Defense Policy

The impact of artificial intelligence technology on deterrence

Mohammad younes Bahadori [1] | Seyed Mohammad Tabatabai [2]

1. Master's degree in International Relations from Allameh Tabatabaei University, Tehran, Iran.
Email: younesbahadori76@gmail.com
2 Professor of International Relations Department, Allameh Tabatabaei University, Tehran, Iran.

Volume info

Vol. 34
Series: 133
Autumn 2026
P.P: 29-60

Article Type

Research Paper

Article History

Received:
2025-10-07
Revised:
2025-12-09
Accepted:
2026-01-05
Published:
2026-02-20

ISSN – E-ISSN

ISSN: 2008-6121
E-ISSN: 2645-5218

Abstract

The present study addresses the issue that the emergence of artificial intelligence is creating a paradigmatic transformation in security studies and challenging the classical concepts of deterrence. This article seeks to answer the main question of how algorithmic deterrence has transformed the security doctrine of great powers? To this end, the study proceeds with the hypothesis that the emergence of algorithmic deterrence, by changing the logic of deterrence from "retaliation" to "prediction", has fundamentally transformed the security doctrine of great powers and created a new competition over information superiority and speed of decision-making. The research method used is descriptive-analytical using scenario writing and a comparative approach. The findings show that each of the powers has adapted to this transformation in a unique way: the United States has moved towards "integrated deterrence", China towards "comprehensive national security" and "smart deterrence", and Russia towards "cognitive warfare". This algorithmic competition has led to strategic instability, reduced human response time, and increased ambiguity in attack attribution.

Keywords: Artificial intelligence security doctrine algorithmic deterrence great powers strategic stability.

Cite this Article: Bahadori, M.Y., & Tabatabai, S.M. (2026). The impact of artificial intelligence technology on deterrence. Scientific Journal of Defense Policy, 34(133), 29-60.

doi : 10.47176/dpj.2026.1869

Publisher: Imam Hossein University.

تاثیر فن آوری هوش مصنوعی بر قدرت بازدارندگی

محمدیونس بهادری [۱] | سیدمحمد طباطبایی [۲]

۱. دانش آموخته کارشناسی ارشد روابط بین الملل دانشگاه علامه طباطبایی، تهران، ایران.
Email: younesbahadori76@gmail.com
۲. استاد گروه روابط بین الملل دانشگاه علامه طباطبایی، تهران، ایران.

چکیده

پژوهش حاضر به این موضوع می‌پردازد که ظهور هوش مصنوعی در حال ایجاد یک دگردیسی پارادایمیک در مطالعات امنیتی است و مفاهیم کلاسیک بازدارندگی را به چالش می‌کشد. این مقاله در پی پاسخ به این سوال اصلی است که بازدارندگی الگوریتمی چگونه موجب تحول در دکترین امنیتی قدرت‌های بزرگ شده است؟ بدین منظور، پژوهش با این فرضیه پیش می‌رود که ظهور بازدارندگی الگوریتمی با تغییر منطق بازدارندگی از «تلافی» به «پیش‌بینی»، باعث تحول بنیادین در دکترین امنیتی قدرت‌های بزرگ شده و رقابتی نوین بر سر برتری اطلاعاتی و سرعت تصمیم‌گیری ایجاد کرده است. روش تحقیق به کار گرفته شده، توصیفی-تحلیلی با بهره‌گیری از سناریونویسی و رویکردی تطبیقی است. یافته‌ها نشان می‌دهد که هر یک از قدرت‌ها به شیوه‌ای منحصربه‌فرد با این تحول انطباق یافته‌اند: ایالات متحده به سمت «بازدارندگی یکپارچه»، چین به سوی «امنیت جامع ملی» و «بازدارندگی هوشمند»، و روسیه به سمت «جنگ شناختی» حرکت کرده‌اند. این رقابت الگوریتمی به بی‌ثباتی راهبردی، کاهش زمان واکنش انسانی و افزایش ابهام در انتساب حملات منجر شده است.

کلیدواژه‌ها: هوش مصنوعی، دکترین امنیتی، بازدارندگی الگوریتمی، قدرت‌های بزرگ، ثبات راهبردی.

استناد: بهادری، محمدیونس، و طباطبایی ، سیدمحمد. (۱۴۰۴). تاثیر فن آوری هوش مصنوعی بر قدرت بازدارندگی. فصلنامه سیاست دفاعی، ۳۴(۱۳۳)، ۲۹- ۶۰. doi : 10.47176/dpj.2026.1869

ناشر: دانشگاه جام امام حسین(ع).

مقدمه

جهان در آغاز قرن بیست‌ویکم، از یک منظر کلان، شاهد یک دگردیسی پارادایمیک در حوزه‌های علمی و فناورانه است که در کانون آن، ظهور و توسعه شتابان هوش مصنوعی قرار دارد. این پدیده، در حال بازنویسی قواعد بازی در بسیاری از حوزه‌ها، از اقتصاد ، جامعه و شاید مهم‌تر از همه، حوزه امنیت بین‌الملل است. اگر در دوران کلاسیک، نظریه و عمل بازدارندگی بر پایه مفاهیم مادی، تقابل سخت و معادله هسته‌ای استوار بود، امروز این فرضیات بنیادین در حال فروپاشی هستند. این دگرگونی به عنوان یک مسئله کلیدی در مطالعات استراتژیک مطرح است.ورود هوش مصنوعی به حوزه نظامی و امنیتی، دکترین امنیتی قدرت‌های بزرگ را به شکلی بنیادین متحول ساخته است. این فناوری، قابلیت‌های بی‌سابقه‌ای را در حوزه نظامی ایجاد کرده است که مفاهیم سنتی بازدارندگی را به چالش می‌کشد. برای مثال، هوش مصنوعی با ارائه سرعت بی‌نظیر در تحلیل داده‌ها و تصمیم‌گیری‌های خودمختار، زمان لازم برای واکنش انسانی را از بین می‌برد. این امر، خطرات یک درگیری ناخواسته را افزایش داده و دکترین‌های مبتنی بر هشدار اولیه و دیپلماسی را ناکارآمد می‌سازد. از سوی دیگر، هوش مصنوعی با افزایش ابهام در تشخیص و احراز هویت عاملان حملات در جنگ‌های هیبریدی و سایبری، کارکرد بازدارندگی مبتنی بر تلافی را به شدت دشوار می‌کند. این پدیده، مرز میان جنگ و صلح را محو کرده و تشخیص یک اقدام خصمانه را پیچیده‌تر می‌سازد.

مسئله بنیادین این پژوهش، مواجهه نظریه بازدارندگی با یک «پارادوکس امنیتی» در عصر هوش مصنوعی است. نظریه کلاسیک بازدارندگی بر مفروضاتی همچون «عقلانیت بازیگران»، «شفافیت در سیگنال‌دهی» و «زمان کافی برای تصمیم‌گیری» استوار است. اما ورود هوش مصنوعی به معادلات امنیتی، دقیقاً همین ستون‌های اصلی را متزلزل کرده است. مسئله اصلی اینجاست که ویژگی‌های ذاتی هوش مصنوعی نظیر سرعت فراتر از شناخت انسانی، ابهام در انتساب حملات و ماهیت «جعبه سیاه» الگوریتم‌ها منطق سنتی «ثبات استراتژیک» را ناکارآمد ساخته‌اند. بنابراین، شکاف اصلی که این پژوهش به دنبال پر کردن آن است، ناتوانی دکترین‌های امنیتی موجود در تبیین وضعیت گذار از «بازدارندگی انسان‌محور» به «بازدارندگی الگوریتمی» است. در حالی که قدرت‌های بزرگ (آمریکا، چین و روسیه) به سرعت در حال ادغام هوش مصنوعی در

زیرساخت‌های نظامی خود هستند، هنوز مشخص نیست که این فناوری چگونه مفهوم «تلافی» را به «پیش‌بینی» تغییر داده و چگونه هر یک از این قدرت‌ها با توجه به فرهنگ استراتژیک متفاوت خود، این تناقض میان «سرعت تکنولوژی» و «کندی دیپلماسی» را در دکترین امنیتی خود حل‌وفصل کرده‌اند. به بیان دقیق‌تر، مسئله این پژوهش پاسخ به این پرسش است که: در شرایطی که هوش مصنوعی مرز میان جنگ و صلح را محو کرده و امکان بازدارندگی از طریق مجازات را دشوار ساخته است، دکترین امنیتی قدرت‌های بزرگ چه تحولی یافته است و این «بازدارندگی الگوریتمی» چگونه بر ثبات راهبردی در نظام بین‌الملل اثر می‌گذارد؟ عدم درک صحیح این تحول، نه تنها باعث فقر ادبیات نظری می‌شود، بلکه در صحنه عمل نیز می‌تواند ریسک درگیری‌های ناخواسته ناشی از خطای محاسباتی را به شدت افزایش دهد.

پیشینه پژوهش

محمدرضا مجیدی و رحیم بایزیدی (۱۴۰۳) در مقاله ای «هوش مصنوعی و تحول پارادایمیک در نظریه و عمل روابط بین‌الملل» این مقاله با استفاده از نظریه انقلاب‌های علمی توماس کوهن، استدلال می‌کند که هوش مصنوعی پتانسیل ایجاد چهارمین تحول پارادایمیک در رشته روابط بین‌الملل را دارد. نویسندگان معتقدند که هوش مصنوعی با توانمندسازی بازیگران غیردولتی مانند شرکت‌های بزرگ، باعث فرسایش هرچه بیشتر حاکمیت دولت‌ها می‌شود. این تحول با نظریه نئولیبرالیسم که بر نقش بازیگران غیردولتی تأکید دارد، انطباق بیشتری داشته و در رقابت با رئالیسم قرار می‌گیرد. این چارچوب نظری، بستری برای درک کاهش انحصار دولت‌ها در حوزه امنیت فراهم می‌کند.

سید عبدالقیوم سجادی (۱۴۰۴) در مقاله ای «هوش مصنوعی و تحول ماهیت امنیت بین‌الملل» سجادی با تکیه بر رویکرد سازه‌انگاری، استدلال می‌کند که هوش مصنوعی دگرگونی گسترده‌ای در مفهوم، ابعاد و مرجع امنیت بین‌الملل ایجاد کرده است. این تحول منجر به جایگزینی امنیت هویتی و داده‌محور به جای امنیت سنتی دولتی، برجسته شدن امنیت فردی و غلبه امنیت سایبری بر امنیت فیزیکی شده است. این مقاله نشان می‌دهد که مرزهای امنیت ملی، بین‌المللی و جهانی با توجه به نفوذ هوش مصنوعی، کم‌رنگ‌تر شده و یکپارچگی مفهومی امنیت را به چالش کشیده است.

کارل مولر (۲۰۲۱) در مقاله ای «اهمیت پایدار بازدارندگی متعارف» مولر در این مقاله بازدارندگی متعارف را در مقابل بازدارندگی هسته‌ای تحلیل می کند و معتقد است که اثربخشی آن به ادراکات مهاجم بستگی دارد و نه لزوماً به توان نظامی صرف. او چهار رویکرد را برای بازدارندگی متعارف برمی‌شمارد: شکست در میدان نبرد، مقاومت تنبیهی، تلافی راهبردی و شکست راهبردی. به گفته او، بازدارندگی زمانی موفق است که تهدیدات به شکل معتبر و واضحی به مهاجم منتقل شوند و برای او جنگ بدتر از هر گزینه دیگری به نظر برسد. این مقاله بر لزوم درک این نکته تأکید دارد که با وجود پیشرفت‌های فناوری، بازدارندگی متعارف همچنان نقشی حیاتی در دکترین امنیتی قدرت‌ها دارد.

اریک اشمیت (۲۰۲۲) در نوشتاری تحلیلی «هوش مصنوعی، رقابت قدرت‌های بزرگ و امنیت ملی» اشمیت توضیح می‌دهد که هوش مصنوعی با افزایش سرعت و پیچیدگی تصمیم‌گیری‌ها، روابط امنیتی میان رقبا را غیرقابل پیش‌بینی می کند. او هشدار می‌دهد که این فناوری می تواند به تقویت توانمندی‌های سایبری و هسته‌ای منجر شود و مدیریت درگیری‌ها را دشوارتر سازد. از دیدگاه او، با ظهور پلتفرم‌های شبکه‌ای جهانی که ریشه در کشورهای رقیب دارند، جوامع آزاد و دموکراتیک آسیب‌پذیرتر خواهند شد. این مقاله، هوش مصنوعی را به عنوان یک عامل کلیدی در رقابت برای رهبری جهانی مطرح می کند.

صدیقه آذین، مهدی هدایتی و احمد جانسیز (۱۴۰۳) در مقاله ای «هوش مصنوعی و ثبات استراتژیک؛ آموزه‌ای ادراکی در زمینه توسعه ابعاد نظامی هوش مصنوعی در کشورهای آمریکا و روسیه» این مقاله با رویکرد سازه‌انگاری، به تحلیل گفتمان‌های رسمی آمریکا و روسیه می‌پردازد. یافته‌ها نشان می‌دهد که هر دو کشور، هوش مصنوعی را به عنوان یک تهدید نظامی از سوی دیگری درک می کنند که منجر به ایجاد یک «چرخه رقابتی از برداشتهای نادرست» شده است. نویسندگان تأکید می کنند که تأثیر هوش مصنوعی بر ثبات استراتژیک، نه تنها به قابلیت‌های فنی آن، بلکه به باورها و ادراکات سیاست‌گذاران درباره اهداف یکدیگر بستگی دارد. این پویایی در فضای بی‌اعتمادی پس از بحران اوکراین تشدید شده است.

علی احمدی، افشین زرگر و علی آدمی (۱۴۰۱) نیز در مقاله ای «نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها: فرصت و تهدیدها» این مقاله به بررسی تأثیرات هوش مصنوعی

و ســایر فناوری‌های نوظهور (مانند چاپ ســه‌بعدی و فناوری فضــایی) بر امنیت و قدرت ملی می‌پردازد. نویسندگان معتقدند که هوش مصنوعی قابلیت‌هایی چون جعل عمیق و فرماندهی جامع نظامی را فراهم می‌کند که تهدیدات امنیتی جدیدی در فضای سایبری و اطلاعاتی ایجاد می‌کنند. این مقاله با تأکید بر اینکه فناوری‌ها فی‌نفسه مضر نیستند، نتیجه می‌گیرد که مدیریت ناصحیح آنها می‌تواند به تضعیف قدرت و امنیت دولت‌ها منجر شود.

محمد ساناالله خان، فرحت اصغر رانا و زهرا عرفان (۲۰۲۵) در پژوهشی با عنوان «جنگ هیبریدی در عصر دیجیتال: قدرت سایبری، هوش مصنوعی و آینده امنیت جهانی» این مقاله، مفهوم «جنگ هیبریدی الگوریتمی» را معرفی می‌کند و نشان می‌دهد که هوش مصنوعی چگونه به عنوان یک «نیروی چندبرابرساز»، حملات سایبری، انتشار اطلاعات نادرست و حملات جنبشی را بهینه‌سازی می‌کند. نویسندگان استدلال می‌کنند که این ترکیب نامتقارن، باعث تشدید ابهام در احراز هویت حملات می‌شود و استراتژی‌های بازدارندگی سنتی مبتنی بر تلافی را ناکارآمد می‌سازد. مقاله در نهایت بر لزوم یک تغییر پارادایم به سمت «انعطاف‌پذیری سراسری جامعه» برای مقابله با این تهدید تأکید دارد.

شن یو (۲۰۲۴) در مقاله ای با عنوان «انقلاب هوش مصنوعی در نظریه بازدارندگی: ۱۰ مفهوم پیشگامانه که امنیت جهانی را متحول می‌کنند» این مقاله به صورت خاص به ۱۰ مفهوم نوآورانه بازدارندگی می‌پردازد که با کاربرد هوش مصنوعی در مطالعات استراتژیک توسعه یافته‌اند. نویسنده به مفاهیمی مانند «بازدارندگی از طریق آشوب» که از غیرقابل پیش‌بینی بودن بهره می‌برد، و «بازدارندگی موبیوس»[1] که مرز میان تهاجم و دفاع را محو می‌کند، اشاره می‌کند. هدف این مفاهیم، فراتر رفتن از بازدارندگی سنتی و ایجاد مکانیزم‌های پیچیده‌تر و انطباق‌پذیرتر برای پیشگیری از درگیری است. این مقاله چشم‌اندازی نظری از آینده بازدارندگی در عصر هوش مصنوعی ارائه می‌دهد.

پاول دوچینه و پیتر پیجرز (۲۰۲۱) در کتابی با عنوان «عنصر مفقود در نظریه بازدارندگی: چارچوب حقوقی» دوچینه و پیجرز با تمرکز بر حملات سایبری به عنوان یک تهدید الگوریتمی، استدلال می‌کنند که قدرت بازدارندگی یک کشور از سه عنصر ظرفیت‌ها، مفاهیم و اراده تشکیل

۱ استعاره ای برگرفته از نوار موبیوس در هندسه است که سطحی یک رویه و بدون مرز مشخص بین درون و بیرون دارد.

شـــده اســـت. در دولت‌های دموکراتیک، چارچوب حقوقی به عنوان یک جزء حیاتی در عنصـــر «مفاهیم» عمل می‌کند. بدون وجود یک مبنای قانونی برای اقدامات تلافی‌جویانه، تهدیدات نظامی در فضـــای ســـایبری بی‌اعتبار و ناکارآمد خواهند بود. این مقاله نشـــان می‌دهد که اعتبار بازدارندگی الگوریتمی نیازمند قوانین واضحی برای احراز هویت، مسئولیت و اختیارات است.

این پژوهش با یک رویکرد متفاوت و نوآورانه، به دنبال پر کردن شکافی است که در ادبیات نظری موجود به چشـــم می‌خورد. در حالی که پژوهش‌های پیشـــین عمدتاً به بررســـی تأثیر هوش مصـــنوعی بر ابعاد نظامی، ژئوپلیتیک و یا تحلیل گفتمان قدرت‌ها پرداخته‌اند، کمتر پژوهشـــی به صورت جامع و نظام‌مند به بررسی چگونگی تحول کلّی دکترین امنیتی قدرت‌های بزرگ در نتیجه ظهور بازدارندگی الگوریتمی پرداخته است. اغلب مطالعات پیشین، به صـورت جزئی و مجزا، بر یک بخش خاص از این پدیده تمرکز دارند؛ برای مثال، برخی به تأثیر هوش مصـــنوعی بر ثبات اســـتراتژیک می‌پردازند، در حالی که برخی دیگر بر ابعاد حقوقی یا نظامی آن تمرکز می‌کنند. اما نوآوری این پژوهش در این اســـت که با ایجاد یک پیوند تحلیلی میان این ابعاد مختلف، نشـــان می‌دهد که هوش مصـــنوعی نه فقط یک ابزار جدید نظامی اســـت، بلکه یک عامل تغییر پارادایم اســت که باعث تغییر درک سـیاسـت‌گذاران از تهدید، منافع و ابزارهای قدرت شـده اسـت. این پژوهش با ارائه یک چارچوب مفهومی جدید، به دنبال پاســـخ به این پرســـش کلیدی اســـت که چگونه بازدارندگی الگوریتمی به عنوان یک مفهوم جامع و نوین، به جایگزینی برای دکترین‌های امنیتی سـنتی تبدیل شـده اسـت. از این رو، این پژوهش با ارائه یک تصـویر کل‌نگر، به غنی‌سـازی ادبیات پژوهشی در حوزه مطالعات استراتژیک کمک شایانی خواهد کرد.

چارچوب مفهومی

نظریه بازدارندگی، به عنوان یک مفهوم اصـلی در مطالعات اسـتراتژیک، بر این اصـل اسـتوار است که می‌توان یک بازیگر را با تهدید به تحمیل هزینه، از انجام اقدامی ناخواسته بازداشت. این نظریه از زمان جنگ جهانی دوم و با ظهور سـلاح‌های هسته‌ای به شـکلی منسـجم درآمده و اساس دکترین امنیتی قدرت‌های بزرگ را تشـــکیل داده اســـت (قاســـمی.۱۳۹۱ :۹۱). در واقع نظریه بازدارندگی، عبارت اســـت از کوشـــش یک بازیگر برای اعمال نفوذ در دیگری تا او را از انجام

یک اقدام مشـــخص بازدارد. این فرآیند در بنیاد خود بر جلوگیری از انجام کار از طریق ایجاد «ترس» اســتوار اســت. این ترس ناشــی از تهدید به تحمیل هزینه‌هایی اســت که برای طرف مقابل غیرقابل قبول باشد، به طوری که تصمیم‌گیرندگان به این نتیجه برسند که منافع مورد نظرشان ارزش پرداخت چنین هزینه‌ای را ندارد .

یک سیستم بازدارندگی پایدار بر سه پایه اصلی استوار است:

۱- قابلیت: به معنای برخورداری از توان کافی (مانند توان هسته‌ای) برای مقابله با دشمن .

۲-اطلاعات: عبارت اســت از دســترســی به حداکثر اطلاعات، اخبار و ارقام نسـبت به موقعیت خود و طرف مقابل.

۳- اعتبار و اراده: صـرف داشـتن توانایی نظامی کافی نیسـت؛ رکن سـوم بر باورپذیری تهدید استوار است، بدین معنا که دشمن باید این ادراک را پیدا کند که طرف مقابل، اراده سیاسی و عزم راسخ برای استفاده از توانایی های خود (اعم از هسته ای یا متعارف) را در صورت لزوم دارد. اگر تهـدیـد معتبر نبـاشـــد یـا بـه درســتی منتقـل نشــود، بـازدارنـدگی شــکســـت خواهـد خورد (Filippidou.2020:1).

نظریه کلاسیک بازدارندگی، آن را به دو نوع اصلی تقسیم می‌کند:

بازدارندگی از طریق انکار : هدف این نوع بازدارندگی، متقاعد کردن مهاجم اســت که حمله او ناموفق خواهد بود یا به اهداف مورد نظرش دست نخواهد یافت (Filippidou.2020:1). این رویکرد بر قابلیت‌های دفاعی متکی اســت و به عنوان راهبردی مطمئن‌تر از بازدارندگی از طریق تنبیه شناخته می‌شود.

بازدارندگی از طریق تنبیه : این رویکرد با تهدید به تحمیل هزینه‌های ســنگین پس از حمله، مهاجم را منصـرف می‌کند این بازدارندگی بر تهدید تلافی‌جویانه اسـتوار اسـت که ممکن اسـت شامل حملات هسته‌ای یا تحریم‌های اقتصادی شدید باشد.

مولفه‌های اصلی بازدارندگی عبارت‌اند از:

* ظرفیت :توانمندی نظامی یا غیرنظامی یک کشور برای اجرای تهدیدات خود.

* اراده :عزم سـیاسـی و آمادگی یک کشـور برای اسـتفاده از ظرفیت‌های خود، که اغلب از طریق سیگنال‌دهی‌های معتبر نشان داده می‌شود.

* ادراک :موفقیت بازدارندگی به این بستگی دارد که مهاجم چگونه تهدیدات را درک و تفسیر می‌کند (Filippidou, 2020, 1).

با توسعه مطالعات روان‌شناسی و علوم شناختی، رویکرد عقلانی محض در بازدارندگی به چالش کشیده شده است. نظریه‌پردازان معتقدند که تصمیم‌گیری‌های استراتژیک صرفاً بر اساس سنجش عقلانی هزینه‌ها و منافع صورت نمی‌گیرد، بلکه عوامل انسانی و غیرعقلانی نیز نقشی محوری ایفا می‌کنند.

هوش مصنوعی عبارت است از قابلیت یک برنامه کامپیوتری برای انجام کارهایی که نیاز به هوش انسانی دارد، ورود هوش مصنوعی و فناوری‌های نوین، مفاهیم کلاسیک بازدارندگی را به شدت به چالش کشیده و زمینه‌ساز تحول در دکترین‌های امنیتی شده است.

چالش‌های فنی و استراتژیک: هوش مصنوعی قابلیت‌های فنی جدیدی را در اختیار قدرت‌ها قرار می‌دهد که می‌تواند بر ثبات استراتژیک تأثیر بگذارد (Schmidt.2022:293). برای مثال، هوش مصنوعی می‌تواند با افزایش سرعت و دقت سیستم‌های هدف‌گیری، به حملات پیش‌دستانه منجر شود و امنیت سیستم‌های هسته‌ای را به خطر اندازد (آذین و همکاران.۱۴۰۳ :۲).

بازدارندگی از طریق آشوب و ابهام: مقاله «انقلاب هوش مصنوعی در نظریه بازدارندگی» مفاهیم نوآورانه‌ای را مطرح می‌کند (Yu. 2024: 1). در «بازدارندگی از طریق آشوب»[1] ،هدف این است که با وارد کردن عناصر غیرقابل پیش‌بینی و پیچیدگی به فضای راهبردی، مهاجم در ارزیابی پیامدهای اقداماتش دچار سردرگمی شود .این نظریه، بازدارندگی را بر اساس نظریه آشوب و پیچیدگی مفهوم‌سازی می‌کند (قاسمی.۱۳۹۵ :۶۳).

* «فوق‌اجبار» و جنگ هیبریدی: الکس ویلنر و کیسی باب مفهوم «فوق‌اجبار»[2] را معرفی می‌کنندآن‌ها می‌گویند هوش مصنوعی با افزایش سرعت و دقت عملیات‌ها، می‌تواند فاصله میان جمع‌آوری اطلاعات و اقدام قهرآمیز را از بین ببرد. این فناوری در «جنگ هیبریدی الگوریتمی» به عنوان یک «نیروی چندبرابرساز» عمل کرده و حملات سایبری و اطلاعات نادرست را به صورت خودکار و در مقیاس وسیع انجام می‌دهد (Wilner & Babb, 2021, 401).

1 Chaos Deterrence
2 Hyper-Coercion

* چارچوب قانونی و سازمانی: بازدارندگی در عصر هوش مصنوعی تنها به توانمندی‌های فنی محدود نمی‌شود.

بلکه یک چارچوب قانونی معتبر برای تعیین مسئولیت، اختیارات و پاسخ‌دهی ضروری است، بدون این چارچوب، هرگونه اقدام قهرآمیز فاقد مشروعیت و اعتبار خواهد بود و بازدارندگی را تضعیف می‌کند (Ducheine & Pijpers, 2021, 475).

این پژوهش با بهره‌گیری از چارچوب مفهومی ارائه شده، تلاش می‌کند تا نشان دهد که چگونه دکترین‌های امنیتی قدرت‌های بزرگ از بازدارندگی سنتی به «بازدارندگی الگوریتمی» در حال گذار هستند. در حالی که نظریه کلاسیک بازدارندگی بر مفاهیم مادی و تقابل سخت متمرکز است، بازدارندگی الگوریتمی، بازدارندگی را به عنوان یک استراتژی جامع می‌نگرد که بر استفاده از قابلیت‌های هوش مصنوعی و داده‌ها برای پیش‌بینی و جلوگیری از اقدامات خصمانه تمرکز دارد. این چارچوب نوین با بررسی ابعاد فنی، ادراکی و حقوقی، به تحلیل این موضوع می‌پردازد که هوش مصنوعی چگونه باعث تغییر درک سیاست‌گذاران از تهدیدات، منافع و ابزارهای قدرت شده است. از این رو، این پژوهش با استفاده از این چارچوب، به بررسی تحولات بنیادین در دکترین‌های امنیتی آمریکا و چین در عصر هوش مصنوعی خواهد پرداخت تا به این نتیجه‌گیری دست یابد که قدرت‌های بزرگ چگونه در حال تطبیق راهبردهای خود با این پدیده نوظهور هستند.

روش شناسی

روش تحقیق به کار گرفته شده، توصیفی-تحلیلی است. پژوهش با توصیف بنیادهای نظری کلاسیک بازدارندگی و تحولات ناشی از هوش مصنوعی، به تحلیل چگونگی دگردیسی دکترین‌های امنیتی قدرت‌های بزرگ می‌پردازد. همچنین از رویکرد تطبیقی برای مقایسه استراتژی‌های ایالات متحده، جمهوری خلق چین و فدراسیون روسیه در مواجهه با مفهوم نوین بازدارندگی الگوریتمی بهره گرفته شده است. این رویکرد تطبیقی، نقاط اشتراک و افتراق در مفاهیم اصلی (مانند کنترل بازتابی روسیه و امنیت جامع چین) را برای درک پیامدهای آن بر ثبات راهبردی جهانی، آشکار می‌سازد.

۱- هوش مصنوعی و تغییر پارادایم‌های امنیتی

پژوهش‌ها نشان می‌دهند که هوش مصنوعی به طور همزمان هم تهدیدات و هم فرصت‌هایی را برای امنیت ملی دولت‌ها ایجاد می‌کند این فناوری به عنوان یک منبع قدرت غنی برای بازیگران بین‌المللی عمل می‌کند و قابلیت‌های جدیدی را در زمینه‌های اقتصادی، اجتماعی، سیاسی و امنیتی فراهم می‌سازد (احمدی و دیگران، ۱۴۰۲: ۴۱). هوش مصنوعی با توانایی درک، پردازش و تحلیل داده‌ها برای ماشین‌ها و دستگاه‌های رایانه‌ای، می‌تواند بسیاری از جنبه‌های زندگی و ساختارهای جوامع بشری را تحت تأثیر قرار دهد . این موضوع سبب شده است که دولت‌ها به فکر تدوین استراتژی‌های امنیت ملی جدیدی باشند که به طور خاص بر هوش مصنوعی و کاربردهای آن تمرکز دارد (Sayler, 2020: 35).

کشورهای پیشرفته به دنبال بهره‌گیری از ظرفیت تحلیلی هوش مصنوعی در زمینه فرماندهی و کنترل نیروهای نظامی هستند با ترکیب داده‌های حاصل از حسگرها در حوزه‌های هوایی، فضایی، سایبری، دریایی و زمینی، هوش مصنوعی می‌تواند یک تصویر عملیاتی مشترک برای تصمیم‌گیرندگان ایجاد کند که به طور بالقوه کیفیت و سرعت تصمیم‌گیری در زمان جنگ را افزایش می‌دهد (احمدی و دیگران، ۱۴۰۲: ۵۳).

* ربات‌ها و وسایل نقلیه خودران: پیشرفت‌های هوش مصنوعی در وسایل نقلیه خودران، مانند پهپادها و خودروهای بدون سرنشین، در منازعات بین‌المللی مؤثر خواهد بود این سیستم‌های خودمختار با استفاده از فناوری‌هایی مانند ادراک بصری، تشخیص گفتار و چهره، می‌توانند طیف وسیعی از عملیات‌ها را بدون دخالت انسان انجام دهند (Hoadley & Lucas, 2018: 12).

* جنگ سایبری: هوش مصنوعی یک فناوری کلیدی در پیشبرد عملیات‌های سایبری نظامی است ابزارهای مجهز به هوش مصنوعی می‌توانند با تشخیص ناهنجاری‌ها در الگوهای فعالیت شبکه، یک مانع پویا و جامع در برابر حملات ارائه دهند (Hoadley & Lucas, 2018: 10).

هوش مصنوعی علاوه بر مزایایی مانند تصمیم‌سازی منطقی و کاهش خطاها، تهدیداتی را برای حکمرانی سیاسی و دموکراسی به دنبال داشته است (احمدی و دیگران، ۱۴۰۲: ۵۵). این فناوری با امکان جمع‌آوری و تحلیل داده‌های گسترده، می‌تواند آزادی بیان و انتشار اطلاعات آزاد را محدود کند (احمدی و دیگران، ۱۴۰۲: ۵۵).

هوش مصـــنوعی در اقتصـــاد جهانی می‌تواند بهره‌وری را افزایش دهد اما پیامدهای عمیق و مخربی نیز دارد (Hoadley & Lucas, 2018: 2). این فناوری ممکن اســـت نابرابری‌های اقتصـادی را تشـدید کرده و شـکاف میان کشـورهای توسـعه‌یافته و در حال توسـعه را افزایش دهد پیش‌بینی می‌شـود که این فناوری تا سـال ۲۰۳۰ حدود ۱۵.۷ تریلیون دلار به تولید ناخالص داخلی جهان اضافه کند (احمدی و دیگران، ۱۴۰۲: ۵۹).

۱-۱.چالش‌ها و فرصت‌های هوش مصنوعی برای امنیت ملی

الف)فرصت‌ها:

* خودمختاری: سـیسـتم‌های خودمختار مجهز به هوش مصـنوعی می‌توانند انسـان‌ها را برای کارهای پیچیده‌تر آزاد کنند و تلفات را کاهش دهند (Sayler, 2020: 24).

* سـرعت و اسـتقامت: هوش مصـنوعی ابزاری منحصـر به فرد برای عملیاتی کردن نبردها در مقیاس‌های زمانی انتهایی معرفی می‌کند (Hoadley & Lucas, 2018: 26).

* برتری اطلاعاتی: سیسـتم‌های اطلاعاتی مجهز به هوش مصـنوعی می‌توانند حجم عظیمی از داده‌هـا را مرتـب و تحلیـل کننـد تـا اطلاعـات مفیـدی را برای تصـــمیم‌گیری اســـتخراج کننـد (Hoadley & Lucas, 2018: 28).

* مقیاس‌پذیری: هوش مصنوعی قادر است با افزایش توانایی‌های انسانی و تزریق سیستم‌های نظامی ارزان قیمت، اثری معادل با چند برابر کردن نیروها ایجاد کند (Sayler, 2020: 27).

ب)چالش‌ها:

* افزایش تهدیدات سـایبری: سیسـتم‌های وابسـته به هوش مصـنوعی، به خصـوص محاسـبات ابری، آسیب‌پذیری‌های سایبری را به شدت افزایش می‌دهند (Sayler, 2020: 28).

* رقابت تسلیحاتی: رقابت استراتژیک بین قدرت‌های دارنده این فناوری می‌تواند به استفاده از ســیســـتم‌های آزمایش نشـــده و ناشـــناخته برای کســـب مزیت رقابتی منجر شـــود که حوادث غیرمنتظره‌ای را به دنبال دارد (Hoadley & Lucas, 2018: 2).

* عدم شفافیت و پاسخگویی: فرآیندهای تصمیم‌گیری در هوش مصنوعی ممکن است شفافیت و پاسخگویی ضعیفی داشته باشند که مسائل اخلاقی را مطرح می‌کند (Hoadley & Lucas, 2018: 33).

* جعل و فریب: فناوری‌های هوش مصنوعی مانند جعل عمیق و حملات هدفمند می‌توانند به عنوان ابزار فریب و اطلاعات نادرست مورد استفاده قرار گیرند (Hoadley & Lucas, 2018: 33).

*ایجاد وابستگی: استفاده راهبردی از ابزارهای اقتصادی و پروژه‌های زیرساختی فناورانه برای ایجاد وابستگی در کشور هدف، منطق بازدارندگی را مختل می‌کند. این رویکرد با ترویج وابستگی فناورانه و سیاسی، تهدید را به اهرمی پنهان برای اعمال نفوذ تبدیل کرده و خطوط قرمز لازم برای بازدارندگی از طریق مجازات را محو می‌سازد(Farrell & Newman, 2019)

در مجموع، هوش مصنوعی یک فناوری با کاربرد دوگانه است که می‌تواند مزیت و فرصت‌های بزرگی را برای صاحبان خود به ارمغان آورد، اما در عین حال، چالش‌های جدی برای حکمرانی و امنیت ملی دولت‌ها ایجاد می‌کند دولت‌ها برای کاهش خطرات ناشی از این فناوری باید سطح دانش خود را ارتقا داده و با استفاده از قواعد و رژیم‌های حقوقی بین‌المللی، بر عملکرد توسعه‌دهندگان هوش مصنوعی نظارت داشته باشند

۲- دکترین‌های امنیتی در حال گذار: بازدارندگی در عصر الگوریتم

۲-۱ .تحول دکترین بازدارندگی در ایالات متحده

دکترین بازدارندگی ایالات متحده از زمان پیدایش سلاح‌های هسته‌ای تاکنون، دستخوش تحولات چشمگیری شده است. این دکترین که در ابتدا به عنوان ابزاری برای جلوگیری از درگیری مستقیم با اتحاد جماهیر شوروی و دیگر قدرت‌های بزرگ تلقی می‌شد، به تدریج به سلاحی برای تغییر رژیم‌های مخالف و حتی جنگ تبدیل شده است این تحول، به ویژه در سیاست تحریمی آمریکا، به وضوح قابل مشاهده است؛ جایی که تحریم‌ها از ابزاری برای بازدارندگی و تغییر رفتار، به اهرمی برای اعمال فشار حداکثری و بی‌ثبات‌سازی حکومت‌های هدف تبدیل شده‌اند (پورحسن.۱۴۰۱: ۲۸۵).

تاریخچه دکترین بازدارندگی آمریکا را می‌توان به پنج موج اصلی تقسیم کرد که هر یک تحت تأثیر شرایط ژئوپلیتیکی، فناوری‌های نوین و تهدیدات متغیر شکل گرفته‌اند (MESA Group, 2023, 5).

موج اول (۱۹۵۵-۱۹۴۵): خوش‌بینی هسته‌ای و انتقام گسترده۱

در این دوره، با توجه به انحصار هسته‌ای ایالات متحده، دکترین «انتقام گسترده» حاکم بود بر اساس این دکترین، هرگونه تجاوزی از سوی دشمن با پاسخی هسته‌ای ویرانگر مواجه می‌شد این رویکرد بر پایه برتری هسته‌ای آمریکا و این فرض استوار بود که دشمنان، بازیگرانی عقلانی هستند و از ترس نابودی کامل، دست به اقدام علیه منافع آمریکا نخواهند زد (MESA Group, 2023, 9).

موج دوم (۱۹۷۲-۱۹۵۵): پاسخ انعطاف‌پذیر۲ و تخریب حتمی متقابل

با دستیابی شوروی به سلاح‌های هسته‌ای، دکترین انتقام گسترده اعتبار خود را از دست داد و جای خود را به «پاسخ انعطاف‌پذیر» داد این استراتژی بر لزوم داشتن گزینه‌های متنوع نظامی، از جمله نیروهای متعارف و سلاح‌های هسته‌ای تاکتیکی، برای پاسخ متناسب به سطوح مختلف تهدید تأکید داشت در این دوره، مفهوم «تخریب حتمی متقابل» نیز شکل گرفت که بر اساس آن، هر دو ابرقدرت توانایی نابودی کامل یکدیگر را داشتند و همین امر مانع از آغاز یک جنگ هسته‌ای می‌شد (MESA Group, 2023, 13).

موج سوم (۱۹۹۱-۱۹۷۲): انتقام محدود۳ و صلح از طریق قدرت

در این دوره، تلاش‌هایی برای کنترل رقابت تسلیحاتی از طریق پیمان‌هایی مانند «سالت» صورت گرفت دکترین بازدارندگی به سمت «انتقام محدود» حرکت کرد که بر پاسخ‌های هسته‌ای متناسب و محدود برای جلوگیری از تشدید درگیری تأکید داشت دولت ریگان نیز با شعار «صلح از طریق قدرت» ، به دنبال تقویت توان نظامی آمریکا برای بازدارندگی شوروی بود

پس از پایان جنگ سرد و ظهور تهدیدات جدیدی مانند «دولت‌های سرکش» و گروه‌های تروریستی، دکترین بازدارندگی نیز دستخوش تغییر شد در این دوره، مفهوم «بازدارندگی متناسب»۴

1 Massive Retaliation
2 Flexible Response
3 Limited Retaliation
4 Tailored Deterrence

مطرح شد که بر لزوم طراحی استراتژی‌های بازدارنده خاص برای هر دشمن، با در نظر گرفتن انگیزه‌ها، توانایی‌ها و آسیب‌پذیری‌های آن، تأکید داشت حملات ۱۱ سپتامبر نیز باعث شد تا مقابله با تروریسم به یکی از اولویت‌های اصلی سیاست امنیتی آمریکا تبدیل شود (MESA Group, 2023, 22).

موج پنجم (۲۰۱۰-تاکنون): بازدارندگی یکپارچه[1] و ترکیبی

در این دوره، با ظهور تهدیدات چندوجهی و پیچیده، مفاهیم جدیدی مانند «بازدارندگی یکپارچه» و «بازدارندگی ترکیبی» مطرح شده‌اند بازدارندگی یکپارچه بر لزوم هماهنگی و استفاده از تمامی ابزارهای قدرت ملی، از جمله دیپلماتیک، اقتصادی، اطلاعاتی و نظامی، برای مقابله با تهدیدات تأکید دارد. بازدارندگی ترکیبی نیز به مقابله با دشمنانی می‌پردازد که از ترکیبی از تاکتیک‌های متعارف و نامتعارف، مانند جنگ سایبری، تبلیغات و عملیات‌های پنهانی، استفاده می‌کنند (MESA Group, 2023, 28).

با توجه به تکثر منابع تهدید در عصر حاضر، از جمله تهدیدات سایبری، اطلاعاتی و همچنین ظهور بازیگران غیردولتی، مفهوم سنتی بازدارندگی که عمدتاً بر تهدیدات نظامی متمرکز بود، کارایی خود را از دست داده است. دوران پس از جنگ سرد، پیچیدگی‌های جدیدی را برای نظریه بازدارندگی به همراه آورد، زیرا دیگر با یک دشمن واحد و قابل پیش‌بینی (اتحاد جماهیر شوروی) روبرو نبودیم و فناوری‌های نوین، ماهیت درگیری‌ها را تغییر داده بودند این امر منجر به گذار از «بازدارندگی از طریق مجازات» به «بازدارندگی از طریق انکار» شد؛ به این معنا که هدف، نه فقط تهدید به تلافی، بلکه غیرممکن ساختن حمله برای دشمن است (Long, 2015, 358).

ورود شتابان هوش مصنوعی به این دکترین، بُعد جدیدی به بازدارندگی یکپارچه بخشیده است. هوش مصنوعی با ترکیب داده‌ها و حسگرها در تمام حوزه‌ها (زمینی، هوایی، فضایی، سایبری)، یک تصویر عملیاتی مشترک فوق‌العاده دقیق و درلحظه برای تصمیم‌گیرندگان ایجاد می‌کند. این قابلیت تحلیلی، توانایی ایالات متحده را برای پیش‌بینی نیّات خصمانه و اجرای مؤثر منطق بازدارندگی الگوریتمی تقویت می‌کند؛ به این معنا که تهدید نه بر تلافی پس از وقوع، بلکه بر خنثی‌سازی حملات از طریق انکار مؤثر و استفاده از سامانه‌های خودمختار و گله‌های پهپادی در زمان واقعی، استوار است. این امر سرعت تصمیم‌گیری‌های فرماندهی و کنترل را به شدت افزایش می‌دهد.

1 Integrated Deterrence

۲-۲ .چین و بازدارندگی هوشمند در چارچوب امنیت جامع

دکترین امنیت ملی چین در دوران جدید، به ویژه تحت رهبری شی جین پینگ، بر پایه مفهوم «امنیت جامع ملی» استوار است. این رویکرد، امنیت را صرفاً در بعد نظامی خلاصه نمی‌کند، بلکه آن را یک مفهوم کل‌نگر می‌داند که ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی و به‌ویژه فناورانه را در بر می‌گیرد. در این چارچوب، توسعه و به‌کارگیری فناوری‌های پیشرفته، به خصوص هوش مصنوعی ،به ابزاری کلیدی برای تحقق اهداف امنیتی و بازدارندگی چین تبدیل شده است. این راهبرد نوین را می‌توان «بازدارندگی هوشمند» نامید که در آن، قدرت سایبری و قابلیت‌های مبتنی بر هوش مصنوعی، نقشی محوری در مهار رقبا و حفاظت از منافع ملی ایفا می‌کنند.

سند «دفاع ملی چین در عصر جدید» که در سال ۲۰۱۹ منتشر شد، به وضوح نشان می‌دهد که چین با چالش‌های امنیتی پیچیده‌ای روبرو است که از رقابت راهبردی قدرت‌های بزرگ تا تهدیدهای ناشی از جدایی‌طلبی، امنیت سایبری و تروریسم را شامل می‌شود (دفتر اطلاعات شورای دولت جمهوری خلق چین.۲۰۱۹ :۴). این سند تأکید می‌کند که انقلاب در حال وقوع در امور نظامی، مبتنی بر فناوری اطلاعات و هوشمندی است و چین برای پر کردن شکاف خود با ارتش‌های پیشرفته جهان، نیازی فوری به بهبود قابلیت‌های اطلاعاتی و توسعه «ارتش هوشمند» دارد (دفتر اطلاعات شورای دولت جمهوری خلق چین.۲۰۱۹ :۶).

بر این اساس، امنیت جامع ملی چین اهداف زیر را دنبال می‌کند:

* حفاظت از حاکمیت و امنیت سیاسی: این امر شامل مقابله با نفوذ خارجی، سرکوب جنبش‌های جدایی‌طلب (در تایوان، تبت و سین‌کیانگ) و تضمین ثبات داخلی و رهبری حزب کمونیست چین است.

* تضمین توسعه اقتصادی پایدار: چین معتقد است بدون یک محیط امن خارجی، توسعه اقتصادی مستمر ممکن نیست.

* حراست از منافع در حوزه‌های نوین: این حوزه‌ها شامل فضای سایبری، فضای بیرونی (ماورای جو) و فضای الکترومغناطیسی است که به عنوان عرصه‌های کلیدی برای رقابت راهبردی و امنیت ملی شناخته می‌شوند.

* دستیابی به برتری فناورانه: چین توسعه فناوری‌های پیشرفته‌ای چون هوش مصنوعی، اطلاعات کوانتومی، داده‌های بزرگ و اینترنت اشیاء را برای مدرن‌سازی ارتش و اقتصاد خود ضروری می‌داند (دفتر اطلاعات شورای دولت جمهوری خلق چین.۲۰۱۹: ۶).

۲-۲-۱.بازدارندگی هوشمند: تلفیق قدرت سایبری و هوش مصنوعی

بازدارندگی هوشمند چین، پاسخی به محیط امنیتی جدید و تلاشی برای ایجاد یک مزیت نامتقارن در برابر رقبای قدرتمند، به ویژه ایالات متحده است. این راهبرد بر چندین ستون استوار است:

حاکمیت سایبری :چین معتقد است که فضای سایبری یک «مرز جدید برای دولت مدرن» است و حاکمیت ملی باید به این حوزه نیز تسری یابداین کشور با رویکرد چندجانبه‌گرای غرب که بر اینترنت آزاد و باز تأکید دارد، مخالف است و آن را ابزاری برای هژمونی آمریکا و دخالت در امور داخلی دیگر کشورها می‌داند پکن با ایجاد «دیوار آتش بزرگ چین» و کنترل شدید بر جریان اطلاعات، به دنبال حفاظت از ثبات سیاسی و اجتماعی خود در برابر آنچه تهدیدات ناشی از اینترنت می‌خواند، است از دیدگاه نظامی، ارتش آزادی‌بخش خلق وظیفه خود می‌داند که از حاکمیت چین در حوزه سایبری دفاع کند، زیرا کنترل این حوزه را برای پیروزی در نبردهای قرن بیست و یکم حیاتی می‌داند (Kolton, 2017, 121).

جنگ اطلاعاتی :نظریه‌پردازان نظامی چین بر این باورند که جنگ‌های آینده، «جنگ‌های اطلاعاتی» و مبتنی بر هوشمندی خواهند بود (دفتر اطلاعات شورای دولت جمهوری خلق چین، ۲۰۱۹، ۶). در این نوع نبرد، پیروزی از آنِ طرفی است که بتواند برتری اطلاعاتی را کسب کرده و از آن برای فلج کردن سیستم‌های فرماندهی، کنترل و ارتباطات دشمن استفاده کند. تأسیس نیروی پشتیبانی راهبردی در سال ۲۰۱۵، که مسئولیت عملیات‌های سایبری، فضایی و جنگ الکترونیک را بر عهده دارد، نشان‌دهنده اهمیت این حوزه در تفکر نظامی چین است (Kolton, 2017, 119).

بازدارندگی از طریق نفوذ و جاسوسی:یکی از مؤلفه‌های اصلی بازدارندگی هوشمند چین، استفاده تهاجمی از فضای سایبری برای جاسوسی و نفوذ به زیرساخت‌های حیاتی دشمن است. این اقدامات سه هدف اصلی را دنبال می‌کنند.

بازدارندگی راهبردی: با نفوذ به زیرساخت‌های حیاتی مانند شبکه‌های برق، سیستم‌های مالی و ارتباطی، چین این پیام را به دشمن می‌دهد که در صورت وقوع درگیری، قادر است خسارات فلج‌کننده‌ای به آن وارد کند (Hjortdal, 2011, 3).

* جاسوسی نظامی-فناورانه: چین با سرقت اطلاعات مربوط به فناوری‌های نظامی پیشرفته، مانند جنگنده ، شکاف فناورانه خود با غرب را کاهش داده و روند مدرن‌سازی نظامی خود را تسریع می‌کند.

* جاسوسی صنعتی: سرقت اسرار تجاری و فناوری‌های صنعتی به شرکت‌های چینی کمک می‌کند تا مزیت رقابتی در اقتصاد جهانی کسب کنند (Hjortdal.2011 ;3).

این رویکرد تهاجمی با مفهوم سنتی بازدارندگی در غرب که بیشتر ماهیتی تدافعی دارد، متفاوت است. چین مفهوم گسترده‌تری به نام «وِیشه»[1] را به کار می‌برد که ترکیبی از بازدارندگی و اجبار است . در این دیدگاه، اقدامات تهاجمی در زمان صلح، مانند حملات سایبری، به عنوان ابزاری مشروع برای وادار کردن رقیب به تغییر سیاست و نمایش قدرت تلقی می‌شود (Kolton.2017:133).

در واقع، سرمایه‌گذاری گسترده چین بر هوش مصنوعی، عنصری کلیدی در راهبرد «بازدارندگی هوشمند» و دستیابی به برتری اطلاعاتی است. جاسوسی سایبری گسترده صنعتی و نظامی چین، نه صرفاً برای سرقت فناوری، بلکه برای جمع‌آوری داده‌های کلان و مدل‌سازی است که پکن از آن برای پیش‌بینی قابلیت‌ها و نیّات راهبردی دشمن بهره می‌گیرد. این تمرکز بر داده‌محوری، جوهره منطق پیش‌بینی در بازدارندگی الگوریتمی را شکل می‌دهد و به چین امکان می‌دهد تا شکاف نظامی خود را با ارتش‌های پیشرفته جهان به سرعت پر کند

۲-۲-۲.اهداف بلندمدت چین

سرمایه‌گذاری گسترده چین بر هوش مصنوعی و ادغام آن در دکترین امنیت جامع، اهداف بلندمدتی را دنبال می‌کند. چین قصد دارد تا سال ۲۰۳۰ به مرکز اصلی نوآوری هوش مصنوعی در جهان تبدیل شود این برتری فناورانه، به پکن امکان می‌دهد تا به اهداف زیر دست یابد:

1 Vishe

* تغییر مسالمت‌آمیز در توازن قدرت بین‌المللی: با تقویت قدرت اقتصادی و نظامی از طریق هوش مصنوعی، چین امیدوار است که بتواند نظم بین‌المللی را به سمت یک ساختار چندقطبی هدایت کرده و نفوذ جهانی خود را افزایش دهد (سیمبر و فصیحی مقدم لاکانی. ۲۰۲۵: ۹).

* ارائه الگوی حکمرانی جایگزین: چین با صادرات فناوری‌های نظارتی و «شهرهای هوشمند» به کشورهای دیگر، به ویژه در آسیای مرکزی، الگوی «اقتدارگرایی دیجیتال» خود را ترویج می‌کند و وابستگی فناورانه و سیاسی این کشورها به خود را افزایش می‌دهد (رضاپور. ۲۰۲۴: ۱۸۲).

* کاهش شکاف نظامی با قدرت‌های بزرگ: هوش مصنوعی به عنوان یک عامل «جهش‌دهنده» در فناوری‌های نظامی تلقی می‌شود که می‌تواند به ارتش چین کمک کند تا شکاف خود را با ارتش‌های پیشرفته جهان به سرعت پر کند (سیمبر و فصیحی مقدم لاکانی. ۲۰۲۵: ۲۶).

در نهایت، بازدارندگی هوشمند چین در چارچوب امنیت جامع، یک راهبرد چندبعدی و پیچیده است که از فناوری به عنوان ابزاری برای اعمال قدرت، حفاظت از منافع ملی و شکل‌دهی به نظم آینده جهانی بهره می‌برد. این رویکرد، چالش‌های جدیدی را برای قدرت‌های غربی ایجاد می‌کند و لزوم درک عمیق‌تر از دکترین‌ها و اهداف راهبردی چین را بیش از پیش نمایان می‌سازد.

۳-۲ . روسیه و بازدارندگی در بستر جنگ شناختی و سایبری

دکترین بازدارندگی فدراسیون روسیه در عصر جدید، با فاصله گرفتن از مفاهیم سنتی متمرکز بر تقابل نظامی، به طور فزاینده‌ای بر ابعاد شناختی و سایبری متکی شده است. مسکو با درک آسیب‌پذیری‌های جوامع باز غربی و برتری خود در به‌کارگیری ابزارهای نامتقارن، جنگ اطلاعاتی را به عنوان یک مؤلفه کلیدی برای حفاظت از حاکمیت، مقابله با نفوذ غرب و پیشبرد اهداف راهبردی خود تعریف کرده است. این رویکرد، که ریشه در تاکتیک‌های دوران شوروی دارد، در فضای دیجیتال امروزی به سلاحی قدرتمند برای ایجاد بازدارندگی و اعمال نفوذ تبدیل شده است.

بر خلاف تصور رایج در غرب که اقدامات روسیه را تهاجمی می‌داند، مسکو بسیاری از فعالیت‌های خود در فضای اطلاعاتی را ماهیتاً تدافعی تلقی می‌کند از دیدگاه کرملین، اینترنت و رسانه‌های غربی ابزارهایی برای تهاجم فرهنگی و سیاسی هستند که با هدف "فرسایش ارزش‌های معنوی و اخلاقی سنتی روسیه" و بی‌ثبات‌سازی دولت به کار می‌روند .نگرانی از وقوع انقلاب‌های

رنگی و بهار عربی، که مسکو آنها را محصول دخالت سایبری غرب می‌داند، این دیدگاه تدافعی را تقویت کرده است (قنبری و خانی. ۱۳۹۹: ۱۱۸).

این رویکرد مدرن، بر پایه دو مفهوم کلیدی از دوران شوروی بنا شده است:

* اقدامات فعال : این مفهوم به مجموعه عملیات‌های پنهان و آشکار برای تأثیرگذاری بر رویدادها و رفتارها در کشورهای خارجی اشاره دارد. اتحاد جماهیر شوروی با بودجه‌ای بالغ بر ۳ تا ۴ میلیارد دلار در سال، از این اقدامات برای انتشار اطلاعات نادرست، جعل اسناد و استفاده از عوامل نفوذی علیه دشمن اصلی خود، یعنی ایالات متحده، بهره می‌برد (Ajir & Vailliant, 2018, 72).

* کنترل بازتابی :این نظریه که بیش از ۴۰ سال در نیروهای مسلح روسیه و شوروی مورد مطالعه قرار گرفته، بر دستکاری ادراک دشمن از واقعیت تمرکز دارد ,هدف، القای اطلاعاتی خاص به فرآیند تصمیم‌گیری حریف است تا او را به اتخاذ تصمیماتی سوق دهد که به ضرر خودش و به نفع روسیه باشد ,این فرآیند نه تنها تصمیم‌گیرندگان کلیدی، بلکه افکار عمومی را نیز هدف قرار می‌دهد (Ajir & Vailliant, 2018, 74).

روسیه با تلفیق این مفاهیم با فناوری‌های نوین، به یک استراتژی جنگ ترکیبی دست یافته است که در آن، مرز میان جنگ و صلح و همچنین اهداف نظامی و غیرنظامی کمرنگ می‌شود.

ژنرال والری گراسیموف، رئیس ستاد کل نیروهای مسلح روسیه، تأکید می‌کند که در جنگ‌های نوین، روش‌های غیرنظامی (سیاسی، اقتصادی، اطلاعاتی) نقشی به مراتب مهم‌تر از اقدامات نظامی متعارف ایفا می‌کنند (قنبری و خانی. ۱۳۹۹: ۱۲۹).

۲-۳-۱.ابزارهای بازدارندگی شناختی و سایبری

روسیه با درک عدم توانایی خود برای رقابت مستقیم با قدرت نظامی و اقتصادی غرب، بر ابزارهای کم‌هزینه و پربازده در فضای اطلاعاتی تمرکز کرده است .مهم‌ترین این ابزارها عبارتند از:

* بهره‌برداری از رسانه‌های اجتماعی: کرملین با استفاده از یک «ارتش ترول» و شبکه‌ای از حساب‌های رباتیک (بات‌ها)، به طور گسترده به انتشار اطلاعات نادرست، دامن زدن به اختلافات اجتماعی و تضعیف اعتماد به نهادهای دموکراتیک می‌پردازد . این عملیات با تکیه بر روایت‌های موجود، گروه‌های مستعد پذیرش پیام و شبکه‌ای از حساب‌های خودکار، به دنبال «فرماندهی روند» در شبکه‌های اجتماعی است.

* کنترل رسانه‌های غربی: روسیه با بهره‌گیری از اصل آزادی بیان در جوامع غربی، رسانه‌های دولتی مانند راشا تودی را به ابزاری قدرتمند برای تبلیغات تهاجمی تبدیل کرده است این رسانه‌ها با تمرکز بر جنبه‌های منفی جوامع غربی و ترویج تئوری‌های توطئه، به دنبال بی‌اعتبار کردن رقبای مسکو هستند علاوه بر این، خرید سهام در روزنامه‌های غربی و انتشار ضمیمه‌های تبلیغاتی، از دیگر تاکتیک‌های روسیه در این حوزه است (Ajir & Vailliant, 2018,75- 79).

* لابی‌گری و نفوذ در جوامع غربی: کرملین با تأمین مالی احزاب سیاسی، تأسیس سازمان‌های غیردولتی و اندیشکده‌های به ظاهر مستقل، و استخدام شرکت‌های لابی‌گری غربی، به دنبال تأثیرگذاری بر نخبگان سیاسی و افکار عمومی در غرب است (Ajir & Vailliant, 2018, 80-81). این اقدامات با هدف تضعیف دموکراسی‌ها از درون و پیشبرد منافع روسیه انجام می‌شود.

این راهبردها با ظهور هوش مصنوعی به شکلی الگوریتمی تقویت شده‌اند. هوش مصنوعی به عنوان یک نیروی چندبرابرساز ، به روسیه امکان می‌دهد که کمپین‌های اطلاعات نادرست و حملات هدفمند را با استفاده از شبکه‌های رباتیک (بات‌ها) و جعل عمیق ، به صورت خودکار و در مقیاس وسیع انجام دهد. این امر، کارایی تاکتیک‌های «کنترل بازتابی» را در فضای دیجیتال امروز به شدت افزایش داده و با ایجاد ابهام عمدی در انتساب و احراز هویت عامل حمله، منطق تلافی‌جویی بازدارندگی کلاسیک را به طور کامل خنثی می‌سازد.»

۲-۳-۲.چالش‌های بازدارندگی در برابر جنگ شناختی

ماهیت جنگ شناختی و سایبری، چالش‌های بنیادینی را برای نظریه بازدارندگی سنتی ایجاد می‌کند. بازدارندگی کلاسیک که بر پایه تهدید به تلافی (مجازات) استوار بود، در این حوزه جدید با مشکلات جدی روبرو است (دهقانی. ۱۳۹۶ :۱۲۸). این چالش‌ها عبارتند از:

* مشکل انتساب :شناسایی قطعی عامل یک حمله سایبری یا یک کمپین اطلاعات نادرست بسیار دشوار است (دهقانی. ۱۳۹۶: ۱۳۱). بازیگران دولتی می‌توانند با استفاده از نیروهای نیابتی و هکرهای خصوصی، مسئولیت اقدامات خود را انکار کنند (قنبری و خانی. ۱۳۹۹: ۱۴۷). این امر، تهدید به تلافی را بی‌اثر می‌سازد، زیرا نمی‌توان با اطمینان گفت چه کسی را باید مجازات کرد.

* فقدان خط قرمزهای مشخص :در حالی که در بازدارندگی هسته‌ای، عبور از خط قرمز (مانند حمله هسته‌ای) کاملاً مشخص است، در فضای سایبری این خطوط بسیار مبهم هستند یک حمله

سایبری تا زمانی که منجر به تخریب فیزیکی نشود، اغلب به عنوان یک "مزاحمت" تلقی می‌شود، نه یک اقدام جنگی در حوزه شـــناختی، این خط قرمز تقریباً وجود ندارد و نمی‌توان تأثیر روانی یک کمپین اطلاعاتی را به سادگی اندازه‌گیری کرد.

* عدم تقارن در آســیب‌پذیری: جوامع باز و دموکراتیک به دلیل آزادی رســانه‌ها و جریان اطلاعات، در برابر جنگ شناختی بسیار آسیب‌پذیرتر از جوامع بسته و اقتدارگرا هستند (Ajir & Vailliant, 2018, 86). این عدم تقارن، امکان پاســخ متقابل را محدود می‌کند، زیرا غرب نمی‌تواند به سادگی از همان ابزارهایی که روسیه علیه آن به کار می‌برد، استفاده کند.

به همین دلیل، برخی تحلیلگران پیشنهاد کرده‌اند که باید یک حوزه ششم جنگ (روانشناختی) را به طور رسـمی به رسـمیت شـناخت که اگرچه با حوزه سـایبری همپوشـانی دارد، اما بر جنبه‌های شناختی و انسانی جنگ اطلاعاتی متمرکز است (Ajir & Vailliant, 2018, 83). این تفکیک می‌تواند به تدوین اســتراتژی‌های بازدارندگی مؤثرتر و متناســب با ماهیت این تهدید نوین کمک کند. در نهایت، بازدارندگی روسـیه در این بسـتر، تلاشـی اسـت برای جبران ضـعف در مؤلفه‌های قدرت متعارف و ایجاد یک موازنه نامتقارن با غرب، از طریق به کارگیری هوشـمندانه اطلاعات به عنوان یک سلاح راهبردی.

۴-۲ . بررسی تطبیقی: نقاط اشتراک و افتراق در رویکرد قدرت‌های بزرگ

با تحلیل رویکردهای ایالات متحده، روســیه و چین در حوزه بازدارندگی و امنیت مدرن، می‌توان شباهت‌ها و تفاوت‌های بنیادینی را در دکترین راهبردی آن‌ها شناسایی کرد. هر سه قدرت، فضای سایبری را به عنوان یک حوزه حیاتی برای امنیت ملی به رسمیت می‌شناسند، اما انگیزه‌ها، مفاهیم و ابزارهای مورد استفاده آن‌ها تفاوت‌های معناداری را نشان می‌دهد.

ویژگی/بعد	ایالات متحده آمریکا US	فدراسیون روسیه RU	جمهوری خلق چین CN
چارچوب کلی	بازدارندگی یکپارچه: استفاده هماهنگ از تمام ابزارهای قدرت (دیپلماتیک، اطلاعاتی، نظامی،	جنگ ترکیبی :تلفیق ابزارهای متعارف و نامتعارف (سایبری، شناختی، نظامی) برای دستیابی به اهداف،	امنیت جامع ملی : رویکردی کل‌نگر که امنیت ملی را شامل ابعاد سیاسی، اقتصادی، نظامی و فناورانه می‌داند.

ویژگی/بعد	ایالات متحده آمریکا US	فدراسیون روسیه RU	جمهوری خلق چین CN
	اقتصادی) برای مهار دشمن.	اغلب زیر آستانه درگیری مسلحانه.	
مفهوم مرکزی بازدارندگی	بازدارندگی :تمرکز بر پیشگیری از اقدام دشمن با تهدید به تحمیل هزینه؛ تفکیک روشن میان بازدارندگی (پیشگیری) و اجبار (وادار کردن).	کنترل بازتابی : دستکاری فرآیند تصمیم‌گیری دشمن از طریق القای اطلاعات هدفمند برای سوق دادن او به سمت اقدامات اشتباه و خود–تخریبی.	وِیشه : مفهومی گسترده که بازدارندگی و اجبار را با هم ترکیب می‌کند و استفاده از اقدامات تهاجمی در زمان صلح را برای وادار کردن رقیب به تغییر رفتار، مشروع می‌داند.
توجیه و قاب‌بندی	دفاعی/هنجاری: حفاظت از یک اینترنت باز، آزاد و امن و دفاع از نظم بین‌المللی مبتنی بر قوانین.	تدافعی: مقابله با نفوذ فرهنگی و سیاسی غرب، جلوگیری از انقلاب‌های رنگی و حفاظت از حاکمیت ملی در برابر تهدیدات اطلاعاتی.	تدافعی: حفاظت از حاکمیت سایبری ، تضمین ثبات داخلی و رهبری حزب کمونیست، و مقابله با هژمونی فناورانه آمریکا.
ابزارهای اصلی نامتقارن	برتری فناورانه و اتحادها: تکیه بر نوآوری‌های تکنولوژیک و شبکه گسترده‌ای از متحدان برای ایجاد بازدارندگی.	جنگ شناختی و اطلاعاتی: استفاده از "ارتش ترول‌ها"، رسانه‌های دولتی (مانند RT) و کمپین‌های اطلاعات نادرست برای ایجاد شکاف اجتماعی و تضعیف نهادهای دموکراتیک.	قدرت اقتصادی و جاسوسی سایبری: بهره‌گیری از «جاده ابریشم دیجیتال» برای ایجاد وابستگی فناورانه و جاسوسی گسترده صنعتی و نظامی برای کاهش شکاف تکنولوژیک.

ویژگی/بعد	ایالات متحده آمریکا US	فدراسیون روسیه RU	جمهوری خلق چین CN
هدف راهبردی نهایی	حفظ رهبری جهانی: تثبیت جایگاه به عنوان قدرت برتر و حفظ نظم بین‌المللی لیبرال.	بی‌ثبات‌سازی و احیای نفوذ: تضعیف نهادهای غربی، ایجاد بی‌ثباتی در غرب و بازگرداندن نفوذ در حوزه "خارج نزدیک" (کشورهای پساشوروی).	تغییر توازن قدرت جهانی: دستیابی به برتری در هوش مصنوعی تا سال ۲۰۳۰ و هدایت مسالمت‌آمیز نظم جهانی به سمت یک ساختار چندقطبی با محوریت چین.

تحلیل تطبیقی

نقاط اشتراک:

* اهمیت فضای سایبری: هر سه قدرت، فضای سایبری را به عنوان یک حوزه راهبردی و تعیین‌کننده برای امنیت ملی و رقابت بین‌المللی به رسمیت می‌شناسند.

* جاسوسی سایبری: هر سه کشور به طور گسترده از ابزارهای سایبری برای جمع‌آوری اطلاعات نظامی، سیاسی و اقتصادی از رقبای خود استفاده می‌کنند.

* توسعه دکترین‌های مدرن: هر سه در حال تطبیق دکترین‌های نظامی خود با واقعیت‌های جنگ‌های نوین هستند و بر اهمیت اطلاعات، هوشمندی و عملیات‌های چندحوزه‌ای تأکید دارند.

نقاط افتراق:

* تفاوت در رویکرد به بازدارندگی: بزرگترین تفاوت در مفاهیم بنیادین بازدارندگی نهفته است. رویکرد آمریکا مبتنی بر یک منطق پیشگیرانه و تهدید به مجازات است، در حالی که "کنترل بازتابی" روسیه بر دستکاری ذهن دشمن و "ویشه" چین بر ترکیبی از پیشگیری و اجبار فعالانه متمرکز است.

* میزان تهاجمی بودن در زمان صلح: روسیه و چین، هر دو، اقدامات تهاجمی در فضای اطلاعاتی و سایبری (مانند کمپین‌های اطلاعات نادرست یا نفوذ به زیرساخت‌ها) را به عنوان بخشی

از رقابت و بازدارندگی مستمر در زمان صلح می‌بینند. در مقابل، دکترین آمریکا این اقدامات را اغلب نقض هنجارهای بین‌المللی و مستلزم پاسخ می‌داند.

* اقتصاد به مثابه سلاح: چین به طور منحصربه‌فردی قدرت اقتصادی و پروژه‌های زیرساختی فناورانه (مانند جاده ابریشم دیجیتال) را با اهداف امنیتی و بازدارندگی خود گره زده است، امری که در رویکرد روسیه و آمریکا کمتر دیده می‌شود.

۳- آینده‌نگری: پیامدها و تحول دکترین‌های بازدارندگی در عصر هوش مصنوعی

جهان امنیتی کنونی در آستانه یک دگردیسی پارادایمیک قرار دارد که در کانون آن، تحول دکترین‌های امنیتی قدرت‌های بزرگ تحت تأثیر هوش مصنوعی است . این فناوری نه تنها یک ابزار نظامی جدید، بلکه به مثابه یک تقویت‌کننده قدرت عمل می‌کند که بنیادهای سنتی نظریه روابط بین‌الملل، به‌ویژه مفهوم بازدارندگی، را بازنویسی می‌نماید این دگرگونی به یک مسئله کلیدی در مطالعات استراتژیک تبدیل شده است و مفاهیم سنتی بازدارندگی نرم را نیز تحت تأثیر قرار می‌دهد (اسلامی و ملکی عزین آبادی.۱۳۹۷ :۱۸۸).

۳-۱. مدل‌های بازدارندگی مبتنی بر پیش‌بینی و یادگیری ماشین

بازدارندگی الگوریتمی، اساس خود را از منطق سنتی تلافی به سمت مدل‌های پیش‌بینی و انکار مبتنی بر داده منتقل می‌سازد هوش مصنوعی با ارائه سرعت بی‌نظیر در تحلیل داده‌ها، قابلیت‌های بی‌سابقه‌ای در حوزه نظامی ایجاد کرده که فرضیات سنتی بازدارندگی را به چالش می‌کشد (عباسی.۲۰۲۲ : ۵۸-۶۰).

سامانه‌های هوش مصنوعی و یادگیری ماشین می‌توانند حجم عظیمی از داده‌های غیرمتجانس (مانند تصاویر ماهواره‌ای، سیگنال‌های ارتباطی، و داده‌های مالی) را پردازش کرده و بینش‌های راهبردی را بسیار سریع‌تر از تحلیلگران انسانی تولید کنند. این توانایی‌ها به فرماندهان نظامی کمک می‌کند تا یک تصویر عملیاتی مشترک فوق‌العاده دقیق و درلحظه داشته باشند و امکان تصمیم‌گیری با کارایی بالا را در کسری از ثانیه فراهم می‌سازد (عباسی.۲۰۲۲ :۶۵-۶۶).

در این مدل نوین، بازدارندگی بر مبنای استفاده از داده‌های کلان استوار است تا نه تنها نیّات و قابلیت‌های خصمانه دشمن را شناسایی کند، بلکه با پیش‌بینی حرکت بعدی بازیگر متخاصم، امکان اقدام پیشگیرانه یا انکار مؤثر را فراهم سازد. هدف اصلی، پیش‌بینی نیّات راهبردی دشمن از طریق مدل‌سازی رفتارهای تاریخی و شناسایی الگوهای نامتعارف در جریان داده‌ها است (عباسی.۲۰۲۲ :۴۵). این تأکید بر «تشخیص قصد» به‌جای «تشخیص ظرفیت»، جوهره اصلی بازدارندگی مبتنی بر پیش‌بینی را شکل می‌دهد.

۲-۳. تهدیدات بازدارندگی دوگانه: هوش مصنوعی علیه انسان و توسط انسان

تهدیدات بازدارندگی در عصر الگوریتمی دارای ماهیتی دوگانه هستند؛ یعنی هم از خودمختاری سامانه‌های هوش مصنوعی (علیه انسان) و هم از سوءاستفاده انسان‌ها از این ابزارها (توسط انسان) پدید می‌آیند.

الف) تهدید ناشی از خودمختاری هوش مصنوعی (علیه انسان)

یکی از جدی‌ترین تهدیدات، توسعه تسلیحات خودمختار مرگبار است که انسان را به‌طور کامل از حلقه تصمیم‌گیری خارج می‌کند این سامانه‌ها قادرند بدون نظارت یا مداخله انسانی، اهداف را انتخاب کرده و با آن‌ها درگیر شوند، که این امر زمان واکنش مورد نیاز برای ارزیابی تهدید، مشورت‌های دیپلماتیک و کاهش تنش انسانی را از بین می‌برد (عباسی.۲۰۲۲: ۱۴۵).

حذف انسان از حلقه تصمیم‌گیری، پتانسیل تصمیم‌گیری‌های پرخطر و غیرقابل پیش‌بینی در زمان بحران را افزایش داده و به‌طور مستقیم خطر تشدید ناخواسته نزاع را تا سطح یک درگیری تمام‌عیار، افزایش می‌دهد. در دوران هوش مصنوعی، خطای انسانی جای خود را به خطای الگوریتمی می‌دهد که می‌تواند با سرعتی تصاعدی منجر به یک فاجعه راهبردی شود و دکترین‌های سنتی مبتنی بر عقلانیت و کنترل انسانی را تضعیف می‌کند.

ب) تهدید ناشی از سوءاستفاده هوش مصنوعی (توسط انسان)

مسئله سوگیری الگوریتمی نشان می‌دهد که سامانه‌های هوش مصنوعی، بازتاب‌دهنده تعصبات موجود در داده‌های آموزشی یا طراحی انسانی خود هستند. این سوگیری‌ها، که ریشه در داده‌های

آموزشـــی جانب‌دارانه دارند، می‌توانند در محیط نظامی موجب تصـــمیمات غیرعادلانه در مورد هدف‌گیری یا عملیات شـــوند و در ســـطح اجتماعی منجر به تشـــخیص غلط خطر برای گروه‌های خاص گردند (عزیزی و صلح چی. ۱۴۰۱. ۱۶).

این تهدید، چالش‌های جدی برای مفاهیم شـفافیت و پاسـخگویی در جنگ ایجاد می‌کند. در صـورت وقوع یک حادثه ناشـی از نقص در داده‌ها یا مدل‌سـازی‌های الگوریتمی، تعیین اینکه چه کســی (برنامه‌نویس، فرمانده، یا ســیاســت‌گذار) مســئولیت نهایی را بر عهده دارد، به یک معمای پیچیده حقوقی و اخلاقی تبدیل می‌شود. این فقدان پاسخگویی مشخص، خود می‌تواند بازدارندگی حقوقی و اخلاقی را تضعیف کند.

۳-۳. بازدارندگی متقارن و نامتقارن در فضای الگوریتمی

هوش مصـنوعی، مرزهای تفکیک‌شـده بازدارندگی متقارن و نامتقارن را از بین برده و فضـای جدیدی برای کنش‌های راهبردی ایجاد کرده است.

الف) چالش نامتقارن: ابهام در احراز هویت و بازدارندگی سایبری

در حوزه نامتقارن، حملات سـایبری و جنگ‌های هیبریدی که هوش مصـنوعی آن‌ها را تقویت کرده، اصـــلی‌ترین چالش را برای بازدارندگی مبتنی بر تلافی ایجاد می‌کنند. هوش مصـــنوعی با اسـتفاده از شـبکه‌های پنهان و بدافزارهای پیشـرفته، ابزار احراز هویت در حمله سـایبری را به شـدت پیچیده و پرابهام می‌سازد

این ابهام در انتســـاب، بازدارندگی مبتنی بر مجازات را خنثی می‌کند، زیرا طرف بازدارنده نمی‌تواند با اطمینان کامل، عامل حمله را شناسایی و تهدید به تلافی متناسب نمایدهمچنین، چالش حقوقی اینجا مطرح اسـت، زیرا عملیات سـایبری به‌سـختی در تعریف «حمله مسـلحانه» مطابق با ماده ۵۱ منشـور سـازمان ملل متحد قرار می‌گیرد و این امر، اعمال حق دفاع مشـروع و دکترین‌های پاسـخ متناسب را با موانع جدی روبرو می‌سازد (حسین نژاد. ۱۴۰۱. ۳۴).

در پاسـخ به این چالش، برخی محققان به مفهوم بازدارندگی نرم اشـاره کرده‌اند که بر اسـاس توانایی ایجاد ابهام اســـتراتژیک در ظرفیت‌های ســـایبری و همچنین افزایش قدرت نرم، در کنار بازدارندگی سخت عمل می‌کند (اسلامی و ملکی عزین آبادی.۱۳۹۷: ۸۸).

ب) تأثیر بر تقابل متقارن: فناوری‌های خودمختار و انبوه

در حوزه متقارن، هوش مصنوعی با توسعه سامانه‌های تسلیحاتی پیشرفته مانند فناوری گله توانمندی‌های بی‌سابقه‌ای در قدرت نظامی متعارف ایجاد می‌کند گله‌های پهپادی و رباتیک که توسط هوش مصنوعی هدایت می‌شوند، می‌توانند به صورت هماهنگ و با غلبه بر دفاع دشمن، اهداف را با دقتی بالا مورد اصابت قرار دهند. این امر دکترین‌های دفاع موشکی سنتی و مفاهیم حفاظت از دارایی‌های استراتژیک را به چالش می‌کشد و نیازمند بازنگری در ساختار نیروها و دکترین‌های متقارن است.

۴-۳. رقابت‌های تسلیحاتی مبتنی بر هوش مصنوعی و خطر بی‌ثباتی راهبردی

تحلیل تطبیقی دکترین‌های امنیتی قدرت‌های بزرگ (ایالات متحده، چین، و روسیه) نشان می‌دهد که گذار به بازدارندگی الگوریتمی (با تغییر منطق از تلافی به پیش‌بینی)، نه تنها یک تغییر ابزاری، بلکه یک عامل اساسی در تشدید بی‌ثباتی راهبردی در نظام بین‌الملل است. این رقابت شتابان که توسط قدرت‌هایی چون ایالات متحده، چین و روسیه دنبال می‌شود، به‌واسطه سه مکانیزم کلیدی، خطر محاسبات اشتباه و تشدید ناخواسته درگیری‌ها را به شکل معناداری افزایش می‌دهد.

برهم خوردن موازنه قوا: رویکردهای محرمانه و غیرشفاف مانند استراتژی «وِیشه» چین و تمرکز روسیه بر «کنترل بازتابی»، هوش مصنوعی را به ابزاری برای تغییر غیرمنتظره موازنه نظامی و اقتصادی به نفع مالک فناوری تبدیل می‌کند. از آنجا که توسعه این فناوری‌ها اغلب محرمانه و غیرشفاف است، طرف‌های مقابل قادر به ارزیابی دقیق قدرت یکدیگر نبوده و این عدم قطعیت، انگیزه برای مسابقه تسلیحاتی شتابان را افزایش می‌دهد. (فتاحی منش،رستمی.۱۴۰۲: ۴۲).

فشردگی زمان تصمیم‌گیری: ظهور دکترین‌هایی مانند «بازدارندگی یکپارچه» ایالات متحده که بر قابلیت‌های تصمیم‌گیری درلحظه تأکید دارد، سرعت بالای سامانه‌های الگوریتمی را به شدت افزایش می‌دهد. در یک بحران، این فشردگی زمانی، امکان لازم برای کاهش تنش و دیپلماسی انسانی را از بین می‌برد و احتمال اتخاذ تصمیمات شتاب‌زده بر اساس اصل «اگر استفاده نکنی، از دست می‌دهی» را افزایش داده و در نهایت، به تشدید سریع بحران و بی‌ثباتی می‌انجامد. (عباسی.۲۰۲۲: ۶۳)

مشکل جعبه سیاه و ابهام در قابلیت‌ها: عدم شفافیت در عملکرد الگوریتم‌های هوش مصنوعی، که به «مشکل جعبه سیاه» معروف است، به طور خاص در جنگ‌های شناختی روسیه و عملیات‌های سایبری چین که ابهام در انتساب حملات را افزایش می‌دهند، نمود می‌یابد. این ابهام ذاتی، اعتماد متقابل را در محیط راهبردی کاهش می‌دهد و سوءبرداشت‌ها، اشتباهات در ارزیابی نیّات، و نهایتاً بی‌اعتمادی عمیق را در میان رقبا افزایش داده و به چرخه باطل مسابقه تسلیحاتی دامن می‌زند. (ریاضی. ۱۴۰۲. ۲۳۸-۲۳۹).

نتیجه‌گیری

تحلیل حاضر نشان می‌دهد که ظهور و توسعه شتابان هوش مصنوعی، صرفاً به مثابه یک ابزار نوین در زرادخانه قدرت‌های بزرگ عمل نکرده، بلکه در حال ایجاد یک دگردیسی پارادایمیک در بنیادهای نظری و عملی امنیت بین‌الملل است. این پژوهش استدلال نمود که گذار از دکترین‌های سنتی به «بازدارندگی الگوریتمی»، منطق راهبردی حاکم بر روابط قدرت‌های بزرگ را متحول ساخته و آن را از «تلافی» به «پیش‌بینی» تغییر داده است. در این پارادایم نوین، سرعت تحلیل داده‌ها و خودمختاری سامانه‌ها، مؤلفه واکنش انسانی را که سنگ بنای بازدارندگی کلاسیک بود، به حاشیه رانده و رقابت امنیتی را وارد مرحله‌ای پیچیده و بی‌ثبات‌کننده کرده است.

بررسی تطبیقی دکترین‌های امنیتی ایالات متحده، جمهوری خلق چین و فدراسیون روسیه حاکی از آن است که هر یک از این قدرت‌ها، متناسب با فرهنگ راهبردی و اهداف ژئوپلیتیکی خود، در حال انطباق با این واقعیت نوین هستند. در پاسخ به این تحول، سه مدل متمرکز بر «بازدارندگی الگوریتمی» پدید آمده است: ایالات متحده با دکترین «بازدارندگی یکپارچه» در پی هم‌افزایی تمامی ابزارهای قدرت ملی است؛ چین در چارچوب «امنیت جامع ملی» و راهبرد «بازدارندگی هوشمند»، هوش مصنوعی را ابزاری کلیدی برای نیل به برتری فناورانه و تغییر مسالمت‌آمیز توازن قوا می‌انگارد؛ و روسیه نیز با تمرکز بر «کنترل بازتابی» و «جنگ شناختی» بر جبران ضعف نسبی خود در قدرت متعارف، به شکلی نامتقارن متمرکز است.

این تحولات برای ثبات راهبردی، پیامدهای عمیقی دارد. تشدید «مسابقه الگوریتمی» میان قدرت‌ها، به دلیل فشردگی زمان تصمیم‌گیری، افزایش ابهام در انتساب حملات سایبری، و امکان

تغییرات ناگهانی در موازنه قوا، خطر محاسبات اشتباه و تشدید ناخواسته درگیری‌ها را به شکل معناداری افزایش می‌دهد. علاوه بر این، ظهور تسلیحات خودمختار مرگبار و چالش‌هایی نظیر «سوگیری الگوریتمی»، ملاحظات جدی حقوقی و اخلاقی را در خصوص مسئولیت‌پذیری در جنگ و انطباق با حقوق بین‌الملل بشردوستانه مطرح می‌سازد. در چنین شرایطی، یک خلأ حکمرانی خطرناک میان سرعت پیشرفت فناوری و کندی فرآیندهای دیپلماتیک برای تدوین هنجارها و رژیم‌های نظارتی بین‌المللی به چشم می‌خورد.

در نهایت، آینده امنیت جهانی به نحوه مدیریت این فناوری تحول‌آفرین وابسته است. جامعه بین‌الملل و به‌ویژه قدرت‌های بزرگ، برای پیشگیری از یک رقابت تسلیحاتی افسارگسیخته و بی‌ثبات‌کننده، نیازمند تدوین یک چارچوب حکمرانی بین‌المللی هستند که شفافیت دکترین‌ها، ایجاد کانال‌های ارتباطی اضطراری و تضمین کنترل معنادار انسان بر سامانه‌های تسلیحاتی را در بر گیرد. در غیر این صورت، جهان در معرض ورود به عصری قرار خواهد گرفت که در آن، تصمیم برای جنگ و صلح، بیش از آنکه محصول خرد انسانی باشد، برآمده از منطق سرد و شکننده الگوریتم‌های غیرپاسخگو و غیرقابل پیش‌بینی خواهد بود.

فهرست منابع

احمدی، علی؛ زرگر، افشین؛ و آدمی، علی. (۱۴۰۱). نقش فناوریهای نوظهور در امنیت و قدرت ملی کشورها: فرصت و تهدیدها. فصلنامه مطالعات بین‌المللی، ۱۸(۴)، ۱۵۹-۱۳۹.

آذین، صدیقه؛ هدایتی شهیدانی، مهدی؛ و جانسیز، احمد. (۱۴۰۳). هوش مصنوعی و ثبات استراتژیک: آموزه‌ای ادراکی در زمینه توسعه ابعاد نظامی هوش مصنوعی در کشورهای آمریکا و روسیه. فصلنامه علمی مطالعات استراتژیک آمریکا، ۴(۱۵)، ۲۷-۱.

اسلامی، م.، و ملکی عزین آبادی، ر. ا. (۱۳۹۷). تحول مفهوم بازدارندگی در پرتو برجستگی امور معنایی در روابط بین‌الملل. دو فصلنامه علمی – پژوهشی مطالعات قدرت نرم، ۸)۱۹.(

پورحسن، ن. (۱۴۰۱). تحول در سیاست تحریمی آمریکا از ابزار بازدارندگی تا جنگ با تأکید بر رویکردهای رسانه‌ای. پژوهشنامه رسانه بین‌الملل، ۷(۱)، ۳۱۱-۲۸۵.

حسین نژاد، ک. (۱۴۰۱). "عملیات سایبری و حمله مسلحانه در معنای ماده ۵۱ منشور سازمان ملل متحد". در: مجموعه مقالات سمپوزیوم تأثیر علم و فناوری‌های نوین بر صلح و امنیت بین‌المللی، انجمن ایرانی مطالعات سازمان ملل متحد.

دفتر اطلاعات شـــورای دولت جمهوری خلق چین. (۲۰۱۹). دفاع ملی چین در عصـــر جدید. (ترجمه شـــورای راهبردی روابط خارجی).

دهقانی، ع. ا. (۱۳۹۶). بازدارندگی ســـایبری در امنیت نوین جهانی: تهدید ســـایبری روســـیه و چین علیه زیر ساختهای حیاتی آمریکا. فصلنامه رهیافتهای سیاسی و بین المللی، ۸(۴)، ۱۴۷-۱۲۱.

رضـــاپور، د. (۱۴۰۳). همکاری چین با آســـیای مرکزی با تأکید بر هوش مصـــنوعی. مطالعات اوراســـیای مرکزی، ۱۷(۱)، ۱۸۷-۱۵۷.

ریاضـی، و. (۱۴۰۲). "الگوی بازدارندگی راهبردی سـازمان‌های نظامی جمهوری اسـلامی ایران در محیط امنیتی." فصلنامه علمی مطالعات بین رشته‌ای دانش راهبردی، ۱۳(۵۰)، ۲۵۲-۲۲۵.

ســـجادی، ســـید عبدالقیوم. (۱۴۰۴). هوش مصـــنوعی و تحول ماهیت امنیت بین‌الملل. فصـــلنامه علمی- تحقیقی مطالعات سیاسی و بین‌المللی، ۲(۵)، ۴۸-۲۵.

ســـیمبر، ر.، و فصـــیحی مقدم لاکانی، س. (۱۴۰۴). اهداف گســـترش هوش مصـــنوعی چین در روابط بین الملل (۲۰۰۶-۲۰۲۴). سیاست جهانی، ۱۴(۱)، ۳۳-۷.

عباسی، ع. (۲۰۲۲). کاربردهای نوین هوش مصنوعی.

عزیزی، ا.، و صلح چی، س. (۱۴۰۱). "هوش مصنوعی و ارزش‌های دموکراتیک". در: مجموعه مقالات سمپوزیوم تأثیر علم و فناوری‌های نوین بر صلح و امنیت بین‌المللی، انجمن ایرانی مطالعات سازمان ملل متحد.

فتاحی منش، م.، و رســـتمی، ف. (۱۴۰۲). تأثیر فناوری‌های هوش مصـــنوعی بر آینده موازنه قوا در غرب آســـیا. فصلنامه غرب آسیا، ۱(۲)، ۵۴-۳۶.

قاسـمی، فرهاد. (۱۳۹۱). بازسـازی مفهومی نظریه بازدارندگی منطقه‌ای و طراحی الگوهای آن بر اسـاس نظریه‌های چرخه قدرت و شبکه. فصلنامه راهبرد دفاعی، ۱۰(۳۸)، ۱۱۸-۹۱.

قوام، ســـید عبدالعلی. (۱۴۰۰). روابط بین‌الملل: نظریه‌ها و رویکردها. تهران: ســـازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).

قاسـمی، فرهاد. (۱۳۹۵). سـیسـتم‌های پیچیده و آشـوبی: الگوی وابسـتگی حسـاس، بازدارندگی و جنگ. سـیاسـت جهانی، ۵(۳)، ۹۲-۶۳.

قنبری، س.، و خانی، ح. (۱۳۹۹). بازدارندگی سایبری روسیه از منظر اروپا. فصلنامه آسیای مرکزی و قفقاز، ۱۱۱، ۱۵۶-۱۱۷.

مجیدی، محمدرضـــا؛ و بایزیدی، رحیم. (۱۴۰۳). هوش مصـــنوعی و تحول پارادایمیک در نظریه و عمل روابط بین‌الملل. پژوهش‌های روابط بین‌الملل، ۱۴(۳)، ۴۹-۳۱.

Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. Strategic Studies Quarterly, 12(3), 70–89.

Bijlsma, T. (2021). What's on the Human Mind? Decision Theory and Deterrence. In F. Osinga & T. Sweijs (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2020 (pp. 437–454). T.M.C. Asser Press.

Cheng, D. (2021). An Overview of Chinese Thinking About Deterrence. In F. Osinga & T. Sweijs (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century-Insights from Theory and Practice (pp. 177–200). T.M.C. ASSER PRESS.

Ducheine, P., & Pijpers, P. (2021). The Missing Component in Deterrence Theory: The Legal Framework. In F. Osinga & T. Sweijs (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2020 (pp. 475–500). T.M.C. Asser Press.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79.

Filippidou, A. (2020). Deterrence: Concepts and Approaches for Current and Emerging Threats. In A. Filippidou (Ed.), ”eterrence. Advanced Sciences and Technologies for Security Applications (pp. 1–18). Springer.

Haney, B. S. (2020). Applied Artificial Intelligence in Modern Warfare and National Security Policy. Hastings Science and Technology Law Journal, 11(1), 61-98.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. Journal of Strategic Security, 4(2), 1–24.

Hoadley, D. S., & Lucas, N. J. (2018). Artificial Intelligence and National Security (CRS Report No. R45178). Congressional Research Service.

Khan, M. S., Rana, F. A., & Irfan, Z. (2025). Hybrid Warfare in the “igital Age: Cyberpower, AI, and the Future of Global Security. Advance Social Science Archive Journal, 4(1), 3050–3065.

Kolton, M. (2017). Interpreting China’s Pursuit of Cyber Sovereignty and its Views on Cyber “eterrence. The Cyber Defense Review, 2(1), 119–154.

Long, A. (2015). ”eterrence: The state of the field. New York University Journal of International Law and Politics, 47(2), 357-377.

Renne, T. (2019). The AI Revolution in Deterrence Theory: 10 Groundbreaking Concepts Reshaping Global Security. Chetar Journal, 15(4), 1-18.

Sayler, K. M. (2020). Artificial Intelligence and National Security (CRS Report No. R45178). Congressional Research Service.

Schmidt, E. (2022). AI, Great Power Competition & National Security. Dædalus, 151(2), 288–298.

The Media Ecology and Strategic Analysis Group. (2023). UNITED STATES DETERRENCE POLICY: 1944-PRESENT: Literature Review. Oklahoma State University.

Wilner, A., & Babb, C. (2021). New Technologies and Deterrence: Artificial Intelligence and Adversarial Behaviour. In F. Osinga & T. Sweijs (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century-Insights from Theory and Practice (pp. 401–417). T.M.C. ASSER PRESS.

Yu, C. (2024). The AI Revolution in Deterrence Theory: 10 Groundbreaking Concepts Reshaping Global Security. CHETAR Journal, 17(4), 1-17.

Zilincik, S., & ”uyvesteyn, I. (2021). Deterrence: A Continuation of Emotional Life with the Admixture of Violent Means. In F. Osinga & T. Sweijs (Eds.), NL ARMS Netherlands Annual Review of Military Studies 2020 (pp. 455–474). T.M.C. Asser Press.