

الگوی تهدیدات فناوری‌های نوین نیروی زمینی ارتش جمهوری اسلامی ایران

وحید ریاضی^۱ | اسماعیل بیابانی^۲ ✉

چکیده:

شناسایی، پیش‌بینی و ارزیابی تهدیدات فناوری‌های نوین با شاخص‌هایی همچون شناخت صحیح و دقیق تهدید، ارزیابی توان و ظرفیت تهدید برای حفظ منافع کشور عزیزمان در نبردهای آینده امری مهم و حیاتی است. در تمامی سطوح و بدنه نیروهای مسلح از جمله ارتش جمهوری اسلامی ایران به‌ویژه نیروی زمینی با توجه به تنوع تجهیزات و تاکتیک‌های رزمی به‌کاررفته و پیشرفت لحظه‌به‌لحظه فناوری‌ها، لزوم بررسی و موشکافی این تهدیدات بیش‌ازپیش احساس شده است. پژوهش حاضر با هدف طراحی الگوی تهدیدات فناوری‌های نوین نیروی زمینی ارتش جمهوری اسلامی ایران صورت گرفته است. این تحقیق از نوع کاربردی- توسعه‌ای بوده که به روش توصیفی - تحلیلی دارای رویکردی آمیخته است. روش جمع‌آوری داده‌ها کتابخانه‌ای و میدانی بوده، مصاحبه عمیق به روش هدفمند با خبرگان به تعداد ۱۱ نفر و حجم نمونه ۸۵ نفر انجام شده است. در بخش کیفی از طریق پالایش، تلخیص، نمایش داده‌ها و تحلیل محتوا انجام شد و در بخش کمی از آمار توصیفی، آمار استنباطی و نرم‌افزار SPSS استفاده شد. به‌منظور دستیابی به طراحی الگوی موردنظر، گویه‌های مربوط به پرسشنامه محقق ساخته احصاء، تکمیل و به جامعه خبره و حجم نمونه ارائه گردید. که محصل آن سه مؤلفه (هوش مصنوعی، روبات‌ها و سربازان آینده/سایبری) و ۱۰ شاخص در حوزه تهدیدات فناوری‌های نوین نزاجا احصاء گردید و تحلیل داده‌ها نیز در این حوزه در بخش کیفی تکمیل و ارائه شد تا زمینه تولید الگو فراهم شود. نتایج حاکی از آن است که مؤلفه‌های هوش مصنوعی، روبات‌ها و سربازان آینده/سایبری با ترکیبی از ۱۰ شاخص در حوزه تهدیدات فناوری‌های نوین نزاجا، اجزای تشکیل‌دهنده الگوی یادشده را فراهم آوردند که در ادامه در جهت اعتبارسنجی آن توسط جامعه خبره تحقیق تأیید شد.

واژگان کلیدی: الگو، تهدید، فناوری‌های نوین، نزاجا

۱- گروه زمینی، دانشکده فرماندهی و ستاد، دانشگاه فرماندهی و ستاد، تهران، ایران، رایانامه:

v.riazi@yahoo.com

۲- گروه لجستیک و مالی، دانشکده پشتیبانی و ستاد، دانشگاه فرماندهی و ستاد، تهران. (نویسنده مسئول).

رایانامه: E.biabany33@casu.ac.ir

مقدمه

تغییرات سریع فناوری‌ها در بخش دفاعی کشورها اثرات شگرفی گذاشته است. این اثرات نبردهای آینده را با ابهام و پیچیدگی‌های روزافزون مواجه می‌کند. در همین راستا پیشرفت‌های قابل ملاحظه فناوری، مدل‌سازی فرآیندهای تولید برای بازار غیرنظامی تسهیل شده است. این تنوع فناوری‌ها دارای کاربردهای مشخصی در زمینه‌های نظامی مشتمل بر حوزه‌های هوش مصنوعی، سامانه‌های خودکار، زیست‌فناوری و محاسبات کوانتومی نیز هستند و نقش مهمی را ایفا می‌کنند (گودرزی، ۱۴۰۰). با تأمل در ادبیات این حوزه متوجه خواهیم شد که جمهوری اسلامی ایران در این زمینه گام‌های مؤثری را برداشته است. دلیل این مهم را می‌توان در ماهیت ضد استکباری، موقعیت خاص ژئوپولیتیکی، حمایت از مستضعفین جهان، حفظ سیاست استقلال‌خواهی و برنامه صلح‌آمیز هسته‌ای جمهوری اسلامی ایران و همچنین تنوع تهدیدها عنوان کرد. از طرفی حضور بازیگران غیردولتی در صحنه‌های جنگ، حمایت و پشتیبانی بازیگران دولتی از آن‌ها، تلاش این بازیگران برای ایجاد هویت و همچنین تحولات فناوری، گسترده شدن تجهیزات مدرن و کنترل از راه دور، شکل‌گیری قدرت‌های هوشمند، گسترده شدن جنگ‌های نیابتی، سوق یافتن جنگ‌ها به درون شهرها، طولانی شدن جنگ‌ها به‌ویژه شکل‌گیری گروه‌های افراطی در منطقه (عراق، سوریه، یمن و ...) و حمایت دشمنان منطقه‌ای و فرا منطقه‌ای از گروه‌های افراطی علیه جمهوری اسلامی ایران و منافع ملی ایران اسلامی، همه و همه حاکی از تغییر ماهیت جنگ‌ها و تنوع سناریوهای دشمن در مقابله با کشورهای مستقل و عدالت‌خواه هست (ثروتی، ۱۳۹۱: ۳۴).

با توجه به این‌که از روش‌های مناسب در فهم ماهیت تهدیدها، طبقه‌بندی آن‌ها بر مبنای عوامل متفاوت آن است؛ می‌توان این‌طور اذعان کرد که بدیهی است ایران اسلامی در مواجهه با تهدیدات پیش رو به‌ویژه در زمینه فناوری‌های نوین، تقویت نیروهای مسلح در مقایسه با توانمندی کشورهای رقیب و متخاصم را در دستور کار قرار داده است. این مقوله در تمامی سطوح و بدنه نیروهای مسلح از جمله ارتش جمهوری اسلامی ایران به‌ویژه نیروی زمینی با توجه به تنوع تجهیزات و تاکتیک‌های رزمی به‌کاررفته و پیشرفت لحظه‌به‌لحظه فناوری‌ها، لزوم بررسی و موشکافی تهدیدات بیش‌ازپیش احساس شده است. اهمیت این موضوع محققین را بر آن داشته تا در این پژوهش به ارائه الگوی تهدیدات فناوری‌های نوین نیروی زمینی ارتش جمهوری اسلامی ایران پردازند.

بیان مسئله

مقام معظم رهبری علیه السلام می‌فرمایند: «... امروز ما باید بدانیم این دشمن ناکام مانده در مقابل ملت ایران نقشه‌اش چیست؟ باید بیدارباشیم (العالم بزمانه لا تهجم علیه اللّوایس: شبهات به کسی که زمانه خود را بشناسد هجوم نمی‌آورد) اگر صحنه را بشناسیم؛ عرصه را بشناسیم؛ دشمن را بشناسیم؛ نقشه دشمن را بدانیم؛ غافلگیر نخواهیم شد...» (بیانات مقام معظم رهبری در دیدار با مردم کازرون، مورخ ۱۳۸۷/۰۲/۱۸). شناسایی، پیش‌بینی و ارزیابی تهدیدات فناوری‌های نوین با شاخص‌هایی همچون شناخت صحیح و دقیق تهدید، ارزیابی توان و ظرفیت تهدید برای حفظ منافع کشور عزیزمان در نبردهای آینده امری مهم و حیاتی است. نیروی زمینی که یکی از نیروهای زیرمجموعه ارتش جمهوری اسلامی ایران است و با همکاری سایر یگان‌های ارتش وظیفه حفظ تمامیت ارضی و حفاظت از مرزهای سرزمینی کشور را بر عهده دارد، از این قاعده مستثنا نیست و به‌طور مکرر در معرض تهدیدهای متنوع است. به همین منظور مسئله مورد توجه این مقاله متکی بر مدون نبودن مطالعات در مورد تهدیدات آینده، پیشرفت فناوری‌های نوظهور و مرزشکنی در صنایع نظامی کشور است که در آموزه‌های نشأت گرفته از جنگ‌های اخیر و وضعیت خاص ژئوپلیتیکی ایران اسلامی است که منجر به تولید دغدغه مبتنی بر چپستی تهدیدها در حوزه فناوری‌های نوین و مؤلفه‌ها و شاخص‌های مؤثر بر آن است. از نگاه ایجابی و به‌اصطلاح اهمیت تحقیق در این مقاله می‌توان به تولید ایده‌های جدید و مناسب در زمینه تهدیدهای فناوری و ایفای تصویری روشن از مهم‌ترین تهدیدات آینده، در تدوین و طرح‌ریزی کارآمد طرح‌های عملیاتی و کسب آگاهی مناسب نسبت به جلوگیری از غافلگیری معرفی کرد و در حوزه سلبی و نگاه ضرورت تحقیق می‌توان به مواردی به شرح ادامه اشاره کرد: کم‌توجهی به این تحقیق روند شکل‌گیری تصمیم‌سازی و تصمیم‌گیری را با ابهام و چالش مواجه می‌کند.

اهداف پژوهش

هدف اصلی تحقیق: طراحی الگوی تهدیدات فناوری‌های نوین نیروی زمینی ارتش جمهوری اسلامی ایران است.

اهداف فرعی شامل:

الف- تعیین مؤلفه‌های اساسی الگوی تهدیدات فناوری‌های نوین نیروی زمینی ارتش جمهوری اسلامی ایران.

ب- تعیین شاخص‌های کلیدی هرکدام از مؤلفه‌های اساسی الگوی تهدیدات فناوری‌های نوین

نیروی زمینی ارتش جمهوری اسلامی ایران.

این تحقیق به دلیل اکتشافی بودن، به دنبال یافتن مؤلفه‌ها و شاخص‌های الگو و طراحی الگو است، فاقد فرضیه بوده و اهداف و سئوالات به‌عنوان اساس کار منظور شده است.

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

اساس و مبانی این تحقیق، برگرفته از نگاه متقن و علمی به مفاهیم و متغیرهایی است که در شناخت و تولید الگویی متناسب با تهدیدهای فناوری‌های نوین نقش ایفا کرده و تأمل در آن‌ها مقاله را به سمت تولید اقناعی الگو هدایت کرده است. در این اثنا نیز نگارندگان در چارچوب نظری تحقیق که برآمده از توصیف مبانی نظری بوده بر محیط‌شناسی و تعامل میان سه رأس اسناد و مدارک، دکترین آجا و اسناد بالادستی توجه داشته تا مؤلفه‌ها و شاخص‌های الگویی تهدیدهای فناوری‌های نوین را احصاء کنند که در ادامه به تشریح آن پرداخته شده است. مدل مفهومی تحقیق با بهره‌گیری از چارچوب نظری، دقت نظر در محیط‌شناسی و استفاده از سایر عناصر شکل‌دهنده که می‌تواند زمینه بهره‌مندی و تولید مؤلفه‌ها و شاخص‌ها در حوزه تهدیدهای فناوری‌های نوین را هویدا کند، استوار شده است.

الگو:

مجموعه نظام‌مندی از مفاهیم، اصول موضوعه و قوانین است که در یک ساختار منطقی برای توضیح و تفسیر یک سامانه از موجودات تکوینی، پدیده‌ها، روش‌ها، فرایندها، تئوری‌ها و نظریه‌ها ارائه می‌شود (خادم دقیق، ۱۳۹۸: ۶۹). سنچولی (۱۳۹۶) الگو را چارچوب نظری و ذهنی معرفی می‌کند که پایه و معیار حرکت است و به عبارتی آن را نقشه راه می‌داند (سنچولی، ۱۳۹۶: ۱۰۴-۷۹). رهبر معظم انقلاب اسلامی علیه‌السلام در معرفی الگو می‌فرمایند: «الگو، یک الگوی منعطف است؛ یعنی قابل انعطاف است. هدف‌ها مشخص است؛ راهبردها ممکن است به‌حسب شرایط گوناگون تغییر پیدا کند و حکم و اصلاح شود» این الگو، نقشه جامع است؛ به ما می‌گوید که به کدام طرف، به کدام سمت، برای کدام هدف داریم حرکت می‌کنیم...» (بیانات مقام معظم رهبری در نخستین نشست اندیشه‌های راهبردی با موضوع الگوی اسلامی ایرانی پیشرفت، مورخ ۱۳۸۹/۰۹/۱۰).

تهدید:

تهدید عبارت از هر چیزی که بتواند ثبات و امنیت را در یک کشور به خطر اندازد، دانسته شده و تهدیدها، منافع ملی را هدف قرار می‌دهند. مفهوم تهدید در نگرش سامانه‌ای، عدم تعادل در سامانه بیان شده است؛ یعنی عاملی که اجازه نمی‌دهد سامانه به اهداف خویش برسد. برای تعریف تهدید می‌بایست به عناصر و عوامل تشکیل‌دهنده گوناگونی توجه کرد و بر اساس آن، تهدیدها را تفکیک نمود. این عناصر و عوامل عبارت‌اند از: منافع ملی، توانمندی موضوع با واحد مورد تهدید، شرایط محیطی، قدرت و توانایی تهدید، زمان (ممکن است موضوعی در یک‌زمان تهدید بوده و در زمان دیگر تهدید نباشد) و تصور از اقدامات یا پدیده‌ها (مرادپان، ۱۳۹۷).

در همین رابطه احساس و درک چیزی به نام تهدید، درکی پسینی، زمینه‌ای و نسبی است. به عبارت دیگر شکل‌گیری تصویری که بیان‌کننده تهدید باشد، نیازمند وجود تصورات مقدماتی است. این تصورات دربردارنده ارزش‌های مهمی است که بقاء آن مسبوق بر ادراک تهدید هستند. از سوی دیگر تهدید کاملاً زمینه‌ای است و تنها در شرایط و اوضاع و احوال خاص به وجود می‌آید. به همین سبب این مفهوم یا درک، کاملاً نسبی است و با تغییر شرایط محیطی، زمانی و حتی ادراک‌کننده محیط، تحول پیدا می‌کند (افتخاری، ۱۳۹۰).

روندهای فناوری‌های دفاعی:

پیشرفت‌های فناوری باعث ایجاد تغییرات اساسی در سازمان‌ها، راهبردها و تدابیر امنیتی و دفاعی شده است. فناوری‌های نوین باعث توزیع و انتشار آگاهی‌ها شده، سرعت تبادل اطلاعات را افزایش داده است و با پشت سر گذاشتن مرزهای قدیمی افق جدیدی را در عملکرد نیروهای نظامی و تحول در حوزه دفاعی و هوشمندی سامانه‌های نظامی گشوده است. این تحولات فناورانه در حوزه‌های فرماندهی و کنترل که مسئول مدیریت و هدایت عملیات نظامی را بر عهده دارد تأثیرات عمیقی برجای گذاشته است. بر این اساس ارتش‌های دنیا و سازمان‌های دفاعی همواره درصدد استفاده از فناوری‌های نوین و پیشرفته به منظور ارتقاء سطح تجهیزات و سامانه‌های دفاعی و هوشمند نمودن این سامانه‌ها جهت مقابله با تهدیدات هوشمند و نوین بوده است (آژانس دفاعی اروپا، ۲۰۲۱). روندهای فناوری‌های دفاعی بر اساس مطالعه رویدادهای آینده فناوری‌ها و سایر گزارش‌های در دسترس به شرح ادامه دسته‌بندی شده است:

- ۱- توسعه سامانه‌های هوشمند
- ۲- رواج سامانه‌های بدون سرنشین و خودکارسازی

- ۳- رشد فناوری‌های سایبری
۴- رشد روزافزون فناوری‌های فضایی
۵- افزایش به‌کارگیری فناوری‌های همگرا
۶- افزایش کاربرد اینترنت (اینترنت اشیا)
۷- رشد انرژی‌های نو (گودرزی، ۱۴۰۰)

هوش مصنوعی و کاربردهای نظامی آن

هوش مصنوعی می‌تواند قابلیت‌های تحرک یگان نظامی را از طریق تشخیص هدف، سامانه‌های سلاح خودکار، ابزارهای حمایتی و برنامه‌ریزی 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. کاربردهای نوین هوش مصنوعی از داده‌کاوی رباتیک و پردازش زبان طبیعی فراتر رفته و حیطه‌هایی همانند مراقبت نظامی، شناسایی، ارزیابی تهدید، فرماندهی و کنترل، مین‌گذاری زیرآب، امنیت سایبری، آنالیز هوشمند و آموزش را در برمی‌گیرد. با این حال، علی‌رغم امکانات قابل‌تصور برای استفاده از هوش مصنوعی در حوزه نظامی، ریسک‌ها و چالش‌های مختلفی از جمله اعتماد، فقدان شفافیت برای تصمیم‌گیری قابل‌تصور است. به‌رحال، نیروهای نظامی عصر جدید، احتمالاً دگرگونی تاریخی دیگری را تجربه می‌کنند. این دگرگونی صرفاً تغییر قابلیت‌های موجود نیروهای مسلح نیست؛ بلکه تغییردهنده اساس نیروهای نظامی مشتمل بر آنچه انجام می‌دهند و چگونگی انجام آن است. از این فناوری می‌توان در حل چالش‌های لجستیکی^۱، 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 غیرنظامی استفاده کرد (محمدی فاتح، ۱۳۹۹).

اینترنت اشیا

اینترنت اشیا از دیگر مؤلفه‌های شکل‌دهنده فناوری نوظهور بوده که تحولات عظیمی در زندگی روزمره بشر ایجاد کرده است. این فناوری به‌عنوان شبکه‌ای جهانی از ماشین‌ها و دستگاه‌هایی است که توانایی تعامل با یکدیگر را دارند و به‌عنوان یکی از مهم‌ترین محورهای

فناوری آینده شناخته شده و توجه قابل‌ملاحظه‌ای از صنعت را به خود اختصاص داده است. به همین دلیل، شورای ملی اطلاعات آمریکا، اینترنت اشیاء را به‌عنوان یکی از شش فناوری دارای پتانسیل تأثیرگذاری بر منافع آمریکا تا سال ۲۰۲۵ میلادی معرفی نموده است (نظری، ۱۴۰۰: ۴). استفاده از اینترنت اشیاء در کاربردهای نظامی به یک ضرورت تبدیل شده است. در عصر حاضر علی‌رغم چالش‌های فراوان مربوط به پذیرش اینترنت اشیاء در حوزه نظامی، پتانسیل بالای اینترنت اشیاء برای روزآمدسازی جنگ‌افزارها، استفاده از داده‌ها و خودکارسازی جهت حفظ جان سربازان و از طرف دیگر کاهش هزینه‌ها و افزایش کارایی پذیرش این فناوری را به امری جذاب برای سازمان‌های دفاعی و نظامی مبدل ساخته است. علی‌هذا به موازات حوزه‌های عملیاتی و اطلاعاتی اینترنت اشیاء با کاهش هزینه‌ها، مدیریت موجودی‌ها، مدیریت تعمیر و نگهداری تجهیزات و ... می‌تواند در بهبود فرایندهای حوزه پشتیبانی سازمان‌های نظامی رونق اساسی ایفا نماید (باقری منش و همکاران، ۱۳۹۸).

روبات

روبات‌ها در سیستم‌های رایانه‌ای متعددی از نبرد قرار گرفته و در فضای سایبری مانور خواهند داد. آن‌ها محافظت از ارتباطات و اطلاعات، دفاع از دستگاه‌های الکترونیکی، جلوگیری یا هشدار در مورد تهدیدات دریافتی و مشاوره به تصمیم‌گیرندگان را بر عهده خواهند گرفت. علاوه بر این، روبات‌ها می‌توانند به‌طور بالقوه اقدامات پیشگیرانه‌ای را مانند جابجایی حضور نیروهای خودی در فضای فیزیکی و سایبری، نفوذ به سیستم‌های دشمن و فریب دادن دشمنان با اطلاعات کاذب و تصمیم‌گیری‌های غلط انجام دهند. برای انجام این نقش‌ها روبات‌های میدان جنگ به‌صورت شبکه‌ای و پویا با یکدیگر، کنترل‌کننده‌های انسانی و همکاران خود ارتباط برقرار می‌کنند. آن‌ها در صورت لزوم خود را سازمان‌دهی خواهند کرد. این روبات‌ها هم می‌توانند دارای استقلال کامل باشند و هم به‌وسیله انسان‌ها کنترل شوند. عوامل تصمیم‌گیرنده در تمام فرآیندهای فرماندهی نیروها و جمع‌آوری اطلاعات جبهه جنگی، نقش مهمی را ایفا می‌کنند. این روبات‌های سایبری صحت اطلاعات را بررسی و اطلاعات اشتباه را فیلتر کرده و تعیین خواهند کرد که چه کسانی دسترسی به چه اطلاعاتی داشته باشند. علاوه بر این آن‌ها وظیفه مسیریابی ارتباطات، اختصاص دادن وظایف به حسگرها و انجام اقدامات هماهنگ با روبات‌های فیزیکی را خواهند داشت (Kott et al, ۲۰۱۵).

انسان‌های تکامل یافته

در میدان‌های جنگ آینده انسان‌های کمی حضور خواهند داشت اما این جنگجویان از نظر

فیزیکی و شناختی دارای قابلیت‌های ویژه‌ای هستند. توانایی‌های آن‌ها عبارت‌اند از توانایی درک حسی بهتر، درک معنایی بهتر و ارتباط با افراد دیگر و با سیستم‌های خودکار در نتیجه، آن‌ها نه تنها کارها را متفاوت انجام می‌دهند بلکه توانایی انجام کارهای بسیار متفاوتی را نیز دارند. گروه‌های متشکل از انسان‌های رباتیک، واحدهای اصلی نیروهای نظامی در جنگ‌های آینده خواهند بود. به همین علت، تقویت توانایی‌های انسانی به منظور همکاری مؤثر با روبات‌ها و عملکرد اثربخش در محیط‌های غنی اطلاعاتی، مهم خواهد بود. انسان‌های تکامل یافته با دسترسی بی‌نظیر به توان حسی و قدرت پردازشی روند یکپارچگی انسان و ماشین را گسترش می‌دهند؛ آن‌ها از روبات‌ها کمک خواهند گرفت تا به تأیید منابع کمک کنند و در نهایت روابط بین انسان و ماشین بهبود می‌یابد (آهنگری، ۱۳۹۸). نیروی انسانی احتمالاً در آینده در عملیات نظامی نقش مهمی بازی می‌کنند، فناوری‌ها نوع عملیات موردنیاز ارتش‌ها را تغییر خواهند داد و همچنین ممکن است انسان‌ها را تغییر دهند. برای به‌کارگیری بیشتر میزان داده‌هایی که حسگرها و دستگاه‌ها در مورد میدان نبرد ارائه می‌دهند، سیستم‌های نرم‌افزاری و سخت‌افزاری برای بهبود آگاهی وضعیت اطلاعات فرماندهان و اپراتورها توسعه خواهند یافت (Herr, ۲۰۱۵).

پیشینه‌های پژوهش

آهنگری و سلطان‌آبادی (۱۳۹۸) در پژوهشی با عنوان واکاوی تهدیدات و چالش‌های دفاعی-نظامی جنگ‌های آینده، ۴ عامل مهم و تأثیرگذار را به‌عنوان جنبه تعیین‌کننده محیط جنگی آینده بیان نموده‌اند که شامل گسترش سیستم‌های هوشمند، فرماندهی و کنترل در محیط نامطلوب، انسان‌های تکامل‌یافته و نبرد قاطع اطلاعاتی است.

همچنین مرادیان و صادقی (۱۳۹۲) در پژوهشی به آینده‌پژوهی تهدیدات نظامی آمریکا علیه جمهوری اسلامی ایران پرداخته‌اند که بر اساس نتایج، مهم‌ترین تهدیدات و توانایی‌های نظامی آمریکا، برای مقابله با ج.ا.ایران در آینده عبارت‌اند از: فناوری ابر طیفی آمریکا، هواپیماهای جاسوسی بدون خلبان، بهره‌مندی آمریکا از پایگاه‌های نظامی در کشورهای منطقه، هواپیماهای راهبردی، توانمندی ارتش آمریکا در به‌کارگیری سلاح‌های هوشمند، ناوهای هواپیمابر و زیردریایی‌های هسته‌ای، استقرار ناوگان دریایی آمریکا در اقیانوس هند، دریای عمان و خلیج فارس، هواپیماهای شناسایی، رادارهای پرنده و بمب‌های هوشمند.

کلان‌روندهای فناوری اطلاعات و ارتباطات، عنوان پژوهشی است که پورعزت و عبدی (۱۳۹۸) با روش توصیفی آن را انجام داده‌اند و در پایان ۷ کلان‌روند حوزه فناوری اطلاعات را بر اساس مطالعه اسناد و مصاحبه با خبرگان به دست آوردند که شامل مدیریت امنیت اطلاعات، شبکه‌های اجتماعی، زیرساخت‌های ارتباطی، شبکه‌های نوآوری در بستر فناوری اطلاعات، هوش مصنوعی، اینترنت اشیا، مراکز داده و پایگاه‌های ذخیره اطلاعات است.

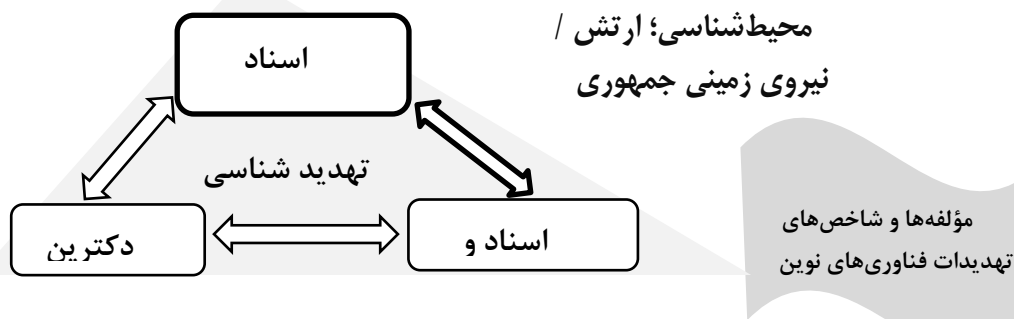
کریمی و عین‌القضاتی (۱۳۹۷) در مقاله‌ای به نقش فناوری‌های آینده در هم‌گرایی و ارتقای توان نظامی بومی پرداخته و این‌گونه بیان نموده‌اند که به‌کارگیری فناوری‌های همگرا به‌عنوان فناوری‌های حساس، توان نظامی امنیت و پیش‌بینی تهدیدات را تقویت نموده و صنایع بومی را در تولید تجهیزات خودکار و بدون سرنشین ارتقاء می‌دهد و منجر به ارتقاء آموزش نیروهای مسلح با استفاده از محیط‌های آموزشی مجازی و شبیه‌سازی می‌شود. همچنین شناسایی و حفاظت در برابر عوامل شیمیایی، بیولوژیکی، رادیولوژیکی و انفجاری تسهیل گردیده و جان سربازان و جنگاوران بهتر از گذشته حفظ شده و درمان‌های غیر دارویی برای تقویت عملکرد جنگاوران را به وجود می‌آورد.

اوهانلان (۲۰۱۸) در نشریه فارن پالیسی روندهای فناوری‌های نظامی آینده ارتش آمریکا را به چهار دسته تقسیم‌بندی می‌کند: اولین فناوری در حوزه حسگرها است که داده‌های مربوط به عملیات‌های نظامی را جمع‌آوری می‌کند. دومین فناوری شامل کامپیوتر و سیستم‌های ارتباطاتی است که داده‌ها را توزیع و پردازش می‌کند. سومین فناوری در حوزه پرتابه‌ها، سکوها و تسلیحاتی و فناوری‌های مرتبط است و چهارم سایر سیستم‌های تسلیحاتی و فناوری‌های نسبتاً جدید هستند. در دسته فناوری‌های مربوط به سیستم‌های ارتباطاتی، زیرساخت‌ها و توانمندی‌های سایبری اینترنت اشیا، محاسبات کوانتومی، کلان داده‌ها و دستگاه‌های تقویت‌کننده انسان جزء فناوری‌های آینده تا سال ۲۰۴۰ خواهند بود (Ohanlan, ۲۰۱۸:۴).

چارچوب نظری تحقیق

چارچوب نظری به مجموعه‌ای از گزاره‌ها گفته می‌شود که به لحاظ نظری قادر به تبیین با طبقه‌بندی متغیر وابسته یا اصلی تحقیق هستند. این گزاره‌ها ممکن است از یک نظریه خاص یا تلفیقی از نظریات مختلف گرفته شده باشند که هم‌گرایی آن‌ها به لحاظ نظری توسط محقق ثابت شده است (ریاضی، ۱۴۰۰). برای این که چارچوب نظری مناسبی ارائه گردد، مسئله

تحقیق انتزاع گردید. به عبارت دقیق تر صورت زیرین مسئله تحقیق کشف شد. بر اساس موارد عنوان شده و متناسب با مطالعات کتابخانه‌ای صورت گرفته، چارچوب نظری^۱ این تحقیق برابر شکل زیر ارائه می‌گردد:



روش‌شناسی پژوهش

این تحقیق با رویکرد آمیخته و با روش توصیفی (موردی-زمینه‌ای) و تحلیلی انجام شده است. محققین قصد دارند وضع موجود یک پدیده در محیط واقعی را بررسی و به صورت منظم و نظام‌دار توصیف نمایند، لذا ابتدا وضعیت موجود را بررسی و تمامی داده‌های مرتبط با موضوع را گردآوری نموده و سپس با استفاده از شواهد به دست آمده از مصاحبه با صاحب‌نظران و همچنین ابزار تفکر انتقادی به تجزیه و تحلیل داده‌ها پرداخته تا به ایده‌های جدیدی در مورد تهدیدات فناوری‌های نوین نیروی زمینی آجا دست یابند. نوع تحقیق کاربردی - توسعه‌ای است. به این نحو که نتایج آن دارای سودمندی علمی و عملی بوده که قابل استفاده در سطوح عملیاتی و تاکتیکی نیروی زمینی ارتش جمهوری اسلامی ایران است، کاربردی محسوب می‌شود و از لحاظ تطبیق نتایج به دست آمده از تحقیق کاربردی با وضعیت جدید انجام شده است و به کشف دانسته‌های جدید دربارهٔ زمینه شناسایی مؤلفه‌ها و شاخص‌های تهدیدات فناوری‌های نوین اقدام شده و سپس به کارگیری آن برای فرآیند و خدمات جدیدتر انجام می‌شود، توسعه‌ای است. برای گردآوری اطلاعات از روش کتابخانه‌ای (فیش‌برداری از اسناد و مدارک معتبر و سایت‌های

معتبر اینترنتی، کتاب‌ها)، همچنین روش میدانی شامل توزیع پرسشنامه بین صاحب‌نظران استفاده شده است. نمونه‌گیری در بخش کیفی انتخاب خبرگان، ۱۱ نفر به روش هدفمند قضاوتی انجام شد که ویژگی‌هایی مانند حداقل مدرک تحصیلی دکتری، حداقل سن خدمتی ۲۸ سال و سابقه خدمت در فاوا، عملیات، آموزش در آجا و نزاجا داشتند. از طرفی به روش نمونه‌گیری باز در بخش کمی شامل ۸۵ نفر از بین خبرگان نظامی و دانشگاهی در سطح نیروهای مسلح و آجا که در تهدیدات و فناوری‌های نوین صاحب‌نظر بوده و دارای ویژگی‌هایی از جمله: دارای مدرک تحصیلی کارشناسی ارشد و دکتری، دارای جایگاه ۱۸ به بالا، دارای سابقه خدمت در مشاغل راهبردی، دارای آثار علمی و پژوهشی در زمینه عنوان اصلی موردبررسی در این تحقیق که با توجه به تخصصی بودن عنوان تحقیق و محدودیت افراد خبره و صاحب‌نظر، جامعه آماری و جامعه نمونه بر هم منطبق و روش نمونه‌گیری به صورت تمام شمار انتخاب شدند.

روایی و پایایی پرسشنامه:

روایی: روایی صوری و محتوایی این پرسشنامه توسط محققین بر روی یک گروه ۱۱ نفره از خبرگان حوزه تهدیدشناسی و آینده‌پژوهی موردبررسی قرار گرفت و سپس سؤالات اولیه در قالب سه عبارت «مناسب است- مناسب است ولی نیاز به تغییر دارد- مناسب نیست» و با استفاده از شاخص روایی محتوایی برای هر سؤال بر اساس رابطه زیر محاسبه شد:

$$N: \text{تعداد کل متخصصین (برابر با ۱۱ نفر)} \\ CVR = \frac{n_e - N/2}{N/2}$$

n_e : تعداد متخصصینی که گزینه «مناسب است» انتخاب کردند.

برای تحلیل و ارزیابی عوامل شناسایی شده در بین جامعه آماری، با استفاده از متغیرهای احصاء شده از مطالعات کتابخانه‌ای و همچنین خروجی پیشنهادی خبرگان، پرسشنامه پژوهش تدوین گردید. به منظور تأیید روایی محتوایی پرسشنامه از ضریب لاوشه استفاده شد که بر اساس نتایج پس از بررسی و ویرایش تعدادی از گویه‌های پرسشنامه، این ضریب در حد خوب (امتیاز ۷۶) ارزیابی گردید.

پایایی:

برای آزمودن پایایی پرسش‌نامه که با طیف لیکرت طراحی شد، از ضریب آلفای کرون باخ و نرم‌افزار آماری SPSS استفاده گردید. این روش برای محاسبه هماهنگی درونی ابزار اندازه‌گیری که خصیصه‌های مختلف را اندازه‌گیری می‌کند به کار می‌رود. در صورتی که میزان آلفای کرون باخ بیش

از ۰/۷ باشد پرسش‌نامه از پایایی لازم برخوردار بوده و هر چه این مقدار به ۱ نزدیک‌تر باشد پرسش‌نامه از پایایی بالاتری برخوردار است. نتیجه نهایی ضریب آلفای کرونباخ ۰,۸۰۸ را نشان داد که بیانگر پایایی قابل قبول پرسشنامه است.

یافته‌های تحقیق

در جداول زیر اطلاعات جمعیت شناختی حجم نمونه شامل سنوات خدمتی، میزان تحصیلات و مشاغل خدمتی آورده شده است.

جدول (۳): توزیع مربوط به سنوات خدمتی حجم نمونه

توزیع سن خدمتی	فراوانی F	فراوانی نسبی	فراوانی درصد
۲۷ تا ۲۵ سال	۲۷	۰,۳۲	۳۲
۲۸ تا ۳۰ سال	۳۲	۰,۳۷	۳۷
بیش از ۳۰ سال	۲۶	۰,۳۱	۳۱
جمع	۸۵	۱	۱۰۰

با توجه به اینکه تمامی افراد حجم نمونه، بالای ۲۵ سال سنوات خدمتی دارند، درمی‌یابیم که جامعه آماری از تجربه کافی جهت پاسخگویی به سؤالات پرسشنامه برخوردار است.

جدول (۴): توزیع مربوط به میزان تحصیلات حجم نمونه

توزیع تحصیلات	فراوانی F	فراوانی نسبی	فراوانی درصد
کارشناسی ارشد	۴۸	۰,۵۶۴	۵۶,۴
دکتری	۳۷	۰,۴۳۶	۴۳,۶
جمع	۸۵	۱	۱۰۰

از آنجاکه همه افراد حجم نمونه دارای مدرک تحصیلی حداقل کارشناسی ارشد هستند، بنابراین جامعه آماری از دانش کافی جهت پاسخگویی به سؤالات پرسشنامه برخوردار است.

جدول (۵): توزیع مربوط به مشاغل خدمتی حجم نمونه

توزیع مشاغل	فراوانی F	فراوانی نسبی	فراوانی درصد
آموزشی	۲۰	۰,۲۳۵	۲۳,۵
عملیاتی	۴۸	۰,۵۶۴	۵۶,۴
فرماندهی	۱۷	۰,۲۰۱	۲۰,۱

۱۰۰	۱	۸۵	جمع
-----	---	----	-----

با توجه به اینکه بیش از ۷۶٪ از افراد حجم نمونه شغل فرماندهی و عملیاتی دارند، بنابراین جامعه آماری از نگرش و بینش کافی جهت پاسخگویی به سؤالات پرسشنامه برخوردار است.

تجزیه و تحلیل داده‌ها

به‌منظور احصاء مؤلفه‌ها و شاخص‌های تهدیدات فناوری‌های نوین، مطالعات اکتشافی و تفکر دقیق در مبانی نظری، ادبیات تحقیق و مصاحبه با خبرگان مدنظر قرار گرفت و بر اساس گام‌های زیر اقدام شد:

گام اول (پالایش): در این گام کلیه اطلاعات و داده‌هایی که گردآوری شده بر اساس اهداف تحقیق جداسازی و دسته‌بندی گردید.

گام دوم (تلخیص): در این گام نتایج گام اول که جدا شده، بر اساس عوامل و شاخص‌های تبیین شده، مورد تشریح و بیان قرار گرفت.

گام سوم (نمایش داده‌ها): در این گام با توجه به گام قبلی، اطلاعات و داده‌های تحلیل شده بر اساس سؤالات و اهداف تحقیق استنباط و استخراج شد.

پس از انجام مراحل گفته شده در نهایت تعداد ۳ مؤلفه و ۱۱ شاخص احصاء گردید که در جدول (۶) نشان داده شده است.

جدول (۶): مؤلفه‌ها و شاخص‌های تهدیدات فناوری‌های نوین

مفهوم	مؤلفه‌ها	شاخص‌ها
تهدیدات فناوری‌های نوین	سایبری آینده/ سربازان	الکترونیکی شدن تجهیزات سبک و فردی سربازان
		فناوری پیشرفته اطلاع‌رسانی
		به‌کارگیری سیستم‌های ویدئویی و اینترنتی
	مصنوعی هوش	هوشمندسازی تجهیزات
		تصمیم‌گیری و کنترل بهینه
		تجزیه و تحلیل کلان داده‌ها
		بینایی رایانه‌ای
	روبات‌ها	کاهش تلفات نیروی انسانی
		قابلیت اجرای عملیات امداد و نجات
ایفای ایده‌آل نقش پشتیبانی از نیروها		

آمار توصیفی

به‌منظور بررسی توصیفی ابعاد، مؤلفه و شاخص‌های پرسشنامه با بهره‌مندی از نرم‌افزار SPSS از شاخص مرکزی (میانگین)، دامنه تغییرات (ماکزیمم و مینیمم) و شاخص پراکندگی (انحراف استاندارد و واریانس) استفاده شده که نتایج آن در جداول زیر آمده است.

جدول (۷): توصیف مؤلفه‌های پژوهش

Descriptive Statistics							مؤلفه‌ها
Variance	Std. Deviation	Mean		Maximum	Minimum	N	
Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Statistic	
۰,۵۶۰	۰,۷۴۸۵	۰,۰۸۸۲۱	۴,۰۴۱	۵,۰۰	۳	۸۵	سربازان آینده/ سایبری
۰,۵۵۳	۰,۷۴۳۵	۰,۰۸۷۲۶	۴,۱۹۴	۵,۰۰	۳	۸۵	روبات‌ها
۰,۷۴۵	۰,۸۶۲۹	۰,۱۰۱۷۰	۳,۹۴۴	۵,۰۰	۳	۸۵	هوش مصنوعی

خروجی اولیه نشان داد مؤلفه‌های روبات‌ها، سربازان آینده سایبری و هوش مصنوعی از میانگین بالاتری نسبت به سایر مؤلفه‌ها برخوردار هستند که برای بررسی دقیق‌تر ساختار، نیاز به آزمون‌های توصیفی است.

جدول (۸): توصیف شاخص‌های پژوهش

Descriptive Statistics							شاخص‌ها
Variance	Std. Deviation	Mean		Maximum	Minimum	N	
Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Statistic	
۱,۰۱۷	۱,۰۰۹	۰,۰۰۹	۴,۲۸۳	۵	۳	۸۵	الکترونیکی شدن تجهیزات سبک و فردی سربازان
۱,۰۰۷	۱,۰۰۳	۰,۰۰۹	۴,۱۸۵	۵	۳	۸۵	فناوری پیشرفته اطلاع‌رسانی
۱,۱۸۴	۱,۰۸۸	۰,۰۱۰	۴,۰۶۸	۵	۳	۸۵	به‌کارگیری سیستم‌های ویدیویی و اینترنتی
۱,۲۴۶	۱,۱۱۶	۰,۰۱۰	۳,۹۰	۵	۴	۸۵	هوشمندسازی تجهیزات
۰,۹۹۹	۰,۹۹۹	۰,۰۰۹	۳,۹۷	۵	۱	۸۵	تصمیم‌گیری و کنترل بهینه
۰,۹۹۸	۰,۹۹۹	۰,۰۱۰	۳,۹۶	۵	۲	۸۵	تجزیه و تحلیل کلان داده‌ها
۱,۱۰۹	۱,۰۵۳	۰,۰۱۱	۳,۹۹	۵	۳	۸۵	بینایی رایانه‌ای
۱,۱۷۸	۱,۰۸۵	۰,۰۱۲	۴,۱۱۷	۵	۳	۸۵	کاهش تلفات نیروی انسانی
۱,۱۸۱	۱,۰۸۷	۰,۰۱۰	۴,۰۶۵	۵	۲	۸۵	قابلیت اجرای عملیات امداد و نجات
۰,۹۹۲	۰,۹۹۶	۰,۰۱۰	۴,۱۲۵	۵	۱	۸۵	ایفای ایده‌آل نقش پشتیبانی از نیروها

به‌منظور شناسایی آزمون‌های مناسب برای تحلیل آماری، سنجش پارامتریک (نرمال) بودن داده‌های آماری را انجام می‌دهیم؛ اگر داده‌ها نا پارامتریک باشند از آزمون کای دو (χ^2) و در غیر این صورت از آزمون تی تک نمونه‌ای (t) استفاده می‌شود. به همین منظور و با توجه به اینکه برای پرسش‌نامه‌هایی با طراحی طیف لیکرت، آزمون چولگی مناسب‌ترین آزمون نرمال سنجی است، از این آزمون استفاده شده است.

جدول (۹): نتایج آزمون چولگی

مؤلفه‌ها	تعداد	میانگین	انحراف استاندارد د	کشیدگی		چولگی	
				Statisti c	Std. Error	Statisti c	Std. Error
الکترونیکی شدن تجهیزات سبک و فردی سربازان	۸۵	۴,۰۴۱	۰,۰۸۸۲	۰,۳۸۹	۰,۵۹۸-	۰,۳۰۲	۰,۵۸۷-
فناوری پیشرفته اطلاع‌رسانی	۸۵	۳,۸۱۹	۰,۱۰۳۴	۰,۵۷۵	- ۰,۸۶۴	۰,۳۰۲	۰,۲۹۵-
هوشمند سازی تجهیزات	۸۵	۳,۹۴۴	۰,۱۰۱۷	۰,۴۵۸	۰,۷۵-	۰,۳۰۴	۰,۰۲۶
به‌کارگیری سیستم‌های اینترنتی و ویدئویی	۸۵	۴,۱۹۴	۰,۰۸۷۶ ۶	۰,۶۴۰	۰,۹۸-	۰,۳۰۲	۰,۲۴۵
تصمیم‌گیری و کنترل بهینه	۸۵	۴,۰۰۹	۰,۰۸۲۷	۰,۷۶۸	۰,۵۹۰	۰,۸۷۸-	۰,۰۹۳
تجزیه و تحلیل کلان داده‌ها	۸۵	۳,۸۰۵	۰,۰۸۷۶	۰,۷۲۲	۰,۵۲۲	۰,۹۸۴-	۰,۰۷۱
بینایی رایانه‌ای	۸۵	۴,۱۲۵	۰,۰۸۸۳	۰,۷۸۹	۰,۶۲۴	۰,۸۸۳-	۰,۰۶۹
کاهش تلفات نیروی انسانی	۸۵	۳,۷۵۰	۰,۰۸۵۶	۰,۹۰۷	۰,۸۲۴	۰,۸۷۰-	۰,۱۹۳
قابلیت اجرای عملیات امداد و نجات	۸۵	۳,۸۷۵	۰,۰۹۰۵ ۱	۰,۸۸۱	۰,۷۷۷	۱,۰۵۳-	۰,۲۱۲
ایفای نقش پشتیبانی از نیروها	۸۵	۳,۵۶۹	۰,۱۱۸۳ ۹	۰,۸۶۵	۰,۷۴۸	۰,۵۳۳-	۰,۰۸۸

نتایج نشان می‌دهد میزان چولگی در بازه (۲,۲-) قرار دارد و داده‌های آماری با احتمال ۹۵٪ (با خطای ۵٪)، در ساختار متغیرها پارامتریک هستند. به عبارت دیگر داده‌های آماری، حول میانگین جامعه پراکندگی داشته‌اند.

در ادامه با توجه به پارامتریک بودن داده‌های آماری از آزمون تی تک نمونه‌ای برای بررسی سطح نظرات مخاطبین و همچنین سنجش اختلاف داشتن یا نداشتن میانگین کلی نظرات

مخاطبین با سطح متوسط رضایت آن‌ها استفاده شد که در طیف لیکرت حد آستانه رضایت‌مندی ضریب ۳ در نظر گرفته شده است تا بتوان با در نظر گرفتن سایر آزمون‌های آماری، کاهش یا افزایش رضایت نسبی مخاطبین از سطح متوسط موردسنجش قرار گیرد.

جدول (۱۰): نتایج آزمون تی تک نمونه‌ای برای مؤلفه‌های پژوهش

One-Sample Test						مؤلفه‌ها
۹۵% Confidence Interval of the Difference		Mean Difference	Sig. (۲-tailed)	Df	T	
Upper	Lower					
۱,۵۵	۰,۰۵	۰,۷۵۰	۰,۰۰۸	۸۴	۳,۰۰۰	سربازان آینده سایبری
۱,۵۱	۰,۶۲	۱,۰۶۷	۰,۰۰۰	۸۴	۵,۱۷۲	هوش مصنوعی
۱,۲۱	۰,۴۱	۰,۸۱۳	۰,۰۰۱	۸۴	۴,۳۳۳	روبات‌ها

جدول (۱۱): نتایج آزمون تی تک نمونه‌ای برای شاخص‌های پژوهش

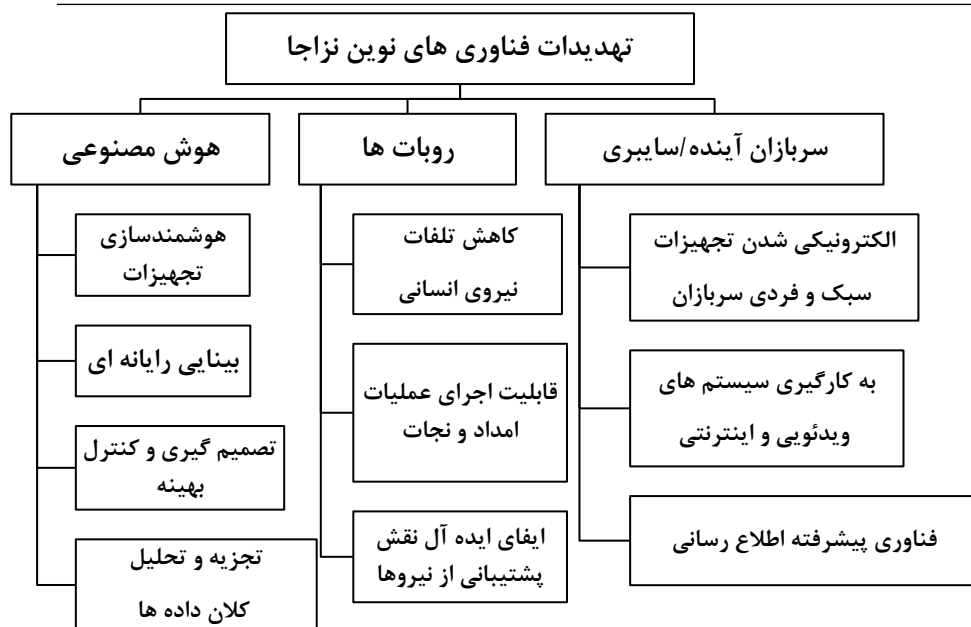
One-Sample Test						شاخص‌ها
۹۵% Confidence Interval of the Difference		Mean Difference	Sig. (۲-tailed)	Df	T	
Upper	Lower					
۱,۳۴	۱,۰۰	۱,۱۶۹	۰,۰۰۰	۸۴	۱۳,۷۱۴	الکترونیکی شدن تجهیزات سبک و فردی سربازان
۱,۰۶	۰,۷۴	۰,۹۰۰	۰,۰۰۰	۸۴	۱۱,۳۶۳	فناوری پیشرفته اطلاع‌رسانی
۱,۱۸	۰,۷۱	۰,۹۴۴	۰,۰۰۰	۸۴	۸,۱۰۸	به‌کارگیری سیستم‌های ویدیویی و اینترنتی
۱,۳۳	۰,۹۳	۱,۱۲۹	۰,۰۰۰	۸۴	۱۱,۱۱۰	هوشمند سازی تجهیزات

۱,۵۵	۱,۲۱	۱,۳۸۰	۰,۰۰۰	۸۴	۱۶,۰۵۵	تصمیم‌گیری و کنترل بهینه
۱,۳۵	۰,۸۲	۱,۰۸۳	۰,۰۰۰	۸۴	۸,۱۷۰	تجزیه و تحلیل کلان داده‌ها
۱,۴۲	۰,۷۵	۱,۰۸۸	۰,۰۰۰	۸۴	۶,۵۷۵	بینایی رایانه‌ای
۱,۴۲	۰,۷۹	۱,۱۰۳	۰,۰۰۰	۸۴	۷,۱۱۵	کاهش تلفات نیروی انسانی
۱,۲۲	۰,۷۸	۱,۰۰	۰,۰۰۰	۸۴	۹,۰۸۳	قابلیت اجرای عملیات امداد و نجات
۱,۴۶	۱,۰۵	۱,۲۵۵	۰,۰۰۰	۸۴	۱۲,۰۴۳	ایفای ایده‌آل نقش پشتیبانی از نیروها

با توجه به سطح خطای ۰,۰۵ در تحلیل داده‌های آماری و این‌که در ستون خروجی Sig تحلیل به ۰,۰۰۰ رسیده است (کم‌تر از سطح خطای پیش‌بینی‌شده)، به این نتیجه می‌رسیم که میانگین کلی نظرات مخاطبین به‌صورت نسبی با سطح متوسط آن تفاوت دارد که با توجه به خروجی کلی تحلیل توصیفی می‌توان این تفاوت را در جهت بیشتر از حد متوسط تفسیر نمود. به‌عبارت‌دیگر با یک اطمینان ۹۵ درصدی می‌توان گفت که بخش قابل‌توجهی از مخاطبین از روند فعالیت‌های صورت گرفته یک رضایت نسبی (بیشتر از حد متوسط) دارند. از طرفی چون هر دو دامنه‌ی آزمون مربوط به متغیرها مثبت است، می‌توان گفت اهمیت متغیرها مورد تأیید مخاطبین قرار گرفته است.

نتیجه‌گیری

پس از انجام مطالعات کتابخانه‌ای، بررسی اسناد معتبر و سایت‌های اینترنتی مرتبط با موضوع پژوهش و همچنین انجام مصاحبه با خبرگان، در پاسخ به سؤال اصلی و سؤال‌های فرعی تحقیق و بر مبنای نتایج به‌دست‌آمده از تجزیه و تحلیل استنباطی و توصیفی، الگویی شامل سه مؤلفه (هوش مصنوعی، روبات‌ها و سربازان آینده/سایبری) و ۱۰ شاخص در حوزه تهدیدات فناوری‌های نوین نزاچا احصاء گردید که این الگو به روش درختی در شکل زیر آمده است:



پیشنهادها

- ۱- در خصوص تدوین راهبردها و یا ارائه الگوی راهبردی دفاع در مقابل هرکدام از حوزه‌های تهدیدات فناوری‌های نوین نزاجا پژوهش‌های جامعی صورت پذیرد.
- ۲- به‌منظور فراگیری و پوشش کامل تهدیدات فناوری‌های نوین در سطح ارتش، در پژوهش‌های مستقل چگونگی این تهدیدات در سایر نیروهای تابعه ارتش مورد مطالعه قرار گیرد.
- ۳- با عنایت به اهمیت بالای تهدیدات فناوری‌های نوین در جنگ‌های آینده، برنامه‌ریزی بلندمدت برای مقابله با این تهدیدات با همکاری نخبگان کشوری و لشگری به‌عنوان یکی از دغدغه‌های فرماندهان عالی‌رتبه نیروی زمینی مدنظر قرار گیرد.

منابع

- قرآن کریم، ترجمه و تفسیر آیت‌الله مکارم شیرازی.
- بیانات و رهنمودهای رهبر معظم انقلاب حضرت امام خامنه‌ای مد ظله العالی.
- آزادی، فرزاد (۱۴۰۰)، "تأثیر تهدیدات آینده بر تئوری بازی جنگ"، مانز، چاپ یکم.
- آهنگری، عرفان؛ سلطان‌آبادی، محمد؛ رضایی، احمد (۱۳۹۸)، "واکاوی تهدیدات و چالش‌های دفاعی - نظامی جنگ‌های آینده"، فصلنامه مطالعات جنگ، سال اول، شماره دوم، صص ۱۴۷-۱۳۲.

- اسکندری، حمید (۱۳۹۰)، "تهدیدات سخت"، بوستان حمید، چاپ یکم.
- افتخاری، اصغر (۱۳۹۰)، "برآورد نظامی تهدید"، انتشارات دانشگاه عالی دفاع ملی.
- بختیاری، حسین؛ صالح نیا، علی (۱۳۹۷)، "اولویت‌بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیل سلسله‌مراتب (AHP)، فصلنامه مطالعات راهبردی سیاست‌گذاری عمومی، دوره ۸، شماره ۲۷.
- ریاضی، وحید و همکاران (۱۴۰۰)، "معرفی مؤلفه‌ها و ابزارهای جنگ ترکیبی آمریکا علیه ج.ا. ایران"، فصلنامه راهبرد دفاعی، دوره ۱۹، شماره ۱.
- خسروی، عباس (۱۳۹۹)، "الگوی جامع رصد تهدیدهای همه‌جانبه"، فصلنامه علمی امنیت ملی، سال ۱۱، شماره ۳۹، صص ۶۷-۹۴.
- سنچولی، زینب (۱۳۹۶)، "تبیین ماهیت الگوی اسلامی ایرانی پیشرفت"، فصلنامه علمی مطالعات الگوی پیشرفت اسلامی ایرانی، دوره ۲، شماره ۳، صص ۷۹-۱۰۴.
- طاهری‌هشی، علی؛ دهقان، حبیب‌اله؛ نادری، علیرضا (۱۳۹۷)، "شناسایی و اولویت‌بندی نوع تهدیدات درصحنه جنگ‌های آینده"، فصلنامه آینده‌پژوهی دفاعی، سال سوم، شماره ۹، صص ۷۹۱ - ۷۸۱.
- طاهری، علی (۱۳۹۵)، "مختصات الگوی تهدیدات صحنه نبردهای آینده در سال ۱۴۰۴"، فصلنامه آینده‌پژوهی دفاعی، شماره اول، صص ۱۲۷ - ۱۰۹.
- فرهنگ، سجاد؛ آروند، حمید. (۱۴۰۲). تأثیر کاربرد هوش مصنوعی در بازی جنگ برای بهبود عملکرد شناختی در نبردهای دریایی آینده، فصلنامه مدیریت نظامی، ۲۳(۴)، ۵۷-۷۸.
- کاظم‌پور، زکریا؛ بهرامی، محسن (۱۳۹۷)، "الگوی ارزیابی تهدیدات هوشمند آینده به روش تحلیل کالبدی تهدید"، فصلنامه آینده‌پژوهی دفاعی، سال سوم، شماره ۱۰، صص ۱۴۷-۱۲۱.
- کلانتری، فتح‌اله (۱۳۹۵)، "مشخصات جنگ‌های احتمالی آینده علیه ج.ا.ایران و راهبردهای مقابله با آن"، فصلنامه راهبرد دفاعی، دوره ۱۴، شماره ۵۶، صص ۱۳۱-۱۰۳.
- مرادیان، حسن؛ صادقی گوغری، سعید (۱۳۹۲)، "آینده‌پژوهی تهدیدات نظامی آمریکا علیه ج.ا.ایران"، فصلنامه علمی پژوهشی امنیت پژوهشی، سال ۱۲، شماره ۴۳، صص ۱۷۱-۱۴۵.
- مرادیان، محسن؛ صادقی، سعید (۱۳۹۷)، "آینده‌پژوهی تهدیدات نظامی آمریکا علیه جمهوری اسلامی ایران"، فصلنامه امنیت پژوهی، شماره ۴۳، صص ۱۷۰ - ۱۴۵.
- مشهدی، حسن؛ امینی‌ورکی، سعید (۱۳۹۴)، "تدوین و ارائه الگوی ارزیابی تهدیدات، آسیب‌پذیری و تحلیل خطرپذیری زیرساخت‌های حیاتی با تأکید بر پدافند غیرعامل"، فصلنامه مدیریت بحران، شماره هفتم.

- مهدیان، حسین؛ ترکاشوند، جلال (۱۳۹۹). الگوی نظام‌مند دفاع از منظر اندیشه دفاعی مقام معظم فرماندهی کل قوا (مدظله‌العالی)، فصلنامه مدیریت نظامی، سال هشتم، شماره ۶.
- مهدیان، حسین؛ ترکاشوند، جلال (۱۴۰۱). الگوی نظام‌مند جهاد تبیین از منظر مقام معظم فرماندهی کل قوا (مدظله‌العالی)، فصلنامه مدیریت نظامی، سال دوم، شماره ۸.
- میلز، گرگ (۱۳۹۸)، "دستور کار امنیتی قرن ۲۱"، حیدر علی بلوچی، انتشارات دانشگاه عالی دفاع ملی.
- نائینی، علی‌محمد (۱۳۸۹)، "بررسی تطبیقی سه‌گانه سخت، نیمه سخت و نرم"، فصلنامه راهبرد دفاعی، شماره ۳۰، صص ۱۷۷ - ۱۵۸.
- هلیلی، خداداد؛ مظلوم، جلیل؛ هادیان، بهرنگ (۱۳۹۴)، "جنگ‌های آینده"، فصلنامه علوم و فنون، دوره ۱۱، شماره ۳۳، صص ۶۳-۴۷.

- Nurul Huda Mahmood, Gilberto Berardinelli, Emil J. Khatib, Ramin Hashemi, Carlos De Lima, Matti latva-aho, "A functional architecture for ۶G special-purpose industrial IoT networks", IEEE Transac. Ind. Inf (۲۰۲۲).
- Bomin Mao, Jijia Liu, Yingying Wu, Nei Kato, Security and privacy on ۶G network edge: a survey, IEEE Commun. Surv. & Tutorials (۲۰۲۳)
- Innocent D. Lubangakene, Bal Virdee, Renu Karthick Rajaguru Jayanthi, Priyanka Ganguly, Effect of metabolite and temperature on artificial human sweat characteristics over a very wide frequency range (۴۰۰ MHz-۱۰.۴ GHz) for wireless hydration diagnostic sensors, Results Eng. ۱۹ (۲۰۲۳).
- Tuan-Vinh Le, Chung-Fu Lu, Chien-Lung Hsu, Trung K. Do, Yen-Fang Chou, Wei-Cheng Wei, A novel three-factor authentication protocol for multiple service providers in ۶G-aided intelligent healthcare systems, IEEE Access ۱۰ (۲۰۲۲).
- Guanjie Li, Chengzhe Lai, Rongxing Lu, Zheng Dong, SecCDV security reference architecture for cybertwin-driven ۶G V۲X, IEEE Transac. Vehicular Technol (۲۰۲۲).