



ابر چالش‌های دفاعی - نظامی جنگ‌های آینده و تأثیر آن بر محیط امنیتی جمهوری اسلامی ایران در هزارهٔ جدید

محسن جمشیدی^۱، شهرام فتاحی^۲، زهره رجبی^۳

تاریخ پذیرش: ۱۴۰۱/۱۰/۱۸

تاریخ دریافت: ۱۴۰۱/۰۲/۲۷

چکیده

توجه به زیرساخت‌های دفاعی و توان رزم، یکی از الزامات مهم برای برنامه‌ریزی بلندمدت در حوزهٔ ابرچالش‌های دفاعی- امنیتی است. این چالش‌ها و شرایط محیطی جنگ‌های آینده در نظام بین‌الملل متأثر از چه پارامترهایی خواهند بود؟ به نظر می‌رسد شرایط و ویژگی محیطی جنگ‌های آینده با توجه به رشد فناوری‌های نوظهور و تأثیر انکارناپذیر آن بر چالش‌های دفاعی- امنیتی، فضای جنگ‌ها بیشتر به سمت جنگ‌های ترکیبی، هوشمند و سیال خواهند رفت. رشد خیره‌کننده فناوری و ارتباطات که ما آن را انقلاب اطلاعات می‌نامیم موج پرقدرتی است که ماهیت و ویژگی جنگ و منازعه را بطور کلی تغییر خواهد داد. عواملی نیز مانند تغییر در ترکیب بازیگران، محیط جنگ و توجه به سامانه‌های هوشمند بر شرایط جنگ‌ها و به تبع آن ساختارهای دفاعی تأثیر گذارند. این پژوهش از نوع آینده‌پژوهی با روش کیفی- تفسیری و رویکرد توصیفی- تحلیلی همچنین از طریق داده‌های موجود (اسنادی/کتابخانه‌ای)، چالش‌های دفاعی و جنگ‌های محتمل در دو دههٔ آینده در محیط بین‌الملل و تأثیر آن‌ها را بر محیط دفاعی- امنیتی جمهوری اسلامی ایران را مورد بررسی، تحلیل و واکاوی قرار داده است.

کلیدواژه: جنگ‌های آینده، فناوری‌های نوظهور، شبکه هوشمند، جنگ‌های ترکیبی.

Email: mohsenmd16@yahoo.com.

۱. دکتری علوم سیاسی، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران (نویسنده مسئول)

۲. استادیار گروه علوم سیاسی، واحد کرمانشاه، دانشگاه آزاد اسلامی، کرمانشاه، ایران.

۳. کارشناسی علوم سیاسی، واحد ایلام، دانشگاه آزاد اسلامی، ایلام، ایران.

مقدمه

تحولات فناورانه نسبت به دهه‌های گذشته پیشرفت چشمگیری داشته و روندهای جهانی به‌عنوان پیشران سرعت توسعه دانش را فراهم آورده است. همانند قرن‌های گذشته فناوری‌های متعددی برای بازار غیرنظامی توسعه یافته‌اند که دارای کاربردهای مشخصی اعم از هوش مصنوعی، سامانه‌های خودمختار، زیست فناوری و محاسبات کوانتومی در زمینه نظامی نیز هستند. فناوری‌ها همچنان در حوزه‌های دفاعی نقش اساسی و مهمی را ایفا می‌کنند و پیشرفت و ظهور فناوری‌های نو می‌تواند به تغییر و هدایت نبردهای آینده کمک نماید. مقابله با تهدیدات جنگ‌های آتی نیازمند شناخت فضای نبرد آینده و استفاده از تمام ظرفیت‌ها و مؤلفه‌های قدرت ملی است. برخی از سازمان‌ها انبوهی از تجهیزات الکترونیکی را صرف‌نظر از کاربردهای نظامی و غیرنظامی آن در مقیاس‌های کوچک و بزرگ استفاده می‌کنند.

این قطعات الکترونیک به اشکال مختلف و در مقیاس‌های مختلف در قالب کامپیوترهای بزرگ و کوچک، ثابت و سیار و یا قطعات کوچک داخل مدارهای پیچیده در ادوات جنگی، جنگنده‌ها، پهبادها، انواع ناوها و ناوچه‌ها، سامانه‌های پدافندی و حتی ماهواره‌ها در کشور استفاده می‌کنند. به علت محدودیت‌های مالی و فناورانه، عموم این تجهیزات از کشورهایی تأمین می‌گردند که خود مخرب‌ترین حملات سایبری را انجام داده‌اند (رمضان زاده و دیگران، ۱۴۰۰: ۶۰).

در عصر فرا صنعتی شاهد وقوع جنگ‌هایی هستیم که به‌مراتب از جنگ‌های گذشته، خطرناک‌تر و مهلک‌تر است. علت آن به دو ویژگی خاصی برمی‌گردد که با امتزاج خود، صحنه جدیدی را در عصر کنونی رقم‌زده است. اولی پیشرفت شگفت‌آور فناوری و دیگری انفجار اطلاعات است که به‌شدت، دقت، وسعت، زمان، میزان تخریب، محیط درگیری در جنگ‌ها تأثیرگذار بوده است. جنگ آینده جنگ بایت‌ها و بیت‌ها خواهد بود. جنگ‌های آینده بر آفندها و پدافندهای دیجیتال استوار بوده و محدود به مرزهای جغرافیایی نبوده و لزوماً به برتری منابع ملی و قومی وابسته نخواهد بود. این تغییر ممکن است تحولاتی پدید آورد که موجب شود گروه‌ها و ملت‌هایی که پیش‌ازاین تهدیدی برای قدرت‌های جهانی به‌حساب نمی‌آمدند تبدیل به تهدیداتی بزرگ‌تر از تسلیحات سنتی از جمله تسلیحات کشتار جمعی شوند.

۱. مبانی نظری

طرح معمای امنیتی (دفاع - تهاجم)

رنالیسم تهاجمی از تبیین سیاست خارجی به فهم سیاست بین‌الملل می‌رسد و رسیدن به امنیت مطلق را مهم‌ترین خواسته قدرت‌های بزرگ می‌داند که تنها از طریق قدرت و دستیابی به هژمون قابل تحصیل است. اما رنالیست‌های تدافعی معتقد هستند که هزینه توسعه‌طلبی عموماً گزاف می‌باشد و نظام بین‌الملل معمولاً اعتدال (میان‌روی) را تشویق می‌نماید (walt,2001: 67).

از نگاه مرشایمر هر قدرت بزرگی که بخواهد فرایند کسب قدرت مطلق را طی نماید و به مرحله هژمون جهانی یعنی امنیت مطلق برسد، باید به همراه انگیزه‌ها و گرایش‌های تجدیدنظر طلبانه در استراتژی‌های کلان جهانی، توزیع قدرت جهانی را به نفع خود متحول کند.

اصطلاح معمای امنیتی اولین بار توسط «جان هرتز» در مقاله‌ای با عنوان: «بین‌الملل‌گرایان آرمان‌گرا و معمای امنیتی» مطرح گردید. او در آن مقاله معمای امنیتی را این‌چنین تعریف می‌نماید: گروه‌ها یا افراد تحریک می‌شوند که به‌منظور در امان ماندن از تأثیر قدرت دیگران، میزان بیشتر و بیشتری از قدرت را کسب نمایند.

این موضوع به‌نوبه خود، دیگران را ناامن‌تر می‌سازد و آنان را وادار می‌سازد تا برای بدترین‌ها محیا شوند. طرح معمای امنیتی در روابط بین‌الملل بیش از جنبه‌های عینی به رویکردهای ذهنی می‌پردازد. یعنی ادراک و برداشت تصمیم‌گیرندگان یک کشور از اقدام یا مواضع دفاعی کشور دیگر تلقی می‌شود. طرح معمای امنیتی حالت عمل و عکس‌العمل خطی نیست، بلکه یک مجموعه‌ای از شرایط بایستی تحلیل شوند (جمشیدی و سعیدی نژاد، ۱۳۹۹: ۲۱۷).

شرایط محیطی جمهوری اسلامی ایران در منطقه تحت نفوذ و محیط دفاعی - امنیتی خود تنها درصدد حصول، حفظ و پیشبرد منافع خود نیست، بلکه با تأسیس یک رژیم ضمنی غیررسمی امنیت منطقه‌ای که از آن تحت عنوان «محور مقاومت» یاد می‌شود، به دنبال حصول، حفظ و پیشبرد منافع خود و متحدان منطقه‌ای خود می‌باشد (جمشیدی و سعیدی نژاد، ۱۴۰۰: ۲۰۸).

علت اصلی شکل‌گیری رژیم ضمنی غیررسمی امنیت منطقه‌ای جمهوری اسلامی در هزاره جدید، که از آن تحت عنوان محور مقاومت یاد می‌گردد، معمای امنیتی (دفاع-تهاجم) ناشی از حضور قدرت‌های منطقه‌ای و بین‌المللی رقیب در محیط دفاعی - امنیتی و محور نفوذ خود می‌باشد.

جمهوری اسلامی ایران باهدف مقابله با پیامدهای حضور قدرتهای رقیب در منطقه و این معمای امنیتی، مبادرت به تشکیل رژیم ضمنی غیررسمی امنیت منطقه‌ای متشکل از بازیگران دولتی و غیردولتی جمهوری اسلامی ایران، جمهوری عربی سوریه، حزب ا... لبنان، گروه‌های چندگانه تشکیل‌دهنده حشد الشعبی عراق، حوثی‌های یمن، جنبش صابرین، جنبش جهاد اسلامی و حماس در فلسطین نموده است. البته لازم به ذکر است که برخی از این بازیگران به‌مرور زمان عضو رژیم گردیدند و از ابتدا در آن حضور نداشتند. برای روشن‌شدن این مسئله بایستی توجه داشت که، ممکن است دولت A به‌منظور افزایش امنیت خود نسبت به خرید جنگنده، تانک، موشک و ... اقدام نماید.

در اینجا یک سؤال مهم بر ذهن متبادر می‌گردد: «هدف دولت A از بزرگ نمودن ارتش و سازوبرگ نظامی خود چیست؟ آیا می‌خواهد قدرت بیشتری را کسب نماید یا می‌خواهد امنیت خود را تضمین نماید؟» این سؤال یک دوراهی را در ذهن ایجاد می‌نماید، که به آن «معمای امنیتی» گفته می‌شود (ادمی و رضایی، ۱۳۹۵: ۷۶).

۲. مروری بر صنایع دفاعی - نظامی کشورها در محیط بین‌الملل

۲.۱. هزینه‌های نظامی

تغییرات سریع محیطی به‌ویژه در حوزه فناوری منجر گردیده تا شاهد انقلاب بزرگی در تغییر نحوه جنگیدن از کلاسیک به سایر شیوه‌ها باشیم. تا جایی که تغییرات اساسی را در اصول رهنامه ارتش آمریکا نیز به‌عنوان قدرتمندترین ارتش دنیا، مشاهده می‌کنیم.

انستیتوی بین‌المللی پژوهش‌های استراتژیک (IISS) در سال ۲۰۲۰ پژوهشی درباره رتبه‌بندی هزینه‌های نظامی ارائه داده است، که فهرست کشورها بر اساس هزینه‌های اختصاص داده‌شده به حوزه نظامی که بر پایه میلیارد دلار است به شرح زیر می‌باشد

در جدول زیر لیست پانزده کشور برتر بر اساس هزینه‌های اختصاص داده‌شده به حوزه نظامی آمده است که توسط موسسه بین‌المللی صلح استکهلم در سال ۲۰۱۸ منتشر شده است

جدول شماره ۱

رتبه	کشور	هزینه نظامی (میلیارد دلار)	درصد نسبت به کل هزینه‌های نظامی در جهان
-	مجموع (جهان)	۱,۷۳۹
۱	ایالات متحده آمریکا	۷۹۶	۴۰
۲	چین	۱۶۶	۱۳
۳	عربستان سعودی	۶۹/۴	۴
۴	روسیه	۶۶/۳	۳/۸
۵	هند	۶۳/۹	۳/۷
۶	فرانسه	۵۷/۸	۳/۳
۷	بریتانیا	۴۷/۲	۲/۷
۸	ژاپن	۴۵/۴	۲/۶
۹	آلمان	۴۴/۳	۲/۵
۱۰	کره جنوبی	۳۹/۲	۲/۳
۱۱	برزیل	۲۹/۳	۱/۷
۱۲	ایتالیا	۲۹/۲	۱/۷
۱۳	استرالیا	۲۷/۵	۱/۶
۱۴	کانادا	۲۰/۶	...
۱۵	ترکیه	۱۸/۲	۱/۰

با نگاهی گذرا به جدول بالا در می‌یابیم که برخی از کشورها همانند آمریکا به تنهایی اندازه چندین قدرت بین‌المللی دیگر برای صنایع نظامی خود سالانه هزینه می‌کنند. همچنین اگر از نگاهی دیگر موضوع را مورد بررسی قرار دهیم به این نکته می‌رسیم که هزینه‌کردن صرفاً به معنای قدرتمند بودن در محیط بین‌المللی نیست، همان‌گونه که در جدول بالا مشاهده می‌کنیم برخی کشورها به صرف هزینه اختصاص یافته سالانه خود به صنایع نظامی اما در محیط بین‌الملل حرفی برای گفتن ندارند.

۲.۲. کمپانی‌های دفاعی - نظامی

با نگاهی به مهم‌ترین کمپانی‌های صنعتی - دفاعی کشورهای جهان در می‌یابیم که شرکت‌های صنایع دفاعی در راستای پیشرفت و توسعه صنعت دفاعی - نظامی هر کشور تأثیر انکارناپذیری دارند.

جدول شماره ۲: کمپانی‌های برتر صنایع دفاعی - نظامی ایالات متحده

ردیف	کمپانی	کشور سازنده	ارزش قرارداد کمپانی با وزارت دفاع	قراردادهای اعطاشده	تعداد کارمندان
۱	لاکهید مارتین	امریکا	۲۹/۴ میلیارد دلار	۶۶/۳۵۳	۱۲۶۰۰۰
۲	بوئینگ	امریکا	۱۴/۶ میلیارد دلار	۱۲/۶۴۵	۱۴۸/۷۵۰
۳	ریتیون	امریکا	۱۲/۳ میلیارد دلار	۱۰/۰۰۰	۶۱۰۰۰
۴	جنرال داینامیکس	امریکا	۱۱/۸ میلیارد دلار	۲۰/۸۲۲	۹۹/۵۰۰
۵	نورثروب گرومن	امریکا	۹/۵ میلیارد دلار	۱۰/۳۹۷	۶۵۰۰۰

۳. جنگ و جنگ‌های آینده

در قرن بیستم بیش از ۲۲۰ جنگ به وقوع پیوسته که بیش از ۲۰۰ میلیون نفر تلفات انسانی داشته است (گودرزی و اجالی، ۱۴۰۰: ۳۵). جنگ‌ها بر اساس هدف، به جنگ عادلانه و غیرعادلانه؛ بر مبنای مقیاس‌های جغرافیایی، به جنگ‌های محلی، منطقه‌ای، فرا منطقه‌ای و جهانی (عمومی)؛ با توجه به انضباط و تاکتیک، به جنگ‌های منظم، کلاسیک و نامنظم (چریکی)؛ بر اساس سطح جغرافیایی، به جنگ‌های دریایی، هوایی و زمینی؛ بر اساس قلمرو، به جنگ‌های داخلی و خارجی تقسیم می‌شوند. با توجه به تعاریف فوق‌الذکر می‌توان گفت که جنگ عبارت است از برخورد مسلحانه بین دو یا چند کشور. از منظر نگاه به آینده می‌توان جنگ را برخورد خشونت‌آمیز و مسلحانه دو یا چند گروه یا کشور برای تصاحب منافع بیشتر در آینده دانست. «کلازویتس» اصل اساسی جنگ را حفظ نیروهای خودی و نابودی نیروهای دشمن، هدف جنگ را خلع سلاح یا سرنگون ساختن دشمن و عام‌ترین اصل پیروزی در جنگ را برتری تعداد افراد نیروهای مسلح دانسته‌است (طاهری هشی و دیگران، ۱۳۹۷: ۱۳۸).

به نظر «بلیک استیلول»^۱ در سال‌های آینده جهان درگیر ۱۰ جنگ متفاوت خواهد بود:

۱. درگیری کره شمالی با سایر کشورها؛ تفاوتی نمی‌کند که کره شمالی با کدام کشور درگیر شود، زیرا شروع جنگ برای این کشور نوعی پیشرفت و برتری محسوب می‌شود.
۲. مشکلات هند و چین؛ امروزه تنش‌های بین هند و چین دوباره شدت گرفته، اما اگر جنگی بین این دو تا کشور درگیر طبق پیش‌بینی‌ها این درگیری بر سر آب خواهد بود.

۳. جنگ داخلی در افغانستان؛ درگیری‌های داخلی در کشور افغانستان بر سر قدرت و همچنین مشکلات این کشور با پاکستان و تنش‌های قومی و قبیله‌ای همچنین معادلات لاینحل در نظام بین‌الملل هستند.
۴. درگیری‌های داخلی در ترکیه؛ بحران هویتی مهم‌ترین چالش و مشکل برای مردم ترکیه است. اردوغان در طی چند سال اخیر در این کشور اقتصاد این کشور را مدرن‌تر کرده، ولی از طرف دیگر دموکراسی این کشور ضعیف‌تر شده است.
۵. درگیری میان رژیم صهیونیستی و نیروهای حزب‌الله؛ سال‌هاست که مشکلات این دو باهمدیگر لاینحل باقی مانده است.
۶. جنگ عراق و سوریه با کردهای این دو کشور؛ در آینده احتمال این می‌رود که کردهای این دو کشور همراه کردهای جنوب ترکیه متحد شده و درگیری‌های تازه‌ای به راه بی‌اندازند. البته احتمال این درگیری وقتی بالا می‌رود که فرماندهی کردها به دست پ.ک.ک افتاده باشد.
۷. تنش‌های داخلی در عراق؛ کشور عراق با توجه چندقومیتی بودن و عدم هم‌پیوستگی در آینده مستعد ناامنی و آشوب خواهد بود.
۸. جنگ روسیه علیه ناتو؛ روسیه با به راه انداختن جنگ در اوکراین نشان داد که پیش روی‌های اخیر ناتو در حوزه نفوذ خودش را اصلاً تحمل نمی‌کند و درصدد تلافی بر خواهد آمد.
۹. درگیری ایالات متحده آمریکا و چین علیه همدیگر؛ بررسی‌های انجام‌شده روی پیشرفت‌های نظامی چین این واقعیت را آشکار می‌سازد که این کشور کارایی بالایی برای نابود کردن تسلیحات نظامی آمریکا دارد.
۱۰. درگیری چین با کشورهای حوزه اقیانوس آرام؛ طبق پیش‌بینی‌ها کشور چین بیشترین سهم را در درگیری‌های آینده خواهد داشت. این کشور در سال ۲۰۱۳ اعلام کرد که جزایر سنکاکو به‌عنوان بخشی از پایگاه‌های هوایی چین در دریای چین شرقی می‌باشد. به خاطر همین موضوع کنکاش و درگیری لفظی زیادی بین چین و ژاپن اتفاق افتاد (www.Bestfarsi.ir).

جدول شماره ۴: برخی از مشخصه‌های جنگ‌های آینده به شرح زیر قابل دسته‌بندی می‌باشند.^۱

رویکرد شبکه‌محوری به جنگ	تهاجم هوایی و موشکی دقیق	درگیری هم‌زمان در سطوح سه‌گانه	عملیات سریع و قاطع
به‌کارگیری تاکتیک ناهم‌تراز، ناهمگون	مدیریت زمان	انجام عملیات پیش‌دستانه	راه‌اندازی ائتلاف و انجام عملیات مرکب
مدنظر قراردادن ابعاد و جنبه‌های مختلف جنگ نرم	تلاش در راستای کاهش هزینه‌های جنگ	استمرار عملیات، به‌صورت ناپیوسته و نامتناسب	انجام عملیات تأثیرمحور یا مبتنی بر تأثیر
استفاده از توانمندی‌های پهپاد	تأکید بر عملیات سایبری و مجازی‌سازی جنگ	توسعه صحنه نبرد و نفوذ بر عمق هدف	سینرژی یا هم‌افزایی قدرت
انتخاب راهبرد آمادی بر مبنای پیش‌بینی متمرکز	مدیریت آستانه تحمل ملت‌ها	تکیه بر عملیات روانی	انجام عملیات غیرخطی
پیوند هنر، علم و فناوری	تغییر در نوع مانور	حمله به مراکز نقل	به‌کارگیری نیروهای ویژه
	تکیه بر جنگ الکترونیک	آفند مسطح و تاکتیک عملیات موزاییکی	ارزیابی همه‌جانبه اطلاعاتی

۳.۱. جنگ‌های آینده و فناوری‌های نوظهور

در عصر پیش روی نقش و تأثیر فناوری در جنگ نرم و جنگ اطلاعات به مراتب بیشتر از جنگ سخت است. تشخیص و برآورد روندهای فناورانه و گستردگی آن همواره چالش‌برانگیز است. زیرا عدم قطعیت‌ها و تحول در مسیر علوم بنیادی می‌تواند تشخیص روندها را دشوار کند و ممکن است ارتباط بین فناوری و پیامدهای بالقوه آن غیرمستقیم و پیچیده باشد. در چشم‌انداز هزاره جدید روندهای مختلفی در حال شکل‌گیری است. بدیهی است که فناوری‌های جدید به‌طور یکنواخت ظهور نخواهند کرد و احتمال زیاد برخی از آن فناوری‌هایی که به‌عنوان پیش‌ران‌های رایج و پویا هستند ظهور کنند. افزایش همگرایی فناوری‌های به‌ظاهر غیر مرتبط و رشد رقابت جهانی موجب تسریع در ظهور فناوری‌های پیشرفته می‌شوند (GlobalTrends2040, 2021:55).

۳.۱.۱. جنگ سایبری (مجازی)

جنگ سایبری به‌نوعی از جنگ گفته می‌شود که طرفین جنگ در آن نبرد از رایانه و شبکه‌های رایانه‌ای (به‌خصوص شبکه اینترنت) به‌عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند. حمله‌های سایبری بین کشورها نخستین بار در سال ۲۰۰۸ با حمله رژیم صهیونیستی و

۱: برای مطالعه بیشتر رجوع شود به: (طاهری هشی، ۱۳۹۷).

امریکا به تأسیسات هسته‌ای ایران شروع شده و تنش‌های سایبری بعدی در ادامه و نیز تاکنون نیز همچنان پابرجا بوده است. در حملات سایبری کشورها همدیگر را مورد حمله قرار می‌دهند، بدون اینکه به مرزهای هم حمله کنند و نتایج دلخواه خود را نیز می‌گیرند. ضمن اینکه هزینه کمتری نیز دارد چون فقط به تعدادی برنامه‌نویس نیاز است. شرکت آمریکایی trend micro اعلام کرد در سه‌ماهه دوم سال ۲۰۱۵ میلادی کشورهای هند (۱۱ درصد)، مصر (۱۶ درصد) و ایران (۱۱ درصد) هدف بیشترین حملات سایبری قرار گرفته‌اند. کشورهای روسیه، چین و امریکا بیشترین تخصص را در حملات سایبری دارند. امریکا ۶۳۰۰ نیرو (سرباز) برای حملات سایبری دارد (fa.m.wikipedia.org).

۳. ۱. ۲. هوش مصنوعی

ربات‌های نظامی و تجاری دردنیای پیش روی در حوزه‌ای تحت عنوان هوش مصنوعی (AI) قرار می‌گیرند، و به این ترتیب آن‌ها را قادر می‌سازند که مسئولیت‌ها و مأموریت‌هایی را به عهده بگیرند. اگرچه کامپیوترها و هوش مصنوعی می‌توانند در بعضی از مهارت‌ها و وظایف قانون بنیاد، برتر از بشر باشند، اما وقتی به قضاوت و دانش احتیاج باشد و میزان عدم اطمینان زیاد گردد، انسان‌ها از کامپیوترها برترند. «هنری کیسینجر» نظریه‌پرداز کهنه‌کار امریکا در مورد پیامدهای کاربرد هوش مصنوعی در عرصه نظامی معتقد است؛ ممکن است دیپلماسی در آینده دیگر نتواند برای متوقف کردن نظامی‌گری مبتنی بر هوش مصنوعی کارایی داشته باشد. ماهیت مخفی و به سرعت متحول شونده هوش مصنوعی بدان معناست که بازیگران دولتی نمی‌توانند آن را به عنوان یک تهدید قطعی مانند تسلیحات هسته‌ای بر روی میز گذاشته و در موردش مذاکره کنند. ایشان پیش‌بینی نموده که الگوریتم‌های هوش مصنوعی روزی به عنوان بخشی از فرایند تصمیم‌گیری نظامی به کار گرفته می‌شوند. اما برنامه ریزان راهبردی باید این موضوع را در بازی‌های جنگی و حتی در موقعیت‌های واقعی از قبل آزمایش کنند تا میزان کارایی آن مشخص شود و ما دریابیم که آیا ما از پس استفاده از چنین الگوریتم‌هایی برمی‌آییم و پیامدهای آن چیست (مراد پیری و خضرابی، ۱۳۹۹: ۱۷۳).

۳. ۱. ۳. نسل چهارم جنگ‌ها

در این نسل تسلط بر روی اراده جامعه هدف مدنظر است و تهاجم به عمق خاک حریف، صرفاً برای نابودی اراده سیاسی است. جنگ‌های رودررو و سنتی با ورود به عصر فناوری وارد نسل دوم

شد. فناوری پیشران اصلی نسل دوم جنگ بود، ایده‌های تاکتیکی عامل بنیادین ظهور نسل سوم و چهارم محسوب گردید و نسل چهارم نیز با محوریت فناوری به منصف ظهور رسید. با پدیدارشدن هر نسل جدید از جنگ، فضای رزم به سمت بی‌نظمی بیشتر پیش‌رفته و بدین ترتیب فرهنگ نظامی که مبتنی بر انضباط شدید تعریف می‌شود، روزه‌روز با ماهیت جنگ مدرن ناسازگارتر می‌شود؛ تاجایی که تضاد و ناسازگاری به معضلی مهم برای بسیاری از ارتش‌های جهان تبدیل شده است. جنگ‌جویان نسل چهارم به‌منظور تحت تأثیر قراردادن شبکه متنوع موردبحث باید شیوه‌های مختلفی را برای ارسال پیام‌های مختلف به کاربندند (رشید و دیگران، ۱۴۰۰: ۱۶۸).

۳. ۱. ۴. جنگ‌های هیبریدی (ترکیبی)

«سان تزو»^۱ در کتاب «هنر جنگ» یا هنر رزم آورده است که جنگ‌های هیبریدی یعنی حمله به راهبردهای دشمن. ابهام، پیچیدگی و چندبعدی بودن؛ این‌ها مهم‌ترین ویژگی‌های مدرن‌ترین شیوه جنگی است. جنگی که در دنیا به آن جنگ هیبریدی و در ایران به آن جنگ ترکیبی می‌گویند. شش ویژگی نبرد ترکیبی (هیبریدی) بر اساس یافته‌های پژوهشگران به شرح زیر تعریف شده‌اند:

۱. ترکیب، قابلیت‌ها و تأثیرات یک نیروی هیبریدی، در محیط پیرامون آن، بی‌همتا هستند؛

۲. هر نیروی هیبریدی یک ایدئولوژی منحصربه‌فرد دارد که منجر به ایجاد نوعی روایت

درونی برای سازمان می‌شود؛

۳. یک نیروی هیبریدی همواره متوجه تهدیدی نسبت به بقای خودش است؛

۴. در جنگ هیبریدی نوعی برتری قابلیت میان طرفین جنگ وجود دارد؛

۵. یک نیروی هیبریدی هم اجزاء متداول و هم اجزاء غیرمتداول را شامل می‌شود؛

۶. نیروهای هیبریدی به دنبال استفاده از عملیات دفاعی هستند (رشید و دیگران، ۱۴۰۰: ۱۷۱).

همچنین از دیدگاه دفاعی - نظامی تأثیر فناوری‌های نوظهور در شکل‌های مختلف و به دلایل گوناگون موردتوجه است. درجایی که تهدید بالقوه عامل شکل‌گیری مفاهیم فنی باشد، یا چگونگی تأثیرگذاری این تهدیدات روی فناوری موجود از نظر تجاری مدنظر باشد، پیش‌بینی دقیق لازم است. بهترین کار شناسایی آن دسته از فناوری‌هایی است که قادر به تزریق حجم وسیعی از پیشرفت‌ها به قابلیت نظامی - دفاعی است. در دنیای تجارت از این فناوری‌ها به‌عنوان فناوری‌های

شالوده شکن یاد می‌شوند. بر اساس گزارش وزارت دفاع استرالیا (۲۰۱۳) هفت حوزه اصلی فناوریانه مؤثر بر دفاع در آینده وجود دارد که عبارت‌اند از:

۱. علوم زیستی؛
 ۲. مواد و ساخت؛
 ۳. محاسبات و هوش مصنوعی؛
 ۴. ارتباطات و حساسیت؛
 ۵. انرژی؛
 ۶. وسایل نقلیه؛
 ۷. فضا.
- همچنین در گزارش مرکز تحقیقات کنگره آمریکا (۲۰۲۰) روند فناوری‌های نوظهور نظامی و دفاعی در کشورهای آمریکا، چین و روسیه را در زمینه زیر معرفی نموده است:

- هوش مصنوعی؛
- تسلیحات کشنده خودکار؛
- تسلیحات فراصوت (هایپرسونیک)؛
- تسلیحات انرژی هدایت‌شده؛
- زیست فن‌آوری؛
- فناوری کوانتوم (گودرزی و جلالی، ۱۴۰۰: ۵۱).

۴. روند فناوری‌های نوظهور دفاعی - نظامی در آینده

روندهای فناوری‌های نوظهور در زمینه دفاعی - نظامی در آینده در محیط بین‌الملل نسبت به گذشته تغییرات زیادی داشته و متفاوت خواهد بود. در ادامه برخی از روندهای فناوری‌های نوظهور را بیان نموده و به صورت مختصر به توضیح خصوصیات و ویژگی‌های آن‌ها می‌پردازیم.

۴.۱. توسعه سامانه‌های هوشمند (هوشمند سازی)

این سامانه‌ها دارای شبکه‌های حسگر کوچک و ربات‌های شخصی شده جهت همانندسازی رفتار و ظاهر انسان تا کثرت همکاری شبکه‌های هوشمند یا مجموعه‌هایی از سکوه‌های محیطی با قدرت

اقدام بدون فرمان انسان خواهند بود. همچنین درزمینه هوشمندسازی، شبکه‌های حسگر هوشمند مفهوم نوینی است که موجب آگاهی کامل سرباز از شرایط میدان نبرد می‌شود. این شبکه بر پایه مجموعه اطلاعات به‌دست‌آمده از تصاویر هم‌زمان، اطلاعات آب‌وهوایی و هدف‌های متحرک استوار است. آمریکا در سال ۲۰۲۰ میلادی حدود ۹۳۰ میلیون دلار درزمینه هوش مصنوعی هزینه نموده است. سایر کشورها نظیر چین و روسیه نیز درزمینه هوش مصنوعی با آمریکا در حال رقابت هستند. روند هوشمندسازی تا چند سال آینده درزمینه زیر اثرگذار خواهد بود:

- استقرار سامانه‌های فیزیکی سایبری به این معنی که حس، کنترل، محاسبه و شبکه را با اشیاء فیزیکی ادغام می‌کند.
- سرمایه‌گذاری بیشتر در هوشمندسازی در حوزه‌های تجاری و استفاده از تکنیک‌های هوش مصنوعی.
- تصمیم‌گیری و کنترل بهینه در سازمان‌ها و نهادهای نظامی و غیرنظامی.
- تجزیه و تحلیل کلان داده‌ها و بینایی رایانه‌ای (گودزی و اجلالی، ۱۴۰۰: ۵۰).

۲.۴. رشد فناوری‌های سایبری

با افزایش روند جهانی فناوری اطلاعات و ارتباطات موضوع فضای سایبری اهمیت یافت. امروزه جهان به کامپیوترها، اطلاعات شخصی و کسب‌وکارهای دیجیتال وابسته است. این امر افراد، سازمان‌ها و کل کشورها را در معرض تهدیدات مهمی و در معرض خطر قرار داده است، که به معنای آن است که شکل جدید از تروریسم سایبری، جرائم اینترنتی، و تقلب‌های اینترنتی در حال ظهور هستند که باید مدیریت شوند. چین یکی از تولیدکنندگان مهم سخت‌افزار و نرم‌افزار رایانه است که آمریکا وابستگی زیادی به قطعات تولیدی این کشور دارد. این امر این احتمال را افزایش می‌دهد که ملل آسیایی این فرایند تولید را به‌عنوان مسیری جهت شروع حملات مجازی درآینده علیه آمریکا به‌کارگیرند. هکرها و یا تروریست‌هایی که در روسیه فعالیت می‌کنند به‌صورت موفقیت‌آمیزی به سامانه‌های آمریکا نفوذ یافته‌اند که نشانگر نقشه‌های حساب‌شده‌ای شبیه به موارد چین است (گودزی و جلالی، ۱۴۰۰: ۵۳).

۳.۴. رواج سامانه‌های بدون سرنشین و خودکارسازی

انگیزه ساخت سامانه‌های بدون سرنشین و رواج آن، به جنگ جهانی دوم برمی‌گردد چون طرف‌های درگیر جنگ از ناحیه هوا ضربات سنگینی متحمل شدند. با توجه به پیش‌بینی بخش‌های صنعتی، تا سال ۲۰۳۵ خودروهای بدون راننده حدود یک پنجم کل فروش خودرو در جهان را از آن خود خواهند کرد و نیمی از فروش خودرو در ایالات‌متحده و چین را نیز مختص به خود خواهند کرد. سامانه‌های خودکار عموماً در چهار دسته درحال توسعه هستند که البته می‌توان کاربردهای تجاری نیز برای آن‌ها متصور شد این چهار دسته عبارت‌اند از:

➤ سامانه‌های خودکار مانند پیشران‌ها و حسگرها، وسایل نقلیه ما فراصوت، وسایل نقلیه هوایی، میکروماهواره‌های کوچک، سامانه‌های پیرانش هوایی هیبریدی- الکتریکی و مدل‌سازی محیط سه‌بعدی؛

➤ گروه‌بندی ماشین- انسان با افزایش عملکرد انسانی؛

➤ تسلیحات اقدام متقابل با قدرت رادیویی بالا؛

➤ رفتار خودکار و یادگیری ماشین.

علاوه بر کارکرد خودرویی رواج سلاح‌های کشنده بدون دخالت انسانی و صرفاً تحت نظارت یک عامل انسانی تا ده سال آینده رواج خواهد یافت و بسیاری از عملیات‌ها در حوزه رزم زمینی به‌وسیله تسلیحات خودکار انجام خواهد گرفت (گودرزی و جلالی، ۱۴۰۰: ۵۴).

۴.۴. رشد روزافزون فناوری‌های فضایی

بیشترین رشد در مسیر کاربردهای غیرنظامی، دفاعی و امنیتی شامل این موارد خواهند بود: ارتباطات راه دور: در این کاربرد، فناوری اطلاعات و ارتباطات بر پایه ماهواره‌های کم ارتفاع و ارزان‌قیمت استوار خواهد بود و ارتباطات اینترنتی، مخابراتی و رادیو و تلویزیونی بر پایه این ماهواره با یکدیگر یکپارچه‌شده، در سطح جهان گسترده می‌شوند و تمامی جهان را زیرپوشش خود خواهند داشت. این رویکرد به طرح مسائل تازه‌ای در زمینه مالکیت و بهره‌برداری از فضا منجر خواهد شد.

مکان‌یابی و ناوبری: استفاده از فناوری «سامانه موقعیت‌یاب جهانی» بر بسیاری از جنبه‌های زندگی تأثیر می‌گذارد. اما مهم‌ترین کاربردهای نظامی آن در هدایت تسلیحات و بالابردن دقت سلاح‌ها است.

مشاهده زمین: دارای کاربردهایی دو منظوره است و مواردی مانند پایش محیط، پایش دگرگونی‌های محیطی و تغییرات آب‌وهوایی و رویدادهای طبیعی و حتی جنبش انسانی و حیوانی را دربر می‌گیرد.

در حال حاضر آمریکا در حوزه فناوری‌های فضایی بسیار پیشرفته است و سفینه‌های فضایی چندبار مصرف تولید کرده است که احتمالاً در ده سال آینده به‌عنوان ابزاری برای تهدید در اختلال سامانه‌های دفاعی کشورها استفاده کند (گودرزی و جلالی، ۱۴۰۰: ۵۵).

۴.۵. افزایش و به‌کارگیری فناوری‌های همگرا

فناوری‌های همگرا می‌توانند در راستای پیشبرد اهداف توسعه پایدار به‌کار روند. افزون بر این، فناوری‌های یادشده می‌توانند موجب تکیه و تأکید بیش‌از اندازه به فناوری شوند. شاید این‌گونه پنداشته شود که اگر فناوری‌های همگرا آسیب و فشارهای وارد بر محیط‌زیست را کاهش دهند، نیازی به محدودسازی مصرف و انتشار گازها و پسماندهای زیان‌بار نباشد. از آنجاکه تکیه و تأکید بیش‌از اندازه به فناوری می‌تواند خطر آفرین باشد، بنابراین اتخاذ سیاست‌های زیست‌محیطی مناسب نیازمند آگاهی از کاستی‌های کنونی و میان‌مدت فناوری است (گودرزی و جلالی، ۱۴۰۰: ۵۶).

۴.۶. افزایش کاربرد اینترنت (اینترنت اشیاء)

اینترنت، همچنان یکی از ابزارهای اصلی برای مدیریت عملیات تروریستی است، به‌ویژه در وضعیتی که شکستن رمزینها هرروز دشوارتر می‌شود. افزون بر این، جرائم اینترنتی می‌تواند به‌عنوان یک منبع مالی برای برخی سازمان‌های تروریستی به کار گرفته شود. از سوی دیگر، افزایش امکان دسترسی به پیشینه عمومی و اطلاعات دیگران در اینترنت، فرصت‌های تازه‌ای را برای تجسس و رهگیری فعالیت‌های تروریستی فراهم خواهد آورد (گودرزی و جلالی، ۱۴۰۰: ۵۶).

۷.۴. رشد انرژی‌های نو

روش‌های کنونی بر تبدیل انرژی نفتی و ذخیره‌های موجود و باقیمانده آن و تولید احتمالی نفت استوار هستند. این رویکرد تکاملی ممکن است ادامه داشته باشد و بازار جهانی را با نوسان‌های قیمت و خطرپذیری به دلیل وابستگی به هیدروکربن روبه‌رو سازد. در پایان این دوره، پیشرفت‌های عمده‌ای در دیگر منابع انرژی، پیش‌بینی می‌شود و به‌احتمال فراوان می‌توان به هم‌جوشی هسته‌ای اشاره کرد. انتظار می‌رود که بازار نیرومندی برای تأمین‌کنندگان کوچک‌تر و اثربخش‌تر پیرامون انرژی در این دوره پدید آید که به‌احتمال فراوان به‌شدت یافتن پژوهش‌ها پیرامون اتانول، متانول، هیدروژن و پیل‌های سوختی منجر خواهد شد (گودرزی و اجلائی، ۱۴۰۰: ۵۷-۵۰).

۵. تأثیر روند گسترش و فعالیت فناوری‌های نوظهور بر محیط امنیتی ج.ا. ایران

پیچیدگی روزافزون تحولات محیط بین‌الملل و تعاملات تنگاتنگ و نزدیک کشورها، فعل‌وانفعالات سیاسی و فرایندهای نظامی، محیط جنگ‌های پیشرفته را از حاکمیت مطلق تاکتیک‌ها و رویه و روش‌ها (راهبردها) نظامی تا حدودی خارج ساخته و حوزه نفوذ و تأثیر عوامل تکنولوژی، اقتصادی، فرهنگی، سیاسی و ... را در این محیط گسترش داده است. ایجاد اختلال در اطلاعات نظامی دیگران از طریق ابزارهای رایانه‌ای و اینترنت، ایجاد آشفتگی و سردرگمی در فرایند تصمیم‌گیری گروه‌های هدف، تلاش برای شکل‌دادن به افکار عمومی جامعه هدف، ایجاد اختلال در تجهیزات راداری، موشکی و پردازش و تحلیل اطلاعات از جمله مصادیق پیشرفت‌های جنگ‌های آینده است. ایران نیز طی سال‌های اخیر تأکید زیادی بر روی قدرت و جنگ نرم داشته و گستردگی دامنه تحولات نرم‌افزاری امنیت بین‌الملل را درک کرده است. کشورهایی که چشم‌اندازهای آتی خود را ترسیم می‌کنند، توانایی بیشتری برای مقابله با تهدیدها و چالش‌های فرارو داشته و می‌توانند به‌گونه‌ای بهتر از فرصت‌های ایجادشده بهره‌برداری نمایند (رستمی، ۱۳۹۵: ۱۸۶-۱۸۴). جنگ‌های آینده با توجه به فناوری‌های نوظهور معمولاً به‌صورت غیرعلنی انجام می‌گیرند، یعنی تا حد ممکن بازیگران قدرت در این عرصه سعی می‌کنند از رویارویی مستقیم پرهیز کنند. معمولاً پاسخگویی در همین فضا صورت نمی‌گیرد بلکه پاسخگویی به آن در یک زمینه چند فضایی (جنگ‌های هیبریدی) صورت می‌پذیرد. از این‌رو ضرورت دارد نیروهای

مسلح ایران متناسب با رویکرد کشورهای فرا منطقه‌ای، خود را با یک ساختار منطقی مجهز به علوم دفاع در حوزه های فناوری نوظهور نمایند (www.defanews.ir).

۶. نتیجه‌گیری و پیشنهاد

گسترش روزافزون فناوری‌های نوظهور و گستردگی ابزار و تجهیزات سخت‌افزاری و نرم‌افزاری، اشکال جدیدی از جنگ را پدید آورده است. مسلماً به دلیل اجبار کشورها/ارتش‌ها در بهره‌برداری از آخرین دستاوردهای فناوری، شناسایی و ورود به موقع و صحیح در عرصه‌های نوین به یکی از دغدغه‌های طراحان و بازیگران حوزه راهبرد و دفاع تبدیل گردیده است. فناوری‌های نوین به صورت یک سلاح جدید، یک منبع انرژی جدید یا یک وسیله ارتباطی جدید همگی موجب شده‌اند که با اصلاح دکترین، سازمان و راهبردهای نظامی، طرف نوآور از جنگ فرسایشی پرهیز کرده و در عوض بعد ذهنی را متحول می‌کند. در آینده اخلاص در شبکه‌های اطلاع‌رسانی و ارتباطی، اخلاص در سامانه‌های که زیرساخت‌های زندگی اجتماعی را هدایت و کنترل می‌کنند، حمله‌های سایبری و نرم‌افزاری، کنترل و هدایت شناخت و انجام عملیات روانی و... نمونه‌هایی از سلاح‌های مورد استفاده در جنگ‌های آینده خواهند بود. در جنگ‌های آینده شاهد تغییراتی در ترکیب بازیگران جنگ نیز خواهیم بود. از این رو نباید تصور شود حتماً جنگ را در قالب دشمنی چهره به چهره دو دولت یا دو قوای مسلح ببینیم. شاید شکل جنگ‌های آینده، درگیری بین ملت‌ها با دولت متجاوز باشد، یا اینکه در تداوم مقابله با متجاوز، ملت‌ها در کنار ارتش و نیروهای مسلح خود قرار گیرند. محیط جنگ یا صحنه نبرد نیز متغیر دیگری است که موجب برتری برخی سلاح‌ها نسبت به برخی دیگر می‌شود. می‌توان جنگ‌های آینده را از نظر محیط به عنوان جنگ در محیط ویژه یاد کرد. همچنین توجه به اصل غافلگیری در جنگ‌های آینده مخصوص سطح تاکتیکی جنگ نیست، بلکه این اصل در سطح راهبردی هم جایگاه ویژه‌ای خواهد داشت. در حالی که در جنگ‌های آینده همچنان انسان‌ها نقش اصلی را بازی خواهند کرد، اما چهار عامل گسترش سامانه‌های هوشمند، انسان‌های تکامل‌یافته، نبرد سریع و قاطع بر سر اطلاعات، استفاده از روش‌های جدید و شبکه‌ای هوشمند برای فرماندهی و کنترل به طور قابل ملاحظه‌ای ماهیت جنگ‌ها را تغییر داده و خواهد داد.

اما در مورد تأثیر این فناوری‌های نوظهور بر محیط امنیتی - دفاعی جمهوری اسلامی ایران بایستی یادآور شد که، وقوع جنگ‌های اخیر در منطقه و هم‌جوار با مرزهای ایران و تجربیات به‌دست‌آمده از این جنگ‌ها، ضرورت و حساسیت توجه به کارکردها و مقدرات اطلاعاتی در صحنه‌های نبرد واقعی را برای سامانه‌های اطلاعاتی جمهوری اسلامی ایران دوچندان نموده است. نقش فناوری‌های نوین اطلاعاتی در جنگ‌های آینده جهت صیانت و حفاظت از یگان‌ها، طرح‌های عملیاتی و مأموریت‌های فرماندهی در عرصه جنگ احتمالی آینده با دشمنی‌های رقیبان منطقه‌ای و بین‌المللی به لحاظ اطلاعات، فناوری و ابزار و تجهیزات در حوزه‌های مختلف «هوا، فضا، زمین و دریا» در سطح جهانی از برتری نسبی برخوردار می‌باشد، ضرورتی انکارناپذیر به شمار می‌رود. نیروهای مسلح می‌بایست همواره روند نوآوری‌ها و پیشرفتهای فناوری را پایش کرده و کاربردها و محصولات تازه را شناسایی کنند. به‌ویژه، می‌بایست به فناوری‌های نوپدید و همگرا توجه ویژه‌ای داشته و از خط‌شکنی‌های آن‌ها آگاه باشند. این مسئله موجب می‌شود نیروهای مسلح از یکسو در دهه آینده به صنایعی روزآمد، پرکاربرد و قدرتمند مجهز شوند و از سوی دیگر، از آمادگی کافی برای رویارویی و سرکوب تهدیدات نوین و فناورانه برخوردار باشند. همچنین در حوزه فناوری‌ها و صنایع دفاعی، برای کسب آمادگی کافی در مسیر رویارویی با تهدیدها و واکنش در برابر مخاطرات، می‌بایست کلان‌روندها و رویدادهای جهانی و عمده فناورانه را شناسایی کرد و نقش و جایگاه نوآوری‌ها و کاربردهای نوین فناورانه را به‌درستی شناخت

موقعیت جغرافیایی جمهوری اسلامی ایران مانند هر کشور دیگری برایش ظرفیت‌ها، فرصت‌ها، محدودیت‌ها، چالش‌ها و تهدیداتی را به وجود می‌آورد. اگر از این ظرفیت‌ها به‌درستی استفاده نشود کشور آسیب می‌بیند و اگر در برابر چالش‌ها و تهدیدات به‌درستی تدبیر نشود محیط امنیتی، منافع ملی و امنیت ملی کشور دچار خسران می‌گردد. با توجه به این اصل که یک اصل پذیرفته‌شده در روابط بین‌دولت‌ها و ملت‌ها است، اساساً برای کشوری همچون ایران که دارای همسایگان متعدد است باید در حوزه سیاست خارجی و محیط امنیتی - دفاعی خود الزامات خاصی را فراهم آورد. هرچند ما در طول سال‌های گذشته با اکثر همسایگان خود روابط مطلوبی داشته‌ایم اما این روابط را هیچ‌گاه در قالب‌های ساختاریافته تعریف نکردیم. مثلاً امروز هیچ رابطه مشخص و تعریف‌شده‌ای از ارتباط با پاکستان یا ترکیه نداریم. این در حالی است که قاعدتاً در وهله اول می‌بایست یک راهبرد کلان نسبت به همسایگان داشت که می‌تواند تحت عنوان راهبرد همسایگی

تعریف شود. لذا اگر همسایگان شرقی و غربی و شمالی و جنوبی خود را باهم مقایسه کنیم درمی‌یابیم که چه همسایگان متنوعی پیرامون خود داشته و قاعدتاً این تنوع، ظرفیت‌های قابل توجهی در خود نهفته دارد. یعنی این ظرفیت‌ها هم می‌تواند موجب توسعه مناسبات و روند صلح و گسترش مناسبات اقتصادی و سیاسی و ... شود و هم می‌تواند تهدیدزا و چالش‌آفرین برای محیط امنیتی- دفاعی و مرزهای ملی و بین‌المللی ایران باشند. در روابط دوجانبه ایران با اکثر همسایگان خود پیمان‌نامه‌های دوجانبه وجود دارد. اما مشکل زمانی است که بازیگران ثالث می‌توانند بر این پیمان‌نامه‌ها تأثیر بگذارند. ایران کشوری است که از فشار قدرت‌های بزرگ چندان تأثیر نپذیرفته اما همسایگان ایران در اکثر مواقع این تأثیرات را پذیرفته‌اند. سیاست خارجی ایران در سال‌های گذشته نیز بیشتر معطوف به ایجاد ارتباط با کشورهای غربی بوده و این مسئله مانع شکل‌گرفتن تفکر منطقه‌ای و منطقه‌گرایی شده است. اما اگر بخواهیم تهدیدات آینده ایران را بررسی کنیم پیشنهاد می‌شود این تهدیدات را به دودسته آشکار و پنهان تقسیم کنیم. برخی از تهدیدات مانند حضور رژیم صهیونیستی در مجاورت مرزهای ایران (هرچند باوجود فناوری‌های نوظهور و جنگ‌های پیش روی دیگر مرزها چندان اهمیتی از این لحاظ نخواهند داشت) یا حضور نظامی آمریکا در منطقه و تنش‌های آشکار برخی از همسایگان با ایران می‌تواند تهدیدات عینی و آشکار باشند. درواقع راه‌های مقابله با این تهدیدات چندان سخت نیست چون ایده‌پردازان و صاحب‌نظران آن‌ها را مشاهده نموده و در مورد راه‌های مقابله با این تهدیدات قطعاً برنامه‌ریزی کرده و خواهند کرد. اما در مورد تهدیدات پنهان مثلاً در حوزه شمال غرب و سدسازی‌هایی که ترکیه در داخل کشور خود انجام می‌دهد. این پروژه تحت عنوان گاپ می‌تواند در آینده هم مناطق شمالی و هم جنوب ایران در دسترسی به آب دچار مشکل عدیده نماید. مشکل و تهدید پنهان دیگر بحران ریزگردها است که زندگی را در نوار غربی و حتی مناطق جنوبی و مرکزی ایران بسیار سخت و طاقت‌فرسا نموده است. یا تهدید دیگر بحث قوم‌گرایی و اقلیت‌های قومی- مذهبی هستند که هرکدام در خارج از کشور نیز دنباله‌ای دارند. که این مورد نیز در آینده می‌تواند باعث چالش جدی هم در شمال غرب و شمال و هم در جنوب و جنوب غرب و هم در شرق و شمال شرق ایران شود.

فهرست منابع

الف. منابع فارسی

- ادمی، علی؛ رضایی، نیما (۱۳۹۵) ماهیت و ابعاد رژیم ضمنی غیررسمی امنیت منطقه‌ای (جمهوری اسلامی) در منطقه غرب آسیا، فصلنامه پژوهش‌های سیاسی جهان اسلام، زمستان، سال ششم، شماره ۴.
- تسلیمی‌کار، بهروز (۱۳۹۹) مشخصات سامانه‌های فرماندهی و کنترل نظامی متناسب با ویژگی‌های محیط جنگ‌های آینده، فصلنامه فرماندهی و کنترل، زمستان، سال چهارم، شماره ۴.
- جمشیدی، محسن؛ سعیدی نژاد، حمیدرضا (۱۳۹۹) بین‌الملل‌گرایی ایالات متحده آمریکا بعد از یازدهم سپتامبر ۲۰۰۱ و سیاست خارجی جمهوری اسلامی ایران (رویکردی ساختاری یا نوکلاسیک)، فصلنامه تخصصی علوم سیاسی، تابستان، سال شانزدهم، شماره ۵۱.
- جمشیدی، محسن؛ سعیدی‌نژاد، حمیدرضا (۱۴۰۰) نظم نوین جهانی و رویکرد ایدئولوژیکی-امنیتی جمهوری اسلامی ایران (طرح معمای امنیتی دفاع - تهاجم و قدرت نرم این کشور در منطقه تحت نفوذ)، مجله سیاست دفاعی، زمستان، سال سی‌ام، شماره ۱۱۷.
- خمسه، عباس؛ رجبی، مهدی (۱۳۹۶) شناسایی و اولویت‌بندی عوامل راهبردی مؤثر بر برون‌سپاری پروژه‌های R&D در صنایع دفاعی با رویکرد آینده‌پژوهی، فصلنامه آینده‌پژوهی دفاعی، سال دوم، شماره ۴.
- رستمی، فرزاد (۱۳۹۵) تحول در ماهیت جنگ‌های آینده جمهوری اسلامی ایران: سناریوها؛ فرصت‌ها و چالش‌ها، مجله سیاست دفاعی، سال بیست و چهارم، شماره ۹۷.
- رشید، غلامعلی؛ پوردستان، احمدرضا؛ رضایی، محسن (۱۴۰۰) عوامل و ویژگی‌های نسل چهارم جنگ‌ها مؤثر بر صحنه جنگ آینده، فصلنامه مطالعات دفاعی استراتژیک، سال نوزدهم، شماره ۸۳.
- رمضان زاده، مجتبی؛ غیوری‌ثالث، مجید؛ احمدوند، علی‌محمد؛ آقایی، محسن؛ نظری‌فرخی، ابراهیم (۱۴۰۰) بررسی قدرت پدافند سایبری نیروهای مسلح با روش برنامه‌ریزی مبتنی بر سناریونویسی، فصلنامه آینده‌پژوهی دفاعی، سال ششم، شماره ۲۰.
- طاهری، محمد؛ محمد زهرایی، سپهر؛ محمدی تودشکی، محمدرضا (۱۳۹۹) فناوری‌ها و روش‌های اجرای بازی جنگ سایبری، دو فصلنامه بازی جنگ، دوره سوم، شماره ۶.
- طاهری‌هشی، علی؛ دهقان، حبیب‌الله؛ نادری، علیرضا (۱۳۹۷) شناسایی و اولویت‌بندی انواع تهدیدات در صحنه جنگ‌های آینده با استفاده از روش ترکیبی AHP - TOPSIS، فصلنامه آینده‌پژوهی دفاعی، سال سوم، شماره ۹.

- گودرزی، غلامرضا؛ اجلالی، محمدمهدی (۱۴۰۰) تحلیل روندهای آینده فناوری‌های دفاعی در افق ده‌ساله، فصلنامه آینده‌پژوهی دفاعی، سال ششم، شماره ۲۳.
- مراد پیری، هادی؛ خضرای، حمیدرضا (۱۳۹۹) نقش فناوری‌های نوین اطلاعاتی در جنگ‌های آینده، دو فصلنامه علمی مطالعات قدرت نرم، سال دهم، شماره ۲.

سایت‌ها و خبرگزاری‌ها

- <https://www.fa.m.wikipedia.org>.
- <https://www.farsnews.ir>.
- <https://www.gunsmonitor.com>.
- <https://www.irna.ir>.
- <https://www.Bestfarsi.ir>.
- <https://www.defanews.ir>.
- <https://www.sashiraz.co.ir>.
- <https://www.sanat.ir>.
- <https://www.tdooffice@mod.ir>.
- <https://www.ecasb.com>.
- <https://www.hesa.ir>.

ب. منابع انگلیسی

- Sayler, Kelley M. (2020). Emerging Military Technologies: Background and Issues for Congress. Publishing: Congressional Research Service. Washington DC.
- Luketic, N. (2013). Future Technology Themes: 2030 to 2060. DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION FISHERMANS BEND (AUSTRALIA).
- Founder of the Office of National Estimates. (2021). Global trends 2040. A Publication of the National Intelligence Council. Office of the Director of National Intelligence.
- Walt, S. M. (2001), "Beyond Bin Laden: Reshaping U.S. Foreign Policy, International Security", Vol. 26, No. 3, Winter, in: https://www.belfercenter.org/sites/default/files/files/publication/walt_winter_01_02.pdf