه مؤلفین معاونت فاوا آجا، ۱۴۰۰ : ۲). از طرفی در بندهای ۵۲ و ۵۳ سیاست‌های کلی برنامه ششم توسعه کشور ابلاغی مقام معظم رهبری (مدظله‌العالی)، افزایش توان دفاعی در تراز قدرت منطقه‌ای در جهت تأمین منافع و امنیت ملی و ارتقاء توان بازدارندگی کشور با توسعه فناوری‌ها و تجهیزات عمده دفاعی برتر ساز متناسب با انواع تهدیدات مورد تأکید قرارگرفته است. بنابراین در این تحقیق، در ابتدا به معرفی اینترنت اشیاء به‌عنوان یکی از پرکاربردترین فناوری‌های روز دنیا و همچنین جنگ سایبر و جنگ الکترونیک به‌عنوان دو حوزه جدید جنگ‌های امروزی پرداخته‌ایم و بعد از بیان همگرایی جنگ سایبر و جنگ الکترونیک، کاربردهای فناوری اینترنت اشیاء و چالش‌های به‌کارگیری آن نیز اشاره شده است.

### اینترنت اشیاء

اصطلاح اینترنت اشیاء اولین بار توسط کوین اشتون در سال ۱۹۹۹ میلادی به‌کاربرده شد و برای نخستین بار توسط انتشارات مؤسسه ام‌آی‌تی[1] به دنیا معرفی گردید و جهانی را توصیف کرد که در آن هر چیزی، ازجمله اشیاء بی‌جان، برای خود هویت رقمی[2] داشته باشند (موحدی صفت، ۱۴۰۰: ۲۲). تجزیه‌وتحلیل گر دیلویت این فناوری را در بین فناوری‌های دیگری مانند هوش مصنوعی[3]، تحلیل کلان داده[4]، نانو فناوری[5]، رباتیک پیشرفته[6]، واقعیت افزوده[7] و ... به‌عنوان فناوری که می‌تواند بیشترین تأثیر را بر سازمان‌ها داشته باشد، معرفی کرده است (Bhatnagar, 2020: 9). رشد

[1] MIT
[2] Digital
[3] Artificial Intelligence
[4] Big Data Analytics
[5] Nano Technology
[6] Advanced Robotics
[7] Augmented reality

سریع اینترنت اشیاء توسط چهار پیشرفت کلیدی در فناوری‌های رقمی هدایت می‌شود. یکی از این موارد، کاهش هزینه و کوچک‌سازی دستگاه‌های میکروارگانیسم مثل مبدل‌ها (حسگرها و محرک‌ها)، واحدهای پردازش (میکرو واپایشگرها[۱]، ریزپردازنده‌ها[۲])، ارائه دروازه قابل‌برنامه‌ریزی و گیرنده‌ها است. عامل دوم، سرعت و انبساط سریع اتصال بی‌سیم است. سوم توسعه ذخیره‌سازی داده و ظرفیت پردازش سامانه‌های محاسباتی است و درنهایت چهارم، ظهور برنامه‌های کاربردی، نوآورانه و تجزیه‌وتحلیل ازجمله پیشرفت‌هایی در فن‌های یادگیری ماشین برای پردازش داده‌های بزرگ است (پورمکاری و همکاران، ۱۳۹۸: ۱۴۳). اینترنت اشیاء دنیای فیزیکی و دنیای مجازی را به یکدیگر وصل می‌کند و شامل هر چیزی، هر وسیله‌ای، هرکسی، هر شغلی، هر خدماتی، هر مسیری، هر شبکه‌ای، هرجایی، هر مکانی، هرزمانی و هر محتوایی[۳] است (Rahul & Alhumiany, 2017: 423).

تولید مقالات حوزه اینترنت اشیاء در دو دهه اخیر رشد چشمگیری داشته که ناشی از پتانسیل بالقوه آن برای کارآمدی خدمات در دنیای واقعی است. در این راستا مجله حس‌گر[۴] بیشترین مقالات را منتشر کرده است. کشور چین نیز در تولید مقالات پیشرو بوده است و مجله چینی ژونگویی[۵] یکی از ده مجله پر تولید در این حوزه است. برخی از رهبران صنعتی آلمان، اینترنت اشیاء را انقلاب چهارم صنعتی، بعد از موتور بخار، تسمه نقاله، مرحله اول آی‌تی[۶] و فناوری خودکارسازی می‌نامند (عاصمی و همکاران، ۱۳۹۷: ۵۱۲). فراگا لاماس و همکاران (۲۰۱۶)[۷] در تحقیقی جامع با عنوان مروری بر اینترنت اشیاء برای دفاع و امنیت عمومی به گستردگی دستگاه‌ها و کاربردهای بی‌شمار اینترنت اشیاء (شکل ۱) اشاره نموده است و از چهار عامل به‌عنوان عوامل کلیدی گسترش اینترنت اشیاء نام‌برده است:

الف) کاهش هزینه‌ها و کوچک‌سازی میکروالکترونیک

ب) سرعت سریع و گسترش اتصال بی‌سیم

پ) گسترش ذخیره اطلاعات و ظرفیت پردازش سامانه‌های اطلاعاتی

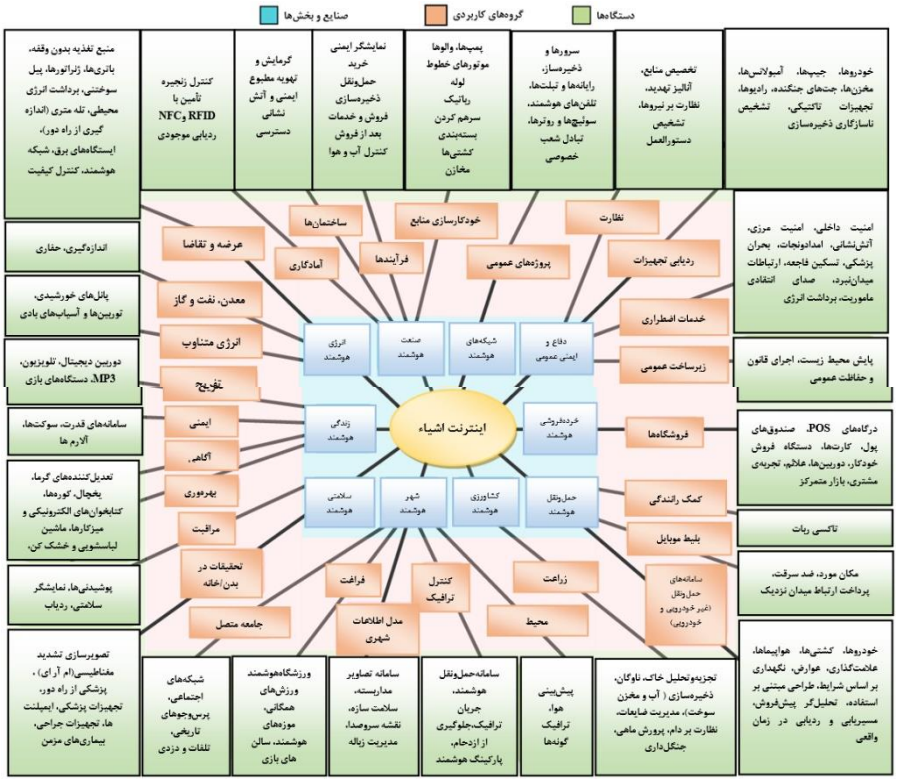
ت) نرم‌افزار و تجزیه و تحلیل‌های نرم‌افزاری نوآورانه (Fraga-Lamas & et al, 2016: 2)

---

[1] Microcontrollers
[2] Microprocessors
[3] Anything, Any device, Anyone, Anybody, Any service, Any business, Any path, Any network, Any place, Anywhere, Anytime & Any context
[4] Sensors
[5] Zhongguo Yi Liao Qi Xie Za Zhi
[6] IT
[7] Fraga-Lamas & et al

پنج نمونه بستر سخت‌افزاری اینترنت اشیاء نیز شامل رزبری‌پای، آردوینو، بیگل‌بون بلک، فیجت، اودو[1] می‌باشد (Maksimović and ets, 2018: 3).

حسگرهای اینترنت اشیاء نیز شامل حسگرهای مغناطیسی، رادیویی، الکتریکی، آراف‌آی‌دی، ان‌اف‌سی، سنجش لرزش، شتاب، شیب، موقعیت، مجاورت، آکوستیک، رطوبت، حرکت، حجم، جابجایی، درجه حرارت، فشار، بار، نیرو، نشتی، رسانایی و شوری آب، کدورت، دید و تضعیف نوری آب و ... است (Jahanbakht & et al, 2021: 6).




**شکل (۱) گسترش دستگاه‌ها و برنامه‌های کاربردی در اینترنت اشیاء**

بوگنار (۲۰۱۸) ساختار سه‌لایه‌ای اینترنت اشیاء را مطابق جدول زیر بیان نموده است. (Bognar, 2018: 380)

**جدول (۱) ساختار سه‌لایه‌ای اینترنت اشیاء**

[1] Raspberry Pi, Arduino, BeagleBone Black, Phidgets, udoo

| فناوری | لایه‌ی اینترنت اشیاء |
|---|---|
| شبکه‌های حسگر، آراف‌آی‌دی، دوربین‌ها، رادارها و ... | لایه احساس (ادراک) |
| زیگ‌بی، بلوتوث، وای فای، ۶ لوپن، شبکه‌های تلفن همراه، جی‌پی‌اس و ... | لایه شبکه |
| خانه هوشمند، مدیریت توان و انرژی، اتومبیل‌های خودران، فناوری ابر و ... | لایه کاربرد |

الف) لایه احساس (ادراک): این لایه با استفاده از حسگرهای نصب‌شده بر روی اشیاء، اطلاعات را جمع‌آوری و آن‌ها را شناسایی می‌کند. به‌عنوان‌مثال برای دادن مسیر به یک مرد نابینا، حسگرهایی که روی چوب هوشمند مرد نابینا نصب‌شده است، موانع را حس کرده و داده‌های حس شده را به لایه شبکه ارسال می‌کند. بنابراین، این لایه داده‌ها را با استفاده از حسگرها جمع‌آوری می‌کند و محرک‌های حیاتی برای برنامه‌های مبتنی بر اینترنت اشیاء است. این حسگرها عبارتند از انواع دوربین‌ها، رادار، سونار، جی‌پی‌اس، شتاب‌سنج، حسگر نور، دما، فشار، رطوبت، آشکارساز رادیو فرکانسی[1]، پارامترهای علائم حیاتی بدن و غیره استفاده می‌شوند.

ب) لایه شبکه: این لایه از شبکه‌ای تشکیل‌شده است که از اجزای سیمی و بی‌سیم با اتصال به اینترنت است. وظیفه اصلی آن دریافت اطلاعات از لایه ادراک و انتقال اطلاعات به لایه کاربردی است. لایه شبکه شامل گره‌های دروازه و یک شبکه دسترسی است که در آن گره‌های دروازه، داده‌ها را از لایه ادراک جمع‌آوری کرده و در اختیار شبکه دسترسی قرار می‌دهند. شبکه دسترسی ممکن است از یک شبکه فیبر نوری قدرت[2] یا یک شبکه دسترسی بی‌سیم مانند زیگبی، بلوتوث، وای فای، شبکه‌های تلفن همراه و ... تشکیل‌شده باشد. درمجموع لایه شبکه وظیفه مسیریابی بسته‌های دریافتی از لایه ادراک را بر عهده دارد.

پ) لایه کاربرد: این لایه شامل برنامه‌ها یا رابط‌های کاربری برای پردازش اطلاعات دریافتی از لایه شبکه و ادراک بر اساس نیاز کاربر است. با توجه به مثال مرد نابینا در بالا، اطلاعات جمع‌آوری‌شده از حسگر می‌تواند برای تبدیل آن به صدا یا نقشه استفاده شود که می‌تواند برای راهنمایی فرد نابینا تحویل داده شود. لایه کاربردی عمدتاً مسئول قالب‌بندی داده‌ها، ارائه و تصمیم‌گیری و کاربردی است که نتیجه نهایی استفاده از فناوری اینترنت اشیاء خواهد بود. (Nitin Gupta & Jyoti Gupta, 2017, P:10).

## جنگ سایبر

[1] RFID: Radio Frequency Identification
[2] Power fiber-optic network

موضوع فناوری اطلاعات و فضای سایبر یکی از موضوعاتی است که از ده سال گذشته تا به امروز با شیب تندی رو به افزایش است و سایبر تقریباً کل فضا و حوزه زندگی بشر را در بر گرفته است (حقگو، ۱۳۹۷: ۱۳۸). در سند راهبردی سایبر وزارت دفاع آمریکا، فرماندهی سایبر ایالات‌متحده به دهمین فرماندهی رزمی مستقل یکپارچه و مسئول اصلی انجام عملیات سایبر تبدیل گردیده است (سجادی اصیل، ۱۳۹۸: ۱۰). شالوده و اساس فضای سایبر بر شبکه جهانی اینترنت بناشده است و برای اینکه انسان‌ها و اشیاء از اجزای این فضا محسوب شوند، باید به این شبکه متصل شوند یا قابلیت ارتباط با افراد و اشیاء دیگر از این طریق را دارا باشند. در این خصوص، آشنایی و آگاهی مسئولین و فرماندهان نیروهای مسلح نسبت به شناخت هر چه بیشتر این‌گونه تحولات و اشراف اطلاعاتی با نگاه راهبردی و عمیق‌تر با فناوری‌های نوظهور فضای سایبر مانند هوش مصنوعی، رایانش ابری، اینترنت اشیاء، زنجیره بلوکی و کلان داده‌ها که از ابزار ضروری تصمیم‌گیری و تبیین برنامه‌های آتی هر کشور است، از اهمیت بالاتری برخوردار است (موحدی صفت، ۱۴۰۰: ۲). جنگ سایبر مقدمه جنگ نظامی است، هر جنگ نظامی یک هدف سیاسی را دنبال می‌کند که هدف سیاسی آن براندازی و برهم زدن کنترل و تعادل امنیتی کشور است، این کار در فضای سایبر امکان‌پذیر است. هیچ عملیات نظامی و تهدید نظامی علیه کشورها اتفاق نمی‌افتد مگر اینکه بخشی از آن تهدید سایبر است، بنابراین جنگ سایبر یکی از ارکان جنگ‌ها در امروز و آینده است که متکی به فناوری اطلاعات و ارتباطات است (محمدی و کریمی قهرودی، ۱۳۹۹: ۷). جنگ سایبر شامل استفاده از حملات رقمی برای حمله به یک ملت که موجب آسیب قابل قیاس با جنگ واقعی می‌شود و سامانه‌های حیاتی رایانه را مختل می‌کند. جنگ سایبر عملیاتی است در راستای راهبرد دفاع ملی برای دستیابی به برتری اطلاعاتی از طریق تأثیرگذاری روی اطلاعات و سامانه‌های اطلاعاتی دشمن در عین راهبری و حفاظت از اطلاعات و سامانه‌های اطلاعاتی خودی است (موحدی صفت، ۱۴۰۰: ۱۴). انجام جنگ سایبر در سامانه‌های ارتباطی دشمن، موجب خواهد شد تا شبکه برق، شبکه کنترل ترافیک هوایی، شبکه بانکی و مالی، شبکه مخابرات و شبکه‌های رادیو، تلویزیون، ماهواره و اینترنت دشمن به‌طور کامل فلج شده و او را درگیر ازهم‌گسیختگی در جامعه، تظاهرات خیابانی و بحران سیاسی کند (بختیاری، ۱۳۹۹: ۵۵).

## جنگ الکترونیک

گسترش فعالیت سامانه‌های ارتباطی و الکترونیکی از طیف الکترومغناطیس و استفاده گسترده و هدفمند از این نوع سامانه‌ها در بخش‌های نظامی و پی بردن به ارزش حیاتی این فناوری در عرصه نبرد، باعث شکل‌گیری شاخه دیگری از دانش و عملیات به نام جنگ الکترونیک شد که بعدها چرچیل آن را جنگ جادو نام نهاد (آذر و محمدحسین، ۱۳۹۷: ۱۹). امروزه هدف اصلی در یک جنگ، حمله به یک ناو، هواپیما و یا اهداف زمینی نیست؛ بلکه حمله به شبکه اطلاعات و ارتباطات دشمن مدنظر است. ازاین‌رو در جنگ‌های آتی، دستگاه‌های هوشمند، رایانه‌ها و سامانه‌های

ایجادکننده اختلال هستند که با داشتن توانایی در ایجاد ارتباط و دریافت اطلاعات، سرنوشت نهایی جنگ را رقم خواهند زد. ماهواره‌های جاسوسی و مخابراتی، هواپیماهای بدون سرنشین، انواع هواپیماهای مخصوص جنگ‌های الکترونیکی، شبکه‌های فرستنده رقمی و انتقال اطلاعات در رایانه‌های کوچک قابل‌حمل توسط سرباز، همه و همه به نحو چشمگیری بر اصول جنگ، اعم از اصل غافلگیری، وحدت فرماندهی و ... تأثیرگذارند. آن‌ها بانفوذ در سامانه اطلاعاتی و ارتباطی دشمن، در اولین گام، سعی در فلج کردن سامانه فرماندهی، نظارت و مراقبت نیروی مسلح می‌نماید. استفاده گسترده از سامانه‌های الکترونیکی و طیف امواج الکترومغناطیسی، در انواع تجهیزات و جنگ‌افزارها و به‌کارگیری آن‌ها در نبردهای امروزی به‌عنوان یک اقدام تاکتیکی و راهبری محسوب می‌شود (نیازمند، ۱۳۹۸: ۱).

جنگ الکترونیک که به‌منظور کنترل، بهره‌برداری و تهاجم نرم و سخت الکترونیک دشمن و حفظ خودی در برابر اقدامات جنگ الکترونیک دشمن به کار می‌رود که شامل تهاجم الکترونیک[1]، حفاظت الکترونیک[2] و پشتیبانی الکترونیک[3] می‌باشد.

تعدادی از مأموریت‌های مهم جنگ الکترونیک در پشتیبانی عملیات رزمی عبارت‌اند از:

الف) تضعیف برتری هوایی نیروی مهاجم با اجرای اختلال و فریب در سامانه‌های راداری، ناوبری، ارتباطی دشمن.

ب) ایجاد تأخیر در سامانه فرماندهی و کنترل و کاستن از سرعت پیشروی یگان‌های نیروی مهاجم با اجرای اختلال و فریب بر روی شبکه‌های ارتباطی، راداری، ناوبری و الکترواپتیک دشمن.

پ) تضعیف شبکه پدافند هوایی ارتفاع پایین، متوسط و بالای دشمن

ت) از کار انداختن سامانه الکترونیکی سلاح‌های دشمن با استفاده از سامانه‌های خود حفاظتی منصوب بر هواپیما، شناور و ادوات زمینی (چف، فلیر، دکوی، اخلال‌گر حرارتی، اخلال‌گرهای خود حفاظتی راداری و ...)

ث) همکاری در طرح‌ریزی شبکه‌های جعلی ارتباطی، راداری و ناوبری به‌منظور گمراه نمودن سامانه جمع‌آوری اطلاعات الکترونیکی دشمن

ج) تعیین مسیر پیشروی و هویت عمده قوا دشمن، همچنین کشف و اعلام خبر در تک هوایی، عملیات تازش هوایی و نفوذ نیروهای ویژه دشمن با استفاده از شنود و تعیین محل رادیویی، راداری و الکترواپتیکی

---

[1] Electronic Attack
[2] Electronic Protection
[3] Electronic Support

مأموریت‌های مستقل جنگ الکترونیک شامل کشف، اختلال و فریب بر روی شبکه ارتباطی و راداری سامانه‌های دفاع موشکی، لینک‌های ارتباطی چند نیرویی راهبردی مانند لینک ۱۶، ماهواره‌های ارتباطی (ثابت و سیار)، دفاع غیرفعال و فعال لیزری، کشف، اختلال، فریب و انهدام پدافند هوایی برد متوسط و بلند، موشک‌های کروز و بالستیک، سونارهای فعال و غیرفعال زیرسطحی و اژدرها، پهپادهای تاکتیکی و راهبردی، رادارهای ارائه فازی هوا پایه، زمین پایه، دریا پایه و فضاپایه و اختلال و فریب سامانه‌های تعیین موقعیت ماهواره‌ای است (اسدالله زاده، ۱۳۹۸: ۱۸ و ۱۹).

## همگرایی جنگ سایبر و الکترونیک

امروزه جنگ سایبر و الکترونیک، نقش تعیین‌کننده‌ای در تاکتیک‌های نظامی کشورها (تهاجمی، تدافعی) دارد (سجادی اصیل و آذر، ۱۳۹۹: ۷). وجوه اشتراک جنگ سایبر و جنگ الکترونیک در اصول و فرایند اجرا و همچنین تأثیرات و پیامدها مشابه آن‌ها در سازمان‌های نظامی، سبب همگرایی بین این دو عرصه و عامل برتری ساز و تعیین‌کننده در نبردهای آینده خواهد بود (فرحبخت و دهقانی، ۱۳۹۸، ۲۰۰). جنگ الکترونیک شبکه محور اقدامی است که در جهت کشف، متوقف نمودن و خنثی نمودن ابزارهای الکترونیکی، مخابراتی، راداری و سامانه‌های الکترواپتیکی دشمن که محدوده بسیار وسیعی از فناوری‌های مختلف دفاعی را در برمی‌گیرد و بر روی توان رزمی حاصل از ارتباطات کارآمد و شبکه شدن تمام عناصر و تجهیزات ارتباطی و اطلاعاتی حاضر در صحنه نبرد تأکید دارد. بدیهی است که تحقق این امر مزایایی چون افزایش سرعت ارتباطات و عملیات، افزایش حساسیت یا کوتاه کردن زمان واکنش به یک وضعیت جدید و غیره را در پی داشته و خطرات و هزینه‌ها را هم به‌شدت کاهش می‌دهد. فناوری‌های مختلفی وجود دارد که هرکدام در شبکه محور نمودن جنگ‌ها و ازجمله جنگ الکترونیک نقش اساسی دارد؛ که ازجمله‌ی این فناوری‌ها می‌توان به معماری‌های شبکه‌ای، ماهواره‌ها، وسایل نقلیه بدون سرنشین، نانو فناوری و حسگرهای زمینی اشاره نمود (پور قهرمانی و همکاران، ۱۳۹۵: ۴۴۳). درمجموع، اقدامات هم‌افزای جنگ الکترونیک و سایبر به منظورهای عمده زیر صورت می‌گیرد:

الف) نفوذ، تخریب و یا اختلال بر روی اطلاعات موجود در حافظه رقمی و کانال‌های ارتباطی

ب) نفوذ و آسیب رساندن به سخت‌افزارها یا انهدام سامانه‌ها.

پ) نفوذ و صدور فرمان‌ها کاذب به‌وسیله جعل هویت و فریب کاربران.

ت) نفوذ و دست‌کاری هدفمند اطلاعات و ایجاد تأخیر در فعالیت شبکه با اشغال پهنای باند.

ث) نفوذ در شبکه‌های اطلاعاتی، پردازشگرهای سلاح و افزودن اطلاعات.

ج) نفوذ در شبکه‌های راداری، ایجاد اهداف کاذب و اجرای فریب راداری.

چ) نفوذ در شبکه‌های ناوبری، افزایش خطای ناوبری و اجرای فریب ناوبری.

ح) نفوذ در لینک، افزایش خطای رادیو کنترل و اجرای فریب ناوبری (اسدالله زاده، ۱۳۹۸: ۱۹).

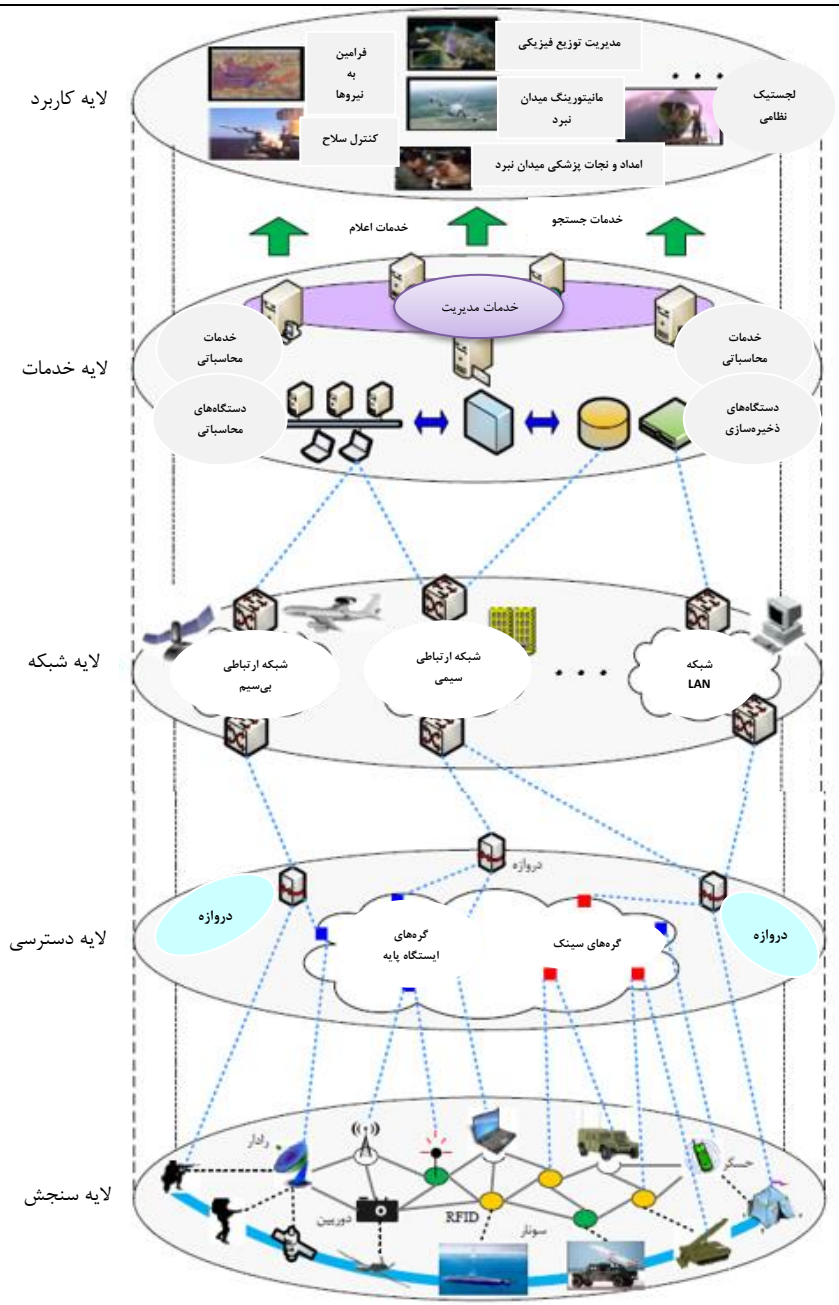
## کاربردهای نظامی اینترنت اشیاء

گسترش روزافزون فناوری در عرصه‌های نظامی، شکل و نحوه جنگ‌ها را به‌طورکلی متحول ساخته است. نفوذ فناوری در ارتش‌های پیشرفته امروزی و در دو بعد نرم‌افزار و سخت‌افزار تا حدی است که به‌جرئت می‌توان گفت دیگر بخش یا یگان نظامی نیست که فاقد نشان‌هایی از فناوری باشد. از مهم‌ترین ویژگی‌های جنگ‌های امروزی می‌توان به جنگ‌افزارهای هدایت دقیق، ربات‌ها، فناوری غیر کشنده، تسلیحات هدایت مستقیم انرژی و ویروس‌های رایانه‌ای اشاره نمود. پیدایش فناوری اینترنت اشیاء، انجام اموری نظیر هدایت و نظارت عملیاتی را در شرایط حساس و بحرانی به‌آسانی امکان‌پذیر ساخته است (شعبانی و همکاران،۱۳۹۵: ۲). معماری و کاربردهای نظامی اینترنت اشیاء با سرعت قابل توجهی در حال گسترش است که بخشی از آن در شکل (۲) نشان داده‌شده است (Fraga Lamas, 3016: 6).


**شکل (۲) معماری و کاربردهای نظامی اینترنت اشیاء**

اینترنت اشیاء نظامی می‌تواند زیرساخت فیزیکی نظامی و زیرساخت اطلاعات را به‌طور عمیق با هم بیامیزد و قابلیت اتصال اشیاء نظامی با یکدیگر را فراهم نماید و امور متنوع نظامی را با دقت بیشتر و پویاتری پیاده‌سازی و مدیریت نماید و میزان کارایی عملیات نظامی را افزایش دهد. (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۷۰).

معماری پنج لایه اینترنت اشیاء نظامی آمریکا به شرح شکل (۳) می‌باشد: (بهشتی آتشگاه، ۱۳۹۷: ۷۳)




**شکل (۳) معماری پنج لایه اینترنت اشیاء نظامی آمریکا**

**آگاهی وضعیتی (سامانه‌های سی۴آی‌اس‌آر، سامانه موقعیت‌یاب جهانی، نقشه‌های رقمی)**

در بررسی کاربرد اینترنت اشیاء در حوزه نظامی چندین حالت استفاده با تأثیر بالا به‌منظور پیاده‌سازی در محیط‌های نظامی مانند تجهیزات هوشمند، لجستیک، مراقبت پزشکی نظامی وجود دارد که آگاهی

وضعیتی هم یکی از آن‌هاست (لک، ۱۳۹۹: ۸۱). از ویژگی‌های اینترنت اشیاء نظامی این است که می‌توان از قابلیت‌های آن، برای ایجاد آگاهی پیشرفته از وضعیت در ناحیه عملیاتی استفاده کرد. فرماندهان نظامی، تصمیم‌گیری‌های خود را بر اساس تحلیل‌های بی‌درنگ ایجادشده به‌وسیله ترکیب داده‌های مربوط به حسگرهای خودکار و گزارش‌های مربوط به میدان عملیاتی، انجام می‌دهند. با استفاده از انواع مختلف حسگرها و نصب آن‌ها در هواپیماها، پهپادها، ماهواره‌ها و ناوها، می‌توان امکان کنترل فعالیت‌های دریایی و ترافیک در نواحی بزرگ، ردیابی شناورهای جنگی و نظارت بر روی شرایط محیطی را فراهم آورد (احمدی و همکاران، ۲۰۱۶: ۷).

دانش، بینش و شناخت کافی از صحنه نبرد، کنترل عملیات و اقدام به‌موقع، از کلیدی‌ترین ویژگی‌های سامانه فرماندهی و کنترل است که این در سایه هوشمندی این سامانه‌ها قابل دستیابی است. استفاده از فناوری نوین اینترنت اشیاء در سامانه‌های فرماندهی و کنترل به خاطر ویژگی‌های خاص این سامانه‌ها ازجمله زمان پردازش، هزینه کم‌تر، تصمیم‌گیری به‌موقع و بلادرنگ از اهمیت زیادی برخوردار است (محمدی و کریمی قهرودی، ۱۳۹۹: ۲). امروزه توسعه کاربردهای نظامی فناوری اینترنت اشیاء با محوریت ایالت متحده آمریکا بر روی کاربرد سامانه سی۴آی‌اس‌آر متمرکز شده است. به‌منظور جمع‌آوری داده‌های نظامی، میلیون‌ها حسگر بر روی حوزه وسیعی از بسترها و سکوها پیاده‌سازی و توسعه داده‌شده‌اند. داده‌های رادار، سونار، ویدئو، فناوری اینفرارد و داده آشکارساز رادیو فرکانسی توسط بسترهای حسگر هوابرد، ماهواره‌های جاسوسی و پرنده‌های بدون سرنشین، ایستگاه‌های زمینی و دریایی، سربازان در میدان نبرد، سامانه‌های زمینی متداول توزیع‌شده[1] و بستر اصلی یکپارچه‌سازی داده سی۴آی‌اس‌آر نظامی جمع‌آوری می‌گردند. این سامانه، تصویر جامعی از موقعیت و وضعیت نیروهای خودی و دشمن ارائه داده و فرماندهان ارشد از طریق مراکز عملیات مرکزی که داده را از بسترهای مختلف جمع‌آوری می‌نمایند، می‌توانند آگاهی وضعیتی جامعی از وضعیت میدان نبرد داشته باشند. (بهشتی و همکاران، ۱۳۹۷: ۶۶).

نسل جدید سامانه‌های مدیریت نبرد شامل تلاش‌هایی برای ایجاد سامانه‌هایی در جهت استفاده از فضای ابری، سایبر و روش‌های ارتباط سریع ماهواره‌ای است. استفاده از این فناوری موجب انتقال سریع و اشتراک‌گذاری حجم بالای اطلاعات بین نیروهای نظامی می‌شود. کاربردی نمودن فناوری‌های نوین بالغ ازجمله اینترنت اشیاء (با استفاده از اینترنت ماهواره‌ای)، هوش مصنوعی و الگوریتم‌های رمزنگاری نوین در جهت بهبود عملکرد واحد فرماندهی و کنترل، برای یکپارچه‌سازی نیروها، کاهش زمان تجزیه‌وتحلیل اطلاعات و خطای انسانی بسیار مؤثر است (گروه مؤلفین معاونت فاوا آجا، ۱۴۰۰ : ۷ و ۱۲). گسترش روزافزون فناوری‌های نوظهور فضای سایبر نیز در عرصه‌های متنوع و به‌ویژه حوزه دفاعی، شکل و نحوه جنگ‌ها را به‌طورکلی متحول ساخته است. با توجه به ویژگی‌های سامانه‌های نوین

[1] Distributed Common Ground System

فرماندهی و کنترل سایبر، فناوری اینترنت اشیاء از ویژگی‌های سرعت در تبادل اطلاعات، آگاهی فراگیر از فضای نبرد، فهم برتر از فضای نبرد پشتیبانی نموده و می‌تواند نقش مؤثری در تحقق آن‌ها ایفا نماید و ارتقاء سامانه‌های نوین فرماندهی و کنترل سایبر را موجب شده است. یکی دیگر از استفاده‌های فناوری اینترنت اشیاء، به‌کارگیری آن در صنایع نظامی و به‌منظور ردیابی و نقشه‌برداری است (محمدی و کریمی قهرودی، ۱۳۹۹: ۵). با کار گذاشتن حسگرها در وسایل متحرک نظامی و گراف نمودن آن‌ها در سامانه، کنترل مسیر آن‌ها امکان‌پذیر می‌گردد (شعبانی و همکاران، ۱۳۹۵: ۶).

با استفاده از حسگر سامانه موقعیت جهانی و اینترنت اشیاء، می‌توان برای ردیابی، نظارت و کمک به افراد، به‌ویژه کودکان و بیماران پریشان‌حال استفاده نمود که در این صورت هزینه و تلاش برای ردیابی آن‌ها کاهش می‌یابد که این قابل تعمیم به بخش‌های نظامی نیز است (Priyanka & et al, 2020: 514). از اینترنت اشیاء در سامانه مشاور ناوبری خودرو[1] و برای ناوبری آسان در ترافیک شبکه‌های جاده‌ای نیز استفاده می‌شود. این فناوری، با در نظر گرفتن سامانه موقعیت‌یاب جهانی، تصمیم‌گیری بهتر، صرفه‌جویی در زمان و همچنین انتخاب مسیرهای جایگزین کم ترافیک را فراهم می‌نماید. اینترنت اشیاء زمینه‌ای است که دنیا را رقمی می‌کند و از فن‌های آن در سامانه اطلاعات جغرافیایی[2] نیز استفاده می‌شود. این سامانه ابزاری قدرتمند است که با داده‌های جغرافیایی رقمی سروکار دارد و یک سامانه پردازشی است که توانایی آن را دارد همه انواع داده‌ها را بر اساس مؤلفه‌های مکانی باهم ترکیب کند. وانگ لی کیون[3] (۲۰۱۲) در تحقیق خود از اینترنت اشیاء به‌عنوان مکمل سامانه اطلاعات جغرافیایی استفاده کرده و ماژول سامانه موقعیت‌یابی جهانی و شناسایی فرکانس رادیویی را برای جمع‌آوری سریع داده‌ها و مکان‌یابی ترکیب نمود. نتایج آزمایش نشان داد که با داشتن شناسایی بی‌سیم اینترنت اشیاء و بیان داده‌های مکانی قوی و ظرفیت تجزیه‌وتحلیل سامانه اطلاعات جغرافیایی، پشتیبانی تصمیم‌گیری پیشرفته‌تری را برای مدیریت کیفیت محیطی فراهم می‌نماید. اینترنت اشیاء و سامانه اطلاعات جغرافیایی باهم ترکیب‌شده‌اند تا درک بهتری از داده‌ها و الگوهای جغرافیایی ارائه دهند. این پیوند به نقشه‌برداری اینترنت اشیاء به روشی تعاملی کمک می‌کند و جهان را هوشمندتر می‌نماید (Priya & et al, 2016: 128). بیش از یک دهه هست که مبحث تحرک و سیار بودن رزم‌آرایی در حوزه نظامی توسعه داده‌شده است. برنامه جنگجوی ارتش نت[4] چندین سال زمان صرف توسعه دستگاه‌های اندرویدی برای پیاده‌نظام و با استفاده از سامانه راه‌انداز اندروید نموده است. این دستگاه‌ها به رادیوی تفنگدار با قابلیت اتصال داده متصل می‌شوند و هدفشان اتصال سربازان

[1] Vehicle Navigation Advisor System
[2] GIS: Geographic Information Systems
[3] Wang, Li-Qun
[4] Nett

میدان نبرد به امکانات و برنامه‌هایی همچون نقشه‌های رقمی، ردیابی نیروها، ترجمه زبان‌ها و تشخیص اهداف ارزشمند است (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۶۸ و ۶۹).

**سامانه‌های خودمختار (سامانه‌های تشخیص و جلوگیری، ربات‌های انبوه)**

مفهوم خودمختاری، کلید چشم‌انداز اینترنت اشیاء است که نویدبخش افزایش یکپارچه‌سازی خدمات سامانه‌های هوشمند است که کاهش‌دهنده مداخلات انسانی است (Sifakis, 2018: 2). سامانه‌های خودمختار وسایلی هستند با ظرفیت و آزادی عمل مستقل و بدون دخالت انسان. خودمختاری در امتداد استمرار کنترل از راه دور تا تفسیر داده و تصمیم‌گیری بر اساس مؤلفه‌های برنامه‌ریزی‌شده تعریف می‌شود. (Barkan & et al, 2011: 1). سامانه‌های تشخیص و جلوگیری، فناوری‌های خودمختاری هستند که به هواپیماهای بدون سرنشین (پهپادها) اجازه می‌دهند با خیال راحت در حریم هوایی غیرنظامی وارد شوند و از برخورد با دیگر هواپیماها، ساختمان‌ها، خطوط برق، پرندگان و سایر موانع جلوگیری کنند. اجزای اصلی این سامانه‌ها، عملگرهای حسی (تشخیص) با هدف شناسایی و ردیابی ترافیک اطراف و عملگرهای اجتناب (جلوگیری)، شناسایی زود هنگام درگیری‌های احتمالی و ایجاد مانورهای مناسب است که توسط پهپاد به‌منظور رفع درگیری‌های شناسایی‌شده انجام می‌شود. حسگرهای صوتی، سامانه‌های الکتریکی نوری[۱]، رادار لیزری (لیدار[۲])، حسگرهای مایکروویو فعال[۳]، دوربین‌های معمولی، حرارتی، رادار موج میلی‌متری[۴] و ترانسپاندر و رسپاندر (فرستنده-پاسخ‌دهنده)[۵] نیز در این سامانه‌ها استفاده می‌شود (Di Vito & et al, 2015: 6, 8 & 12)

ربات‌های انبوه نیز شامل گروهی از ربات‌های خودمختار در ابعاد کوچک است که دارای ارتباط، هماهنگی و همکاری بین یکدیگر هستند و در این حالت کار گروهی، عملکرد بهتری نسبت به یک ربات پیچیده منفرد خواهند داشت. در ربات‌های انبوه، کنترل بر اساس تعریف غیرمتمرکز و بین ربات‌های گروه توزیع می‌شود و استحکام سامانه و تحمل خطا را بهبود می‌بخشد. همچنین این ویژگی در اغلب موارد، امکان ظهور رفتارهای جمعی را از تعامل ربات با یکدیگر و با محیط از طریق حسگرها و محرک‌های تجسم‌یافته آن‌ها فراهم می‌نماید (Nedjah & SilvaJuniorba, 2019:1). در ایالت متحده، رباتیک انبوه در دو حوزه کلیدی ارتش و دانشگاه در حال رشد است. اندیشکده مرکز امنیت جدید آمریکا[۶] در سال ۲۰۱۵ گزارشی با عنوان «انبوه آینده، کیفیت و کمیت»[۷] را منتشر کرد و توضیح داد که افزایش آسیب‌پذیری دارایی کشتی‌ها و هواپیماها، ارتش ایالت متحده را بر آن داشته تا بر روی

[1] Electro-Optical Systems
[2] LIDAR: Laser Identification Detection and Ranging
[3] Active Microwave Sensors
[4] MMW Radar: Millimeter Wave Radar
[5] Transponder (Transmitter-Responder)
[6] CNAS: Center for New American Security
[7] The coming swarm: The Quality of Quantity

نوآوری‌های کوچک مانند فناوری‌های رباتیک نوظهور سرمایه‌گذاری کند که می‌توانند به‌عنوان یک گروه بجنگند. علاوه بر این آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی (دارپا)، توسعه پهپادهایی به نام گرملینز[1] را تأیید کرده است (prakash, 2018:3). ویژگی‌های ربات‌های انبوه شامل خودمختاری، مقیاس‌پذیری و استحکام، هماهنگی غیرمتمرکز و انعطاف‌پذیری است. ربات‌های انبوه برای نظارت بر محیط، جستجوی بازماندگان، مکان‌یابی منابع خطرناک مانند نشت مواد شیمیایی، گاز، آلودگی سمی، مواد رادیواکتیویته، نشت لوله و در کشاورزی کاربرد دارند. ربات‌های انبوه می‌توانند منطقه وسیعی را تحت پوشش قرار دهند و در حل مشکلاتی که در سامانه‌های اینترنت اشیاء با آن مواجه می‌شوند، مانند سازگاری مشترک، کنترل توزیع‌شده، خودسازمان‌دهی و مدیریت برنامه‌ریزی منابع مفید هستند (Giandomenico, 2019:1). ریز پرنده‌ها و میکرو پهپادها که دارای هوش مصنوعی بوده و قابلیت حمله خودکار و گروهی دارند، از تجهیزات و قابلیت‌هایی مانند؛ دوربین دید در شب، ضبط صدا، حسگر تشخیص چهره، فشارسنج برای حفظ ارتفاع، گردش نما برای ثبات و کنترل، حمل مواد منفجره، رایانه‌های کوچک آن بورد[2]، سامانه تشخیص و جلوگیری، وای فای به‌منظور مقاصد جاسوسی و عملیات سایبر، آنتن‌های رادیویی خاص جهت کارهای مخابراتی و دریافت پیام و همچنین برای ایجاد تعادل در هنگام پرواز، حسگرهای کوچک فروسرخ و ردیاب، ارسال داده‌های رقمی، حسگرهای راهکنشی[3]، نمونه‌گیری از سلول فرد و تجزیه‌وتحلیل دی‌ان‌ای[4] و مخابره اطلاعات شخص بعد از تطبیق با بانک اطلاعاتی خود و همچنین تزریق تگ میکرو آراف‌آی‌دی برخوردار می‌باشند (گروه مترجمین سازمان تحقیقات و جهاد خودکفایی آجا، ۱۳۹۹، ص ۴۰ و ۴۱).

**جنگ‌افزارها (هدف‌گیری دقیق، سامانه‌های کنترل آتش، سامانه‌های بدون سرنشین)**

ایده کلیدی اینترنت اشیاء این است که سلاح‌ها می‌توانند با اتصال به سامانه واحد، مزیت‌های بیشتری داشته باشند. اینترنت اشیاء می‌تواند تمامی انواع نیروها (زمینی، هوایی، دریایی و پدافند) را به هم متصل نموده و بسترهای سلاح در میدان نبرد را به یک شبکه اطلاعات واحد وصل نماید و یک شبکه یکتا تشکیل دهد که در آن تسهیم (به اشتراک‌گذاری) بلادرنگ اطلاعات، کوتاه شدن زمان اخذ تصمیم و زمان اعلام فرمان‌ها و افزایش بهره‌وری عملیات مشترک را توسعه خواهد داد (بهشتی و همکاران، ۱۳۹۷: ۶۹). با توسعه فناوری اینترنت اشیاء، کاربردهای نظامی آن تنها به حوزه لجستیک محدود نشده و اینترنت اشیاء ارزش ویژه‌ای برای شناسایی نظامی، نظارت و کنترل محیطی و پیرامونی، جنگ‌افزارهای بدون سرنشین و مانند آن به ارمغان می‌آورد. اینترنت اشیاء برای تجهیزات گوناگون و

[1] Gremlins
2 On Board
[3] Tacticy
[4] DNA

گسترده نظامی همانند وسایل نقلیه، سامانه‌های پشتیبانی و حتی سلاح‌های مختلف قابل‌استفاده است (لک، ۱۳۹۹: ۸۲).

نیروی هوایی آمریکا در جدیدترین آزمایش میدانی با متحدان خود برای ساختن سامانه‌های شبیه به اینترنت اشیاء میدان نبرد، هوش مصنوعی، فضای ابری و سایر قابلیت‌های فنی، از فناوری تحت عنوان «زنجیره کشتار»[1] که شامل مراحلی برای شلیک هوشمند است، استفاده نمود. در بیانیه مطبوعاتی نیروی هوایی ایالت متحده به آزمایش‌هایی دیگر در آینده برای ایجاد ارتباط بین اف۳۵بی و کی‌سی۴۶[2] شکاری و مرکز کنترل زمینی با استفاده از استانداردهای تجاری مسیریابی اینترنتی اشاره‌شده است. در این حالت به دلیل ارتباطات تصویری، آنچه را که صدها مایل دورتر در هوا اتفاق می‌افتد، می‌بیند (گروه مؤلفین معاونت فاوا آجا، ۱۴۰۰: ۱۱ و ۸). سامانه‌های تسلیحاتی مستقل ایالات‌متحده همچون فالانکس و سنتورین سی-رام[3] را ربات‌های قاتل می‌نامند، چراکه توانایی هدف گرفتن و حمله کردن به‌صورت خودکار در شرایط درگیری را دارا هستند. این سامانه‌های تسلیحاتی را می‌توان به‌راحتی با حسگرهای متصل مبتنی بر اینترنت اشیاء مدیریت کرده و با هوش مصنوعی به آن‌ها منطق بخشید (گروه نویسندگان مرکز تحقیقات اینترنت اشیاء ایران، ۱۴۰۰). یکی دیگر از کاربردهای اینترنت اشیاء، استفاده در صنایع هوافضا است (محمدی و کریمی قهرودی، ۱۳۹۹: ۵). هواپیماها و وسایل هوایی، موتورهای جت پیشرفته مجهز به حسگرهایی شده‌اند که می‌توانند چندین ترابایت داده را در هر پرواز، به دست آورند. این اطلاعات در ترکیب با داده‌های در حین پرواز، موجب بهبود کارایی موتور و در نتیجه کاهش هزینه‌های سوختی، تشخیص خطاهای کم‌تر یا کوتاه کردن مدت‌زمان لازم برای پرواز می‌شوند (احمدی، ۲۰۱۶: ۹).

در مفهوم جنگ شبکه محور یا نمونه جدیدتر آن یعنی اینترنت اشیاء نظامی، مهمات نیز قابلیت شبکه شدن را خواهند داشت و این امر از طریق اجازه دادن به سلاح‌های هوشمند به‌منظور ردیابی و ره‌گیری اهداف سیار یا هدایت پرواز قابل تحقق و انجام است. یک نمونه اولیه و مقدماتی، موشک حمله زمینی تام‌هاوک[4] یا همان تی‌ال‌ای‌ام[5] است که سلاح برتر نیروی دریایی ایالات‌متحده آمریکا به شمار می‌آید. نوع قالب تی‌ال‌ای‌ام-۴ یک خط ارتباطی ماهواره‌های دوطرفه دارد که اجازه می‌دهد تا بتوان مسیر موشک را به سمت یک هدف جدید هدایت نمود یا این‌که موشک به‌آرامی به سمت یک هدف پیش برود؛ درحالی‌که توسط دوربینی که بر روی آن نصب‌شده است فیلم صحنه نبرد مربوط را به کماندوها ارسال می‌کند. آن‌ها می‌توانند اهداف جدیدی را به آن اختصاص دهند و میزان تخریب ناشی

[1] Kill chains
[2] F-35B & KC-46
[3] C-RAM
[4] Tomahawk
[5] TLAM: Tomahawk Land Attack Missile

از برخوردهای دیگر را ارزیابی نمایند. (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۶۷ و ۶۸). هوشمند سازی سامانه‌ها و به‌کارگیری آن‌ها تحت شبکه‌های پیشرفته، زمینه کاربرد اینترنت اشیاء (نظامی) را با ویژگی‌های خاص آن فراهم نموده است. به‌گونه‌ای 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 تصمیم‌سازی و تصمیم‌گیری خبره، به سهولت اهداف دور از دسترس و پنهان را که تحت تدابیر پدافند غیرعامل مناسبی هم قرار دارند، مورد اصابت قرار می‌دهند (فرج پور، ۱۳۹۹: ۴۶). امروزه توسعه کاربردهای نظامی فناوری اینترنت اشیاء با محوریت ایالت متحده آمریکا بر روی کاربردهای سامانه‌های کنترل آتش متمرکز شده است (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۶۴). سامانه‌های کنترل آتش می‌توانند با کمک شبکه‌های حسگر انتها به انتها[1] و همچنین تحلیل‌های رقمی، پاسخ‌دهی و واکنش‌های کاملاً خودکاری را در قبال تهدیدهای بی‌درنگ انجام دهند و قدرت شلیک را با دقت بالایی مشخص کنند. به‌عنوان‌مثال، سامانه جنگی حفاظت از نیروی دریایی ایالات‌متحده، علاوه بر کنترل و فرمان، امکان دفاع موشکی بالستیک بی‌سابقه‌ای را نیز فراهم آورده است. مهمات نیز می‌توانند به حالت متصل درآمده و بدین ترتیب سلاح‌های هوشمند می‌توانند اهداف سیار و متحرک را ردیابی کرده و یا در حالت پرواز هدایت نمایند. به‌عنوان نمونه مهمی از این قبیل سلاح‌ها، می‌توان به موشک جنگی زمینی تام‌هاوک و گونه‌های مختلف از آن، یعنی سلاح‌های بمب‌افکن دقیق نیروی دریایی ایالات‌متحده برای حمله در محدوده‌های طولانی، متوسط و اهداف راهبردی اشاره کرد. علاوه بر این، ارتش قسمتی از سرمایه خود را صرف پهپادهایی با پایداری طولانی‌مدت کرده است تا اهداف ارزشمندتری را به دام انداخته و در ضمن، کاربردهای چند پهپادی جدیدی را معرفی نماید (پورمکاری و همکاران، ۱۳۹۸: ۱۴۷). سامانه نظارتی نیروی دریایی آمریکا که یک سامانه کنترل آتش یکپارچه برای کشتی‌های سطحی است، امکان ترکیب (عملکردی) کامل با سامانه‌های کنترل آتش خودکارسازی سازی شده را داراست. این سامانه امکان فرماندهی و کنترل را به‌صورت کنترل تجهیزات سلاح‌ها در کشتی‌های جنگی سطحی ایالات‌متحده از توپخانه دریایی و اژدر گرفته تا موشک‌های کروز هدایت‌شونده علیه سلاح‌های ضد موشک فراهم می‌نماید. سامانه راداری ای‌ان/ اسپای[2] می‌تواند مهمات هدایت‌شونده را تشخیص داده، ره‌گیری نموده و هدایت نماید به‌گونه‌ای که در یک‌زمان قادر است تا به‌طور کاملاً خودکار صد هدف را تعقیب و ره‌گیری نماید (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۶۶ و ۶۷). اکثر سامانه‌های بدون سرنشین، خودمختار (خودکار[3]) نیستند و به‌صورت کنترل از راه دور و توسط کاربر انسانی هدایت و کنترل می‌شوند که خودکارسازی را می‌توان هدف

[1] End-to-End
[2] AN/SPY
[3] Automatic

نهایی اینترنت اشیاء نامید؛ بدین معنی که در مفهوم اینترنت اشیاء، دستگاه‌های هوشمند مختلف به‌صورت خودکار و بدون دخالت انسان با یکدیگر ارتباط برقرار نموده و فعالیت می‌نمایند. کاربرهای نهایی اینترنت اشیاء از حسگرها، آراف‌آی‌دی‌ها و تحلیل‌های رقمی استفاده می‌کنند تا پاسخ‌های خودکارسازی شده و خودکار تولید نمایند. اتوماسیون به‌طور معناداری کشندگی و بقای جنگ‌افزارها و همچنین کارایی عملیات نظامی را افزایش داده و در مقابل تعداد نفرات موردنیاز برای اتمام یک مأموریت و احتمال بروز خطای انسانی را کاهش داده و زمان واکنش را بهبود می‌بخشد (بهشتی آتشگاه و همکاران، ۱۳۹۷: ۷۱). با توسعه فناوری‌های مبتنی بر اینترنت و همچنین نیاز به کنترل تجهیزات مختلف از راه دور، کنترل از راه دور ربات (تله رباتیک) از طریق فناوری اینترنت اشیاء با بهره‌گیری از بستر اینترنت در ادوات نظامی کشورهای پیشرفته‌ای همچون آمریکا، انگلیس، آلمان، فرانسه و ... به‌سرعت رشد و گسترش‌یافته است (شعبانی و همکاران، ۱۳۹۵: ۲). وسایل بدون سرنشین همچون پهپادها، وسایل نقلیه زمینی بدون سرنشین و زیردریایی‌های بدون سرنشین، به‌طور عمده به‌منظور مراقبت مورد استفاده قرار می‌گیرند. درهرحال، نحوه تکامل این وسایل در جهت پوشش تمام حوزه‌های نظامی است. در جریان عملیات نظامی در عراق، حدود شانزده پهپاد (پری دیتور و گلوبال هاک) در عملیات حضور داشتند که تمام آن‌ها توسط ارتباطات ماهواره‌ای از مراکز فرماندهی در آمریکا و از راه دور پایش می‌شدند. هر وسیله نقلیه بدون سرنشین به مقدار قابل‌توجهی پهنای باند برای پایش و برای ارسال پیام‌های شناسایی نیاز دارد، همچنین وسایل نقلیه بدون سرنشین می‌توانند به‌عنوان گره‌هایی برای تقویت پیام‌های مخابراتی در سراسر شبکه جنگ شبکه محور به کار روند (پور قهرمانی و همکاران، ۱۳۹۵: ۴۴۴)

با توجه به هزینه‌های سنگین مالی و انسانی جنگنده‌ها، وجود نقاط کور عملکردی و محدودیت‌های جغرافیایی سامانه‌های جنگ الکترونیک استقراری، اهمیت تأثیرگذاری حوزه‌های حمله الکترونیکی، محافظت الکترونیکی و پشتیبانی الکترونیکی، امروزه دکترین دفاعی و تهاجمی کشورها به سمت تلفیق پهپاد و جنگ الکترونیک، معطوف شده است. پهپادهای شناسایی و جنگ الکترونیک در ابعاد مینی پهپاد تا پهپاد غول‌پیکر باقابلیت حمل محموله‌های شناسایی اپتیکی، دید در شب، شناسایی سیگنال‌های راداری و مخابراتی، عکس‌برداری راداری، شناسایی راداری و ارسال تصویر زنده، اخلال مخابراتی و راداری نویزی و فریب، ارتباطات ماهواره‌ای، پشتیبانی شناسایی و عملیاتی ارزنده‌ای را برای نیروهای اطلاعاتی و عملیاتی (رزمی) فراهم می‌آورند. در زمینه پهپادهای رزمی و انتحاری نیز تجهیز آن‌ها به انواع سلاح‌های رزمی ازجمله راکت‌ها، موشک‌ها، بمب‌ها، رادارهای کنترل آتش موشک و اخلال‌گرها، جایگزین مناسبی برای جنگنده‌ها را فراهم آورده است (شریفی و لشگریان، ۱۳۹۶: ۱) . پهپادها در جنگ سایبر نیز با موفقیت استفاده‌شده‌اند. وزارت دفاع آمریکا، برنامه‌هایی برای کنترل تعداد زیادی از وسایل نقلیه بدون سرنشین و پهپاد از طریق شبکه‌های متصل و اینترنت اشیاء دارد. برنامه‌های نرم‌افزاری برای گوشی‌های هوشمند و تبلت‌ها که به سربازان اجازه می‌دهد نه‌تنها پهپادها را

خلبانی (هدایت) کنند، بلکه اطلاعات، ویدئوهای شناسایی و تصاویر را از ایستگاه‌های کنترل زمینی[1] یا مستقیماً از پهپادها به اشتراک بگذارند و دریافت کنند (Zhu, L. & et al, 2020:527).

ربات‌های زمینی نیز به این علت که محیط‌های زمینی برای عملیات ناوبری خودکار، خیلی بغرنج و پیچیده‌اند، در مراحل توسعه و گسترش هستند. عمده‌ترین موانع برای ربات‌های زمینی، عبور از سرزمین‌های صخره‌ای، برفی، بیابانی دارای پوشش گیاهی و یا بدون پوشش گیاهی است. قابلیت‌های جدید می‌تواند شامل گشت‌های خیابانی، شناسایی، تیراندازی به دشمن از فاصله دور، امنیت محل و بازرسی وسایل نقلیه مانند پست‌های دیده‌بانی و نگهبانی باشد. ربات‌ها قادر به حرکت از میان برف، ماسه و حتی حرکت در زیر آب تا عمق صد پایی هستند و می‌توانند همانند اعضای یک گروه و یا بعضاً به‌صورت خودمختار کار کنند. ربات‌ها قادر به کشف عوامل شیمیایی روی وسایل و تجهیزات می‌باشند. در آینده، فناوری رباتیک می‌تواند خودش را از طبقه‌بندی تقویت‌کننده نیرو به یک نیروی تهاجمی مبدل سازد. ربات‌ها به‌طور چشم‌گیری برای خدماتی مانند سامانه دفاع پیرامونی، اطلاعات، شناسایی و یا حتی به‌عنوان سامانه تسلیحاتی مورداستفاده واقع می‌شوند. کنار هم گذاشتن هوش مصنوعی و فناوری رباتیک ازنظر نظامی، آینده کاربرد ربات‌ها را هیجان‌انگیزتر خواهد ساخت (فلسفی و صادقی، ۱۳۹۸: ٤). نمونه‌ای دیگر از سامانه‌های بدون سرنشین مجهز به فناوری اینترنت اشیاء که شباهت زیادی به اژدرها دارند، زیردریایی‌های هوشمند خودرانی[2] هستند که با استفاده از فناوری چاپ سه‌بعدی توسط شرکت فناوری دایو[3] ساخته شده‌اند. این زیردریایی‌ها مجهز به دوربین‌ها و همچنین طیف متنوعی از حسگرهای پیشرفته و دقیق هستند. (گروه مترجمین جهاد و خودکفایی آجا، ۱۴۰۰: ۴۲). خودروهای رباتیک زرهی[4] ارتش آمریکا نیز که ازجمله‌ی آن‌ها تانک بدون سرنشین است، دارای قابلیت‌هایی مانند؛ ایجاد درگیری مؤثر با دشمن، اختلال در سامانه‌های الکترونیکی و ارتباطی دشمن، ایجاد پرده دود در مقابل پیشروی نیروهای خودی، شکار پهپادهای دشمن، علامت‌گذاری میدان مین و انجام عملیات در محل‌های آلوده میکروبی شیمیایی است (نصیری، ۱۳۹۹: ٤٤).

**کارکنان (رزمندگان و فرماندهان)**

پیدایش فناوری اینترنت اشیاء که انجام اموری نظیر هدایت و نظارت عملیاتی را در شرایط حساس و بحرانی به‌آسانی امکان‌پذیر ساخته است، مرهون پیشرفت‌هایی است که در این عرصه صورت گرفته است. جنگ‌های امروزی ما را به‌سوی دوران جدیدی از تحولات سوق می‌دهند که ازلحاظ دامنه و هم ازلحاظ ابعاد بی‌سابقه هستند. این دوران جدید باعث تغییر و تحول در ساختار کلی جنگ‌ها با تکیه‌بر

[1] GCS: Ground Control Stations
[2] AUV: Autonomous Underwater Vehicles
[3] Dive Technologies
[4] RCV: Robotic Combat Vehicle

فناوری‌های جدید برای کم‌ترین تلفات و استفاده از دقیق‌ترین و هوشمندترین ابزار در آینده گشته است. با پیشرفت فناوری، عملیات نظامی در آینده غیرخطی و هم‌زمان است و صحنه نبرد ۳۶۰ درجه خواهد بود و جنگ به فضا نیز گسترش می‌یابد. چنین جنگ‌هایی به کارکنانی نیاز دارد که بتوانند با ابزارهای پیشرفته در آن‌ها شرکت کنند (محمدی و کریمی قهرودی، ۱۳۹۹: ۷). امروزه نیروهای نظامی، نیازمند رزمندگان متفکری هستند که بتوانند در محیط جنگ رقمی مبارزه نمایند. نیروهای نظامی متوازن و معتبری که به‌وسیله راهبردها و افکار عملیاتی صحیح، هدایت و به‌وسیله سلاح‌هایی با فناوری بالا تجهیز و آماده جنگ شده و به‌وسیله شایستگی‌های حرفه‌ای بجنگند، این‌ها جهت‌های توسعه‌ی نیروهای نظامی آینده است (مهدی نژاد نوری و همکاران، ۱۳۹۹: ۲۳۷).

امروزه در یک میدان نبرد، حسگرهای فراوانی روی تجهیزات رزمندگان، خودروهای زرهی، سلاح‌ها و سایر ادوات می‌تواند نصب شود و به‌طور مداوم فرمانده عملیات یا گروه پشتیبانی را از وضعیت فعلی افراد و موقعیت آن‌ها آگاه سازد. می‌تواند گروه پزشکی را از سلامت رزمندگان آگاه سازد و یا گروه تأمین را آگاه نگه دارد تا به‌موقع و در زمان و مکان مناسب عملیات تأمین را صورت دهد (مینایی بیدگلی و میرزایی قاضیانی، ۱۳۹۹: ۱۵). حسگرهای پوشیدنی، هنگامی‌که در مقیاس گروهی به کار گرفته شوند، اطلاعاتی را فراهم می‌آورند که این اطلاعات می‌توانند از سی۴آی‌اس‌آر پشتیبانی کنند (پور مکاری و همکاران، ۱۳۹۸: ۱۴۹). همراه با ظهور الگوی اینترنت اشیاء و فناوری‌های توانمندی مانند واقعیت افزوده، سامانه‌های فیزیکی سایبر، هوش مصنوعی، بلاک چین یا محاسبات لبه‌ای، همگرایی سریع نساجی و الکترونیک را در لباس رزمندگان شاهد هستیم که امکان ادغام یکپارچه و عظیم حسگرها را در منسوجات فراهم می‌کند. پارچه‌های هوشمندی که می‌توانند با گوشی‌های هوشمند ارتباط برقرار کنند و باوجود آن‌ها اطلاعات حیات‌سنجی مانند ضربان قلب، دما، تنفس، استرس، حرکت، شتاب یا حتی سطوح هورمونی بدن دریافت گردد (Fernández-Caramés & Fraga-Lamas, 2018:1).

از اینترنت اشیاء می‌توان در برخی از آموزش‌ها و فعالیت‌های شبیه‌سازی رزمندگان استفاده نمود، مانند کاربرد دریافت‌کننده‌های پوشیدنی برای شبیه‌سازی میدان جنگ. در نمونه‌ای از آموزش، می‌توان از دوربین‌ها و حسگرهای حرکتی و صوتی جهت ردیابی نیرو در حین عملیات آموزشی استفاده نمود. سامانه، داده‌ها را به سمت دستگاه‌های سیار و آموزش‌دهندگان ارسال می‌کند و آن‌ها با توجه به این داده‌ها، می‌توانند راهنمایی‌هایی را بلادرنگ انجام دهند و آمارها و ویدئوهای ویرایش شده‌ای را جهت بازبینی پس از آموزش به وجود بیاورند. نمونه دیگر، راه‌حل‌های آموزشی مکعب سامانه‌های چندگانه یکپارچه درگیری لیزری است که با استفاده از لیزرها و نمایش‌های بصری، میدان جنگ را جهت رزمندگان و فرماندهان شبیه‌سازی می‌نمایند. آن‌ها از ابزارهای ارتباطی، مدل‌سازی رایانه‌ی و یادگیری مبتنی بر علوم عصبی، برای ارائه یک تجربه‌آموزشی در زمان واقعی، استفاده می‌کنند. (پور مکاری و همکاران، ۱۳۹۸: ۱۵۰). در سطح رزمندگان، از ردیابی به‌منظور پیگیری رهیافت فعالی به سمت رفع نیازهای عملیاتی استفاده می‌شود. موارد لازم برای رزمندگان (نظیر آب، غذا، باتری یا فشنگ) می‌توانند

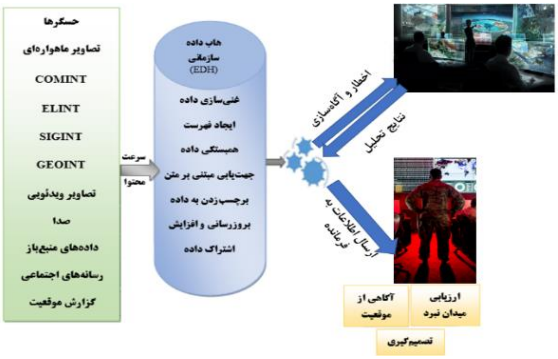
تحت نظارت قرارگرفته شوند و در صورت نیاز به تأمین مجدد این موارد، هشدارهایی به سمت بخش‌های مربوط ارسال شود (احمدی و همکاران، ۲۰۱۶: ۱۰).

مفهوم رزمنده با استفاده از شبکه اطلاعاتی در طول برنامه نت وریر[1] ظاهر شد که استفاده از دستگاه‌های اندرویدی مداوم را برای ارتش ایالات‌متحده توسعه داد. این دستگاه‌ها معادل نظامی تلفن‌های همراه هوشمند سامسونگ گلکسی نوت دو هستند که ازلحاظ تجاری در دسترس هستند و رزمندگان را قادر می‌سازد تا اطلاعات دقیق‌تری از طریق برنامه‌های نظامی مانند ردیابی نیروی آبی (خودی)، نقشه‌های سه‌بعدی و برنامه‌های هدف به دست آورند (Bognar,2018, P: 383). اینترنت اشیاء فرصت‌های جدیدی را ایجاد کرده است و امکان توسعه انواع خدمات در حوزه‌های متنوع را فراهم ساخته است که یکی از کاربردهای آن در شبکه‌های اجتماعی است که می‌تواند مورداستفاده رزمندگان سایبر قرار بگیرد. سامانه‌های فرماندهی و کنترل، ابزاری مناسب برای کمک به فرماندهان در تصمیم‌گیری و ابلاغ دستورها، بررسی وضعیت و گزارش‌گیری هستند. خبرگان نظامی (فرماندهان) همواره درصدد بهره‌گیری از روزآمدترین و کارآمدترین شبکه‌های ارتباطی، سامانه‌ها و حسگرهای جمع‌آوری اطلاعات و سامانه‌های پردازشی و اطلاعاتی مرتبط با فناوری‌های نوظهور نظیر اینترنت اشیاء می‌باشند. پشتیبانی تصمیم‌گیری فرماندهی و کنترل به‌سرعت در اختیار داشتن اطلاعات مناسب، در مکان مناسب، برای تصمیم‌گیری درست وابسته است و فناوری اینترنت اشیاء می‌تواند در جمع‌آوری اطلاعات اولیه از طریق سامانه‌ها و حسگرهای محیطی از محیط عملیات کمک قابل‌توجهی نماید (محمدی و کریمی قهرودی، ۱۳۹۹: ۵ و۶). یکی از بزرگ‌ترین شکاف‌های موجود داده‌های سامانه دفاع و امنیت ملی، تجزیه‌وتحلیل رقمی است که شامل جمع‌آوری داده‌ها، تحول، ارزیابی و به اشتراک‌گذاری آن‌ها است. بیشتر اطلاعات حجیم جمع‌آوری‌شده توسط حسگرها هرگز استفاده نمی‌شوند و اطلاعات مورد دریافتی در سناریوهای شرایط بحرانی، منجر به تأخیر فراوانی خواهد شد. این تأخیرها می‌تواند باعث شکست یا قصور در انجام مأموریت‌ها و یا تصمیم‌گیری اجباری بدون حقایق مربوط شود. افسران این‌گونه سفارش‌ها را بر روی کاغذ امضاء کرده و شماره‌های زنجیره را به‌صورت دستی وارد رایانه می‌نمایند. این رویکرد مناسب نیست و خطرات ناشی از خطاهای انسانی را به وجود می‌آورد. بخش اعظم ارزش اینترنت اشیاء، به خودکارسازی تولید بستگی دارد که به سامانه‌ها اجازه می‌دهد سریع‌تر و با دقت بیشتری نسبت به انسان‌ها واکنش نشان دهند. تعداد کمی از سامانه‌های نظامی واکنش‌های کاملاً خودکار خود را دارند. به‌عنوان‌مثال، اغلب هواپیماهای بدون سرنشین موجود، مستقل نیستند و توسط کاربران از راه دور کنترل می‌شوند (پور مکاری و همکاران، ۱۳۹۸: ۱۵۲). با 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 (بهشتی آتشگاه و همکاران، ۱۳۹۷،

[1] Nett Warrior

۶۴). فرماندهان نظامی از دامنهٔ وسیعی از اطلاعات تهیه‌شده توسط حسگرها و دوربین‌های نصب‌شده در زمین و خودروهای باسرنشین یا بدون سرنشین یا سربازان، استفاده می‌کنند. این دستگاه‌ها و واسطه‌ها، به بررسی ناحیهٔ عملیاتی پرداخته و داده‌ها را به یک پایگاه، منتقل می‌کنند. برخی از این داده‌ها ممکن است در مرکز فرماندهی تشدید شده و با داده‌های مربوط به منابع دیگر ترکیب شوند (احمدی و همکاران، ۲۰۱۶: ۷).

در شکل (۴) کاربرد اینترنت اشیاء مبتنی بر سامانه جمع‌آوری اطلاعات موردنیاز فرمانده نشان داده‌شده است. اطلاعات از حسگرها، ماهواره، سامانه‌های جنگ الکترونیک، الینت، کامینت، سیگینت، رسانه‌های اجتماعی و سایر منابع به‌منظور غنی‌سازی، کشف همبستگی، اشتراک و به‌روزرسانی در یک هاب داده سازمانی[1] جمع‌آوری می‌شود. این اطلاعات پس از تحلیل‌های پیشرفته و بلادرنگ برای ایجاد اخطار، آگاه‌سازی و یا ارزیابی میدان نبرد مورداستفاده قرار می‌گیرند. فناوری اینترنت اشیاء در فرایند جمع‌آوری اطلاعات اشاره‌شده در این قسمت می‌تواند نقش مهمی را ایفا نماید. (محمدی و کریمی قهرودی، ۱۳۹۹: ۹)




**شکل (۴) کاربرد اینترنت اشیاء مبتنی بر سامانه جمع‌آوری اطلاعات موردنیاز فرمانده**

ارتش آمریکا با استفاده از تلفن‌های هوشمند تجاری، نیروهای خود را مجهز کرده است. این کاربرد، در پی این است که ارتش بتواند با استفاده از فناوری اینترنت اشیاء، کارایی و مؤثر بودن خود را در جنگ‌های آینده افزایش دهد (شعبانی و همکاران، ۱۳۹۵: ۷). در بخش الزامات و خدمات کاربردی برای فرماندهان با استفاده از تلفن‌های همراه هوشمند (به‌عنوان یکی از تجهیزات کاربردی در فناوری اینترنت اشیاء) می‌توان به خدماتی شامل گفتگو، صوت، آگاهی وضعیتی، رایانامه، ویدئو، چاپ، آگاهی وضعیت جغرافیایی، اشتراک‌گذاری پوشه‌ها، خدمات پیام‌رسان سازمانی، لیست آدرس جهانی، صفحات وب و ترجمه زبان اشاره نمود (Fraga Lamas & et al, 2016:14). صحنه‌های عملیات اخیر، شاهد

[1] Enterprise Data Hub

پذیرش سریع و استفاده وسیع از اتاق‌های چت و سامانه‌های پیام‌رسان در شبکه‌های فرماندهی و کنترل بوده‌اند. خدمات پیام‌رسان آنی و چت، اگرچه در اصل برای مصارف تجاری ایجاد شد، اما با استفاده از پروتکل‌هایی به‌سادگی در شبکه‌های نظامی منطبق شدند. این چت‌ها اغلب حالت محرمانه انجام می‌شوند و دارای مزیت‌هایی می‌باشند که می‌توانند میزان سرعت ارتباطات بین مشارکت‌کنندگان در شبکه را افزایش دهند برخلاف پست‌های الکترونیکی که کاربران، پیام‌ها را مشاهده کرده و در مقابل به آن‌ها پاسخ خواهند داد (کیخسروی، ۱۳۹۹: ۱۰۳).

**چالش‌های به‌کارگیری فناوری اینترنت اشیاء**

مانند هر فناوری نوظهوری که تا زمان تکمیل شدن با مشکلات و چالش‌های مختلفی روبرو است، اینترنت اشیاء نیز به‌خصوص در زمینه امنیت و حریم خصوصی از این قاعده مستثنا نیست. (کرامتی مقدم و همکاران، ۱۴۰۰: ۴۵). در نظرسنجی که از ۱۷۰ شرکت پیشرو اینترنت اشیاء صورت گرفته است، ۸۵ درصد گفته‌اند که نگرانی‌های امنیتی همچنان مانع بزرگی برای پذیرش اینترنت اشیاء است. حملات سایبر اینترنت اشیاء در سال ۲۰۲۱ نسبت به سال قبل، بیش از دو برابر شده است. آسیب‌پذیری‌ها در دستگاه‌های اینترنت اشیاء به مجرمان سایبر این امکان را می‌دهد تا به داده‌های حساس دسترسی پیدا کنند و حملات بیشتری را علیه سایر سامانه‌ها متصل انجام دهند. (گروه مؤلفین معاونت فاوا آجا، ۱۴۰۰: ۱۸). مسئله امنیت در شبکه اینترنت اشیاء آن‌قدر حساس و بحرانی است که یکی از عوامل اجرایی نشدن کامل این شبکه‌ها در سال‌های گذشته محسوب می‌شود (شعبانی و همکاران، ۱۳۹۵: ۱۰). اینترنت اشیاء ترکیبی از دنیای واقعی و مجازی را در هر کجا و در هر زمان ممکن می‌سازد که بدین سبب توجه هکرها را مجذوب خود می‌کند؛ زیرا ترک دستگاه‌ها بدون دخالت انسان برای مدت طولانی می‌تواند منجر به سرقت شود و اینترنت اشیاء موارد بسیاری از این قبیل را در برمی‌گیرد (کرامتی مقدم و همکاران، ۱۴۰۰: ۴۹). در سال ۲۰۱۹، اتحادیه فیدو[1] نیز یک کارگروه را تعیین نمود تا به استانداردهای امنیتی اینترنت اشیاء در فرآیندهای معمولی و روزمره مانند حمل‌ونقل، دستگاه‌های دارای رمز عبور پیش‌فرض معتبر اختصاص دهند. این کارگروه متشکل از اعضای شرکت‌های آمازون، گوگل، اینتل، مایکروسافت، کولکام و دیگران است (گروه مؤلفین معاونت فاوا آجا، ۱۴۰۰: ۱۸). هرچند اینترنت اشیاء با چالش‌های زیادی مانند استانداردسازی، مقیاس‌پذیری، قابلیت همکاری و امنیت نیز روبرو است و استقرار آن به زمان نیاز دارد، ولیکن استفاده از این فناوری در بعضی مناطق به ازای هر دلار هزینه شده، بازدهی بالا و پس‌انداز قابل‌توجه هزینه را به دنبال خواهد داشت (Fraga-Lamas &et al, 2016:35).

[1] FIDO

## پیشینه‌های پژوهش

بهشتی آتشگاه و همکاران (۱۳۹۷) مفاهیم و چالش‌های امنیتی اینترنت اشیاء نظامی با محوریت مکانیسم امآی‌اوتی ایالات‌متحده آمریکا پرداخته و نتایج این تحقیق نشان می‌دهد که اینترنت اشیاء توسعه حوزه نظامی را به‌طور عمده‌ای پیش خواهد برد و به نظر می‌رسد که به‌زودی شاهد شبکه‌های اینترنت اشیاء نظامی باشیم که در آن نقش انسان کم‌رنگ‌تر از قبل خواهد شد. اینترنت اشیاء نظامی با محوریت ایالات‌متحده آمریکا، شامل سی۴آی‌اس‌آر، سامانه‌های کنترل آتش، لجستیک، آموزش، شبیه‌سازی و تحرک است و معماری آن نیز شامل پنج لایه سنجش، دسترسی، شبکه، سرویس و کاربرد است. پورمکاری (۱۳۹۸) در تحقیق خود به کاربردهای فناوری اینترنت اشیاء با تأکید بر مأموریت نیروی هوایی ارتش جمهوری اسلامی ایران پرداخته است و کاربردهای آن را شامل استفاده در سامانه سی۴آی‌اس‌آر، سامانه‌های کنترل آتش (شلیک)، آمادها، نظارت و مدیریت ناوگان، سنجش شخصی، مراقبت بهداشتی سربازان و آموزش نیروی اجرایی، مدیریت انرژی، نظارت، امکانات استقرار، سامانه مدیریت و برنامه‌ریزی بیان نموده است.

محمدی و کریمی قهرودی (۱۳۹۹) به بررسی چگونگی توسعه سامانه‌های فرماندهی و کنترل سایبر در جمهوری اسلامی ایران با فناوری اینترنت اشیاء پرداخته‌اند و نتایج این تحقیق حاکی از آن است که پشتیبانی تصمیم‌گیری فرماندهی و کنترل به‌سرعت در اختیار داشتن اطلاعات مناسب، در مکان مناسب، برای تصمیم‌گیری درست وابسته است و فناوری اینترنت اشیاء می‌تواند در جمع‌آوری اطلاعات اولیه از طریق سامانه‌ها و حسگرهای محیطی از محیط عملیات کمک قابل‌توجهی نماید. با توجه به ویژگی‌های سامانه‌های نوین فرماندهی و کنترل سایبر که به‌صورت ذاتی هوشمند هستند، می‌توان نتیجه‌گیری کرد که فناوری اینترنت اشیاء از ویژگی‌های سرعت در تبادل اطلاعات، آگاهی فراگیر از فضای نبرد، فهم برتر از فضای نبرد، استفاده وسیع از فناوری اطلاعات و ارتباطات، سامانه‌های نوین فرماندهی و کنترل سایبر پشتیبانی نموده و می‌تواند نقش مؤثری در تحقق آن‌ها ایفا نماید. تحقیق لطفی (۱۴۰۰) نیز باهدف تبیین چگونگی ارتقاء امنیت یگان‌های آجا با بهره‌گیری از فناوری اینترنت اشیاء در بعدهای قابلیت کنترل از راه دور، قابلیت ثبت رویدادها، قابلیت هوشمندی و همچنین قابلیت رصد و ارزیابی صورت گرفته است. نتایج تحقیق انجام‌شده نشان می‌دهد، در صورت برخورد فعالانه آجا به‌جای اتخاذ رویکردی منفعل در رابطه با فناوری‌های به‌روز، می‌تواند نسبت به ایجاد دیدگاهی صحیح در ارکان تصمیم‌گیر آجا و سازمان‌های تابعه ایجاد نموده و قبل از ناچار شدن آجا به استفاده از فناوری‌های معرفی‌شده جدید، سازوکار استفاده بهینه و به‌دوراز هرگونه دغدغه در راستای مأموریت‌های آجا ایجاد نمود.

بوگنار (۲۰۱۸) در تحقیقی با عنوان امکانات و چالش‌های امنیتی استفاده از اینترنت اشیاء برای اهداف نظامی، به اهمیت کاربرد فناوری اینترنت اشیاء در نیروهای دفاعی مجارستان به‌عنوان عضوی از ناتو اشاره‌کرده است که شامل مشارکت در برنامه انرژی هوشمند ناتو و ایجاد سد مرزی هوشمند (با

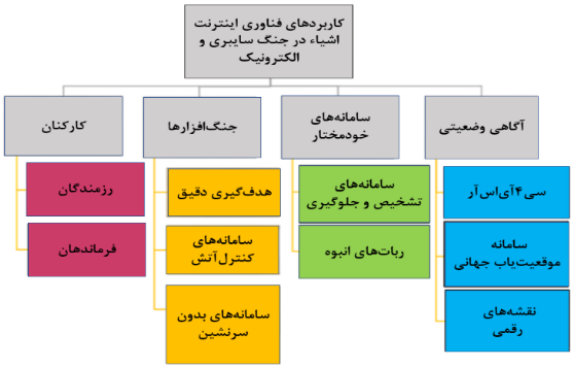
استفاده از حسگرها) در مرز مجارستان و صربستان جهت کنترل مهاجرت غیرقانونی و یا استفاده از سامانه تعاملی لیزر یکپارچه چندگانه[1] جهت آموزش نظامی است. در تحقیق گاتارانه و راسکار (۲۰۱۹) با عنوان شیوه‌های اینترنت اشیاء در کاربردهای نظامی در مورد کاربردهای مختلفی که باید برای محیط نظامی بر اساس اینترنت اشیاء اجرا شود، بحث شده است. این کاربردها شامل سلامتی و ایمنی جنگجویان، شناسایی و از بین بردن دشمن، پشتیبانی لجستیکی، تجهیزات، مهمات، ارتباطات بین دستگاه‌ها در میدان جنگ و برنامه‌های شهر هوشمند برای مواجه با بلایا است.

## چارچوب مفهومی

در این پژوهش، محققین در پی بررسی کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک بوده‌اند، بنابراین در این پژوهش که از نوع تابع‌محور بوده یک متغیر تابع و چند متغیر مستقل جزء در نظر گرفته شده است که شامل:

**متغیر وابسته (تابع):** کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک

**متغیرهای مستقل جزء:** آگاهی وضعیتی، سامانه‌های خودمختار، جنگ-افزارها و کارکنان




**نمودار (۱) چهارچوب مفهومی پژوهش**

## روش‌شناسی پژوهش

### نوع و روش اجرای پژوهش

با توجه به اینکه هدف از این پژوهش بررسی تبیین کاربردهای فناوری اینترنت اشیاء در بعدهای آگاهی وضعیتی، سامانه‌های خودمختار، جنگ‌افزارها و کارکنان جنگ سایبر و الکترونیک و یافتن پاسخی برای سؤالات مطرح‌شده بوده است به این صورت که نتایج آن مورداستفاده سیاست‌گذاران حوزه جنگ سایبر و الکترونیک قرار گیرد و سبب ارتقاء عملکرد آن‌ها گردد، بنابراین ازنظر نوع تحقیق کاربردی و توسعه‌ای بوده است. از طرفی در این پژوهش، محقق به جمع‌آوری اطلاعات واقعی و مفصل از پدیده‌ها جهت تبیین موضوع و تشریح کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک پرداخته

[1] MILES: The Multiple Integrated Laser Engagement System

است و سعی شده تا این کاربردها را آن‌گونه که هست با تمرکز به زمان حال (وضعیت فعلی) و با در نظر گرفتن رویدادها و آثار گذشته که به شرایط موجود مربوط می‌شوند، مورد بررسی، توصیف و تفسیر قرار داده، بنابراین روش تحقیق از نوع توصیفی و موردی-زمینه‌ای است. همچنین محقق در این پژوهش، با استفاده از ادبیات نظری و مصاحبه با خبرگان و متخصصان مربوط، اطلاعات و داده‌های موردنیاز را با ابزارهای اسناد و مدارک، مصاحبه و پرسش‌نامه جمع‌آوری نموده و سپس بر اساس دیدگاه و نگرش جامعه نمونه، نتایج پرسش‌نامه را تحلیل کمی نموده و درنهایت با روش تحلیل آمیخته به نتیجه‌گیری و ارائه کاربردهای مناسب دست یافته است. جامعه آماری در این تحقیق شامل کلیه کارکنان پایور دارای مدارک تحصیلی کارشناسی تا دکتری در رشته‌های مرتبط با الکترونیک (متخصص در فناوری اینترنت اشیاء)، رایانه (متخصص در جنگ سایبر)، مخابرات و جنگال (متخصص در حوزه جنگ الکترونیک) و در محدوده درجات افسر ارشدی به بالا بوده‌اند. دلیل توجیهی گزینش این گروه از طبقات شغلی بدین لحاظ بوده که افراد آن به جهت موقعیت شغلی (سابقه و تجربه) از ویژگی‌ها و خصوصیات لازم در این زمینه برخوردار بوده و با کاربردهای فناوری اینترنت اشیاء در حوزه جنگ سایبر و الکترونیک آشنایی داشته‌اند. به همین منظور تنگناها، نارسایی‌ها و مشکلات موجود در رابطه با موضوع تحقیق را به‌خوبی لمس نموده‌اند. ازاین‌رو جامعه آماری پژوهش از نوع جامعه خبرگانی و محدود و تعداد آنان با اعمال ضریبی، ۱۰۰ نفر بوده است. با توجه به اینکه تعداد افراد جامعه موردمطالعه (با در نظر گرفتن ضریب)، ۱۰۰ نفر در نظر گرفته‌شده است، مطالعه به‌صورت تمام شمار انجام‌شده، حجم نمونه بر جامعه آماری منطبق است و تمامی افراد جامعه موردمطالعه قرارگرفته‌اند. پژوهشگر در این پژوهش از سه ابزار مصاحبه، مطالعه اسناد و مدارک و توزیع پرسش‌نامه استفاده نموده است. از اسناد و مدارک موجود در سطح ارتش جمهوری اسلامی ایران و خارج از آن به‌منظور توسعه ابعاد نظری و شناسایی هر چه بیشتر مؤلفه‌ها و شاخص‌ها استفاده و از سؤالات مصاحبه به‌منظور شناخت عمیق‌تر متغیرهای موردبررسی از طریق جمع‌آوری نظرات خبرگان و نیز از پرسش‌نامه تهیه‌شده جهت تعیین مقدار کمی شاخص‌ها استفاده‌شده است. محقق در ابتدا با استفاده از روش‌های آمار توصیفی از قبیل شمارش فراوانی، تعیین درصدها، محاسبه میانگین، انحراف معیار، واریانس و همچنین رتبه‌بندی ابعاد، مؤلفه‌ها و شاخص‌ها با استفاده از نمره میانگین در نرم‌افزار اس‌پی‌اس‌اس[1] اقدام و سپس با استفاده از روش تحلیل کیفی و محتوایی، اطلاعات نظری جمع‌آوری‌شده در ادبیات نظری و نظرات خبرگان برای دستیابی به اهداف پژوهش تحلیل گردیده است.

به‌منظور روایی مصاحبه در ابتدا یک نمونه از سؤالات آماده‌شده، به گروهی از صاحب‌نظران سطح ارتش که در زمینه‌های الکترونیک، سایبر، مخابرات و جنگال متخصص و آشنا به فناوری اینترنت اشیاء بوده‌اند، ارائه و نظرات آنان خواسته‌شده و سپس نظرات مشترک ثبت و نظرات متناقض مجدداً به گروه

[1] SPSS

دیگری از متخصصان و صاحب‌نظران ارائه گردید. پاسخ مشترک آنان نیز ثبت و اشتراکات ثبت‌شده، پایه سؤالات صاحب‌نظران تشکیل شد. ضمن اینکه سؤال‌های مصاحبه به تأیید استادان راهنما و مشاور رسیده است. به‌منظور افزایش سطح پایایی سؤالات مصاحبه تلاش گردیده است ساختار و نگارش سؤالات به نحوی تنظیم گردد که حداقل ابهام را در ذهن پاسخ‌دهنده ایجاد نماید و پژوهشگر را به اهداف پژوهش برساند. انتخاب صاحب‌نظران نیز از میان متخصصان خبره و دارای تجربه در زمینه‌های الکترونیک، سایبر، مخابرات و جنگال متخصص و آشنا به فناوری اینترنت اشیاء انتخاب گردیده‌اند. همچنین برای بالا بردن پایایی پاسخ‌های مصاحبه، سؤالات در زمانی دیگر با تعدادی از صاحب‌نظران مطرح گردیده است و با اخذ پاسخ‌هایی نسبتاً مشابه در خصوص موضوع تحقیق، پایایی مصاحبه حاصل‌شده است. برای اطمینان از روایی اسناد و مدارک از کتابخانه‌ها، مراکز تحقیقاتی و کلیه کتب و مقالات معتبری که در خصوص موضوع تحقیق، تدوین گردیده است، استفاده‌شده است. در این راستا تلاش شده است از اسناد و مدارکی که از اعتبار علمی لازم برخوردار بوده، بهره گرفته شود. همچنین پژوهشگر ضمن فیش‌برداری، منابع مربوط را دقیقاً در ذیل هر مطلب درج نموده است و کلیه متون و ادبیات گردآوری‌شده را ازلحاظ محتوایی و ارتباط با قلمرو موضوعی پژوهش به تأیید اساتید راهنما و مشاور رسانیده است. در راستای پایایی اسناد و مدارک پژوهش، محقق تلاش نموده تا از اسناد، مدارک مرتبط با موضوع پژوهش استفاده نماید و از سوی دیگر، منابعی مورد بهره‌برداری قرارگرفته است که از تکرارپذیری بالایی در بین سایر تحقیقات سالیان اخیر برخوردار بوده است. در این راستا از مشورت متخصصین امر و نظرات ارزشمند اساتید راهنما و مشاور نیز استفاده نموده است. پرسش‌نامه نیز پس از تهیه، مورد قضاوت افراد آگاه و مطلع و صاحب‌نظر قرارگرفته است و جهت استانداردسازی به مشاوره گذاشته‌شده است و نقطه نظرات متخصصان ازنظر صوری، محتوایی و اثربخشی آن، بررسی و نکات ذکرشده در پرسش‌نامه اعمال گردیده است. در این راستا، تعدادی پرسش‌نامه به جامعه آماری ارائه و با جمع‌آوری نظرات آن‌ها ازنظر فرم، محتوای سؤالات، نحوه نگارش و با لحاظ نمودن نقطه نظرات آن‌ها، موجبات روایی بیشتر پرسش‌نامه را فراهم گردیده است.

برای آزمون قابلیت پایایی پرسش‌نامه که با طیف لیکرت پنج‌تایی طراحی‌شده، از ضریب آلفای کرون‌باخ استفاده‌شده است. با بهره‌گیری از نرم‌افزار آماری اس‌پی‌اس‌اس، سؤالات پرسش‌نامه مورد تجزیه‌وتحلیل قرارگرفته است و ضریب آلفای کرونباخ به‌دست‌آمده، مبنای استفاده یا عدم استفاده از پرسش‌نامه مذبور شده است.

**جدول (۲) نتایج آزمون پایایی پرسش‌نامه به روش آلفای کرونباخ**

| بعد | تعداد سؤالات | ضریب آلفای کرونباخ |
|---|---|---|
| آگاهی وضعیتی | ۷ | ۰/۸۳۵ |
| سامانه‌های خودمختار | ۵ | ۰/۸۱۸ |
| جنگ‌افزارها | ۹ | ۰/۸۴۴ |
| کارکنان | ۶ | ۰/۸۲۳ |

**تجزیه‌وتحلیل داده‌ها**

برای دستیابی به هدف اصلی پژوهش یعنی «تبیین کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک»، در ابتدا به تبیین چهار هدف فرعی پرداخته‌شده است که پس از تجزیه‌وتحلیل اطلاعات جمع‌آوری‌شده از طریق پرسش‌نامه، مصاحبه با صاحب‌نظران و بررسی اسناد و مدارک در رابطه با موضوع پژوهش با روش توصیفی و با استفاده از جداول توزیع فراوانی و همچنین استفاده از نمره میانگین در نرم‌افزار اس‌پی‌اس‌اس، نتایج زیر حاصل گردید:

**هدف اول:** کاربردهای فناوری اینترنت اشیاء در بعد «آگاهی وضعیتی» جنگ سایبر و الکترونیک و در مؤلفه‌های سی۴آی‌اس‌آر (سه شاخص)، سامانه موقعیت‌یاب جهانی (دو شاخص) و نقشه‌های رقمی (دو شاخص) مورد ارزیابی قرار گرفت. نتایج حاصل گویای این مطلب است که بیش از ۸۳٪ افراد جامعه نمونه، با شاخص‌های ارائه‌شده در مورد کاربردهای فناوری اینترنت اشیاء در بعد آگاهی وضعیتی جنگ سایبر و الکترونیک، موافق و کاملاً موافق بوده‌اند و در ضمن چون میانگین این مؤلفه ۴.۲۸ (۴<۴.۲۸<۵) است، بنابراین با کاربردهای آن موافق می‌باشند.

**هدف دوم:** کاربردهای فناوری اینترنت اشیاء در بعد «سامانه‌های خودمختار» جنگ سایبر و الکترونیک و در مؤلفه‌های سامانه‌های تشخیص و جلوگیری (دو شاخص) و ربات‌های انبوه (دو شاخص) مورد ارزیابی قرار گرفت. نتایج حاصل گویای این مطلب است که بیش از ۸۰٪ افراد جامعه نمونه، با شاخص‌های ارائه‌شده در مورد کاربردهای فناوری اینترنت اشیاء در بعد سامانه‌های خودمختار جنگ سایبر و الکترونیک، موافق و کاملاً موافق بوده‌اند و در ضمن چون میانگین این مؤلفه ۴.۲ (۴<۴.۲<۵) است، بنابراین با کاربردهای آن موافق می‌باشند.

**هدف سوم:** کاربردهای فناوری اینترنت اشیاء در بعد «جنگ‌افزارهای» جنگ سایبر و الکترونیک و در مؤلفه‌های سامانه‌های کنترل آتش (سه شاخص)، سامانه‌های بدون سرنشین (سه شاخص) و هدف‌گیری دقیق (سه شاخص) مورد ارزیابی قرار گرفت. نتایج حاصل گویای این مطلب است که بیش از ۸۵٪ افراد جامعه نمونه، با شاخص‌های ارائه‌شده در مورد کاربردهای فناوری اینترنت اشیاء در بعد جنگ‌افزارهای جنگ سایبر و الکترونیک، موافق و کاملاً موافق بوده‌اند و در ضمن چون میانگین این مؤلفه ۴.۴۴ (۴<۴.۴۴<۵) است، بنابراین با کاربردهای آن موافق می‌باشند.

**هدف چهارم:** کاربردهای فناوری اینترنت اشیاء در بعد «کارکنان» جنگ سایبر و الکترونیک و در مؤلفه‌های رزمندگان (سه شاخص) و فرماندهان (سه شاخص) مورد ارزیابی قرار گرفت. نتایج حاصل گویای این مطلب است که بیش از ٪۸۴ افراد جامعه نمونه، با شاخص‌های ارائه‌شده در مورد کاربردهای فناوری اینترنت اشیاء در بعد کارکنان جنگ سایبر و الکترونیک، موافق و کاملاً موافق بوده‌اند و در ضمن چون میانگین این مؤلفه ۴.۳۳ (۴<۴.۳۳<۵) است، بنابراین با کاربردهای آن موافق می‌باشند.

## نتیجه‌گیری و پیشنهادها

درمجموع نتایج تحلیل کیفی و کمی صورت گرفته به‌منظور دستیابی به هدف اصلی پژوهش (تبیین کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک) به شرح زیر است:

تعداد چهار بعد از بعدهای مورداستفاده قرارگرفته با میانگین بیش از چهار و بر اساس نمره میانگین، به ترتیب زیر می‌توانند به‌عنوان کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک مدنظر قرار گیرند:

**جدول (۳) اولویت‌بندی کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک (بعدها)**

| اولویت | مؤلفه‌ها | نمره میانگین |
|---|---|---|
| ۱ | جنگ‌افزارها | ۴.۳۳۵ |
| ۲ | کارکنان | ۴.۳۳۱ |
| ۳ | آگاهی وضعیتی | ۴.۲۷۴ |
| ۴ | سامانه‌های خودمختار | ۴.۱۸۶ |

تعداد ۱۰ مؤلفه از مؤلفه‌های مورداستفاده قرارگرفته با میانگین بیش از چهار و بر اساس نمره میانگین، به ترتیب زیر می‌توانند به‌عنوان کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک مدنظر قرار گیرند:

**جدول (۴) اولویت‌بندی کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک (مؤلفه‌ها)**

| اولویت | مؤلفه‌ها | نمره میانگین |
|---|---|---|
| ۱ | کنترل آتش | ۴.۳۷۶ |
| ۲ | سی۴آی‌اس‌آر | ۴.۳۵۳ |
| ۳ | رزمندگان | ۴.۳۴۳ |
| ۴ | سامانه‌های بدون سرنشین | ۴.۳۳۳ |
| ۵ | فرماندهان | ۴.۳۲ |
| ۶ | هدف‌گیری دقیق | ۴.۳۰۶ |
| ۷ | ربات‌های انبوه | ۴.۲۵۳ |
| ۸ | سامانه موقعیت‌یاب جهانی | ۴.۲۴ |
| ۹ | نقشه‌های رقمی | ۴.۲۳ |
| ۱۰ | سامانه‌های تشخیص و جلوگیری | ۴.۱۲ |

تعداد ۲۷ شاخص از شاخص‌های مورداستفاده قرارگرفته با میانگین بیش از چهار به ترتیب اولویت‌های زیر (به همراه ذکر بعد و مؤلفه هر شاخص) می‌توانند به‌عنوان کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک مدنظر

قرار گیرند: (قابل‌ذکر اینکه شاخص‌های (۱۶ و ۲۶)، (۱ و ۱۵)، (۱۷ و ۲۳)، (۱۰ و ۱۳) و همچنین (۱۲ و ۵) نمره یکسانی کسب نموده‌اند که ملاک جایگاه آن‌ها در جدول (۵-۱)، رتبه مؤلفه‌های آن‌ها بوده است.)

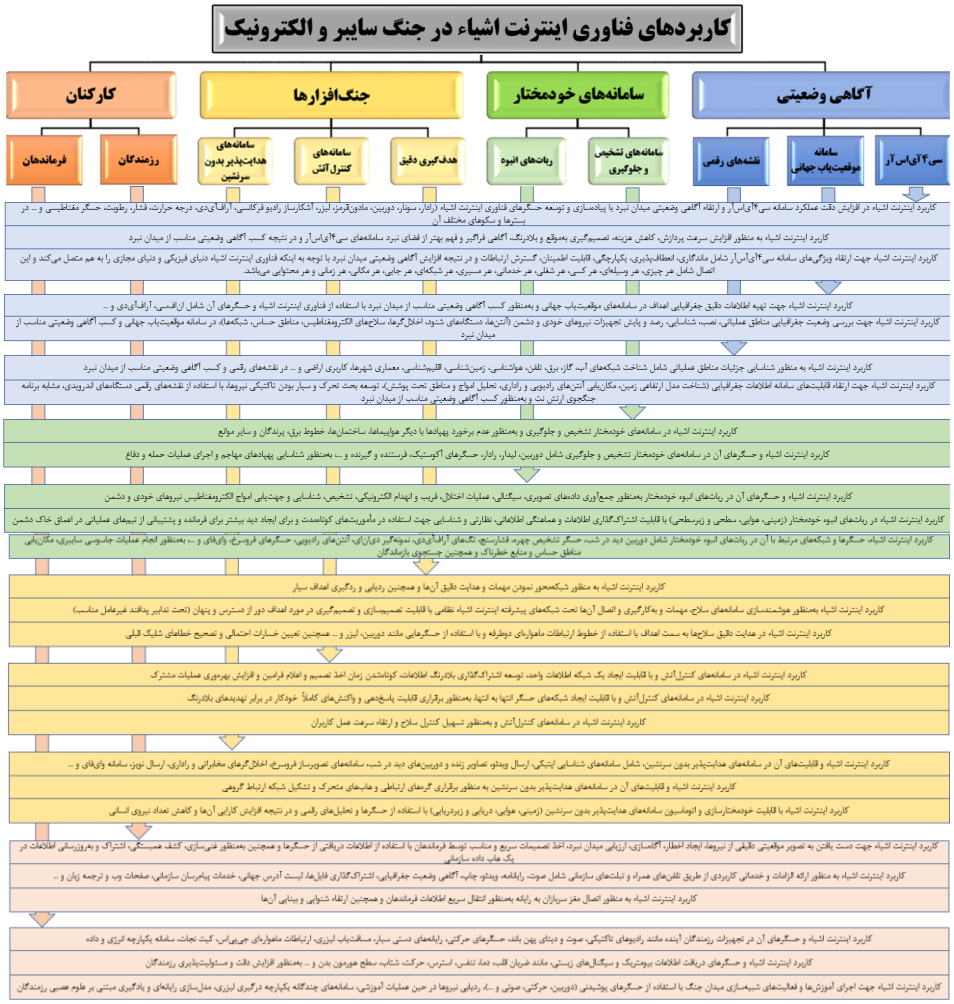
**جدول (۵) اولویت‌بندی کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک (شاخص‌ها)**

| اولویت | بعد | مؤلفه | شماره شاخص | شاخص | نمره میانگین |
|---|---|---|---|---|---|
| ۱ | جنگ‌افزارها | سامانه‌های بدون سرنشین | Q۲۱ | کاربرد فناوری اینترنت اشیاء باقابلیت خودمختار سازی و خودکارسازی سامانه‌های بدون سرنشین (زمینی، هوایی، دریایی و زیردریایی) با استفاده از حسگرها و تحلیل‌گرهای رقمی و درنتیجه افزایش کارایی آن‌ها و کاهش نیروی انسانی | ۴.۴۴ |
| ۲ | جنگ‌افزارها | سامانه‌های کنترل آتش | Q۱۶ | کاربرد فناوری اینترنت اشیاء در سامانه‌های کنترل آتش و با قابلیت ایجاد یک شبکه اطلاعات واحد، توسعه اشتراک‌گذاری بلادرنگ اطلاعات، کوتاه شدن زمان اخذ تصمیم و اعلام فرمان‌ها و افزایش بهره‌وری عملیات مشترک | ۴.۴۳ |
| ۲ | کارکنان | فرماندهان | Q۲۶ | کاربرد فناوری اینترنت اشیاء در ارائه الزامات و خدمات کاربردی از طریق تلفن‌های همراه و تبلت‌های سازمانی شامل صوت، رایانامه، ویدئو، چاپ، آگاهی وضعیت جغرافیایی، اشتراک‌گذاری فایل‌ها، لیست آدرس جهانی، خدمات پیام‌رسان سازمانی، صفحات وب و ترجمه زبان و ... برای فرماندهان | ۴.۴۳ |
| ۴ | کارکنان | فرماندهان | Q۲۵ | کاربرد فناوری اینترنت اشیاء جهت دست یافتن به تصویر موقعیتی دقیق از نیروها، ایجاد اخطار، آگاه‌سازی، ارزیابی میدان نبرد، اخذ تصمیمات سریع و مناسب توسط فرماندهان با استفاده از اطلاعات دریافتی از حسگرها و همچنین به‌منظور غنی‌سازی، کشف همبستگی، اشتراک و به‌روزرسانی اطلاعات در یک هاب داده سازمانی | ۴.۴۱ |
| ۵ | آگاهی وضعیتی | سی۴ آی‌اس‌آر | Q۱ | کاربرد فناوری اینترنت اشیاء در افزایش دقت و عملکرد سامانه‌های سی۴آی‌اس‌آر با پیاده‌سازی و توسعه حسگرهای آن شامل رادار، سونار، دوربین، مادون‌قرمز، لیزر، آشکارساز رادیو فرکانسی، آراف‌آی‌دی، درجه حرارت، فشار، رطوبت، حسگر مغناطیسی، حسگر صوتی، حسگر شیمیایی، حسگر نور محیط و ... در بسترها و سکوهای مختلف | ۴.۳۸ |
| ۶ | جنگ‌افزارها | هدف‌گیری دقیق | Q۱۵ | کاربرد فناوری اینترنت اشیاء در هدایت دقیق سلاح‌ها به سمت اهداف با استفاده از خطوط ارتباطات ماهواره‌ای دوطرفه و با استفاده از حسگرهای مانند دوربین، لیزر و ... همچنین تعیین خسارات احتمالی و تصحیح خطاهای شلیک قبلی | ۴.۳۸ |
| ۷ | آگاهی وضعیتی | سی۴ آی‌اس‌آر | Q۳ | کاربرد فناوری اینترنت اشیاء در ارتقاء ویژگی‌های سامانه سی۴آی‌اس‌آر شامل ماندگاری، انعطاف‌پذیری، یکپارچگی، قابلیت اطمینان، گسترش ارتباطات با این تعریف که این فناوری دنیای فیزیکی و دنیای مجازی را به هم متصل می‌کند و این اتصال شامل هر چیزی، هر وسیله‌ای، هرکسی، هر شغلی، هر خدماتی، هر مسیری، هر شبکه‌ای، هرجایی، هر مکانی، هرزمانی و هر محتوایی است. | ۴.۳۷ |
| ۸ | جنگ‌افزارها | سامانه‌های کنترل آتش | Q۱۷ | کاربرد فناوری اینترنت اشیاء در سامانه‌های کنترل آتش و باقابلیت ایجاد شبکه‌های حسگر انتها به انتها، به‌منظور برقراری قابلیت پاسخ‌دهی و واکنش‌های کاملاً خودکار در برابر تهدیدهای بلادرنگ | ۴.۳۶ |
| ۹ | کارکنان | رزمندگان | Q۲۳ | کاربرد فناوری اینترنت اشیاء و حسگرهای دریافت اطلاعات حیات‌سنجی و سیگنال‌های زیستی، مانند ضربان قلب، دما، تنفس، استرس، حرکت، شتاب، سطح هورمون بدن و ... به‌منظور افزایش دقت و مسئولیت‌پذیری رزمندگان | ۴.۳۶ |
| ۱۰ | کارکنان | رزمندگان | Q۲۴ | کاربرد فناوری اینترنت اشیاء در اجرای آموزش‌ها و فعالیت‌های شبیه‌سازی میدان جنگ با استفاده از حسگرهای پوشیدنی (دوربین، حرکتی، صوتی و ...)، ردیابی نیروها در حین عملیات آموزشی، سامانه‌های چندگانه یکپارچه درگیری لیزری، مدل‌سازی رایانه‌ای و یادگیری مبتنی بر علوم عصبی رزمندگان | ۴.۳۵ |
| ۱۱ | جنگ‌افزارها | سامانه‌های کنترل آتش | Q۱۸ | کاربرد فناوری اینترنت اشیاء در سامانه‌های کنترل آتش و به‌منظور تسهیل کنترل سلاح و ارتقاء سرعت عمل کاربران | ۴.۳۴ |

| اولویت | بعد | مؤلفه | شماره شاخص | شاخص | نمره میانگین |
|---|---|---|---|---|---|
| ۱۲ | جنگ‌افزارها | سامانه‌های بدون سرنشین | Q۱۹ | کاربرد فناوری اینترنت اشیاء و حسگرها و شبکه‌های مختلف آن در سامانه‌های بدون سرنشین، شامل سامانه‌های شناسایی اپتیکی، ارسال ویدئو، تصاویر زنده و دوربین‌های دید در شب، سامانه‌های تصویرساز فروسرخ، اخلال‌گرهای مخابراتی و راداری، ارسال نویز، سامانه وای فای و ... | ۴.۳۳ |
| ۱۳ | کارکنان | رزمندگان | Q۲۲ | کاربرد فناوری اینترنت اشیاء و حسگرهای آن در تجهیزات رزمندگان آینده مانند رادیوهای تاکتیکی، صوت و دیتای پهن باند، حسگرهای حرکتی، رایانه‌های دستی سیار، مسافت یاب لیزری، ارتباطات ماهواره‌ای جی‌پی‌اس، کیت نجات، سامانه یکپارچه انرژی و داده و ... | ۴.۳۳ |
| ۱۴ | آگاهی وضعیتی | سی۴ آی‌اس‌آر | Q۲ | کاربرد فناوری اینترنت اشیاء به‌منظور افزایش سرعت پردازش، کاهش هزینه، تصمیم‌گیری به‌موقع و بلادرنگ، آگاهی فراگیر و فهم بهتر از فضای نبرد سامانه‌های سی۴آی‌اس‌آر | ۴.۳۱ |
| ۱۵ | جنگ‌افزارها | هدف‌گیری دقیق | Q۱۳ | کاربرد فناوری اینترنت اشیاء باقابلیت شبکه محور نمودن سلاح‌ها (چف، فلیر، دکوی، بمب‌های صوتی، گرافیتی، اخلال‌گرهای حرارتی، راداری و ...) و هدایت دقیق آن‌ها و همچنین ردیابی و ردگیری اهداف سیار | ۴.۲۹ |
| ۱۶ | سامانه‌های خودمختار | ربات‌های انبوه | Q۱۰ | کاربرد فناوری اینترنت اشیاء و حسگرهای آن در ربات‌های انبوه خودمختار به‌منظور جمع‌آوری داده‌های تصویری، سیگنالی، عملیات اختلال، فریب و انهدام الکترونیکی، تشخیص، شناسایی و جهت‌یابی امواج الکترومغناطیس نیروهای خودی و دشمن | ۴.۲۹ |
| ۱۷ | سامانه‌های خودمختار | ربات‌های انبوه | Q۱۲ | کاربرد فناوری اینترنت اشیاء، حسگرها و شبکه‌های مرتبط با آن در ربات‌های انبوه خودمختار شامل دوربین دید در شب، حسگر تشخیص چهره، فشارسنج، تگ‌های آراف‌آی‌دی، نمونه‌گیر دی‌ان‌ای، آنتن‌های رادیویی، حسگرهای فروسرخ، وای فای و ... به‌منظور انجام عملیات جاسوسی سایبری، مکان‌یابی مناطق حساس و منابع خطرناک و همچنین جستجوی بازماندگان | ۴.۲۷ |
| ۱۸ | آگاهی وضعیتی | سامانه موقعیت‌یاب جهانی | Q۵ | کاربرد فناوری اینترنت اشیاء به‌منظور بررسی وضعیت جغرافیایی مناطق عملیاتی، نصب، شناسایی، رصد و پایش تجهیزات نیروهای خودی و دشمن (آنتن‌ها، دستگاه‌های شنود، اخلال‌گرها، سلاح‌های الکترومغناطیس، مناطق حساس، شبکه‌ها)، در سامانه موقعیت‌یاب جهانی | ۴.۲۷ |
| ۱۹ | جنگ‌افزارها | هدف‌گیری دقیق | Q۱۴ | کاربرد فناوری اینترنت اشیاء به‌منظور هوشمند سازی سامانه‌های سلاح، مهمات و به‌کارگیری و اتصال آن‌ها تحت شبکه‌های پیشرفته اینترنت اشیاء نظامی باقابلیت تصمیم‌سازی و تصمیم‌گیری در مورد اهداف دور از دسترس و پنهان (تحت تدابیر پدافند غیرعامل مناسب) | ۴.۲۵ |
| ۲۰ | آگاهی وضعیتی | نقشه‌های رقمی | Q۷ | کاربرد فناوری اینترنت اشیاء به‌منظور ارتقاء قابلیت‌های سامانه اطلاعات جغرافیایی (شناخت مدل ارتفاعی زمین، مکان‌یابی آنتن‌های رادیویی و راداری، تحلیل امواج و مناطق تحت پوشش)، توسعه بحث تحرک و سیار بودن تاکتیکی نیروها، با استفاده از نقشه‌های رقمی دستگاه‌های اندرویدی، مشابه برنامه جنگجوی ارتش نت | ۴.۲۴ |
| ۲۱ | جنگ‌افزارها | سامانه‌های بدون سرنشین | Q۲۰ | کاربرد فناوری اینترنت اشیاء و قابلیت‌های آن در سامانه‌های بدون سرنشین، شامل برقراری گره‌های ارتباطی و هاب‌های متحرک، تشکیل شبکه ارتباط گروهی | ۴.۲۳ |
| ۲۲ | آگاهی وضعیتی | نقشه‌های رقمی | Q۶ | کاربرد فناوری اینترنت اشیاء در نقشه‌های رقمی و به‌منظور شناسایی جزئیات مناطق عملیاتی شامل شناخت شبکه‌های آب، گاز، برق، تلفن، هواشناسی، زمین‌شناسی، اقلیم‌شناسی، معماری شهرها، کاربری اراضی و ... | ۴.۲۲ |
| ۲۳ | آگاهی وضعیتی | سامانه موقعیت‌یاب جهانی | Q۴ | کاربرد فناوری اینترنت اشیاء و حسگرهای آن شامل ان‌اف‌سی، آراف‌آی‌دی و ...، در سامانه‌های موقعیت‌یاب جهانی به‌منظور تهیه اطلاعات دقیق جغرافیایی اهداف | ۴.۲۱ |
| ۲۴ | سامانه‌های خودمختار | ربات‌های انبوه | Q۱۱ | کاربرد فناوری اینترنت اشیاء در ربات‌های انبوه خودمختار (زمینی، هوایی، سطحی و زیرسطحی) با قابلیت اشتراک‌گذاری اطلاعات و هماهنگی اطلاعاتی، نظارتی و شناسایی جهت استفاده در مأموریت‌های کوتاه‌مدت و برای ایجاد دید بیشتر برای فرمانده و پشتیبانی از گروه‌های عملیاتی در اعماق خاک دشمن | ۴.۲ |
| ۲۵ | سامانه‌های | سامانه‌های | Q۸ | کاربرد فناوری اینترنت اشیاء در سامانه‌های خودمختار تشخیص و جلوگیری و | ۴.۱۵ |

| اولویت | بعد | مؤلفه | شماره شاخص | شاخص | نمره میانگین |
|---|---|---|---|---|---|
| | خودمختار | تشخیص و جلوگیری | | به‌منظور عدم برخورد پهپادها با دیگر هواپیماها، ساختمان‌ها، خطوط برق، پرندگان و سایر موانع | |
| ۲۶ | کارکنان | فرماندهان | Q۲۷ | کاربرد فناوری اینترنت اشیاء جهت اتصال مغز رزمندگان به رایانه به‌منظور انتقال سریع اطلاعات فرماندهان و همچنین ارتقاء شنوایی و بینایی | ۴.۱۲ |
| ۲۷ | سامانه‌های خودمختار | سامانه‌های تشخیص و جلوگیری | Q۹ | کاربرد فناوری اینترنت اشیاء و حسگرهای آن در سامانه‌های خودمختار تشخیص و جلوگیری شامل دوربین، لیدار، رادار، حسگرهای آکوستیک، فرستنده و گیرنده و ... به‌منظور شناسایی پهپادهای مهاجم و اجرای عملیات حمله و دفاع | ۴.۰۹ |

با توجه به مطالعات و نتایج حاصل، مدل مفهومی پژوهش به شرح ذیل ارائه می‌گردد:




با توجه به آنچه از نتایج این تحقیق حاصل گردید و بر اساس مدل مفهومی تبیین کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و الکترونیک به نظر می‌رسد کاربردی نمودن این فناوری کمک شایانی به

ارتقاء توان رزمی ارتش جمهوری اسلامی ایران و دیگر نیروهای مسلح خواهد نمود، لذا پیشنهادهایی برای رسیدن به هدف فوق در قالب پیشنهادهای اجرایی و پژوهشی در ادامه بیان می‌گردد:

## پیشنهادهای اجرایی:

۱) تحقیق، توسعه و آموزش‌های لازم در حوزه فناوری نوظهور اینترنت اشیاء انجام و سطح دانش کارکنان نیروهای مسلح جمهوری اسلامی ایران در استفاده از این فناوری در بخش‌های مربوط ارتقاء یابد.

۲) اعزام تعدادی از افسران رسته‌های الکترونیک، سایبر، مخابرات و جنگال به کشورهای دوست و هم‌پیمان مانند چین و هند به‌منظور کسب تجربیات آموزشی و ارتقاء دانش اینترنت اشیاء

۳) تأکید و حمایت ویژه از طرح‌ها و ایده‌ها کارکنان نخبه نیروهای مسلح در ارتباط با فناوری اینترنت اشیاء با توجه به بیان اهمیت و سرعت رشد تأمل‌برانگیز آن

۴) حمایت از شرکت‌های دانش‌بنیان و توسعه کانال‌های تعاملی و ارتباطی آن‌ها با نیروهای مسلح، انعقاد تفاهم‌های همکاری مشترک و سرمایه‌گذاری در جهت تحقیق، توسعه و تولید محصولات مرتبط با کاربرد فناوری اینترنت اشیاء

۵) انجام اقدامات مناسب و هم‌راستا با اقدامات دیگر کشورهای پیش رو در جهت بومی‌سازی زیرساخت‌های ارتباطی، سخت‌افزاری و نرم‌افزاری و طراحی شبکه اینترانت بومی داخلی نیروهای مسلح

۶) در نظر گرفتن تلفن‌های همراه و تبلت‌های سازمانی بومی و مختص ارتش و نرم‌افزارهای کاربردی داخلی و واگذاری آن‌ها به فرماندهان و رزمندگان در سطوح مختلف آجا جهت استفاده از قابلیت‌های آن‌ها شامل ارسال صوت، رایانامه، ویدئو، چاپ، آگاهی وضعیت جغرافیایی، اشتراک‌گذاری فایل‌ها، لیست آدرس جهانی، خدمات پیام‌رسان سازمانی

۷) انجام اقدامات لازم در جهت توسعه نسل پنج و نسل شش اینترنت و برقراری ارتباطات سریع، دقیق و پایدار و همچنین با توجه به نقش بسیار حیاتی اینترنت ماهواره‌ای در جنگ‌های آینده و حتی حال حاضر، می‌بایست انجام مطالعات تحقیقاتی فنی و تخصصی آن با جدیت در دستور کار معاونت‌های مطالعاتی و تحقیقاتی و ستادهای برتر قرار گیرد.

۸) اجرای عملی به‌کارگیری حسگرهای فناوری اینترنت اشیاء شامل ان‌اف‌سی، آراف‌آی‌دی، حسگر موقعیت‌یاب جغرافیایی بر روی تجهیزات و سامانه‌های جنگ الکترونیک (آنتن‌ها، دستگاه‌های شنود، اخلال‌گرها، بمب‌های صوتی و گرافیتی و ...)

۹) نسبت به بررسی و استفاده کاربردی از قابلیت‌های نقشه‌های رقمی و سامانه موقعیت‌یاب جهانی در شناسایی مناطق هدف در جنگ الکترونیک برای مثال شبکه‌های برق، نیروگاه‌ها و تهیه برآورد و پیوست جنگ الکترونیک اقدام نماید.

۱۰) در صورت تأمین و یا ساخت ربات‌های انبوه توسط معاونت‌های مربوط نسبت به استفاده کاربردی و عملی فناوری اینترنت اشیاء و حسگرهای آن شامل آنتن‌های رادیویی، حسگرهای فروسرخ، وای فای، انواع دوربین‌های معمولی، حرارتی، دید در شب و حسگرهای تشخیص چهره و ... در جهت انجام مأموریت شناسایی، حمله و دفاع الکترونیکی اقدام نماید.

۱۱) بررسی چگونگی مقابله با تهدیدات ربات‌های انبوه و سامانه‌های بدون سرنشین و اجرای حملات سایبر بر روی آن‌ها و یا استفاده از قابلیت‌های آن‌ها شامل شبکه‌های وای فای، تگ‌های آراف‌آی‌دی و نمونه‌گیرهای دی‌ان‌ای، به‌منظور اجرای عملیات جاسوسی سایبر در صورت تأمین و یا ساخت نمونه‌های داخلی

۱۲) در صورت تأمین و تهیه حسگرهای دریافت اطلاعات حیات‌سنجی و سیگنال‌های زیستی مانند حسگرهای تشخیص ضربان قلب، دمای بدن، تنفس، استرس، حرکت، شتاب، سطح هورمون بدن، استفاده کاربردی از آن‌ها توسط کارکنان سایبر و الکترونیک و بررسی تأثیر آن‌ها در افزایش دقت و مسئولیت‌پذیری کارکنان

۱۳) بررسی دقیق خلأهای امنیتی اینترنت اشیاء در برابر حملات سایبر و راه‌های رفع آن با زیر نظر داشتن اقدامات آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی آمریکا (دارپا) و اتحادیه فیدو

۱۴) بررسی راه‌کارهای حمله و نفوذ سایبر به سامانه‌های تشخیص و جلوگیری و ربات‌های انبوه و یا هک نقشه‌های رقمی رزمندگان دشمن

**پیشنهادهای پژوهشی:**

۱) بررسی کاربردهای فناوری اینترنت اشیاء در جنگ سایبر و یا جنگ الکترونیک به‌صورت جداگانه و بررسی جزئی‌تر و تخصصی‌تر در هر یک از مؤلفه‌های ذکرشده در این پژوهش، برای مثال؛ بررسی جزئیات کاربردهای اینترنت اشیاء در سامانه سی۴آی‌اس‌آر.

۲) بررسی تخصصی قابلیت‌ها، ساختار و عملکرد اینترنت ماهواره‌ای، اینترنت اشیاء زیر آب، ربات‌های انبوه، سامانه‌های تشخیص و جلوگیری و بررسی فعالیت‌های دارپا و اتحادیه فیدو در راستای ارتقاء امنیت به‌کارگیری اینترنت اشیاء.

۳) بررسی تخصصی‌تر معماری جنگ شبکه‌ای اینترنت اشیاء و شناخت اجزاء و ارتباطات مربوط.

۴) بررسی چگونگی ارتباط مغز رزمندگان به رایانه و انتقال سریع اطلاعات فرماندهان

۵) بررسی تخصصی تجهیزات رزمندگان آینده و قابلیت‌های این تجهیزات در حوزه‌های نبرد ازجمله پوشیدنی‌های هوشمند باقابلیت ارتباط با تلفن‌های همراه و کسب اطلاعات حیات‌سنجی مانند ضربان قلب، دما، تنفس، استرس، حرکت، شتاب

## قدردانی

از خبرگان توانمندی که در طول پژوهش، دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند و استواری پژوهش حاضر بر مشارکت و دانش این بزرگواران قرارگرفته است، بسیار سپاسگزاریم.

## منابع

- احمدی، لیلا و همکاران. (۲۰۱۶). *بررسی مکانیسم‌های دفاعی و لجستیک در اینترنت اشیاء*، پنجمین اجلاس بین‌المللی علم و مهندسی پاریس.
- آذر، داود و محمدحسین، حمید. (۱۳۹۷). *کلیات جنگ الکترونیک پیشرفته*، تهران: انتشارات دافوس آجا.
- اسدالله زاده، محمد. (۱۳۹۸). *طرح‌ریزی تمرینات تاکتیکی جنگ الکترونیک*، تهران: انتشارات دافوس آجا.
- بختیاری، ایرج. (۱۳۹۹). تحلیل محیطی آینده فرماندهی و کنترل در حوزه دفاع هوافضایی از منظر چالش ها و فرصت ها. *فرماندهی و کنترل*، ۴(۲ ): ۱-۲۰.
- بهشتی آتشگاه، محمد و همکاران. (۱۳۹۷). مفاهیم و چالش‌های امنیتی اینترنت اشیاء نظامی با محوریت مکانیسم MIoT ایالات‌متحده آمریکا، *فصلنامه علمی-پژوهشی فرماندهی و کنترل*. ۲ (۳): ۶۴-۷۸.
- پراکاش، آبیشور. (۲۰۱۸). *ربات‌های انبوه: افق‌های جدید در تحقیقات نظامی*، در دسترس از سایت (www.roboticsbusinessreview.com) به تاریخ ۱۴۰۰/۱۲/۱۰.
- پورقهرمانی، نوروز؛ عبدی، فریدون و مقدم شهابی، افسانه. (۱۳۹۵). *بررسی جنگ الکترونیک شبکه محور به عنوان یکی از نشانه های بلوغ جنگ سایبر درسالهای اخیر*،کنفرانس ملی پدافند غیرعامل در قلمرو فضای سایبر،مراغه،https://civilica.com/doc/649586.
- غلام نژاد، پژمان، غلامی؛ محمود و پورمکاری، علیرضا. (۱۳۹۸). کاربردهای نظامی اینترنت اشیا با تأکید بر مأموریت های نیروی هوایی ارتش جمهوری اسلامی ایران. *علوم و فنون نظامی*، ۱۵(۴۹ ): ۱۴۱-۱۶۳.
- حقگو، رضا. (۱۳۹۷). *فضای مجازی (فرصت‌ها و تهدیدها)*، معاونت تربیت و آموزش آجا، تهران.
- سجادی اصیل وحید و آذر، داود. (۱۳۹۹). *عملیات سایبری در طرح‌ها و برنامه‌های وزارت دفاع آمریکا*، تهران: انتشارات دافوس آجا.
- سیاست‌های کلی برنامه ششم توسعه کشور ابلاغی مقام معظم رهبری (مد ظله العالی)، سر فصل امور دفاعی و امنیتی، بندهای ۵۲ و ۵۳
- شریفی تهرانی، امید و لشگریان، حمیدرضا.(۱۳۹۶). نقش پهپاد در حوزه جنگ الکترونیک، نیازها و چالش‌های تلفیق، *سومین اجلاس ملی اویونیک ایران*، تهران.

- شعبانی، مهدی و همکاران. (۱۳۹۵). *به‌کارگیری اینترنت اشیاء در شبکه C4I با تکیه‌بر آگاهی وضعیت*، دانشگاه خوارزمی، نهمین اجلاس ملی فرماندهی و کنترل.
- سلیمانزاده نجفی، نیره سادات ؛ عاصمی، عاصفه ؛ سهرابی، مظفر چشمه؛ شعبانی، احمد. (۱۳۹۷). مطالعه کتاب سنجی تولیدات علمی حوزه اینترنت اشیا در پایگاه مدلاین: تحلیل هم رخدادی واژگان. *پایش*. ۱۳۹۷; ۱۷ (۵) :۵۰۷-۵۲۰.
- فرج‌پور، عباس. (۱۳۹۸). ارائه الگوی راهبردی بومی برای سازمان‌های شبکه‌ای در نیروهای مسلح با نگاه به جنگ‌های آینده، دانشگاه عالی دفاع ملی.
- فرح بخت، احمدرضا، و دهقانی، مهدی. (۱۳۹۸). همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان های نظامی. *امنیت ملی*، ۹(۳۱ ): ۱۹۹-۲۱۹.
- فلسفی، سپهدار؛ و صادقی، علی‌رضا. (۱۳۹۸). سناریوی جنگ الکترونیک نیروهای مسلح با استکبار جهانی مبتنی بر فناوری‌های نوظهور در افق ۲۰۳۰، پنجمین همایش ملی علوم و مهندسی دفاعی، تهران، دانشگاه افسری و تربیت پاسداری امام حسین (ع).
- کرامتی مقدم و همکاران. (۱۴۰۰). مروری بر تأثیرات اینترنت اشیاء در زندگی مردم و آینده پیش روی آن، *نشریه پژوهش‌های نوین در مدیریت کارآفرینی و توسعه کسب‌وکار*، ۲(۶): ۶۷-۴۲.
- کیخسروی، مصطفی. (۱۳۹۹). *چگونگی به‌کارگیری سامانه فرماندهی و کنترل در فرماندهی جنگ الکترونیک راهبردی ارتش جمهوری اسلامی ایران*، پایان‌نامه جهت اخذ درجه کارشناسی ارشد، دانشگاه فرماندهی و ستاد آجا، تهران.
- گروه مترجمین سازمان تحقیقات و جهاد خودکفایی آجا. (۱۳۹۹). برترین ریز پرنده‌های جهان، *فصلنامه علمی تحقیقاتی محقق*، شماره ۹۰.
- گروه مترجمین علوم، تحقیقات و فناوری آجا. (۱۴۰۰). پهپاد هاروپ، *فصل‌نامه علمی تحقیقاتی محقق*، شماره ۹۱.
- گروه مؤلفین معاونت فاوا آجا. (۱۴۰۰). سامانه مدیریت نبرد پیشرفته (ABMS) رهیافتی نوین در فرماندهی و کنترل هوشمند، گاهنامه علمی و خبری عصر جدید ارتباطات و فناوری اطلاعات، شماره دوم.
- گروه نویسندگان مرکز تحقیقات اینترنت اشیاء ایران. (۱۴۰۰). ارتباط صنایع نظامی و اینترنت اشیاء، در دسترس از سایت (www.iotiran.com) به تاریخ ۱۴۰۰/۷/۳۰
- لطفی، محمد. (۱۴۰۰). *ارتقاء امنیت یگان‌های ارتش جمهوری اسلامی ایران با بهره‌گیری از فناوری اینترنت اشیاء*، پایان‌نامه جهت اخذ کارشناسی ارشد، دانشگاه فرماندهی و ستاد آجا.
- لک، بهزاد. (۱۳۹۹). راهبردهای بکارگیری اینترنت اشیا در ماموریت های پلیس آگاهی. *پژوهش های مدیریت انتظامی (مطالعات مدیریت انتظامی)*، ۱۵(۱ ): ۷۵-۱۰۰.

- محمدی، حافظ و کریمی قهرودی، محمدرضا. (۱۳۹۹). توسعه سامانه‌های «فرماندهی و کنترل سایبری» در جمهوری اسلامی ایران با فناوری «اینترنت اشیاء»، دوازدهمین اجلاس ملی فرماندهی و کنترل ایران.
- مهدی‌نژاد نوری، محمد؛ جبار رشیدی، علی؛ احمدی حاجی آبادی، سید احمد و تیلا، شعبان . (۱۳۹۶). تأثیر متقابل دفاع دانش‌بنیان و جنگ‌های آینده. *مطالعات دفاعی استراتژیک*. ۱۵(۶۷): ۲۶۰-۲۳۵.
- موحدی صفت، محمدرضا. (۱۴۰۰). فضای سایبر، تحولات و تهدیدات. دانشگاه فرماندهی و ستاد آجا، تک‌نگاشت شماره ۸.
- مینایی بیدگلی، بهروز و میرزایی قاضیانی، علی. (۱۳۹۸). مروری بر کاربردهای نظامی و چالش‌های تحقیقاتی در زمینه امنیت اینترنت اشیاء. *فصلنامه پژوهش‌های کاربردی در فنی و مهندسی*، ۲ (۱۰).
- نامداری، امیر. (۱۳۹۹). *چگونگی به‌کارگیری فناوری اینترنت اشیاء در فرماندهی آماد و پشتیبانی نیروی هوایی ارتش جمهوری اسلامی ایران*، پایان‌نامه کارشناسی ارشد، رشته مدیریت (آماد)، دانشگاه فرماندهی و ستاد آجا.
- نصیری، موسی. (۱۳۹۹). به‌کارگیری خودروهای رزمی زرهی رباتیک توسط ارتش آمریکا، مجله محقق، جهاد و خودکفایی آجا، شماره ۹۰.
- نیازمند، میلاد. (۱۳۹۸). سخن سردبیر، فصلنامه فنی-تخصصی جنگ الکترونیک، فرماندهی جنگ الکترونیک نهاجا، شماره ۲۰.
- Barkan, Nir & et al. (2011). Robotics And Autonomous Systems, the Industrial college of the Forces (ICAF), National Defence University.
- Bhatnagar, Rishi. (2020). Internet of Things (IoT) | The rise of the connected world, Confederation of indian industry 125 years since 1895,deloitte.
- Bognar, Eszter Katalin. (2018). Possibilities and security challenges of using IoT for military purposes, Hadmérnök (Military engineer), XIII Volume 3.
- Di Vito, Vittorio & et al. (2015). Sense and Avoid: Systems and Methods, Encyclopedia of Aerospace Engineering.
- Fernández-Caramés, Tiago & Fraga-Lamas, Paula. (2018). Towards The Internet of Smart Clothing: A Review on IoT Wearables and Garments for Creating Intelligent Connected E-Textiles, Department Computer Engineering, Faculty of Computer Science, Universidade da Coruña Spain.
- Fraga-Lamas, Paula & et al. (2016). A Review on Internet of Things for Defense and Public Safety. Department Electronics and Systems, Faculty of Computer Science, Universidade da Coruna. Sensors.
- Giandomenico, Spezzano. (2019). Swarm Robotics, Special Issue Published in Applied Sciences.

- Gupta, Nitin & Gupta, Jyoti. (2017). Internet of Things (IoT): a vision of any-time any-place for any-one, International Robotics & Automation Journal, india, Volume 2 Issue 6.
- Gotarane, Vishal & Raskar, Sandeep. (2019). IoT Practices in Military Applications, Proceedings of the Third International Conference on Trends in Electronics and Informatics.
- Jahanbakht, Mohammad & et al. (2021). Internet of Underwater Things and Big Marine Data Analytics–A Comprehensive Survey, IEEE communication Surveys & Tutorials.
- Maksimović, Mirjana and ets. (2015). Raspberry Pi as Internet of Things hardware: Performances and Constraints, Conference: IcETRAN, Vrnjacka Banja, Serbia.
- Nedjah, Nadia & SilvaJuniorba, Luneque .(2019). Swarm and Evolutionary Computation,Department of Electronics Engineering and Telecommunication, Faculty of Engineering, State University of Rio de Janeiro, Brazil, Volume 50
- Priyanka, Sonam & et al. (2020). Human Tracking System Based on GPS and IOT (Internet of Things), Proceeding of the International Conference on Computer Networks, Big Data and IoT.
- Priya, R. Vishnu & et al. (2016). GIS Enabled Internet of Things (IoT) Applications: An Overview, World Scientific News 41.
- Rahul, mohd & Alhumiany, hesham. (2017) An Analysis of Internet of Things(IoT): Novel Architectures, Modern Applications,Security Aspects and Future Scope with Latest Case Studie, International Journal of Engineering Research & Technology (IJERT), Vol. 6 Issue.
- Sifakis, joseph. (2018). Autonomous System-An Architectural Characterization, univ. Grenoble Alpes. Verimag laboratory.
- Wani, Umer. (2019). An introduction to IoT, its architecture and various protocols. Chapter outline, Department of Computer Science & Engineering.
- Zhu, L. & Majumdar, S. & Ekenna, C. (2020). An invisible warfare with the internet of battlefield things: A literature review, Department of Educational Psychology and Methodology.