IRI Military Command and Staff University

Quarterly Journal of Cognitive Warfare Sciences and Technologies

https://www.jcwst.ir/

Online: 2645-7172

Designing a Model for Technology-Driven Cognitive Threats in the Cyberspace Domain

Farzad Kazemi[1] |

1. Faculty of command & staff, University, Tehran, Iran. f.kazemi@causu.ac.ir

Article Info

Article type:

Research Article

Article history:

Received

28 Nov 2025

Received in revised form

10 Dec 2025

Accepted

16 Dec 2025

Published online

19 Dec 2025

Keywords:

Cognitive Threats, Technology-Driven, Cyberspace, Cyber Warfare, Cognitive Security, Structural Equation Modeling

ABSTRACT

Background and Objective: With the rapid evolution of cyber technologies, a new domain of threats centered on cognitive manipulation has emerged. These threats, which ultimately aim to influence human perception, beliefs, and decision-making, have a complex and technology-driven nature. This study aimed to design a model of technology-driven cognitive threats in the cyberspace domain.

Methods: This research was conducted using a sequential exploratory mixed-methods approach. In the qualitative phase, semi-structured interviews were conducted with 15 experts in cybersecurity and cognitive warfare. The data were analyzed using MAXQDA software through theoretical coding (open, axial, and selective). In the quantitative phase, the statistical population consisted of 210 managers and specialists in the cyber field, selected through stratified random sampling. The data collection tool was a researcher-made questionnaire whose validity and reliability were confirmed. Quantitative data were analyzed using SmartPLS software and structural equation modeling.

Findings: The qualitative findings led to the extraction of 7 main categories (Driving Technologies, Cognitive Targets, Influence Strategies, Dissemination Platforms, Security Consequences, Organizational Actors, and Operation Timing) and 21 concepts. Quantitative findings showed that all relationships between the categories were significant. The strongest relationship was observed between Cognitive Targets and Security Consequences (β=0.79), followed between Driving Technologies and Cognitive Targets (β=0.73). The model fit indices (GoF=0.65) and R^2 values (0.71 for Security Consequences and 0.69 for Cognitive Targets) confirmed the desirable fit of the model.

Conclusions: The designed model reveals that technology-driven cognitive threats are a complex and multidimensional phenomenon in which emerging technologies target cognitive objectives through digital platforms, leading to security consequences. This model can serve as a suitable basis for designing defensive and countermeasure strategies against cognitive cyber threats.

Cite this article: Author, A. A., Author, B. B., & Author, C. C. (year). Article title. *Journal Title*, 56 (1), 1-20.

DOI: https://www.jcwst.ir/article_236370.html

Publisher: IRI Military Command and Staff University

فصلنامه علمی علوم و فناوری‌های جنگ شناختی
https://www.jcwst.ir/
شاپای الکترونیکی: ۲۶۴۵-۷۱۷۲
دانشگاه فرماندهی و ستاد آجا

طراحی الگوی تهدیدات شناختی فناوری‌محور در عرصه فضای سایبر

فرزاد کاظمی[۱] |
دانشجوی دکتری مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. farzadkazmiuod@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:
تاریخ دریافت:
۱۴۰۴/۰۹/۰۷
تاریخ بازنگری:
۱۴۰۴/۰۹/۱۹
تاریخ پذیرش:
۱۴۰۴/۰۹/۲۵
تاریخ انتشار:
۱۴۰۴/۰۹/۲۸

کلیدواژه‌ها:
تهدیدات شناختی، فناوری‌محور، فضای سایبر، جنگ سایبری، امنیت شناختی، مدل‌سازی معادلات ساختاری.

چکیده

زمینه و هدف: با تحولات پرشتاب فناوری‌های سایبری، عرصه جدیدی از تهدیدات با محوریت دستکاری شناختی شکل گرفته است. این تهدیدات که هدف نهایی آن‌ها تاثیرگذاری بر ادراک، باورها و تصمیم‌گیری انسان‌ها است، ماهیتی پیچیده و فناوریمحور دارند. پژوهش حاضر با هدف طراحی الگوی تهدیدات شناختی فناوری‌محور در عرصه فضای سایبر انجام شد.

روش‌ها: این پژوهش با رویکرد آمیخته انجام شد. در بخش کیفی، با ۱۵ متخصص حوزه سایبری و جنگ شناختی مصاحبه نیمه ساختاریافته شد و داده‌ها با نرم‌افزار MAXQDA و از طریق کدگذاری نظری (کدگذاری باز، محوری و انتخابی) تحلیل گردید. در بخش کمی، جامعه آماری شامل ۱۱۰ نفر از مدیران و متخصصان حوزه سایبری بود که با روش نمونه‌گیری تصادفی طبقه‌ای انتخاب شدند. ابزار گردآوری داده‌ها پرسشنامه محقق ساخته بود که روایی و پایایی آن تأیید شد. داده‌های کمی با نرم‌افزار SmartPLS و روش مدل‌سازی معادلات ساختاری تحلیل شد.

یافته‌ها: یافته‌های کیفی منجر به استخراج ۷ مقوله اصلی (فناوری‌های محرک، اهداف شناختی، راهبردهای تاثیرگذاری، بسترهای انتشار، پیامدهای امنیتی، عوامل سازمانی و زمان‌بندی عملیات) و ۲۱ مفهوم شد. یافته‌های کمی نشان داد تمامی روابط بین مقوله‌ها معنی‌دار هستند. قوی‌ترین رابطه بین اهداف شناختی و پیامدهای امنیتی و سپس بین فناوری‌های محرک و اهداف شناختی مشاهده شد. شاخص‌های برازش مدل و مقادیر R^2 (برای پیامدهای امنیتی ۰/۷۱ و برای اهداف شناختی ۰/۶۹) برازش مطلوب مدل را تأیید کردند.

نتیجه‌گیری: الگوی طراحی شده نشان می‌دهد تهدیدات شناختی فناوری‌محور، پدیده‌ای پیچیده و چندبعدی است که در آن فناوری‌های نوین از طریق بسترهای دیجیتال، اهداف شناختی را نشانه رفته و منجر به پیامدهای امنیتی می‌شوند. این الگو می‌تواند مبنای مناسبی برای طراحی راهبردهای دفاعی و مقابله‌ای در برابر تهدیدات شناختی سایبری باشد.

استناد: نام خانوادگی، نام؛ نام خانوادگی، نام؛ و نام خانوادگی، نام (سال). عنوان مقاله. *عنوان مجله*، ۲ (۴)، ۱-۲۰.
DOI: https://www.jcwst.ir/article_236370.html

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

.

مقدمه؛

جهان معا صر شاهد دگرگونی بنیادین در عر صه منا سبات امنیتی و تهاجمات راهبردی ا ست، به‌گونه‌ای که ف ضای سایبر به عنوان عر صه‌ای نوین، نه تنها بستری برای تبادل اطلاعات، که به یک حوزه نبرد تمام‌عیار تبدیل شـــده اســـت. در این میان، پیچیده‌ترین و موذی‌ترین گونه تهدیدات، تهدیدات شـناختی هسـتند که هدف نهایی آن‌ها نه سـیسـتم‌های رایانه‌ای، بلکه قوه ق ضاوت، باورها و اراده ان سان‌ها ا ست (Masakowski & Colleagues, 2023) . این تهدیدات با بهره‌گیری از فناوری‌های پیشـرفته‌ای همچون هوش مصـنوعی، دیپ‌فیک، ربات‌های اجتماعی و مهندسـی اطلاعات، به‌صـورت سـازمان‌یافته به دسـتکاری ادراکات فردی و جمعی می‌پردازند (Snider et al, 2021). اگرچه مطالعات پراکنده‌ای به بررسی جنبه‌های مختلف جنگ سایبری یا جنگ شـــناختی پرداخته‌اند، اما تمرکز غالب آن‌ها بر روی جنبه‌های فنی امنیت ســـایبری یا تاکتیک‌های روانی به صـــورت مجزا بوده اســـت. آنچه در ادبیات موجود به عنوان یک شـــکاف پژوهشـــی بارز خودنمایی می‌کند؛ نبود یک الگوی جامع اســـت که بتواند نحوه تعامل و تقویت متقابل فناوری و شناخت را در چارچوب یک مدلی یکپارچه تبیین نماید. به عبارت دیگر، پاسخ رو شنی به این پر سش ا سا سی وجود ندارد که فناوری‌های نوظهور سایبری چگونه به صورت سیستماتیک، چرخه حیات تهدیدات شناختی را شکل داده و تقویت می‌کنند؟

تمرکز این مقاله بر طراحی الگوی تهدیدات شناختی فناوری‌محور در عر صه فضای سایبر ا ست. ضرورت انجام این پژوهش را می‌توان در چند محور خلاصه کرد: اولاً، درک این الگو برای تدوین راهبردهای دفاعی و پدافند غیرعامل در برابر جنگ های ترکیبی نوین حیاتی اســـت. ثانیاً، سـیاسـت‌گذاران و فرماندهان نظامی برای اتخاذ تصـمیمات آگاهانه در شـرایط بحران، نیازمند درکی عمیق از مکانیســـم‌های پنهان این تهدیدات هســـتند. ثالثاً، جامعه علمی برای توســـعه چارچوب‌های نظری و روش‌های مقابله‌ای، به یک نق شه راه رو شن از این پدیده نیاز مبرم دارد. ارمغان این پژوهش برای جامعه علمی و دفاعی، ارائه یک الگوی بوم‌شـــناختی اســـت که در آن، ارتباط پویا بین مولفه‌های فناورانه (مانند ابزارها)، مولفه‌های شناختی (مانند باورها و تصمیمات) و مولفه‌های کنشـــگری (مانند بازیگران دولتی و غیردولتی) ترســـیم می‌شـــود. این مدل نه تنها شـکاف موجود در ادبیات را پر می‌کند، بلکه مبنایی برای ارزیابی آســـیب‌پذیری و شـــبیه‌ســـازی سناریوهای تهدید فراهم خواهد آورد.

اهداف اصلی این مقاله به شرح زیر است:

۱. شناسایی و استخراج مولفه‌های کلیدی تشکیل‌دهنده تهدیدات شناختی فناوری‌محور در عرصه سایبر.

۲. تبیین روابط و ساختار ارتباطی بین این مولفه‌ها و طراحی یک الگوی مفهومی.
۳. اعتبارسنجی الگوی طراحی‌شده از طریق روش‌شناسی آمیخته.

نوآوری این مقاله در نگاه سیستماتیک و یکپارچه به پدیده تهدیدات شناختی سایبری است. در حالی که پژوهش‌های پیشین عمدتاً به بررسی تک‌بعدی این پدیده پرداخته‌اند، این پژوهش با تلفیق حوزه‌های علوم شناختی، فناوری اطلاعات و مطالعات امنیتی، به ارائه مدلی می‌پردازد که قابلیت تبیین پویایی و پیچیدگی ذاتی تهدیدات عصر حاضر را دارا می‌باشد.

مرور پیشینه و مبانی نظری؛

مرور پیشینه؛

جنگ شناختی به عنوان یک ابزار برای دستیابی به اهداف توسعه‌طلبانه قدرت‌های استکباری بدون درگیری نظامی مطرح است. این نوع جنگ از ظرفیت‌های نبرد غیرجنبشی، فضای سایبری، اطلاعات، روان شناسی و مهندسی اجتماعی برای پیروزی در جنگ بدون روبرو شدن مستقیم در میدان جنگ استفاده می‌کند. جنگ شناختی یک پدیده نوین است که در دنیای امروز اهمیت زیادی پیدا کرده است روند شکل‌گیری و توسعه فناوری‌های پیشرفته و پیش‌بینی‌ناپذیر مرتبط با فضای سایبر، نشان می‌دهد این فناوری‌ها، زمینه ساز یک انقلاب صنعتی نوین و جهش تاریخی خواهد بود که پیامدهای آن، همه ارکان زندگی بشر را تحت‌تأثیر قرار خواهد داد. وابستگی به فضای سایبر در جهان آینده یک تصویر خیالی نیست؛ بلکه واقعیتی انکارناپذیر و اجتناب‌ناپذیر است. در کشورهای پیشرفته در زمینه فناوری اطلاعات و ارتباطات، بخش عمده‌ای از فعالیت‌های اقتصادی، اجتماعی و زیست‌محیطی مبتنی بر فضای سایبر است (عراقی و همکاران، ۱۴۰۱).

مهم‌ترین تهدید حملات سایبری، لزوماً پیامدهای درجه یک آن‌ها مانند تخریب سیستم‌های فیزیکی، سرقت داده‌ها یا از دست دادن دسترسی نیست در حالی که این پیامدها همچنان مایه نگرانی هستند؛ تمرکز بر اثرات مستقیم، پیامدهای خطرناک‌ترِ آسیب‌های روانی بلندمدت و آسیب‌های اجتماعی آن را که مهم‌تر هستند؛ پنهان می‌کند. این دیدگاه، بُعد انسانی حملات سایبری مانند رفاه، روحیه و آسیب‌پذیری افراد را هدف قرار می‌دهند. برای بسیاری از عاملان سایبری، از تروریست‌ها گرفته تا هکرهای تحت حمایت دولت و سازمان‌های جنایی، هدف اصلی حملات، ایجاد اضطراب و وحشت و انتشار اطلاعات نادرست در بین عموم مردم است. به عبارت دیگر، این‌ها اهداف غیرفیزیکی هستند که اثربخشی آن‌ها را نمی‌توان به سادگی با وزن کردن آوار، شمارش اجساد یا محاسبه منابع مالی از دست رفته سنجید (Snider et al, 2021) .

مبانی نظری

تهدیدات شناختی فناوری محور در عرصه سایبری

لغت نامه‌های معتبر بین‌المللی تعاریف کمابیش مشابهی از تهدید ارائه داده است. لغت نامه وبستر تهدید را بیان و ابراز قصد آسیب رساندن، نابودی یا تنبیه کردن دیگران از روی انتقام یا ارعاب می‌داند. لغت‌نامه آکسفورد نیز در تعریف تهدید، آن را قصد ابراز شده برای صدمه، یا آسیب‌رسانی یا دیگر اقدامات خصمانه علیه کسی معرفی می‌کند. در اصطلاح نیز تهدید عبارت است از وضعیتی که در آن، خطر یا آسیب جدی، ارزش‌های اساسی و حیاتی نیز تهدید یک بازیگر را مورد هدف قرار می‌دهد. (آکسفورد،۲۰۲۴)

شناخت عبارت است از اقدامات ذهنی یا فرآیندهای کسب دانش و فهم از طریق تفکر، تجربه شناخت و حواس، ازجمله آگاهی، استدلال و قضاوت (طالبی، محجوب عشرت‌آبادی و آقایی: ۱۴۰۲:۴۵۰). با این تعریف از شناخت حالا تعریف علوم شناختی، مطالعهٔ علمی و بین‌رشته‌ای دنیای پیچیده ذهن است که از یک‌سو مرتبط با رشته‌هایی مانند علم اعصاب، روان‌شناسی، فلسفه، زبان شناسی، جامعه شناسی و از سوی دیگر مرتبط باهوش مصنوعی، رباتیک، شبکه‌های عصبی مصنوعی و رایانه است. به‌عبارت‌دیگر، موضوعی به پیچیدگی ذهن یا مغز به همکاری و ارتباط محققان این رشته‌ها نیاز دارد تا بتوان فرایندهای شناختی مانند حافظه، یادگیری، ادراک، توجه، استدلال، آگاهی، حل مسئله، تصمیم‌گیری، خلاقیت، تصویر سازی ذهنی و ... را مطالعه کرد. این علم در دههٔ پنجاه پایه‌گذاری و در دهه هفتاد تشکیلاتی شد و در دهه نود چنان پیشرفتی داشت که "دهه مغز" نام‌گذاری شد (هارتلی و جابسون، ترجمه طالبی و همکاران،۱۴۰۱:۴۴۹). در نتیجه جنگ شناختی، فعالیت‌هایی که در هماهنگی با سایر ابزارهای قدرت انجام می‌شوند تا بر نگرش‌ها و رفتار از طریق تأثیرگذاری، محافظت و مختل کردن شناخت فردی و گروهی برای به دست آوردن برتری بر دشمن تأثیر بگذارند (ناتو،۲۰۲۱). جنگ شناختی به‌معنای استفاده از تکنیک‌ها و روش‌های روان شناختی و اطلاعاتی برای تأثیرگذاری بر رفتار و تصمیمات دشمن است. این نوع جنگ شامل فعالیت‌هایی است که به‌منظور ایجاد سردرگمی، تضعیف انسجام اجتماعی و تغییر در ادراکات عمومی انجام می شود. جنگ شناختی به‌ویژه در عصر دیجیتال و با گسترش رسانه‌های اجتماعی و فناوری‌های اطلاعاتی، اهمیت بیشتری یافته و به‌عنوان یک ابزار مؤثر در استراتژی‌های نظامی و سیاسی به‌کار گرفته می‌شود . مهم‌ترین ویژگی جنگ شناختی، متکی بودن این نوع جنگ به زیرساخت‌های فناوری و رسانه‌ای نوین است که ذهن و تفکر انسان را مورد هدف قرار می‌دهد که به خاطر همین پیچیدگی، از آن به‌عنوان جنگ موریانه‌ای نام می‌برند جنگی که شکل پیشرفته‌تر و تکامل‌یافته‌تر جنگ نرم

هستند (Braddon, D. A, 2019). تهدیدهای شناختی نیز به مجموعه‌ای از خطرات و چالش‌ها اشاره دارند که بر فرآیندهای ذهنی، تفکر و تصمیم‌گیری انسان تأثیر می‌گذارند. این تهدیدها می‌توانند ناشی از عوامل مختلفی از جمله فناوری، رسانه‌ها و محیط اجتماعی باشند و ممکن است باعث ایجاد اختلال یا انحراف در نحوه پردازش اطلاعات و قضاوت افراد شوند. به عبارتی دیگر تهدیدات شناختی به اقدامات یا شرایطی اطلاق می‌شود که به‌طور مستقیم یا غیرمستقیم بر عملکرد شناختی افراد تأثیر منفی می‌گذارند. این تهدیدها می‌توانند ناشی از عوامل مختلفی مانند فناوری‌های نوین، اطلاعات نادرست، دستکاری‌های روانی یا حتی طراحی‌های نادرست سیستم‌های فناورانه باشند که منجر به کاهش توانایی‌های شناختی مانند توجه، حافظه، تصمیم‌گیری یا قضاوت می شوند (گاساندارم و تامیلا، ۲۰۲۳). با توجه به تعاریف مطرح شده قبلی در حوزه فناوری محور، تهدیدهای شناختی اغلب به سوءاستفاده از فناوری‌های دیجیتال برای تأثیرگذاری بر تفکر و رفتار افراد اشاره دارند (گرین فیلد، ۲۰۱۵). تهدیدهای شناختی فناوری محور شامل هرگونه خطر، حمله یا نقض امنیت و حریم خصوصی که در حوزه شناختی به‌وسیله فناوری‌های اطلاعاتی و ارتباطاتی (سخت و یا نرم) ایجاد می‌شود. این تهدیدها می‌توانند شامل بکارگیری هوش مصنوعی، کلان داده‌ها، ادغام اطلاعاتی، فضای سایبری، رسانه‌های اجتماعی، چت باتها، محاسبات شناختی، یادگیری عمیق، یادگیری ماشین و سایر اقدامات مرتبط با تهدیدات فناوری محور در حوزه شناختی باشند (دیویا گوپتا[1]، ۲۰۱۹:۴۵). در پایان امنیت سایبری عبارت است از مجموعه‌ای از ابزارها، سیاست‌ها، مفاهیم امنیتی، تدابیر امنیتی، دستورالعمل‌ها، رویکردهای مدیریت ریسک، اقدامات، آموزش، بهترین شیوه‌ها، تضمین و فناوری‌هایی است که می‌توانند برای محافظت از محیط سایبری و دارایی‌های سازمان و کاربر استفاده شوند. دارایی‌های سازمان و کاربر، شامل دستگاه‌های محاسباتی متصل، کارکنان، زیرساخت‌ها، برنامه‌های کاربردی، خدمات، سیستم‌های مخابراتی و کل اطلاعات منتقل شده و یا ذخیره شده در محیط سایبری است (Sarker ,2021).

عرصه فناوری سایبری و ابعاد آن

عرصه فناوری سایبری به قدری جدید است که بسیاری از اصطلاحات مورد استفاده در آن برای بسیاری نا آشنا بوده و یا بسته به منبع تعاریف متعددی دارد (کلو، ۲۰۱۷). فضای سایبری همه رایانه‌ها و شبکه‌های موجود را در بر می‌گیرد، حتی رایانه‌هایی که از شبکه‌ها جدا هستند که در اصطلاح به آن‌ها شکاف هوایی[2] گفته می‌شود. این حوزه شامل رایانه‌های تعبیه شده در وسایل

1 Divya Gupta

2 Air-gapped

و تجهیزات از قبیل آن‌هایی که در خودروها به کار می‌روند نیز می‌شـــود؛ دســـت کم در هر خودروی مدرن و امروزی یک رایانه وجود دارد و بعضی از آن‌ها تا بیش از ۳۰ رایانه دارند. فضای سایبری از طریق کد و سوئیچ‌های روشن / خاموش قابل کنترل است؛ عرصه فناوری سایبری شامل فضای سایبری و تمامی بازیگران انسانی و نهادی است که به کنترل و اداره این فضا می‌پردازند؛ این عرصه همچنین شامل کلیه دستگاه‌ها و محصولاتی سخت افزاری و نرم افزاری می شود که در، یا از طریق فضای سایبری کنترل می شوند. عرصه سایبری، فضای سایبری را تحت تأثیر قرار داده و از آن تأثیر می‌پذیرد و بخش انسانی نیز پاسخگوی ورودی‌های انسانی با ماهیت روان شناختی اجتماعی و سیاسی است. امنیت سایبری، شامل اقداماتی جهت محافظت از فضای سایبری در برابر اقدامات خصمانه است. امنیت سایبری همچنین شامل اقدامات برای محافظت از عرصه فناوری سایبری در برابر تهدیدات ناشی از فضای سایبری است. هنگامی که امنیت ســایبری حوزه‌های نظامی را شــامل می‌شــود به آن دفاع ســایبری اطلاق می‌شــود (هارتلی و جابسون، ترجمه طالبی و همکاران، ۱۴۰۱: ۴۳).

جنگ شناختی سایبری و ابعاد آن

جنگ شناختی به عنوان یک ابزار برای دستیابی به اهداف توسعه‌طلبانه قدرت‌های استکباری بدون درگیری نظامی مطرح اســـت. این نوع جنگ از ظرفیت‌های نبرد غیرجنبشـــی، فضـــای سایبری، اطلاعات، روان شناسی و مهندسی اجتماعی برای پیروزی در جنگ بدون روبرو شدن مستقیم در میدان جنگ استفاده می‌کند. جنگ شناختی یک پدیده نوین است که در دنیای امروز اهمیت زیادی پیدا کرده اســـت. روند شـــکل‌گیری و توســـعه فناوری‌های پیشـــرفته و پیش‌بینی‌ناپذیر مرتبط با فضـــای ســـایبر، نشـــان می‌دهد این فناوری‌ها، زمینه‌ســـاز یک انقلاب صنعتی نوین و جهش تاریخی خواهد بود که پیامدهای آن، همه ارکان زندگی بشر را تحت‌تأثیر قرار خواهد داد. وابستگی به فضای سایبر در جهان آینده یک تصویر خیالی نیست؛ بلکه واقعیتی انکارناپذیر و اجتناب‌ناپذیر است. در کشورهای پیشرفته در زمینه فناوری اطلاعات و ارتباطات، بخش عمده‌ای از فعالیت‌های اقتصادی، اجتماعی و زیست‌محیطی مبتنی بر فضای سایبر است (عراقی و همکاران، ۱۴۰۱).

تهدید ســایبری به عنوان یک حوزه نوظهور از عملیات ســیاســی-نظامی معرفی می‌شــود که از پیوند عملیات روانی و جنگ سایبری، زاده شده است. همانطور که در اسناد اولین نشست ناتو در مورد جنگ سایبری در سال ۲۰۲۱ گزارش شده است، هدف اصلی جنگ سایبری ایجاد کنترل و ســلطه از طریق دســتکاری مکانیســم‌های شــناختی جمعیت اســت که از بازنمایی‌های خودجوش واقعیت پشتیبانی می‌کنند. برای این منظور، جنگ سایبری دهه‌ها پیشرفت در علوم

مغز و رفتار، در فناوری‌های محاسباتی و شبکه و سیستم‌های پیچیده و تطبیقی را با هم ترکیب می‌کند. جنگ سایبری عناصری از این مجموعه دانش را برای پشتیبانی از مداخلات بر روی جمعیت‌های غیرنظامی و پرسنل نظامی به طور یکنواخت، صرف نظر از زمان صلح یا جنگ، پیاده‌سازی می‌کند. به ویژه، هدف قرار دادن شناخت انسان در کاربردهای نظامی به پیشرفت‌های علمی وابسته است که به درمان‌ها و شیوه‌های درمانی بهبود زندگی برای شرایط شناختی و عصبی کمک کرده‌اند (Pastor, 2021) . مهم‌ترین تهدید حملات سایبری، لزوماً پیامدهای درجه یک آن‌ها مانند تخریب سیستم‌های فیزیکی، سرقت داده‌ها یا از دست دادن دسترسی نیست در حالی که این پیامدها همچنان مایه نگرانی هستند، تمرکز بر اثرات مستقیم، پیامدهای خطرناک‌ترِ آسیب‌های روانی بلندمدت و آسیب‌های اجتماعی آن را که مهم‌تر هستند؛ پنهان می‌کند. این دیدگاه، بُعد انسانی حملات سایبری مانند رفاه، روحیه و آسیب‌پذیری افراد را هدف قرار می‌دهند. برای بسیاری از عاملان سایبری، از تروریست‌ها گرفته تا هکرهای تحت حمایت دولت و سازمان‌های جنایی، هدف اصلی حملات، ایجاد اضطراب و وحشت و انتشار اطلاعات نادرست در بین عموم مردم است. (Snider et al, 2021).

ظاهراً امنیت سایبری در حال تبدیل شدن به یک جایگاه مهم برای زندگی روزمره است و نقش مهمی در تلاش‌های بخش‌های مختلف از جمله سازمان‌های دولتی، شرکت‌های خصوصی و بخش دولتی ایفا می‌کند. دشمنان می‌توانند تأثیر خود را با راه‌اندازی وب سایت‌های واسطه‌ای، مانند سایت‌های خبری جعلی یا وبلاگ‌ها، گسترش دهند که این کار امروزه سریع و آسان شده است فناوری دیپ‌فیک به سرعت در دسترس قرار گرفته است و به هر کسی با مهارت‌های کامپیوتری متوسط اجازه می‌دهد تصاویر، صدا و ضبط‌های ویدئویی بسازد که به نظر می‌رسند اصالت دارند، اما این‌گونه نیستند. اگرچه این محتوای جعلی و بسیار متقاعدکننده ممکن است در دستکاری مخاطبان هدف مؤثر باشد، اما می‌تواند اثر سردکننده‌ای در حوزه شناختی نیز داشته باشد، زیرا حضور فزاینده مواد دیپ‌فیک در اینترنت ممکن است به کاهش اعتماد به شواهد دیجیتال منجر شود. بنابراین، اینترنت و رسانه‌های اجتماعی به‌عنوان وسیله‌ای برای انتقال پیام و برنامه‌های دشمن عمل می‌کنند. ما پیش‌بینی می‌کنیم که این روند ادامه یافته و جنگ شناختی آینده را شکل دهد (Masakowski & Colleagues,2023:68).

همچنین می‌توان بیان کرد که فضای مجازی امروز رسانه کلیدی برای اکثر فرآیندهای روزانه است. فضای سایبری حاوی محاصره فیزیکی نیست، بنابراین تهاجم سایبری و جنگ سایبری محدود به یک قدرت متأثر نمی‌شود و اغلب به غول‌های بزرگ‌تری سرایت می‌کند؛ بنابراین تهاجم روسیه در فضای سایبری و محدود به اوکراین نیست (Vasilovich,2023:229-231).

ویژگی‌های اصلی تهدیدات فناوری سایبری:

امروزه فناوری سایبری از طریق فضای مجازی و خوشه های ملی آن، کانال اصلی نفوذ شناختی ا ست. از طریق گروه‌ها و جوامع مختلف، ر سانه‌های الکترونیکی و سایر ا شکال ارتباطی، اهداف جامعه به اندازه کافی تحت تأثیر تنظیم و کنترل قرار می گیرند. در نهایت منجر به تغییر در جهان بینی، ارزش ها، دانش، ادراکات، دیدگاه ها و فرصت هایی برای نوع خاصی از استعمار دیجیتال می شود. بنابراین می‌توان ویژگی‌های ا صلی تهدیدات فناوری عر صه سایبری را شامل موارد ذیل عنوان کرد:

- مقیاس جهانی: تهدیدات سایبری می‌توانند به سیستم‌های امنیتی سرایت کنند در این دنیا اینترنت هیچ محدودیتی ندارد.
- ناشناس بودن: اغلب حملات از طریق اقدامات ناشناس یا از طریق استفاده از هویت‌های جعلی انجام می‌شود که شناسایی مجرمان را دشوارتر می‌کند.
- پیچیدگی مکانی سم حمله: به‌عنوان یک قاعده، مجرمان اقدامات مخرب خود و فن‌های مختلف را پنهان می‌کنند.
- بهره‌برداری از فناوری های جد ید: مجر مان به‌طور مداوم روش های خود را بهبود می‌بخشند و از فناوری‌های جدید مانند هوش مصنوعی، یادگیری ماشینی و روش‌های رمزنگاری برای ارتقای اثربخ شی بدون حمله و بدون شنا سایی ا ستفاده می‌کنند. این ویژگی‌های تهدیدات سایبری، مبارزه با آن‌ها را به‌طور ویژه دشوار می‌سازد و نیاز به بهبود مستمر در فناوری امنیت سایبری و استراتژی برای حفاظت از سیستم‌های اطلاعاتی و داده‌ها دارد؛ بنابراین، در اذهان عمومی فعلی، مهم‌ترین مشکلات امنیت سایبری کاملاً بر اساس تهاجم پیش‌بنی و انجام می‌شود (Vasilovich: 231-233).

تأثیر فناوری سایبری در جنگ شناختی:

عملیات شناختی هدفمند، خودسرانه و آزمایشی امروزه عمدتاً در فضای اطلاعاتی انسان‌ها و از طریق حوزه‌های مجازی رخ می‌دهد؛ پیشرفت‌های جنگ شناختی با کاربرد و ادغام هوش مصنوعی محدود در زندگی روزمره ما درهم تنیده شده است. این فناوری‌ها عملکردهای شناختی پایه‌ای را هدف قرار می‌دهند که برای بقا تکامل یافته‌اند. به عنوان مثال، غول‌های رسانه‌های اجتماعی با تغییر الگوریتم‌های خود و افزایش تعامل کاربران از طریق نمایش محتوای تحریک‌کننده احساسات، همان مکانیسم‌ها را فعال می‌کنند. این محتوا، منجر به پردازش اکتشافی بیشتر و رفتار خودکار می‌شود. احساسات ما توسط سیستم عصبی خودمختار هدایت می‌شوند و تنظیم آن‌ها دشوار است، چرا که می‌توانند؛ هم توجه و هم رفتار را هدایت کنند.

مطالعات نشان داده‌اند که تحریک خشم موجب پاسخ‌های احساسی شدید در افراد می‌شود. این امر می‌تواند به سرایت احساسی اجتماعی منجر شود که موجب تفکر گروهی شده و در سطوح راهبردی بالاتر ممکن است تصمیم‌گیری‌های پرریسک‌تری را به دنبال داشته باشد.

یکی از انواع فعالیت‌های اطلاعاتی سایبری مخرب که احزاب سیاسی رادیکال خشونت‌طلب درگیر آن هستند، انتشار اطلاعات تبلیغاتی آنلاین است که برای جذب هرچه بیشتر افراد و جذب اعضای جدید طراحی شده است. ارتباطات معطوف به جذب تروریست‌ها معمولاً با هدف جذب زیرگروه‌های ضعیف و به حاشیه رانده شده در جامعه طراحی می‌شود. در نتیجه، اثربخشی این تبلیغات از نظر جذب و رادیکالیزه شدن به احساسات فرد در مورد بی‌عدالتی، بیگانگی یا گناه بستگی دارد. جذب‌شدگان بالقوه تروریست و اعضای فعلی سازمان تروریستی می‌توانند از طریق تعامل تعاملی، نوعی جامعه مجازی ایجاد کنند که می‌تواند حس تعلق را نیز ارتقا داده و حس اجتماع را تقویت کند. در نبرد برای محبت های امت، جنگ روایتی از به کارگیری سلاح‌های گرم متعارف و قدرت نظامی پیشی گرفته است. جنگ اطلاعاتی تهاجمی متمرکز بر تبلیغات، مؤلفه کلیدی مبارزه داعش است. بنابراین، رسانه‌ها و منابع اینترنتی در صورت استفاده مناسب، می‌توانند سلاح روانی قدرتمندی باشند. این نوع تروریسم روایت‌محور و تشدید شده، به عنوان سلاح نامتقارن اصلی داعش ظهور کرده است. سازمان‌های تروریستی و شورشی امروزه با استفاده از طیف گسترده‌ای از کانال‌های شبکه‌های اجتماعی عمومی، روشی مستقیم‌تر و شخصی‌تر برای پیام‌رسانی ایجاد کرده‌اند؛ برخی از نمونه‌های این پلتفرم‌ها شامل توییتر و تلگرام و موارد دیگر است (R. Borum, 2022). به گفته ویلکینسون، وقتی کسی در یک جامعه دموکراتیک از تروریسم صحبت می‌کند، منظورش رسانه نیز هست. زیرا تروریسم ذاتاً یک سلاح روانی است که به انتقال تهدید به جامعه گسترده‌تر وابسته است (A. Chuipka, 2022).

عملیات در عرصه سایبری

فعالیت‌ها در دامنه‌های فضایی، سایبری و الکترومغناطیسی برای تأثیرگذاری بر شناخت انسان‌ها اهمیت بسیاری دارد. اطلاعاتی که به ایجاد روایت‌ها کمک می‌کند، عمدتاً از طریق فعالیت‌ها در دامنه‌های فضایی، سایبری و الکترومغناطیسی جمع‌آوری می‌شود. به علاوه، گسترش اطلاعات نادرست و سیگنال‌دهی از طریق روش‌های سایبری در تأثیرگذاری بر ادراکات دشمنان مؤثر است. همچنین در دامنه شناختی انسان، سرعت و دقتی که رهبران سیاسی و نیروهای نظامی به اطلاعات، اتخاذ تصمیمات مؤثر و مهارت در ایجاد سردرگمی دشمنان، ارسال اطلاعات نادرست و داده‌ها و ایجاد پیچیدگی برای دشمنان می‌تواند به دستیابی به برتری نسبی در کیفیت و سرعت تصمیم‌گیری کمک کند. عملیات در حوزه‌های فضایی، سایبری و

الکترومغناطیسی می‌تواند به عملیات در حوزه شناختی کمک کرده و به‌صورت مستقیم بر ادراک دشمن تأثیر بگذارد (کی تاکی، ۲۰۲۵).

الف- جمع‌آوری اطلاعات کمک‌کننده در ایجاد روایت‌ها

برای شکل‌گیری یک روایت قانع‌کننده، ضروری است که شواهد مربوط به آن جمع‌آوری شود. به ویژه، اگر یک دشمن در فعالیت‌های غیرقانونی درگیر باشد، ضروری است که اطلاعاتی درباره این فعالیت‌ها از طریق تمامی حوزه‌ها جمع‌آوری شود. از میان این حوزه‌ها، استفاده از وسایل فضایی، سایبری و الکترومغناطیسی اهمیت ویژه‌ای دارد. به عنوان مثال، در طول جنگ اوکراین، ماهواره‌ها شواهدی از جنایات نظامی روسیه در منطقه بوچا جمع‌آوری کردند. ایالات متحده همچنین با شنود مکالمات، اطلاعات محرمانه‌ای درباره آغاز جنگ از سوی روسیه به دست آورد. گسترش اطلاعات نادرست و سیگنال‌دهی از طریق روش‌های سایبری، فعالیت‌های سایبری و الکترومغناطیسی می‌توانند در مسیر تصمیم‌گیری یک دشمن تداخل ایجاد کنند. رووینر اشاره کرد که بسیاری از حملات سایبری روسیه در جنگ اوکراین به منظور تأثیرگذاری بر افکار عمومی از طریق پخش اطلاعات نادرست، به‌علاوه سرقت اطلاعات، انجام شد (Rovner, 2022). وایلد نیز اظهار کرد که عملیات سایبری روسیه به تأثیرگذاری در شناخت و ادراک اوکراین و جامعه بین‌المللی متمرکز بود (White House, 2022) . قبل از جنگ در اوکراین، برخی مقالات اشاره کردند که با آغاز جنگ، روسیه می‌تواند حمله سایبری عظیمی به شبکه برق راه‌اندازی کند که منجر به خاموشی‌های وسیع و از بین رفتن گرما و برق میلیون‌ها اوکراینی در سرمای طاقت‌فرسا شود (Alperovitch, 2022). در واقع، در تاریخ ۲۳ دسامبر ۲۰۱۵، یک حمله سایبری روسی باعث شد که برق در غرب اوکراین به طور همزمان قطع شود و ۲۲۵،۰۰۰ خانوار اوکراینی تحت تأثیر قرار گرفتند (Lee, Assante & Conway, 2022). ارسال سیگنال‌ها از طریق چنین فعالیت‌های سایبری می‌تواند ادراکات کشورهای دیگر یا مردم را تحت تأثیر قرار دهد (Lasiello, 2021).

ب- ارسال اطلاعات و داده‌های نادرست[1]

عمل ارسال اطلاعات نادرست به نیروهای دشمن به منظور فریب و سردرگمی آن‌ها از زمان‌های قدیم وجود داشته است، اما با پیشرفت فناوری اطلاعات و ارتباطات، روش‌ها تغییر کرده‌اند. در طول حمله روسیه، هکرهای اوکراینی حساب‌های کاربری جعلی از زنانی جذاب راه‌اندازی کردند و روس‌ها را فریب دادند تا عکس‌هایی از خود ارسال کنند. ارتش اوکراین از این عکس‌ها برای تعیین محل پایگاه‌های روس استفاده کرده و سپس آن‌ها را هدف قرار داد و نابود کرد (Lasiello, 2021).

1 False Informatio

ج- افزودن پیچیدگی به دشمنان[1]

استفاده از فریب‌ها و دیگر روش‌ها برای ایجاد ظاهری از وجود واحدها یا دارایی‌هایی که وجود ندارند، یک تکنیک قدیمی است. علاوه بر فریب‌های متعارف، تعدادی از سلاح‌های بدون سرنشین نیز می‌توانند در آینده استفاده شوند. همچنین، عملیات در حوزه‌های فضایی، سایبری و الکترومغناطیسی می‌تواند فعالیت‌های شناسایی و نظارتی دشمن را فریب دهد. چنین فعالیت‌هایی می‌توانند پیچیدگی‌های تصمیم‌گیری دشمن را اضافه کرده و مزیت نسبی در کیفیت و سرعت تصمیم‌گیری فراهم کنند.

د- حفظ و اختلال در زیرساخت‌های ارتباطی[2]

از آنجایی که انتشار اطلاعات حیاتی است، لازم است که زیر ساخت‌های ارتباطی حفظ شوند. علاوه بر این، خرابکاری در زیر ساخت‌های ارتباطی برای مختل کردن انتشار اطلاعات از سوی دشمن مؤثر است. روسیه در آغاز حمله به اوکراین، حملات سایبری را علیه دولت، نیروهای نظامی و سیستم‌های کامپیوتری زیرساخت‌های حیاتی اوکراین انجام داد که منجر به نقص برخی از سیستم‌های اوکراینی شد (Cattler & Black, 2022). که توسط نیروهای نظامی و نهادهای اطلاعاتی اوکراین استفاده می‌شد، نیز از کار افتاد. در پاسخ، اوکراین با حمایت نیروهای سایبری ایالات متحده و شرکت‌های فناوری پیشرفته، زیر ساخت‌های اطلاعاتی و ارتباطی خود را حفظ کرد (Detsch & Yang, 2022). به همین ترتیب، اوکراین توانست اطلاعات را به سرعت در سطح جهانی منتشر کند.

جنگ الکترونیک شناختی

جنگ الکترونیکی یا الکترومغناطیسی، شامل استفاده از طیف الکترومغناطیسی یا انرژی هدایت‌شده برای جلوگیری از عملیات دشمن با جلوگیری از دسترسی حریف یا حمله به او و در عین حال تضمین دسترسی نیروهای خودی به طیف الکترومغناطیس است. زمین، دریا، هوا یا فضا حوزه‌هایی هستند که سیستم‌های سرنشین‌دار و بدون سرنشین می‌توانند جنگ الکترومغناطیسی را بر روی اهدافی مانند ارتباطات، رادار یا سایر دارایی‌های غیرنظامی و نظامی اعمال کنند. در زمان صلح، عملیات مشترک طیف الکترومغناطیسی ،دسترسی کاربران مشترک به طیف الکترومغناطیسی را هماهنگ می‌کند در حالی که در زمان درگیری، مزایای تاکتیکی، عملیاتی و استراتژیک و برتری الکترومغناطیس از طریق بهره‌برداری، حمله و محافظت از اقدامات نظامی در محیط عملیاتی الکترومغناطیسی هدف قرار می‌گیرد. (U.S. Military

1 Adding Complexity To Adversaries

2 Maintaining and interfering with communications infrastructure

(Joint Tactical Networking Center.2022 جمع‌آوری و اقدام بر اساس داده‌ها، وابستگی ارتش به طیف الکترومغناطیس را افزایش داده است. جنگ الکترونیک طیف الکترومغناطیسی را کنترل می‌کند تا تهدیدات بالقوه را شنا سایی، تجزیه و تحلیل و ردیابی کند. جنگ الکترونیک، آگاهی موقعیتی را برای بینش‌های دیپلماتیک، اقدامات دفاعی و گزینه‌های تهاجمی برای هر کشور فراهم می‌کند. جنگ الکترونیک، عملیات مشترک طیف الکترومغناطیسی را ممکن می‌سازد. در محیط عملیات، نیروهای مسلح از داده‌ها بهره‌برداری، محافظت و حمله می‌کنند. جنگ الکترونیک پیشرفته‌تر می‌تواند داده‌های دشمنان را شناسایی، رهگیری و رمزگشایی کند. همچنین می‌تواند انرژی هدایت‌شده‌ای را برای مختل کردن عملیات دشمن، کاهش تأثیر درگیری‌ها یا جلوگیری از برخی درگیری‌های مسلحانه قبل از شروع آن‌ها، ساطع کند. به‌کارگیری سیستم‌های شناختی در جنگ الکترونیک به پر سنل ارتش کمک می‌کند تا الگوها را شناسایی کرده و سیستم‌ها را بهبود بخشند. سیستم‌های جنگ الکترونیک شناختی، حجم زیادی از داده‌ها را از طیف وسیعی از منابع تفسیر می‌کنند تا فرضیه‌هایی برای برنامه‌های عملیاتی ارائه دهند. ترکیب استراتژی‌های انسانی با ورودی کامپیوتر، موفقیت رویکرد جنگ الکترونیک شناختی را تضمین می‌کند. واگذاری جمع‌آوری داده‌ها و محاسبات احتمال به کامپیوترها، به انسان‌ها زمان می‌دهد تا فکر کنند، خلاق باشند و از هوش خود برای یافتن بهترین راه‌حل‌ها استفاده کنند (BARBU, 2022).

جنگ الکترونیک شناختی در جنگ‌های آینده تعیین‌کننده خواهد بود. سیستم‌های جنگ الکترونیک باید به سیگنال‌های ناشناخته قبلی در دنیای دیجیتال اینترنت اشیاء نظامی پاسخ دهند، از طریق درک حسگرهای تجمیع‌شده، سیستم‌های جنگ الکترونیک باید بتوانند با بازخوردهای بلادرنگ سازگار شوند. بازخوردهای بلادرنگ از طریق اتوماسیون، یادگیری می‌تواند سریع‌تر از آنچه انسان‌ها می‌توانند بر ا ساس داده‌ها ا ستدلال کنند، رخ دهد. این سازگاری به کارکنان نظامی اجازه می‌دهد تا در ماموریت‌های خود موفق باشند. کاربردهای نظامی فناوری شناختی برای محافظت از عملکرد خود به امنیت نیاز دارند و هوش م صنوعی و یادگیری ما شینی در انجام این عملکرد قوی و مؤثر هستند (Haigh and Andrusenko, 2021).

رویکردهای غیرنمادین، مانند شبکه‌های عمیق، بر روی داده‌های خام عمل می‌کنند. اخیراً، رویکردهای ترکیبی این دو را با هم ترکیب می‌کنند. دانش نمادین فضای جستجو را کاهش می‌دهد، ویژگی‌ها را می سازد و کارایی ج ستجو را بهبود می‌بخ شد. مدل‌ها را تو ضیح می‌دهد. رویکردهای ترکیبی، که به عنوان یادگیری ما شین مبتنی بر دانش یا هوش م صنوعی ع صبی- نمادین شناخته می‌شوند، سریع‌تر راه‌حل‌ها را پیدا می‌کنند و یادگیرنده را قادر می‌سازند حتی بدون داده‌های آموزشی کار کند و پس از آموزش در دنیای واقعی به خوبی کار کند (BARBU, 2022)

امنیت اطلاعات، برای توصیف فرآیند کنترل جریان اطلاعات استفاده می‌شود که می‌تواند تخریب اطلاعات خرابکارانه در یک کشور خودکامه یا تلاش برای کنترل تبادل تصاویر و فیلم های مستهجن باشد. امنیت اطلاعات با امنیت سایبری در هم تنیده است. هوش مصنوعی زیر شاخه‌های زیادی را در بر می‌گیرد که مفاهیم گسترده‌تر ارزیابی وضعیت و تصمیم‌گیری را پوشش می‌دهد. تکنیک‌های هوش مصنوعی شامل برنامه‌ریزی، بهینه‌سازی و ترکیب داده‌ها هستند، در حالی که حوزه‌های کاربردی پشتیبانی یادگیری شامل بینایی ماشین، پردازش زبان طبیعی، رباتیک و لجستیک می شوند. یادگیری ماشینی می‌تواند عملکرد اثربخشی پارازیت را پیش‌بینی کند و یاد بگیرد که کدام تکنیک برای کدام رفتارهای مشاهده‌شده ساطع‌کننده مناسب است. یادگیری ماشینی مبتنی بر داده، بازخورد عملکرد را در مورد این پیش‌بینی‌ها ارائه می‌دهد. یادگیری ماشینی مفهومی در هوش مصنوعی است و شبکه‌های عمیق تکنیک‌هایی در یادگیری ماشینی هستند که چیزی بیش از یادگیری عمیق هستند. اگرچه شبکه‌های عمیق بیشترین میزان دیده شدن را دارند، اما نباید یادگیری ماشینی یا سایر رویکردهای هوش مصنوعی را نادیده گرفت (BARBU, 2022).

پنتاگون در حال سرمایه‌گذاری روی قابلیت‌های تهاجمی جنگ الکترونیک شناختی مبتنی بر هوش مصنوعی است. این فناوری‌ها به طور مؤثرتری به فریب یا ایجاد اختلال در رادار دشمن کمک می‌کنند. دارپا در حال کار بر روی پروژه‌هایی است که هوش مصنوعی را در اقدامات پشتیبانی الکترونیک به کار می‌گیرند و ارتباطات بی‌سیم یا راداری را هدف قرار می‌دهند. پردازش تطبیقی فضا-زمان[1]، مبتنی بر هوش مصنوعی برای غلبه بر اختلال دشمن با استفاده از الگوریتم‌های یادگیری ماشینی برای حس کردن، بررسی و توصیف تهدیدها و سپس تولید خودکار اقدامات متقابل در زمان واقعی در نظر گرفته شده است. قابلیت اخلال رادار آرایه اسکن الکترونیکی فعال اف-۳۵ و اخلالگر نسل بعدی نیروی دریایی، نمونه‌هایی از جنگ الکترونیک شناختی هستند (DefenseOne website:2025/03/07:1600).

رسانه‌های اجتماعی در عرصه فناوری سایبری به‌عنوان تهدید کننده شناختی:

رسانه‌های اجتماعی، یک فعال‌کننده فناوری قدرتمند برای جنگ شناختی در همه سطوح است، از شکل‌دهی به روایت‌های استراتژیک و تأثیرگذاری بر آگاهی جمعی گرفته تا فریب تاکتیکی در میدان نبرد. نمونه‌هایی از تاکتیک‌های رایج شامل استفاده از حساب‌های جعلی و سرقت‌شده برای نفوذ و تأثیرگذاری بر گفت‌وگوهای داخلی، هدف‌گیری دقیق افراد و مخاطبان خاص، و توزیع

1 space-time adaptive processing

محتوای کاذب و گمراه‌کننده و رفتار هماهنگ غیراصلی برای تقویت یا سرکوب روایت‌ها یا مواد انتخابی می‌شود (Masakowski & Colleagues,2023:70).

مطالعات آماری نشان داده‌اند که در رسانه‌های اجتماعی، دروغ در تمام دسته‌های اندازه‌گیری شده اطلاعات، بیشتر، سریع‌تر، عمیق‌تر و گسترده‌تر از حقیقت پخش می‌شود. برخی مطالعات نشان داده‌اند که مقابله با دروغ‌ها با نفی آن‌ها در واقع اثر معکوس دارد و گفته‌های نادرست را تقویت می‌کند. می‌توان منطقی استدلال کرد که هر کسی که کنترل زیرساخت‌های معنابخش (شبکه‌های اجتماعی، رسانه‌های خبری، ناشران دانشگاهی) را در دست دارد، می‌تواند در تحمیل نحوه تفسیر رویدادهای فوری و تاریخ نیز از مزیت برخوردار باشد. بنابراین، معنابخشی، که همه چیز را از معنای کلمات منفرد گرفته تا معنای رویدادهای جهانی در بر می‌گیرد، به عنوان مسیری مهم برای جنگ شناختی با بکارگیری فناوری رسانه اجتماعی، شناخته شده است (Justin B, 2021).

توانایی‌های شناختی ما ممکن است توسط رسانه‌های اجتماعی و دستگاه‌های هوشمند تضعیف شود. استفاده از شبکه‌های اجتماعی می‌تواند سوگیری‌های شناختی[1] و خطاهای ذاتی تصمیم‌گیری[2] را افزایش دهد. در کتاب فکر کردن، سریع و آهسته، دانیل کانمان، به‌خوبی درباره سوگیری‌های شناختی و خطاهای ذاتی تصمیم‌گیری بحث شده است. در این زمینه، فیدهای خبری و موتورهای جستجوگر نتایجی را ارائه می‌دهند که با ترجیحات ما مطابقت بیشتری دارند. ما معمولاً اطلاعات جدید را به‌گونه‌ای تفسیر و تأیید می‌کنیم که با باورهای پیش‌فرض ما مطابقت داشته باشند. برنامه‌های پیام‌رسان اجتماعی به‌سرعت کاربران را با اطلاعات جدید به‌روز می‌کنند و باعث ایجاد سوگیری می‌شوند به‌این‌ترتیب ما اهمیت رویدادهای اخیر را نسبت به گذشته بیش‌ازحد درک می‌کنیم (ترابی،۱۴۰۰).

در دنیای امروز باید به این باور رسید که قدرت اثرگذاری بر اذهان، حرف نخست را در جنگ شناختی می‌زند. در این جنگ خاموش، خزنده و موزی باید به این آگاهی رسید که حضور شبکه‌های اجتماعی بیگانه در قلمروی اطلاعاتی داخلی می‌تواند آثار مخربی را بر اذهان داخلی بگذارد و سرنوشت کشور را در حوزه ذهن رقم بزند. شبکه‌های اجتماعی در بستر فضای سایبری با استفاده از گوشی‌های هوشمند در دست خواص و عوام بدون کسب اجازه و مجوز وارد حریم خصوصی کشور و افراد می‌شوند و خاک‌ریزهای ذهنی افراد را تصرف کرده و به‌تبع آن باورها و درنهایت ارزش‌های فردی و اجتماعی را تغییر می‌دهند (کافی، ۱۴۰۰).

---

1 Cognitive Biases

2 Innate Decision Errors

شبکه‌های اجتماعی و پلتفرم‌های دیجیتال به ابزارهای ضروری در تهدیدهای شناختی تبدیل شده‌اند، زیرا امکان انتشار سریع و کارآمد دانش دستکاری‌شده را در سراسر جهان فراهم می‌کنند. این پلتفرم‌ها نه تنها دسترسی ساده به مخاطبان بزرگ، بلکه ابزارهای پیچیده‌ای برای سفارشی‌سازی و بهبود ارتباطات و در نتیجه بهینه‌سازی تأثیر آن‌ها بر نظرات و اقدامات مردم را فراهم می‌کنند. پیام‌های دستکاری‌شده، اطلاعات نادرست و تبلیغات به طور گسترده در سایت‌های رسانه‌های اجتماعی شناخته شده از جمله فیس‌بوک، توییتر، اینستاگرام و تیک‌تاک توزیع می‌شوند. این پلتفرم‌ها به بازیگران جنگ شناختی اجازه می‌دهند تا به سرعت مطالب ویروسی را با قدرت تغییر دیدگاه عمومی ایجاد و منتشر کنند. (Bradshaw and Howard, 2019) .

عرصه شناختی به طور عمیقی بر انسجام اجتماعی، قطب‌بندی سیاسی و اعتماد به نهادهای دموکراتیک تأثیر می‌گذارد. بازیگران جنگ شناختی می‌توانند با سوءاستفاده از نقاط ضعف شناختی و تغییر ادراکات، کل جوامع را بی‌ثبات کنند، بنابراین پایه‌های دموکراسی را به خطر می‌اندازند و بین مردم تفرقه ایجاد می‌کنند. استفاده زیاد از شبکه‌های اجتماعی و پلتفرم‌های دیجیتال در محیطی که قبلاً ذکر شد، این پدیده را تشدید می‌کند. انسجام اجتماعی، پیوند و احساس تعلقی است که افراد ساکن در یک جامعه را به هم پیوند می‌دهد. حملات مستقیم به این انسجام توسط جنگ شناختی شامل اطلاعات نادرست، تبلیغات و روایت‌های دروغین است که تفرقه و خصومت را بین بسیاری از گروه‌های اجتماعی تشویق می‌کند. (McCarty, et al. 2016) . نمونه‌های قابل توجه جنگ شناختی، همه‌پرسی برگزیت و رقابت ریاست جمهوری ایالات متحده در سال ۲۰۱۶ هستند. در این موارد، از پروفایل‌های روان‌نگارانه ایجاد شده از اطلاعات شخصی میلیون‌ها کاربر فیس‌بوک برای هدف قرار دادن تبلیغات سیاسی خاص در طول همه‌پرسی و انتخابات مشخص استفاده شد. کارول کادولادر می‌گوید: کمبریج آنالیتیکا با تأثیر واضح و آشکار بر جامعه و ارزش‌های دموکراسی، از داده‌های شخصی برای ساخت مدل‌های دقیق روانشناسی رأی‌دهندگان و ارائه پیام‌های شخصی سازی شده با هدف دستکاری رفتار انتخاباتی استفاده کرد مداخله خارجی که به ویژه به روسیه نسبت داده می‌شود، شامل کمپین‌های اطلاعات نادرست و تبلیغات رسانه‌های اجتماعی بود که به منظور قطبی کردن جمعیت آمریکا و از بین بردن اعتماد به سیستم رأی‌گیری انجام می‌شد (Mueller, 2019).

رسانه‌های اجتماعی و ربات‌های اجتماعی

محبوبیت و باز بودن شبکه های اجتماعی باعث ظهور ربات های اجتماعی با توانایی تصمیم گیری مستقل می‌شود. مانند کاربران قانونی، ربات‌های اجتماعی می‌توانند از طریق کنترل برنامه دوست پیدا کنند؛ توییت ارسال کنند؛ صحبت کنند؛ چت کنند و غیره. سالج و همکاران

اشـاره می‌کند که حدود ۸،۵٪ از حسـاب‌های توییتر ربات‌های اجتماعی هسـتند که در اخبار، رویدادها، ارتباطات تجاری و سایر وظایف شرکت دارند. اکثر ربات های اجتماعی با ارائه خودکار اخبار و اطلاعات خوش‌خیم، راحتی را برای تبادل اطلاعات برای کاربران فراهم می‌کنند، اما ربات‌های اجتماعی مخربی نیز وجود دارند که می توانند شـایعات و اطلاعات مضـر را منتشـر کنند. اخیرا تعداد زیادی از روش‌های تشخیص ربات‌های مخرب پیشنهاد شده‌اند که می‌توان آنها را به روش‌های مبتنی بر رفتار، محتوا محور و مبتنی بر نفوذ طبقه‌بندی کرد. (Bin et al, 2019).

الف- روش های تشخیص مبتنی بر رفتار:

تجزیه و تحلیل و استخراج داده‌های رفتاری ربات‌های اجتماعی در شبکه‌های اجتماعی موجود بسیار ارزشمند است. بوشماف و همکاران، تفاوت‌های بین ربات‌های اجتماعی و کاربران انسانی را از نظر تعداد دوستان، فاصله زمانی پست، محتوای پست و تفاوت‌های ویژگی حساب تجزیه و تحلیل می‌کند و یک روش تشخیص تصادفی ربات اجتماعی مبتنی بر رفتار پیشنهاد می‌کند. هاسـتاین و همکاران، تفاوت‌های بین کاربران واقعی توییتر و ربات‌های اجتماعی را در بازتوییت مقالات علمی تجزیه و تحلیل می‌کند و متوجه می‌شـود که ربات‌های اجتماعی در بازتوییت (شـامل موضـوعات، منابع و غیره) انتخابی نیسـتند. گیلانی و همکاران. یک مطالعه تطبیقی بر روی رفتار ربات‌های انسـانی و اجتماعی در پسـت‌گذاری و بازتوییت در توییتر انجام دادند و متوجه شدند که ربات‌های اجتماعی علیرغم تأثیر کلی ضعیفشان، نقش بسیار مهمی در انتقال اطلاعات دارند. علاوه بر این، وارول و همکاران دریافتند که در مقایسه با کاربران انسانی، انتخاب تعامل ربات‌های اجتماعی دلخواه‌تر اسـت و ارتباطات دو طرفه کمتری بین آن‌ها و کاربران انسانی وجود دارد.

ب- روش‌های تشخیص مبتنی بر محتوا:

که بر تعیین اینکه آیا پیام ارسال شده توسط کاربر یک پیام مخرب است یا خیر تمرکز می‌کنند. به طور کلی، اینکه آیا لینک موجود در محتوای پیام به صـفحه مخرب اشـاره می‌کند یا خیر، می‌توان برای تعیین اینکه آیا حسابی که پیام را منتشر کرده است؛ ربات اجتماعی مخرب است یا خیر. به عنوان مثال، توماس و همکاران، یک طرح تشخیص لینک در زمان واقعی را پیشنهاد می‌کند که ویژگی های صـفحات لینک مرتبط را با بازدید از هر لینک منتشـر شـده اسـتخراج می‌کند. علاوه بر این، ربات‌های اجتماعی را می‌توان از طریق تغییرات در ویژگی های محتوای پیام شناسایی کرد.

ج- روش‌های تشخیص مبتنی بر تأثیر:

که ربات‌های اجتماعی را از دیدگاه تأثیر اجتماعی تشخیص می‌دهند. به عنوان مثال، مسیاس و همکاران انجام مطالعات تطبیقی در مورد تجزیه و تحلیل تاثیر ربات‌های اجتماعی و پیشنهاد مخرب استراتژی‌های رفتاری آن‌ها ، از جمله ارسال منظم توییت‌ها در مورد یک موضوع داغ خاص در فواصل زمانی مختلف ارسال و یکپارچگی ویژگی‌ها را بررسی نمودند.

رسانه اجتماعی و جعل عمیق

یک نظرسنجی انجام شده توسط مرکز تحقیقات پیو نشان می دهد که نزدیک به ۲۳ درصد از آمریکایی های مصاحبه شده تاکنون اخبار جعلی را در شبکه های اجتماعی بازنشر کرده و به اشتراک گذاشته اند. علاوه بر این، وجود ربات‌های اجتماعی، بات نت ها و ترول ها نیز یک مشکل جدی در پلتفرم های رسانه های اجتماعی بوده است. گزارش شده است که ۶۰ میلیون ترول ممکن است اخبار جعلی را در فیس بوک منتشر کنند. علاوه بر این، رواج اخبار جعلی در شبکه های اجتماعی مخاطب را سردرگم می کند، وحشت ایجاد می کند و امنیت عمومی و امنیت شناخت جمعی را به طور جدی تحت تاثیر قرار می دهد. یک نگرانی فوری این است که توسعه فناوری هوش مصنوعی، الزامات بیشتری را برای شناسایی اخبار جعلی مطرح می‌کند. تحقیق درباره اخبار جعلی از متن به تصاویر، ویدیوها و صداهای با کیفیت بالا، تولید شده و دستکاری شده توسط ماشین در مقیاس وسیع گسترش می یابد به عنوان مثال، دیپ فیکس، صداها یا ویدیوهایی از افراد واقعی ایجاد می‌کند که هرگز توسط شبکه‌های عصبی نگفته یا انجام نداده‌اند، که به طور گسترده برای جعل سخنرانی‌های سیاستمداران و شواهد غیرقانونی استفاده شده است و در نتیجه به احساسات عمومی آسیب می‌رساند و وضعیت سیاسی به طور جدی تأثیر می‌گذارد. به طور خلاصه، اخبار جعلی می توانند احساسات، نظرات و سایر فعالیت های شناختی را از طریق تعاملات انسانی و محتوایی تحت تأثیر قرار دهند. با این ایده که برخی از اطلاعات به دلیل نفوذ محتوای آنها به ترجیحات شناختی کلی موفق می‌شوند، درک مکانیسم شناخت و انتشار اخبار جعلی قبل از بررسی واقعیت بسیار مهم است (Bin et al, 2019).

سوگیری رسانه‌ای، این یکی از انواع سوگیری شناختی است به این معنی که روزنامه نگاران به دلیل نظرات جزئی خود قادر به گزارش رویدادهای خبری منصفانه و عینی نیستند. همانطور که جیمیسون و همکاران اذعان دارند، رسانه‌های خبری فقط حقایق را گزارش نمی‌کنند؛ بلکه اغلب تحت تأثیر نفوذ دولت، هدف قرار دادن ترجیحات مخاطبان، فشار حامیان مالی و غیره قرار می گیرند. تحت تأثیر همه جانبه جنبه های مختلف و همچنین هدف تعقیب عناوین، رسانه‌ها اغلب ادعاها را بدون تأیید کامل منتشر می‌کنند که فرصتی برای انتشار اخبار جعلی

فراهم می‌کند. عوامل زیادی در انتشـــار اخبار جعلی نقش دارند؛ مانند محدودیت شـــناختی خوانندگان، قابلیت اســتفاده از پلتفرم‌های رســانه‌های اجتماعی و جمعیت شــناســی مخاطبان. برخی از مطالعات در مورد ویژگی های انتشار و ساختار اخبار جعلی انجام شده است. به عنوان مثال، دیفنزو و همکاران دریافتند که شـایعات حاوی احسـاسـات منفی احتمال بیشـتری برای انتشار دارند. گواس و همکاران بیان می‌کند که محافظه کاران بیشتر احتمال دارد اخبار جعلی را به اشتراک بگذارند (Bin et al, 2019).

چت‌بات‌ها

دسته‌ای از عامل‌های نرم‌افزاری محاوره‌ای هوشمند هستند که توسط ورودی زبان طبیعی (که می‌تواند به صورت متن، صدا یا هر دو باشد) فعال می شوند. آن‌ها در پاسخ، خروجی مکالمه‌ای ارائه می‌دهند و در صـــورت دریافت دســـتور، گاهی اوقات می‌توانند وظایفی را نیز اجرا کنند. چت‌بات نرم‌افزاری اســـت که برای ایجاد تعامل بین کاربر و کامپیوتر به زبان طبیعی، مشـــابه چت‌های انسانی، استفاده می شود. چت‌بات‌ها پس از دریافت ورودی از یک انسان و پاسخ به مشتری، در یک گفتگو با مشتری شرکت می‌کنند. این کار باعث می شود کاربر هنگام چت با کامپیوتر باور کند که با یک انسـان چت می‌کند. برنامه چت‌بات به دانشـجو کمک می‌کند تا در مورد فرآیند پذیرش دانشگاه، اطلاعات کسب کند و از هر مکانی که به اینترنت متصل است؛ پاسـخ‌های سـریع دریافت کند. این سـیسـتم چت‌بات با ارائه اطلاعات مورد نیاز دانشـجویان یا والدین، حجم کار بخش پذیرش را در دانشـگاه کاهش می‌دهد و همچنین حجم کار بخشـی را که باید دائماً به تمام سوالات دانشجویان پاسخ دهد؛ کاهش می‌دهد (Venkat et al, 2019).

اگرچه فناوری‌های چت‌بات از دهه ۱۹۶۰ وجود داشته‌اند و از اوایل دهه ۱۹۸۰ بر توسعه رابط کاربری در بازی‌ها تأثیر گذاشته‌اند، اما اکنون آموزش و پیاده‌سازی چت‌بات‌ها آسان‌تر است. این امر به دلیل کد منبع باز فراوان، پلتفرم‌های توسـعه گسـترده و گزینه‌های پیاده‌سـازی از طریق نرم‌افزار به عنوان ســرویس (ســاس[1]) اســت. چت‌بات‌ها علاوه بر افزایش تجربیات مشـــتری و پشتیبانی از یادگیری، می‌توانند برای مهندسی آسیب‌های اجتماعی یعنی برای پخش شایعات و اطلاعات نادرســت، یا حمله به افراد به دلیل ارســال افکار و نظرات خود به صــورت آنلاین نیز استفاده شوند (Benton, 2017). چت خدمات مشتری و تعاملات رسانه‌های اجتماعی تجاری به طور فزاینده‌ای توسط عوامل هوشمند مدیریت می‌شوند که بسیاری از آن‌ها با هویت‌های انسانی و حتی شخصیت‌های انسانی توسعه یافته‌اند (Simonite, 2017). اگرچه خود این فناوری جدید نیست، اما قابلیت‌های زبانی قابل اعتماد، در دسترس بودن از طریق نرم‌افزار به عنوان سرویس

1 SAAS: Software as a Service

و افزودن هوش از طریق یادگیری ماشین، محبوبیت آن را افزایش داده است. بین سال‌های ۲۰۰۷ تا ۲۰۱۵، چت‌بات‌ها در یک سوم تا نیمی از کل تعاملات آنلاین شرکت داشتند و از آن زمان به بعد، میزان به‌کارگیری چت‌بات‌های جدید افزایش یافته است. ربات‌های اجتماعی و محاوره‌ای می‌توانند برای شرکت‌هایی که از آن‌ها برای کاهش زمان پاسخگویی، ارائه خدمات بهتر به مشتری، افزایش رضایت و افزایش تعامل استفاده می‌کنند، مفید باشند. متأسفانه، برخی از چت‌بات‌ها به‌طور خاص برای مضر بودن طراحی شده‌اند. به‌عنوان مثال، شبکه‌هایی از کاربران جعلی (که در توییتر سیبیل نامیده می شوند) برای افزایش مصنوعی تعداد فالوورها پیاده سازی شده‌اند تا جایگاه اجتماعی کاربرانی که آن‌ها را خریداری می‌کنند، افزایش یابد، اخبار یا شایعات جعلی پخش شود و حتی کاربرانی که عقاید سیاسی خاصی را ابراز می‌کنند، مرعوب شوند (Ferrara et al, 2016).

انواع چت‌بات‌ها

چت بات ها با ربات ها، کامپیوتر های آلوده‌ای که اغلب نرم‌افزار های مخرب را اجرا می‌کنند و می‌توانند به عنوان بات‌نت‌ها برای هماهنگی حملات انکار سرویس در مقیاس بزرگ به هم متصل شوند، متفاوت هستند. با این حال، چت‌بات‌ها می‌توانند از بات‌نت‌ها برای شکل‌دهی به ادراکات اجتماعی راه‌اندازی شوند. هیچ‌کس که وقت خود را آنلاین می‌گذراند، از آسیب بالقوه چت‌بات‌ها در امان نیست (McElrath, 2017).

الف- ربات‌های گفتاری[1]:

به عنوان سیستم‌های تعاملی هوشمند، قادرند با کاربران در قالب گفت‌وگوی طبیعی تعامل داشته باشند، اطلاعات ارائه دهند، پاسخگویی کنند و حتی تصمیمات را تحت تأثیر قرار دهند. این فناوری‌ها در فضای مجازی، شبکه‌های داخلی نظامی و محیط‌های آموزشی کاربردهای فراوانی دارند. اما در عصر جنگ شناختی، چت باتها تنها یک ابزار تعاملی نیستند ؛ بلکه عامل‌های بالقوه القاء اطلاعات گمراه‌کننده، اختلال در سواد رسانه‌ای، تشویش توجه، و خطای استراتژیک هستند. ربات‌های گفتاری، برنامه‌های هوشمندی هستند که توسط الگوریتم‌های پردازش زبان طبیعی، یادگیری ماشینی و گاهی اوقات با استفاده از شبکه‌های عمیق یادگیری، قادر به تعامل با کاربران در قالب گفتار یا متن هستند.

اقدامات این ربات‌ها می‌توانند شامل موارد ذیل باشد:

۱- پاسخگویی خودکار به سؤالات؛

۲- شبیه‌سازی گفتار و شخصیت انسانی؛

1 Artificial Intelligence Markup Language

۳- القاء اطلاعات هدفمند و شخصی‌سازی‌شده؛
۴- تشویش توجه و القاء اضطراب؛
۵- دستکاری درک واقعیت و تصمیم‌گیری؛

مؤلفه‌های اصلی ربات‌های گفتاری در محیط‌های هوشمند:

مؤلفه پردازش زبان طبیعی با تشخیص و پاسخگویی معنایی به زبان انسانی به‌منظور القاء اطلاعات گمراه‌کننده و تغییر درک زبان

مؤلفه مدل‌های هوشمند پاسخگویی با ربات‌هایی که بدون دخالت انسان به‌منظور دستکاری درک اجتماعی و سناریوهای استراتژیک واکنش نشان می‌دهند.

ب- ربات‌های شخصی‌سازی‌کننده[1]: ربات‌هایی که بر اساس رفتار کاربر، اطلاعاتی به‌منظور القاء اطلاعات هدفمند و تغییر باورها طراحی می‌کنند.

ربات‌های احساساتی[2]، ربات‌هایی که با استفاده از تجزیه و تحلیل احساسات فرد به‌منظور تولید اضطراب، تشویش اطلاعاتی و تغییر تصمیم‌گیری، احساسات را تشخیص یا القاء می‌کنند.

ربات‌های تعاملی در فضای مجازی[3] : ربات‌هایی که در محیط‌های واقعیت مجازی و افزوده، اطلاعات را به منظور تحریف واقعیت و اختلال در درک موقعیت منتشر می‌کنند.

این مؤلفه‌ها، در کنار هم، یک سیستم هوشمند تعاملی[4] را تشکیل می‌دهند که می‌تواند در جنگ شناختی، ابزاری برای القاء اضطراب، تغییر درک واقعیت و دستکاری در تصمیم‌گیری باشد. ربات‌های گفتاری یکی از مهم‌ترین ابزارهای القاء تهدید در محیط‌های نظامی هستند، چرا که:

- با استفاده از داده‌های رفتاری، قادرند اطلاعات را شخصی‌سازی کنند.
- بدون تماس فیزیکی، فرآیندهای شناختی را دستکاری می‌کنند.
- درک واقعیت، ارزیابی خطر و تصمیم‌گیری را دچار خطا می‌کنند.
- وابستگی شناختی را افزایش می‌دهند و مقاومت شناختی را کاهش می‌دهند.

در محیط‌های نظامی، چت بات‌ها به‌عنوان یک ابزار ارتباطی و تصمیم‌گیری به کار گرفته می‌شوند. اما با ظهور فناوری‌های هوشمند، شبکه‌های اجتماعی داخلی و ربات‌های روانشناختی هوشمند، این سیستم‌ها در معرض تهدیدهایی قرار گرفته‌اند که قابلیت شناسایی در چارچوب‌های قدیمی وجود ندارد. این تهدیدها می‌توانند:

- واحدهای عملیاتی را دچار خطای استراتژیک کنند.

---

1 Personalized Chatbot

2Interactive AI System

3 Virtual Interaction Bots

- احساسات را تحت تأثیر قرار دهند و انگیزه را کاهش دهند.
- درک خطر را دچار تغییر کنند.
- وابستگی به سیستم‌های هوشمند را افزایش دهند.
- اعتماد به منبع اطلاعاتی را کاهش دهند.

کاربردهای نظامی و امنیتی ربات‌های گفتاری:

- ربات‌های داخلی در واحدهای فرماندهی
- استفاده از ربات‌ها در مرکز فرماندهی برای ارائه اطلاعات، انتقال دستورات و مدیریت اطلاعات.
- ربات‌های اطلاعاتی در شبکه‌های داخلی
- ربات‌هایی در شبکه‌های داخلی نظامی جهت دستکاری اطلاعات و تغییر تصمیمات به کار می‌روند.
- شبیه‌سازی‌های روانی و آموزشی
- استفاده از ربات‌های هوشمند در شبکه‌های آموزشی و شبیه‌سازی‌های عملیاتی برای افزایش مقاومت شناختی در برابر تهدیدهای احساسی و روانشناختی.
- شبکه‌های داخلی اطلاعاتی
- ربات‌هایی که با استفاده از داده‌های رفتاری، اطلاعات را به شکلی طراحی می‌کنند که بیشترین تأثیر را بر ذهن فرماندهان داشته باشد.
- ارزیابی خطر و تصمیم‌گیری استراتژیک
- استفاده از داده‌های احساسی در واحدهای فرماندهی برای ارزیابی واکنش‌های گروهی و تصمیم‌گیری در شرایط بحرانی.

چت بات‌ها و تهدیدهای فناوری شناختی

الف- تشویش اطلاعاتی[1]: ربات‌های هوشمند و شخصی‌سازی‌کننده قادرند اطلاعات متضاد، غلط یا بی‌ربط را منتشر کنند و الگوهای توجه و تصمیم‌گیری فردی را دچار اختلال کنند. مثلا، یک فرمانده در معرض اطلاعات متضاد در یک مرکز فرماندهی دیجیتال قرار می‌گیرد. این تشویش اطلاعاتی می‌تواند واحدهای عملیاتی را دچار خطای استراتژیک کند؛ بدون اینکه متوجه شود.

دستکاری درک واقعیت[2]: ربات‌های هوشمندی که با استفاده از فناوری پردازش زبان طبیعی و تحلیل احساسات محتوایی تولید می‌کنند که باعث تغییر درک واقعیت شود. مثلا یک ربات اطلاعاتی در شبکه داخلی فرماندهی، محتوایی را منتشر می‌کند که یک واحد دوست را به عنوان دشمن معرفی کند و فرمانده را دچار خطای استراتژیک کند. ج- تغییر الگوهای

1 Information Overload & Confusion
2 Reality Distortion through Chatbots

تصمیم‌گیری[1]: سیستم‌هایی که از داده‌های رفتاری فرماندهان استفاده می‌کنند و به‌صورت زیرکانه، تصمیمات را دچار تغییر کنند؛ بدون اینکه فرد متوجه شود. یک ربات هوشمند در واحدهای فرماندهی و کنترل، با القاء اطلاعات انتخابی، فرماندهان را به سمت یک سناریوی خاص هدایت کند. در واقع بات‌های گفتاری در حوزه تهدیدهای فناوری محور جنگ شناختی، یک عامل تغییردهنده باور هستند؛ چرا که باورها و تصمیم‌گیری‌ها را بدون تماس فیزیکی دچار تغییر می‌کنند.

نقش بات‌های گفتاری در فناوری اجتماعی (فضای مجازی و سواد رسانه‌ای[2])

فضای مجازی به عنوان یک جبهه جنگ شناختی به‌ویژه در شبکه‌های داخلی نظامی و اطلاعاتی، یک محیط تعاملی است که می‌تواند بدون دخالت فیزیکی، فرآیندهای شناختی را دچار تغییر کند. این فضا می‌تواند شامل موارد ذیل باشد:

الف- شبکه‌های داخلی اطلاعاتی

ب - محیط‌های شبیه‌سازی‌شده

ج- ربات‌های هوشمند اطلاعاتی

د- پلتفرم‌های تعاملی دیجیتال

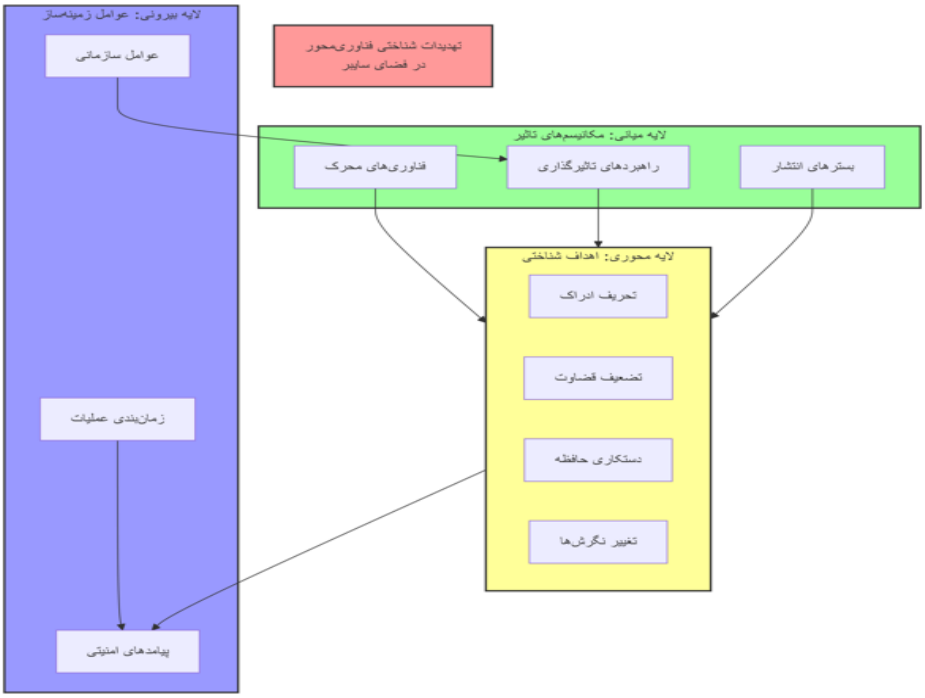
سواد رسانه‌ای و شناختی

سواد رسانه‌ای، به معنای درک صحیح از منبع، نوع و هدف اطلاعات منتشرشده در فضای مجازی ا ست. اما در حوزه جنگ شناختی، سواد ر سانه‌ای باید به سواد شناختی تعمیم یابد؛ یعنی فهم اینکه چگونه فناوری می‌تواند فرآیندهای شناختی را دستکاری کند.

1 Decision Pattern Manipulation

2 Media Literacy

مدل مفهومی:



شرح مدل مفهومی پژوهش:

الف- هسته مرکزی (اهداف شناختی):

- تحریف ادراک :ایجاد تصویر شده از واقعیت
- تضعیف قضاوت :کاهش توانایی تصمیم‌گیری منطقی
- دستکاری حافظه :تاثیرگذاری بر یادآوری و تفسیر رویدادها
- تغییر نگرش‌ها :دگرگونی باورها و ارزش‌های پایه

ب- لایه میانی (مکانیسم‌های تاثیر):

- فناوری‌های محرک :هوش مصنوعی، دیپ فیک، ربات‌های اجتماعی
- راهبردهای تاثیرگذاری :جنگ روایی، قطبی‌سازی، عملیات اطلاعاتی
- بسترهای انتشار :شبکه‌های اجتماعی، پیام‌رسان‌ها، پلتفرم‌های رسانه‌ای

ج- لایه بیرونی (عوامل زمینه‌ساز):

- عوامل سازمانی :بازیگران دولتی و غیردولتی
- زمان‌بندی عملیات :حملات مستمر و ضربتی
- پیامدهای امنیتی :بی‌ثباتی اجتماعی، تضعیف مشروعیت

روش‌شناسی

این پژوهش با رویکرد آمیخته انجام شده است. در ابتدا داده‌های کیفی گردآوری و تحلیل شده و سپس بر اساس یافته‌های کیفی، مدل کمی طراحی و آزمون شده است. این رویکرد به دلیل ماهیت اکتشافی موضوع و نیاز به توسعه یک مدل بومی مناسب بوده است. جامعه آماری در بخش کیفی شامل کلیه متخصصان حوزه امنیت سایبری، جنگ شناختی و فناوری‌های نوین بود که با استفاده از روش نمونه‌گیری هدفمند و با معیار اشباع نظری، ۱۵ نفر از متخصصان انتخاب شدند. در بخش کمی نیز جامعه آماری شامل مدیران ارشد، فرماندهان و متخصصان حوزه سایبری در سازمان‌های دفاعی و امنیتی بود که با استفاده از فرمول کوکران و روش نمونه‌گیری تصادفی طبقه‌ای، ۱۱۰ نمونه انتخاب شدند.

در بخش کیفی از مصاحبه نیمه ساختاریافته عمیق استفاده شد. پایایی مصاحبه‌ها از طریق توافق درون‌موضوعی و پایایی بین‌کدگذاران (۰/۸۵) تأیید شد. روایی نیز از طریق روایی محتوایی (نظر سنجی از متخصصان) و روایی سازه تأمین گردید. در بخش کمی، پرسشنامه محقق ساخته بر اساس مدل استخراج شده از بخش کیفی طراحی شد که شامل ۴۵ گویه در مقیاس لیکرت ۵ درجه‌ای بود. روایی پرسشنامه از طریق روایی محتوایی (CVR=0/85) و روایی سازه (تحلیل عاملی تأییدی) و پایایی آن از طریق ضریب آلفای کرونباخ (۹۲/۰) و پایایی ترکیبی (۹۴/۰) تأیید شد. در مرحله کیفی، داده‌ها با استفاده از نرم‌افزار MAXQDA نسخه ۲۰۲۰ و با روش کدگذاری نظری (کدگذاری باز، محوری و انتخابی) تحلیل شدند. در مرحله کمی، داده‌ها با استفاده از نرم‌افزار SmartPLS نسخه ۳ و با روش مدل‌سازی معادلات ساختاری تحلیل گردیدند. در این پژوهش، رضایت آگاهانه شرکت‌کنندگان، محرمانه ماندن اطلاعات، حق انصراف در هر مرحله از پژوهش و امانت‌داری در تجزیه و تحلیل داده‌ها رعایت شده است.

تجزیه و تحلیل یافته‌ها

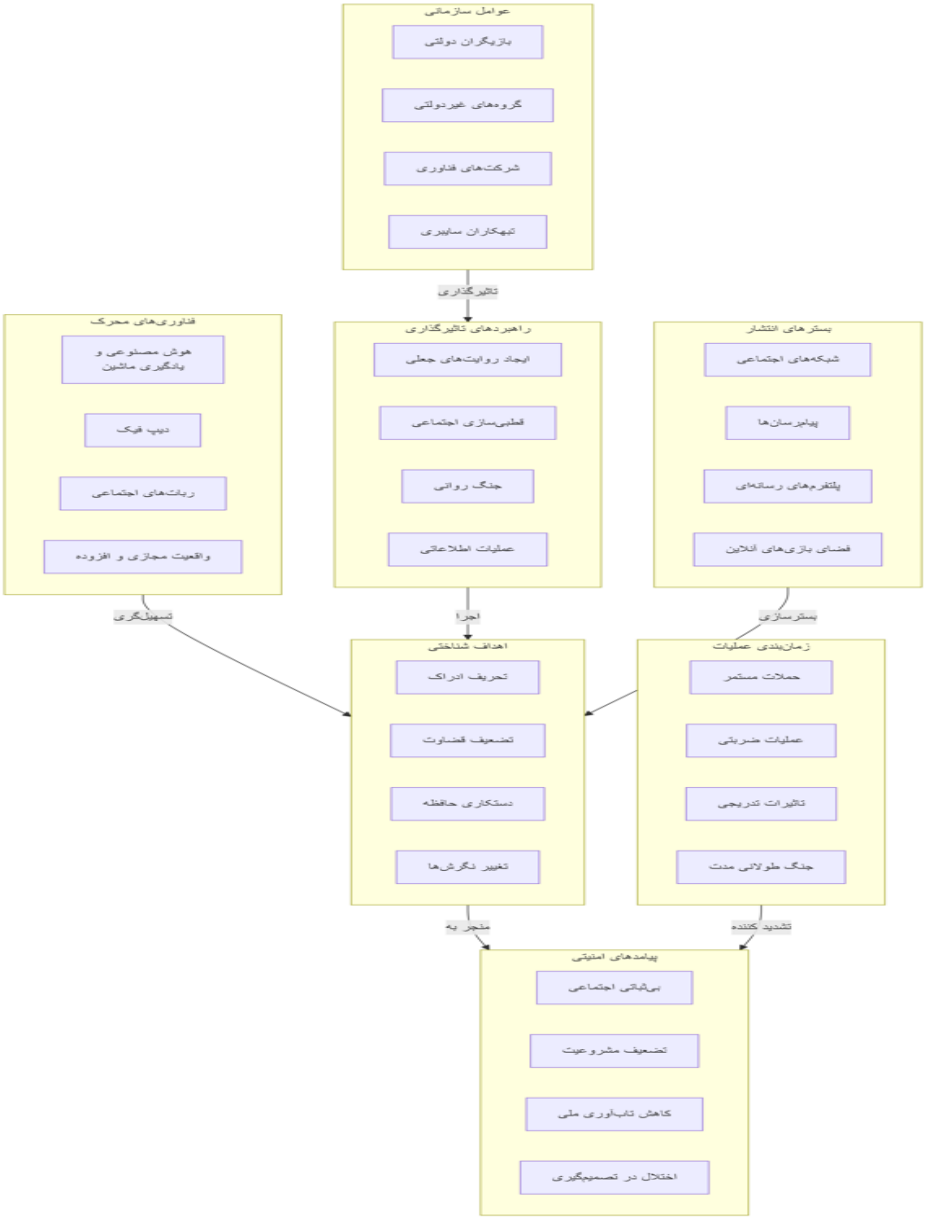
الف- یافته‌های کیفی: با استفاده از روش کدگذاری نظری در نرم‌افزارMAXQDA ، داده‌های حاصل از مصاحبه‌ها در سه مرحله کدگذاری باز، محوری و انتخابی تحلیل شد. در مرحله کدگذاری باز، ۱۴۳ کد اولیه استخراج شد که در ادامه در قالب ۲۱ مفهوم و ۷ مقوله اصلی دسته‌بندی گردید.

جدول ۱: مقوله‌های اصلی و مفاهیم تشکیل‌دهنده الگوی تهدیدات شناختی فناوری‌محور

مقوله اصلی	مفاهیم تشکیل‌دهنده
فناوری‌های محرک	هوش مصنوعی و یادگیری ماشین، دیپ فیک، ربات‌های اجتماعی، واقعیت مجازی و افزوده
اهداف شناختی	تحریف ادراک، تضعیف قضاوت، دستکاری حافظه، تغییر نگرش‌ها

راهبردهای تاثیرگذاری	ایجاد روایت‌های جعلی، قطبی‌سازی اجتماعی، جنگ روانی، عملیات اطلاعاتی
بسترهای انتشار	شبکه‌های اجتماعی، پیام‌رسان‌ها، پلتفرم‌های رسانه‌ای، فضای بازی‌های آنلاین
پیامدهای امنیتی	بی‌ثباتی اجتماعی، تضعیف مشروعیت، کاهش تاب‌آوری ملی، اختلال در تصمیم‌گیری
عوامل سازمانی	بازیگران دولتی، گروه‌های غیردولتی، شرکت‌های فناوری، تبهکاران سایبری
زمان‌بندی عملیات	حملات مستمر، عملیات ضربتی، تاثیرات تدریجی، جنگ طولانی مدت

نمودار ۱: مدل نهایی کیفی تهدیدات شناختی فناوری‌محور در فضای سایبر



نمودار شامل نمایش ارتباط بین مقوله‌های اصلی و مفاهیم تشکیل‌دهنده است؛

- فلش‌ها نشان‌دهنده روابط علی و تاثیرگذاری بین مولفه‌ها هستند؛ جهت فلش‌ها مسیر تاثیرگذاری را نشان می‌دهد
- هسته مرکزی مدل، «اهداف شناختی» است که سایر مولفه‌ها به سمت آن همگرا می‌شوند

این مدل کیفی نشـــان می‌دهد که تهدیدات شـــناختی فناوری‌محور یک ســـیســـتم پیچیده با تعاملات چندســـطحی اســـت که در آن فناوری‌های نوین به عنوان محرک اصـــلی، از طریق بســـترهای دیجیتال و با راهبردهای تاثیرگذاری مشـــخص، اهداف شـــناختی را نشـــانه رفته و در نهایت منجر به پیامدهای امنیتی می‌شوند.

ب- یافته‌های کمی

۱- آماره‌های توصیفی

میانگین ســـنی شـــرکت‌کنندگان ۴۲ ســـال با انحراف معیار ۵/۸ ســـال بود. ۷۸ درصـــد از شرکت‌کنندگان دارای مدرک کارشناسی ارشد و بالاتر بودند و میانگین سابقه فعالیت تخصصی در حوزه سایبری ۱۵ سال و حوزه شناختی ۱۰ سال بود.

۲- ارزیابی مدل اندازه‌گیری

برای ســـنجش پایایی و روایی مدل از شـــاخص‌های پایایی ترکیبی، میانگین واریانس اســـتخراج شده و بارهای عاملی استفاده شد.

جدول ۲: شاخص‌های برازش مدل اندازه‌گیری

سازه	پایایی ترکیبی	میانگین واریانس استخراج شده	بارهای عاملی
فناوری‌های محرک	0/89	0/67	0/71-0/85
اهداف شناختی	0/91	0/72	0/74-0/88
راهبردهای تاثیرگذاری	0/87	0/69	0/70-0/83
بسترهای انتشار	0/85	0/65	0/68-0/81
پیامدهای امنیتی	0/92	0/75	0/76-0/89
عوامل سازمانی	0/84	0/64	0/67-0/80
زمان‌بندی عملیات	0/86	0/68	0/69-0/82

همانطور که ملاحظه می‌شود، تمامی شاخص‌ها در محدوده قابل قبول قرار دارند که نشان‌دهنده برازش مناسب مدل اندازه‌گیری است.

۳- ارزیابی مدل ساختاری

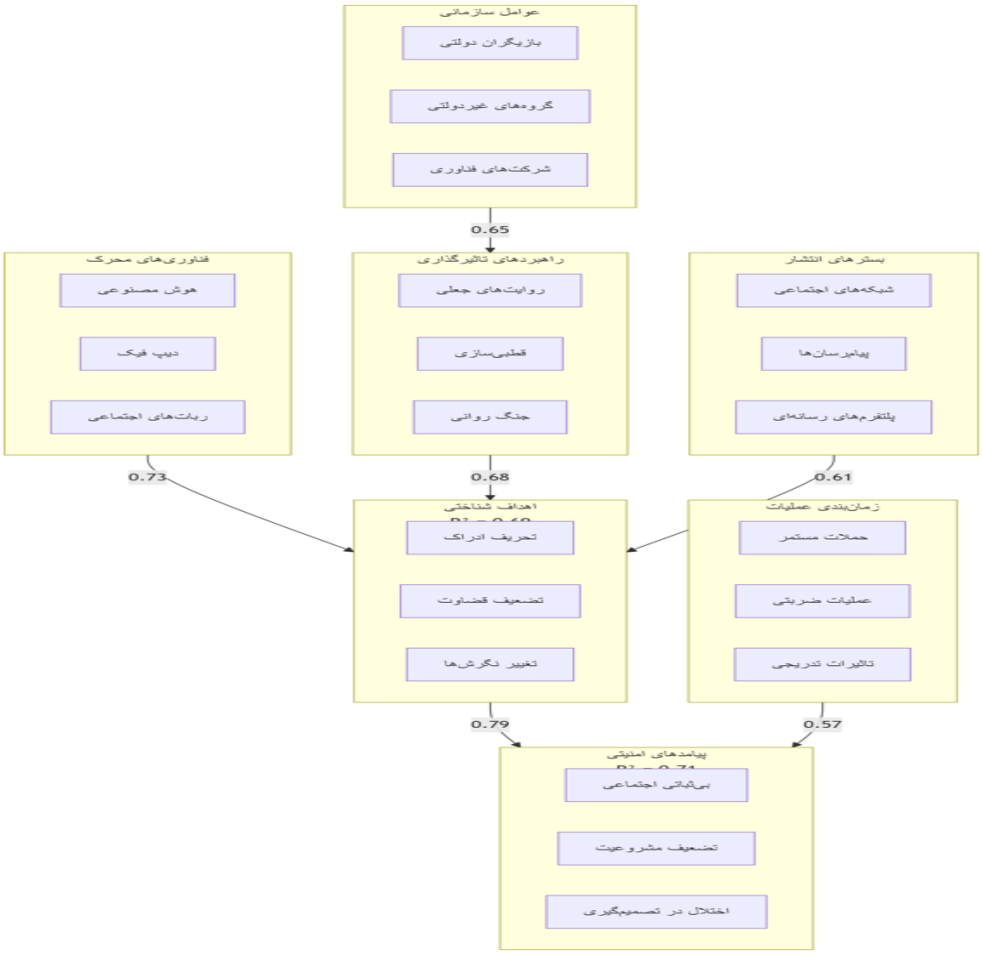
برای بررسی فرضیه‌های پژوهش از ضرایب مسیر و مقدار t استفاده شد.

جدول ۳: نتایج آزمون فرضیه‌های پژوهش

رابطه	ضریب مسیر	مقدار t	نتایج
فناوری‌های محرک ← اهداف شناختی	0/73	8/45	تأیید
راهبردهای تاثیرگذاری ← اهداف شناختی	0/68	7/92	تأیید

بسترهای انتشار ← اهداف شناختی	0/61	6/78	تأیید
اهداف شناختی ← پیامدهای امنیتی	0/79	9/12	تأیید
عوامل سازمانی ← راهبردهای تاثیرگذاری	0/65	7/23	تأیید
زمان‌بندی عملیات ← پیامدهای امنیتی	0/57	6/15	تأیید

نمودار ۲: مدل نهایی پژوهش با ضرایب مسیر



شاخص‌های برازش کلی مدل نیز حاکی از برازش مطلوب مدل است:

- GoF = 0/65
- R^2برای سازه پیامدهای امنیتی = ۷۱/۰
- R^2برای سازه اهداف شناختی = ۶۹/۰

این نتایج نشان می‌دهد که مدل طراحی شده از توانایی مناسبی برای تبیین تهدیدات شناختی فناوری‌محور در فضای سایبر برخوردار است.

بحث و نتیجه‌گیری

این پژوهش با هدف طراحی الگوی تهدیدات شناختی فناوری‌محور در عرصه فضای سایبر انجام شد. یافته‌های پژوهش نشان داد که تهدیدات شناختی در فضای سایبر از پیچیدگی بالایی برخوردار بوده و دارای ابعاد چندگانه‌ای ا ست. در این بخش، یافته‌های پژوهش با توجه به مبانی نظری و پیشینه پژوهش مورد بحث و تحلیل قرار می‌گیرد.

یافته‌های کیفی پژوهش نشان داد که الگوی تهدیدات شناختی فناوری‌محور از هفت مقوله اصلی تشکیل شده است. این یافته با نتایج پژوهش‌های (Masakowski & Colleagues, 2023و Pastor, 2021) همسو است که بر نقش محوری فناوری‌های نوین در جنگ شناختی تأکید داشتند. مقوله فناوری‌های محرک به عنوان هسته مرکزی الگو شناسایی شد که نشان‌دهنده تحول بنیادین در ماهیت تهدیدات شناختی در عصر دیجیتال است. از سوی دیگر، یافته‌های کمی پژوهش نشان داد که تمامی روابط بین مقوله‌ها در سطح ۰۵/۰ معنی‌دار هستند. قوی‌ترین رابطه به ترتیب بین اهداف شناختی ← پیامدهای امنیتی (۷۹/۰) و فناوری‌های محرک ← اهداف شناختی (۷۳/۰) مشاهده شد. این نتایج با یافته‌های (Snider et al, 2021) و (Shandler et al, 2023)همخوانی دارد که بر پیامدهای روانی بلندمدت تهدیدات سایبری تأکید کرده بودند.

یافته‌های این پژوهش از چند جهت با پژوهش‌های پیشین تفاوت دارد:

اولاً، در حالی که پژوهش‌های پیشین عمدتاً بر جنبه‌های فنی تهدیدات سایبری متمرکز بودند، این پژوهش با رویکردی جامع به بررسی ابعاد شناختی این تهدیدات پرداخته است.

ثانیاً، مدل ارائه شده در این پژوهش بر خلاف مدل‌های خطی پیشین، دارای رویکردی سیستمی و پویا است که قادر به تبیین تعامل پیچیده بین فناوری، شناخت و امنیت است.

ثالثاً، این پژوهش برای اولین بار به بررسی نقش زمان‌بندی عملیات به عنوان یک مقوله مستقل در تهدیدات شناختی پرداخته است.

نتیجه‌گیری

الگوی نهایی استخراج شده در این پژوهش نشان می‌دهد که تهدیدات شناختی فناوری‌محور در فضای سایبر، پدیده‌ای پیچیده، چندبعدی و پویا است که از تعامل سه حوزه فناوری، شناخت و امنیت شکل می‌گیرد. این الگو می‌تواند مبنای مناسبی برای:

۱. درک عمیق‌تر از ماهیت تهدیدات شناختی در عصر دیجیتال
۲. طراحی راهبردهای دفاعی و مقابله‌ای مؤثر

۳. توسعه سیستم‌های پایش و هشدار زودهنگام
۴. آموزش و توانمندسازی نیروهای متخصص در حوزه امنیت سایبری باشد.

محدودیت‌های پژوهش

این پژوهش با محدودیت‌هایی همراه بود که از جمله آن‌ها می‌توان به:

- محدود بودن جامعه آماری به متخصصان داخلی؛
- پویا و سریع‌التغییر بودن حوزه تهدیدات سایبری؛
- حساسیت بالای اطلاعات در حوزه امنیت سایبری؛

پیشنهادهای پژوهشی

۱. انجام پژوهش‌های مشابه در سایر کشورها برای مقایسه تطبیقی؛
۲. بررسی نقش فرهنگ و زمینه اجتماعی در مقابله با تهدیدات شناختی؛
۳. طراحی و اعتبارسنجی راهبردهای مقابله‌ای بر اساس مدل ارائه شده؛
۴. بررسی تأثیر تهدیدات شناختی بر گروه‌های مختلف اجتماعی؛

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱- توسعه سامانه پایش هوشمند تهدیدات شناختی با استفاده از هوش مصنوعی؛
۲- آموزش و توانمندسازی نیروهای متخصص در حوزه جنگ شناختی سایبری؛
۳- تدوین راهبرد جامع مقابله با تهدیدات شناختی در سطح ملی؛
۴- تقویت همکاری‌های بین‌المللی در زمینه امنیت سایبری؛
۵- سرمایه‌گذاری در پژوهش و توسعه فناوری‌های دفاع سایبری؛

تضاد منافع:

بدین وسیله نویسندگان تصریح می‌نمایند که هیچ گونه تضاد منافعی در خصوص پژوهش حاضر وجود ندارد.

منابع

منابع فارسی:

- ترابی، قاسم؛ طاهری زاده و ناصر، محمد (۱۴۰۰). انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل. مطالعات بین‌المللی، ۱۷(۴)، ۶۵-۴۷.
- دین اس. هارتلی و کنث او. جابسون، برتری شناختی تبدیل اطلاعات به قدرت، مترجمین مرتضی طالبی ، حسن محجوب عشرتآبادی و محسن آقایی، انتشارات دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

- عراقی، عبدالله، بیدگلی، محمد، و رجبی ده برزوئی، اصـــغر (۱۴۰۱). واکاوی اهداف جنگ شـــناختی دشـــمن و راهکارهای تاب آوری مقابله با آن با تأکید بر آموزه های قرآن. فصـــلنامه علمی مطالعات دفاع مقدس، ۸(۴)، ۱۴۳- ۱۶۲.
- کافی، سعید، (۱۴۰۰) راهبردهای آینده‌پژوهانه جمهوری اسلامی ایران در تقابل با تهدیدهای امنیتی جنگ شناختی غرب، دومین همایش سراسری پیشران‌ها و تهدیدهای فراروی انقلاب اسلامی در گام دوم انقلاب اسلامی
- کی تاکی (۲۰۲۵)، جنگ محور شناختی: مدل‌سازی رویکرد غیرمستقیم در جنگ‌های آینده، مؤسسه هادسن، واشنگتن دی.سی، ایالات متحده آمریکا

منابع انگلیسی:

- ARIE PERRY(2025), GREENFIELD NEUROPATHY 2015,CRC PRESS, NEW EDITION 2025
- Bradshaw, S., and Howard, P. N, (2019), philhoward.org. Accessed 02 06, 2024. https://demtech. oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf.
- Karen Haigh; Julia Andrusenko, Cognitive Electronic Warfare: An Artificial Intelligence Approach , Artech, 2021.
- McCarty, N., Keith T. P., and Howard R., 2016. "Polarized America, Second Edition, The Dance of Ideology and Unequal Riches". 272. London: MIT Press Cambridge.
- Mueller, R. S, (2019), "The Mueller Report: Report on the Investigation into Russian Interference in the 2016 Presidential Election". 445. e-artnow, ebook.
- Venkat N. Gudivada, Sharath Pankanti, Guna Seetharaman, Yu Zhang (2019), Trinity UniversityCognitive Computing Systems: Their Potential and the Future, Digital Object Identifier 10.1109/MC.2019.2904940
- Nicole Radziwill,Morgan C. Benton (2017), Evaluating Quality of Chatbots and Intelligent Conversational Agents
- He, J., & Andrusenko, A. (2021). Artificial intelligence and the future of warfare. Chatham House, The Royal Institute of International Affairs. https://www.chathamhouse.org
- Simonite, T. (2017), Customer Service Chatbots Are About to Become Frighteningly Realistic. MIT Technology Review.
- Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96-104.
- McElrath, L. (2017), Watching the hearings, I learned my “Bernie bro” harassers may have been Russian bots. Shareblue.
- Masakowski &Colleagues (2023), Mitigating And Responding To Cognitive Warfare, North Atlantic Treaty Organization, Science And Technology Organization, Ac/323(Hfm-356)Tp/1120
- DefenseOne website:2025/03/07:1600

- Justin B. Moore, Jenine K. Harris, and Ellen Hutti (2021), Falsehood flies, and the truth comes limping after it: social media and public health". In: Current Opinion in Psychiatry 34, pp. 485–490.
- Cattler, D & Black, D (2022), "The myth of the missing cyberwar: Russia's hacking succeeded in Ukraine And poses a threat elsewhere, elsewhere, too, Foreign Affairs
- Detsch, J & Yang, M (2022), 'Russia prepares destructive cyberattacks", Foreign Policy
- U.S. Military. Joint Tactical Networking Center. 2020. Available online: https://www.jtnc.mil/ (accessed on 29 May 2020).
- U.S. Military. Joint Tactical Networking Center. 2020. Available online: https://www.jtnc.mil/ (accessed on 29 May 2020).
- Alida Monica Doriana BARBU (2022), THE COGNITIVE ELECTRONIC WARFARE IN THE AGE OF ARTIFICIAL INTELLIGENCE , DOI: 10.53477/2784-2487-24-02
- R. Borum (2022), Psychology of terrorism, Tampa: University of South Florida,
- Rovner, J (2022), 'Sabotage and war in cyberspace, War on the Rocks, 19 July, viewed 2 June 2024
- White House (2022), 'Remarks by President Biden providing an update on Wilde, G (2022), 'Assess Russia's cyber performance without repeating its past mistakes", War on the Rocks, 21 July, viewed 2 June 2024
- Alperovitch, D 2022, 'How Russia has turned Ukraine into a cyber-battlefield, Foreign Affairs, 28 January, viewed 2 June 2024,
- A. Chuipka (2022), The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorists? University of Ottawa,
- Gaiduk Oleg Vasilovich, Zverev Volodymyr Pavlovich (2021), Department of Software Security Engineering and Cybersecurity, National Trade and Economic University, Kiev, Ukraine
- Pastor, A. (2023). Cognitive warfare. https://doi.org/10.31234/osf.io/zgsej
- B. Prebot, Claverie and F. Du Cluzel (2021), Cognitive Warfare : La guerre cognitique. Remiere reunion scientifique Cognitive Warfare. Innovation Hub NATO, 2021.
- NATO STO (2020). NATO Science & Technology Trend Report, 2020. Science & Technology Trends 2020 2040. Exploring the S&T Edge. NATO Science & Technology Organization, Neuilly-sur-Seine, France.
- Braddon, D. A. (۲۰۱۹). The New Science of Warfare. New York
- Mathura Shanmugasundaram & Arunkumar Tamilarasu (2023), The impact of digital technology, social media, and artificial intelligence on cognitive Functions, Harvard Medical School, Harvard University, Boston, MA, United States, Independent Researcher, Boston, MA, United States
- Iqbal H. Sarker (2021), Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective, SN Computer Science 2:15
- Divya Gupta, Tanishka Garg, Latika Khar (2019), International ournal of Advanced Trends in Computer Applications

- Snider, Keren L.G., Ryan Shandler, Shay Zandani, and Daphna Canetti (2021). “Cyberattacks, Cyber Threats, and Attitudes toward Cybersecurity Policies.”Journal of Cybersecurity 7 (1): tyab019.