

Preparedness and Response to Modern Warfare Threats: A Look into the Future

Hassan Araghizadeh¹, Mohammad Gharari^{2*}

¹ Trauma Research Center, Baqiyatallah University of Medical Sciences, Tehran, Iran

² Ghaem Pars University of Industries, Tehran, Iran

Received: 6 October 2024 Accepted: 1 November 2024

Abstract

Background and Aim: Identifying, predicting, and evaluating the threats posed by emerging technologies, with indicators such as accurate and precise threat recognition, and assessing the threat's power and capacity to safeguard the interests of our beloved country in future battles, is a crucial matter. Generating new and appropriate ideas in the field of technological threats and providing a clear picture of the most important future threats will help develop and plan effective responses to threats and prevent surprises. The purpose of this study is to gain a better understanding of the roadmap and the need for the transformation of science and technology in health, relief, and medical treatment for the armed forces in preparing for and responding to modern warfare threats.

Methods: This qualitative study was conducted using the content analysis method of documents. First, by reviewing electronic resources, all available documents and articles related to preparedness and response to modern warfare threats were identified. After a multi-stage screening, 20 documents were finally selected and analyzed after coding.

Results: Based on the findings of this study, threat assessments in modern warfare include artificial intelligence, the Internet of Things, robots, enhanced humans, unmanned technologies (drones), biological, chemical, and nuclear events and threats, cyber/electromagnetic events and threats, gene editing technologies and gene weapons, genetically modified products, quantum biology, cyborgs, cognitive warfare, and more.

Conclusion: Planning, up-to-date, and comprehensive periodic training and exercises for the armed forces' medical centers in providing an appropriate response to mission requirements in dealing with modern warfare threats can save the lives of the wounded and injured and improve the healing process.

Keywords: Preparedness, Modern Warfare, Threats, Health, Relief and Medical Treatment.

* Corresponding Author: Mohammad Gharari

Address: Ghaem Pars University of Industries, Tehran, Iran.

E-mail: m.gharari@yahoo.com



آمادگی و مقابله با تهدیدات جنگ نوین با نگاهی به آینده

حسن عراقی زاده^۱، محمد قراری^{۲*}

^۱ مرکز تحقیقات تروما، دانشگاه علوم پزشکی بقیه الله (عج)، تهران، ایران

^۲ دانشگاه صنایع قائم (عج) پارس، تهران، ایران

دریافت مقاله: ۱۴۰۳/۰۷/۱۸ پذیرش مقاله: ۱۴۰۳/۰۹/۱۱

چکیده

زمینه و هدف: 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. تولید ایده‌های جدید و مناسب در زمینه تهدیدهای فناوری و ایفای تصویری روشن از مهم‌ترین تهدیدات آینده، به تدوین و طرح‌ریزی کارآمد پاسخ‌های مناسب به تهدیدات و جلوگیری از غافلگیری کمک خواهد نمود. هدف از این مطالعه درک بهتری از برنامه‌های پیش‌رو و نیاز برای تحول علم و فناوری بهداشت، امداد و درمان نیروهای مسلح در آمادگی و مقابله با تهدیدات جنگ نوین می‌باشد.

روش‌ها: این مطالعه کیفی به روش تحلیل محتوای اسناد انجام شد. ابتدا با مرور منابع الکترونیکی، تمامی اسناد و مقالات موجود مرتبط با آمادگی و مقابله با تهدیدات جنگ نوین شناسایی شد. پس از غربالگری چند مرحله‌ای نهایتاً ۲۰ سند انتخاب و پس از کدگذاری آنالیز انجام شد.

یافته‌ها: بر اساس یافته‌های این مطالعه مهمترین برآورد تهدیدات در جنگ نوین عبارتند از: هوش مصنوعی، اینترنت اشیا، ربات، انسان‌های تکامل‌یافته، فناوری‌های بدون سرنشین (پهپاد)، حوادث و تهدیدات زیستی، شیمیایی و هسته‌ای، حوادث و تهدیدات سایبری/الکترومغناطیسی، فناوری‌های ویرایش ژن و سلاح‌های ژنی، محصولات تراریخته، کوانتوم زیستی، موجودات سایبورگ، جنگ شناختی.

نتیجه‌گیری: برنامه‌ریزی، آموزش و تمرین‌های دوره‌ای به روز و جامع مراکز درمانی نیروهای مسلح، در پاسخگویی مناسب به نیازمندی‌های مأموریتی در مقابله با تهدیدات جنگ نوین می‌تواند جان مجروحان و مصدومان را نجات و موجب ارتقاء بهبود انجام فرایند درمان شود.

کلیدواژه‌ها: آمادگی، جنگ نوین، تهدیدات، بهداشت، امداد و درمان.

* نویسنده مسئول: محمد قراری

آدرس: دانشگاه صنایع قائم (عج) پارس، تهران، ایران.

ایمیل: m.gharari@yahoo.com

مقدمه

با سیری در روند جنگ‌های گذشته به این واقعیت پی می‌بریم که به مرور زمان و با به کارگیری دانش در عرصه‌های مختلف نبرد، رویکرد جنگ‌ها از انسان محوری در جنگ‌های ابتدایی به جنگ افزارمحوری در نسل‌های بعدی تغییر یافته؛ به گونه‌ای که سبب کم رنگ‌تر شدن حضور انسان در جنگ‌ها شده است. مفاهیمی چون جنگ دور ایستا، جنگ سایبری، جنگ افزارهای بدون سرنشین و ... شاهدی بر این مدعا است. بر این اساس در جنگ‌های آینده، برتری اطلاعاتی و دانشی، شایستگی محوری محسوب می‌شود (۱). ویژگی‌های کلیدی تسلیحات آینده و درگیری‌های نظامی آن، استفاده از وسایل نقلیه بدون سرنشین کاملاً رایج خواهد بود که احتمالاً منجر به درگیری فیزیکی بین آن‌ها می‌انجامد. پیش‌بینی می‌شود که درگیری‌های نظامی آینده بدون خونریزی باشد. علاوه بر این، بدون تخریب فیزیکی، دشمن با نفوذ در شبکه‌های برق و اطلاعات، سیستم‌های بانکی، اقتصادی و اجتماعی و ... آسیب می‌بیند و حتی در صورت خشونت، فناوری استفاده از آن را دقیق‌تر و مؤثرتر می‌کند. دقت هدف‌گیری به ویژه با استفاده از ابزارهای الکترونیکی بهبود می‌یابد. همچنین می‌توانیم شاهد یک جنگ محیطی پیچیده باشیم که می‌تواند بیماری‌های گیاهان و انسان‌ها را به حشرات یا هیبریدها سرایت کند. محصولات و دام‌ها را می‌توان از بین برد و انسان‌ها را ناتوان یا از بین برد. جهانی شدن، انتشار فناوری و اطلاعات به جامعه امکان دسترسی به فرصت‌های فناوری پیچیده را می‌دهد. این احتمال تعداد حملات تروریستی را افزایش می‌دهد (۲).

تهدیدات فناوری زمانی اهمیت خود را نشان می‌دهد که به عنوان سلاح به کار گرفته شود، 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. تولید ایده‌های جدید و مناسب در زمینه تهدیدهای فناوری و ایفای تصویری روشن از مهم‌ترین تهدیدات آینده، به تدوین و طرح‌ریزی کارآمد پاسخ‌های مناسب به تهدیدات و جلوگیری از غافلگیری کمک خواهد نمود (۳).

هدف این تحقیق کمک به توسعه علوم، فراهم نمودن زمینه لازم برای ارتقاء بهره‌وری، جهت‌گیری و جهت‌دهی‌های لازم به صنایع دفاعی، توسعه و تولید هدفمند تجهیزات و همچنین هم‌افزایی نظری و فکری میان تصمیم‌گیران راهبردی برای تأمین نیازهای مقابله با تهدیدات جنگ نوین در حوزه بهداشت، امداد و درمان نیروهای مسلح می‌باشد.

روش‌ها

مطالعه کیفی حاضر با استفاده از بررسی متون و بهره‌گیری از پایگاه‌های استنادی انجام شد. ابتدا با مرور منابع الکترونیک تمامی

اسناد، بازبینی‌ها و راهنماهای موجود مرتبط با تهدیدات جنگ نوین شناسایی شد. کلیه فایل‌های مولتی مدیا شامل صوتی، نوشتاری و تصویری مرتبط نیز از طریق جستجو در اینترنت و با مراجعه به وب سایت‌ها و پایگاه‌های داده‌ای و نیز تجارب و مشاهدات میدانی با کلیدواژه‌هایی مبتنی بر معیارهای فوق جستجو و جمع‌آوری گردید. جهت ورود داده‌ها، از کلیدواژه‌های مرتبط با آمادگی، جنگ نوین، تهدیدات، بهداشت، امداد و درمان و ... جهت جستجو در پایگاه‌های داده‌های معتبر استفاده شد.

فقط اسنادی که با ذکر مرجع مشخص و معتبر ارائه یا ابلاغ شده بودند، بررسی شدند و اسناد غیرمعتبر از مطالعه خارج شدند. سپس از شیوه تحلیل داده‌های متنی با عنوان کدگذاری باز استفاده شد. بدین صورت که کدها از متن مطالعات استخراج گردید (کدگذاری مرتبه اول) و سپس بر روی این کدهای مستخرج، مجدداً کدگذاری دیگری صورت گرفت که منجر به شکل‌گیری مفاهیم گردید (کدگذاری مرتبه دوم) و در آخر بر روی مفاهیم نیز کدگذاری دیگری صورت گرفت (کدگذاری مرتبه سوم) و مؤلفه‌ها استخراج گردید و سپس تلخیص داده‌ها صورت پذیرفت. در مرحله آخر، به تدوین و تحلیل داده‌ها پرداخته شد.

نتایج و بحث

یافته‌های به دست آمده نشان داد که در مطالعات گذشته در خصوص تهدیدات جنگ نوین در حوزه بهداشت، امداد و درمان به طور کامل بررسی نشده است. بنابراین با توجه به لزوم آمادگی برای شرایط پیش‌رو، آشنایی با این تهدیدات ضروری است. در این مطالعه تهدیدات جنگ نوین در حوزه بهداشت، امداد و درمان در ۲۳ بخش مورد بررسی قرار گرفته و سپس اهداف، سیاست‌ها، اولویت‌ها و ویژگی‌های کلی بهداشت، امداد و درمان نیروهای مسلح با توجه به ویژگی‌های تهدیدات جنگ نوین ارائه می‌گردد.

هوش مصنوعی برنده جنگ‌های آینده

پیشرفت‌های فناورانه، فنون نظامی را نیز دستخوش تغییر کرده است. حال و هوای حماسی جنگ‌ها تدریجاً جای خود را به فناوری‌های نظامی داده است و لشکری از ربات‌ها، پهپادها، ریزموجودات میکروسکوپی و ریزپرنده‌ها امواج مغناطیسی همه به صف شده‌اند. با توجه به توانایی عظیم هوش مصنوعی (Artificial Intelligence) در جنگ مدرن بسیاری از قدرتمندترین کشورها در جهان سرمایه‌گذاری‌های خود را برای ارتش و امنیت خود افزایش داده‌اند. با توجه به اینکه به زودی هوش مصنوعی عملاً همچون تمام دیگر شئون زندگی ما نقشی همواره فزاینده در امور نظامی ایفاء خواهد کرد احتمالاً هر چه می‌گذرد نقش انسان‌ها حتی در تصمیم‌گیری‌های اتمی بیشتر تقلیل خواهد یافت. بر این اساس هوش مصنوعی می‌تواند سلاح-های واقعی یا سایبری را به شکل فوری و مستقیم در دسترس قرار دهند؛ سلاح‌هایی که امکان تصمیم‌گیری برای حمله را بسیار سریعتر از انسان‌ها دارند. سیستم‌های هوش مصنوعی می‌توانند

یابلو بالارین اوسیتو، مشاور امنیت سایبری و عضو کارگروه رویه‌های نوظهور در موسسه ISACA می‌گوید: «سربازان آینده ممکن است با بیوتکنولوژی یا حتی نانوتکنولوژی ارتقاء یابند و این فناوری‌ها سربازان را قادر می‌سازند تا از آسیب‌های میدان نبرد جان سالم به در ببرند. اوسیتو در ادامه می‌وید که سربازان از اسکلت‌های رباتیک در کنار هواپیماهای تهاجمی بدون سرنشین کاملاً مستقل استفاده خواهند کرد. ژنرال رابرت کان پیش بینی کرده است که یک چهارم نیروهای آمریکایی تا سال ۲۰۳۰ از این نوع خواهند بود و ارتش این کشور را کوچک‌تر، مرگبارتر، قابل اعزام‌تر به هر نقطه‌ای از جهان و چابک‌تر خواهند کرد.

اوسیتو تصریح می‌کند: «استفاده از ربات‌ها و سیستم‌های خودمختار (خودروهای زمینی بدون سرنشین، اسکلت‌های رباتیک و حتی سیستم‌های جنگی مستقل) در جنگ‌ها می‌تواند خطرات را برای سربازان انسانی کاهش دهد و قابلیت‌ها در میدان نبرد را افزایش دهد (۷).

انسان‌های تکامل یافته

سرباز آینده یک خودروی جنگی مجهز است که یک شخص داخل آن است. اول از همه، این یک اسکلت بیرونی با ژنراتورهای زانوی بیونیک، صفحات بالستیک انعطاف‌پذیر برای محافظت از بدن و یک تفنگ تهاجمی یکپارچه است. سیستم واقعیت افزوده این امکان را می‌دهد که به سرعت و با کیفیت، مبارزان (دوست-دشمن) را شناسایی نموده و بر اساس نقشه نبرد آنلاین تصمیم گرفته شود. جدیدترین سیستم‌های هدست دارای حفاظت صدا، رابط تطبیق‌پذیر، سلاح‌ها و سیستم‌های اصلی خواهند بود. انواع جدیدی از استتار نیز در حال توسعه هستند، از جمله منسوجات الکترونیکی، منسوجات هوشمند و استتار چند طیفی را می‌توان نام برد (۸). همچنین واقعیت مجازی و واقعیت افزوده به سربازان اجازه خواهند داد تا از دریچه نگاه هواپیماهای بدون سرنشین یا خودروهای با خلبان رباتیک و به کمک نمایشگرهای هدآپ (نمایشگرهایی که روی سر و چشم خلبانان و سربازان قرار می‌گیرند) تصاویر میدان نبرد را مشاهده کنند (۷).

آندرسن چنگ، موسس و رئیس اجرایی کمپانی-Post Quantum در این زمینه هشدار داده و می‌گوید: «کامپیوترهای کوانتومی جدید قادر خواهند بود حملات مخربی را ممکن سازند که می‌توانند شبکه‌های انرژی و سیستم بانکداری جهانی را از بین ببرند. کامپیوترهای کوانتومی به جای صفر و یک از بیت‌های کوانتومی استفاده می‌کنند که می‌توانند همزمان هر دوی آن‌ها باشند و سطح بی سابقه‌ای از قدرت محاسباتی را ممکن کنند.

محققان امنیتی نگرانند که قدرت کامپیوترهای کوانتومی بتواند رمزنگاری کلید عمومی (PKI) را ناکارآمد سازد. این فناوری برای امنیت اطلاعات در همه حوزه‌ها، از بانکداری گرفته تا ارتش مورد استفاده قرار گرفته است. چنگ تصریح می‌کند: «کامپیوترهای کوانتومی میلیون‌ها برابر سریع‌تر از «کامپیوترهای کلاسیک»

اهداف و تکنیک‌ها را سریع‌تر از انسان درک کرده و بر اساس هر تغییر ایجاد شده تصمیم جدیدی بگیرند. شناسایی مؤلفه‌های تأثیرگذار هوش مصنوعی و سایبر و تأثیر ابعاد آن در صحنه نبرد جنگ‌های آینده، باعث تقویت بررسی فرآیندهای عملیاتی و ایجاد درک صحیح از شرایط صحنه نبرد برای تصمیم‌گیران جهت اخذ تصمیم‌گیری‌های به موقع، مؤثر، نوآورانه و در نهایت کاهش خطای انسانی در سطوح راهبردی عملیاتی و تاکتیکی خواهد شد (۴).

اینترنت اشیاء

در عصر حاضر، ظرفیت بالای اینترنت اشیاء برای روزآمدسازی جنگ افزارها، 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. از طرف دیگر حوزه سلامت هوشمند نیز یکی از پرکاربردترین زیرحوزه‌های اینترنت اشیاء محسوب می‌گردد. تلفیق این دو حوزه عملکردی باعث هم افزایی و بالا بردن قابلیت‌های کاربردی اینترنت اشیاء در صحنه نبرد می‌گردد. همگرایی اینترنت اشیاء نظامی با پزشکی در صحنه نبرد، قابلیت‌های ارتقاء یافته‌ای را ایجاد نموده که می‌تواند هم‌افزایی و بهره‌وری در صحنه نبرد و اثر بخشی اقدامات و یکپارچگی در سامانه‌های فرماندهی و کنترل را افزایش دهد (۵).

اینترنت اشیاء در صنایع نظامی شامل طیف وسیعی از دستگاه‌هایی می‌شود که دارای توانایی‌های مختلف از طریق رابط‌های مجازی یا سایبری هستند که در سیستم‌ها ادغام شده‌اند. این دستگاه‌ها شامل مواردی مانند حسگرها، وسایل نقلیه، ربات‌ها، پهپادها، دستگاه‌های پوشیدنی برای انسان، بیومتریک، مهمات، زره پوش، سلاح و سایر فناوری‌های هوشمند می‌شوند.

کاربردهای نظامی اینترنت اشیاء شامل شبکه‌ای از سنسورها، پوشیدنی‌ها و دیگر دستگاه‌های (Internet of Things: IoT) است که از محاسبات ابری و لبه‌ای برای ایجاد یک نیروی جنگ منسجم استفاده می‌کند. با توجه به پیشرفت‌های صورت گرفته در خصوص کاربرد اینترنت اشیاء در صنایع نظامی، آگاهی از تمامی تاکتیک‌های جنگ الکترونیک به منظور شناسایی تهدیدات میدان نبرد و شکست عملیات‌های الکترونیکی دشمن امری اجتناب‌ناپذیر برای کشورها محسوب می‌شود. از این رو ادغام سیستم‌های اینترنت اشیاء همچون سنسورها، محرک‌ها و سیستم‌های کنترل در زیرساخت‌های نظامی موجود، می‌تواند نیروی ارتش را کارآمدتر و مؤثرتر نماید.

باید گفت در جنگ‌های آینده دیگر سرباز، تانک و توپ خانه نقش اساسی در نتایج یک جنگ را رقم نمی‌زند، بلکه این دستگاه‌های هوشمند همچون رایانه‌ها و سامانه‌های کنترل و فرماندهی نوین هستند که با داشتن توانایی در ایجاد ارتباط و دریافت اطلاعات سرنوشت نهایی جنگ را تعیین می‌کنند (۶).

ربات‌ها

قدرتمند، رمزگشایی شوند. وی در این باره می‌گوید: «هر داده‌ای که بتواند در ۵ تا ۱۵ سال آینده نیز همچنان حساس باشد و با استانداردهای ایمن کوانتومی محافظت نشود، ممکن است به همین زودی از دست رفته تلقی شود (۷)».

فناوری‌های بدون سرنشین (پهپاد)

حوادث و تهدیدات زیستی

انواع تروریسم (بیو تروریسم، تروریسم کشاورزی، تروریسم شیمیایی، تروریسم پرتوی، تروریسم فیزیکی، تروریسم غذایی، تروریسم دارویی)

حوادث و تهدیدات شیمیایی

حوادث و تهدیدات هسته‌ای و پرتوی

حوادث و تهدیدات سایبری / الکترونیک (ریز پرنده‌ها)

و الکترومغناطیس

ترکیبی (سایبری، شیمیایی، زیستی و پرتوی) (CBRE)

بیماری‌های نوپدید و باز پدید و ناشناخته

فناوری‌های ویرایش ژن و سلاح‌های ژنی (پایان پروژه

ژنوم انسان - سرقت اطلاعات ژنتیکی، حفاظت از ژنوم و ...)

کوانتوم زیستی (زیست فناوری) و الکتروژنیک

روندها و ابر روندهای (Mega Trends & Trend)

حوزه سلامت

رصد وضعیت سلامت در سطح ملی و در سطح بین‌المللی حاکی از وجود تغییرات کلانی در نظام و ساختارهای سلامت، مدیریت سلامت و حتی تعریف سلامت می‌باشد، برخی از این روندها به دلیل پیشرفت‌های عظیم فناورانه و برخی به دلیل تغییر مناسبات اجتماعی و سبک زندگی می‌باشند. انسان، اندیشه و اقدامات او، در بروز این روندها، انفعال از آن‌ها و داشتن نقشی فعال در آن‌ها عنصری محوری است. برخی از ابرروندهای حاکم در حوزه سلامت بدین شرح می‌باشد:

- ۱) روندهای کلان نظام سلامت متأثر از فناوری‌های دیجیتال و هوش مصنوعی؛
- ۲) مراقبت‌های سلامت از راه دور و یا سلامت دیجیتال (Electronic Health, Mobile Health)؛
- ۳) سیستم‌های ثبت داده‌های بزرگ (Big Data) سلامت، و پردازش و تحلیل هوشمند آن‌ها و کاربرد آن‌ها در دانش سلامت؛
- ۴) اهمیت پزشکی P۴ که شامل پیش‌بینی، پیشگیری، تشخیص فردمحور و مشارکت بیمار بر اساس فناوری‌های امیکس در بستر توجه به تعاملات اجتماعی و فناوری‌های هوش مصنوعی؛
- ۵) تحولات سلامت مبتنی بر پدیده سالمندی (در سی سال آینده جمعیت سالمند کشور به ۲۵ درصد کل جمعیت خواهد رسید)؛
- ۶) تغییر در الگوی اپیدمیولوژیک بیماری‌ها و پر رنگ شدن

خواهند بود، به لطف این واقعیت که آن‌ها از «کیوبیت» استفاده می‌کنند که می‌تواند یک، صفر یا همزمان هر دوی آن‌ها باشد. این بهبود توانی به این معنی است که ما روزی شاهد جهش در فناوری کوانتومی خواهیم بود و باید قبل از این اتفاق آماده باشیم نه اینکه بعد از محقق شدن آن واکنش نشان دهیم.

یک رقابت تسلیحات کوانتومی مخفیانه در حال رخ دادن است که وضعیت دقیق آن را نمی‌دانیم. زمانی که یک کامپیوتر با قدرت کافی عملیاتی شود، ابری قارچی را در افق نخواهیم دید، بلکه باید انتظار حملاتی را داشته باشیم که همه چیز؛ از زیرساخت‌های انرژی گرفته تا مؤسسات مالی را تحت تاثیر قرار می‌دهند.

چنگ می‌گوید گروه‌هایی پیشاپیش در حال سرقت اطلاعات رمزنگاری شده هستند تا پس از فعال شدن یک کامپیوتر قدرتمند، رمزگشایی شوند. وی در این باره می‌گوید: «هر داده‌ای که بتواند در ۵ تا ۱۵ سال آینده نیز همچنان حساس باشد و با استانداردهای ایمن کوانتومی محافظت نشود، ممکن است به همین زودی از دست رفته تلقی شود (۷)».

کامپیوترهای کوانتومی

- ۱) آندرسن چنگ، موسس و رئیس اجرایی کمپانی Post-Quantum در این زمینه هشدار داده و می‌گوید: «کامپیوترهای کوانتومی جدید قادر خواهند بود حملات مخربی را ممکن سازند که می‌توانند شبکه‌های انرژی و سیستم بانکداری جهانی را از بین ببرند. کامپیوترهای کوانتومی به جای صفر و یک از بیت‌های کوانتومی استفاده می‌کنند که می‌توانند همزمان هر دوی آن‌ها باشند و سطح بی سابقه‌ای از قدرت محاسباتی را ممکن کنند.
- ۲) محققان امنیتی نگرانند که قدرت کامپیوترهای کوانتومی بتواند رمزنگاری کلید عمومی (PKI) را ناکارآمد سازد. این فناوری برای امنیت اطلاعات در همه حوزه‌ها، از بانکداری گرفته تا ارتش مورد استفاده قرار گرفته است. چنگ تصریح می‌کند: «کامپیوترهای کوانتومی میلیون‌ها برابر سریع‌تر از «کامپیوترهای کلاسیک» خواهند بود، به لطف این واقعیت که آن‌ها از «کیوبیت» استفاده می‌کنند که می‌تواند یک، صفر یا همزمان هر دوی آن‌ها باشد. این بهبود توانی به این معنی است که ما روزی شاهد جهش در فناوری کوانتومی خواهیم بود و باید قبل از این اتفاق آماده باشیم نه اینکه بعد از محقق شدن آن واکنش نشان دهیم.

۳) یک رقابت تسلیحات کوانتومی مخفیانه در حال رخ دادن است که وضعیت دقیق آن را نمی‌دانیم. زمانی که یک کامپیوتر با قدرت کافی عملیاتی شود، ابری قارچی را در افق نخواهیم دید، بلکه باید انتظار حملاتی را داشته باشیم که همه چیز؛ از زیرساخت‌های انرژی گرفته تا مؤسسات مالی را تحت تاثیر قرار می‌دهند.

۴) چنگ می‌گوید گروه‌هایی پیشاپیش در حال سرقت اطلاعات رمزنگاری شده هستند تا پس از فعال شدن یک کامپیوتر

که انرژی را در کنترل خود بگیرد، می‌تواند هر پنج قاره را کنترل کند و هر کسی که پول را در کنترل خود بگیرد، می‌تواند جهان را کنترل کند. او حتی گفته است که «کاستن از میزان جمعیت این مناطق، باید بالاترین اولویت سیاست خارجی ما در قبال جهان سوم باشد» (۱۲).

موجودات سایبورگ و ریز پرنده‌های زیستی (۱۱)

جانوران سایبورگی، حیواناتی هستند که به وسیله فناوری‌های نوین، توانمندی‌های طبیعی‌شان تقویت می‌شود یا قابلیت‌های جدیدی به آن‌ها افزوده می‌شود. نمونه‌های برجسته جانوران سایبورگی به کارگیری میکروچیپ‌ها در بدن حشرات مانند سوسک‌ها به منظور کنترل حرکت آن‌ها است. این فناوری در پروژه‌های جست‌وجو و نجات کاربرد دارد. ماهی‌های سایبورگی: تجهیز ماهی‌ها به سنسورهای زیست‌محیطی برای پایش وضعیت آلودگی آب.

موش‌های سایبورگی: اتصال الکترودها به مغز موش‌ها برای کنترل رفتار آن‌ها از طریق تحریک مغزی.

فناوری‌های اصلی در توسعه جانوران سایبورگی:

- ۱) نانو فناوری: نانو حسگرها و روبات‌های میکروسکوپی به طور مستقیم در بدن جانوران تعبیه می‌شوند که قابلیت‌هایی همچون تشخیص سموم یا انتقال اطلاعات را فراهم می‌آورند.
- ۲) هوش مصنوعی (AI): استفاده از الگوریتم‌های پیشرفته برای تحلیل داده‌ها و کنترل رفتار جانوران از راه دور.
- ۳) ایمپلنت‌های الکترونیکی: ابزارهایی که به سیستم عصبی یا عضلانی حیوانات متصل می‌شوند و امکان ارسال سیگنال‌های مستقیم را فراهم می‌آورند.

کاربردهای جانوران سایبورگی

- ۱) جست‌وجو و نجات: حشرات سایبورگی قادرند به راحتی به مناطق خطرناک وارد شوند و اطلاعاتی از محل قربانیان فراهم کنند.
- ۲) سوسک‌هایی که مجهز به میکروفون و حسگرهای گاز هستند، می‌توانند در کشف افراد زنده زیر آوار کمک کنند.
- ۳) پایش محیط زیست: ماهی‌ها و حشرات سایبورگی با سنسورهای زیست‌محیطی می‌توانند به دانشمندان در پایش کیفیت آب و هوا کمک کنند.
- ۴) تحقیقات علمی: موش‌های سایبورگی برای مطالعه عملکرد مغز، بیماری‌های عصبی و پیشرفت‌های دارویی به کار گرفته می‌شوند.
- ۵) کاربردهای نظامی: جانوران سایبورگی، همچون پرندگان و حشرات مجهز به دوربین‌ها و سنسورهای پیشرفته، در عملیات‌های جاسوسی و نظارتی مورد استفاده قرار می‌گیرند. نمونه‌های واقعی جانوران سایبورگی سوسک‌های سایبورگی در دانشگاه کارولینای شمالی: با اتصال میکروچیپ‌ها به سیستم عصبی سوسک‌ها، محققان توانسته‌اند حرکت آن‌ها را کنترل کنند. این سوسک‌ها برای جست‌وجو و نجات در

بیماری‌های غیر واگیر در کنار پاندمی‌های واگیر؛
تغییرات آب و هوایی در دنیا و ایران و پیامدهای آن بر سلامت؛

۸) تغییر پارامترها و دینامیک اجتماع مبتنی بر نقش رسانه و مسائل اجتماعی جدید و گسترش بیماری‌های ناشی از آسیب‌های اجتماعی از قبیل بیماری‌های شناختی، اخلاقی و جنسی؛
۹) تحول در نظام آموزش پزشکی مبتنی بر ابر روندهای پیش رو؛ (۹)

مهندسی ژنتیک موجودات و محصولات تراریخته (SGMOs و MGMOs)

تغلب هدفمند در مواد غذایی، دارویی، آرایشی، مکمل‌ها، افزودنی‌ها، طعم دهنده‌ها و غیره

مهندسی حشرات غیر مفید و تهدیدات ناشی از آن (حشرات قاتل، مسلح، زامبی و ...)

حشراتی که توسط قارچ‌ها زامبی می‌شوند: شکم این زنجره (جیرجیرک دشتی) کشتگاه قارچ‌هایی می‌شود که مغزش را از پیش در استیلا دارند. در واقع زنجره برده قارچ‌ها می‌شود.

نمونه دیگر تخم نماتودها است که در حاشیه آب‌های کم‌عمق خوراک حشراتی مثل ملخ و جیرجیرک می‌شود. داخل بدن حشره رشد می‌کند و طولش به چند برابر طول حشره می‌رسد. بعد حرکات حشره را در استیلا خود درمی‌آورد و وادارش می‌کند تا به نزدیکی آب برود و داخل آب خودکشی کند تا نماتود در آب جفت‌گیری بکند.

وقتی مورچه زامبی هم رفتارش در اختیار قارچ‌هایی خاص در می‌آید، وادارش می‌کنند به جای مرتفعی، مثلاً بالای درخت، برود تا کلاهک قارچ کله مورچه را بشکافد و هاگ‌هایش را برای آلوده کردن قربانیان بعدی پراکنده کند (۱۰).

مهندسی حشرات مفید و تغییر ماهیت آن‌ها به حشرات مضر و مخرب (زنبور عسل، گرده افشان‌ها و کنترل گرهای زیستی)؛ (۱۱)

برنامه‌های هدفمند دشمن در زمینه جنگ جمعیت، نابابوری و عقیم سازی جمعیت (مهندسی ویروس، محصولات تراریخته و آنتی‌بادی‌های ضد اسپرم و ...)
هدف جمعیت‌زدایی همچنان به طور کامل دنبال می‌شود؛ و درست مقابل چشمان ما نیز این کار صورت می‌گیرد. در مطالعه‌ای که روس‌ها در سال ۲۰۱۳ انجام دادند معلوم شد پستاندارانی که مواد غذایی دستکاری ژنتیکی مصرف می‌کنند با مشکلات باروری مواجه می‌شوند. عقیم سازی با استفاده از مواد دستکاری ژنتیکی شده تصادفی نیست. مونسانتو از دهه ۱۹۶۰ چنین چیزی را برنامه‌ریزی کرده است. هنری کیسینجر (دست پروده بنیاد راکفلر) گوینده این اظهارنظر در اوایل دهه ۷۰ است: «هر کسی که تأمین مواد غذایی را در کنترل خود بگیرد، مردم را کنترل می‌کند؛ هر کسی

مناطق زلزله‌زده به کار می‌روند (۱۳).

جنگ شناختی

جنگ شناختی به عنوان یک چالش نوین در دنیای امروز، تهدیدات و فرصت‌های جدیدی را برای کشورهای مختلف ایجاد کرده است. این نوع جنگ، با استفاده از ابزارهای روانی، اطلاعاتی و فناوری‌های نوین، به طور عمده بر افکار عمومی، سیاست‌ها و تصمیم‌گیری‌ها تأثیر می‌گذارد. از جمله چالش‌های اصلی جنگ شناختی می‌توان به پیچیدگی تهدیدات، حملات سایبری و تأثیرات روانی این نوع جنگ اشاره کرد. فرصت‌هایی همچون پیشرفت در فناوری اطلاعات و توانمندی‌های سایبری به عنوان ابزارهایی برای مقابله با این تهدیدات شناخته می‌شوند. همچنین تهدیداتی چون اخبار جعلی، بی‌ثباتی اجتماعی و سیاسی و تغییر هویت ملی در اثر جنگ شناختی مطرح شده‌اند. در این راستا، قابلیت‌های ضروری برای مقابله با این تهدیدات شامل تقویت توانمندی‌های سایبری، آموزش نیروی انسانی و پیش‌بینی سناریوهای شناختی هستند (۱۴). در نبردهای نوظهور که روش و راه کنش‌های جنگ تغییر شگرفی نموده است عدم توجه به این تهدیدات و نداشتن یک الگوی مناسب برای جواب‌گویی در صحنه جنگ‌های آینده می‌تواند باعث ایجاد غافلگیری راهبردی و بروز بحران گردد. زیرا ابزارها و تجهیزات فعلی کارایی لازم را در جنگ احتمالی آینده نخواهند داشت. بنابراین علاوه بر ایجاد و تولید الگوی تسلیحات مورد نیاز بهداشتی و درمانی سراسری ملی، باید بتوان تسلیحات بهداشتی و درمانی جدید زمینی، هوایی، دریایی و پدافندی (عامل و غیر عامل) در نیروهای مسلح را تهیه و آماده برای تهدیدات آینده نمود.

اهداف، سیاست‌ها و اولویت‌های بهداشت، امداد و درمان نیروهای مسلح در آمادگی و مقابله با تهدیدات جنگ نوین

- ۱) ایجاد و ارتقای مهارت‌های کارکنان در زمینه امداد و نجات با آموزش‌های مرتبط در سطوح مختلف.
- ۲) ایجاد ظرفیت مدیریت سلامت در بحران و بلایا برای حداکثر بهره‌برداری از کلیه منابع و امکانات و مراکز بهداشتی درمانی کشوری و لشکری به هنگام بحران و جنگ.
- ۳) افزایش قابلیت‌های طب رزم، به ویژه در سطح بیمارستان‌ها با توانمندی در درمان مصدومین جنگ نوین به خصوص تهدیدات زیستی، تقویت سامانه‌های امدادی و درمانی متحرک متناسب با نیاز و تقویت امداد و انتقال.
- ۴) توسعه چشمگیر سامانه‌های سلامت محور هوشمند (سلامت دیجیتال).
- ۵) افزایش رده‌ها و یگان‌های عملیاتی برخوردار از سامانه‌های پزشکی از راه دور (تله مدیسین) به ویژه پاسگاه‌های مرزی، سایت‌ها و ...
- ۶) راه‌اندازی شبکه و مراکز مراقبت و کنترل بیماری‌ها (M.C.D.C) در سطح ن.م.

۷) افزایش تخت‌ها و بخش‌های مرتبط با طب رزم و تهدیدات زیستی به ویژه تخت‌های سوختگی، ICU و تخت‌های عفونی.

۸) افزایش آمادگی دفاعی و تاب‌آوری کارکنان رسته بهداشت و درمان.

۹) تقویت، چابک‌سازی و به روز کردن سامانه‌های امداد و انتقال، متناسب با تهدیدات.

ویژگی‌های کلی بهداشت، امداد و درمان نیروهای مسلح با توجه به ویژگی‌های تهدیدات جنگ نوین

- ۱) منعطف بودن سازمان بهداری رزمی؛
- ۲) برخورداری از قدرت پیش‌بینی نسبت به وضعیت‌های متغیر؛
- ۳) برخورداری از خودمختاری در رده‌های عمل‌کننده؛
- ۴) افزایش قدرت تحرک در ترابری عملیات امداد، بهداشت، درمان و انتقال؛
- ۵) اجرای عملیات امداد، بهداشت، درمان و انتقال سریع و برق‌آسا؛
- ۶) آماده ارائه خدمات درمانی در هر زمان و مکان.

نتیجه‌گیری

با توجه به اینکه تحول علم و فناوری و افق بهداشت، امداد و درمان نیروهای مسلح در چشم انداز ۵ ساله آینده دستیابی به بالاترین توان و آمادگی رزمی در زمینه بهداشت، امداد و درمان و ایستادن در بالاترین رتبه در منطقه غرب آسیا و قرارگرفتن در بین ۵ ارتش برتر جهان می‌باشد، برای دستیابی به این هدف علاوه بر برنامه‌ریزی، آموزش و تمرین‌های دوره‌ای به روز و جامع مراکز درمانی نیروهای مسلح، می‌بایست برنامه‌هایی برای دیده‌بانی، آمادگی و مقابله با تهدیدات جنگ نوین در نظر گرفته تا در پاسخگویی مناسب به نیازمندی‌های مأموریتی در مقابله با تهدیدات جنگ نوین بتواند موجب ارتقاء بهبود انجام فرایند درمان و نجات جان مجروحان و مصدومان را فراهم آورد.

برنامه‌های پیشنهادی برای دیده‌بانی، آمادگی و مقابله با تهدیدات جنگ نوین

- ۱) آینده‌پژوهی در خصوص تدوین راهبردها و یا ارائه الگوی راهبردی دفاع در مقابل هرکدام از حوزه‌های تهدیدات فناوری‌های نوین بهداشت، امداد و درمان (در قالب پروژه‌های تحقیقاتی کاربردی)؛
- ۲) برنامه‌ریزی بلندمدت در تهدیدات فناوری‌های نوین در جنگ‌های آینده برای مقابله با این تهدیدات با همکاری نخبگان کشوری و لشکری؛
- ۳) آموزش، تمرین و برگزاری رزمایش‌های تخصصی با بهره‌گیری از تجربیات داخلی به منظور افزایش توانمندی، آمادگی و مقابله هوشمندانه کشور در برابر انواع تهدیدات؛
- ۴) ضرورت دیده‌بانی سیاست‌ها، راهبردها، برنامه‌های هدفمند،

- امنیت روانی و آرامش بخشی اجتماعی؛
- ۷) ثبت و صیانت از اطلاعات ژنتیکی کشور (ذخایر ژنتیکی، بیوبانک‌ها و ذخیره‌گاه‌های طبیعی)؛
- ۸) بهداشت و پیشگیری و محدودسازی (قرنطینه) - اورژانس و امداد و نجات - درمان؛
- ۹) مستندسازی اقدامات انجام شده در مقابله با تهدیدات شامل آثار مکتوب، فیلم، صوت، عکس و تجهیزات.
- تضاد منافع:** بدین وسیله نویسندگان تصریح می‌نمایند که هیچ‌گونه تضاد منافی در مطالعه حاضر وجود ندارد.

- توان و قابلیت‌های کشورهای متخاصم در حوزه تهدیدات جنگ نوین به‌ویژه پایگاه‌های و آزمایشگاه‌های فرا سرزمینی آمریکا و رژیم صهیونی (با توجه به تعدد و تنوع مراکز و پایگاه‌های تحقیقاتی زیستی، شیمیایی، هسته‌ای و ...).
- ۵) ضرورت دیده‌بانی و ایجاد آمادگی در مقابله با انواع تروریسم (بیو تروریسم، تروریسم کشاورزی، تروریسم شیمیایی، تروریسم پرتوی، تروریسم فیزیکی، تروریسم غذایی، تروریسم دارویی، تروریسم ترکیبی CBRNE)؛
- ۶) ارزیابی خطر تهدیدات و مخاطرات به منظور ایجاد آمادگی و قدرت پاسخ سریع به حوادث حوزه سلامت، تاب‌آوری ملی و

منابع

- Bartczak SE. Identifying barriers to knowledge management in the United States military. Auburn University; 2002.
- UK Ministry of Defence. Strategic Trends Programme: Global Strategic Trends. Out to 2045. Development, Concepts, Doctrine Centre; 2017.
- Riazi V, Biabany E. The pattern of threats of new technologies of the Islamic Republic of Iran Army's ground forces. Military Management Quarterly. 2025;24(96):58-77. [In Persian]
- Yeganeh Mohammadi M, Naderi A. Smartization, Artificial Intelligence, and Cyber in Future Wars. The First National Conference on Command and Management in Future Wars; 2023. [In Persian]
- Farzin Fard M, Karimi Ghahrudi M. Convergence of Military and Medical IoT and Security Challenges. 12th National Command and Control Conference of Iran; 2020. [In Persian]
- Internet of Military Things. Available from: https://en.wikipedia.org/wiki/Internet_of_Military_Things
- How will future wars be? From quantum computers to robotic skeletons. 2023. Available from: <https://faradeed.ir/fa/tiny/news-139570> [In Persian]
- NATO Working Group meeting. National Soldier Modernisation Programme; 2018.
- Shiraz University of Medical Sciences, Policy Research Center. National Conference on Basic Sciences and Health Promotion; 2022. [In Persian]
- Get to know the real-world zombies. 2025. Available from: khabaronline.ir/xnsG4 [In Persian]
- Estimation of threats in the field of biology and health. National Conference on Passive Defense in the Health System; 2024. [In Persian]
- Parliament of Australia. Who controls the food supply controls the people. <https://www.aph.gov.au/DocumentStore.ashx?id=40c4c531-0e4f-4f8d-a590-7179092490ac&subId=741094>
- Cyborg animals: transforming insects into robots. 2024. Available from: <https://www.shotx.ir/robot/28685-cyborg-animals-transform-insects-with-robots> [In Persian]
- Mohammadi A, Ebrahimi H, Esfandiar V. Examining the Challenges, Opportunities, Threats, and Key Capabilities in Cognitive Warfare: An Approach to Future Command and Management. The Second National Conference on Command and Management in Future Wars with a Cognitive Approach; 2024. Available from: <https://civilica.com/doc/2172879>