آینده‌پژوهی دفاعی، سال پنجم، شماره ۱۷، تابستان ۱۳۹۹

تاریخ دریافت: ۱۳۹۹/۰۳/۱۶ تاریخ پذیرش: ۱۳۹۹/۰۷/۰۳

از صفحه ۱۴۳ تا صفحه ۱۷۱

شناسایی و رتبه‌بندی فناوری‌های اطلاعاتی نوظهور در بخش دفاعی- نظامی

اصغر محمدی فاتح*[۱]

سید عباس ابراهیمی[۲]

چکیده

در چند سال اخیر یک نیاز جدی برای فهم اثرات فناوری‌های اطلاعاتی نوظهور با محوریت هوش مصنوعی و اینترنت اشیاء در سازمان‌ها بوجود آمده است. در این راستا، هدف تحقیق حاضر، شناسایی و رتبه‌بندی فناوری‌های اطلاعاتی نوظهور در عرصه دفاعی- نظامی است. این پژوهش با بهره‌گیری از روش کیفی صورت پذیرفته است، مطالعهٔ اسناد کتابخانه‌ای و مصاحبهٔ با ۹ نفر از کارشناسان و صاحب‌نظران خبرهٔ فناوری اطلاعات با طراحی پرسش‌نامهٔ دلفی انجام شده است، در این زمینه اتفاق نظر استادان، صاحب‌نظران و کارشناسان با استفاده از روش دلفی گرفته شد، بدین‌طریق در جمع‌بندی مقوله‌ها یک اجماع نظری از نقطه نظرهای کارشناسان حاصل گردید. یافته‌های تحقیق حاکی از این است که تعداد ۲۳ فناوری اطلاعاتی نوظهور در بخش دفاعی موثر است که رتبه آن‌ها از طریق آزمون کندال تعیین شد. همچنین بر اساس میانگین نمره خبرگان به ترتیب برای تقلید، تطبیق و تسلّط نسبت به این فناوری‌ها، ۴، ۷، و ۱۳ سال زمان نیاز است. بالاخره بر اساس نظر خبرگان، این فناوری‌ها از نظر کاربرد در سه مقوله تکنیکی، تاکتیکی و راهبردی طبقه‌بندی شدند. مساعدت نظری مقاله، شناسایی و طبقه‌بندی تعداد ۲۳ فناوری اطلاعاتی نوظهور در دو بُعد تملک فناوری و نوع کاربرد فناوری در بخش دفاعی است.

واژه‌های کلیدی:

فناوری اطلاعات، هوش مصنوعی، کلان داده‌ها، اینترنت اشیاء.

[۱]. استادیار گروه مدیریت، دانشکده مدیریت و علوم نظامی، دانشگاه افسری امام علی(ع)، تهران، ایران

[۲]. استادیار گروه مدیریت، دانشکده اقتصاد، مدیریت و علوم اداری، دانشگاه سمنان، سمنان، ایران

* نویسنده مسئول: Email: amohammadi1360@yahoo.com

مقدمه

تحول دیجیتال[1] که کلیدی‌ترین بخش فناوری اطلاعات در سال ۲۰۲۰ محسوب می‌شود به دنبال تغییر کلیه شئون حیات بشری است که از طریق تبدیل بیت‌ها به ارزش صورت می‌گیرد (Menon, 2020). هزارهِ جدیدِ دیجیتال نوع جدیدی از نوآورانی است که به دنبال استفاده از ماشین‌های هوشمند هستند (Reis et al, 2019). همانطور که کوستین[2](۲۰۱۸) اشاره کرده است، در زمینه تکنولوژی‌های دیجیتال، سه روند جهانی بنام هوش مصنوعی، بلاکچین و کلان‌داده قابل ردیابی است که البته اینترنت اشیاء در مرکزیّت این روندها قرار دارد. تولید داده‌های گسترده جهانی، افزایش قدرت محاسباتی برای پردازش، پیشرفت تحلیل‌های کمی و الگوریتم‌های ریاضی در حوزه فناوری اطلاعات باعث شده است که یک هم‌افزایی بین کلان داده‌ها، هوش مصنوعی و اینترنت اشیاء بوجود آید و این حوزه‌ها با هم مطرح شوند (Uzair Mehmood et al, 2019). به خصوص، فناوری کلان داده[3] توانسته است نظام‌هایِ اطلاعاتی موجود از قبیل داده‌کاوی، یادگیری ماشینی، هوش محاسباتی، وب‌معنایی و شبکه‌های اجتماعی را به چالش بکشد (Simone, 2020; outsourceindia, 2020). بدون شک همه سازمان‌ها به دنبال اطلاع از این تغییراتی هستند که ممکن است در آینده نزدیک بر فعالیت‌های آنها سایه افکند و لذا شناسایی مقیاس و سطح تاثیر این فناوری‌های نوظهور و نوع تاثیر آنها شایان توجه است که البته این تشخیص و اشراف، ذیل موضوعاتی چون کنکاش محیطی[4]، پایش فناوری[5]، آگاهی فناوری[6] و دیدبانی فناوری[7] مطرح شده است (میرشاه ولایتی و نظری‌زاده، ۱۳۹۸). لذا مطالعه اکتشافی در خصوص سطح و نوع تاثیرات فناوری‌های اطلاعاتی نوپدید در عرصه دفاعی- نظامی شایان توجه است. یافته‌های مطالعاتیِ مشترک ۲۶ مرکز جهانی در سال ۲۰۱۸ نشان می‌دهد که گروه‌های تروریستی می‌توانند از اشکال مختلفّ هوش مصنوعی و یادگیری ماشینی برای انجام عملیات نظامی، جمع‌آوری اطلاعات و حملات سایبری استفاده کنند و مقیاس و تاثیرات حملات را گسترده کنند (Bhatnagar and Cotton, 2018). بر اساس سند وزارت دفاع آمریکا و آفریقای جنوبی، فناوری‌های رسانه‌ای موجود در اینترنت باعث شده است که گروه‌های نظامیِ افراطی، افراد معمولی را به استخدام خود درآورند و با

1. Digital Transformation
2. Kostin
3. Big data
4. Environmental Scanning
5. Technology Monitoring
6. Technology Intelligence
7. Technology Scouting

تامینِ مالیِ الکترونیکی به اعمال تروریستی در کشورها بپردازند[1]. از طرفی، جنبه‌های مثبت هوش مصنوعی برای کشور و سازمان استفاده‌کننده بسیار زیاد است و در این میان صرفه اقتصادی پهبادها و دفع حملات سایبری قابل ذکر است (همان منبع). به هر حال توسعهٔ فناوری، تهدیدها و فرصت‌های جدیدی ایجاد می‌کند؛ چرا که قابلیت‌های جدیدی برای دشمنان بالقوه فراهم می‌کند و از طرفی تغییرات فنّاورانهٔ گنجانده شده در مفاهیم عملیاتی جدید می‌توانند اثربخشی دفاعی دشمنان بالقوه و همچنین قابلیت‌های نیروهای مسلح را به میزان زیادی تغییر دهند. این تغییر می‌تواند به صورت تدریجی یا سریع روی دهد و موجب کاهش هزینه‌های دفاعی و افزایش اثربخشی نیروهای مسلح شود و یا خطرهایی از قبیل منسوخ شدن تجهیزات نیروهای مسلح ایجاد کند (فولادی، ۱۳۹۵).

شایان ذکر است که دانش علمی و فناوری‌های نوظهور حاصل از آن به‌سرعت در حال گسترش است و مطالعه آن می‌تواند طیف وسیعی از راه‌حل‌های مواجهه با تهدیدات متغیر را در اختیار قرار دهد. پیش‌بینی و کسب آمادگی جهت مواجهه با چالش‌های پیش‌رو از طریق نوآوری، انعطاف و سرعت عمل در رویکردهای دفاعی در معیت بهره‌برداری سریع برای رسیدن به یک برتری نظامی بسیار ضروری می‌نماید. پیشرفت در تکنولوژی نظامی، کماکان یک شرط لازم در حفظ امنیت ملی است که با تکیه بر بهره‌مندی از فناوری‌های نوظهور که می‌تواند بنیان توانمندی‌های فنی آینده را تشکیل دهد بیش از پیش محقق می‌گردد. لذا با توجه به اهمیت بالای فناوری‌های اطلاعاتی نوپدید، پیش‌بینی روندها و همچنین تغییرات در این عرصه برای اثربخشی قابلیت‌های دفاعی مختلف حیاتی است و لذا ارزیابی و پایش فناوری در سطوح مختلف تکنیکی، تاکتیکی و راهبردی به عنوان یکی از مؤلفه‌های اصلی طرح‌ریزی دفاعی بلندمدت در کشورهای پیشرفته است. از این‌رو، سازمان‌های دفاعی و نظامی باید بهترین شیوه‌ها را برای پایش و رصد گونه‌های مختلف فناوری اطلاعات اتخاذ کنند. بنابراین، رمز تحول‌آفرینی موفقیت‌آمیز، شناسایی و سرمایه‌گذاری صحیح در فناوری‌های اطلاعاتی نوظهور به منظور کسب منفعت کامل از این فناوری‌ها در جنگ شبکه‌محور و خلق هم‌افزایی در تمامی مراحل توسعه است. در این میان نقش اتاق‌های فکر و متخصصان و نخبگان نظامی در رصد فناوری‌های اطلاعاتی نوپدید بسیار برجسته است. در این مقاله هدف این است که از طریق مراجعه به دیدگاه خبرگان حوزه دفاعی و متخصص؛ فناوری‌های اطلاعاتی نوظهور در بخش دفاعی-نظامی شناسایی و رتبه‌بندی شوند. از طرفی، سرمایه‌گذاری در حوزه فناوری‌های

[1]. South African Defense Review-2015

نوظهور و گسیل منابع به سمت آنها، مستلزم شناخت ماهیت فناوری‌ها از نظر عملیاتی، تاکتیکی و راهبردی است که در این تحقیق به آنها پرداخته شده است. بالاخره، روند زمانی تملک فناوری‌های اطلاعاتی موضوعی است که بایستی در دستور کار محافل آینده‌پژوهی کشور قرار بگیرد تا مشخص شود که بخش دفاعی در چه افق زمانی می‌تواند به این فناوری‌ها تسلط کامل داشته باشد.

مبانی نظری پژوهش

هوش مصنوعی و کاربردهای نظامی آن

هوش مصنوعی می‌تواند قابلیت‌های تحرک یگان نظامی را از طریق تشخیص هدف[1]، سیستم‌های سلاح خودکار[2]، ابزارهای حمایتی و برنامه‌ریزی[3] بهبود بخشد. این فناوری در همه زمینه‌های نظامی(زمین، دریا، هوا، فضا، اطلاعات) و در تمام سطوح دفاعی (سیاسی، راهبردی، عملیاتی و تاکتیکی) کاربرد دارد. هوش مصنوعی و ارتباط آن با شبکه جهانی اینترنت، هسته اصلی فناوری اطلاعات در بخش دفاعی تلقی می‌شود. به همین دلیل موضوعی تحت عنوان حاکمیت هوش مصنوعی مطرح شده است که بر متغیرهایی همانند پویایی‌های رقابت نظامی، نابرابری‌های اجتماعی و اقتصادی، آگاهی‌های عامه مردم و پایش تمرکز کرده است (Perry & Uuk, 2019). کاربردهای نوین هوش مصنوعی از داده‌کاوی، رباتیک و پردازش زبان طبیعی فراتر رفته و حیطه‌هایی همانند مراقبت نظامی، شناسایی، ارزیابی تهدید، مین‌گذاری زیر آب، امنیت سایبری، آنالیز هوشمند، فرماندهی و کنترل، و آموزش در بر می‌گیرد (Svenmarck et al, 2018). بنابراین توسعه خط‌مشی‌های دولتی در خصوص چگونگی استفاده از هوش مصنوعی و اثرات بالقوه آن در آینده جوامع، ضروری است. با این حال، علی‌رغم ممکنات قابل تصور برای استفاده از هوش مصنوعی در حوزه نظامی، ریسک‌ها و چالش‌های مختلفی از جمله اعتماد، فقدان شفافیت برای تصمیم‌گیری قابل تصور است. برخی محققان از اعمال رژیم‌های قانونی برای جلوگیری از ظهور هوش مصنوعی مضر حمایت کرده‌اند (Hughes, 2007)؛ در حالی که محققان دیگر از اختصاص پاداش‌های تشویقی برای توسعه امن هوش مصنوعی سخن گفته‌اند (scherer, 2016). کشورهای متخاصم از جمله آمریکا و رژیم صهیونستی در توسعه بعد نظامی هوش مصنوعی و استفاده از آن در کشتار مردم به هیچ قانونی پایبند نبوده و در این میان

---

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

رقابت چین و آمریکا هم در این شاخه از علم بسیار برجسته است. برخی محققان معتقدند که دولت چین در جلوگیری از انتشار ویروس کرونا از ابزارهای هوش مصنوعی جدید برای پایش استفاده کرده است (Yuan, 2020). به هرحال، نیروهای نظامی عصر جدید، احتمالاً دگرگونی تاریخی دیگری را تجربه می‌کنند و آن تاثیر هوش مصنوعی است. این دگرگونی صرفا تغییر قابلیت‌های موجود نیروهای مسلح نیست؛ بلکه تغییر دهنده اساس نیروهای نظامی مشتمل بر آنچه که انجام می‌دهند و چگونگی انجام آن است (Spiegeleire et al., 2017). همچنین در سطح تاکتیکی می‌تواند کنترل خودکار سیستم‌های بدون انسان را به طور موثر انجام دهد. به عبارت دیگر از این فناوری می‌توان در حل چالش‌های لجستیکی، حمایت از بازی‌های جنگ، مکانیزه کردن نبرد از طریق حذف عامل انسانی، بهینه‌سازی و توسعه سرعت سلاح‌ها و تشخیص کلیه پدیده‌های منطقه نبرد اعم از اهداف نظامی و غیر نظامی استفاده کرد (Button, 2017). اما در تمامی زمینه‌های مذکور چالش‌ها و محدودیت‌هایی از جمله ضعف دقّتمندی، ضعف شفافیت، برنامه پیچیده و تفسیرناپذیرِ ماشین و... وجود دارد که بایستی برطرف شوند (Svenmarck et al., 2018). به همین دلیل حوزه هوش مصنوعی خطرناک بوده و اعتماد کافی به این حوزه وجود ندارد. بر اساس جدیدترین مطالعات، نیروی دریایی ایالات متحده در حال گذار از جنگ سکّوپایه به جنگ شبکه‌پایه است. این مفهوم به جای تکیه بر ویژگی‌های خاص خود سکّو، بر حسگرها و سیستم‌های نظارت و مراقبت گروهی از کشتی‌های جنگی، زیردریایی‌ها یا هواپیماها تکیه دارد (قاضی میرسعید، ۱۳۹۷). هوش مصنوعی، زیر شاخه‌های زیادی دارد و در این میان شبکه‌های عصبی مصنوعی به عنوان بخش مهمی از حوزه هوش مصنوعی، یک سیستم رایانه‌ای یا الگوریتمی است که متشکل از نرونهای مصنوعی برای مدل‌سازی مغز انسان و سیستم عصبی است (Svenmarck et al., 2018). شبکه‌های عصبی مصنوعی رشد سریعی در حوزه نظامی به خصوص در کمک به رزم، کشف تهدیدات، ارتقای عملکرد رادار و تشخیص و طبقه‌بندی نویز[1] داشته است (سایت هوافضای آمریکا، ۲۰۲۰). برنامه‌ریزان ارتش آمریکا سعی می‌کنند از شبکه‌های عصبی مصنوعی برای پیوند شبکه سنسورهای هوشمند به مجموعه‌ای از آشکارسازهای ارزان و رایج استفاده کنند. همچنین این فناوری در شبیه‌سازی رزم و سلاح‌ها قابل کاربرد است. بالاخره، واقعیت افزوده[1] به عنوان

[1]. Identify military impulse noise

بخشی از شاخه هوش مصنوعی می‌تواند شکاف مهارتی را در تعمیر و نگهداری از بین برده و امروزه توسط خطوط هوایی بین المللی مورد استفاده قرار می‌گیرد.

اینترنت اشیاء و کاربردهای نظامی آن

هوشمندسازی اشیاء موضوعی است که در سال‌های اخیر مورد توجه قرار گرفته است. در این راستا از اشیاء هوشمند در بستر اینترنت برای کنترل، راحتی، امنیت و صرفه‌جویی منابع استفاده می‌شود. شیء هوشمند، دستگاهی است که دارای قطعه ارتباطی، ریزپردازنده و حسگر با عملگر مخصوص می‌باشد که قابلیت اتصال به شبکه داخلی و حتی اینترنت را دارد. با مطرح شدن موضوع هوشمندسازی، بحث اینترنت اشیاء و امنیت آن بر اساس پروتکل‌های موجود در شبکه اینترنت مورد توجه ویژه‌ای قرار گرفته است (غنمی، ۱۳۹۸). رشد اینترنت اشیاء توسط چهار پیشرفت در فناوری‌های دیجیتال شکل گرفته است: یکی میکروارگانیسم حسگر است که با هزینه اندک ایجاد می‌شود، دیگری فناوری اتصال بی‌سیم و رشد آن است، دیگری افزایش ذخیره‌سازی داده و ظرفیت پردازش سیستم‌های پردازشی و در نهایت، پیشرفت‌های مربوط به یادگیری ماشین که برای پردازش داده‌های بزرگ مناسب است. اینترنت اشیاء به عنوان یکی از شش فناوری دارای پتانسیل تاثیرگذاری بر منافع آمریکا تا سال ۲۰۲۵ تشخیص داده شده است. اینترنت اشیا پیامدهای مهمی در حوزهٔ لجستیک، زنجیره تامین، اتوماسیون صنعتی، حمل و نقل کالاها، ایمنی و البته نظامی دارد (Perwej et al, 2019). یکی از کاربردهای مهم نظامی اینترنت اشیاء، شبیه‌سازی زندهِ نظامی و غلبه بر چالش‌های امنیتی است (Sfar & Challa, 2017). این مفهوم در حوزه نظامی، قابلیت تاکتیکی دارد؛ یعنی هنگامی که جنگاور در منطقه شهری می‌جنگد، امکان اتصال وی به سنسورها میسر می‌شود. شبکه‌های به هم پیوسته‌ای از سنسورها می‌توانند وضعیت اقتصادی، زیرساختی و جمعیت شهر را به جنگاور نشان دهند و او را در ردیابی مکان‌ها یاری رساند. جنبه دیگر اینترنت اشیاء این است که امکان آموزش مردم در جنگ وجود خواهد داشت؛ چرا که امروزه با افزایش سیستم‌های سلاح شبکه‌ای، آموزش در حین نبرد مرسوم بوده و بنابراین شبیه‌سازهای آموزشی بایستی به طور مجازی در اتصال باشند. به هر حال شبیه‌سازهایِ آموزشِ تحت شبکه و ابزارهای یادگیری مجازی در تمامی حوزه‌های خدماتی در حال رشد است. بعلاوه از اینترنت اشیاء در تحلیل اعتمادپذیری، پیش‌بینی شکست، پایش فضای نبرد، آشکارسازی ورودهای غیرقانونی و کنترل مرزهای جغرافیایی استفاده می‌شود (Winkler et al., 2019). اساساً جنگ شبکه‌محور به کلی با

[1]. Augmented reality

موضوع اینترنت اشیاء مرتبط است. الگوی جنگ شبکه‌محور سه حوزه را باهم ترکیب کرده است: حوزه فیزیکی، حوزه اطلاعات و حوزه شناختی. در حوزه فیزیکی، در هنگام رخداد رویدادها و اجرای عملیات، داده‌ها ساخته می‌شوند. در حوزه اطلاعاتی، داده‌ها منتقل و ذخیره‌سازی می‌شوند. در نهایت در حوزه شناختی، داده‌ها مورد پردازش و تحلیل قرارگرفته و در تصمیم‌گیری از آن‌ها استفاده می‌شود. سه حوزه جنگ شبکه محور، مستقیما بر اساس اینترنت اشیاءِ تجاریِ امروزی تفسیر می‌شوند (غلام‌نژاد و همکاران، ۱۳۹۸).

داده‌های بزرگ و کاربردهای نظامی آن

استفاده بلادرنگ و موثر از داده‌های بیشتر و افزایش سرعت انتقال و پردازش داده‌ها در مدیریت عملیات نظامی از حساسیت و جایگاه حیاتی برخوردار بوده و برای کسب برتری نظامی در جنگ‌های آینده ضروری است (هلیلی و همکاران، ۱۳۹۴). به دلیل تنوع و تعدد ابزارهای موجود در صحنه نبردهای امروزی، موضوع تجزیه و تحلیل حجم عظیمی از داده‌ها مطرح می‌شود. به خاطر تنوع و پیچیدگی محیط عملیاتی و استفاده از سامانه‌های ناهمگون، حجم عظیمی از داده‌های ساختاریافته و غیرساختار یافته از این ابزارها در حال تولید و تبادل است. منابع این داده‌ها هم ماشینی است و هم انسانی. منابع ماشینی داده‌ها از تجهیزات مختلفی مانند کشتی‌ها و ناوها، پهپادها، هواپیماها، رادارها، ماهواره‌ها، پرنده‌های ردگیری، حسگرهای بیسیم، به دست می‌آید؛ و منابع انسانی داده‌ها هم از سایتها و شبکه‌های اجتماعی تولید می‌شود. تنها فناوری لازم برای تحلیل این حجم از داده‌ها، همان کلان داده است که البته برخی بسترهای آن مانند نرم‌افزار هادوپ و مپ‌ردیوس در حال شکل‌گیری است. بنابراین می‌توان گفت که در عصر حاضر منابع داده‌های نظامی بسیار متنوع و پیچیده است لذا یکی از مهمترین نقش‌های محوری سامانه‌ها و جنگ‌افزارهای پیشرفته در سازمانهای نظامی، تلاش برای جمع‌آوری هرچه بیشتر اطلاعات و محافظت از اطلاعات حساس در برابر دسترسی غیر مجاز است. سازمانهای نظامی در زمان صلح و جنگ با دریافت اطلاعات و تجزیه و تحلیل مناسب آنها، سعی در شناسایی و واکنش مناسب به این اطلاعات هستند. به عنوان مثال یکی از کاربردهای مهم کلان‌داده در پیش‌بینی فعالیت‌های تبهکارانه و شناسایی و ردگیری تروریسم سایبری است که توسط آژانس امنیت ملی[1] آمریکا از آن برای تامین امنیت ملی استفاده می‌شود. علاوه بر حوزه نظامی، داده‌های ایستگاه‌های هواشناسی، سامانه‌های امواج رادیویی، مبادلات شبکه‌های اجتماعی آنلاین، متون و اسناد اینترنتی، نمایه‌های جست وجوهای

[1]. National security agency

اینترنتی، اطلاعات سامانه‌های خرید و پژوهش‌های زمین‌شناسی نمونه‌هایی از داده‌ها در مقیاس بزرگ هستند که نیازمند استفاده از فناوری‌های مختلف تحلیل کلان داده هستند. همانطور که اشاره شد سازمان‌ها در هر صنعتی که دارای داده‌های حجیم هستند، می‌توانند از تحلیل‌های دقیق خود در کسب بینش و دقیق‌بینی جهت حل مشکلات واقعی نفع ببرند. داده‌های عظیم برای پردازش شدن در یک زمان معقول به نرم‌افزارهای به شدت موازی شده با قابلیت اجرا روی ده‌ها، صدها یا هزاران سرور نیاز دارند.

رایانش ابری و کاربردهای نظامی آن

محاسبات ابری، الگویی برای ایجاد دسترسی آنی و مناسب سازمان‌ها به یک منبع مشترک و قابل تنظیم اطلاعات است. این الگو درشبکه‌ها، سرورها، انبارها و برنامه‌های نرم‌افزاری که به سرعت قابل اصلاح و ارائه هستند و نیاز بسیار کمی به مدیریت و تعامل با شرکت خدمات‌رسانی اینترنتی دارند، قابل اجرا است. شرکت‌ها به جای خرید مجوز نرم‌افزارهای اضافی و سخت‌افزارها برای کارکنان و بخش‌های مختلف خود، می‌توانند به کمک تأمین‌کنندگان خدمات ابری توان محاسباتی خود را افزایش دهند. اما محاسبات ابری خود شامل گسترهٔ وسیعی از خطراتی است که نیازمند مراقبت‌های اضافی و سرمایه‌گذاری در سیستم‌های پیشرفته است؛ سیستم‌هایی که بتوانند به دقت تهدیدهای نوظهور را شناسایی، تحلیل و طبقه‌بندی کند (Premsankar et al., 2018). رایانش ابریِ دفاعی زیرساخت یکپارچه و توزیع‌شده‌ای است که می‌تواند تمامی سازمان‌های دفاعی کشور را با یکدیگر هماهنگ نماید. هدف از حرکت سازمان‌های دفاعی به محیط ابری استفاده از سامانه‌های قدرتمند در محیط شبکه برای کاهش هزینه‌ها و افزایش بهره‌وری و عملکرد می‌باشد. لذا رایانش ابری بر اساس حساسیت سازمانهای دفاعی علاوه بر کاهش هزینه‌های مراکز داده و افزایش بهره‌وری، محیطی یکپارچه را برای این سازمان‌ها ایجاد نماید (Takai, 2012). مهاجرت سازمان‌های دفاعی به محیط رایانش ابری باعث می‌شود تا زیرساخت‌های فناوری اطلاعات این سازمان‌ها در جهت بهره‌برداری حداکثری از اطلاعات و خدمات تغییر کرده و مدل‌های جدیدی برای عرضه خدمات فراهم گردد و خدمات و کارکردهای دفاعی در یک بستر یکپارچه و با حداکثر بهره‌وری بکار گرفته شود. همچنین، استفاده از سامانه‌های یکپارچه ابری باعث افزایش قابلیت دسترسی‌پذیری، کارایی، توسعه‌پذیری و کاهش هزینه‌ها می‌شود. مرکز فناوری اطلاعات وزارت دفاع[1] آمریکا به‌منظور شناسایی فرصت‌ها و مزیت‌هایی که بر اثر استفاده از رایانش ابری فراهم می‌شود، برنامه‌ریزی‌های لازم

[1]. CIO (Chief Information Officer)

برای تبدیل این وزارتخانه از یک حالت تکراری، پرزحمت، طاقت‌فرسا و پرهزینه به یک مجموعه چالاک، امن و کم‌هزینه را انجام داده و پروژه مهاجرت را در دست اقدام دارد. هدف اصلی از رایانش ابری در وزارت دفاع آمریکا پشتیبانی از مأموریت سازمانی در همه مکان‌ها و همه زمان‌ها و بر روی همه تجهیزات دارای هویت در وزارت دفاع است (ولوی و همکاران، ۱۳۹۶). در حوزه رایانش ابری، تاکنون چارچوب‌های معماری امنیتی متنوعی مانند سازمان ملی استاندارد و فناوری، وزارت دفاع، دارپا، آژانس امنیت اطلاعات و شبکهٔ اروپا[1] و اتحادیه امنیت ابری ارائه شده است. تاکنون دو معماری مهم DoDAF و C4ISR که مختص سازمان‌های نظامی هستند، در حال بازتعریف شدن در محیط رایانش ابری هستند. یکی از مهم‌ترین موضوعاتی که باید در ابر حوزه دفاعی به آن توجه ویژه شود قابلیت دسترسی است. از آنجا که فعالیت‌های موجود در ابر دفاعی می‌تواند بحرانی بوده و دارای نقطه پایان زودهنگام باشد، نیاز است سیستم‌ها به طور مستمر فعال بوده و قابلیت پاسخگویی به نیازهای کاربران را داشته باشد (Mazhar et al., 2015).

ارتباط متقابل چهار فناوری اطلاعاتی نوپدید و زیر حوزه‌ها

همانطور که اشاره شد به دلیل افزایش تولید داده‌ها در سطح جهانی و افزایش قدرت محاسباتی برای پردازش داده‌ها، پیشرفت الگوریتم‌های ریاضی، باعث شده است که دو حوزه کلان داده‌ها و هوش مصنوعی در کنار هم قرار گیرند. در تعریفِ قبلیِ کلان داده‌ها از سه "وی"[2] (سرعت، حجم و تنوع) استفاده می‌شد ولی امروزه مشخصه هشت "وی" جایگزین شده است. یعنی سرعت[3]، حجم[4]، ارزش[5]، تنوع[6]، تغییرپذیری[7]، انتشار[8]، چسبندگی[9] و صحت[10] (Mehmood et al., 2019). کلان داده‌های امروز چنان وسیع و پیچیده است که با الگوریتم‌ها و نرم‌افزارهای سنتی قابل مدیریت نیست و در این میان شاخه‌ای از هوش مصنوعی به نام روش یادگیری عمیق[11] (DL) می‌تواند از حجم وسیعی از داده‌ها بهره‌برداری کند. اینترنت اشیاء، تحلیل

1. European Network and Information Security Agency
2. V
3. Volume
4. Velocity
5. Value
6. Variety
7. Ariability
8. Virality
9. Viscosity
10. Veracity
11. Deep learning

داده‌های بزرگ و یادگیری عمیق، در کنار یکدیگر جامعه hi-tech را بوجود می‌آورند (Kumar et al., 2019). بهره‌مندی از هوش مصنوعی در حوزه‌های نظامی بی‌پایان است و از تحلیل‌های برخط، حملات سایبری، آشکارسازی فریب و هدایت خودکار پهباد گرفته تا اشکال جدید کنترل و فرماندهی (مانند سیستم مدیریت خودکار منطقه نبرد) که می‌تواند کلان داده‌ها را تحلیل کرده و توصیه‌هایی ارائه کند (Raska, 2020). با این حال تفاوت‌هایی بین هوش مصنوعی و کلان داده‌ها وجود دارد. کلان داده‌ها در اتخاذ تصمیم بر اساس نتایج عمل نمی‌کنند و صرفا سعی در یافتن نتایج درست دارد، در حالی که هوش مصنوعی به دنبال تصمیم‌گیری و یادگیری برای اتخاذ تصمیم بهتر است. کلان داده‌ها در بادی امر برای کسب بینش مناسب هستند اما هدف هوش مصنوعی تلاش برای انجام وظیفه‌ای است که قبلا انسان انجام می‌داد ولی دقت و کارآیی لازم را نداشت و با خطا همراه بود.

در خصوص ارتباط کلان داده‌ها با رایانش ابری باید گفت که رایانش ابری، نوعی فناوری قدرتمند برای اجرای محاسبات پیچیده و سنگین است که نیاز به استفاده از سخت‌افزارهای گران را حذف نموده، فضای محاسباتی و نرم‌افزار مورد نیاز را در اختیار کاربر قرار می‌دهد. همچنین، رایانش ابری، یک الگوی جدید زیرساخت محاسباتی محسوب می‌شود که روشی مناسب برای پردازش داده‌های حجیم در ابر را فراهم می‌آورد و توسط همه انواع منابعِ در دسترس، قابل استفاده است. بنابراین می‌توان گفت که محاسبات ابری، ارتباط نزدیکی با داده‌های بزرگ دارند؛ داده‌های بزرگ به عنوان هدف عملیات محاسبه فشرده داده‌هاست و بر ظرفیت ذخیره‌سازی یک سیستم ابری تأکید دارد؛ در حالی که هدف اصلی محاسبات ابری، استفاده از محاسبات عظیم و ذخیره منابع تحت مدیریت متمرکز می‌باشد به طوری که برنامه‌های داده‌های بزرگ را با ظرفیت محاسباتی تفصیلی، ارائه می‌کند. به طور کلی توسعه محاسبات ابری، راه‌حل‌هایی را برای ذخیره‌سازی و پردازش داده‌های بزرگ ارائه می‌نماید. از سوی دیگر، ظهور داده‌های بزرگ نیز به توسعه محاسبات ابری سرعت می‌بخشد (حبیبی، ۱۳۹۶). بنابراین می‌توان گفت که هم BD و هم IoT با جمع‌آوری داده‌ها ارتباط دارند. با این حال تفاوت‌هایی همانند منبع داده و قیود زمانی دارند. در خصوص ارتباط هوش مصنوعی و اینترنت اشیاء باید گفت که این دو حوزه به طور نزدیکی با هم ارتباط متقابل دارند. هنگامی که صدها و هزاران ماشین که در قالب شبکه‌های صنعتی باهم کار می‌کنند، تحلیل کوهی از داده‌های خلق شده توسط این ماشین‌ها خارج از توانایی انسان است (Nigania, 2019). در اینجا الگوریتم‌های یادگیری ماشینی می‌توانند از فرصت کارآیی استفاده کرده و هشدارهای لازم را در خصوص مسائل نوپدید بدهند. این وظیفه اولیه هوش مصنوعی در محیط اینترنت

اشیاء تلقی می‌شود. به موازات رشد شبکه‌های اینترنت اشیاء از نظر اندازه و پیچیدگی، آن‌ها به طور فزآینده به هوش مصنوعی و یادگیری ماشینی وابسته‌اند (Marr, 2019).

بالاخره، رایانش ابری تسهیل‌کننده سیستم‌های اینترنت اشیاء از طریق افزودن به قدرت ذخیره‌سازی و پردازش داده‌ها است. در حقیقت دو معماری رایج در عرصه اینترنت اشیاء عبارت‌اند از محاسبات ابری و محاسبات مه[1] که از تحلیل و مدیریت حجم وسیعی از داده‌ها در سیستم‌های اینترنت اشیاء حمایت می‌کنند (Kumar et al., 2019). کاهش هزینه سازمان بعد از اجرای اینترنت اشیا در حوزه مدیریت مهم است. استفاده بهینه از سرمایه پولی سازمان مستلزم این است که اینترنت اشیا مبتنی بر ابر اداره شود. چنانچه سامانه‌های رایانش ابری به صورت استیجاری مورد استفاده قرار گیرند عملا این فناوری هزینه کلانی را به سازمان تحمیل نمی‌کند و کاهش هزینه‌های جانبی سازمان را در بر خواهد داشت غلام‌نژاد و همکاران، ۱۳۹۸).

مبانی تجربی پژوهش

سایت کسب و کار مبتنی بر فناوری اطلاعات[2] آمریکا در سال ۲۰۲۰، ده روندِ محرکِ فناوری اطلاعات آینده را معرفی کرده است که عبارت‌اند از معماری پلتفورم، پلتفورم‌های اجتماعی، رایانش ابری، امنیت داده‌ها، محرمانگی داده‌ها، علم تجزیه و تحلیل، معماری و تجربه کاربر. همچنین سایت ویستاکالگ در سال ۲۰۱۹ روندهای جاری فناوری اطلاعات را به ترتیب در کلمات ذیل خلاصه کرده است: رایانش ابری، محاسبات موبایل و کاربردها، تحلیل‌های کلان داده و اتوماسیون. همچنین این سایت روندهای نوپدید فناوری اطلاعات در سال ۲۰۱۹ را به ترتیب در شش طبقه ذیل معرفی کرده است: هوش مصنوعی و ماشین‌های هوشمند، واقعیت مجازی، واقعیت افزوده، داده‌های بلاکچین[3]، امنیت و محرمانگی سایبری[4] و اینترنت اشیاء. بالاخره این سایت در اهمیت نیروی انسانی مورد نیاز برای کار با فناوری‌های اطلاعاتی نوپدید و کاهش ریسک‌های این حوزه به موضوع کار راهه شغلی فناوری اطلاعات اشاره کرده است و معتقد است که نهضت فناوری اطلاعات نوین نیازمند کارکنانی است که آموزش‌های لازم را برای نوآوری در عرصه داده‌کاوی و محاسبات ابری را داشته باشند. در راستای این مطالعات، سازمان‌های نظامی هم کاربردهای این فناوری‌ها را در بخش‌های مختلف خود بررسی کرده‌اند که به برخی از آن‌ها اشاره می‌شود:

---

1. Cloud and fog/edge computing
2. Itbusinessedg
3. Blockchain Data
4. Cyber-Privacy and Security

❖ راسکا[1](۲۰۲۰) در مقاله خود با عنوان" رقابت‌های استراتژیک برای فناوری‌های نظامی نوپدید" به مقایسه تطبیقی چین، آمریکا و روسیه پرداخته است. این محقق معتقد است که چین به دنبال کسب مزیت نظامی از فناوری‌های نوپدید از قبیل ارتباطات و محاسبات کوانتومی، وسایل فراصوت، هوش مصنوعی،کاربردهای کلان داده، محاسبات ابری، پرینت سه بعدی، غیرمادی‌ها و بیوتکنولوژی است. به اعتقاد این محقق چین با این فناوری‌ها، یک پایگاه صنعتی-نظامی مدرنی ایجاد کرده است که می‌تواند همگرایی فناوری‌های صنعتی و نظامی را تقویت کند. کشور روسیه هم مشابه چین اقدامات فناورانه را در دستور کار قرار داده است که در این میان اتکا به سلاح‌های هسته‌ای در برابر آمریکا بسیار قابل توجه است. همچنین روسیه ضمن توجه به نیروهای راهبردی هوافضای خود، به وسایل بازگشتی مافوق صوت[2] تمرکز کرده است. این کشور مشابه آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی آمریکا (DARPA)، یک بنیاد تحقیقاتی پیشرفته برای رصد فناوری‌های پر ریسک همانند وسایل مافوق صوت، هوش مصنوعی، اشیاء زیرآبی بدون سرنشین، فناوری‌های شناختی و سلاح‌های هدایت انرژی[3]تاسیس شده است. بالاخره، آمریکا به فناوری‌هایی که می‌توانند سازه‌های عملیاتی و سازمانی را تقویت کند تمرکز کرده است. لذا این کشور به دنبال تقویت سطح عملیاتی جنگ از طریق چابک‌سازی نهادی است. همچنین تمرکز بر فناوری سایبری و تقویت بخش خصوصی با هدف تبدیل فناوری‌های تجاری به نظامی از اولویت‌های آمریکا است. این کشور به دنبال تقویت ماشین‌های یادگیرنده، یکپارچه‌سازی حوزه هوش مصنوعی با خودکارسازی برای کسب مزیت، جنگ الکترونیک، حمله سایبری، همکاری انسان-ماشین، بصری‌سازی رایانه‌ای برای کمک به تصمیمات بهتر و سریع‌تر، سلاح‌های خودکار و مبتنی بر شبکه و پلتفرم‌های بدون انسان و با انسان است.

❖ چاین[4](۲۰۱۹) در مطالعه خود با عنوان:"*تکنولوژی، جنگ و دولت:گذشته، حال و آینده*" معتقد است که دولت آمریکا بعد از آغاز جنگ سرد، بودجه تحقیقات دفاعی خود را با فناوری‌های نوپدید، همراستا کرده است. این فناوری‌ها عبارت‌اند از: اینترنت،

---

1. Raska
2. Hypersonic reentry vehicles
3. Directed energy weapons
4. Chin

واقعیت مجازی، سفر جت، اشتراک داده‌ای[1]، تلویزیون مدار بسته، موقعیت‌یابی جهانی، فناوری پرتاب موشک،کنترل از راه دور، مایکروویو، رادار، ارتباطات بی‌سیم و مراقبت ماهواره‌ای.

- اسپگلیر[2]، ماس[3] و اسویجز[4](۲۰۱۷) در مرکز مطالعات راهبردی هیگ[5] کاربردهای استراتژیک هوش مصنوعی را در آینده سازمانهای نظامی به تفصیل بررسی کرده‌اند. در این مطالعه به مواردی مانند بازی جنگ، ارتقاء لجستیک، پایش ماهواره‌ها و سفینه فضایی، رباتیک، مدیریت ترافیک، کشتی‌ها و زیردریایی، خودکارسازی وسایل نقلیه و... اشاره شده است.
- بیکر و همکاران[6](۲۰۱۳) با همکاری شرکت آم آی‌تی‌آرای[7] کاربردهای اولیه کلان داده‌ها را در قالب مطالعه موردی در ارتش آمریکا بررسی کرده‌اند. نتایج این مطالعه، کاربردهای اولیه کلان داده‌ها در ارتش را تایید کرده است. در این مطالعه کلان داده‌های مربوط به امکانات نظامی، محل استقرار سربازان، خدمات درمانی، در سه بعد سرعت انتقال، حجم و تنوع بررسی شده است.

در جدول (۱) خلاصه‌ای از کاربردهای فناوری‌های اطلاعات نوظهور در بخش دفاعی و غیر دفاعی ارائه شده است.

1. data joining
2. Spiegeleire
3. Maas
4. Sweijs
5. The Hague Centre for Strategic Studies
6. Becker et al
7. The MITRE Corporation

جدول (۱) جمع‌بندی کاربردهای فناوری اطلاعات نوپدید(یافته‌های تحقیق)

نوع فناوری	کاربردهای غیر نظامی	کاربردهای دفاعی- نظامی	منبع
هوش مصنوعی و شاخه‌های آن	صرفه‌جویی در انرژی، آسایش زندگی، کاربرد سیستمهای هوشمند در افزایش بهره‌وری اقتصادی و خلق ثروت. کشف جرم، تشخیص چهره به صورت خودکار، مراقبت‌های بهداشتی و اجتماعی	صرفه اقتصادی پهپادها و دفاع حملات سایبری، داده‌کاوی، رباتیک و پردازش زبان طبیعی فراتر رفته و حیطه‌هایی همانند مراقبت نظامی، شناسایی، ارزیابی تهدید، مین‌گذاری زیر آب، امنیت سایبری، آنالیز هوشمند، فرماندهی و کنترل، و آموزش، کنترل و رصد بیماری، می‌تواند قابلیت‌های تحرک یگان نظامی را از طریق تشخیص هدف، سیستم‌های سلاح خودکار، ابزارهای حمایتی و برنامه‌ریزی، حل چالش-های لجستیکی، حمایت از بازی‌های جنگ، مکانیزه کردن نبرد از طریق حذف عامل انسانی، بهینه‌سازی و توسعه سرعت سلاح‌ها و تشخیص کلیه پدیده‌های منطقه نبرد، کمک به رزم، کشف تهدیدات، ارتقای عملکرد رادار و تشخیص و طبقه‌بندی نویز، شبیه-سازی رزم و سلاح‌ها، کشف شکاف مهارتی در تعمیر و نگهداری، تحلیل‌های برخط، حملات سایبری، آشکارسازی فریب و هدایت خودکار پهپاد، جنگ الکترونیک، حمله سایبری، همکاری انسان-ماشین، بصری‌سازی رایانه‌ای برای کمک به تصمیمات بهتر و سریع‌تر، سلاح‌های خودکار و مبتنی بر شبکه، پلتفرم-های بدون انسان و با انسان، بازی جنگ، ارتقاء لجستیک، پایش ماهواره‌ها و سفینه فضایی، رباتیک، مدیریت ترافیک، کشتی‌ها و زیردریایی، خودکارسازی وسایل نقلیه،	Mehmood,2019, Perry & Uuk,2019, Spiegeleire,2017, Johannsen, solka & rigsby,2018
کلان داده‌ها	بهینه‌سازی عملیاتی، هوش عملی، پیش بینی‌های دقیق، عیب‌یابی خرابی و تقلب، بهبود تصمیم‌گیری،اکتشافات علمی، ساخت شهر هوشمند، حمل و نقل هوشمند، بهداشت و درمان هوشمند، دولت هوشمند، کتابخانه، کمک شفافیت، ارتقای عملکرد سازمانی، تقسیم بندی مشتریان، یافتن بازارهای جدید، ایجاد فرصت‌های شغلی، هواشناسی، تجارت و بورس، تحلیل‌های امنیتی و سیاسی، صرفه جویی در انرژی، آسایش زندگی.	بهینه‌سازی کارآیی تجهیزات، هدایت نیروها، کنترل ماشین هوشمند بدون سرنشین، مدل‌سازی و پیش‌بینی، کسب دانش و بینش نظامی، افزایش توان عملیاتی، کمک به تصمیمات راهبردی، تحلیل داده های مربوط به امکانات نظامی، محل استقرار سربازان، خدمات درمانی، عملیات ضد تروریستی، تدارکات نظامی، توسعه فناوری نظامی، پزشکی قانونی نظامی، سامانه های اطلاعاتی جغرافیایی، تصویر عملیاتی مشترک، تصمیم سازی نظامی، توسعه هوش نظامی	دره‌مند و همکاران، ۱۳۹۷؛ هلیلی و همکاران، ۱۳۹۴ Mehmood,2019, Becker et al,2013

نوع فناوری	کاربردهای غیر نظامی	کاربردهای دفاعی- نظامی	منبع
اینترنت اشیاء	لجستیک، زنجیره تامین، اتوماسیون صنعتی، حمل و نقل، ایمنی، شهر هوشمند، کنترل ترافیک، امنیت عمومی، کشف خطا، مکان‌یابی، پایش برخط، کشتی‌رانی و دریانوری، نظارت بر انرژی در کارخانه، ایمنی کارگران.	شبیه‌سازی زندهِ نظامی و غلبه بر چالش‌های امنیتی، تامین مالی الکترونیکی، کمک به آموزش حین نبرد، تحلیل اعتمادپذیری، پیش‌بینی شکست در جنگ، پایش فضای نبرد، آشکارسازی ورودهای غیرقانونی به منطقه خودی، کنترل مرزهای جغرافیایی، هوافضا	Winkler et al,2019 Sfar,2017 Perwej et al,2019, Sfar & Challa,2017
رایانش ابری	ذخیره‌سازی و پردازش داده‌های زیاد، ساخت شهر هوشمند، محاسبات نرم افزاری دستگاه‌های نظارتی، دستگاه‌های ذخیره‌سازی، استفاده حداکثری از منابع سیستم‌ها، کاهش هزینه‌ها.	افزایش انعطاف‌پذیری، چابکی و صرفه‌جویی، بهره-وری، ذخیره‌سازی داده‌ها، کمک به ابزارهای تحلیل پلتفرم‌های بصری‌سازی، یکپارچگی زیرساخت فناوری	Takai,2012 Mazhar et al,2015

روش‌شناسی پژوهش

این پژوهش از لحاظ جهت‌گیری، کاربردی و از لحاظ هدف، اکتشافی است. از نظر ماهیت پژوهش نیز از رویکرد کیفی برای دستیابی به نتایج استفاده شده است. ابزار اصلی این پژوهش، منابع کتابخانه‌ای، داده‌های میدانی و روش دلفی است.

شرکت‌کنندگان در تحقیق دلفی از ۵ تا ۲۰ نفر را شامل می‌شوند. معمولاً پژوهش دلفی با یک پرسشنامه که توسط محقق طراحی شده و به گروهی از متخصصان فرستاده می‌شود آغاز می‌شود. پرسشنامه‌ها به طریقی تنظیم می‌شوند که این امکان به وجود آید تا مخاطبین ضمن استنباط کردن و فهمیدن مساله مطرح شده، واکنش‌های فردی خود را بروز دهند. وقتی پرسشنامه‌ها برگشت داده شد، طیف پاسخ‌ها و دلایلی که متخصصان برای پاسخ‌هایشان بیان کرده‌اند مورد بررسی قرار گرفته و تلخیص می‌شوند. برای اطمینان از ادامه یا توقف راندهای دلفی، روش‌های مختلفی وجود دارد. زائو و همکاران[1] (۲۰۰۳) معتقدند که برای پایان دادن به راندهای تکنیک دلفی می‌توان از ضریب هماهنگی کندال استفاده کرد. به همین دلیل در این پژوهش برای تعیین میزان توافق جمعی خبرگان، از ضریب هماهنگی کندال استفاده شده است. ضریب کندال بین ۰ و ۱ متغیر است. اگر ضریب کندال صفر باشد یعنی عدم توافق کامل و اگر یک باشد یعنی توافق کامل وجود دارد. تعداد خبرگان این تحقیق نه نفر از نخبگان آجا و دارای درجه سرهنگی در رشته فناوری اطلاعات بوده به گونه‌ای که پایان‌نامه کارشناسی ارشد و دکتری ایشان در حوزه مدیریت فناوری اطلاعات و مدیریت دانش بوده است.

1. Zhao

جدول (۲) اطلاعات پنل دلفی

ردیف	خبره	علت انتخاب
۱	خبره ۱	دکترای IT (دولت الکترونیک)
۲	خبره ۲	تالیف ۶۰ مقاله و ۱۰ عنوان کتاب در عرصه مدیریت دانش و IT
۳	خبره ۳	مسئولیت در حوزه فاوای آجا و رساله دکتری در حوزه رایانش ابری
۴	خبره ۴	دکترای اطلاعات و دانش‌شناسی
۵	خبره ۵	انجام پایان نامه ارشد و دکتری در حوزه IT
۶	خبره ۶	رسته رایانه و رساله دکتری در حوزه مدیریت دانش
۷	خبره ۷	دکترای IT و پایان‌نامه ارشد و دکتری در حوزه مدیریت دانش و IT
۸	خبره ۸	دکترای IT و صاحب نظر در عرصه دفاعی
۹	خبره ۹	دکترای IT و انجام رساله دکتری در حوزه ITIL

تجزیه و تحلیل داده‌ها

یافته‌های تحقیق در دور اول دلفی

اجرای روش دلفی فازی بر اساس مطالعات (فرتاش و همکاران، ۱۳۹۵) به صورت ذیل است: گام نخست انتخاب خبرگان و تشریح مسائل ۲) تهیه پرسشنامه و ارسال آن به خبرگان ۳) دریافت نظر خبرگان و تجزیه و تحلیل آن‌ها ۴) طبقه‌بندی پاسخ‌ها و اعلام توافقات ۵) آیا اجماع به خوبی صورت گرفته است؟ و در نهایت در گام آخر به تهیه گزارش از فرایند دلفی و تحلیل آن می‌پردازیم.

روش دلفی به عنوان یک ابزار کارا برای تعیین موضوعات مهم و اولویت‌بندی توصیفی عوامل در تصمیم‌های مدیریتی شناخته می‌شود. در مرحلهٔ نخست فناوری‌های اطلاعاتی از متون و مقالات نظامی استخراج و در قالب پرسشنامه طیف لیکرت در اختیار خبرگان قرار گرفت تا در طیف ۵ گزینه‌ای میزان قابلیت کاربرد آتی آن‌ها را تعیین کنند. همچنین فناوری‌های اطلاعاتی جدیدی که مد نظر ایشان است را در پرسشنامه اضافه کنند تا در راند بعدی، نظر کلیه خبرگان راجع به فناوری‌های جدید پرسیده شود. از میان ۲۳ عامل ذکر شده در پرسشنامه اول ۲۲ عامل دارای میانگین ۴ و بالاتر بوده‌اند و ۱ عامل میانگین کمتر از ۴ را بدست آورد و این عامل (تولید افزوده) در این مرحله از پرسشنامه حذف شد. برای تعیین میزان اتفاق نظر میان اعضای پانل در نتایج دور اول دلفی، از ضریب هماهنگی کندال استفاده شده است با اجرای آزمون دبلیو کندال ضریب **w** برابر با ۰/۴۳ حاصل شد. نتیجه دور اول دلفی در جدول (۳) ارائه شده است.

جدول (۳) نتایج میزان توافق دور اول دلفی

N	۹
Kendall's W(a)	./۴۳۵
Chi-Square	۲۰۱/۱۹۵
df	۲۳
Asymp. Sig.	۰/۰۰۰

جدول (۴) نتایج پرسشنامه دور اول دلفی

ردیف	فناوری‌های اطلاعاتی نوظهور	میانگین	انحراف معیار	میانگین رتبه	اهمیت بر اساس میانگین رتبه
۱	هوش مصنوعی	۵	۰	۱۵/۸۶	۱
۲	اینترنت اشیاء	۴/۸۶	./۳۷	۱۴/۷۱	۲
۳	داده‌های بزرگ	۴/۲۸	./۹۵	۱۰	۹
۴	واقعیت مجازی	۴/۴۲	./۵۳	۹/۹۳	۱۲
۵	واقعیت‌افزوده	۴/۲۸	./۴۸	۸/۳۶	۱۱
۶	وسایل فراصوت	۴/۴۲	./۷۸	۱۰/۵۷	۸
۷	رایانش ابری	۴/۱۴	./۸۹	۸/۷۹	۱۳
۸	رایانش مه و لبه	۴	./۸۱	۷/۴۳	۱۶
۹	محاسبات کوانتومی	۴/۷۱	./۷۵	۱۳/۶۴	۲
۱۰	ماشین یادگیری	۴/۲۸	./۴۸	۸	۱۵
۱۱	رباتیک	۵	./۰۱	۱۵/۸۶	۱
۱۲	فناوری بلاکچین	۴	۱	۸/۳۶	۱۴
۱۳	سلاح‌های هدایت انرژی	۴/۵۷	./۵۳	۱۱/۵۷	۷
۱۴	ارتباطات نوری مرئی	۴/۵۷	./۷۸	۱۲/۷۱	۵
۱۵	شبکه‌های عصبی مصنوعی	۴/۷۱	./۴۸	۱۲/۵۸	۶
۱۶	یادگیری عمیق	۵	۰	۱۵/۸۶	۱
۱۷	مواد هوشمند	۴/۷۱	./۴۸	۱۳/۰۷	۴
۱۸	پرنده‌های بدون سرنشین	۵	۰	۱۵/۸۶	۱
۱۹	تولید افزوده	۳/۷۱	./۹۵	۶/۳۶	۱۷
۲۰	سیستم های ارتقای سرباز	۵	۰	۱۵/۸۶	۱
۲۱	ظهور و بروز الکترو مغناطیس	۴/۷۱	./۴۸	۱۳/۲۱	۳
۲۲	استفاده از سنسورهای پیشرفته	۴/۷۱	./۴۸	۱۲/۷۱	۵
۲۳	فناوری‌های جنگ سایبری	۴/۸۵	./۳۷	۱۴/۷۱	۲

یافته‌های تحقیق در دور دوم دلفی

بر اساس یافته‌های دور دوم، میانگین، انحراف معیار، و میانگین رتبه تعداد ۲۴ فناوری مشخص شد. بر اساس جدول شماره ۴، فناوری‌های رایانش ابری، رایانش مه و لبه و همچنین فناوری بلاکچین دارای پائین‌ترین میانگین و رتبه هستند. همچنین برای بررسی روایی، از نظر خبرگان (عمدتا خبرگان شاغل در صنایع دفاعی کشور)، استفاده شده است. اما بر اساس نظر ایشان، فناوری هوش مصنوعی، فناوری جاسوسی به عنوان مهمترین فناوری در آینده بخش دفاعی کاربرد خواهند داشت. برای ادامه یا توقف فن دلفی، از آزمون کندال استفاده شد که مقدار این آزمون ۰/۵۹ حاصل شد که نشان‌دهنده توافق متوسط است.

جدول (۵) نتایج میزان توافق دور دوم دلفی

N	۹
Kendall'sW(a)	۰/۵۹۱
Chi-Square	۱۲۷/۶۷۰
df	۲۶
Asymp. Sig.	۰/۰۰۰

جدول (٦) نتایج پرسشنامه دور دوم دلفی

ردیف	فناوری‌های اطلاعاتی نوظهور	میانگین	انحراف معیار	میانگین رتبه	اهمیت بر اساس میانگین رتبه
۱	هوش مصنوعی	۵	۰	۱۸/۶۲	۱
۲	اینترنت اشیاء	۴/۹۲	./۲۷	۱۷/۸۱	۲
۳	داده‌های بزرگ	۴/۶۱	./۷۶	۱۵/۱۲	۱۲
۴	واقعیت مجازی	۴/۳۸	./۵	۱۱/۳۱	۱۵
۵	واقعیت‌افزوده	۴/۲۳	./۴۳	۹/۳۸	۱۹
۶	وسایل فراصوت	۴/۳۰	./۴۸	۱۰/۱۹	۱۸
۷	رایانش ابری	۳/۴۶	./۵۱	۳/۸۱	۲۲
۸	رایانش مه و لبه	۳/۶۱	./۵۰	۴/۶۲	۲۱
۹	محاسبات کوانتومی	۴/۶۹	./۶۳	۱۵/۳۸	۱۱
۱۰	ماشین یادگیری	۴/۳۸	./۵۰	۱۱/۱۵	۱۶
۱۱	رباتیک	۴/۸۴	./۳۷	۱۶/۸۵	۵
۱۲	فناوری بلاکچین	۳/۰۷	./۲۷	۱/۸۸	۲۳
۱۳	سلاح‌های هدایت انرژی	۴/۸۴	./۳۷	۱۶/۷۷	۷

ردیف	فناوری‌های اطلاعاتی نوظهور	میانگین	انحراف معیار	میانگین رتبه	اهمیت بر اساس میانگین رتبه
۱۴	ارتباطات نوری مرئی	۴/۵۳	./۵۱	۱۳/۱۲	۱۴
۱۵	شبکه‌های عصبی مصنوعی	۴/۸۴	./۳۷	۱۶/۸۱	۶
۱۶	یادگیری عمیق	۴/۷۶	./۴۳	۱۵/۷۳	۱۰
۱۷	مواد هوشمند	۴/۸۴	./۳۷	۱۶/۹۲	۴
۱۸	پرنده‌های بدون سرنشین	۴/۹۲	./۲۷	۱۷/۷۳	۳
۱۹	سیستم های ارتقای سرباز	۴/۳۰	./۴۸	۱۰/۳۵	۱۷
۲۰	ظهور و بروز الکترو مغناطیس	۴/۶۹	./۴۸	۱۴/۹۲	۱۳
۲۱	استفاده از سنسورهای پیشرفته	۴/۹۲	./۲۷	۱۷/۷۳	۳
۲۲	فناوری‌های جنگ سایبری	۴/۹۲	./۲۷	۱۷/۸۱	۲
۲۳	شبکه‌های اجتماعی هوشمند	۴	۰	۶/۶۵	۲۰
۲۴	سلاح‌های لیزری خودکار	۵	./۴۳	۱۵/۸۵	۹
۲۵	فناوری جاسوسی	۵	۰	۱۸/۶۲	۱
۲۶	فناوری پوشیدنی	۴/۷۶	./۴۳	۱۵/۸۸	۸

یافته‌های تحقیق در دور سوم دلفی

در این مرحله از دلفی هم شرط میانگین بالاتر از ۴ انتخاب شد. در این مرحله از دلفی فناوری های پوشیدنی دارای میانگین پائینی می‌باشد. برای تعیین میزان اتفاق نظر میان اعضای خبرگان نتایج دور سوم دلفی نیز از ضریب هماهنگی کندال استفاده شده است. لذا با اجرای آزمون دبلیو کندال ضریب **W** برابر با ۰/۶۶۱ می‌باشد. با توجه به آنکه مقدار ضریب توافق در حد قابل قبول و حد میانگین متوسط و قوی است (**W**=۰/۶۶۱). لذا ادامه اجرای دلفی متوقف شد.

جدول(۷) نتایج میزان توافق دور سوم دلفی

N	۹
Kendall'sW(a)	۰/۶۶۱
Chi-Square	۲۱/۹۰۳
df	۳۲
Asymp. Sig.	۰/۰۰۰

جدول (۸) نتایج پرسشنامه دور سوم دلفی

ردیف	فناوری‌های اطلاعاتی نوظهور	میانگین	انحراف معیار	میانگین رتبه	اهمیت بر اساس میانگین رتبه
۱	هوش مصنوعی	۴/۹۰	./۲۰	۱۸/۴۰	۱
۲	اینترنت اشیاء	۴/۸۰	./۱۳	۱۷/۷۳	۲
۳	داده‌های بزرگ	۴/۶۷	./۴۰	۱۶/۳۳	۳
۴	واقعیت مجازی	۴/۶۷	./۱۷	۱۶/۲۷	۴
۵	واقعیت‌افزوده	۴/۶۰	./۲۶	۱۵/۶۳	۵
۶	وسایل فراصوت	۴/۴۷	./۳۲	۱۴/۳۳	۶
۷	محاسبات کوانتومی	۴/۴۵	./۳۲	۱۴/۲۷	۷
۸	ماشین یادگیری	۴/۴۰	./۴۱	۱۳/۶۰	۸
۹	رباتیک	۴/۳۶	./۳۶	۱۳/۴۷	۹
۱۰	فناوری جاسوسی	۴/۲۷	./۲۵	۱۲/۲۳	۱۰
۱۱	سلاح‌های هدایت انرژی	۴/۳۳	./۳۲	۱۲/۸۳	۱۱
۱۲	ارتباطات نوری مرئی	۴/۳۰	./۰۲	۱۲/۷۷	۱۲
۱۳	شبکه‌های عصبی مصنوعی	۴/۲۷	./۱۱	۱۲/۱۷	۱۳
۱۴	یادگیری عمیق	۴/۲۰	./۲۱	۱۱/۵۳	۱۴
۱۵	مواد هوشمند	۴/۲۰	./۳۶	۱۱/۵۳	۱۵
۱۶	سلاح های لیزری خودکار	۴/۲۰	./۲۹	۱۱/۴۷	۱۶
۱۷	سیستم های ارتقای سرباز	۴/۳۳	./۳۵	۱۰/۸۷	۱۷
۱۸	ظهور و بروز الکترو مغناطیس	۴/۲۲	./۱۹	۱۰/۸۳	۱۸
۱۹	استفاده از سنسورهای پیشرفته	۴/۲۰	./۲۱	۹/۴۵	۱۹
۲۰	فناوری‌های جنگ سایبری	۴/۱۸	./۳۰	۹/۳۲	۲۰
۲۱	شبکه‌های اجتماعی هوشمند	۴/۰۸	./۴۱	۵/۹۰	۲۱
۲۲	پرنده‌های بدون سرنشین	۴/۰۱	./۷۰	۴/۷۳	۲۲
۲۳	فناوری پوشیدنی	۳/۰۹	./۷۲	۴/۰۸	۲۳

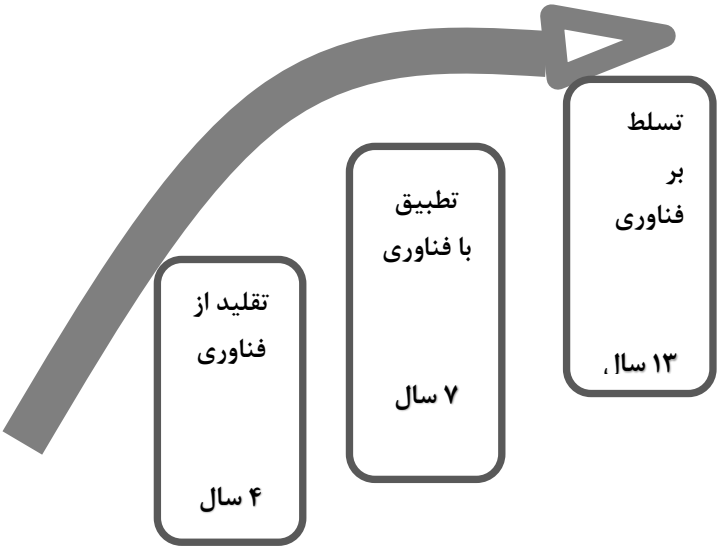
روند تملک فناوری‌ها در بخش دفاعی

در مرحله دوم از خبرگان درخواست شد تا بازه زمانی تسلط کامل بخش دفاعی ایران بر این فناوری‌ها را مشخص کنند. لذا از ایشان درخواست شد تا مشخص کنند که بخش دفاعی ایران در حال حاضر نسبت به فناوری‌ها کدام یک از حالت‌های تقلیدی (منظور از تقلید، درک اولیه و

حداقلی از دانش فنی و تلاش در جهت جذب فناوری است)، تطبیقی (انطباق با شرایط محلی و تطبیق سخت‌افزارها از طریق تحقیق بر روی مواد، فرایندها و...) و یا تسلط (پیشگام شدن در یک فناوری و ایجاد نوآوری) را دارد. به عبارت دیگر خبرگان مدت زمان لازم را (بر حسب سال) برای تقلید از فناوری‌ها، تطبیق و سازگاری با فناوری‌ها و تسلط کامل بر فناوری‌ها را مشخص کردند. به طور متوسط زمان لازم برای تقلید از فناوری‌های اطلاعاتی نوظهور، ۴/۱۲ سال؛ زمان لازم برای تطبیق(سازگاری) با فناوری‌ها، ۷/۱۸ سال و نهایتا زمان لازم برای تسلط کامل به فناوری‌ها و ایجاد نوآوری در این عرصه ۱۲/۷۳ سال می‌باشد. درجدول (۵) و نمودار (۱)، میانگین امتیازات ۲۶ فناوری نوظهور در سه دوره تقلید، تطبیق و تسلط آورده شده است.

جدول (۹) میانگین نمرات خبرگان به تملک فناوری‌ها

خبرگان	تقلید از فناوری	تطبیق با فناوری	تسلط بر فناوری
خبره۱	۱/۲۶	۳/۱۳	۶/۶۹
خبره۲	۰/۴۷	۲/۱۷	۶/۳۰
خبره۳	۵/۵۲	۱۳/۴۷	۲۲/۳۹
خبره۴	۶	۴/۱۰	۱۵
خبره۵	۶/۰۴	۹/۷۱	۱۳/۵
خبره۶	۲	۳/۵	۶
خبره۷	۶/۷	۱۳	۲۰
خبره۸	۵	۸/۵	۱۱
خبره ۹	۵	۸/۴۴	۱۳
میانگین	۴/۱۲	۷/۱۸	۱۲/۷۳



نمودار (۱) دوره زمانی تملک فناوری‌های اطلاعاتی نوظهور

تعیین ابعاد تکنیکی، تاکتیکی و راهبردی فناوری‌ها

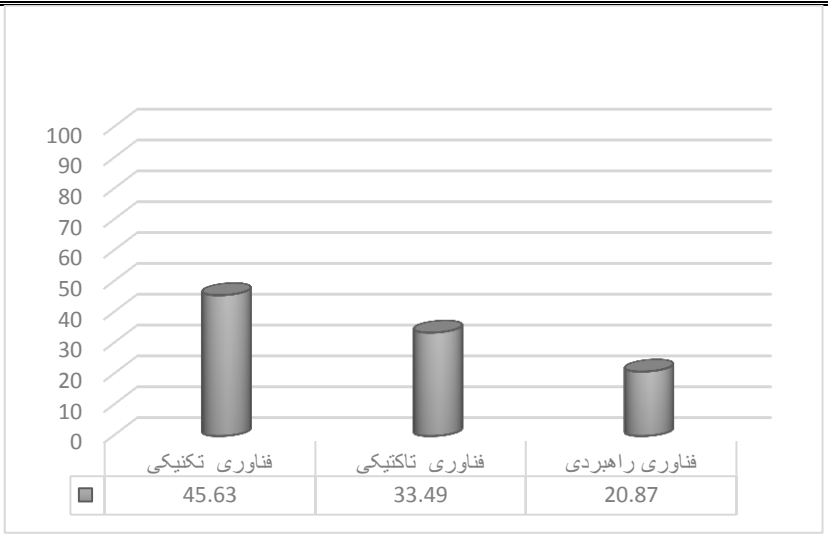
شکی نیست که فناوری اطلاعات به عنوان پدیده‌ای غیر قابل انکار در ساختار تمامی سازمان‌ها عجین شده و کاربرد آن از بالاترین سطوح تا جزیی‌ترین فعالیت‌ها جاری است. اما مدیریت درست بر فناوری اطاعات زمانی تحقق خواهد یافت که نوع کاربری آنها از نظر تکنیکی، تاکتیکی و راهبردی مشخص شود. کاربرد راهبردی فناوری اطلاعات به مفهوم تاثیرگذاری کلان‌تر، عمیق‌تر، بلندمدت‌تر و گسترده‌تر است. در مقابل، کاربرد تاکتیکی به صورت مقطعی و در افق زمانی کوتاه‌تر و با حوزه‌ی اثر کوچک‌تر مورد استفاده قرار می‌گیرد. بر طبق ادبیات مدیریت راهبردی، تاکتیک نسبت به راهبرد، عمق کمتری داشته و راه‌های رسیدن به آن را مشخص می‌کند. بنابراین برای رسیدن به هدف راهبردی، در مقاطع مختلف تاکتیک‌های متفاوتی انتخاب می‌شوند. در نهایت در هر حوزه‌ای، تکنیک کوچک‌ترین واحد یادگیری یک مهارت است. گورلا و همکاران(۲۰۱۰) تاثیر فناوری های اطلاعاتی را در سه سطح طبقه‌بندی کرده‌ند: ۱- تاثیر استراتژیک که بر اهداف سازمانی، استراتژی‌ها و سیاست‌ها تاکید دارد ۲- تاثیر تاکتیکی که بر تخصیص منابع و نظارت بر عملکرد تمرکز دارد. ۳- تاثیر عملیاتی که با کاربرد منابع و بهره‌وری نیروی کار مرتبط است (Gorla et al, 2010). از طرفی محققان معتقد هستند که جنگ اطلاعاتی را باید از منظر ابعاد مختلف از جمله در سطح تکنیک، تاکتیک و راهبرد بررسی کرد. مثلاً در یک جنگ الکترونیک، حملات مختل‌کننده علیه حسگرها بر اساس

آگاهی از مشخصات تکنیکی و عملیاتی حسگرها می‌باشد(Wik, 2007). لذا موفقیت در جنگ اطلاعاتی و تامین امنیت، نیازمند فناوری‌های اطلاعاتی مرتبط می‌باشد(Reuter, 2019).

در این مرحله از تحقیق از خبرگان درخواست شد تا نوع کاربرد فناوری‌های اطلاعاتی نوظهور را مشخص کنند. بر اساس نظرات خبرگان نوع فناوری‌ها و درصد هر یک از نظر کاربردهای تکنیکی، تاکتیکی و راهبردی بر اساس جدول (۶) و نمودار (۲) می‌باشد.

جدول (۱۰) فراوانی فناوری‌های اطلاعاتی بر اساس نوع کاربرد

خبرگان	فناوری‌های تکنیکی	فناوری‌های تاکتیکی	فناوری‌های راهبردی
خبره۱	۱۵	۴	۷
خبره۲	۲	۱۴	۸
خبره۳	۳	۱۳	۹
خبره۴	۲۳	۸	۹
خبره۵	۱۴	۷	۳
خبره۶	۱۹	۳	۵
خبره۷	۹	۱۵	۴
خبره۸	۱۶	۱۳	۶
خبره ۹	۱۰	۱۲	۷
فراوانی	۱۱۳	۸۹	۵۸
نام فناوری	هوش مصنوعی، اینترنت اشیاء، واقعیت مجازی، واقعیت‌افزوده، ماشین‌یادگیری، ارتباطات نوری مرئی، شبکه عصبی مصنوعی، پرنده بدون سرنشین، مواد هوشمند، سلام‌های خودکار لیزری	داده بزرگ، الکترو مغناطیس، پرنده‌های بدون سرنشین، اینترنت اشیاء، فناوری جاسوسی، هوش مصنوعی	وسایل فراصوت، محاسبات کوانتومی، سلاح هدایت انرژی، فناوری سایبری، داده بزرگ، یادگیری عمیق، سیستم ارتقای سرباز، سنسورهای پیشرفته، شبکه اجتماعی هوشمند،



نمودار (۲) درصد فناوری‌های تکنیکی، تاکتیکی و راهبردی

بحث و نتیجه‌گیری

امروزه با افزایش استفاده از محیط‌های فراگیر، محیطی که نیاز بشر را در هر زمان و هر مکان فراهم می‌سازد فناوری اطلاعاتی و ارتباطاتی در حوزه تعاملی انسانی و ماشینی با سرعتی غیرقابل تصور پیشرفت نموده است. با پیش‌بینی و شناخت چالش‌ها، فرصت‌ها و روند توسعه فناوری‌های محیط‌های فراگیر برای تقویت حوزه‌های تحقیقاتی راهبردی، تبدیل چالش به فرصت، فراهم‌سازی نیازهای پیاده‌سازی برای کشورها به یک ضرورت تبدیل شده است. از سوی دیگر صنایع نظامی و دفاعی به شدت مبتنی بر فناوری اطلاعات بوده و ضرورت رصد و مدیریت انواع این فناوری‌ها در این صنایع مشهود است. از سوی دیگر، سرعت بالای تغییر و تحولات در محیط فناورانه، توانایی برنامه‌ریزی و تصمیم‌گیری در این حوزه را بدون درک شایسته از موقعیت حال و آینده فناوری، ناممکن ساخته است. سازمان‌هایی که دیجیتالی شدن را پذیرفته‌اند، در تدارک سرمایه‌گذاری در زیرساخت فناوری اطلاعات، اینترنت اشیاء، یادگیری ماشینی و هوش مصنوعی هستند. بنابراین فناوری‌های عصر اطلاعات که در بخش خصوصی و در تعامل با بخش نظامی توسعه یافته‌اند، بایستی به صورت فوری و بلادرنگ در ساختار نیروهای نظامی یکپارچه شوند. اما برای یکپارچه‌سازی و گنجاندن انواع فناوری‌های اطلاعاتی در بخش دفاعی و نظامی کشور، شناسایی، طبقه‌بندی و تعیین حیطه کاربرد این فناوری‌های نوظهور بسیار مهم است. در این تحقیق ابتدا از طریق فن دلفی و در دو مرحله، تعداد ۲۶ فناوری

اطلاعاتی نوظهور شناسایی شد. در دور دوم دلفی دو فناوری شبکه‌های اجتماعی هوشمند و فناوری جاسوسی، فناوری پوشیدنی، سلاح‌های لیزری هم برای حوزه دفاعی موثر تشخیص داده شد. همچنین در این مرحله، فناوری بلاکچین (رتبه ۲۳)، رایانش ابری (رتبه ۲۲)، رایانش مه و لبه (رتبه ۲۱) به دلیل رتبه پائین در آینده بخش دفاعی قابلیت کاربرد چندانی ندارند. مهمترین دلیل عدم تایید این فناوری‌ها توسط خبرگان، فقدان آگاهی جهانی در خصوص امنیت آنها و مسائل حقوقی است. در خصوص فناوری بلاکچین باید گفت که استفاده گسترده از وسایل اینترنت اشیاء توسط دولت منجر به بهره‌گیری از بلاکچین برای ایجاد امنیت در این وسایل خواهد شد؛ به عنوان مثال بلاکچین در ردیابی و تایید مسیر عناصر قراردادها می‌تواند آسیب‌های زنجیره تامین را کاهش داده و صحت مجوزها را بررسی کند. کاربرد دیگر این فناوری، امنیت سایبری است و استفاده از بلاکچینِ خصوصی و کنسرسیومی و با اتکا به کلیدهای رمزنگاری و امضای دیجیتال می‌تواند امنیت سایبری را تضمین کند. فناوری بلاکچین برای ثبت و تصدیق فعالیت چاپ سه بعدی، احراز هویت، کمک به حکومت و دولت هم مناسب است. در نهایت رتبه پایین رایانش ابری هم مسائل امنیت و محرمانگی است که بخش دفاعی به راحتی نمی‌تواند اطلاعات سری خود را در این بخش قرار دهد. در مرحله بعد از خبرگان دلفی درخواست شد وضعیت بخش دفاعی ایران در خصوص این فناوری‌ها را در سه دوره زمانی تقلید، تطبیق و تسلط مشخص کنند. بر اساس یافته‌های تحقیق برای تسلط کامل بخش دفاعی ایران به این فناوری‌ها حدودا ۱۲ الی ۱۳ سال زمان نیاز است. خبرگان در خصوص نوع کاربرد فناوری‌ها هم نظرات خود را ارائه کردند و بیش از ۴۵ درصد فناوری‌ها کاربردی تکنیکی داشته و ۵۵ درصد کاربرد تاکتیکی و راهبردی دارد (نمودار ۲ و جدول ۵). اما برخی از خبرگان در تکمیل پرسشنامه دلفی، حیطه کاربرد برخی فناوری‌ها را چندگانه اعلام کردند. برای مثال از نظر برخی خبرگان این تحقیق، فناوری کلان داده، سلاح‌های هدایت انرژی، سیستم‌های ارتقای سرباز، فناوری جنگ سایبری و شبکه‌های اجتماعی هوشمند دارای هر سه کاربرد تکنیکی، تاکتیکی و راهبردی هستند. همانطور که در ادبیات تحقیق اشاره شد، هوش مصنوعی و شاخه‌های آن هر سه نوع کاربرد را دارد؛ از طرفی اینترنت اشیاء در حوزه دفاعی دارای کاربرد تاکتیکی است که البته در این تحقیق هم به این نوع کاربرد اشاره شده است.

پیشنهادها

- احصاء ساز و کارهای پیاه‌سازی خدمات فناوری اطلاعات و ارتباطات(ITIL) در سازمان‌های دفاعی -نظامی به منظور ایجاد قابلیت در جذب و بومی‌سازی فناوری های نوظهور دفاعی.

- پیشنهاد می‌شود از طریق خبرگانی از ارتش و سپاه مهمترین فناوری‌های دفاعی آینده در قالب پروژه تحقیقاتی شناسایی شود.
- با توجه به اینکه در این تحقیق، کلان‌داده رتبه بالایی کسب کرده است، پیشنهاد می‌شود امکان‌سنجی کاربرد و استفاده از این فناوری در بخش‌های دفاعی مورد بررسی قرار گیرد.
- پیشنهاد می‌گردد که بخش دفاعی به استفاده از فناوری‌های مبتنی بر اینترنت اشیاء در حوزه‌هایی همچون ردیابی نهادهای زنجیره تأمین، کنترل از راه دور فرآیندهای زنجیره تأمین، تهیه داده‌های لازم جهت کمک به اتخاذ تصمیمات تاکتیکی و استراتژیک، اشتراک اطلاعات در زنجیره تامین دفاعی و همچنین ارتباط و هماهنگی بین اپراتورها، همت گمارد.
- در این تحقیق فناوری هوش مصنوعی، رتبه بالایی کسب کرده است. بنابراین پیشنهاد می‌شود حوزه‌های هوش مصنوعی مانند یادگیری عمیق و شبکه‌های عصبی مصنوعی در عملیات اطلاعاتی پیچیده و رصد اطلاعاتی و...مورد استفاده قرار گیرد.
- باتوجه به دیدگاه مقام معظم رهبری در خصوص هم‌افزایی در نیروهای مسلح، پیشنهاد می‌شود از فناوری‌های اطلاعاتی نوظهور در ایجاد هم‌افزایی و به خصوص کمک به ایجاد تعامل‌های بین سازمانی استفاده شود.
- پیشنهاد می‌شود مرکز رشد و پژوهشکده فناوری‌های نوظهور آجا با محوریت دافوس تشکیل و در کنار چین، روسیه و آمریکا، به چهارمین قطب فناوری دفاعی جهان تبدیل شود.

منابع

- حبیبی، مجید. (۱۳۹۶). داده‌های بزرگ و کاربردها. *فصلنامه ره‌آورد نور*، ۵۹ (۱۶).
- غلام‌نژاد، پژمان؛ غلامی، محمود؛ و پورمکاری، علیرضا. (۱۳۹۸). کاربردهای نظامی اینترنت اشیاء با تاکید بر ماموریت های نیروهای هوایی ارتش. *فصلنامه علوم و فنون نظامی*، ۱۵ (۴۹): ۱۶۳-۱۴۱.
- غنمی، حمید. (۱۳۹۸). بررسی چالش اعتماد در امنیت اینترنت اشیاء و شناخت تهدیدات، بایدها و نبایدهای امنیتی آن. *پایان‌نامه کارشناسی ارشد*. دانشگاه آزاد واحد صفادشت.
- فرتاش، کیارش، محسنی کیاسری، مصطفی، سعدآبادی، علی اصغر. (۱۳۹۲). نقش توانمندی مدیریت فناوری در فرآیند توسعه محصولات جدید دفاعی (یافته‌های تجربی). *مدیریت نوآوری*، ۵(۲): ۱۳۵-۱۶۲.
- فولادی، قاسم. (۱۳۹۵). *کارگاه آموزشی طرح‌ریزی دفاعی بلند مدت*. موسسه تحقیقاتی و آموزشی دفاعی. مرکز آینده پژوهی علوم و فناوری دفاعی.
- قاضی، میرسعید، سید علیرضا. (۱۳۹۷). سناریوهای جنگ‌های زمینی احتمالی آینده علیه ج.ا.ایران و دلالت‌های آن برای دانشگاه افسری امام علی(ع) نزاجا. *رساله دکتری مدیریت صنعتی*. تهران: دانشگاه صنعتی مالک اشتر.
- میرشاه‌ولایتی، فرزانه. و نظری‌زاده، فرهاد. (۱۳۹۸). الگوی دیدبانی فناوری: فرآیند و ساختاری برای رصد تحول فناورانه. *فصلنامه آینده‌پژوهی دفاعی*، ۴ (۱۳): ۶۸-۴۱.
- ولوی، محمدرضا؛ موحدی، محمد رضا و باقری، ایمان.(۱۳۹۶). ارائه الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط ابری. *فصلنامه مدیریت نظامی*. ۱۷ (۶۵): ۱۳۰-۱۰۶.
- Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.
- Bhatnagar, S., Cotton, T., Brundage, M., Avin, S., Clark, J., Toner, H., & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Authors are listed in order of contribution Design Direction.
- Button, R. W. (2017). Artificial intelligence and the military. *RAND Blog*, *July*, *9*.
- Chin, W. (2019). Technology, war and the state: past, present and future. International Affairs, 95(4), 765-783.
- Gorla, N., Somers, T. M., & Wong, B. (2010). Organizational impact of system quality, information quality, and service quality. *The Journal of Strategic Information Systems*, *19*(3), 207-228.
- Hughes, J. J. (2007). Global technology regulation and potentially apocalyptic technological threats. *Nanoethics: the ethical and social implications of nanotechnology. Hoboken, NJ: John Wiley*, 201-214.
- Johannsen, D. Solka, L. and Rigsby, T. (2018). The Rapid Rise of Neural Networks for Defense: A Cautionary Tale.

- Kostin, K. B. (2018). Foresight of the global digital trends. *Strategic management*, *23*(1), 11-19..
- Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*, *6*(1), 111.
- Mehmood, M. U., Chun, D., Han, H., Jeon, G., & Chen, K. (2019). A review of the applications of artificial intelligence and big data to buildings for energy-efficiency and a comfortable indoor living environment. *Energy and Buildings*, *202*, 109383.
- Menon, R.(2020). Big Data Trends: Our Predictions for 2020 PLUS What Happened in 2019. Available at www.infoworks.io.
- Nigania, J. (2019). In 2019 IoT Seems To Be More Embedded In Our Daily Life. Available at www.houseofbots.com.
- Outsource2india. (2020). Big Data in2020: future, growth, and challenges. www.outsource2india.com.
- Perry, B. Uuk, .R. (2019). AI Governance and the Policymaking Process: Key Considerations for Reducing AI Risk. *Big data and cognitive computing*.
- Perwej, Y., AbouGhaly, M. A., Kerim, B., & Harb, H. A. M. (2019). An extended review on internet of things (iot) and its promising applications. *Communications on Applied Electronics (CAE), ISSN*, 2394-4714.
- Premsankar, G. Francesco, M.D. and Talb, T. (2018).Edge computing for the internet of thing: a case study. Internet of Things Journal.
- Raska, M. (2019). Strategic Competition for Emerging Military Technologies. *PRISM*, *8*(3), 64-81.
- Reis, J., Santo, P. E., & Melão, N. (2019, April). Artificial intelligence in government services: A systematic literature review. In *World conference on information systems and technologies* (pp. 241-252). Springer, Cham..
- Reuter, C. (2019). Information Technology for Peace and Security–Introduction and Overview. In *Information Technology for Peace and Security* (pp. 3-9). Springer Vieweg, Wiesbaden.
- Scherer, M. U. (2015). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harv. JL & Tech.*, *29*, 353.
- Sfar, A. R., Chtourou, Z., & Challal, Y. (2017, February). A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges. In *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)* (pp. 101-105). IEEE.
- Simone, S. (2020). Ten Predictions for Big Data in 2020. www.dbta.com.
- Spiegeleire, D. Maas, M. and Sweijs, T. (2017). Artificial Intelligence. And the future of defense. The Hague Centre for Strategic Studies. (HCSS).
- SPiNN program. (2020). Researchers to infuse DSP with neural network kernels to enhance performance of radar and communications available at www.militaryaerospace.com.

- Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018, May). Possibilities and challenges for artificial intelligence in military applications. In *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*.
- Takai, M. (2012). DoD Cloud Computing Strategy. Department of Defense Chief Information Officer.
- Wik, M. W. (2002). Revolution in information affairs: Tactical and strategic implications of Information Warfare and Information Operations. *A. Jones, GL Kovacic h & PG Luzwick (eds.), Global informafion warfare*, 579-628.
- Wik, M. W. (2002). Revolution in information affairs: Tactical and strategic implications of Information Warfare and Information Operations. *A. Jones, GL Kovacic h & PG Luzwick (eds.), Global informafion warfare*, 579-628.
- Yuan, S. (2020). How China is using AI and big data to fight the coronavirus. *Al Jazeera*, *1*.
- Zhao, Z., Klemas, V. V., Zheng, Q., & Yan, X. H. (2003). Satellite observation of internal solitary waves converting polarity. *Geophysical Research Letters*, *30*(19).