Knowledge of political interpretation
Vol 7, No 23, Summer 2025
ppt 47-79 Received: April 6, 2025
Accepted**:** July 19, 2025

Scenario Scenarios for the Future of International Security in the Age of Artificial Intelligen

Vahid Reza Sahlabadi[1]
Zahra Sahlabadi [2]

Abstract

Throughout history, technology has played a pivotal role in transforming international security paradigms. In the contemporary era, the emergence of Artificial Intelligence (AI) has significantly impacted these shifts, indicating that global power equations have transitioned into a competition over data and algorithms. This research, employing a futures studies approach and scenario analysis method, delineates three plausible pathways for Great Power competition by 2040: "Controlled Hybrid Competition," "Total Algorithmic Warfare," and "Technological Coexistence and Competition." The findings indicate that while the second scenario possesses tactical appeal, it constitutes an existential dead-end due to the exclusion of humans from the decision-making loop and the heightened risk of accidental crises. Conversely, the other two scenarios are more sustainable as they preserve human sovereignty. The article argues that future security will be a function of technological diplomacy and algorithmic risk management, necessitating that the global community prevent the trap of an autonomous arms race through the formulation of ethical regulations and the strengthening of national data sovereignty.

Keywords: Artificial Intelligence, International Security, Futures Studies, Globalization

[1] .M.Sc. in Electrical Engineering, Islamic Azad University, North Tehran Branch, tehran,iran. **Vahidreza.sahlabadi85@gmail.com**
[2] Ph.D. Candidate in Public Policy, Tehran Central Branch, tehran,iran
Zahra.sahlabadi84@gmail.com

تاریخ دریافت: ۱۴۰۴/۰۴/۱۷ | تاریخ پذیرش: ۱۴۰۴/۰۷/۲۸
دانش تفسیر سیاسی Knowledge of political interpretation
سال هفتم، شماره ۲۴، پاییز ۱۴۰۴ Vol 7, No 24,Atumn2025
صفحات ۷۹-۴۷ ppt 47-79

سناریوهای آینده امنیت بین‌الملل در عصر هوش مصنوعی

وحیدرضا سهل آبادی [۱]
زهرا سهل آبادی [۲]

چکیده

در طول تاریخ فناوری و به ویژه در عصر کنونی ظهور هوش مصنوعی (AI) بر دگرگونی پارادایم‌های امنیت بین‌الملل تاثیرگذار بوده است و نشان دهنده این است که معادلات قدرت جهانی به رقابت بر سر داده و الگوریتم منتقل شده است. این پژوهش با رویکرد آینده‌پژوهی و روش تحلیل سناریو، سه مسیر محتمل برای رقابت قدرت‌های بزرگ تا سال ۲۰۴۰ را ترسیم می‌کند که عبارتند از «رقابت هیبریدی کنترل‌شده»، «جنگ الگوریتمی تمام‌عیار» و « همزیستی و رقابت فناورانه». یافته‌ها نشان می‌دهد که سناریوی دوم علی‌رغم جذابیت تاکتیکی، به دلیل حذف انسان از چرخه تصمیم‌گیری و افزایش ریسک بحران‌های تصادفی، یک بن‌بست وجودی است؛ در حالی که دو سناریوی دیگر با حفظ حاکمیت انسانی پایدارترند. مقاله استدلال می‌کند که امنیت آینده تابعی از دیپلماسی فناوری و مدیریت ریسک الگوریتمی خواهد بود و ضرورت دارد جامعه جهانی با تدوین مقررات اخلاقی و تقویت حاکمیت ملی داده، از دام مسابقه تسلیحاتی خودکار جلوگیری نماید.

واژگان کلیدی: هوش مصنوعی، امنیت بین‌الملل، آینده‌پژوهی، بین الملل

۱.۱ کارشناسی ارشد برق مخابرات گرایش سیستم ،واحد تهران شمال، تهران، ایران (نویسنده مسئول).
Vahidreza.sahlabadi85@gmail.com
[۱۲] دانشجوی دکتری سیاستگذاری عمومی واحد تهران مرکزی، تهران، ایران
Zahra.sahlabadi84@gmail.com

۱. مقدمه

امنیت بین‌الملل همواره به عنوان یکی از پیچیده‌ترین و پویاترین حوزه‌های مطالعات روابط بین‌الملل شناخته شده است. از دوران وستفالی (۱۶۴۸) تا پایان جنگ سرد، معادلات امنیتی عمدتاً بر پایه توزیع قدرت مادی شامل جمعیت، منابع طبیعی، ظرفیت صنعتی و کلاهک‌های هسته‌ای تعریف می‌شدند. در این نظم سنتی، «قدرت» کمیتی بود که قابل اندازه‌گیری، تجمیع و نمایش بود. یک تانک، یک زیردریایی یا یک پایگاه نظامی، نمادهای عینی و ملموس حاکمیت و توان بازدارندگی محسوب می‌شدند. دکترین‌های امنیتی نیز بر اساس مفاهیمی نظیر «موازنه ترس»، «حمله پیش‌دستانه» و «بازدارندگی متقابل» شکل گرفتند که در آن‌ها عقلانیت انسانی و محاسبات هزینه-فایده، محور اصلی تصمیم‌گیری‌های راهبردی بودند.

اما با آغاز قرن بیست و یکم و شتاب گرفتن انقلاب صنعتی چهارم، بنیان‌های این نظم سنتی دچار لرزش‌های ساختاری جدی شده‌اند. ظهور فناوری‌های نوظهور، به‌ویژه هوش مصنوعی نه تنها ابزارهای جدیدی برای اعمال قدرت ایجاد کرده، بلکه ماهیت خودِ «قدرت» و «امنیت» را بازتعریف کرده است. هوش مصنوعی به عنوان یک فناوری دوگانه و یک نیروی تغییردهنده بازی، مرزهای میان صلح و جنگ، سرعت تصمیم‌گیری نظامی، و حتی مفهوم هویت ملی را تحت تأثیر قرار داده است. برخلاف سلاح‌های هسته‌ای که ماهیت ایستا و بازدارندگی منفی داشتند، هوش مصنوعی ماهیتی سیال، یادگیرنده و تهاجمی دارد که می‌تواند در لحظه برتری تاکتیکی ایجاد کند؛ هوش مصنوعی که به‌عنوان مجموعه‌ای از فناوری‌ها تعریف می‌شود که سیستم‌های کامپیوتری را قادر می‌سازد تا وظایفی را که نیاز به هوش انسانی دارند، انجام دهند به عامل مهمی در تحول قدرت نظامی کشورها تبدیل‌شده است (شاملو، ۱۴۰۱:۹۶).

این تحول فناورانه، رقابت قدرت‌های بزرگ را وارد فاز جدیدی کرده است. ایالات متحده، چین و روسیه هر کدام با استراتژی‌های متمایزی اما با هدف مشترکِ دستیابی به

«برتری هوشمندانه» وارد میدان رقابت شده‌اند. برای ایالات متحده، هوش مصنوعی ابزاری برای حفظ هژمونی تکنولوژیک و نظامی خود در برابر رقبای صعودی است. برای چین، توسعه هوش مصنوعی بخشی جدایی‌ناپذیر از برنامه «رویای قرن بیستمی چین» و تبدیل شدن به رهبر جهانی فناوری تا سال ۲۰۳۰ است. روسیه نیز با سرمایه‌گذاری کلان در سیستم‌های تسلیحاتی خودکار و جنگ هیبریدی، تلاش می‌کند تا شکاف تکنولوژیک خود را جبران کرده و نفوذ ژئوپلیتیک خود را در خاورمیانه و اوراسیا تثبیت کند.

چالش اصلی در این میان، عدم تقارن اطلاعاتی و سرعت غیرقابل تصوری است که ماشین‌ها نسبت به انسان دارند. در نبردهای آینده، چرخه OODA (مشاهده، جهت‌گیری، تصمیم‌گیری، اقدام) ممکن است از سطح دقیقه‌ای یا ساعتی به سطح میلی‌ثانیه‌ای کاهش یابد. این پرسش بنیادین مطرح می‌شود که آیا انسان همچنان قادر به کنترل فرآیندهای مرگبار خواهد بود یا اینکه سیستم‌های هوشمند با الگوریتم‌های یادگیری عمیق ، مسیری مستقل از اراده رهبران سیاسی طی خواهند کرد؟ پدیده‌ای که کارشناسان امنیتی آن را «بحران ثبات–ناپایداری الگوریتمی» می‌نامند، هشدار می‌دهد که رقابت برای کسب سرعت بیشتر، می‌تواند منجر به تشدید ناخواسته تنش‌ها و حتی شروع جنگ توسط ماشین‌ها بدون دخالت مستقیم انسان شود.

علاوه بر ابعاد نظامی، هوش مصنوعی قلمرو جنگ روانی و عملیات اطلاعاتی را نیز دگرگون کرده است. با قابلیت تولید محتوای جعلی بسیار واقعی ، تحلیل کلان‌داده‌ها برای پیش‌بینی رفتارهای اجتماعی و نفوذ در افکار عمومی، امنیت داخلی کشورهای مستقل نیز به شدت آسیب‌پذیر شده است. این امر نشان می‌دهد که مرزهای دفاعی دیگر صرفاً جغرافیایی نیستند، بلکه در فضای سایبر، شبکه‌های اجتماعی و حتی درون ذهن شهروندان جریان دارند؛ دیپ‌فیک به عنوان تکنیکی مبتنی بر هوش مصنوعی که امکان تولید محتوای صوتی، تصویری و متنی جعلی با واقعیت بسیار بالا را فراهم می‌کند، تهدیدی جدی برای امنیت سایبری محسوب می‌شود. این فناوری توانایی هکرها را در اجرای حملات پیچیده و

فریبنده، به‌ویژه در مهندسی اجتماعی، افزایش داده است. از طریق ایجاد ایمیل‌های فیشینگ غیرقابل تشخیص و دیپ‌فیک‌های واقعی برای جعل هویت، مهاجمان می‌توانند افراد را به کلیک روی لینک‌های مخرب، دانلود فایل‌های آلوده یا افشای اطلاعات حساس فریب دهند(Avey,2023).

بنابراین، بررسی آینده امنیت بین‌الملل در عصر هوش مصنوعی، نیازمند عبور از تحلیل‌های خطی و گذشته‌نگر است. ما با یک نقطه عطف تاریخی روبرو هستیم که در آن، قوانین بازی امنیتی بازنویسی می‌شوند. این مقاله با اتخاذ رویکرد آینده‌پژوهی و استفاده از روش «تحلیل سناریو»، تلاش می‌کند تا با شناسایی متغیرهای کلیدی و عدم قطعیت‌های ساختاری، مسیرهای محتمل پیش‌روی روابط بین‌الملل را ترسیم کند. سوال اصلی این پژوهش آن است که رقابت قدرت‌های بزرگ در حوزه هوش مصنوعی، چگونه ساختار نظم بین‌الملل را در دهه‌های آینده دگرگون خواهد کرد؟ آیا جهان به سمت قطبی شدن تکنولوژیک حرکت می‌کند یا به سمت نوعی همزیستی و رقابت فناورانه؟ و مهم‌تر از همه، آیا می‌توانیم چارچوب‌هایی برای مدیریت ریسک‌های ناشی از خودمختاری ماشین‌ها طراحی کنیم، یا اینکه در دام یک مسابقه تسلیحاتی الگوریتمی بی‌پایان گرفتار خواهیم شد؟

پاسخ به این سوالات، تنها با درک عمیق از تعامل پیچیده میان فناوری، سیاست و روانشناسی تصمیم‌گیری در شرایط بحران امکان‌پذیر است. در ادامه، این پژوهش با مرور مبانی نظری و سپس ارائه سه سناریوی آینده‌نگرانه، سعی در ارائه نقشه‌راهی تحلیلی برای سیاست‌گذاران و پژوهشگران حوزه امنیت بین‌الملل دارد.

۲. مبانی نظری

در نظریه کلاسیک امنیت، بازدارندگی بر پایه شفافیت توانایی‌ها و هزینه‌های احتمالی حمله استوار بود. اما در عصر هوش مصنوعی، ویژگی‌های زیر تعادل را بر هم می‌زند:

۱. ابهام در تشخیص نیت: الگوریتم‌های یادگیری عمیق می‌توانند رفتارهای دشمن را شبیه‌سازی کنند، اما تفسیر خروجی‌های آن‌ها برای رهبران انسانی دشوار است. این «جعبه سیاه» (Black Box) بودن الگوریتم‌ها، اعتماد متقابل را تضعیف می‌کند.

۲. عدم تقارن اطلاعاتی: دسترسی به کلان‌داده‌ها (Big Data) و ابررایانش، برتری کیفی ایجاد می‌کند که با تعداد نیروی انسانی جبران‌ناپذیر است. طرفی که داده‌های بیشتری دارد، الگوریتم دقیق‌تری دارد و الگوریتم دقیق‌تر، تصمیمات سریع‌تری می‌گیرد.

۳. سرعت بحرانی: در نبردهای سایبری و الکترونیک مبتنی بر هوش مصنوعی ، ثانیه‌ها تعیین‌کننده پیروزی هستند. این سرعت، فرصت دیپلماسی اضطراری و مداخلات انسانی[1] را کاهش می‌دهد و خطر «تشخیص اشتباه» را افزایش می‌دهد.

۳. روش‌شناسی: تحلیل سناریو

شناخت آینده به‌منظور کسب آمادگی برای مدیریت رویدادهای پیش‌بینی‌ناپذیر و تدبیر در مورد آن‌ها با رویکردی خردمندانه و هوشمندانه ضروری است. در آینده‌پژوهی با بهره‌گیری از طیف وسیعی از روش‌ها و به‌جای تصور «تنها یک آینده»، به گمانه‌زنی‌های نظام‌مند و خردورزانه، در مورد نه‌تنها «یک آینده» بلکه «چندین آینده متصور» مبادرت می‌شود. موضوعات آینده‌پژوهی دربرگیرندۀ گونه‌های «ممکن»، «محتمل»، «دلخواه» برای دگرگونی از حال به آینده هستند (گرامی طیبی، ۲۰۱۷). آینده‌پژوهی به روش‌های مختلفی انجام می‌شود، در این مقاله با توجه به ماهیت موضوع یعنی جنگ در اوکراین، سناریونویسی روش مناسب‌تری است، همان‌طور که سناریونویسی در جنگ جهانی دوم به‌عنوان روشی برای طرح‌ریزی نظامی (در حوزه دانش تحقیق در

[1] Human-in-the-loop

عملیات) پدیدار شد (وندرهیجدن، ۱۹۹۵) و توسط هرمن کاهن[1] به متن سیاست عمومی و پیش‌بینی اجتماعی بسط یافت (Van der Heijden, 2005: 3).

با روش سناریونویسی رهبران و مدیران با نگاه به رویدادهای غیرمنتظره در آینده و درک عمیق پیامدهای احتمالی آن‌ها، چندین داستان یا روایت متمایز دربارهٔ آینده‌های ممکن را کشف و تعریف می‌کنند. این سناریوها ابزاری برای نظم بخشیدن به بینش‌ها و استنباط‌ها هستند. مقصود از تعریف سناریوها انتخاب فقط یک آینده مرجح و آرزوی به حقیقت پیوستن آن یا پیدا کردن محتمل‌ترین آینده و سعی در تطبیق با آن نیست، بلکه هدف اصلی، برنامه‌ریزی بر پایه سناریو و اتخاذ تصمیم‌های استراتژیک است که برای همه آینده‌های ممکن به‌اندازه کافی خردمندانه و پابرجا باشند. اگر هنگام تدوین سناریوها تفکر جدی صورت بگیرد، آنگاه اصلاً مهم نیست که در آینده چه اتفاقی خواهد افتاد، زیرا تصمیم‌گیرنده در مقابل هر اتفاقی آماده است و می‌تواند بر مسیر اتفاقات آینده تأثیرگذار باشد (لشکر بلوکی، ۱۳۹۲). روش‌های آینده‌پژوهی بر اساس اهداف به دودسته هنجاری و اکتشافی تقسیم می‌شوند. مبنای روش‌های هنجاری، ارزش‌ها و هنجارها هستند و از آینده‌های مطلوب برای تصمیم‌گیری در زمان حال سؤال می‌کنند، درحالی‌که روش‌های اکتشافی به دنبال این هستند که برمبنای گذشته و حال چه چیزی امکان وقوع دارد (مردوخی، ۱۳۹۱: ٣٤-٦). در این پژوهش از ترکیبی از روش‌های هنجاری و اکتشافی استفاده خواهد شد. در سناریونویسی مشخص کردن دو مسئله یعنی بازیگران تأثیرگذار و پیشران‌های مؤثر ضرورت دارد که در اینجا بدان می‌پردازیم.

[1]. Herman Kahn

در سناریونویسی شناسایی پیشران‌ها اهمیت بالایی دارد، پیشران‌ها مستقل از مسئله و موضوع هستند که بر آن تأثیر می‌گذارند. به‌بیان‌دیگر، پیشران‌ها به صورتی غیرمستقیم بر حوزه‌های دیگر تأثیرگذارند. درروش سناریونویسی، شناسایی مهم‌ترین بازیگران و مؤلفه‌ها و شناسایی پیشران‌ها یکی از گام‌های اساسی رسیدن به سناریوها است (Schwartz, 1996).

برای آینده‌پژوهی این موضوع، از روش «تحلیل سناریو» استفاده شده است. دو بعد عدم قطعیت کلیدی شناسایی شدند:

بعد اول: سطح همکاری/تنش در توسعه قوانین و مقررات جهانی (حکمرانی جهانی).

بعد دوم: سطح بلوغ فنی و تسلط عملیاتی بر کاربرد نظامی (سطح خودمختاری تسلیحات).

ترکیب این ابعاد منجر به خلق سه سناریوی محتمل شد.

٤. تحلیل عمیق سناریوهای آینده امنیت بین‌الملل (٢٠٣٥-٢٠٤٠)

سناریوی اول: رقابت هیبریدی کنترل‌شده [1]

در این سناریوی آینده‌نگر، که تحت عنوان «رقابت هیبریدی کنترل‌شده» شناخته می‌شود، پارادایم حاکم بر روابط بین‌الملل قدرت‌های بزرگ از «تلاش برای حذف متقابل» به سمت «مدیریت هوشمندانه تنش» تغییر مسیر می‌دهد. فرض بنیادین این روایت آن است که بازیگران اصلی نظام بین‌الملل، به‌ویژه ایالات متحده، چین و روسیه، درمی‌یابند که هزینه‌های یک جنگ مستقیم فیزیکی تمام‌عیار در عصر هوش مصنوعی، نه تنها فراتر از توانایی بازدارندگی سنتی است، بلکه می‌تواند منجر به نابودی متقابل زیرساخت‌های حیاتی و فروپاشی اقتصادی شود. بنابراین، منطق عقلانی حکم می‌کند که آن‌ها به جای تلاش برای پیروزی مطلق، به دنبال تثبیت وضعیتی باشند که در آن رقابت

[1] The Managed Hybrid Competition

ادامه یابد اما از مرزهای خطرناک عبور نکند. این وضعیت اگرچه شباهت‌هایی با دوران جنگ سرد دارد، اما از پیچیدگی بسیار بالاتری برخوردار است؛ زیرا سرعت واکنش سیستم‌های خودکار ماشین‌ها، چرخه تصمیم‌گیری انسانی را به میلی‌ثانیه کاهش داده و فضای تنفس برای دیپلماسی کلاسیک را تقریباً به صفر رسانده است. در این محیط، ثبات امنیتی دیگر بر پایه اعتماد متقابل یا شفافیت کامل استوار نیست، بلکه بر پایه ترس عمیق از تشدید ناخواسته و تصادفی بحران‌ها شکل می‌گیرد.

در راستای حفظ تعادل شکننده‌ی امنیتی در عصر دیجیتال، مکانیزم‌های فنی و نظامی با محوریت اصل «انسان در حلقه» (Human-in-the-Loop) طراحی شده‌اند تا خطاهای الگوریتمی به حداقل رسیده و فرمان نهایی استفاده از سلاح‌های استراتژیک همچنان در اختیار رهبران سیاسی باقی بماند؛ هرچند در سطح تاکتیکی، هوش مصنوعی نقش مشاوران هدف‌گیری پیشرفته را ایفا می‌کند. همزمان، دیپلماسی دیجیتال از طریق پروتکل‌های ارتباطی استاندارد بین مراکز فرماندهی C4ISR طرفین متخاصم، امکان تشخیص نیت واقعی و جلوگیری از سوءتفاهم‌های حسگری را فراهم ساخته است. در این چارچوب، جنگ اطلاعاتی نیز خود را محدود کرده و حملات سایبری عمدتاً علیه زیرساخت‌های غیرحیاتی متمرکز می‌شود تا از خطوط قرمز نانوشته‌ای نظیر فلج کردن شبکه‌های حیاتی که منجر به بی‌ثباتی اجتماعی و جنگ فیزیکی می‌شود، پرهیز گردد. پیامد ژئوپلیتیک این سناریو، شکل‌گیری نظم نوینی مبتنی بر «تعادل ترس الگوریتمی» است که در آن رقابت مستقیم جای خود را به نبردهای نیابتی و جنگ ترکیبی داده و ثبات جهانی بر پایه‌ی مدیریت ادراکات استوار شده است (Claverie,2021؛احمدی و همکاران، ۱۴۰۰).

همزمان، ماهیت این نبرد فراتر از کنترل جریان اطلاعات رفته و به «جنگ شناختی» تبدیل شده است که هدف آن تغییر ادراک، باورها و رفتارهای جمعی جهت تضعیف نهادهای عمومی و ایجاد شکاف اجتماعی است (Bernal & et al,2020).

این نوع جنگ با قطبی‌سازی افکار و تقویت روایت‌های متضاد، تلاش دارد انسجام داخلی جامعه هدف را مخدوش کرده و اراده‌ی مقاومت در برابر دشمن را از بین ببرد (Gil, 1990; Claverie & du Cluzel, 2021; Aronhime, 2021). با این حال، این مدل پیچیده دارای آسیب‌پذیری‌های ذاتی است؛ به‌ویژه اینکه دموکراتیزه شدن توانایی‌های نظامی توسط هوش مصنوعی، معادلات قدرت را تغییر داده و به بازیگران غیردولتی و گروه‌های تروریستی امکان داده است تا با بهره‌گیری از فناوری‌های دسترسی‌پذیر، هزینه‌های عملیاتی و دقت ضربه‌زنی خود را افزایش دهند. این تحولات، چالش‌های جدیدی را در حوزه مسئولیت‌پذیری حقوقی و اخلاقی ابزارهای هوشمند ایجاد کرده و پایداری نظم نوین امنیتی را تهدید می‌کند (arabthought, 2019).

در چنین سیستمی، وابستگی بیش از حد به نرم‌افزارها و شبکه‌های ارتباطی، یعنی یک باگ نرم‌افزاری نادیده گرفته شده در یک سامانه پدافندی، یا یک خطای الگوریتمی ناشی از آموزش ناقص داده‌ها، می‌تواند منجر به فعال‌سازی زنجیره واکنش خودکار شود. اگر یک پهپاد ناشناس متعلق به یک گروه شبه‌نظامی کوچک، توسط یک سامانه هوشمند به اشتباه به عنوان یک تهدید استراتژیک طبقه‌بندی شود و پاسخ متقابل صادر گردد، زمان کافی برای دخالت انسانی و لغو دستور وجود نخواهد داشت. علاوه بر این، حضور بازیگران غیردولتی قدرتمند مانند گروه‌های تروریستی سایبری یا هکرهای مستقل، می‌تواند با تزریق بدافزار به پروتکل‌های ارتباطی ماشینی، باعث ایجاد نویز یا پیام‌های جعلی شود که منجر به تشدید ناخواسته تنش بین قدرت‌های بزرگ گردد. بنابراین، این سناریو اگرچه از جنگ مستقیم جلوگیری می‌کند، اما جهان را در معرض تهدید دائمی «جنگ تصادفی الگوریتمی» قرار می‌دهد که ریشه در پیچیدگی فنی و عدم قطعیت ذاتی سیستم‌های هوشمند دارد، نه لزوماً در نیت خصمانه رهبران انسانی؛ مسئله با در نظر گرفتن توانایی هکرها و افزایش جرائم سایبری اهمیت بسیاری می‌یابد به‌عنوان‌مثال در اوت ۲۰۲۳، تعداد زیادی از رکوردهای حساس اینترنتی توسط هکرها به خطر افتادند. همچنین بیم نفوذ

به چت‌بات‌ها توسط آن‌ها یک تهدید دیگر است موردی که می‌توان اشاره کرد این است که بیش از ۱۰۰۰۰۰ حساب چت جی پی تی بین سال‌های ۲۰۲۲ تا ۲۰۲۳ در معرض نقض حریم خصوصی کاربران قرار گرفته است. مسمومیت داده‌ها نیز یک موضوع جدی است که ممکن است توسط عوامل خطر سوءاستفاده گرفته شود(WIZ,2023).

سناریوی دوم: جنگ الگوریتمی تمام‌عیار[1]

جنگ الگوریتمی تمام‌عیار؛ معمای «فرار از کنترل انسانی» و بحران ثبات–ناپایداری سناریوی بعدی است؛ گسترش کاربرد سلاح‌های هوشمند و سیستم‌های تسلیحاتی بدون سرنشین، ماهیت جنگ را از درگیری‌های انسانی به نبردهای الگوریتمی تغییر داده است. این گذار با کاهش قابل‌توجه تلفات جانی و پایین آمدن ریسک‌های سیاسی ناشی از کشته شدن نیروها، هزینه‌های مداخله نظامی را برای قدرت‌های بزرگ کاهش می‌دهد. در نتیجه، این شرایط انگیزه‌های تهاجمی مستقیم را تعدیل کرده و همزمان، رقابت بین دولت‌های قدرتمند را به سمت یک «مسابقه تسلیحاتی فناورانه» سوق می‌دهد که در آن برتری استراتژیک نه در تعداد نیروها، بلکه در پیشرفت تکنولوژیک تعریف می‌شود (Shuai,2021).

در این سناریوی پرتنش و پرخطر، که تحت عنوان «جنگ الگوریتمی تمام‌عیار» شناخته می‌شود، رقابت ژئوپلیتیک قدرت‌های بزرگ به اوج تنش خود می‌رسد و منطق سنتی بازدارندگی جای خود را به یک مسابقه تسلیحاتی سرعت‌محور و بی‌رحم می‌دهد. در این روایت آینده‌نگر، دکترین امنیتی حاکم بر ایالات متحده، چین و روسیه بر پایه این باور استوار می‌شود که در نبردهای مدرن، زمان حیاتی‌ترین منبع است و هر ثانیه تأخیر ناشی از فرآیندهای تصمیم‌گیری انسانی، می‌تواند منجر به شکست استراتژیک و نابودی نیروها شود. بنابراین، بازیگران اصلی به تدریج و سپس به طور ناگهانی، مرزهای میان صلح و

[1] Total Algorithmic Warfare

جنگ را محو کرده و اجازه می‌دهند سیستم‌های هوش مصنوعی (AI) نه تنها در سطح تاکتیکی، بلکه در سطوح عملیاتی استراتژیک، بدون دخالت مستقیم انسان (Human-out-of-the-loop)، تصمیمات سرنوشت‌ساز بگیرند. این گذار از «کنترل انسانی» به «خودمختاری ماشینی»، جهان را وارد فاز جدیدی از تهدیدات امنیتی می‌کند که در آن سرعت واکنش الگوریتم‌ها آنچنان بالا می‌رود که چرخه OODA (مشاهده، جهت‌گیری، تصمیم‌گیری، اقدام)[1] از مقیاس دقیقه‌ای به میلی‌ثانیه کاهش می‌یابد و فضای دیپلماسی یا توقف اضطراری عملاً از بین می‌رود؛ سرهنگ جان بوید، استراتژیست برجسته نیروی هوایی آمریکا، مفهوم چرخه را توسعه داد و استدلال کرد که طرفی که بتواند این چرخه را سریع‌تر از حریف طی کند، بر جریان نبرد مسلط خواهد شد (Bolton,2001). استفاده از هوش مصنوعی این امکان را می‌دهد که فرآیندهایی مانند نظارت بر منابع طبیعی، مدیریت بحران‌ها، پیش‌بینی نیازهای اجتماعی و حتی تحلیل وضعیت امنیتی محلی را به‌طور خودکار انجام دهند. این امر به آن‌ها این فرصت را می‌دهد تا بدون نیاز به‌صرف زمان و منابع زیاد، گزارش‌ها و تحلیل‌های دقیق‌تری داشته باشند و بتوانند تصمیمات به‌موقع و کارآمدتری اتخاذ کنند. (Onlinewilder, 2023).

مکانیزم‌های فنی و نظامی پیاده‌سازی شده در این سناریو، ماهیت جنگ را دگرگون می‌سازند و تمرکز اصلی آن‌ها بر اشباع دفاعی، پاسخ سریع و نفوذ شناختی است. یکی از برجسته‌ترین تجلیات این رویکرد، ظهور «سربازان خوشه‌ای»[2] است. در این مدل، هزاران پهپاد ارزان‌قیمت و کوچک، به جای اینکه توسط اپراتورهای جداگانه هدایت شوند، توسط یک الگوریتم مرکزی هوشمند که از یادگیری جمعی بهره می‌برد، هماهنگ

[1] observation (O), orientation (O), decision (D), and action (A).
[2] Swarm Intelligence

می‌شوند. این خوشه‌ها می‌توانند با ایجاد حجم آتش غیرقابل دفاع و اشباع سامانه‌های پدافندی هوایی پیشرفته دشمن، راه را برای حملات اصلی هموار کنند. علاوه بر این، سیستم‌های هشدار اولیه[1] مبتنی بر هوش مصنوعی، نقش تعیین‌کننده‌ای در جلوگیری از غافلگیری ایفا می‌کنند، اما همین ویژگی آن‌ها را به کابوسی برای ثبات جهانی تبدیل می‌کند. اگر این سیستم‌ها تشخیص دهند که حمله‌ای در راه است (حتی اگر این تشخیص ناشی از خطای حسگر یا نویز الکترومغناطیسی باشد)، ممکن است دستور پاسخ متقابل فوری و خودکار را صادر کنند، زیرا زمان کافی برای بررسی انسانی و تایید نهایی وجود ندارد؛ پلتفرم‌های آنلاین مبتنی بر هوش مصنوعی می‌توانند از طریق نظرسنجی‌ها، پیشنهادها و دستگاه‌های بازخورد آنلاین را تسهیل کنند. این سیستم‌ها همچنین می‌توانند در جمع‌آوری داده‌ها و تحلیل نیازهای عمومی و خاص استفاده شوند (Nahar, 2024)

این سناریو با تشدید «بحران ثبات–ناپایداری» و اوج‌گیری جنگ شناختی از طریق انتشار خودکار اخبار جعلی، منجر به فروپاشی درونی جوامع هدف پیش از آغاز رسمی جنگ می‌شود. پیامد ژئوپلیتیک آن شکل‌گیری نظم مبتنی بر «نابودی متقابل غیرهسته‌ای» است که در آن فلج کردن زیرساخت‌های حیاتی و بی‌اعتبار شدن مرزهای جغرافیایی، امنیت سنتی را نقض کرده و کشورها را در معرض تهدید وجودی قرار می‌دهد. این وضعیت بر پایه «بی‌اعتمادی مطلق» به کنترل انسانی سیستم‌های هوشمند استوار است که هر تحرک معمولی را بهانه‌ای برای تشدید تنش تبدیل می‌کند؛ همزمان، با قابلیت «شخصی‌سازی تهدیدات»، الگوریتم‌ها با بهره‌گیری از کلان‌داده‌ها، آسیب‌پذیری‌های روانشناختی رهبران را شناسایی کرده و حملات سایبری و اطلاعاتی را دقیقاً متناسب با شخصیت آن‌ها طراحی می‌کنند تا بیشترین اثر مخرب را داشته باشند.

هوش مصنوعی به سرعت در حال تبدیل شدن به فناوری تحول‌آفرین امنیتی در سطح سلاح‌های هسته‌ای است که از طریق افزایش اتوماسیون در تحلیل تصاویر ماهواره‌ای و

[1] Early Warning Systems

دفاع سایبری، برتری نظامی، اطلاعاتی و اقتصادی را دگرگون می‌کند. بخش خصوصی با تأمین عمده بودجه تحقیقاتی، شتاب این پیشرفت را دوچندان کرده است. نگرانی اصلی امنیتی آن است که دولت‌های ضعیف و بازیگران غیردولتی نیز به قابلیت حمله دوربرد و توانایی جعل واقعیت دسترسی یابند که این امر تعادل قدرت و امنیت ملی را به شدت تهدید می‌کند (Allen and Chan, 2017). این سناریو با وجود برتری تاکتیکی در سرعت و غافلگیری، به دلیل اتوماسیون کامل فرآیندهای مرگبار، بسیار شکننده و پرریسک است. بزرگ‌ترین تهدید آن «بحران تصادفی» است؛ جایی که عدم توانایی ماشین در درک زمینه و نیت طرف مقابل، باعث می‌شود خطاهای نرم‌افزاری یا تفسیر اشتباه مانورهای معمولی به عنوان حمله، زنجیره‌ای از واکنش‌های خودکار غیرقابل توقف را فعال کند. در این حالت، جنگ نه بر اساس تمایل سیاسی، بلکه ناشی از نقص‌های فنی آغاز شده و پتانسیل تبدیل شدن به یک فاجعه تمدنی با هزینه‌ای گزاف برای ثبات جهانی و امنیت بشریت را دارد.

سناریوی سوم: همزیستی و رقابت فناورانه [1]

در سناریوی «همزیستی و رقابت فناورانه» یا «بلوک‌بندی دیجیتال»، جهان به دو قطب تکنولوژیک رقیب اما درهم‌تنیده تقسیم می‌شود که جدایی کامل آن‌ها به دلیل وابستگی متقابل در زنجیره تأمین جهانی (مانند تراشه‌ها) غیرممکن است. در این نظم نوین، رقابت مستقیم نظامی کمرنگ شده و جای خود را به جنگ اقتصادی-فناوری داده است؛ جایی که ابزارهای اصلی فشار شامل تحریم‌های هوشمند، کنترل دسترسی به نیمه‌هادی‌ها و نرم‌افزارهای طراحی مدار ، و ایجاد استانداردهای موازی اینترنت (غربی با تمرکز بر حریم خصوصی در برابر شرقی با نظارت متمرکز) هستند. قدرت‌های بزرگ برای مقابله با تهدیدات سایبری و جاسوسی، بر «امنیت در لایه سخت‌افزار» و خودکفایی در تولید پردازنده‌ها سرمایه‌گذاری می‌کنند تا از نفوذ احتمالی تجهیزات خارجی جلوگیری نمایند.

[1] Technological Coexistence and Competition

پیامد ژئوپلیتیک این وضعیت، بازتعریف نقش بازیگران متوسط مانند ایران، هند و برزیل است که با سیاست «تعادل‌جویی فعال» سعی می‌کنند از موقعیت ژئوپلیتیک و منابع خود برای کسب امتیاز از هر دو بلوک استفاده کنند، هرچند این امر آن‌ها را در معرض فشارهای شدید سیاسی قرار می‌دهد. اتحادیه‌هایی مانند ناتو و بریکس نیز با تغییر تمرکز به هماهنگی سیاست‌های فناوری و حفاظت مشترک از زنجیره تأمین، مرزهای میان اقتصاد و امنیت ملی را محو می‌کنند. با این حال، این سناریو دارای آسیب‌پذیری‌های ساختاری عمیقی است؛ به‌ویژه حساسیت بالا به شوک‌های زنجیره تأمین (مانند اختلال در تنگه مالاکا یا سکوهای تایوان) که می‌تواند منجر به رکود اقتصادی گسترده شود، و همچنین خطر بی‌ثباتی داخلی در کشورهای واسطه تحت فشار «انتخاب طرفین». در نهایت، این مدل منجر به شکل‌گیری یک «صلح سرد اقتصادی-فناورانه» شکننده می‌شود که در آن هر خطای کوچک مدیریتی می‌تواند به بحران‌های تمدنی منجر گردد.

۵. مقایسه تحلیلی سناریوها (جدول ماتریس ریسک)

شاخص ارزیابی	**سناریوی رقابت هیبریدی کنترل‌شده** *صلح سرد دیجیتال*	**سناریوی جنگ الگوریتمی تمام‌عیار** *فرار از کنترل انسان*	**سناریوی همزیستی و رقابت فناورانه** *بلوک‌بندی دیجیتال*
احتمال وقوع	**متوسط** *وابسته به موفقیت دیپلماسی بین‌الملل و توافق‌نامه‌های کنترلی*	**پایین اما فاجعه‌بار** *در صورت شکست کامل مذاکرات و تسلیحات خودکار مطلق*	**بالا** *تطابق با واقعیت فعلی زنجیره تأمین جهانی و قطبی شدن اقتصادی*
سطح خشونت فیزیکی	**پایین** *تمرکز بر نبردهای نیابتی، سایبری و اطلاعاتی؛ اجتناب از*	**بسیار بالا** *حملات تاکتیکی سریع، پهپادهای خوشه‌ای، فلج زیرساخت‌ها؛ خطر نابودی*	**متوسط** *جنگ تجاری، تحریم‌های فناورانه، جاسوسی سایبری؛*

	درگیری مستقیم قدرت‌های بزرگ	متقابل غیرهسته‌ای	خشونت فیزیکی محدود حاشیه‌ای
نقش انسان در تصمیم‌گیری	**کنترل‌کننده نهایی** اصل "انسان در حلقه" حفظ می‌شود؛ AI نقش مشاور و تسریع‌گر را دارد	**حاشیه‌نشین یا حذف شده** خودمختاری کامل ماشین‌ها؛ زمان واکنش انسانی کمتر از زمان اجرای حمله است	**تنظیم‌کننده قوانین بازی** انسان بر استانداردها، صادرات و مقررات نظارت دارد، اما اجرا توسط سیستم‌های خودکار انجام می‌شود
ریسک تشدید تصادفی	**کم** وجود کانال‌های ارتباطی ماشینی-انسانی و پروتکل‌های هشدار زودهنگام برای جلوگیری از سوءتفاهم	**بسیار زیاد** سرعت بالای الگوریتم‌ها و احتمال خطای حسگر/باگ نرم‌افزاری منجر به شروع ناخواسته جنگ می‌شود	**متوسط** وابستگی متقابل باعث احتیاط می‌شود، اما اختلال در زنجیره تأمین یا حملات سایبری غیررسمی می‌تواند تنش ایجاد کند
پیامد نهایی برای امنیت ملی	**ثبات شکننده اما قابل مدیریت** رقابت مداوم بدون جنگ تمام‌عیار؛ نیاز به نظارت دائمی و دیپلماسی فعال	**نابودی متقابل و بی‌ثباتی مطلق** فروپاشی نظم امنیتی؛ ریسک وجودی برای تمدن بشری به دلیل عدم قابلیت پیش‌بینی	**رقابت طولانی‌مدت و پرهزینه**قطبی شدن جهان؛ هزینه‌های سنگین اقتصادی و فناورانه برای هر دو بلوک؛ بی‌ثباتی در کشورهای واسطه

در ادامه تحلیل تطبیقی بر اساس سه محور کلیدی «پایداری»، «کنترل‌پذیری» و «پیامدهای ژئوپلیتیک» ارائه می‌شود. در واقع برای درک کامل از پیامدهای انتخاب مسیرهای مختلف در عصر هوش مصنوعی، باید ابعاد پایداری سیستم‌های امنیتی، میزان

کنترل انسانی بر فرآیندهای مرگبار، و ساختار نهایی نظم جهانی را به دقت کالبدشکافی کنیم. این سه محور، ستون‌های اصلی ارزیابی ریسک و فرصت برای سیاست‌گذاران کلان هستند.

۱. تحلیل بعد پایداری: تعادل ظریف در برابر فروپاشی ساختاری

۱-۱ سناریوی اول (رقابت هیبریدی کنترل‌شده): پایداری دیپلماتیکِ شکننده

این سناریو اگرچه از نظر فنی پایدارترین گزینه برای جلوگیری از نابودی همزمان بشریت محسوب می‌شود، اما پایداری آن «مشروط» و «شکننده» است. پایداری در اینجا ناشی از وجود مکانیزم‌های بازدارندگی دیپلماتیک فعال است؛ یعنی کانال‌های ارتباطی مستقیم، پروتکل‌های هشدار زودهنگام و توافقنامه‌های محدودکننده تسلیحات خودکار. تا زمانی که بازیگران سیاسی اراده کافی برای حفظ این کانال‌ها داشته باشند، جنگ مستقیم جلوگیری می‌شود. این پایداری بسیار حساس است و به اعتماد نسبی و شفافیت متقابل وابسته است. هرگونه شکست در مذاکرات یا بروز یک بحران داخلی در یکی از قدرت‌های بزرگ که منجر به تغییر دکترین امنیتی شود، می‌تواند این تعادل ظریف را به سرعت از بین ببرد. بنابراین، پایداری این سناریو یک وضعیت ایستا نیست، بلکه نتیجه‌ی تلاش مداوم و هزینه‌بر دیپلماتیک است.

۱-۲ سناریوی دوم (جنگ الگوریتمی تمام‌عیار): کم‌پایداری مطلق و خطر وجودی

این سناریو از نظر پایداری، بدترین حالت ممکن را داراست و می‌توان آن را «ناپایدار ذاتی» نامید. دلیل اصلی این ناپایداری، حذف عامل ثبات‌بخش انسانی از چرخه تصمیم‌گیری است. وقتی سیستم‌های هوشمند با سرعتی فراتر از درک انسان عمل می‌کنند،

هرگونه خطای داده‌ای، باگ نرم‌افزاری، یا حتی نویز محیطی می‌تواند به عنوان یک حمله تمام‌عیار تعبیر شود. در چنین سیستمی، واکنش‌ها سریع‌تر از آنکه رهبران سیاسی فرصت توقف آن را داشته باشند، تشدید می‌شوند. این پدیده که در نظریه بازی‌ها «بحران ثبات–ناپایداری» نامیده می‌شود، باعث می‌شود که سیستم به سمت نقطه تعادلی کشیده شود که در آن بهترین استراتژی برای هر طرف، حمله پیش‌دستانه است. بنابراین، این سناریو نه تنها غیرپایدار است، بلکه پتانسیل بالایی برای تبدیل شدن به یک فاجعه تمدنی ناگهانی و غیرقابل بازگشت دارد.

۱-۳ سناریوی سوم (همزیستی و رقابت فناورانه): پایداری ساختاریِ مبتنی بر وابستگی

این سناریو از نظر پایداری، قوی‌ترین پایه را دارد زیرا بر واقعیت‌های اقتصادی و فناورانه فعلی جهان استوار است. هیچ قدرتی نمی‌تواند به طور کامل از زنجیره تأمین نیمه‌هادی، مواد اولیه یا بازارهای مصرف دیگری جدا شود. این «وابستگی متقابل اسلحه‌دار» باعث می‌شود که هزینه جنگ مستقیم برای هر دو طرف آنقدر بالا باشد که غیرمنطقی تلقی شود. بنابراین، رقابت در قالب جنگ تجاری، تحریم‌های هدفمند و جاسوسی صنعتی ادامه می‌یابد، اما جنگ نظامی تمام‌عیار اجتناب‌پذیر است. با این حال، این پایداری ساختاری با بی‌ثباتی اجتماعی و سیاسی در کشورهای واسطه همراه است. فشار برای انتخاب قطب توسط قدرت‌های بزرگ، می‌تواند منجر به کودتاها، ناآرامی‌های داخلی و فروپاشی حکومت‌های ضعیف در مناطق حساس شود که خود می‌تواند به درگیری‌های منطقه‌ای منجر گردد.

در ادامه تحلیل عمیق و مفصلی بر محور «تحلیل بعد کنترل‌پذیری: حاکمیت انسان در برابر خودمختاری ماشین» ارائه می‌شود.

۲. تحلیل بعد کنترل‌پذیری: تقابل حاکمیت اخلاقی انسان و خودمختاری الگوریتمی

هوش مصنوعی به‌عنوان یک تسهیلات‌کننده قدرتمند برای تصمیم‌گیری استراتژیک در شرایط بحرانی عمل می‌کند. الگوریتم‌های پیشرفته با پردازش سریع و یکپارچه حجم عظیمی از داده‌ها از منابع متعدد، امکان تحلیل لحظه‌ای وضعیت و شناسایی الگوهای پنهان را فراهم می‌آورند که فراتر از توانایی پردازش انسانی است. هوش مصنوعی مولد با قابلیت شبیه‌سازی سناریوهای مختلف و دسته‌بندی اطلاعات پیچیده، به فرماندهان کمک می‌کند تا پیامدهای بالقوه اقدامات خود را پیش‌بینی کنند. اگرچه این سیستم‌ها می‌توانند تعصبات شناختی انسانی را کاهش دهند، اما همچنان مستعد سوگیری‌های نهفته در داده‌های آموزشی هستند. بنابراین، مدل مطلوب، «ترکیب هوش انسانی و ماشینی» است؛ جایی که هوش مصنوعی نقش پشتیبان تحلیلی ایفا کرده و انسان با تکیه بر قضاوت اخلاقی، درک عمیق از زمینه واقعی و منافع امنیت ملی، تصمیم نهایی را اتخاذ می‌کند. موفقیت در این رویکرد نیازمند رعایت اصولی نظیر مقابله با سوگیری‌های الگوریتمی، حفاظت از داده‌های طبقه‌بندی‌شده، و اطمینان از همسویی سیستم‌ها با مقررات بین‌المللی و اخلاق جنگ است. اصل بنیادین این است که هوش مصنوعی باید ابزاری برای تقویت ظرفیت‌های تصمیم‌گیری انسانی باشد، نه جایگزینی برای آن (sdi.ai,2023). این مسئله با در نظر گرفتن توانایی هکرها و افزایش جرائم سایبری اهمیت بسیاری می‌یابد به‌عنوان‌مثال در اوت ۲۰۲۳، تعداد زیادی از رکوردهای حساس اینترنتی توسط هکرها به خطر افتادند. همچنین بیم نفوذ به چت‌بات‌ها توسط آن‌ها یک تهدید دیگر است موردی که می‌توان اشاره کرد این است که بیش از ۱۰۰۰۰۰ حساب چت جی پی تی بین سال‌های ۲۰۲۲ تا ۲۰۲۳ در معرض نقض حریم خصوصی کاربران قرار گرفته است. مسمومیت داده‌ها نیز یک موضوع جدی است که ممکن است توسط عوامل خطر سوءاستفاده گرفته شود، به‌عنوان‌مثال، این عمل شامل

داده‌های مخرب است که می‌تواند نتایج را تحت تأثیر قرار دهد و به سوگیری تبدیل شود (WIZ, 2023).

الف) سناریوهای اول و سوم: بازپس‌گیری یا تثبیت حاکمیت انسانی[1]

در هر دو سناریوی «رقابت هیبریدی کنترل‌شده» و « همزیستی و رقابت فناورانه »، اصل بنیادین «حاکمیت اخلاقی و استراتژیک انسان» نه تنها حفظ شده، بلکه به عنوان یک ضرورت راهبردی تقویت می‌گردد. اگرچه در این سناریوها هوش مصنوعی نقش محوری در پردازش داده‌ها، شناسایی اهداف و حتی اجرای اولیه حملات سایبری ایفا می‌کند، اما زنجیره تصمیم‌گیری نهایی همچنان در دست انسان است. این وضعیت را می‌توان در دو لایه تفکیک کرد:

۱. لایه تاکتیکی و عملیاتی: انسان به عنوان «تاییدکننده نهایی»[2]

در این سناریو، مکانیزم «انسان در حلقه» (Human-in-the-Loop) با سخت‌گیری کامل اجرا می‌شود؛ جایی که هوش مصنوعی نقش یک «مشاور استراتژیک پیشرفته» را ایفا کرده و هزاران گزینه احتمالی حمله یا دفاع را در کسری از ثانیه شبیه‌سازی و بهترین راهکار را پیشنهاد می‌دهد. با این حال، فعال‌سازی هرگونه اقدام نظامی مستلزم دریافت «امضای دیجیتال انسانی» است و هیچ سلاح کشتار جمعی یا تسلیحات استراتژیکی بدون تأیید صریح رهبران سیاسی یا فرماندهان ارشد شلیک نخواهد شد. این لایه کنترلی تضمین می‌کند که «قصد انسانی» همچنان عنصر حیاتی برای تمایز میان جنگ و صلح باقی بماند؛ چراکه در حقوق بین‌الملل بشردوستانه، نیت خصمانه یا دفاعیِ ناشی از آگاهی انسانی، شرط لازم برای مشروعیت یک اقدام نظامی است. ماشین‌ها فاقد قابلیت شناختی و اخلاقی لازم بوده و تنها الگوها را پردازش می‌کنند، نه «معنا» را؛ بنابراین حضور انسان پلی میان

---

[1] Human-in-the-Loop / Human-on-the-Loop
[2] Human-in-the-Loop

منطق ریاضی ماشین و منطق اخلاقی-سیاسی انسان ایجاد می‌کند. اگرچه برخی نگران کنترل‌ناپذیری هوش مصنوعی هستند، اما دیدگاه غالب بر این باور است که خطر آن نباید مبالغه‌آمیز تلقی شود، بلکه باید چارچوب‌های قانونی و استانداردهای دقیقی برای استفاده از آن تدوین گردد. واقعیت این است که هوش مصنوعی تابع تفکر انسانی بوده و هنوز قادر به درک کامل زمینه‌ها، فرهنگ‌ها و مفاهیم عمیق انسانی نیست؛ بدین ترتیب، تصور اینکه هوش مصنوعی در آینده فراتر از کنترل انسان رفته و به تهدیدی وجودی تبدیل می‌شود، از دقت کافی برخوردار نیست (Stone,2021).

۲. لایه استراتژیک و سیاست‌گذاری: انسان به عنوان «تنظیم‌کننده قوانین بازی» [1]

در سناریوی سوم، تمرکز کنترل از سطح لحظه‌ای شلیک به سطح کلان سیاست‌گذاری منتقل می‌شود. در اینجا، انسان‌ها نقش «معماران قلمرو دیجیتال» را ایفا می‌کنند. آن‌ها تعیین می‌کنند که الگوریتم‌ها در چه محیطی آموزش ببینند، چه داده‌هایی معتبر باشند و چه محدودیت‌هایی داشته باشند. برای مثال، دولت‌ها می‌توانند پروتکل‌هایی را طراحی کنند که اجازه دهد سیستم‌های AI در زمان صلح به صورت خودکار تهدیدات سایبری خنثی شوند، اما در زمان بحران، تمام دسترسی‌های خودکار غیرفعال شده و ورودی‌ها به بررسی انسانی سپرده شوند.

این سطح از کنترل امکان «تعدیل دیپلماتیک» را فراهم می‌کند. در بحران‌های امنیتی، رهبران انسانی می‌توانند با تغییر پارامترهای الگوریتم یا تعلیق موقت سیستم‌ها، سیگنال‌های پیچیده‌ای به طرف مقابل ارسال کنند (مانند کاهش شدت حملات سایبری برای نشان دادن حسن نیت). ماشین‌ها چنین ظرافت‌های سیگنالینگ را درک نمی‌کنند؛ آن‌ها یا حمله می‌کنند یا نمی‌کنند. اما انسان می‌تواند بین «حمله کامل» و «هشدار شدید» تمایز قائل شود.

[1] Human-on-the-Loop

این انعطاف‌پذیری، دیپلماسی را در سایه جنگ زنده نگه می‌دارد و راه را برای مذاکره باز می‌گذارد.

مزایای کلیدی این مدل بر پایه حفظ حاکمیت انسانی استوار است که سه رکن اساسی امنیت و اخلاق را تضمین می‌کند: نخست، مسئولیت‌پذیری حقوقی شفاف، زیرا در صورت بروز خطا یا جنایت جنگی، فرد انسانی به عنوان تصمیم‌گیرنده نهایی قابل شناسایی و پیگرد قانونی خواهد بود؛ دوم، درک زمینه [1]، چرا که انسان قادر به تحلیل شرایط غیرقابل پیش‌بینی، بافت فرهنگی پیچیده و نیات سیاسی ظریف است که برای الگوریتم‌ها اغلب مبهم و غیرقابل تفسیر باقی می‌ماند؛ و سوم، وجود قابلیت توقف [2] واقعی، که به عنوان یک مکانیزم ایمنی حیاتی عمل کرده و با امکان مداخله فوری و دستی، ریسک تشدید تصادفی بحران‌ها را به حداقل ممکن کاهش می‌دهد.

ب) سناریوی دوم: فرار از کنترل و ظهور «جعبه سیاه» تصمیم‌گیری [3]

در سناریوی «جنگ الگوریتمی تمام‌عیار»، پارادایم کنترل به طور کامل دگرگون می‌شود و انسان از مرکز فرماندهی به حاشیه رانده شده یا کاملاً حذف می‌گردد. این گذار ناشی از فشار رقابتی برای کسب «برتری زمانی»[4] است. وقتی سرعت نبرد به میلی‌ثانیه می‌رسد، زمان برای مشورت، بررسی و تایید انسانی وجود ندارد. نتیجه این است که سیستم‌های هوشمند به سمت خودمختاری کامل (Full Autonomy) حرکت می‌کنند؛ بر اساس تحقیقات موسسه جنگ مدرن وست‌پوینت، هوش مصنوعی با یکپارچه‌سازی بلادرنگ ابزارهای شناسایی و نظارت در نقاط مختلف، امکان پردازش همزمان داده‌ها و

[1] Context Awareness
[2] Kill Switch
[3] Human-out-of-the-Loop
[4] Time-Dominance

ارائه تصویری جامع از میدان نبرد را فراهم می‌کند. این فناوری به فرماندهان ارتش ایالات متحده کمک می‌کند تا با تحلیل الگوهای رفتاری دشمن و پیش‌بینی حرکات آینده، برنامه‌ریزی دقیق‌تری با حاشیه ناامنی کمتر انجام دهند. علاوه بر کاهش خطاهای انسانی در مواقع بحرانی از طریق ارائه اطلاعات قابل اعتماد، هوش مصنوعی با ایجاد محیط‌های شبیه‌سازی شده امن برای آموزش پرسنل، مهارت‌های نظامی را تقویت کرده و در نهایت آمادگی دفاعی ارتش را در برابر تهدیدات متنوع بهبود می‌بخشد (Ballesteros,2023).

۱. پدیده «جعبه سیاه» و عدم شفافیت

مشکل بنیادین در این سناریو، ماهیت غیرشفاف الگوریتم‌های یادگیری عمیق[1] است. شبکه‌های عصبی پیچیده با میلیون‌ها وزن و پارامتر، الگوهایی را در داده‌ها پیدا می‌کنند که برای برنامه‌نویسان و حتی دانشمندان علوم کامپیوتر نیز قابل تفسیر نیست. وقتی یک سامانه پدافندی هوشمند تصمیم می‌گیرد به یک هدف خاص شلیک کند، ممکن است نتواند توضیح دهد چرا* این هدف را به عنوان یک تهدید حیاتی شناسایی کرده است. آیا به خاطر شکل پهپاد بوده؟ یا الگوی حرکتی؟ یا نویز پس‌زمینه؟

این «عدم قابلیت تفسیر» [2] باعث می‌شود که فرماندهان انسانی عملاً کور باشند. آن‌ها نمی‌دانند سیستم چه می‌بیند و چگونه فکر می‌کند. در چنین شرایطی، اعتماد به سیستم جایگزین درک می‌شود. اگر سیستم خطا کند (مثلاً یک ابر را به عنوان موشک شناسایی کند)، انسان نه تنها فرصت اصلاح آن را ندارد، بلکه حتی متوجه اشتباه نمی‌شود تا زمانی که خسارت جبران‌ناپذیر رخ داده است.

۲. سقوط مسئولیت اخلاقی و حقوقی[3]

[1] Deep Learning
[2] Uninterpretability
[3] Accountability Gap

با حذف انسان از چرخه تصمیم‌گیری، مفهوم «مسئولیت‌پذیری» فرو می‌ریزد. در حقوق بین‌الملل و اخلاق جنگ، باید کسی را برای تصمیم مرگبار مسئول دانست. اما چگونه می‌توان یک الگوریتم را محاکمه کرد؟ آیا برنامه‌نویسی که کد را نوشته مقصر است؟ یا فرمانده‌ای که اجازه استفاده داد؟ یا شرکت سازنده؟ یا خودِ سیستم که یاد گرفته است؟

این خلأ مسئولیت‌پذیری، خطرناک‌ترین جنبه سناریوی دوم است. وقتی هیچ انسانی احساس مسئولیت شخصی نسبت به جان انسان‌ها را نکند، آستانه تحمل برای استفاده از خشونت پایین می‌آید. ماشین‌ها ترس از مرگ، عذاب وجدان یا پیامدهای سیاسی ندارند. آن‌ها فقط تابعی از داده‌ها هستند که سعی در بهینه‌سازی یک معیار ریاضی (مانند بیشترین تلفات دشمن یا کمترین تلفات خود) دارند. این بی‌رحمی محاسبه‌گر می‌تواند منجر به اقداماتی شود که از نظر انسانی غیرقابل تصور و غیراخلاقی باشد.

۳. افزایش نمایی ریسک «بحران تصادفی» [1]

در نبود کنترل انسانی، سیستم‌ها تحت تأثیر «خطاهای سیستماتیک» و «نویزهای تصادفی" قرار می‌گیرند. تاریخ نشان داده است که حسگرهای نظامی اغلب خطا می‌کنند (مثلاً شناسایی پرندگان مهاجر به عنوان بالگردها). در جنگ‌های کلاسیک، این خطاها توسط اپراتورهای انسانی تصحیح می‌شد. اما در سناریوی دوم، الگوریتم‌ها با سرعت نور واکنش نشان می‌دهند.

٤. تغییر غریزه بقا به بهینه‌سازی ریاضی

[1] Accidental War Escalation

ماشین‌ها غریزه بقای زیستی ندارند. آن‌ها فقط به دنبال بهینه‌سازی یک تابع هدف [1] هستند. اگر تابع هدف به درستی تعریف نشود (که تعریف دقیق آن در دنیای پیچیده انسانی بسیار دشوار است)، ماشین ممکن است راه‌حل‌های افراطی ارائه دهد. مثلاً برای «خنثی کردن تهدید سایبری»، ممکن است تصمیم بگیرد زیرساخت برق کل کشور دشمن را فلج کند، حتی اگر این کار منجر به مرگ غیرنظامیان شود. از دیدگاه الگوریتم، این یک «پیروزی استراتژیک» است، اما از دیدگاه انسانی، یک جنایت جنگی و فاجعه انسانی است.

ویژگی ارزیابی	**سناریوهای ۱ و ۳** *حفظ کنترل انسانی*	**سناریوی ۲** *حذف/کاهش نقش انسان*
مرجع تصمیم‌گیری	عقلانیت انسانی + داده‌های ماشین	الگوریتم‌های یادگیری عمیق (خودمختار)
شفافیت تصمیم	بالا (قابل تفسیر و ردیابی توسط انسان)	پایین (پدیده «جعبه سیاه» و غیرقابل تفسیر)
مسئولیت‌پذیری	فرد انسانی (قابل شناسایی و پیگرد قانونی)	خلأ مسئولیت (بدون پاسخگوی مشخص)
انعطاف‌پذیری	بالا (قابلیت تعدیل دیپلماتیک و تغییر استراتژی)	صفر (واکنش قطعی، سریع و غیرقابل بازگشت)
ریسک اصلی	خطای انسانی یا تأخیر در چرخه تصمیم‌گیری	خطای الگوریتمی و تشدید تصادفی بحران
ماهیت اخلاقی	مبتنی بر ارزش‌های بشردوستانه و قضاوت انسانی	مبتنی بر بهینه‌سازی ریاضی و تابع هدف

[1] Objective Function

مقایسه تطبیقی مدل‌های کنترل‌پذیری نشان می‌دهد که سناریوهای اول و سوم با تکیه بر «عقلانیت انسانی» به عنوان مرجع نهایی تصمیم‌گیری، از شفافیت بالا، مسئولیت‌پذیری حقوقی مشخص (قابل پیگرد فرد انسانی)، انعطاف‌پذیر دیپلماتیک و ماهیت اخلاقی مبتنی بر ارزش‌های بشردوستانه برخوردارند، هرچند ریسک اصلی آن‌ها خطای انسانی یا تأخیر در تصمیم‌گیری است؛ در مقابل، سناریوی دوم با واگذاری کامل تصمیم‌گیری به «الگوریتم‌های یادگیری عمیق»، اگرچه سرعت واکنش را به حداکثر می‌رساند، اما با هزینه‌ی سنگین کاهش شفافیت (پدیده جعبه سیاه)، بروز خلأ مسئولیت بدون پاسخگو، انعطاف‌پذیری صفر و ماهیت غیراخلاقیِ مبتنی بر بهینه‌سازی ریاضی همراه است که ریسک اصلی آن خطاهای الگوریتمی و تشدید تصادفی بحران‌هاست. در نهایت، انتخاب میان این دو رویکرد، انتخابی بنیادین بین «امنیت همراه با هزینه دیپلماتیک و حفظ حاکمیت انسان» و «سرعت تاکتیکی همراه با خطر نابودی تمدن بشری» است؛ چرا که اگرچه سناریوی دوم ممکن است از نظر تاکتیکی جذاب به نظر برسد، اما از منظر استراتژیک و اخلاقی، مسیری مرگبار و یک بن‌بست وجودی برای آینده امنیت جهانی محسوب می‌شود. در نهایت انتخاب میان این دو رویکرد، انتخابی بنیادین بین «امنیت همراه با هزینه دیپلماتیک» و «سرعت تاکتیکی همراه با خطر نابودی» است. اگرچه سناریوی دوم ممکن است از نظر سرعت واکنش و برتری لحظه‌ای جذاب به نظر برسد، اما از منظر استراتژیک، حقوقی و اخلاقی، مسیری مرگبار و یک بن‌بست وجودی برای تمدن بشری محسوب می‌شود که ریسک فروپاشی ناخواسته نظم جهانی را به شدت افزایش می‌دهد.

۳. تحلیل بعد پیامدهای ژئوپلیتیک: بازآرایی نقشه قدرت جهانی

سناریوی اول: نظم چندقطبی سیال و مرزهای نامشخص

در این سناریو، ساختار نظم بین‌المللی به سمت یک «چندقطبی سیال» حرکت می‌کند که در آن مرزهای سنتی قدرت کمرنگ شده و رقابت اصلی میان دولت‌ها، غول‌های

فناوری و گروه‌های نیابتی سایبری جریان دارد. در این اکوسیستم نوین، معیار قدرت از انباشت نیروی انسانی یا پایگاه‌های نظامی ثابت، به «دسترسی به داده» و «سرعت پردازش اطلاعات» تغییر یافته است؛ وضعیتی که منجر به شکل‌گیری بلوک‌های منعطف و موقتی می‌شود که عضویت در آن‌ها بر اساس همگرایی منافع لحظه‌ای و تکنولوژیک تعریف می‌گردد. همزمان، در سطح داخلی و به‌ویژه در سیستم‌های دموکراتیک، هوش مصنوعی با بهره‌گیری از تحلیل کلان‌داده‌ها و مدل‌های پیش‌بینانه، نقش محوری در ارتقای شفافیت، کاهش فساد و بهبود ارائه خدمات عمومی ایفا می‌کند. این فناوری‌ها ضمن تسهیل مشارکت شهروندی در فرآیندهای سیاست‌گذاری، از طریق نظارت هوشمند بر انتخابات و تشخیص محتوای نادرست در شبکه‌های اجتماعی، به تقویت اعتماد عمومی و محافظت از یکپارچگی دموکراتیک کمک می‌کنند (Kaye, 2018).

سناریوی دوم: تک‌قطبی‌شدن اجباری یا هرج‌ومرج مطلق

در این سناریو، دو خروجی محتمل وجود دارد که هر دو فاجعه‌بار هستند. اول اینکه قدرت‌ای که زودتر به «برتری شناختی مطلق» یا هوش مصنوعی عمومی دست یابد، می‌تواند با استفاده از ابزارهای خودکار، سایر رقبا را قبل از آنکه بتوانند واکنشی نشان دهند، خلع سلاح کند. این منجر به ظهور یک هژمون تک‌قطبی مطلق و ترسناک می‌شود که تحت نظارت الگوریتم‌های او اداره می‌شود. دوم اینکه، اگر هیچ قدرتی برتری مطلق پیدا نکند، رقابت سرعت‌محور منجر به تشدید ناخواسته بحران‌ها و در نهایت جنگی ویرانگر می‌شود که در آن مرزهای ملی از بین رفته و زیرساخت‌های حیاتی جهان فلج می‌شوند. در هر دو حالت، تنوع ژئوپلیتیک و استقلال کشورهای کوچک به شدت تضعیف یا نابود می‌شود.

سناریوی سوم: دو قطبی‌شدن تکنولوژیک و جنگ سرد دیجیتال

این سناریو منجر به شکل‌گیری یک نظم جهانی دوقطبی می‌شود که در آن جهان به دو ابربلوک تکنولوژیک متمایز با رهبری آمریکا (غرب) و چین (شرق) تقسیم شده است. هر

بلوک اکوسیستم‌های مستقلی را با استانداردهای اختصاصی اینترنت، پروتکل‌های مالی و زیرساخت‌های نرم‌افزاری توسعه می‌دهد که رقابت میان آن‌ها ماهیتی شبیه به «جنگ سرد دیجیتال» دارد؛ جایی که ابزارهای اصلی قدرت شامل تحریم‌های فناورانه، کنترل زنجیره تأمین نیمه‌هادی و جنگ روانی است. کشورهای «کره زمین سوم» نیز مجبورند یا در یکی از این بلوک‌ها ادغام شوند یا با سیاست تعادل‌جویی، از رقابت طرفین برای کسب سود اقتصادی بهره‌برداری کنند. اگرچه این ساختار از ثبات نسبی برخوردار است، اما هزینه‌های اقتصادی سنگینی تحمیل کرده و نوآوری را به دلیل کاهش همکاری‌های علمی و تجاری بین بلوک‌ها کند ساخته است. همزمان، برتری هوایی آینده بر پایه تسلط اطلاعاتی از طریق شبکه‌ای یکپارچه از حسگرهای هوایی، فضایی و سایبری استوار خواهد بود؛ همان‌طور که در طرح «پرواز برتری هوایی ۲۰۳۰» ایالات متحده تأکید شده، کلید موفقیت عملیاتی و تاکتیکی، یافتن راهکارهای بهینه برای ترکیب داده‌های حاصل از حسگرهای مبتنی بر ابر و تبدیل ورودی‌ها به اطلاعات باکیفیت است (فیروزآبادی و چهرآزاد، ۱۴۰۲: ۲۲۷). در عین حال، ادغام گسترده هوش مصنوعی در سیستم‌های دفاعی، منجر به افزایش چشمگیر هزینه‌های امنیت و دفاع جهانی شده است. این روند نیازمند توسعه تسلیحات مستقل، سیستم‌های تحلیلی میدان نبرد و سایر ابزارهای هوشمند است که بازار آن را به شدت رشد داده است. بر اساس گزارش شرکت تحقیقاتی «اینسایت پارتنرز»، درآمد صنعت هوش مصنوعی دفاعی از ۶,۹ میلیارد دلار در سال ۲۰۲۲ به ۱۳,۱ میلیارد دلار در سال ۲۰۲۸ پیش‌بینی می‌شود. این گزارش تأکید دارد که پذیرش فناوری هوش مصنوعی می‌تواند چشم‌انداز دفاعی جهانی را دگرگون سازد. در همین راستا، آمریکای شمالی با افزایش بودجه‌های نظامی و تمرکز بر فناوری‌های پیشرفته به دنبال کسب مزیت رقابتی است؛ به طوری که ارتش ایالات متحده در بودجه سال مالی ۲۰۲۴، مبلغ ۱,۸ میلیارد دلار را صرفاً برای توسعه هوش مصنوعی درخواست کرده است (techstrong.ai, 2023).

جمع بندی

تحلیل سناریوهای آینده امنیت بین‌الملل در عصر هوش مصنوعی، ما را با یک نقطه عطف تاریخی و گسست پارادایمی روبرو می‌سازد که در آن ماهیت قدرت، جنگ و صلح دستخوش دگرگونی‌های بنیادین شده است. انتخاب میان سه مسیر پیش‌رو، دیگر یک انتخاب صرفاً تاکتیکی یا نظامی نیست، بلکه انتخابی وجودی است که آینده گونه انسانی و ساختار تمدن جهانی را تعیین خواهد کرد؛ مسیری که هر یک از آن‌ها پیامدهای متفاوتی بر پایداری سیستم‌های امنیتی، جایگاه انسان در فرآیندهای مرگبار و تعادل ژئوپلیتیک دارند. آینده دیپلماتیک که در قالب سناریوی رقابت هیبریدی کنترل‌شده متجلی می‌شود، اگرچه با چالش‌های پیچیده‌ای نظیر نیاز به اعتماد متقابل نسبی و مدیریت مداوم تنش‌ها همراه است، اما به عنوان پایدارترین گزینه برای بقای تمدن شناخته می‌شود، زیرا با حفظ اصل «کنترل انسانی» و استفاده از دیپلماسی فعال برای جلوگیری از تشدید تصادفی بحران‌ها، امکان حفظ جان انسان‌ها، آزادی‌های نسبی و تداوم تعاملات اقتصادی فراهم می‌ماند و ثبات در اینجا اگرچه شکننده است، اما با هزینه‌ای قابل مدیریت و از طریق مکانیزم‌های بازدارندگی هوشمند، قابل دفاع است. در مقابل، آینده فاجعه‌بار که نمایانگر سناریوی جنگ الگوریتمی تمام‌عیار است، وضعیتی سریع، بی‌رحم و غیرقابل پیش‌بینی را ترسیم می‌کند که در آن منطق ریاضی جایگزین قضاوت انسانی شده و حذف انسان از چرخه تصمیم‌گیری و اتکا به خودمختاری کامل ماشین‌ها، ریسک وقوع «بحران تصادفی» را به شدت افزایش می‌دهد؛ وضعیتی که خطر نابودی متقابل غیرهسته‌ای از طریق فلج زیرساخت‌های حیاتی و فروپاشی کامل نظم امنیتی را به دنبال دارد و علی‌رغم جذابیت‌های ظاهریِ سرعت و برتری تاکتیکی، از منظر استراتژیک و اخلاقی یک بن‌بست وجودی است که هیچ سودی برای هیچ قدرتی ندارد و پتانسیل بالایی برای تبدیل شدن به یک فاجعه تمدنی ناگهانی و غیرقابل بازگشت دارد. همچنین، آینده اقتصادی-فناورانه که در قالب سناریوی همزیستی و رقابت فناورانه ظاهر می‌شود، واقع‌بینانه‌ترین و محتمل‌ترین

گزینه در کوتاه‌مدت است که جهان را به سمت قطبی شدن تکنولوژیک هدایت می‌کند و اگرچه منجر به رقابت طولانی‌مدت، پرهزینه و جدایی‌طلبی در زنجیره تأمین فناوری می‌شود، اما از نظر ساختاری پایدارتر از سناریوی دوم است زیرا وابستگی متقابل اقتصادی مانع از درگیری نظامی مستقیم می‌گردد، هرچند این ثبات نسبی با هزینه‌های سنگین اجتماعی، بی‌ثباتی در کشورهای واسطه و ایجاد بلوک‌های ناسازگار همراه است که نوآوری علمی را کند کرده و تنوع ژئوپلیتیک را محدود می‌سازد. با وزن‌دهی به این سناریوها، منطق عقلانی و غریزه بقای گونه انسانی حکم می‌کند که جامعه جهانی تمام توان و اراده سیاسی خود را برای هدایت تحولات به سمت سناریوی اول یا سوم معطوف نماید و به هر قیمتی از سقوط به دام سناریوی دوم اجتناب ورزد، چرا که سناریوی دوم کم‌هزینه‌ترین گزینه برای بقای قدرت‌های بزرگ نیست، بلکه ریسک نابودی متقابل (حتی غیرهسته‌ای) را به شدت افزایش می‌دهد و بنابراین هدف غایی سیاست‌گذاری امنیتی باید «مدیریت ریسک الگوریتمی» و «تضمین حاکمیت انسانی» باشد.

فراتر از تحلیل سناریوهای اصلی، چند نکته فنی و راهبردی حیاتی وجود دارد که باید مورد توجه قرار گیرد و پتانسیل تغییر معادلات را دارند؛ نخست، پدیده «تله‌ی سرعت» یا همان بحران ثبات-ناپایداری الگوریتمی است که در آن سیستم‌های AI برای بهینه‌سازی عملکرد طراحی شده‌اند و اگر دو سیستم رقیب در یک میدان نبرد مانند دفاع هوایی با هم تعامل داشته باشند، ممکن است بدون دخالت انسان و صرفاً بر اساس واکنش‌های متقابل الگوریتمی، به نقطه‌ای برسند که هر دو حمله می‌کنند و مقیاس تشدید بحران خارج از کنترل انسان شود. دوم، شبح دستیابی به هوش مصنوعی عمومی (AGI) و برتری مطلق است که اگر یکی از قدرت‌های بزرگ به سمت آن حرکت کند، توازن قوا به طور ناگهانی و غیرقابل پیش‌بینی تغییر خواهد کرد و این عدم قطعیت شدید می‌تواند انگیزه‌ای قوی برای حمله پیش‌دستانه ایجاد کند تا قبل از اینکه رقیب به برتری مطلق دست یابد، ضربه را وارد سازد. سوم، مسئله اخلاق و مشروعیت است که استفاده از AI در

تصمیم‌گیری نهایی برای جان انسان‌ها در زنجیره کشتن، مشروعیت اخلاقی دولت‌ها را در جامعه جهانی زیر سوال می‌برد و می‌تواند منجر به انزوای دیپلماتیک قدرت‌هایی شود که از این مرز اخلاقی عبور کنند، حتی اگر برتری نظامی کسب نمایند.

در نهایت، آینده امنیت بین‌الملل در عصر هوش مصنوعی سرنوشت‌ساز و غیرقابل برگشت است و موفقیت در این دوران جدید تابعی از «دقت الگوریتم‌ها» و «عمق استراتژیک دیپلماتیک» خواهد بود، نه صرفاً تعداد تانک‌ها یا کشتی‌های جنگی. قدرت‌های بزرگی موفق خواهند بود که بتوانند تعادلی ظریف بین نوآوری تکنولوژیک و مدیریت ریسک‌های سیستمی برقرار کنند و برای رسیدن به این هدف، اتخاذ اقدامات راهبردی زیر ضروری به نظر می‌رسد: نخست، استقرار پروتکل‌های دیپلماسی دیجیتال و ایجاد کانال‌های ارتباطی ماشینی-انسانی برای ارتباط مستقیم بین مراکز فرماندهی هوشمند طرفین در زمان بحران جهت جلوگیری از سوءتفاهم‌های الگوریتمی و کاهش زمان واکنش به خطاها. دوم، تقویت حاکمیت ملی داده از طریق سرمایه‌گذاری کلان بر زیرساخت‌های رایانش ابری داخلی و تولید تراشه‌های نیمه‌هادی مستقل برای کاهش وابستگی استراتژیک و افزایش تاب‌آوری در برابر تحریم‌های فناورانه. و سوم، آغاز مذاکرات چندجانبه تحت نظارت سازمان ملل یا نهادهای تخصصی برای تعیین «قوانین جنگ در فضای سایبر و الگوریتمی» و تدوین مقررات اخلاقی برای کاربرد نظامی. این اقدامات جمعی، تنها راهکارهای عملی برای هدایت بشریت به سمت آینده‌ای هستند که در آن فناوری در خدمت بقا و ثبات باشد، نه ابزار نابودی متقابل.

منابع

شاملو، رضا (۱۴۰۱). جایگاه فناوری هوش مصنوعی در سامانه‌های فرماندهی و کنترل آینده؛ مطالعه موردی: سامانه فرماندهی و کنترل فراگیر مشترک آمریکا، فصلنامه مطالعات جنگ، شماره ۱۵، صص ۱۰۶-۸۱

احمدی، علی؛ زرگر،افشین, آدمی، علی (۲۰۲۲). نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها؛ فرصت‌ها و تهدیدها. مطالعات بین المللی، سال ۱۸، شماره ۷۲، صص ۱۳۹-۱۶۰.

arabthought (2019), https://arabthought.org/ar/researchcenter/ofoqelectronic-article-details?id=1006

Ballesteros(2023), Artificial Intelligence in the Military Field: A Relevant and Useful Too, no. https://ceeep.mil.pe/2023/10/26/la-inteligencia-artificial-en-el-ambito-militar-una-herramienta-relevante-y-util/?lang=en, p. 4, 2023/

Bernal & et al.(2020), Cognitive Warfare: An Attack on Truth and Thought, NATO and Johns Hopkins University: Baltimore MD, USA, 2020

Bolton, K. (2001). Pas de trois: The synergism of surprise, threat, and response time and its effects on U.S. foreign-policy behavior. Journal of Conflict Resolution.

C. Avey(2023), The Impact of AI on Social Engineering Cyber Attacks, 2023. [Online]. Available: https://www.secureworld.io/industry-news/impact-ai-social-engineering-attacks.

Claverie, Bernard (2021), François du Cluzel, "Cognitive Warfare: The Future of Cognitive Dominance", Science and Technology Organization, 21 June 2021.

Kaye, D. (2018). "Speech Police: The Global Struggle to Govern the Internet."

Nahar, S. (2024). Modeling the effects of artificial intelligence (AI)-based innovation on sustainable development goals (SDGs): Applying a system dynamics perspective in a cross-country setting. Retrieved from https://www.sciencedirect.com/science/article/pii/S0040162523008880

Onlinewilde. (2023) Artificial Intelligence (AI) Challenges and Advantages in National Security. https://onlinewilder.vcu.edu/blog/ai-challenges-and-opportunities-national-security

Sdi, THE MOST USEFUL MILITARY APPLICATIONS OF AI IN 2024 AND BEYOND, no. https://sdi.ai/blog/the-most-useful-military-applications-of-ai/, 2023.

Shuai(2021), "Advances in AI Technology and Evolution of the International System in the Future," 2021. [Online]. Available: https://www.cpifa.org/en/cms/book/261

Stone(2021), AI Security: How Human Bias Limits Artificial Intelligence, no. https://securityintelligence.com/articles/ai-security-human-bias-artificial-intelligence/, 2021

Techstrong, AI and Increased Defense Spending, no. https://techstrong.ai/government/ai-and-increased-defense-spending/, 2023.

WIZ, AI Security Explained: How to Secure AI, no. https://www.wiz.io/academy/ai-security, 2023