DOI: 10.22034/isj.2026.601039.2514

International Studies Journal (ISJ)
Vol. 22, No. 4 (88), Spring 2026
Reseived Date: 2025/7/25
Accept Date: 2026/3/19
Article Type: Original Research
PP: 81-101

فصلنامه مطالعات بین‌المللی
سال ۲۲، شماره ٤ (۸۸)، بهار ١٤٠٥
تاریخ دریافت: ١٤٠٤/٥/٣
تاریخ پذیرش: ١٤٠٤/١٢/٢٨
نوع مقاله: علمی- پژوهشی
صفحات: ١٠١-٨١

بازدارندگی شناختی؛ رسانه، هوش مصنوعی و تحول مفهوم بازدارندگی در روابط بین‌الملل

دکتر مهدی عباسی*

This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

چکیده

گسترش رسانه‌های شبکه‌ای، عملیات اطلاعاتی و کاربردهای فزاینده هوش مصنوعی، محیط بازدارندگی را دگرگون کرده و فرایندهای ادراک، ارزیابی ریسک و تصمیم‌گیری حریف را به بخشی از رقابت راهبردی تبدیل ساخته است. خلأ اصلی ادبیات، فقدان چارچوبی منسجم برای پیوند بازدارندگی، جنگ شناختی و محیط رسانه‌ای ـ الگوریتمی است. پرسش اصلی پژوهش آن است که رسانه‌های شبکه‌ای و هوش مصنوعی چگونه با تغییر محیط ادراکی ـ تصمیمی، بازدارندگی شناختی را به لایه‌ای مکمل در بازدارندگی چندحوزه‌ای تبدیل می‌کنند؟ پژوهش با تحلیل مفهومی انتقادی و بازخوانی هدفمند ادبیات نظری منتشرشده از ۲۰۰۱ تا اکتبر ۲۰۲۶ در حوزه‌های بازدارندگی، بازدارندگی سایبری، جنگ شناختی، عملیات اطلاعاتی، هوش مصنوعی و ثبات راهبردی انجام شده است. سطح تحلیل، تعامل راهبردی دولت‌ها با تمرکز بر فرایندهای ادراکی و تصمیمی رهبران و نهادهای تصمیم‌گیر است و پژوهش محدود به حوزه جغرافیایی خاصی نیست. بازدارندگی شناختی به تغییر محاسبات حریف درباره احتمال موفقیت، هزینه، ریسک و پیامدهای عملیات شناختی اشاره دارد. یافته‌ها پنج سازوکار انکار و تاب‌آوری، کشف و انتساب، تحمیل هزینه، سلب مشروعیت و پیام‌رسانی راهبردی را مشخص می‌کنند. هوش مصنوعی از طریق افزایش سرعت تحلیل، شخصی‌سازی پیام، کشف الگو و تقویت انتساب می‌تواند این سازوکارها را فعال کند و در مقابل، با ابهام الگوریتمی، سوگیری خودکارسازی و فشردگی زمان تصمیم، کارکرد آنها را مختل سازد. بر این اساس، تحول بازدارندگی در گسترش محیط، ابزارها و سازوکارهای اثرگذاری بر تصمیم حریف قابل مشاهده است.

کلیدواژگان

بازدارندگی شناختی، هوش مصنوعی، رسانه‌های شبکه‌ای، جنگ شناختی، بازدارندگی چندحوزه‌ای.

* استادیار، گروه علوم سیاسی، دانشگاه پیام نور، تهران، ایران./ نویسنده مسئول/ ایمیل: abbasi_m@pnu.ac.ir

Article Link: https://www.isjq.ir/article_256210.html
Online ISSN: 2676-5136 Print ISSN: 2045-1735

مقدمه

بازدارندگی از مفاهیم مطالعات امنیتی و راهبردی است و بر منصرف‌کردن حریف از اقدام خصمانه از طریق اثرگذاری بر محاسبات او استوار است. با گسترش رسانه‌های شبکه‌ای و هوش مصنوعی، این محاسبات در فضایی شکل می‌گیرند که سرعت توزیع اطلاعات، شخصی‌سازی پیام، دستکاری ادراک، ابهام در انتساب و اتکا به سامانه‌های الگوریتمی افزایش یافته است. مسئله صرفاً افزوده‌شدن ابزارهای جدید نیست؛ رسانه و هوش مصنوعی بر تولید، توزیع و تفسیر اطلاعات و فرایند تصمیم اثر می‌گذارند. ازاین‌رو، «تحول» در این پژوهش به معنای جایگزینی بازدارندگی کلاسیک نیست، بلکه به تغییر در موضوع، ابزارها و محیط شکل‌گیری تصمیم اشاره دارد.

پرسش اصلی پژوهش آن است که رسانه‌های شبکه‌ای و هوش مصنوعی چگونه با تغییر محیط ادراکی ـ تصمیمی، بازدارندگی شناختی را به لایه‌ای مکمل در بازدارندگی چندحوزه‌ای تبدیل می‌کنند؟ فرضیه اصلی آن است که افزایش قابلیت‌های رسانه‌ای و هوش مصنوعی به‌خودی‌خود موجب تقویت بازدارندگی نمی‌شود؛ اثر بازدارنده زمانی شکل می‌گیرد که این قابلیت‌ها با کاهش احتمال موفقیت عملیات شناختی، افزایش امکان کشف و انتساب و انتقال معتبر هزینه‌های اقدام، محاسبات حریف را تغییر دهند. در مقابل، ابهام الگوریتمی، فشردگی زمان تصمیم و کاهش کنترل انسانی می‌توانند همین ظرفیت‌ها را به عامل بی‌ثباتی تبدیل کنند. بازدارندگی شناختی با جنگ شناختی ـ متمرکز بر اثرگذاری بر فرایندهای شناختی ـ و بازدارندگی سایبری ـ معطوف به مهار رفتار خصمانه در حوزه سایبر ـ متفاوت است.

پژوهش حاضر با رویکرد کیفی، مرور هدفمند ادبیات و تحلیل مفهومی ـ تطبیقی انجام شده است. دامنه زمانی منابع از ۲۰۰۱ تا اکتبر ۲۰۲۶ در نظر گرفته شده است؛ انتخاب سال ۲۰۰۱ از آن روست که از آغاز دهه ۲۰۰۰ بحث درباره امکان و محدودیت‌های بازدارندگی در محیط اطلاعاتی و سایبری به‌صورت مشخص وارد ادبیات امنیتی شد و امتداد بررسی تا اکتبر ۲۰۲۶ امکان پوشش تحولات جدید جنگ شناختی و هوش مصنوعی را فراهم می‌کند. منابع بر اساس ارتباط مستقیم با بازدارندگی، بازدارندگی سایبری، جنگ شناختی، عملیات اطلاعاتی و هوش مصنوعی انتخاب شدند. تحلیل در سه مرحله شامل استخراج مؤلفه‌های مؤثر بر ادراک و تصمیم حریف، مقایسه سازوکارهای بازدارندگی و ترکیب مفهومی یافته‌ها انجام شد. واحد تحلیل، گزاره‌ها و استدلال‌های نظری مرتبط با تغییر محاسبات راهبردی حریف بود. هدف پژوهش، تبیین جایگاه، سازوکارها و محدودیت‌های بازدارندگی شناختی در محیط امنیتی معاصر است.

۱-پیشینه پژوهش

بخشی از ادبیات جدید بازدارندگی به پیامدهای تحول فناوری و گسترش حوزه‌های غیرنظامی منازعه پرداخته است. زالا (Zala, 2024) با بررسی تأثیر هوش مصنوعی بر ثبات راهبردی استدلال می‌کند که ورود سامانه‌های هوشمند به فرایندهای هشدار، فرماندهی و تصمیم‌گیری می‌تواند ظرفیت بازدارندگی را افزایش دهد، اما فشردگی زمان تصمیم و نگرانی از حمله پیش‌دستانه، هم‌زمان احتمال

بی‌ثباتی راهبردی را نیز بالا می‌برد. هدلینگ و اُردن نیز در بررسی عملیات اطلاعات نادرست، «انتساب» عامل خارجی را واجد ظرفیت بازدارنده می‌دانند؛ زیرا افشا می‌تواند امکان تحمیل هزینه سیاسی و حیثیتی و سلب مشروعیت از عامل عملیات را فراهم کند (Hedling & Ördén, 2025: 969–975). این مطالعات نشان می‌دهند که فناوری و اطلاعات وارد محاسبات بازدارندگی شده‌اند، اما چگونگی پیوند این تحولات با محیط شناختی و فرایند تصمیم‌گیری همچنان نیازمند صورت‌بندی دقیق‌تری است.

بخش دیگری از پژوهش‌ها تحول محیط اطلاعاتی و ظهور جنگ شناختی را بررسی کرده‌اند. دپّه و شال (Deppe & Schaal, 2024) با تحلیل چارچوب جنگ شناختی ناتو، کانون این نوع منازعه را فرایندهای ادراک، داوری و تصمیم‌گیری انسان می‌دانند. رحیمی (۱۴۰۳) جنگ شناختی را در پیوند با تهدیدهای ترکیبی بررسی کرده و نقش کلان‌داده، گردش اطلاعات، سواد رسانه‌ای و تفکر انتقادی را برجسته ساخته است. محجوب و همکاران (۱۴۰۵) نیز تهدیدهای شناختی را در سطوح فردی، فناوری‌محور و فرایندمحور تحلیل کرده و سوگیری شناختی، اضافه‌بار اطلاعاتی، هوش مصنوعی و تحلیل کلان‌داده را از عوامل ایجاد آسیب‌پذیری شناختی برشمرده‌اند. برآیند این دسته از مطالعات، آشکارشدن اهمیت حفاظت از فرایند ادراک و تصمیم است؛ مسئله‌ای که می‌تواند مستقیماً با منطق بازدارندگی پیوند یابد.

دسته دیگری از مطالعات بر رابطه فناوری‌های دیجیتال با آسیب‌پذیری و تاب‌آوری شناختی تمرکز دارند. فردهایم و پامنت (Fredheim & Pamment, 2025) توضیح می‌دهند که مدل‌های زبانی بزرگ ظرفیت تولید محتوای اقناعی، شخصی‌سازی پیام و اجرای عملیات نفوذ را افزایش می‌دهند و هم‌زمان می‌توانند برای شناسایی و مقابله با این عملیات به کار روند. طالبی و محجوب عشرت‌آبادی (۱۴۰۳) نیز «زیست‌بوم آمادگی شناختی دفاع سایبری» را بر پایه تعامل انسان، فناوری و فرایندهای سایبرشناختی تبیین کرده‌اند. اهمیت این مطالعات برای بحث حاضر در نشان‌دادن ماهیت دوگانه فناوری است؛ فناوری می‌تواند هم منبع آسیب‌پذیری شناختی و هم بخشی از ظرفیت مقاومت و بازدارندگی باشد.

در مطالعات داخلی، وحدانی‌نیا وحدانی‌نیا (۱۴۰۴) با ارائه مدلی سناریومحور برای سیاست‌گذاری دفاع شناختی ایران، پیوند میان سطوح راهبردی، نهادی، رسانه‌ای و فناورانه را مورد توجه قرار داده‌اند. این رویکرد، دفاع شناختی را از سطح ابزارهای رسانه‌ای فراتر می‌برد و آن را در قالب مجموعه‌ای از ظرفیت‌های سازمانی و راهبردی صورت‌بندی می‌کند. با وجود این، مسئله اصلی آن سیاست‌گذاری دفاع شناختی در سطح ملی است و نسبت این ظرفیت‌ها با تحول مفهوم بازدارندگی در روابط بین‌الملل مستقیماً موضوع پژوهش قرار نگرفته است.

پراکندگی این ادبیات میان مطالعات بازدارندگی، جنگ شناختی و هوش مصنوعی پیامد نظری مشخصی دارد: هنوز به‌روشنی معلوم نیست قابلیت‌های رسانه‌ای و الگوریتمی تحت چه شرایطی محاسبات حریف را تغییر می‌دهند، چه زمانی به بازدارندگی منجر می‌شوند و در چه شرایطی خود می‌توانند بی‌ثباتی را افزایش دهند. این گسست، قدرت تبیینی ادبیات بازدارندگی را در مواجهه با

منازعات چندحوزه‌ای و شناختی محدود می‌کند. پژوهش حاضر با تمرکز بر این مسئله، سازوکارهای پیونددهنده محیط رسانه‌ای ـ الگوریتمی با ادراک، محاسبه ریسک و تصمیم حریف را در قالب مفهوم بازدارندگی شناختی بررسی می‌کند.

۲- چارچوب مفهومی پژوهش

بازدارندگی در این پژوهش به فرایندی راهبردی اطلاق می‌شود که طی آن یک بازیگر با تأثیرگذاری بر محاسبات طرف مقابل، می‌کوشد او را از انجام یا ادامه اقدام خصمانه منصرف کند. این تأثیرگذاری از طریق افزایش هزینه مورد انتظار، کاهش احتمال موفقیت یا افزایش ادراک مخاطره صورت می‌گیرد. ادراک و تصمیم‌گیری از ابتدا در منطق بازدارندگی حضور داشته‌اند؛ تحول موردنظر این پژوهش در «ورود ادراک» نیست، بلکه در دگرگونی شرایطی است که محاسبه بازدارنده در آن انجام می‌شود. میانجی‌گری الگوریتمی، سرعت گردش اطلاعات، شخصی‌سازی پیام و ابهام در منشأ و اعتبار داده‌ها، اتکا به مفروضات عقلانیت باثبات و محاسبه‌پذیری نسبتاً روشن هزینه ـ فایده را دشوارتر کرده و عدم‌قطعیت را به درون فرایند تصمیم منتقل کرده‌اند. ازاین‌رو، تحول بازدارندگی شناختی به تغییر محیط و سازوکارهای شکل‌گیری محاسبات حریف مربوط است. مزر نیز بازدارندگی را فرایندی برای شکل‌دهی به انگیزه‌ها، برداشت‌ها و محاسبات مهاجم بالقوه می‌داند (Mazarr, 2018: 2–7).

«محیط اطلاعاتی ـ شناختی»[1] فضایی است که در آن اطلاعات تولید، توزیع، دریافت و تفسیر می‌شود و بر شکل‌گیری برداشت و تصمیم اثر می‌گذارد. در این چارچوب، رسانه‌های نوین عمدتاً به رسانه‌های شبکه‌ای[2] و پلتفرم‌های دیجیتال اطلاق می‌شوند که تولید و توزیع محتوا در آنها در تعامل میان کاربران، پلتفرم‌ها و الگوریتم‌ها صورت می‌گیرد. شخصی‌سازی، الگوریتم‌های توصیه‌گر، داده‌های رفتاری و بازنشر شبکه‌ای می‌توانند میزان دیده‌شدن، اعتبار و تفسیر پیام را تغییر دهند. ازاین‌رو، رسانه بخشی از محیط شکل‌گیری محاسبات حریف است. در همین محیط، کشف و انتساب عملیات به عامل خارجی نیز می‌تواند ناشناس‌ماندن مهاجم را دشوار و امکان تحمیل هزینه سیاسی، حقوقی و حیثیتی را فراهم کند (Hedling & Ördén, 2025: 969-975).

«جنگ شناختی»[3] به اقداماتی اشاره دارد که نحوه دریافت، تفسیر و پردازش اطلاعات و در نهایت نگرش و رفتار افراد و تصمیم‌گیرندگان را هدف قرار می‌دهند. فناوری‌های دیجیتال، شبکه‌های اجتماعی و داده‌های انبوه، امکان شناسایی آسیب‌پذیری‌های شناختی و هدف‌گیری دقیق‌تر مخاطبان را افزایش داده‌اند (Deppe & Schaal, 2024: 3-6). «تاب‌آوری شناختی»[4] در این مقاله خود بازدارندگی محسوب نمی‌شود، بلکه زمانی با منطق بازدارندگی پیوند می‌یابد که پیشاپیش احتمالِ موفقیت عملیات شناختی را کاهش دهد و محاسبات مهاجم را درباره امکان دستیابی به هدف تغییر

---

1. Informational-Cognitive Environment
2. Networked Media
3. Cognitive Warfare
4. Cognitive Resilience

دهد. بنابراین، کارکرد بازدارنده آن در «انکار موفقیت مورد انتظار» است، نه صرفاً بازیابی پس از وقوع حمله. اُردن نیز ذهن و فرایندهای شناختی انسان را در ادبیات جدید جنگ شناختی بخشی از محیط امنیتی و در معرض آسیب‌پذیری می‌داند (Ördén, 2024: 610–615).

هوش مصنوعی در این پژوهش به قابلیت‌های محاسباتیِ تحلیل داده، شناسایی الگو، تولید محتوا، پیش‌بینی و پشتیبانی تصمیم اشاره دارد. در حوزه شناختی، این قابلیت‌ها تولید محتوای مصنوعی، پروفایل‌سازی رفتاری[1] شخصی‌سازی پیام و عملیات نفوذ را تسهیل می‌کنند و در سوی دفاعی برای کشف نفوذ، تحلیل تهدید و افزایش آگاهی موقعیتی به کار می‌روند. پیوند هوش مصنوعی با رسانه‌های شبکه‌ای، سرعت، مقیاس و دقت هدف‌گیری را افزایش داده و هم‌زمان عدم‌قطعیت درباره منشأ، اعتبار و تفسیر اطلاعات را تشدید می‌کند. ازاین‌رو، هوش مصنوعی می‌تواند با تقویت کشف و انکار، ظرفیت بازدارندگی را افزایش دهد یا با فشرده‌کردن زمان تصمیم، کاهش نظارت انسانی و وابستگی به خروجی الگوریتمی، احتمال سوءبرداشت و تشدید بحران را بالا ببرد (Zala, 2024: 155–159).

بر پایه این مفاهیم، «بازدارندگی شناختی» فرایندی راهبردی است که با کاهش احتمال موفقیت عملیات شناختی و افزایش احتمال کشف، هزینه و ریسک ادراک‌شده، انگیزه اقدام خصمانه را کاهش می‌دهد. برآیند ترکیب ادبیات بازدارندگی، بازدارندگی سایبری و جنگ شناختی، پنج سازوکار انکار و تاب‌آوری، کشف و انتساب، تحمیل هزینه، سلب مشروعیت و پیام‌رسانی راهبردی است. این طبقه‌بندی، صورت‌بندی تحلیلی نویسندگان است و از چارچوب واحدی اقتباس نشده است. بازدارندگی شناختی نیز لایه‌ای مکمل در بازدارندگی چندحوزه‌ای محسوب می‌شود.

کاربرد این چارچوب در آزمون فرضیه، بررسی تأثیر رسانه‌های شبکه‌ای و هوش مصنوعی بر محیط اطلاعاتی ـ شناختی، ادراک حریف از هزینه، ریسک و احتمال موفقیت و در نهایت تصمیم و رفتار اوست. فرضیه زمانی حمایت می‌شود که این تغییرات، از طریق سازوکارهای پنج‌گانه، محاسبات حریف را تحت تأثیر قرار دهند؛ بدون آنکه بازدارندگی شناختی جایگزین بازدارندگی کلاسیک شود.

[1]. Behavioral Profiling



شکل ۱- مدل مفهومی بازدارندگی شناختی در عصر رسانه و هوش مصنوعی

Figure 1. Conceptual Model of Cognitive Deterrence in the Age of Media and Artificial Intelligence

منبع: (نویسنده، ۱۴۰۴)؛(Source: (Author, 2026

۳- تاریخچه موضوع

مفهوم بازدارندگی در روابط بین‌الملل عمدتاً در بستر رقابت هسته‌ای جنگ سرد شکل گرفت و بر تهدید معتبر به تحمیل هزینه و تأثیرگذاری بر محاسبات حریف استوار بود. با این حال، بازدارندگی از آغاز ماهیتی ادراکی داشت و موفقیت آن به برداشت طرف مقابل از توانایی، اراده و اعتبار تهدید وابسته بود (Mazarr, 2018: 2-7). با گسترش تهدیدهای سایبری و اطلاعاتی، بازدارندگی از حوزه صرفاً نظامی فراتر رفت و حفاظت از شبکه‌های اطلاعاتی و فرایندهای تصمیم‌گیری اهمیت یافت. ظهور جنگ شناختی و سپس هوش مصنوعی این تحول را تشدید کرد؛ به‌گونه‌ای که ادراک، اعتماد و رفتار به اهداف رقابت راهبردی تبدیل شدند (Deppe & Schaal, 2024: 1-6). در این محیط، «بازدارندگی شناختی» ناظر بر تأثیرگذاری بر ادراک ریسک، محاسبات و تصمیم حریف است.

٤- بازآرایی منطق بازدارندگی در محیط شناختی ـ الگوریتمی

در بازدارندگی کلاسیک، هدف اصلی منصرف‌کردن حریف از اقدام خصمانه از طریق کاهش

احتمال موفقیت یا افزایش هزینه مورد انتظار است. تحول موردنظر این پژوهش در کنارگذاشتن این منطق نیست، بلکه در تغییر چهار مؤلفه آن رخ می‌دهد: موضوع اثرگذاری، ابزار، محیط و الگوی تصمیم. در محیط شناختی ـ الگوریتمی، موضوع اثرگذاری از رفتار نهایی حریف به شرایطی گسترش می‌یابد که محاسبه راهبردی او در آن شکل می‌گیرد؛ ابزارها علاوه بر تهدید و پیام‌رسانی متعارف، شامل رسانه‌های شبکه‌ای، داده‌های رفتاری و قابلیت‌های هوش مصنوعی می‌شوند؛ محیط تصمیم تحت میانجی‌گری پلتفرم‌ها و الگوریتم‌ها قرار می‌گیرد؛ و محاسبه هزینه ـ فایده نیز در شرایطی از عدم‌قطعیت، فشار زمانی و شخصی‌سازی اطلاعات انجام می‌شود. بنابراین، فناوری به‌خودی‌خود منشأ تحول نیست؛ نقش آن از آنجا ناشی می‌شود که قابلیت دیده‌شدن، اعتبار، سرعت، هدف‌گیری و تفسیر اطلاعات را تغییر می‌دهد و از این طریق محیط تصمیم را بازآرایی می‌کند.

بر همین مبنا، بازدارندگی شناختی با مفاهیم مجاور یکسان نیست. بازدارندگی سایبری، رفتار خصمانه در حوزه سایبر را موضوع اصلی مهار قرار می‌دهد و بازدارندگی چندحوزه‌ای بر هماهنگی پاسخ‌ها در حوزه‌های مختلف تأکید دارد؛ معیار متمایزکننده بازدارندگی شناختی، «موضوع مستقیم اثرگذاری» است: شرایط ادراکی و تصمیمی‌ای که حریف بر اساس آنها احتمال موفقیت، هزینه، ریسک و پیامدهای اقدام را محاسبه می‌کند. ازاین‌رو، ابزارهای سایبری، رسانه‌ای و هوش مصنوعی می‌توانند در خدمت بازدارندگی شناختی قرار گیرند، اما هیچ‌یک به‌تنهایی معادل آن نیستند.

نوع بازدارندگی	موضوع مستقیم اثرگذاری	ابزار غالب	ویژگی متمایزکننده
بازدارندگی کلاسیک	تصمیم حریف درباره اقدام نظامی	انکار، مجازات و تهدید معتبر	تغییر محاسبه هزینه ـ فایده
بازدارندگی سایبری	رفتار خصمانه در فضای سایبر	دفاع سایبری، انتساب و پاسخ متقابل	تمرکز بر یک حوزه عملیاتی
بازدارندگی چندحوزه‌ای	رفتار حریف در چند حوزه متصل	ترکیب ابزارهای نظامی، سایبری، اقتصادی و اطلاعاتی	هماهنگی میان حوزه‌های پاسخ
بازدارندگی شناختی	شرایط ادراکی و تصمیمی حریف	رسانه، داده، انتساب، پیام‌رسانی و هوش مصنوعی	اثرگذاری بر نحوه شکل‌گیری محاسبه راهبردی

جدول ۱- تمایز بازدارندگی کلاسیک، سایبری، چندحوزه‌ای و شناختی

Table 1– Distinctions between classical, cyber, multi-domain, and cognitive deterrence

منبع: (نویسنده، ۱۴۰۴)؛Source: (Author, 2026)

٤-١- از عقلانیت مفروض به ادراک و چارچوب تصمیم

تحلیل منابع نشان می‌دهد که تحول شناختی بازدارندگی به معنای کشف اهمیت ادراک نیست؛ ادراک همواره بخشی از بازدارندگی بوده است. تغییر اصلی در آن است که محیط معاصر، خودِ

فرایند شکل‌گیری ادراک و محاسبه را به موضوع مستقیم رقابت تبدیل کرده است. در الگوهای کلاسیک، فرض بر آن بود که بازیگر پس از دریافت پیام بازدارنده، توان و اراده طرف مقابل را ارزیابی و درباره هزینه و منفعت اقدام تصمیم‌گیری می‌کند. در محیط رسانه‌ای ـ الگوریتمی، این ارزیابی پیش از رسیدن به مرحله تصمیم تحت تأثیر انتخاب و برجسته‌سازی اطلاعات، شخصی‌سازی محتوا، سرعت گردش روایت‌ها و ابهام درباره منشأ و اعتبار داده‌ها قرار می‌گیرد. ازاین‌رو، آنچه دگرگون شده صرفاً محتوای پیام بازدارنده نیست، بلکه شرایط تولید و پردازش آن محاسبه است.

تحلیل شناختی بریجیکیان نشان می‌دهد که تصمیم‌گیرندگان هزینه و منفعت را مستقل از زمینه ارزیابی نمی‌کنند؛ نقطه مرجع، ادراک سود یا زیان و میزان پذیرش ریسک بر واکنش آنها به تهدید اثر می‌گذارد. بازیگری که وضعیت موجود را در حوزه زیان ادراک می‌کند، ممکن است در برابر افزایش فشار به‌جای عقب‌نشینی، آمادگی بیشتری برای پذیرش مخاطره پیدا کند. در نتیجه، افزایش شدت تهدید الزاماً رابطه‌ای خطی با افزایش بازدارندگی ندارد (Berejikian, 2002: 165–175). اهمیت این استدلال برای پژوهش حاضر در آن است که محیط رسانه‌ای ـ الگوریتمی می‌تواند بر همان نقطه مرجع، ادراک زیان و ارزیابی ریسک اثر بگذارد و در نتیجه محاسبه‌ای را تغییر دهد که تصمیم بازدارنده بر آن استوار است.

بریجیکیان و جاستوان نیز نشان می‌دهند که اثر تهدید به ویژگی‌های ادراکی و گرایش مخاطب به پذیرش ریسک وابسته است؛ بنابراین، سطح واحدی از اعتبار یا هزینه برای همه بازیگران پیامد مشابهی ندارد (Berejikian & Justwan, 2019: 25–30). برآیند این امر آن است که بازدارندگی شناختی از «پیام بازدارنده» فراتر می‌رود و شرایط تفسیر آن پیام را نیز در بر می‌گیرد. در اینجا، رسانه‌های شبکه‌ای با تعیین برجستگی و گردش روایت‌ها و هوش مصنوعی با تحلیل داده، شخصی‌سازی پیام و تسریع پردازش اطلاعات، دو نقش متمایز اما مرتبط ایفا می‌کنند: اولی ساختار توزیع و مشاهده اطلاعات را تغییر می‌دهد و دومی قابلیت تحلیل، هدف‌گیری و تولید محتوا را افزایش می‌دهد.

این تحول در عین حال به معنای کنارگذاشتن عقلانیت نیست، بلکه به محدود و زمینه‌مندشدن آن اشاره دارد. تصمیم همچنان بر ارزیابی هزینه، منفعت و ریسک استوار است، اما این متغیرها در محیطی محاسبه می‌شوند که کیفیت داده، فشار زمانی، میانجی‌گری الگوریتمی و احتمال دستکاری اطلاعات بر نتیجه اثر می‌گذارند. در مطالعات مربوط به کاربرد هوش مصنوعی در بازدارندگی هسته‌ای نیز جانسون نشان می‌دهد که افزایش سرعت پردازش و ورود سامانه‌های خودکار می‌تواند زمان تصمیم را کاهش داده و شرایط ارزیابی راهبردی را تغییر دهد؛ این نتیجه در این مقاله نه به‌عنوان شاهدی عام برای همه اشکال بازدارندگی، بلکه به‌عنوان نمونه‌ای محدود از تأثیر فناوری بر ساختار تصمیم مورد استفاده قرار می‌گیرد (Johnson, 2020b: 424–425). براین اساس در محیط شناختی ـ الگوریتمی، قدرت مادی همچنان جایگاه خود را در منطق بازدارندگی حفظ می‌کند، اما اثرگذاری آن بیش از گذشته به نحوه ادراک، پردازش و تفسیر اطلاعات از سوی حریف وابسته شده است. در چنین

شرایطی، فرایند شکل‌گیری برداشت حریف از توان، هزینه و ریسک نیز به یکی از مؤلفه‌های مؤثر بر کارکرد بازدارندگی تبدیل می‌شود.

٤-٢- از بازدارندگی تک‌حوزه‌ای به بازدارندگی چندحوزه‌ای

در مرحله مقایسه سازوکارهای بازدارندگی، منابع نشان دادند که اقدام شناختی الزاماً با پاسخ هم‌حوزه مواجه نمی‌شود؛ ازاین‌رو، بازدارندگی شناختی در معماری چندحوزه‌ای معنا می‌یابد و به پیوند ابزارهای سایبری، سیاسی، اقتصادی، اطلاعاتی و در صورت لزوم نظامی در یک محاسبه واحد بازدارنده وابسته است. گسترش سایبر، عملیات اطلاعاتی و تهدیدهای ترکیبی، محدودیت الگوی بازدارندگی مبتنی بر یک حوزه مشخص را آشکار کرده است. منطق هسته‌ای کلاسیک در محیطی شکل گرفت که قابلیت‌ها، بازیگران، خطوط قرمز و پیامدهای استفاده از سلاح تا حدی قابل مشاهده و نسبت‌دادن بود؛ اما در فضای سایبری و اطلاعاتی، این عناصر با ابهام بیشتری همراه‌اند. بلنک نشان می‌دهد که بازدارندگی به شبکه‌های ارتباطی معتبر، امکان ارزیابی اطلاعات و فهمی نسبتاً مشترک از قابلیت و اراده طرف مقابل وابسته است. جنگ اطلاعاتی با تحریف اطلاعات، اختلال در ارتباطات و دشوارکردن تشخیص عامل، هدف و انگیزه عملیات، همین پیش‌شرط‌ها را تضعیف می‌کند (Blank, 2001: 127-132).

در چنین شرایطی، بازدارندگی سایبری از رابطه ساده میان «تهدید» و «پاسخ» فاصله می‌گیرد. برنتلی معتقد است تحلیل بازدارندگی در قالب یک حوزه بسته، از کاستی‌های بخشی از ادبیات سایبری است؛ زیرا مسئله اصلی، جایگاه فناوری‌های دیجیتال در ساختار گسترده‌تر بازدارندگی میان دولت‌هاست (Brantly, 2018: 31–34). اهمیت این بحث برای بازدارندگی شناختی در آن است که آثار یک اقدام سایبری یا اطلاعاتی می‌تواند از سطح فنی فراتر رود و بر ادراک تهدید، اعتبار طرف مقابل و ارزیابی هزینه و ریسک اثر بگذارد؛ در نتیجه، پاسخ نیز ممکن است اقتصادی، دیپلماتیک، حقوقی، سایبری یا نظامی باشد.

سوئسانتو و اسمیتس نیز تحول بازدارندگی سایبری را در ادغام آن با رقابت امنیتی چندحوزه‌ای توضیح می‌دهند. در این برداشت، انکار، مجازات، درهم‌تنیدگی منافع و سلب مشروعیت در پیوند با یکدیگر عمل می‌کنند (Soesanto & Smeets, 2021: 391–396). این منطق زمانی به بازدارندگی شناختی مرتبط می‌شود که اثر این ابزارها از طریق تغییر برداشت حریف از احتمال موفقیت، هزینه و پیامدهای اقدام وارد فرایند تصمیم شود. جنگ شناختی نیز مجموعه‌ای از ابزارهای سنتی و نوظهور را برای اثرگذاری بر جمعیت، رهبران سیاسی و تصمیم‌گیرندگان نظامی به کار می‌گیرد و در چارچوب ناتو با تاب‌آوری، فرافکنی قدرت، فرماندهی میان‌حوزه‌ای و دفاع یکپارچه چندحوزه‌ای پیوند خورده است (Deppe & Schaal, 2024: 2–4). ازاین‌رو، حوزه شناختی در این معماری، محل ادراک و تفسیر آثار اقدامات سایر حوزه‌هاست.

نقش شرکت‌های فناوری و بازیگران غیردولتی این معماری را پیچیده‌تر کرده است. تجربه جنگ روسیه و اوکراین نشان داد که شرکت‌های خصوصی از طریق تأمین ارتباطات، خدمات ابری، اطلاعات تهدید و امنیت شبکه، مستقیماً بر مقاومت دولت‌ها اثر می‌گذارند و ممکن است در محاسبات امنیتی طرف مقابل به اهداف راهبردی تبدیل شوند (Lilly et al., 2023: 71-79). در نتیجه، بازدارندگی

الزاماً رابطه‌ای دولت‌به‌دولت نیست و تعیین هدف، مسئولیت و سطح اعمال هزینه به شبکه‌ای از دولت‌ها و شرکت‌ها وابسته است.

انتساب نیز به ابزاری چندحوزه‌ای تبدیل شده است. انتساب جمعی عملیات سایبری می‌تواند با مشروعیت‌زدایی، ایجاد هزینه حیثیتی و تقویت هنجارهای رفتار مسئولانه همراه شود (NATO CCDCOE, 2023: 424-425). هدلینگ و اُردن نیز افشای عامل عملیات اطلاعات نادرست را قابل پیوند با تحریم، کیفرخواست و اقدامات متقابل می‌دانند؛ فرایندی که از طریق سلب مشروعیت و نمایش قابلیت کشف، اثر بازدارنده ایجاد می‌کند (Hedling & Ördén, 2025: 975–983). بنابراین در محیط چندحوزه‌ای، کارکرد بازدارندگی به میزان انسجام میان ابزارهای نظامی، سایبری، اطلاعاتی و شناختی و سازگاری سیگنال‌های ارسالی در حوزه‌های مختلف وابسته است.

٤-۳- رسانه‌ای و پلتفرمی‌شدن محیط بازدارندگی

ورود رسانه‌های شبکه‌ای به رقابت راهبردی، ساختار تولید و توزیع ادراک را دگرگون کرده است. تحول دیجیتال نه در ماهیت عملیات روانی، بلکه در مقیاس، سرعت، قابلیت هدف‌گیری، تکثر بازیگران و معماری انتشار رخ داده است. روگه اینترنت را تقویت‌کننده‌ای برای عملیات اطلاعاتی می‌داند که به دلیل اتصال گسترده، تأخیر پایین، هزینه اندک، حذف واسطه‌های سنتی و امکان ناشناس‌ماندن، ظرفیت مدیریت ادراک را افزایش داده است (Rugge, 2018: 1-3). در این بستر، رسانه از وسیله انتقال پیام به محیط انتخاب و برجسته‌سازی آن تبدیل شده و الگوریتم‌های توزیع و داده‌های رفتاری، سهم اصلی را در قدرت ارتباطی ایفا می‌کنند. فردهایم و پمنت نشان می‌دهند که مدل‌های زبانی بزرگ با تولید محتوای متقاعدکننده در مقیاس انبوه، هزینه ورود به عملیات نفوذ[1] را کاهش داده و تشخیص رفتارهای هماهنگ را دشوارتر کرده‌اند (Pamment & Fredheim, 2025: 319-323).

ادبیات جنگ شناختی این مسئله را به سطح پردازش و واکنش مخاطب می‌برد. برخلاف جنگ اطلاعاتی با تمرکز بر کنترل داده، جنگ شناختی در پی تغییر واکنش افراد به اطلاعات است؛ جایی که فناوری‌های دیجیتال و هوش مصنوعی مرز میان مناقشه طبیعی و بهره‌برداری سازمان‌یافته از شکاف‌های اجتماعی را مبهم می‌سازند (Deppe & Schaal, 2024: 2-4). مانیترا و پرابانداری نیز نشان می‌دهند که الگوریتم‌ها با گزینش، قالب‌بندی و پروفایل‌سازی رفتاری[2] محرک‌های عاطفی و سوگیری‌های شناختی را برای اثرگذاری بر درک مشروعیت و تهدید به کار می‌گیرند (Manitra, Prabandari & 2026: 4-9).

این شرایط منطق بازدارندگی را دگرگون کرده است. نخست، علامت‌دهی دیگر در انحصار دولت فرستنده نیست و پیام در انبوه بازتفسیرهای پلتفرمی دچار دگرگونی می‌شود. دوم، اعتبار منابع رسمی و اعتماد عمومی به بخشی از توان بازدارنده تبدیل شده است؛ زیرا بدون اعتماد، پاسخ‌دهی به عملیات نفوذ ناممکن خواهد بود. سوم، هدف مهاجم الزاماً ترویج روایت جایگزین نیست، بلکه ایجاد

---

[1]. Influence Operations

[2]. Behavioral Profiling

تردید بنیادین و اختلال در تصمیم‌گیری جمعی است. پارک و نَن با اشاره به هوش مصنوعی مولد یادآور می‌شوند که فناوری هم‌زمان ابزار تولید اطلاعات دستکاری‌شده و وسیله کشف و مهار آن است (Nan & Park, 2026: 1508-1515). رحیمی نیز بر پیوند جنگ شناختی با کلان‌داده‌ها و نقش سواد رسانه‌ای و تفکر انتقادی در کاهش اثربخشی عملیات شناختی تأکید می‌کند (رحیمی، ۱۴۰۳: ۶۶-۶۱)؛(Rahimi, 2024: 61–66). بر این اساس، تاب‌آوری اطلاعاتی صرفاً کارکردی دفاعی ندارد؛ هنگامی که مهاجم احتمال موفقیت دستکاری را پایین ارزیابی کند، منفعت مورد انتظار عملیات کاهش می‌یابد. در محیط پلتفرمی نیز رسانه فقط مجرای انتقال پیام نیست، بلکه بر اعتبار، برجستگی و تفسیر آن اثر می‌گذارد. ازاین‌رو، بخشی از کارکرد بازدارندگی به توان اثرگذاری بر شرایط دیده‌شدن و تفسیر پیام وابسته می‌شود، نه کنترل کامل آن.

٤-٤- الگوریتمی‌شدن تصمیم راهبردی؛ دوگانگی ثبات و بی‌ثباتی

ورود هوش مصنوعی به بازدارندگی رابطه‌ای خطی میان فناوری و افزایش قدرت ایجاد نمی‌کند. همان قابلیت‌هایی که با افزایش سرعت تحلیل، کشف تهدید و آگاهی موقعیتی می‌توانند بازدارندگی را تقویت کنند، در صورت کاهش نظارت انسانی یا تشدید فشار زمانی قادرند احتمال سوءبرداشت و تشدید ناخواسته را نیز افزایش دهند.تأثیر هوش مصنوعی بر بازدارندگی به دیپ‌فیک و عملیات رسانه‌ای محدود نیست، بلکه ورود الگوریتم‌ها به مشاهده، تحلیل، پیش‌بینی، تشخیص تهدید و اجرای تصمیم را نیز دربرمی‌گیرد. در نتیجه، رابطه سنتی «انسان ـ انسان» به روابط انسان ـ ماشین و ماشین ـ ماشین گسترش می‌یابد. گزارش رَند هشدار می‌دهد که تصمیم‌گیری با سرعت ماشین یا خروج بخشی از آن از کنترل مستقیم انسان، می‌تواند الگوهای علامت‌دهی، تشخیص اراده و کنترل تشدید را مختل کند (Wong et al., 2020: 1-2).

هوش مصنوعی با تحلیل سریع داده‌های حجیم، افزایش آگاهی موقعیتی، شناسایی ناهنجاری‌ها و تقویت دفاع سایبری، ظرفیت بازدارندگی از طریق انکار را افزایش می‌دهد. بااین‌حال، ابهام الگوریتمی، بهره‌برداری خصمانه و کاهش نظارت انسانی می‌تواند مدیریت بحران را دشوار سازد (Zieliński, 2025: 366-369). رقابت آمریکا، چین و روسیه برای ادغام هوش مصنوعی و سامانه‌های خودکار نیز ممکن است استقرار زودهنگام فناوری‌هایی را تشویق کند که ایمنی و پاسخگویی آنها هنوز تثبیت نشده است (Khan et al., 2021: 19-21, 38-39).

جانسون تأکید می‌کند که هوش مصنوعی مستقلاً دگرگون‌کننده نیست، بلکه از طریق ترکیب با قابلیت‌های سایبری، پهپادهای گروهی، سلاح‌های فراصوت و سامانه‌های هشدار، سرعت جنگ و فشار زمانی را افزایش می‌دهد. اثر آن نیز بیش از عملکرد واقعی، به ادراک دولت‌ها وابسته است؛ تصور تهدیدشدن توان ضربه دوم می‌تواند انگیزه «استفاده کن یا از دست بده» را تقویت کند (Johnson, 2020a: 17-20). زالا نیز ثبات‌زایی یا بی‌ثبات‌سازی هوش مصنوعی را تابع پیوند آن با فرماندهی، هشدار و دفاع موشکی می‌داند؛ پیوندی که ممکن است بازدارندگی را تقویت یا اقدام پیش‌دستانه را تحریک کند (Zala, 2024: 154-163).

اعتماد انسان به الگوریتم نیز متغیر است. آزمایش هورووویتز و کان نشان می‌دهد «سوگیری

خودکارسازی»[1] می‌تواند خروجی هوش مصنوعی را جایگزین ارزیابی مستقل اطلاعات کند؛ خطری که در بحران‌های سریع تشدید می‌شود (Kahn, 2024: 1-6 & Horowitz). همچنین، ماشین ممکن است تفاوت میان تهدید، اطمینان‌بخشی و پیشنهاد کاهش تنش را درک نکند و مسیر خروج را فرصت حمله تلقی کند (Wong et al., 2020: 66-67). حفظ نظارت انسانی می‌تواند برای کاهش تنش زمان ایجاد کند، درحالی‌که خودمختاری بالا خطر تشدید ناخواسته را افزایش می‌دهد (Johnson, 2020b: 435-437). افزون‌براین، نظارت و تحلیل خودکار نیز ابهام راهبردی را حذف نمی‌کنند (Karadeniz, 2025: 426). بنابراین، الگوریتمی‌شدن بازدارندگی عدم‌قطعیت را از میان نمی‌برد، بلکه آن را به داده‌ها، منطق تصمیم، میزان خودمختاری و واکنش ماشین منتقل می‌کند.

٤-۵- معماری بازدارندگی شناختی

برآیند ترکیب و مقایسه ادبیات بازدارندگی، بازدارندگی سایبری و جنگ شناختی در این پژوهش به استخراج پنج سازوکار انکار و تاب‌آوری، کشف و انتساب، تحمیل هزینه، سلب مشروعیت و پیام‌رسانی راهبردی انجامیده است. این طبقه‌بندی صورت‌بندی تحلیلی نویسندگان بر پایه تلفیق سازوکارهایی است که به‌صورت پراکنده در منابع مختلف مطرح شده‌اند؛ ازاین‌رو، منابع هر سازوکار در ادامه به‌طور مستقل بررسی می‌شوند.

نخست، در سطح انکار و تاب‌آوری، هدف کاهش احتمال دستیابی مهاجم به نتیجه مطلوب است. بازدارندگی لزوماً با تهدید به مجازات آغاز نمی‌شود، بلکه افزایش هزینه نفوذ، حفاظت از دارایی‌ها و توان بازیابی می‌تواند منفعت مورد انتظار مهاجم را بکاهد. سوئسانتو و اسمیتس بازدارندگی از طریق انکار را در کنار مجازات قرار داده و تاب‌آوری را به رکن موج جدید بازدارندگی پیوند می‌زنند (Smeets & Soesanto, 2021: 391-396). در مطالعات آمادگی سایبری نیز چرخه‌های مبتنی بر شناسایی، دفاع، کشف، پاسخ و بازیابی مستقیماً به بازدارندگی از طریق انکار متصل می‌شوند (NATO CCDCOE, 2023: 208-209). طالبی و محجوب عشرت‌آبادی نیز این منطق را در قالب زیست‌بوم فنی ـ اجتماعی آمادگی شناختی شامل کارکنان، فرایندها، فناوری و عوامل محیطی تبیین کرده‌اند (طالبی و محجوب عشرت‌آبادی، ۱۴۰۳: ۱۴۷–۱۵۲)؛(Talebi & Mahjoub Eshratabadi, 2024: 147–152).

دوم، کشف و انتساب، مزیت ناشناس‌ماندن و انکارپذیری عملیات شناختی را مهار می‌کند. بااین‌حال، انتساب فقط امری فنی نیست. هدلینگ و اُردن با مفهوم «حلقه عدم قطعیت» نشان می‌دهند دولت‌ها حتی با وجود شواهد فنی، گاه به دلایل سیاسی از انتساب عمومی پرهیز می‌کنند؛ درحالی‌که انتساب عمومی با آشکارسازی هویت و روش مهاجم و اثبات اراده مدافع، کارکرد بازدارنده می‌یابد(Hedling & Ördén, 2025: 975–986). انتساب‌های جمعی نیز در ارسال علامت یکپارچه و تثبیت هنجارهای رفتاری مؤثرند (NATO CCDCOE, 2023: 424-425).

سوم، تحمیل هزینه فراتر از مقابله‌به‌مثل صرفاً شناختی است. برنتلی تأکید می‌کند که بازدارندگی دیجیتال باید از مرزهای درون‌حوزه‌ای بگذرد و تمامی ابزارهای تغییردهنده محاسبه هزینه ـ فایده، اعم

[1]. Automation Bias

از ابزارهای تحریمی، دیپلماتیک، حقوقی یا پاسخ‌های سایبری را به‌کار گیرد (Brantly, 2018: 31-34). شرط کلیدی، شفافیت آستانه واکنش و درک‌پذیری رابطه میان رفتار ممنوع و پاسخ متناسب برای جلوگیری از سوءبرداشت است.

چهارم، پیام‌رسانی راهبردی تنها نمایش قدرت نیست. نظریه شناختی بازدارندگی هشدار می‌دهد که تهدید بیش‌ازحد تهاجمی ممکن است حریف را در چارچوب زیان قرار دهد و ریسک‌پذیری او را افزایش دهد (Berejikian, 2002: 180-181). ازاین‌رو، پیام بازدارنده باید هم‌زمان توان مقاومت، آمادگی پاسخ و مسیر خویشتنداری را منتقل کند؛ مؤلفه‌ای که در سطح سیاستی به دکترین و دیپلماسی فعال پیوند می‌خورد (مداح و نورمحمدی، ۱۴۰۵: ۴۹–۵۵).

پنجم، سلب مشروعیت و هنجارسازی با افشای شبکه، روش و هدف عملیات، محتوای آن را از گفت‌وگوی عادی به «رفتار دستکاری‌گرانه» تبدیل می‌کند و از طریق افزایش هزینه حیثیتی، بازدارندگی ایجاد می‌کند (Soesanto & Smeets, 2021: 392–393). راهبرد نام‌گذاری و رسواسازی در کنار مجازات‌های سیاسی، این کارکرد را تقویت می‌کند (Ördén & Hedling, 2025: 975-983).

این پنج سازوکار در یک معماری هم‌افزا عمل می‌کنند؛ چنان‌که در مدل سناریومحور وحدانی‌نیا و وحدانی‌نیا نیز پیوند سطح راهبردی، هماهنگی نهادی، سیاست روایی، سواد رسانه‌ای و فناوری شناختی برجسته شده است (وحدانی‌نیا و وحدانی‌نیا، ۱۴۰۴: ۱۶۱)؛(Vahdaninia & Vahdaninia, 2025: 161). این وابستگی متقابل مانع تقلیل بازدارندگی شناختی به ابزاری منفرد یا صرفاً قدرت رسانه‌ای می‌شود. ترکیب یافته‌های نظری این پژوهش نشان می‌دهد که بازدارندگی شناختی را نمی‌توان به یک ابزار، مانند تبلیغات، انتساب یا تهدید به مجازات، فروکاست. کارکرد بازدارنده زمانی شکل می‌گیرد که مجموعه‌ای از سازوکارهای مکمل، هم‌زمان احتمال موفقیت عملیات خصمانه را کاهش دهند و هزینه و ریسک ادراک‌شده آن را افزایش دهند.

٦-٤- پارادوکس‌ها و حدود بازدارندگی شناختی

گسترش بازدارندگی به حوزه شناختی، در کنار افزایش ابزارهای اثرگذاری، محدودیت‌ها و پارادوکس‌هایی ایجاد می‌کند. یکی از مهم‌ترین آنها رابطه غیرخطی میان شدت تهدید و رفتار حریف است. در منطق ساده مجازات، افزایش هزینه باید احتمال اقدام خصمانه را کاهش دهد؛ اما بریجیکیان نشان می‌دهد فشار شدید می‌تواند بازیگری را که خود را در موقعیت زیان می‌بیند، به پذیرش ریسک بیشتر سوق دهد. تهدید شدید ممکن است هم اعتبار بازدارندگی را افزایش دهد و هم حریف را متقاعد کند که حتی امتیازدهی نیز امنیت او را تضمین نمی‌کند (Berejikian, 2002: 180–181). ازاین‌رو، در بازدارندگی شناختی افزایش فشار الزاماً به افزایش اثر بازدارنده منجر نمی‌شود.

پارادوکس دوم به رابطه اطلاعات و بازدارندگی مربوط است. بازدارندگی به اطلاعات معتبر و امکان تفسیر سیگنال‌های طرف مقابل وابسته است، درحالی‌که عملیات اطلاعاتی و شناختی همین زیرساخت معرفتی را هدف می‌گیرند. کاهش اعتماد به داده‌ها، اختلال در ارتباطات و دشوارشدن تشخیص عامل حمله می‌تواند تصمیم‌گیری معتبر را تضعیف کرده و طرفین را به سناریوهای بدبینانه سوق دهد (Blank, 2001: 125–132). بنابراین، عملیات شناختی ممکن است نه‌فقط موضوع

بازدارندگی، بلکه یکی از پیش‌شرط‌های آن را نیز تضعیف کند.

هوش مصنوعی این مسئله را با «پارادوکس سرعت» تشدید می‌کند. افزایش سرعت تشخیص و پاسخ می‌تواند غافلگیری را کاهش دهد، اما زمان لازم برای بررسی اطلاعات، تماس دیپلماتیک و اصلاح سوءبرداشت را نیز محدود می‌کند. سامانه‌های خودکار ممکن است در سطح عملیاتی مزیت ایجاد کنند، اما هم‌زمان مسیرهای کاهش تنش را در سطح راهبردی محدود سازند (Wong et al., 2020: 83–85). همچنین ابهام الگوریتمی و کاهش نظارت انسانی در کنار سرعت و دقت بیشتر، آثار دوگانه هوش مصنوعی بر بازدارندگی را نشان می‌دهد (Zieliński, 2025: 382–383).

اتکای بیش از حد به الگوریتم نیز می‌تواند استقلال تصمیم را تضعیف کند. هنگامی که خروجی سامانه هوشمند جایگزین ارزیابی مستقل شود، خطای داده یا مدل مستقیماً به تصمیم راهبردی منتقل می‌شود. هورورویتز و کان این مسئله را در قالب سوگیری خودکارسازی بررسی کرده‌اند (Horowitz & Kahn, 2024: 1–6). محجوب و همکاران نیز اضافه‌بار اطلاعاتی، سوگیری، فناوری و فرایند تصمیم را از عوامل تهدید شناختی می‌دانند (محجوب و همکاران، ۱۴۰۵: ۲۸۹–۲۹۶)؛ (Mahjoub et al., 2026: 289–296). بنابراین، تاب‌آوری شناختی باید نهاد تصمیم‌گیر را نیز در برابر وابستگی فناورانه مقاوم سازد.

انتساب نیز واجد دوگانگی است. مهاجم باید احتمال شناسایی خود را جدی بداند، اما انتساب شتاب‌زده یا سیاسی‌شده می‌تواند اعتبار مدافع را کاهش دهد. تصمیم به انتساب فقط فنی نیست و تحت تأثیر زمان، سیاست و هزینه‌های احتمالی قرار دارد (Hedling & Ördén, 2025: 975–986). حضور بازیگران غیردولتی و شرکت‌های فناوری نیز مسئولیت و شناسایی عامل را پیچیده‌تر می‌کند.

بازدارندگی شناختی در عین حال با آزادی و استقلال شناختی مرتبط است. تعریف هر روایت مخالف به‌عنوان عملیات خصمانه می‌تواند مرز میان امنیت اطلاعاتی و کنترل سیاسی را مخدوش کند. مقابله با نفوذ باید با آزادی بیان، حقوق اطلاعاتی و استقلال شناختی سازگار باشد (Manitra & Prabandari, 2026: 12–16). افزون بر این، وابستگی دولت‌ها به شرکت‌های خصوصی در ارتباطات، داده و زیرساخت دیجیتال می‌تواند بخشی از ظرفیت بازدارندگی را از کنترل مستقیم دولت خارج کند؛ تجربه استارلینک در جنگ اوکراین نمونه‌ای از این وابستگی است (Lilly et al., 2023: 78–80).

در مجموع، مرز میان بازدارندگی مؤثر و بی‌ثباتی شناختی باریک است: فشار شدید می‌تواند ریسک‌پذیری را افزایش دهد، سرعت زیاد امکان اصلاح خطا را کاهش دهد، اتکای الگوریتمی استقلال تصمیم را محدود کند و کنترل افراطی اطلاعات اعتماد اجتماعی را فرسایش دهد. ازاین‌رو، کارآمدی بازدارندگی شناختی به تنظیم متوازن قدرت، فناوری، اعتماد و کنترل انسانی وابسته است.

نتیجه‌گیری

در محیط رسانه‌ای ـ الگوریتمی، اثر بازدارندگی به نحوه ورود قابلیت‌های مادی به محاسبات حریف وابسته‌تر شده است. بازیگر زمانی می‌تواند رفتار طرف مقابل را مهار کند که ارزیابی او از احتمال

موفقیت، خطر کشف، هزینه‌های احتمالی و پیامدهای اقدام تغییر کند. بازدارندگی شناختی در این چارچوب بخشی از معماری بازدارندگی معاصر است و رسانه‌ها، داده‌ها و سامانه‌های الگوریتمی می‌توانند بر فرایند شکل‌گیری این محاسبات اثر بگذارند.

این تحول، دامنه ظرفیت‌های مؤثر بر بازدارندگی را گسترش داده است. اعتبار اطلاعات، توان انتساب، انسجام نهادی و حفظ کیفیت تصمیم‌گیری در شرایط فشار فناورانه می‌توانند بر محاسبات مهاجم اثرگذار باشند. تحلیل پژوهش نشان می‌دهد کارکرد بازدارنده از ترکیب چند سازوکار حاصل می‌شود: کاهش احتمال موفقیت عملیات از طریق انکار و تاب‌آوری، افزایش خطر شناسایی از طریق کشف و انتساب، افزایش هزینه و کاهش مشروعیت اقدام، همراه با پیام‌رسانی راهبردی معتبر. اتکای منفرد به هر یک از این سازوکارها لزوماً نتیجه بازدارنده ایجاد نمی‌کند.

گسترش بازدارندگی به حوزه شناختی در عین حال می‌تواند منابع تازه‌ای از بی‌ثباتی ایجاد کند. کنترل شدید محیط اطلاعاتی ممکن است اعتماد عمومی را کاهش دهد، خودکارسازی تصمیم زمان اصلاح خطا را محدود کند و فشار بیش از اندازه، ریسک‌پذیری حریف را افزایش دهد. ازاین‌رو، کارآمدی بازدارندگی شناختی به تناسب ابزارهای بازدارنده با شرایط تصمیم‌گیری و محدودکردن آثار ناخواسته فناوری وابسته است. بررسی تجربی این روابط و مقایسه موارد موفق و ناموفق می‌تواند حدود اعتبار این الگو را دقیق‌تر مشخص کند.

هدف پژوهش، تبیین جایگاه بازدارندگی شناختی در تحول بازدارندگی معاصر و شناسایی سازوکارها و محدودیت‌های آن بود. یافته‌ها از فرضیه پژوهش حمایت می‌کنند و نشان می‌دهند رسانه‌های شبکه‌ای و هوش مصنوعی زمانی واجد اثر بازدارنده می‌شوند که از طریق کاهش احتمال موفقیت، افزایش خطر کشف و هزینه‌های اقدام و تغییر ارزیابی حریف از ریسک و پیامدها بر تصمیم او اثر بگذارند. این ظرفیت در چارچوب بازدارندگی چندحوزه‌ای عمل می‌کند و میزان کارآمدی آن به شرایط نهادی، فناورانه و تصمیمی هر بازیگر وابسته است.

منابع فارسی

۱. محجوب، ح.، طالبی، م.، و شکوری، س. (۱۴۰۵). تهدیدات شناختی سازمان‌های اطلاعات در پاردایم شناختی جنگ (مطالعه موردی یک سازمان اطلاعاتی نظامی) .*آینده‌پژوهی دفاعی*، *۱۱*(۴۰)، ۲۸۹–۳۲۴. DOI: 10.22034/dfsr.2026.2065922.1922

۲. جهان‌دیده، ا.، و میرفخرائی، س. ح. (۱۴۰۳). کاربرد هوش مصنوعی در بخش نظامی؛ مطالعه موردی: ایالات متحده آمریکا و چین. *فصلنامه مطالعات بین‌المللی*، *۲۱*(۲)، ۲۹۵–۳۱۳. https://doi.org/10.22034/isj.2024.397508.2018

۳. رحیمی، ص. (۱۴۰۳). جنگ‌شناختی و تهدیدهای ترکیبی در چشم‌انداز آینده: مفاهیم، ابزارها و راهکارهای پیشگیرانه .*آینده‌پژوهی دفاعی*، *۹*(۳۵)، ۶۱–۹۱. DOI: 10.22034/dfsr.2024.2041829.1830.

۴. طالبی، م.، و محجوب عشرت‌آبادی، ح. (۱۴۰۳). زیست‌بوم آمادگی شناختی دفاع سایبری. *آینده‌پژوهی دفاعی*، *۹*(۳۴)، ۱۴۷–۱۸۲. DOI: 10.22034/dfsr.2024.2043105.1838 .

۵. وحدانی‌نیا، ذ.، و وحدانی‌نیا، و. (۱۴۰۴). مدلی برای سیاست‌گذاری دفاع شناختی ایران؛ یک رویکرد سناریومحور. *آینده‌پژوهی دفاعی*، ۱۰(۳۸)، ۱۶۱–۲۰۲. DOI: 10.22034/dfsr.2025.2062373.1914.

English References

1. Berejikian, J. D. (2002). A cognitive theory of deterrence. *Journal of Peace Research, 39*(2), 165–183. https://doi.org/10.1177/0022343302039002002
2. Berejikian, J. D., & Justwan, F. (2019). Testing a cognitive theory of deterrence. In A. I. Harrington & J. W. Knopf (Eds.), *Behavioral economics and nuclear weapons* (pp. 25–55). University of Georgia Press. https://doi.org/10.2307/j.ctv5npjp8.7
3. Blank, S. (2001). Can information warfare be deterred? *Defense Analysis, 17*(2), 121–138. https://doi.org/10.1080/07430170120064212
4. Brantly, A. F. (2018). The cyber deterrence problem. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *2018 10th International Conference on Cyber Conflict (CyCon X): Maximising effects* (pp. 31–54). NATO CCD COE Publications. https://doi.org/10.23919/CYCON.2018.8405009
5. Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data, 7*, 1452129. https://doi.org/10.3389/fdata.2024.1452129
6. Fredheim, R., & Pamment, J. (2025). Assessing the risks and opportunities posed by AI-enhanced influence operations on social media. *Place Branding and Public Diplomacy, 21*(3), 319–326. https://doi.org/10.1057/s41254-023-00322-5
7. Hedling, E., & Ördén, H. (2025). Disinformation, deterrence and the politics of attribution. *International Affairs, 101*(3), 967–986. https://doi.org/10.1093/ia/iiaf012
8. Horowitz, M. C., & Kahn, L. (2024). Bending the automation bias curve: A study of human and AI-based decision making in national security contexts. *International Studies Quarterly, 68*(2), sqae020. https://doi.org/10.1093/isq/sqae020
9. Izycki, E., van Niekerk, B., & Ramluckan, T. (2023). Cyber diplomacy: NATO/EU engaging with the Global South. In T. Jančárková, D. Giovannelli, K. Podiŋš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 417–435). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10182095
10. Johnson, J. S. (2020a). Artificial intelligence: A threat to strategic stability. *Strategic Studies Quarterly, 14*(1), 16–39. DOI: 10.2307/26891882
11. -Johnson, J. S. (2020b). Deterrence in the age of artificial intelligence & autonomy: A

paradigm shift in nuclear deterrence theory and practice? *Defense & Security Analysis, 36*(4), 422–448. https://doi.org/10.1080/14751798.2020.1857911

12. Karadeniz, Ç. (2025). Review of *Deterrence under uncertainty: Artificial intelligence and nuclear warfare*, by E. Geist. *Insight Turkey, 27*(2), 426–428. https://doi.org/10.25253/99.2025272.23
13. Khan, A., Imam, I., & Azam, A. (2021). Role of artificial intelligence in defence strategy: Implications for global and national security. *Strategic Studies, 41*(1), 19–40. https://doi.org/10.53532/ss.041.01.0058
14. Lilly, B., Geers, K., Rattray, G., & Koch, R. (2023). Business@War: The IT companies helping to defend Ukraine. In T. Jančárková, D. Giovannelli, K. Podiņš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 71–83). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10181980
15. Manitra, R. R. M., & Prabandari, A. P. (2026). AI in hybrid conflicts: Towards a legal framework for cognitive warfare. *Cogent Social Sciences, 12*(1), 2681304. https://doi.org/10.1080/23311886.2026.2681304
16. Mazarr, M. J. (2018). *Understanding deterrence* (PE-295-RC). RAND Corporation. https://doi.org/10.7249/PE295
17. Ördén, H. (2024). The neuropolitical imaginaries of cognitive warfare. *Security Dialogue, 55*(6), 607–624. https://doi.org/10.1177/09670106241253527
18. Özkan, B. E., & Tolga, İ. B. (2023). Zero-day operational cyber readiness. In T. Jančárková, D. Giovannelli, K. Podiņš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 199–215). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10181814
19. Park, S., & Nan, X. (2026). Generative AI and misinformation: A scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation. *AI & Society, 41*(2), 1501–1515. https://doi.org/10.1007/s00146-025-02620-3
20. Rugge, F. (2018). *"Mind hacking": Information warfare in the cyber age* (Analysis No. 319). Italian Institute for International Political Studies.
21. Smith, M. W., & Dean, T. (2023). The irregulars: Third-party cyber actors and digital resistance movements in the Ukraine conflict. In T. Jančárková, D. Giovannelli, K. Podiņš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 103–119). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10182061

22. Soesanto, S., & Smeets, M. (2021). Cyber deterrence: The past, present, and future. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020* (pp. 385–400). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_20
23. Wong, Y. H., Yurchak, J. M., Button, R. W., Frank, A. B., Laird, B., Osoba, O. A., Steeb, R., Harris, B. N., & Bae, S. J. (2020). *Deterrence in the age of thinking machines*. RAND Corporation. https://doi.org/10.7249/RR2797
24. Zala, B. (2024). Should AI stay or should AI go? First strike incentives & deterrence stability. *Australian Journal of International Affairs, 78*(2), 154–163. https://doi.org/10.1080/10357718.2024.2328805
25. Zieliński, T. (2025). The integration of artificial intelligence in modern deterrence: Opportunities and challenges. *Journal of Modern Science, 64*(4), 365–386. https://doi.org/10.13166/jms/214331

Translated References to English

1. Berejikian, J. D. (2002). A cognitive theory of deterrence. *Journal of Peace Research, 39*(2), 165–183. https://doi.org/10.1177/0022343302039002002
2. Berejikian, J. D., & Justwan, F. (2019). Testing a cognitive theory of deterrence. In A. I. Harrington & J. W. Knopf (Eds.), *Behavioral economics and nuclear weapons* (pp. 25–55). University of Georgia Press. https://doi.org/10.2307/j.ctv5npjp8.7
3. Blank, S. (2001). Can information warfare be deterred? *Defense Analysis, 17*(2), 121–138. https://doi.org/10.1080/07430170120064212
4. Brantly, A. F. (2018). The cyber deterrence problem. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), *2018 10th International Conference on Cyber Conflict (CyCon X): Maximising effects* (pp. 31–54). NATO CCD COE Publications. https://doi.org/10.23919/CYCON.2018.8405009
5. Deppe, C., & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data, 7*, 1452129. https://doi.org/10.3389/fdata.2024.1452129
6. Fredheim, R., & Pamment, J. (2025). Assessing the risks and opportunities posed by AI-enhanced influence operations on social media. *Place Branding and Public Diplomacy, 21*(3), 319–326. https://doi.org/10.1057/s41254-023-00322-5
7. Hedling, E., & Ördén, H. (2025). Disinformation, deterrence and the politics of attribution. *International Affairs, 101*(3), 967–986. https://doi.org/10.1093/ia/iiaf012
8. Horowitz, M. C., & Kahn, L. (2024). Bending the automation bias curve: A study of human

and AI-based decision making in national security contexts. *International Studies Quarterly, 68*(2), sqae020. https://doi.org/10.1093/isq/sqae020

9. Izycki, E., van Niekerk, B., & Ramluckan, T. (2023). Cyber diplomacy: NATO/EU engaging with the Global South. In T. Jančárková, D. Giovannelli, K. Podiŋš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 417–435). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10182095
10. Jahandideh, A., & Mirfakhraie, S. H. (2024). Artificial intelligence in military applications: A case study of the United States and China. *International Studies Journal, 21*(2), 295–313. https://doi.org/10.22034/isj.2024.397508.2018 **(In Persian)**
11. Johnson, J. S. (2020a). Artificial intelligence: A threat to strategic stability. *Strategic Studies Quarterly, 14*(1), 16–39. DOI: 10.2307/26891882
12. -Johnson, J. S. (2020b). Deterrence in the age of artificial intelligence & autonomy: A paradigm shift in nuclear deterrence theory and practice? *Defense & Security Analysis, 36*(4), 422–448. https://doi.org/10.1080/14751798.2020.1857911
13. Karadeniz, Ç. (2025). Review of *Deterrence under uncertainty: Artificial intelligence and nuclear warfare*, by E. Geist. *Insight Turkey, 27*(2), 426–428. https://doi.org/10.25253/99.2025272.23
14. Khan, A., Imam, I., & Azam, A. (2021). Role of artificial intelligence in defence strategy: Implications for global and national security. *Strategic Studies, 41*(1), 19–40. https://doi.org/10.53532/ss.041.01.0058
15. Lilly, B., Geers, K., Rattray, G., & Koch, R. (2023). Business@War: The IT companies helping to defend Ukraine. In T. Jančárková, D. Giovannelli, K. Podiŋš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 71–83). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10181980
16. Mahjoub, H., Talebi, M., & Shakouri, S. (2026). Cognitive threats to intelligence organizations in the cognitive paradigm of warfare: A case study of a military intelligence organization. *Ayandehpazhuhi-ye Defa'i, 11*(40), 289–324. https://doi.org/10.22034/dfsr.2026.2065922.1922 **(In Persian)**
17. Manitra, R. R. M., & Prabandari, A. P. (2026). AI in hybrid conflicts: Towards a legal framework for cognitive warfare. *Cogent Social Sciences, 12*(1), 2681304. https://doi.org/10.1080/23311886.2026.2681304
18. Mazarr, M. J. (2018). *Understanding deterrence* (PE-295-RC). RAND Corporation. https://doi.org/10.7249/PE295

19. Ördén, H. (2024). The neuropolitical imaginaries of cognitive warfare. *Security Dialogue, 55*(6), 607–624. https://doi.org/10.1177/09670106241253527
20. Özkan, B. E., & Tolga, İ. B. (2023). Zero-day operational cyber readiness. In T. Jančárková, D. Giovannelli, K. Podiņš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 199–215). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10181814
21. Park, S., & Nan, X. (2026). Generative AI and misinformation: A scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation. *AI & Society, 41*(2), 1501–1515. https://doi.org/10.1007/s00146-025-02620-3
22. Rahimi, S. (2024). Cognitive warfare and hybrid threats in the future outlook: Concepts, tools, and preventive strategies. *Ayandehpazhuhi-ye Defa'i, 9*(35), 61–91. https://doi.org/10.22034/dfsr.2024.2041829.1830 **(In Persian)**
23. Rugge, F. (2018). *"Mind hacking": Information warfare in the cyber age* (Analysis No. 319). Italian Institute for International Political Studies.
24. Smith, M. W., & Dean, T. (2023). The irregulars: Third-party cyber actors and digital resistance movements in the Ukraine conflict. In T. Jančárková, D. Giovannelli, K. Podiņš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 103–119). NATO CCDCOE Publications. https://doi.org/10.23919/CyCon58705.2023.10182061
25. Soesanto, S., & Smeets, M. (2021). Cyber deterrence: The past, present, and future. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020* (pp. 385–400). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-419-8_20
26. Talebi, M., & Mahjoub Eshratabadi, H. (2024). The ecosystem of cognitive readiness in cyber defense. *Ayandehpazhuhi-ye Defa'i, 9*(34), 147–182. https://doi.org/10.22034/dfsr.2024.2043105.1838 **(In Persian)**
27. Vahdaninia, Z., & Vahdaninia, V. (2025). A model for cognitive defense policymaking in Iran: A scenario-based approach. *Ayandehpazhuhi-ye Defa'i, 10*(38), 161–202. https://doi.org/10.22034/dfsr.2025.2062373.1914 **(In Persian)**
28. Wong, Y. H., Yurchak, J. M., Button, R. W., Frank, A. B., Laird, B., Osoba, O. A., Steeb, R., Harris, B. N., & Bae, S. J. (2020). *Deterrence in the age of thinking machines*. RAND Corporation. https://doi.org/10.7249/RR2797
29. Zala, B. (2024). Should AI stay or should AI go? First strike incentives & deterrence stability. *Australian Journal of International Affairs, 78*(2), 154–163.

https://doi.org/10.1080/10357718.2024.2328805

30. Zieliński, T. (2025). The integration of artificial intelligence in modern deterrence: Opportunities and challenges. *Journal of Modern Science, 64*(4), 365–386. https://doi.org/10.13166/jms/214331