



The Structure and Basics of Cognitive Warfare with the Approach of Disseminating False Information Against the Target Community

Mohammad Hossein Esmaili¹ | Seyedeh Mahnaz Hosseini²

¹ PhD student, Media Management, University of Tehran. Mh.esmaeili@ut.ac.ir

² MSc, Social Communication Sciences, Social Security Organization. hmahnaz656@gmail.com

Article Info

Article type:

Research Article

Article history:

Received

25 Nov 2025

Received in revised form

27 June 2026

Accepted

24 July 2026

Published online

31 July 2026

Keywords:

*cognitive warfare,
misinformation,
cyber space and security*

ABSTRACT

Cognitive warfare shifts the battlefield from physical domains to the human dimension, targeting perception, judgment, and decision-making. While its objective of influencing minds is historically rooted, this study examines how disinformation and specific social processes increase societal vulnerability to these threats, aiming to enhance societal awareness of its mechanisms.

Methodology: This study employs a qualitative, descriptive-analytical approach. Data collection integrated library-based research—systematic reviews of scholarly articles, security reports, and psychological texts—with field-based analysis of empirical cases and real-world cognitive operations within cyberspace and media environments. Data were processed using conceptual, deductive, and comparative analysis.

Results: The findings reveal that while the concept is not new, advancements in cognitive psychology, the exploitation of cognitive biases, and the expansion of social media have exponentially increased the scope and speed of cognitive warfare. Crucially, the study concludes that modern geopolitical success requires a synergistic integration of kinetic, information, and cognitive warfare; isolated military action is no longer sufficient for sustainable strategic outcomes.

Cite this article:

DOI: <https://doi.org/10.22034/jcwst.2026.562090.1013>



Publisher: IRI Military Command and Staff University



ساختار و مبانی جنگ شناختی با تأکید بر بروز اطلاعات نادرست در برابر جامعه‌ی هدف

محمدحسین اسمعیلی درجوزی^۱ | سیده مهناز حسینی^۲

^۱ دانشجوی دکتری، مدیریت رسانه، دانشگاه تهران. Mh.esmaeili@ut.ac.ir

^۲ کارشناسی ارشد، علوم ارتباطات اجتماعی، سازمان تأمین اجتماعی، hmahnaz656@gmail.com

اطلاعات مقاله چکیده

نوع مقاله:

مقاله پژوهشی

تاریخچه مقاله:

تاریخ دریافت:

۱۴۰۴/۰۴/۰۴

تاریخ بازنگری:

۱۴۰۵/۰۴/۰۶

تاریخ پذیرش:

۱۴۰۵/۰۵/۰۲

تاریخ انتشار:

۱۴۰۵/۰۵/۰۹

کلیدواژه‌ها:

جنگ شناختی،

اطلاعات نادرست،

فضای سایبری و

امنیت.

جنگ شناختی، مستلزم انتقال کانون منازعه از حوزه‌های فیزیکی و نظامی به بُعد شناختی است؛ جایی که ادراک، باور، قضاوت و تصمیم‌گیری فردی و جمعی، به هدف اصلی عملیات تبدیل می‌شود. اگرچه این پدیده در ادبیات معاصر به‌عنوان مفهومی نوین مطرح شده است؛ اما هدف بنیادین آن، یعنی تأثیرگذاری بر ذهن و شناخت بازیگران ژئوپلیتیک، ریشه‌ای تاریخی دارد. مسئله‌ی محوری این مقاله، بررسی چگونگی بهره‌گیری از اطلاعات نادرست در جنگ شناختی و تحلیل روندهای اجتماعی‌ای است که زمینه‌ساز افزایش آسیب‌پذیری جوامع در برابر این نوع تهدیدات می‌شوند. نگارنده، در این راستا، می‌کوشد تبیین کند که جوامع چگونه می‌توانند نسبت به خطرات جنگ شناختی آگاه شده و با فنون و سازوکارهای آن آشنایی پیدا کنند. پژوهش حاضر، از نظر ماهیت، کیفی و از حیث روش، توصیفی-تحلیلی است. گردآوری داده‌ها، با بهره‌گیری از دو شیوه‌ی کتابخانه‌ای و میدانی انجام شده است؛ به‌گونه‌ای که در بخش کتابخانه‌ای، اسناد علمی، مقالات پژوهشی، گزارش‌های امنیتی و متون نظری مرتبط با جنگ شناختی، اطلاعات نادرست و روان‌شناسی شناختی مورد بررسی قرار گرفته و در بخش میدانی، نمونه‌ها و مصادیق عینی عملیات شناختی در فضای سایبری و رسانه‌ای تحلیل شده‌اند. تجزیه و تحلیل داده‌ها، مبتنی بر تحلیل مفهومی، استنتاجی و تطبیقی بوده و پیوند میان تحولات شناختی، فناوری‌های نوین و الگوهای نوظهور منازعه بررسی شده است. یافته‌های پژوهش، نشان می‌دهد که اگرچه ماهیت جنگ شناختی پدیده‌ای کهن محسوب می‌شود؛ اما توسعه‌ی دانش روان‌شناسی شناختی، شناخت سوگیری‌های ذهنی و گسترش فضای سایبری و شبکه‌های اجتماعی، موجب افزایش چشمگیر دامنه، سرعت و اثربخشی آن شده است.

استناد:

DOI: <https://doi.org/10.22034/jcwst.2026.562090.1013>



ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

جنگ شناختی، از نگاه برخی پژوهشگران، ششمین حوزه‌ی جنگ به‌شمار می‌رود و ماهیت آن بر تأثیرگذاری و شکل‌دهی به افکار افراد و گروه‌ها متمرکز است. این نوع جنگ، برخلاف عملیات روان‌شناختی سنتی، فقط جمعیت‌ها را مورد هدف قرار نمی‌دهد؛ بلکه در فرایندهای تفکر فردی و گروهی نفوذ می‌کند و بر نحوه‌ی ادراک اطلاعات، شکل‌گیری باورها و احساسات انسانی تأثیر می‌گذارد. این فرایند، در نهایت تصمیم‌گیری انسان را در سطحی ناخودآگاه دست‌کاری می‌کند. درحالی‌که جنگ‌های فرسایشی متعارف، معمولاً دارایی‌ها، منابع فیزیکی یا نیروهای نظامی را هدف قرار می‌دهند، جنگ شناختی، به سطحی عمیق‌تر از ذهن انسان نفوذ کرده و با تغییر و بازآرایی فرایندهای شناختی -ازجمله استدلال، قضاوت و واکنش‌های عاطفی- زمینه را برای تحقق اهداف راهبردی فراهم می‌سازد (Libicki, 2021; Frayssé, 2022).

در واقع بایستی گفت که جنگ شناختی، به استفاده‌ی راهبردی از اطلاعات و تاکتیک‌های روانی با هدف تضعیف عملکردهای شناختی دشمن، اختلال در فرایندهای تصمیم‌گیری و تأثیرگذاری بر اراده‌ی درگیر شدن در نبرد اشاره دارد. همان‌طور که ماهیت جنگ تکامل می‌یابد، عرصه‌ی نبرد از حوزه‌ی فیزیکی به حوزه‌ی شناختی گسترش یافته است؛ حوزه‌ای که در آن به نیاز و تمرکز بیشتر بر دفاع در برابر چنین حملاتی در نیروهای مسلح معاصر تأکید می‌شود. جنگ شناختی، در قالب تلاش‌های پنهان و غیرمستقیم ظهور می‌کند؛ ازجمله کمپین‌های اطلاعات نادرست که برای ایجاد سردرگمی طراحی شده‌اند، انتشار محتوای جعلی عمیق که به‌دروغ به رهبران نسبت داده می‌شود، دست‌کاری رسانه‌های اجتماعی با استفاده از ربات‌ها و مزارع ترول و نیز تبلیغات هدفمند با هدف ایجاد استرس و اضطراب. این تاکتیک‌ها، به‌طور قابل توجهی آمادگی نظامی را مختل کرده، اعتماد اجتماعی و سازمانی را کاهش می‌دهد و در نهایت، کارآمدی تصمیم‌گیری‌ها و مؤلفه‌های راهبردی عملیات نظامی را مختل می‌سازد (van der Linden et al., 2020; Libicki, 2021).

توسعه‌ی راهبردهای مبارزات ضدشناختی منسجم و اخلاق‌محور برای از بین بردن سریع اطلاعات نادرست از طریق جایگزینی آن با اطلاعات واقعی و بی‌اعتبارسازی روایت‌های فریبنده در کانال‌های ارتباطی مختلف، تلاشی بسیار حیاتی در این حوزه‌ی مهم به‌شمار می‌رود. در کنار آن، پرورش نیروی «آگاهی شناختی» در میان کارکنان و نیروهای عملیاتی -از طریق برنامه‌های آموزشی جامع- ضرورتی کلیدی است. این برنامه‌ها باید افراد را به مهارت‌های تشخیص اطلاعات نادرست، ایمن‌سازی در برابر تاکتیک‌های نفوذ و اعتبارسنجی اطلاعات از منابع قابل اعتماد مجهز سازد تا ساختار سازمانی در برابر حملات ادراکی و عملیات فریب تقویت شود.

از آنجاکه فناوری‌های پیشرفته مانند سیستم‌های هوش مصنوعی، ربات‌ها و سیستم‌های بدون سرنشین خودران به اجزای جدایی‌ناپذیر عملیات نظامی تبدیل شده‌اند، مزایای فوق‌العاده‌ای را به‌عنوان افزایش‌دهنده‌ی نیرو ارائه می‌کنند؛ اما در صورت بهره‌برداری توسط دشمنان، آسیب‌پذیری‌های بالقوه‌ای را نیز ایجاد خواهند کرد؛ از این‌رو، اولویت‌دهی به آموزش‌های فناوری‌محور، عملیات شبیه‌سازی‌شده و کسب تجربه‌ی عملی میان کارکنان، برای پرورش مهارت‌های لازم امری حیاتی است. این امر باید همراه با درک عمیق پیامدهای اخلاقی، خطرات امنیتی و نقاط ضعف بالقوه مرتبط با ادغام این قابلیت‌های پیشرفته صورت پذیرد. با توجه به سرعت بی‌وقفه‌ی نوآوری‌های فناوری و تمایل فزاینده‌ی دشمنان به بهره‌برداری از پیشرفت‌ها در راستای اهداف جنگ شناختی، سرمایه‌گذاری در تحقیقات علوم و فناوری دفاعی برای تمامی حاکمیت‌ها -چه غربی و چه شرقی- به‌منظور توسعه‌ی ابزارها و قابلیت‌های لازم برای دفاع در برابر تهدیدات شناختی در همه‌ی حوزه‌های عملیاتی، امری ضروری است (Libicki, 2021; Frayssé, 2022).

شکست روبه‌رشد در مقابله با این تهدیدات در فضای نبرد شناختی، می‌تواند پیامدهای عمیقی بر اثربخشی نیروهای رزمی و امنیت ملی داشته باشد. اکنون به نظر می‌رسد که «جنگ شناختی»، به‌عنوان آخرین رویکرد در حوزه‌ی امنیت تلقی شود (Tsikhelashvili, 2023).

«تهدیدات شناختی»، به آن دسته از فعالیت‌هایی اطلاق می‌شود که مستقیماً بر شناخت انسان، بدون اعمال نیروی فیزیکی یا اجبار قبلی تأثیر می‌گذارد. جنگ شناختی را می‌توان به‌عنوان بخشی از جنگ هیبریدی نیز درک کرد که یکی دیگر از مفاهیم رایج در ادبیات علمی و نظامی است. در واقع جنگ هیبریدی، استفاده‌ی هوشمندانه و البته غیرمستقیم از همه‌ی ابزارها، در تمامی حوزه‌ها و به‌منظور تأثیرگذاری بر ابعاد «فیزیکی، مجازی و شناختی» است. چالش اصلی در اجرای موفقیت‌آمیز جنگ هیبریدی، در همگام‌سازی این قابلیت‌ها و عملیات‌ها، از جمله جنگ شناختی، نهفته است (Mattis, 2023). سیاست «سه جنگ» جمهوری خلق چین، با استفاده از «افکار عمومی، ابزارهای روانی و قانونی» برای دستیابی به پیروزی (Takagi, 2022)، نمونه‌ای معاصر از جنگ هیبریدی-شناختی است. در این رویکرد، هدف نهایی و استراتژیک چین، این است که مستقیماً بر ذهن حریف خود تأثیر گذارد و مقاومت آن را بدون هرگونه درگیری فیزیکی، بشکند.

بررسی‌های پژوهشی، تهدیدات شناختی با استفاده از ابزارهای اطلاعاتی مانند کلمات، روایت‌ها و تصاویر بر ذهن انسان را نشان می‌دهد و این تأثیرگذاری، در قواعد مختلفی بروز می‌یابد. درحالی‌که تأثیرگذاری بر شناخت انسان می‌تواند با استفاده از تکنیک‌های متقاعدکننده‌ی خوش‌خیم باشد، ماهیت بدخیم‌تر یا دست‌کاری‌کننده‌تری نیز در پی خواهد داشت. این روش‌ها،

سابقه‌ی تاریخی دارند؛ در طول جنگ سرد، شوروی و ایالات متحده، از تکنیک‌های شناختی دست‌کاری برای دستیابی به اهداف خود در دکترین مربوط به اقدامات فعال و جنگ سیاسی استفاده کردند. همچنین پیام‌های ساختگی، داده‌های دست‌کاری‌شده یا اطلاعات نادرست، اغلب به‌منظور برانگیختن سوگیری‌های شناختی و اکتشافی انسان، تحت‌تأثیر قرار دادن و دست‌کاری فرایندهای مشورت و تصمیم‌گیری مورد استفاده قرار می‌گرفتند (Rid, 2020).

بیان مسئله

این پژوهش، بر این مسئله‌ی محوری متمرکز است: چگونه اطلاعات نادرست برای تأثیرگذاری بر شناخت سایر بازیگران ژئوپلیتیک مورد استفاده قرار می‌گیرد؟ چه روندی در این زمینه‌ی مهم جریان پیدا خواهد کرد؟ جوامع چطور از خطرات جنگ شناختی آگاه شوند و با فنون آن آشنایی پیدا کنند؟ از منظر پژوهشی، هرچند جنگ شناختی به‌تنهایی عامل پیروزی در میدان نبرد نیست؛ اما اثربخشی آن در حداکثر میزان ممکن تنها از طریق ترکیب و هماهنگی دقیق با سایر ابزارهای قدرت دولتی (مجموعه جنگ هیبریدی) حاصل می‌شود؛ بنابراین، اگر در تاکتیک‌های جنگ شناختی - حتی با نامی جدید- نوآوری خاصی وجود نداشته است، چرا این فعالیت‌ها در قالب اطلاعات نادرست مورد توجه قرار گرفته‌اند؟ علاوه‌بر این، اگرچه به نظر می‌رسد که اطلاعات نادرست، سلاح انتخابی برای تأثیرگذاری بر شناخت انسان است، باید پرسیم که این ابزار مهم چگونه کار می‌کند؟

این تحقیق، در پی ارائه‌ی معرفی فرصت‌ها و چالش‌های جنگ شناختی و استفاده از اطلاعات نادرست در چارچوب یک گزارش توصیفی-تحلیلی است که مبتنی بر مشاهدات و بررسی مطالب علمی بین‌المللی هم‌راستا با موضوع باشد. متعاقباً در شرح نوع دست‌کاری‌های احتمالی توسط اطلاعات نادرست و جنگ شناختی، از روش تحلیلی استنتاجی بهره گرفته شده است. در نهایت، نتایج این تحقیق، راهکارهای پیشنهادی را در راستای پاسخ به سؤال اصلی تحقیق، از دل منابع بازتحلیل‌شده، استخراج و ارائه خواهد کرد.

روش‌شناسی تحقیق

این پژوهش از نظر هدف، توسعه‌ای-تحلیلی و از نظر ماهیت، کیفی است. روش تحقیق به‌صورت توصیفی-تحلیلی انجام شده و بر مطالعه‌ی نظام‌مند ادبیات علمی و اسناد معتبر بین‌المللی در حوزه‌ی جنگ شناختی و اطلاعات نادرست استوار است. داده‌ها از طریق مطالعه‌ی اسنادی، شامل مقالات علمی، گزارش‌های نهادهای نظامی و امنیتی (مانند ناتو) و آثار نظری اندیشمندان این

حوزه گردآوری شده‌اند. تحلیل داده‌ها با استفاده از رویکرد تحلیل مفهومی و استنتاجی و مقایسه‌ی دیدگاه‌های نظری انجام گرفته است. چارچوب تحلیلی پژوهش، بر تبیین پیوند میان جنگ شناختی، اطلاعات نادرست و سوگیری‌های شناختی متمرکز است. روایی پژوهش، از طریق هم‌پوشانی منابع معتبر و تطبیق متقابل داده‌ها تأمین شده است. در نهایت، براساس یافته‌ها، راهکارهای دفاعی و سیاستی برای مقابله با تهدیدات شناختی استخراج و ارائه شده‌اند.

تجزیه و تحلیل

بررسی جریان مفهومی جنگ شناختی در نظام بین‌المللی

جنگ عملیاتی، مستقیماً از طریق اعمالی رخ می‌دهد که هدف آن وادار ساختن حریف به انجام اراده است. تحمیل اراده به حریف را می‌توان از طریق ابزارهای نظامی به‌دست آورد؛ اما از طریق روش‌های دیپلماتیک، اقتصادی یا اطلاعاتی نیز اعمال می‌شود. فیلسوف مشهور عصر باستان چین، «سان تزو»، استدلال کرد که تحت سلطه درآوردن ارتش دشمن بدون جنگ، اوج واقعی برتری است.

بنابراین، می‌توان بین «جنگ» و «جنگ‌ها» تمایز قائل شد؛ جنگ -به‌ویژه در مفهوم حقوقی- درگیری مسلحانه‌ای بین دو یا چند دولت (نهادهای دولتی) است (Sawyer, 1994). در مقابل، جنگ‌ها، عملیاتی است برای تحت سلطه درآوردن سایر گروه‌های دشمن، دوست یا بی‌طرف به هر وسیله‌ای که در دسترس باشد. در همین رابطه، مهاجرت فراملی اجباری، همان‌طور که بین بلاروس و لهستان مشاهده می‌شود (Walker, 2023)، می‌تواند به‌عنوان شکلی از جنگ‌ها، القا یا اجبار تغییر سیاست دیده شود. نتیجه این است که جنگ شناختی، هنر ترغیب بازیگر دیگر به پذیرش اراده‌ی خود با استفاده و تمرکز بر بُعد شناختی است. درحالی که تمامی اشکال جنگ، به‌طور مستقیم یا غیرمستقیم بر اراده‌ی حریف تأثیر می‌گذارند، جنگ شناختی باید از مفاهیم سنتی صرفاً مبتنی بر حملات جنبشی، متمایز گردد.

بی‌تردید، این نوع جنگ مدرن، صرفاً مربوط به قلمرو یا تسلط بر منابع نیست؛ در واقع تضاد بین ادراکات، باورها یا حتی برخورد تمدن‌ها یا فرهنگ‌های مختلف است.

جنگ شناختی پدیده‌ای جدید در قرن پیش رو

در بُعد شناختی، تهدید یا حتی مفهوم جنگ بر سر ادراکات، موضوع چندان جدیدی نیست. این امر، از زمان جنگ پلوپونز و دوباره در جنگ سی‌ساله، جنگ داخلی اسپانیا و اخیراً در طول جنگ سرد مشهود بوده است. هریک از این برخوردها، یک بُعد شناختی روشن مرتبط با برخورد در

جهان‌بینی‌ها، نظام‌های اعتقادی و مذاهب داشتند (Wanless & Berk, 2021). با این حال، تهدیدات شناختی و جنگ، امروزه به دلیل دو تحول کلیدی رایج شده است: نخست، ظهور روان‌شناسی شناختی و دوم، پیدایش فضای مجازی (که منجر به گسترش عامل نخستین شده است). فضای مجازی، بخشی از محیط اطلاعاتی را تشکیل می‌دهد که دولت‌ها همواره از آن در تلاش برای نفوذ استفاده کرده‌اند. پیدایش فضای مجازی، نه تنها لایه‌های جدیدی به فضای اطلاعات اضافه کرده است، بلکه مهم‌تر از آن، قفل محیط اطلاعات را با معرفی لایه‌های مجازی، اشیای مجازی (داده‌ها) و شخصیت‌های مجازی گشوده است. درحالی‌که در گذشته، عملیات اطلاعاتی و نفوذ با استفاده از روش‌های دست‌وپاگیر از جمله پخش جزوه، رشوه، یا پخش رادیویی انجام می‌شد؛ اما امروزه عمدتاً از طریق رسانه‌های اجتماعی انجام می‌شود.



شکل ۱. دلایل بروز تهدیدات شناختی در نظام بین‌المللی (Jayamaha & Matisek, 2018)

توییت یا پیامی مستقیم، می‌تواند با سرعت نور به مویرگ‌های جامعه برسد. علاوه بر این، فضای مجازی برای ایجاد تصاویر مجازی خاص (دیپ‌فیک، واقعیت مجازی)، میم‌ها، شخصیت‌های مجازی (حساب‌های کاربری فیس‌بوک، ایکس [توییتر سابق] یا اینستاگرام) یا دیگر جوامع رسانه‌های اجتماعی مفید است و اطلاعات را به روشی بدون فیلتر، ویروسی و مسری منتشر می‌کند که هرگز محدود به مرزهای ملی نیست.

کنترل بازتابی، تکنیک اولیه در دکترین اقدامات فعال است که با هدف یافتن مزایای راهبردی در محیط اطلاعاتی با فریب، تحریک، براندازی و انتشار اطلاعات نادرست همراه می‌شود (Radin et al., 2020). به عنوان نمونه، روسیه، با همین مکانیسم به عنوان بازیگری مشهور، با بهره‌برداری از سوگیری‌های شناختی، یعنی محدودیت‌های ظرفیت پردازش اطلاعات انسانی، ناخودآگاه بر مخاطبان هدف تأثیر می‌گذارد (Korteling, 2018).

محققان بین‌المللی، از جمله آرکیلا^۱، رونفلد^۲، استینون^۳ و استون^۴، پیش‌بینی کردند که جنگ بعدی، احتمالاً جنگی خواهد بود که در آن فضای سایبری و فعالیت‌های رسانه‌های اجتماعی از اقدامات جنبشی حمایت می‌کنند و یا حتی بالعکس، در آن عملیات سایبری نقش اصلی را بازی می‌کند (Arquilla, & Ronfeldt, 1997). این ایده، پس از مداخله در انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶ و حمله‌ی «نه پتیا»^۵ در سال ۲۰۱۷ به سیستم مالی اوکراین که ظاهراً هر دو توسط بازیگران دولتی (مورد حمایت) روسیه انجام شد، مورد توجه ناظران بین‌المللی قرار گرفت. در حالی که اخیراً جنگ در اوکراین، جنگی نیست که در آن عملیات سایبری غالب باشد، با این وجود، درگیری مداوم در فضای سایبری، بزرگ‌ترین عملیات سایبری است که تاکنون شاهد آن بوده‌ایم (Digital Security Unit, 2022). در جنگ اوکراین، بازیگران دولتی و غیردولتی روسیه و اوکراین، درگیر فعالیت‌های اطلاعاتی (از طریق فضای سایبری یا موارد دیگر) هستند که زیرساخت‌های حیاتی را از طریق حملات سایبری و عملیات نفوذ دیجیتال تضعیف می‌کنند (Schulze & Kerttunen, 2023). این اقدام به نظر کمی عجیب است؛ زیرا مؤثرترین عملیات، حملات سایبری به زیرساخت‌های حیاتی نیست، بلکه فعالیت‌های شناختی با استفاده از فضای سایبری به‌عنوان بُرداری مهم و قابل مشاهده است (Cyber Peace Institute, 2023). در حالی که بیشتر حملات سایبری در طول جنگ روسیه و اوکراین در قالب موانع صرف برچسب‌گذاری می‌شوند (Arnold et al, 2024)؛ اما اثر هم‌زمان عملیات نفوذ دیجیتال از نظر راهبردی برای هر دو طرف، مهم و کلیدی است. اقدامات روسیه، بر جمعیت داخلی تأثیر می‌گذارد و روایت‌های طرفدار با آن باعث ایجاد اختلاف و تضعیف روحیه‌ی اوکراینی می‌شود. با این حال، مؤثرترین فعالیت‌های شناختی، عملیات اوکراینی است که بر مخاطبان غربی در راستای جلب حمایت از آرمان اوکراین تأثیر می‌گذارد که از نظر راهبردی مهم و تأثیرگذار است (Brittain-Hale, 2023).

آناتومی و ساختار اطلاعات نادرست در جنگ شناختی؛ چگونگی کارکرد این اطلاعات

شکی نیست که کلمات، خواه اقناع‌کننده، اجباری و یا دست‌کاری شده، تأثیرگذارند. هدف فعالیت‌های شناختی، تأثیرگذاری بر شناخت انسان بدون تهدید یا تحمیل نیروی جنبشی است

^۱ Arquilla

^۲ Ronfeldt

^۳ Stiennon

^۴ Stone

^۵ حمله‌ی سایبری ژوئن ۲۰۱۷، حملات سایبری در ابعاد جهانی به برخی از بزرگ‌ترین شرکت‌های جهان در آمریکا، اروپا و بخشی از آسیا است که نیروگاه هسته‌ای «چرنوبیل» و شرکت بزرگ نفت و گاز «روس نفت» روسیه را مورد تهاجم قرار داده است.

و هدف نهایی جنگ شناختی، «تداخل مستقیم یا کنترل ناخودآگاه مغز دشمن» است (Takagi, 2021). این جنگ، یک اپراتور را قادر می‌سازد تا «آسیب روحی، سردرگمی و توهّمات را در دشمن ایجاد کند و آن‌ها را مجبور به زمین گذاشتن سلاح و در نهایت تسلیم شدن می‌کند». تمامی عملیات‌های تأثیرگذار، صرفاً از روش‌های ناخودآگاه استفاده نمی‌کنند؛ بلکه عملیات نفوذ اجباری، درک عمدی و فرایند تصمیم‌گیری مستقل، دسترسی مخاطب هدف را کوتاه کرده یا دور می‌زند و آن‌ها را مجبور می‌کند آگاهانه انتخابی «ناخواسته» را انجام دهند. مخاطب هدف، به خوبی از اقدام قهری آگاه است و در مقابل هیچ گزینه‌ی دیگری برای آن باقی نمی‌گذارد.

در همین حال، عملیات نفوذ به‌خودی‌خود بدخیم نیست؛ بلکه از هدف عملیات نفوذ متقاعدکننده، به‌عنوان تغییر وزن و تعداد گزینه‌های موجود برای مخاطبان هدف یاد می‌شود؛ به‌طوری که آن‌ها انتخابی داوطلبانه (مایل به آن را) انجام می‌دهند که اصولاً به نفع عامل تأثیرگذار است. جنگ افکار عمومی جمهوری خلق چین، نمونه‌ای از عملیات نفوذ متقاعدکننده با استفاده از رسانه‌ها، از جمله شبکه‌ی جهانی تلویزیون چین^۱ و گلوبال تایمز، برای ترسیم تصویری خوش‌خیم اما قلاب‌دار از جمهوری خلق چین است (Charon & Vilmer, 2021).

درحالی‌که عملیات نفوذ متقاعدکننده و اجباری از تکنیک‌های عقلانی و آگاهانه استفاده می‌کند، عملیات نفوذ از نوع دست‌کاری، از تکنیک‌های ناخودآگاه و پنهان بهره می‌برد و فرایند تصمیم‌گیری مستقل را واژگون یا غصب می‌کند؛ روشی که اغلب برای انحراف مخاطبان هدف به قضاوت‌های بازتابی و مغرضانه براساس جست‌وجوی شناختی و اجتماعی، به‌جای تأملات عقلانی استفاده می‌شود و «اطلاعات نادرست» نامیده می‌شود.

اطلاعات نادرست، ذاتاً فریبنده است و از روش‌های اکتشافی و سوگیری‌هایی استفاده می‌کند تا مخاطبان هدف را از فرایندهای تصمیم‌گیری منطقی به نفع آنچه پتی^۲ و کاجیوپو^۳ «مسیر پیرامونی» می‌نامند، دور کند. مسیر پیرامونی با فریب دادن مخاطب هدف به سمت موضوعات واقع‌بینانه‌ی اجتماعی (مانند فقر، مسائل نژادی، یا خشونت پلیس) و سپس آسیب رساندن به توانایی آن‌ها در پردازش داده‌های دریافتی مربوط به آن موضوع و با پیوند دادن موضوع به سوگیری‌های ناخودآگاه، هم‌گرایی را شکل می‌دهد. اطلاعات نادرست ارائه‌شده برای آسیب رساندن به مردم، با چارچوبی خاص و متناسب با مخاطبان هدف تنظیم می‌شود. به‌دلیل بار بیش از حد داده‌ها یا کمبود زمان، گروه‌ها یا افراد قادر به تأیید یا درک داده‌های دریافتی نیستند. در انتخابات ۲۰۱۶ ایالات متحده، پُست‌هایی منتشر شد که مناطق و حوزه‌های مذهبی در این کشور

¹ CGTN

² Petty

³ Cacioppo

را هدف قرار می‌داد و ادعا داشت که نامزد کلینتون از برابری جنسیتی حمایت می‌کند یا حتی اظهار می‌کرد که خودش هم‌جنس‌گرا است. افراد عمیقاً مذهبی، برابری جنسیتی یا ازدواج هم‌جنس‌گرایان را قبول ندارند و از این‌رو، احتمالاً کلینتون را به این احساسات منفی متصل می‌کنند. به همین ترتیب، پُست‌هایی مبنی بر حمایت پاپ از ترامپ به اشتراک گذاشته شد (Cialdini, 2007).

اطلاعات نادرست، برخلاف سخنان مشوق نفرت‌انگیز (ترولینگ) یا «داده‌های گمراه‌کننده و ناخواسته عمدی»، با هدف به‌دست آوردن یا کمک به هدفی راهبردی ایجاد می‌شود. اطلاعات نادرست، ظاهری مختلف دارد؛ نخست، ممکن است عمداً دروغ و یا برای فریب دادن ساخته می‌شود. دوم، اطلاعات نادرست زمانی رخ می‌دهد که محتوا و زمینه‌ی یک پیام با هم هماهنگ نباشند. فرض کنید ماکرون، رئیس‌جمهور فرانسه قرار بود سخنرانی رسمی به زبان خارجی یا در حین پخش در خیابان سِسمی ایراد کند. در این صورت، امکان دارد محتوا درست باشد؛ اما به‌دلیل ناسازگاری با زمینه، پیام همچنان گمراه‌کننده خواهد بود. به‌دنبال این منطق، تبلیغاتی که در آن پیام «قاب‌بندی‌شده»، توسط هرکهای «خرس قطبی کارتونی» یا حتی عمداً گمراه‌کننده ارائه می‌شود، نباید اطلاعات نادرست تلقی شود؛ زیرا زمینه‌ی موجود با محتوای پیام، مطابقت نزدیک دارد.

دفاع در برابر جنگ شناختی در فضای نبرد مدرن

جنگ شناختی، به استفاده‌ی راهبردی از اطلاعات و تاکتیک‌های روانی با هدف تضعیف عملکردهای شناختی دشمن، فرایندهای تصمیم‌گیری و تصمیم کلی برای درگیر شدن در جنگ اشاره دارد. همان‌طور که ماهیت درگیری‌ها تکامل می‌یابد، عرصه‌ی نبرد به حوزه‌ی شناختی نیز گسترش یافته و بر نیاز و تمرکز بیشتر بر دفاع در برابر چنین حملاتی در نیروهای مسلح معاصر تأکید می‌شود. در واقع، جنگ شناختی به اشکال مختلفی از تلاش‌های مخفیانه ظاهر می‌شود؛ از جمله کمپین‌های اطلاعات نادرست برای ایجاد سردرگمی، انتشار رسانه‌های جعلی که دروغ به رهبران را نسبت می‌دهند و دست‌کاری رسانه‌های اجتماعی با استفاده از ربات‌ها و مزارع ترول و تبلیغات هدفمند با هدف ایجاد استرس و اضطراب. این تاکتیک‌ها، به میزان قابل توجهی آمادگی نظامی را ضعیف کرده، اعتماد اجتماعی و سازمانی را کاهش می‌دهد و فرایند تصمیم‌گیری و اثربخشی تلاش‌های عملیاتی را مختل می‌سازند (Le Guyader, 2022).

اقدامات دفاعی و پیشگیرانه برای مقابله‌ی مؤثر با تهدیدات جنگ شناختی، امری ضروری و حیاتی است. این اقدام، مستلزم افزایش آگاهی از موقعیت شناختی با بهره‌گیری از قابلیت‌های نظارت،

تجزیه و تحلیل و اسناد پیشرفته برای شناسایی سریع و مقابله با اطلاعات نادرست، دروغ‌های عمیق، روایت‌های فریبنده و عملیات نفوذ است.

به‌علاوه این، تقویت انعطاف‌پذیری شناختی با تقویت شبکه‌ها، نیروها و زیرساخت‌های حیاتی در برابر بهره‌کشی شناختی و مهندسی اجتماعی، بسیار مهم و کلیدی است (New perspectives on cognitive warfare, 2024).

توسعه‌ی استراتژی‌های مبارزات ضدشناختی منسجم و مبتنی بر اخلاق برای از بین بردن سریع اطلاعات نادرست با اطلاعات واقعی و بی‌اعتبار کردن روایت‌های فریبنده در کانال‌های ارتباطی مختلف، تلاشی بسیار حیاتی در این زمینه است. پرورش نیروی «آگاهی شناختی» که شامل برنامه‌های آموزشی جامع برای تجهیز کارکنان به مهارت‌هایی برای تشخیص اطلاعات نادرست، ایمن‌سازی در برابر تاکتیک‌های نفوذ و اعتبارسنجی اطلاعات از منابع قابل اعتماد است، به همان اندازه مهم تلقی می‌شود.

از آنجاکه فناوری‌های پیشرفته مانند سیستم‌های هوش مصنوعی، ربات‌ها و سیستم‌های بدون سرنشین خودران به اجزای جدایی‌ناپذیر عملیات نظامی تبدیل می‌شوند، مزایای فوق‌العاده‌ای را به‌عنوان افزایش‌دهنده‌ی نیرو ارائه می‌کنند؛ اما در صورت بهره‌برداری توسط دشمنان، آسیب‌پذیری‌های بالقوه‌ای را نیز ایجاد می‌کنند؛ از این‌رو، ناتو بایستی آموزش، عملیات و تجربه‌ی عملی برای پرورش مهارت‌های فناوری‌محور بین کارکنان خود را در اولویت قرار دهد و اطمینان حاصل کند که آن‌ها پیامدهای اخلاقی، خطرات و آسیب‌پذیری‌های مرتبط با ادغام این قابلیت‌های پیشرفته را درک می‌کنند (Dawson, 2020). با توجه به سرعت بی‌وقفه‌ی نوآوری‌های فناوری و تمایل فزاینده‌ی دشمنان برای بهره‌برداری از پیشرفت‌ها به‌منظور اهداف جنگ شناختی، سرمایه‌گذاری در تحقیقات علوم و فناوری دفاعی برای ناتو به‌منظور توسعه‌ی ابزارها و قابلیت‌های لازم برای دفاع در برابر تهدیدات شناختی در همه‌ی حوزه‌های عملیاتی، ضروری است. شکست روبه‌رشد در مقابله با این تهدیدات در فضای نبرد شناختی، می‌تواند پیامدهای عمیقی در کاهش اثربخشی نیروهای رزمی و نیز امنیت ملی داشته باشد (Hung & Hung, 2022).

حفاظت در برابر اطلاعات نادرست

مقابله با اطلاعات نادرست نه تنها از نظر عملی، بلکه از نظر حقوقی و اخلاقی نیز بسیار چالش‌برانگیز است. افزایش آگاهی و بهداشت دیجیتال برای افزایش انعطاف‌پذیری در جامعه مفید خواهد بود؛ به‌ویژه زمانی که نسبت دادن به کمپین‌های اطلاعات نادرست دشوار است. با این حال، تنش‌ی اساسی برای سیستم‌های دموکراتیک باز و شفاف وجود دارد؛ از یک سو، تمایل به توقف یا مقابله

با کمپین‌های اطلاعات نادرست توسط بازیگران متخاصم مانند روسیه همواره دیده می‌شود (Hoyle & Pijpers, 2022)؛ و ازسوی دیگر، «حفظ ارزش‌هایی که دموکراسی غربی بر پایه‌ی آن بنا شده است (آزادی اطلاعات و بیان)، برای حفظ آن و مشروعیت نهادهای دموکراتیک مهم است».

نقض این ارزش‌ها، به‌عنوان عملی ریاکارانه به تصویر کشیده می‌شود و توسط بازیگران متخاصم بیشتر مورد سوءاستفاده قرار می‌گیرد. نمونه‌ای از آن ممنوعیت «روسیه‌ی امروز» (آرتی) و اسپوتنیک توسط اتحادیه‌ی اروپا در سال ۲۰۲۲ است که در درجه‌ی نخست، اعتراض آژانس‌های روزنامه‌نگاران اتحادیه‌ی اروپا را برانگیخت؛ زیرا اصول و آزادی‌های اساسی که در قوانین بین‌المللی حقوق بشر بیان شده (مانند کنوانسیون اروپایی حقوق بشر که فدراسیون روسیه نیز عضو آن بوده) را نقض کرد.

هلمن^۱ و واگنسسون^۲، چهار راه را برای مقابله با جنگ اطلاعاتی روسیه و دشمنان دنیای غرب از نگاه خود طبقه‌بندی کرده‌اند که از یک سو براساس مفهوم درگیری و یا عدم درگیری و ازسوی دیگر، بر پایه‌ی تمرکز درونی بر مخاطبان داخلی یا بیرونی برنامه‌ریزی شده است. راه‌های مطرح‌شده عبارت‌اند از: (۱) رویارویی، (۲) مسدود کردن، (۳) طبیعی‌سازی و (۴) نادیده گرفتن. همچنین این الگو می‌تواند برای ارزیابی کلی‌تر مقابله با اطلاعات نادرست مورد استفاده قرار گیرد. ممنوعیت «آرتی» و «اسپوتنیک»، نمونه‌ای از جلوگیری انتشار اطلاعات نادرست از رسانه‌های روسی برای ترویج روایت جنگ طرفدار روسیه در زمانی است که اعضای اتحادیه‌ی اروپا حمایت خود را از اوکراین ابراز می‌کردند. «اطلاعات بلاک»^۳ جمهوری خلق چین، بخشی از اقدامات تقابلی آن و نمونه‌ی دیگری از این راه به‌شمار می‌رود و هدف آن، مسدود کردن و محافظت فعال از جمعیت داخلی است (Charon & Vilmer, 2021).



^۱ Hellman

^۲ Wagnsson

^۳ بلاک، در رایش، به‌ویژه مبحث انتقال داده و ذخیره‌سازی، دنباله‌ای از بیت‌ها یا بایت‌ها است که طول ثابتی دارد. فرایند قرار دادن داده‌ها در بلاک‌ها را بلاک‌بندی می‌گویند و داده‌هایی که از چنین ساختاری برخوردارند، داده‌های بلاک‌بندی‌شده نام دارند. بلاک‌بندی، برای تسهیل کردن نقل‌وانتقال اطلاعات استفاده می‌شود.

شکل ۲. چهار راه برای مقابله با جنگ اطلاعاتی (هلمن و واگنسون)

روشی منفعل‌تر می‌تواند کمپین‌های آگاهی در برابر اطلاعات نادرست متخاصم در رسانه‌های اجتماعی یا بسته‌های آموزشی برای دانش‌آموزان دبیرستانی باشد که نتیجه‌ی آن، نادیده گرفتن اطلاعات نادرست خواهد بود. این روند، در انتخابات میان‌دوره‌ای ۲۰۱۸ و انتخابات ریاست‌جمهوری ۲۰۲۰ آمریکا قابل توجه بود. پس از افشای دخالت روسیه در انتخابات ریاست‌جمهوری ۲۰۱۶، رأی‌دهندگان درخصوص پیام‌هایی که در شبکه‌های اجتماعی پخش می‌شد، دیگر ساده‌لوح نبودند. همچنین یک بُعد می‌تواند بر منبع اطلاعات نادرست یا آنچه گیرنده به‌عنوان چنین اطلاعاتی درک می‌کند، تمرکز داشته باشد. یک گزینه‌ی خوش‌خیم، تقویت ارزش‌های اصلی جامعه‌ی خود و متقاعد کردن سایر کشورها برای پذیرش این ارزش‌ها است. بسیاری از کشورهای غربی، از حقوق بشر فردی در کشورهای دارای حقوق بشر جمعی حمایت می‌کنند. راهکار دیگر، مقابله‌ی مستقیم و قاطعانه با اطلاعات نادرست و به عبارتی، مقابله‌ی آتش با آتش است. فعالیت‌های مخفیانه‌ی نیروهای مسلح، به‌ویژه سرویس‌های اطلاعاتی دولتی، می‌تواند در سیاست مقابله‌ای ضداطلاعات غلط نقش مؤثری داشته باشد. این مسئله، نشان می‌دهد که سازمان‌های دولتی پایین‌تر از آستانه‌ی استفاده از نیروی مسلحانه عمل می‌کنند و اغلب این اقدامات، در صلاحیت دولت دیگری قرار می‌گیرد؛ و این امر می‌تواند عواقب قانونی داشته باشد؛ زیرا این فعالیت‌ها ممکن است فراتر از جاسوسی سنتی باشند (Social Sciences in China, 2017). به‌طرز متناقضی، بسیاری از کشورهای غربی، چارچوب قانونی و عرفی محکمی برای استقرار نیروهای نظامی جنبشی دارند. باین‌حال، آن‌ها تمایل بسیار کمی به استقرار نیروهای امنیتی در حوزه‌ی شناختی و در مناطقی با اثرات زیر آستانه‌ی نیروی فیزیکی از خود نشان می‌دهند.

سوگیری‌های شناختی؛ زیربنای روانی در بروز اطلاعات نادرست در جامعه‌ی هدف

سوگیری‌های شناختی، الگوهای سیستماتیک انحراف از هنجار یا عقلانیت در قضاوت است که اغلب به‌دلیل تلاش مغز برای ساده‌سازی و پردازش اطلاعات رخ می‌دهند. آن‌ها می‌توانند به‌طور قابل توجهی بر فرایندها و رفتارهای تصمیم‌گیری تأثیر گذارند و همچنین به ابزاری قدرتمند در جنگ شناختی تبدیل شوند.

برخی از سوگیری‌های کلیدی و مهم مورد استفاده در جنگ شناختی عبارت‌اند از:

- **سوگیری تأیید:** تمایل به جست‌وجو، تفسیر، حمایت و یادآوری اطلاعات، به‌گونه‌ای که باورها یا فرضیه‌های قبلی فرد را تأیید می‌کند.

- **اکتشافی و در دسترس بودن:** برآورد بیش از حد اهمیت اطلاعاتی که به راحتی در دسترس هستند و اغلب برای دست کاری درک عمومی، با در معرض تکرار قرار گرفتن، مورد استفاده قرار می گیرد (Tversky & Kahneman, 1974).
- **تعصب لنگر انداختن:** این سوگیری، تمایل انسان به اتکای بیش از حد، به اولین بخش از اطلاعات ارائه شده هنگام تصمیم گیری را مطرح می سازد (Furnham & Boo, 2011).

دیدگاه جامعه شناختی در زمینه انتشار اطلاعات نادرست

اطلاعات نادرست، زمانی منتشر می شود که اطلاعات فریبنده یا گمراه کننده وجود دارد و اغلب توسط بسترهای^۱ رسانه های اجتماعی تقویت می شود. نظریه های جامعه شناختی، نشان می دهند که گسترش اطلاعات نادرست از طرق زیر صورت می پذیرد:

اثبات اجتماعی: مردم به مطابقت با آنچه فکر می کنند و دیگران انجام می دهند، تمایل دارند و این روند به دلیل محبوبیت اطلاعات نادرست و ویروسی، معتبر به نظر می رسد.

قطبش گروهی: پدیده ای است که در آن، نگرش های غالب یک گروه با گذشت زمان شدیدتر می شود و برای عمیق تر کردن شکاف های اجتماعی، مورد سوءاستفاده قرار می گیرد.

نتیجه گیری

جنگ شناختی می تواند با انتشار اطلاعات نادرستی که با باورهای از پیش موجود فرد هم سو است، جوهره ی «هویت» فرد را مورد دست کاری قرار دهد و وابستگی های گروهی قوی تری را نسبت به آنچه به طور ارگانیک احساس می شود، در جامعه ی هدف تقویت کند. علاوه بر این، اگر پیامی منجر به ناهماهنگی شناختی شود، استفاده از این وضعیت روانی، ناراحت کننده بوده و ارائه ی پیامی که ناهماهنگی درونی را برطرف می کند، بسیار ساده و بدون پیچیدگی است. علاوه بر این، اصل «هزینه ی غیریکنواخت اطلاعات»، از سوگیری افراد برای تکیه بر شواهدی که به راحتی به دست می آیند، سوءاستفاده می کند؛ به ویژه اگر ناراحتی روانی، ناشی از ناهماهنگی شناختی باشد. به علاوه، اطلاعاتی که دارای ظرفیت منفی هستند، به راحتی قابل باور بوده و با دیگران به اشتراک گذاشته می شوند.

دانشمندان شناختی، عصب شناسان، روان شناسان، مهندسين کامپیوتر و سایبری، در ابتدا برای مقابله ی مؤثر با تلاش های جنگ شناختی خصمانه و برای حمایت از دستور کار جنگ تهاجمی، باید در تلاشی ملی و فراگیر هماهنگ شوند. ایجاد اتاق عملیات مشترک شناختی و راهبردهایی

¹ Platform

برای دفاع در برابر حملات شناختی، به‌منظور محافظت از جمعیت داخلی و رهبران از اثرات بی‌ثبات‌کننده، امری کاملاً ضروری است. همچنین برای مقابله‌ی مؤثر با تهدیدات جنگ شناختی، اقدامات دفاعی و پیشگیرانه، امری حیاتی است. این اقدام، مستلزم افزایش آگاهی از موقعیت شناختی با بهره‌گیری از قابلیت‌های نظارت، تجزیه‌وتحلیل و اسناد پیشرفته برای شناسایی سریع و مقابله با اطلاعات نادرست، دروغ‌های عمیق، روایت‌های فریبنده و عملیات نفوذ است. علاوه‌بر این، تقویت انعطاف‌پذیری شناختی با تقویت شبکه‌ها، نیروها و زیرساخت‌های حیاتی در برابر بهره‌کشی شناختی و مهندسی اجتماعی، بسیار مهم و کلیدی است.

جنگ شناختی، امنیت ملی و فرایندهای تصمیم‌گیری جمعیت‌های درگیر در این نوع جنگ مدرن را در سطح بی‌سابقه‌ای تحت‌تأثیر قرار می‌دهد؛ بنابراین، ایجاد اتاق عملیات مشترک شناختی برای دفاع در برابر این حملات، امری بسیار ضروری است. به‌علاوه، برای تغییر طرز فکر و عمل دشمنان، لازم است همانند رویکرد چینی‌ها و روس‌ها، فرماندهی جنگ شناختی با دقت و حساسیت بالا ایجاد شود. تاکنون در بسیاری از جوامع، از جمله وزارت دفاع ایالات متحده، هیچ دکترین جامعی در این زمینه تدوین نشده است. حتی اگر ناتو جنگ شناختی را مهم‌ترین میدان نبرد زمان کنونی نامیده باشد، دنیای غرب نه‌تنها بایستی دانشمندان شناختی، روان‌شناسان، مهندسين کامپیوتر و سایبری و دانشمندان علوم اعصاب را در تلاشی فراملی برای دفاع از خود در برابر اثرات بی‌ثبات‌کننده‌ی ویرانگر جنگ شناختی گرد هم آورد، بلکه لازم است فرماندهی جنگ شناختی و راهبردهایی را به کار گیرد تا از جمعیت و رهبران در برابر تلاش‌های خصمانه‌ی شناختی، محافظت نماید.

به‌طور خلاصه، اگر تمامی جوامع بشری به این حوزه‌ی مهم توجه نکنند، در این جنگ شکست خواهند خورد و ایجاد قابلیت‌های تهاجمی و دفاعی در این حوزه‌ی ششم جنگ، اقدامی کاملاً ضروری است.

هرچند ماهیت جنگ شناختی، مفهومی کهن است؛ اما توسعه‌ی روان‌شناسی شناختی و آغاز به کار فضای سایبری، به جنگ شناختی دامنه‌ی گسترده‌تری بخشیده و اثربخشی آن را به‌طور چشمگیری افزایش داده است. جنگ شناختی می‌تواند ابزار مفیدی در جعبه‌ابزار ترکیبی یک دولت یا بازیگران دولتی و یا حتی غیردولتی باشد. با این حال، نزاع، رقابت، یا حتی جنگ و درگیری مسلحانه بین دولت‌ها، تنها در صورتی می‌تواند نتیجه‌ساز باشد که تعامل بین جنگ جنبشی، اطلاعاتی و شناختی هماهنگ و هم‌سو شود و لازم است این عناصر دارای وحدت هدف و هماهنگی در اجرا باشند. جنگ شناختی، به‌تنهایی عامل پیروزی نهایی نخواهد بود؛ زیرا اطلاعات نادرست که تکنیکی ضروری برای انجام این نوع جنگ است، به‌طور مستقیم بر شناخت انسان

تأثیر می‌گذارد. اطلاعات نادرست، با استفاده از چارچوب‌ها، روایت‌ها یا تصاویر دارای زمینه یا محتوای عمداً گمراه‌کننده، از دست‌کاری ناخودآگاه مغز انسان بهره می‌برد و با توسل به اکتشافات و سوگیری‌های شناختی، فرایند تصمیم‌گیری منطقی را دور می‌زند. حال در این راستا، چه روندی رخ می‌دهد؟ چه معنایی برای عملیات در جنگ شناختی و اطلاعات نادرست آینده وجود دارد؟

درحالی‌که پیشرفت‌ها و چالش‌های متعددی به ذهن متبادر می‌شود، در این پژوهش، سه مورد برجسته‌تر از سایرین است:

۱. **فناوری‌های جدید** (مانند مدل‌های زبان بزرگ هوش مصنوعی، از جمله چت.جی.پی.تی)؛ به‌عنوان مولد اطلاعات نادرست. از آنجاکه آناتومی این نوع اطلاعات براساس عملکرد شبکه‌های عصبی ما انجام می‌پذیرد، اطلاعات نادرست نیز می‌تواند براساس الگوریتم‌های موجود تولید شود. تجزیه و تحلیل کلان‌داده‌ها می‌تواند رفتار را براساس همبستگی‌ها به‌جای علیت پیش‌بینی کند و با استناد به حالتی تقریباً قطعی از رفتار انسان است. اطلاعات نادرست آینده، توسط انسان‌های حيله‌گر ساخته نمی‌شود، بلکه با قدرت محاسباتی محض ساخته خواهد شد و آن را حتی قدرتمندتر و در عین حال گریزان و غیرقابل کنترل می‌کند.

۲. **احتمال هجوم بازیگران خصوصی و غیردولتی وجود دارد**؛ اگر اطلاعات نادرست ابزاری برای به‌دست آوردن مزایای راهبردی باشد، تصور می‌شود که بازیگران دولتی آن را تحریک خواهند کرد. درحالی‌که منابع این بازیگران تقریباً نامحدود است؛ اما تعداد بازیگران محدود بوده و اقدامات آن‌ها نیز توسط مرزهای قانونی و اخلاقی که منعکس‌کننده جهان‌بینی‌ها و فرهنگ‌های آن‌ها است، محدود می‌شود. با هجوم بازیگران غیردولتی، تعداد بازیگران به‌طور تصاعدی افزایش یافته و اگر آن‌ها مایل یا قادر به استفاده از فناوری‌های جدید باشند، ممکن است به مجموعه‌ای فزاینده از بازیگران در درگیری و جنگ تبدیل شوند که تحت‌تأثیر قوانین بین‌المللی قرار نگرفته‌اند؛ که نمونه‌هایی از این امر، در طول کارزار اخیر روسیه در اوکراین دیده شده است.

۳. **در نهایت، تهدید در بُعد شناختی در عدم تقارن بین جهان‌بینی‌ها، به‌ویژه بین لیبرال دموکرات و اقتدارگرا، بین دولت‌ها یا حتی درون یک حاکمیت نهفته است.** جهان‌بینی‌های متفاوت، نباید در جامعه‌ای سالم مشکل‌ساز باشد. وجود آن‌ها، منعکس‌کننده ارزش‌های اصلی دموکراتیک و آزادی بیان است. با این حال، اگر گروه‌هایی در جامعه در حباب‌های رسانه‌های اجتماعی که دیگر به هم متصل نیستند، محبوس شوند، به‌مرور چنین مسئله‌ای مشکل‌ساز خواهد شد.

توصیه‌های کلیدی

سیاست‌گذاران دفاعی، باید بُعد شناختی را به‌عنوان حوزه‌ای مستقل و رسمی در دکتین دفاعی به رسمیت بشناسند و آن را هم‌تراز با سایر حوزه‌های عملیاتی تعریف کنند. آموزش نظام‌مند سواد شناختی، تفکر انتقادی و تصمیم‌گیری مبتنی بر شواهد برای فرماندهان و نیروهای مسلح باید به‌منظور کاهش اثر سوگیری‌های شناختی در اولویت قرار گیرد. ایجاد سازوکارهای دائمی پایش و هشدار زودهنگام شناختی برای شناسایی عملیات اطلاعات نادرست و دست‌کاری ادراکی پیش از تبدیل‌شدن به بحران امنیتی، امری ضروری است. به‌کارگیری هوش مصنوعی و تحلیل داده‌های کلان در دفاع شناختی باید هم‌زمان با تدوین چارچوب‌های اخلاقی و حقوقی شفاف انجام شود. هماهنگی نهادی میان بخش‌های نظامی، اطلاعاتی، رسانه‌ای و مدنی برای افزایش تاب‌آوری شناختی جامعه، اهمیت راهبردی دارد. مفهوم بازدارندگی، باید بازتعریف شود تا پاسخ‌گویی مؤثر به تهدیدات شناختی زیر آستانه‌ی درگیری نظامی را نیز در بر گیرد. در نهایت، حمایت پایدار از پژوهش‌های میان‌رشته‌ای علوم شناختی و رفتاری، شرط اساسی انطباق سیاست دفاعی با الگوهای نوظهور جنگ شناختی است.

منابع

- Arnold, K., Pijpers, P., Ducheine, P., & Schrijver, P. (2024). Assessing the Dogs of Cyberwar: Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War. *e R U*, 231.
- Arquilla, J., & Ronfeldt, D. (1997). *In Athena's camp: Preparing for conflict in the information age*. Rand corporation.
- Brittain-Hale, A. (2023). Clausewitzian Theory of War in the Age of Cognitive Warfare. *The Defense Horizon Journal*.
- Charon, P., & Vilmer, J. B. J. (2021). Chinese influence operations: A machiavellian moment. *Report by the Institute for Strategic Research (IRSEM), Paris, Ministry for the Armed Forces*.
- Cialdini, R. B. (2007). *Influence: the psychology of persuasion* (Revision Edition). New York: Harper.
- Claverie, B., Prébot, B., Buchler, N., & Du Cluzel, F. (2022). Cognitive Warfare: The Future of Cognitive Dominance. *Bruxelles: NATO Science and Technology Organization*, 2022-03.
- Cyber Peace Institute. (2023). *Cyber Dimensions of the Armed Conflict in Ukraine*.
- Dawson, J. (2021). Microtargeting as information warfare. *The Cyber Defense Review*, 6(1), 63-80. doi: 10.31235/osf.io/5wzuq.
- Digital Security Unit. (2022). Special Report: Ukraine – An Overview of Russia's Cyberattack Activity in Ukraine. *Microsoft*, 2022; Office for Budget Responsibility, *Fiscal Risks and Sustainability*, 49-50.

- Frayssé, O. (2022). *Cognitive warfare: The battle for hearts and minds*. NATO Strategic Communications Centre of Excellence.
- Hellman, M., & Wagnsson, C. (2017). How can European states respond to Russian information warfare? An analytical framework. *European Security*, 26(2), 153-170.
- Hoyle, A., & Pijpers, P. (2022). Stemming the Narrative Flow: The Legal and Psychological Grounding for The European Union's Ban on Russian State-Sponsored Media. *Defence Strategic Communications*, 11, 51-80, <https://doi.org/10.2139/ssrn.4220510>.
- Iasiello, E. (2016). China's three warfares strategy mitigates fallout from cyber espionage activities. *Journal of Strategic Security*, 9(2), 45-69.
- Jayamaha, B. B., & Matissek, J. (2018). Social media warriors: Leveraging a new battlespace. *The US Army War College Quarterly: Parameters*, 48(4), 4.
- Korteling, J. E., Brouwer, A. M., & Toet, A. (2018). A neural network framework for cognitive bias. *Frontiers in psychology*, 9, 1561.
- Korteling, J. E., Duistermaat, M., & Toet, A. (2018). Subconscious manipulation in psychological warfare.
- Le Guyader, H. (2022). Cognitive domain: A sixth domain of operations. *Cognitive Warfare: The Future of Cognitive Dominance*, 3-1.
- Mattis, P. (2018). China's 'Three Warfares' in Perspective. *War on the Rocks*, 30.
- Libicki, M. C. (2021). *The cognitive domain of warfare*. Center for Technology and National Security Policy, National Defense University.
- New perspectives on cognitive warfare. Accessed: Feb. 25, 2024. [Online]. Available: <https://www-spiedigitalibrary-org.wrs.idm.oclc.org/conference-proceedings-of-spie/12547/125470I/New-perspectives-on-cognitive-warfare/10.1117/12.2666777.full>.
- Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. L. Berowitz (Ed.), *Advances in Experimental Psychology* Vol. 19, pp. 124-203.
- Radin, A., Demus, A., & Marcinek, K. (2020). Understanding Russian subversion: Patterns, threats, and responses.
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Ross, A. (2016). Will the Next War Be a Cyberwar. *Policy Review*, 16-19.
- Sawyer, R. D. (Ed.). (1994). *The art of war* (Vol. 68). Westview Press.
- Schulze, M., & Kerttunen, M. (2023). *Cyber operations in Russia's war against Ukraine: Uses, limitations, and lessons learned so far* (No. 23/2023). SWP Comment.
- Stiennon, R. (2015). *There Will Be Cyberwar*. IT-Harvest Press.
- Takagi, K. (2022). The future of China's cognitive warfare: lessons from the war in Ukraine. *War on the Rocks*, 22.
- Thomas, T. (2004). Russia's reflexive control theory and the military. *Journal of Slavic Military Studies*, 17(2), 237-256.
- Tsikhelashvili, N. (2023). Cognitive Warfare Through Reflexive Control Strategy In Georgia. *The Defence Horizon Journal*.

- United States Senate Committee on Intelligence (2019). Report on Russian Active Measures Campaigns and Interference in the 2016 U.S. *Election – Russia's Use of Social Media*. 2, 12-13.
- Van Der Linden, S., Roozenbeek, J., & Compton, J. (2020). Inoculating against fake news about COVID-19. *Frontiers in Psychology*, 11, 566790.
- Von, C.C. (1989). *On War*, ed. Michael Howard and Peter Paret (Princeton University Press), 75.
- Walker, S. (2023). Beatings, Dog Bites, and Barbed Wire: Life and Death on the Poland-Belarus Border, *The Guardian*, <https://www.theguardian.com/world/2023/oct/02/beatings-dog-bites-and-barbed-wire-life-and-death-on-the-poland-belarus-border>.
- Wanless, A., & Berk, M. (2021). The Changing Nature of Propaganda. in *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*, ed. T. Clack and R. Johnson, 1st ed, Routledge, 66.
- Zhipeng, H. (2017). The Chinese Expression of the International Rule of Law. *Social Sciences in China*, 38(3), 175-188.