فصلنامهٔ علمی راهبرد دفاعی، سال بیست و دوم شمارهٔ ۸۶، تابستان ۱۴۰۳

اگر کشوری امروز در علوم شناختی و فناوری‌های مرتبط با آن عقب بماند همان سرنوشت کسانی که در انقلاب صنعتی عقب ماندند را دچار خواهد شد.

مقالهٔ پژوهشی: بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی– امنیتی جمهوری اسلامی ایران

حمید اسماعیلی[۱]، ابوذر میارعباسی[۲]

تاریخ دریافت: ۱۴۰۲/۱۱/ ۱۲ **تاریخ پذیرش ۱۴۰۳/۰۱/۲۷**

چکیده

امروزه علوم و فناوری‌های شناختی به‌عنوان یکی از پیشرفته‌ترین رشته‌های علمی و فناوری شناخته‌شده‌اند و به دلیل تأثیر فراوان این حوزه بر جنبه‌های مختلف اجتماعی، سیاسی، اقتصادی، نظامی و ...، هزینه‌های قابل‌توجهی صرف این پژوهش‌ها می‌شود. هدف این مقاله بررسی قابلیت‌های متنوع علوم و فناوری‌های شناختی در حوزه دفاع و امنیت است. این پژوهش از نوع کیفی بوده و از روش گروه کانونی برای جمع‌آوری داده‌ها استفاده‌شده است. در این روش، نظرات خبرگان مرتبط با موضوع جمع‌آوری و تجزیه‌وتحلیل شده است. یافته‌های این پژوهش نشان می‌دهد که علوم و فناوری‌های شناختی می‌توانند در حوزه‌های مختلف دفاع و امنیت از قبیل تقویت ذهن با ایجاد انعطاف‌پذیری شناختی، تربیت و پرورش ابر سرباز جهت افزایش عملکرد انسانی، طراحی و تولید تسلیحات شناختی جهت مقابله با تهدیدات جنگ شناختی، همجوشی انسان و ماشین و غیره کاربرد داشته باشند. استفاده از قابلیت‌های علوم و فناوری‌های شناختی در حوزه دفاع و امنیت می‌تواند دستاوردهای گسترده‌ای درزمینه بهبود تشخیص و پیشگیری از تهدیدات امنیتی، مدیریت مخاطرات مرتبط با دفاع و امنیت و ایجاد امکان جمع‌آوری، تحلیل و استفاده از حجم عظیم داده‌ها به‌صورت سریع و هوشمند، به همراه داشته باشد و عدم توجه به این قابلیت‌ها می‌تواند عواقب جدی و ناخوشایندی به همراه داشته باشد. به‌هرحال علوم و فناوری‌های شناختی قابلیت‌های متعددی برای ارتقای توان دفاعی و امنیتی کشورها دارند و استفاده از این قابلیت‌ها می‌تواند به افزایش امنیت و ثبات در جهان کمک کند.

واژگان کلیدی: علوم شناختی، فناوری‌های شناختی، روانشناسی شناختی، علوم اعصاب شناختی، هوش مصنوعی، حوزه‌های دفاعی– امنیتی

۱. نویسنده مسئول: دانش‌آموخته دانشگاه عالی دفاع ملی، تهران، ایران.

۲. دانشجوی دکتری امنیت ملی.

مقدمه

در دنیای امروز، علوم و فناوری‌های شناختی به‌عنوان یکی از پیشرفته‌ترین رشته‌های علمی و فناوری شناخته‌شده‌اند. این حوزه با مطالعه‌ی ذهن و فرآیندهای شناختی انسان، دریچه‌ای نو به‌سوی درک و ارتقای عملکرد انسان درزمینه‌های مختلف گشوده است. در بخش دفاع و امنیت، قابلیت‌های علوم و فناوری‌های شناختی می‌توانند به‌طور فزاینده‌ای اهمیت پیدا کنند. این قابلیت‌ها شامل فناوری‌های هوش مصنوعی، یادگیری ماشین، تحلیل داده‌ها، تشخیص الگو، تحلیل زبان طبیعی و سایر فناوری‌های مرتبط است. با استفاده از این فناوری‌ها، می‌توان بهبود قابل‌توجهی در تشخیص و پیشگیری از تهدیدات امنیتی و نیز مدیریت بهتر مخاطرات مرتبط با حوزه‌ی دفاع و امنیت داشت.

۱. کلیات

۱-۱. بیان مسئله

«اگر کشوری امروز در علوم شناختی و فناوری‌های مرتبط با آن عقب بماند همان سرنوشت کسانی که در انقلاب صنعتی عقب ماندند را دچار خواهد شد.»[۱]

در دنیای پیچیده و پویای امروز، امنیت و دفاع ازجمله مهم‌ترین نیازهای جوامع بشری به شمار می‌روند. با توجه به تحولات سریع درزمینه‌های مختلف، ازجمله علوم و فناوری های رفتار انسان، همواره نیاز به روش‌ها و ابزارهای نوینی برای ارتقای امنیت و دفاع احساس می‌شود. در این میان، علوم و فناوری‌های شناختی با ارائه درک عمیق‌تر از نحوه عملکرد مغز و ذهن انسان، پتانسیل قابل‌توجهی برای ارائه راه‌حل‌های نوآورانه در این حوزه دارند. علوم شناختی به مجموعه‌ای از رشته‌های علمی گفته می‌شود که به مطالعه ذهن و مغز انسان می‌پردازند. این رشته‌ها شامل حوزه‌هایی مانند روانشناسی، علوم اعصاب، هوش مصنوعی و زبان‌شناسی هستند. یافته‌های علوم شناختی می‌تواند درزمینه‌های مختلفی ازجمله امنیت و دفاع کاربرد داشته باشد.

---

۱. دیدار مسئولان و محققان ستاد توسعه علوم شناختی با مقام معظم رهبری، ۳ /۱۰/ ۱۳۹۷.

علاوه بر این، علوم و فناوری شناختی می‌توانند در جمع‌آوری، تحلیل و استخراج اطلاعات مفیدی برای امنیت ملی و بین‌المللی نقش داشته باشند. با استفاده از فناوری های مختلف مانند استخراج اطلاعات، تحلیل شبکه‌ها و پردازش تصویر، می‌توان از حجم عظیم داده‌ها اطلاعات مفیدی را استخراج کرده و در تصمیم‌گیری‌های امنیتی مؤثر بود. به‌طورکلی، قابلیت‌های علوم و فناوری شناختی در بخش دفاع و امنیت می‌توانند بهبود قابل‌توجهی در تشخیص، پیشگیری و مدیریت تهدیدات امنیتی به همراه داشته باشند. با پیشرفت این فناوری‌ها، امکانات و کاربردهای بیشتری نیز پیش رو خواهند بود. علوم شناختی می‌تواند در درک بهتر رفتار دشمن، پیش‌بینی اقدامات آن‌ها، طراحی سامانه‌های آموزشی و تمرینی مؤثرتر برای نیروهای نظامی و امنیتی و توسعه ابزارهای نوین برای جمع‌آوری و تجزیه‌وتحلیل اطلاعات استفاده شود. با توجه به اهمیت روزافزون علوم و فناوری‌های شناختی در حوزه امنیت و دفاع، ضروری است که قابلیت‌ها و چالش‌های مرتبط با کاربرد این علوم به‌طور دقیق موردبررسی قرار گیرد.

۱-۲. اهمیت و ضرورت تحقیق

در دنیای پیچیده و پویای امروز، حفظ امنیت ملی و دفاع از مرزها از اهمیتی حیاتی برخوردار است. در این راستا، همواره شاهد نوآوری‌ها و تحولات فناورانه‌ای هستیم که ماهیت جنگ و درگیری را دگرگون می‌کنند. علوم و فناوری‌های شناختی نیز از این قاعده مستثنی نیستند و به‌سرعت در حال تبدیل‌شدن به ابزاری قدرتمند برای ارتقای توان دفاعی و امنیتی کشورها هستند.

تحقیق در مورد قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی و امنیتی از به دلایل زیر حائز اهمیت است:

۱. نتایج این تحقیق می‌تواند به توسعه سیستم‌های دفاعی هوشمندتر و کارآمدتر در نیروهای مسلح کمک کند. به‌عنوان‌مثال، می‌توان از این فناوری‌ها برای طراحی الگوریتم‌های پیشرفته تشخیص هدف، سامانه‌های جنگ الکترونیکی و سامانه‌های

تصمیم‌گیری خودکار استفاده کرد. این امر به نیروهای نظامی این امکان را می‌دهد تا با دقت و سرعت بیشتری به تهدیدات واکنش نشان دهند و درعین‌حال تلفات جانی و خسارات مالی را به حداقل برسانند.

۲. نتایج این پژوهش می‌تواند برای آموزش و شبیه‌سازی واقع‌گرایانه‌تر سناریوهای جنگی مورداستفاده قرار گیرد. این امر به سربازان و کارکنان نظامی این امکان را می دهد تا در شرایطی امن و کنترل‌شده، مهارت‌ها و تاکتیک‌های خود را ارتقا دهند.

۳. با گسترش روزافزون وابستگی به زیرساخت‌های دیجیتال، امنیت سایبری به یک اولویت امنیتی ملی تبدیل‌شده است. نتایج این پژوهش می‌تواند برای توسعه روش‌های پیشرفته‌تر شناسایی و خنثی‌سازی حملات سایبری، محافظت از اطلاعات حساس و ایمن‌سازی شبکه‌های رایانه‌ای مورداستفاده قرار گیرد.

٤. دستاوردهای این تحقیق می‌تواند برای درک بهتر انگیزه‌ها، تصمیم‌گیری‌ها و اقدامات دشمن مورداستفاده قرار گیرد. این امر به رهبران نظامی و غیرنظامی این امکان را می‌دهد تا استراتژی‌های مؤثرتری برای پیشگیری از درگیری‌ها و مدیریت بحران‌ها تدوین کنند.

۵. این پژوهش برای توسعه ابزارها و فناوری‌هایی برای حفظ صلح و ثبات مانند سامانه‌های نظارت، صلح‌بانی و حل‌وفصل منازعات می‌تواند مورداستفاده قرار گیرد.

ضمناً غفلت از انجام این تحقیق می‌تواند پیامدهای زیر را به دنبال داشته باشد:

۱. اگر این پژوهش در خصوص قابلیت‌های علوم و فناوری‌های شناختی در حوزه دفاع و امنیت انجام نشود، کشور از سایر رقبا در این حوزه عقب خواهد ماند. این عقب‌ماندگی می‌تواند منجر به آسیب‌پذیری بیشتر در برابر تهدیدات نوین و کاهش توانایی در حفظ امنیت ملی گردد.

۲. بدون انجام این پژوهش، نیروهای مسلح از مزایای سامانه‌های هوشمند و کارآمد محروم خواهند ماند. این امر می‌تواند به کاهش دقت و سرعت عمل آن‌ها در مقابله با تهدیدات و درنتیجه افزایش تلفات جانی و خسارات مالی منجر شود.

۳. با گسترش روزافزون تهدیدات سایبری، عدم انجام این پژوهش می‌تواند کشور را در برابر حملات سایبری آسیب‌پذیرتر کند. این آسیب‌پذیری می‌تواند منجر به سرقت اطلاعات حساس، اختلال در زیرساخت‌های حیاتی و ایجاد خسارات اقتصادی و اجتماعی گسترده گردد.

با توجه به موارد فوق، تحقیق در مورد قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی و امنیتی امری ضروری برای حفظ امنیت ملی و ارتقای صلح و ثبات در جهان است. سرمایه‌گذاری در این حوزه می‌تواند منجر به توسعه فناوری‌های جدیدی شود که به نفع نیروهای نظامی، کارکنان امنیتی و شهروندان عادی باشد.

۱-۳. پیشینهٔ تحقیق

کانادا، پیشرو در تحقیقات علوم و فناوری‌های شناختی، در سال‌های اخیر گام‌های مهمی برای استفاده از این پیشرفت‌ها در بخش‌های دفاعی و امنیتی خود برداشته است. دولت کانادا در مراکز تحقیقاتی مانند تحقیق و توسعه دفاعی کانادا[1] سرمایه‌گذاری می‌کند که به پروژه‌های هوش مصنوعی، یادگیری ماشینی و تعامل انسان و رایانه می‌پردازد. این پیشرفت‌ها مستقیماً به افزایش قابلیت‌های دفاعی کانادا ترجمه می‌شود. کمک‌ها و منابع مالی به استارت‌آپ‌ها برای تقویت نوآوری و تجاری‌سازی راه‌حل‌های علوم و فناوری شناختی برای دفاع و امنیت ارائه می‌شود. این امر مشوق توسعه ابزارهای جدید در این حوزه است. دولت فعالانه با دانشگاه‌هایی مانند مک گیل و اتاوا در پروژه‌های هوش مصنوعی و یادگیری ماشینی که به‌طور خاص برای برنامه‌های دفاعی و امنیتی طراحی شده‌اند، همکاری می‌کند. این شکاف بین تحقیقات دانشگاهی و نیازهای دفاعی در دنیای

1. DRDC

واقعی را پر می‌کند. کانادا با شناخت مشکلات احتمالی، مقررات و سیاست‌هایی را برای کنترل استفاده از علوم و فناوری شناختی در دفاع و امنیت وضع نموده است. استراتژی ملی هوش مصنوعی ۲۰۱۷ نمونه‌ای از این تمرکز بر توسعه و کاربرد مسئولانه هوش مصنوعی در این حوزه است. کشور کانادا از هوش مصنوعی برای تجزیه‌وتحلیل داده‌ها، شناسایی تهدید و هدف‌گیری دقیق در عملیات نظامی، از یادگیری ماشینی برای پیش‌بینی رفتار دشمن، شناسایی حملات سایبری و بهبود امنیت کلی سایبری، از رابط انسان و رایانه برای نمایش اطلاعات در زمان واقعی و کارآمد جهت بهره‌مندی پرسنل و از واقعیت مجازی و افزوده، برای آموزش پرسنل حوزه دفاعی و امنیتی و شبیه‌سازی عملیات نظامی استفاده می‌کند (CIFAR, 2023).

ایالات‌متحده آمریکا، در خط مقدم نوآوری‌های علمی و فناوری، به‌طور فعال کاربرد علم و فناوری شناختی را در استراتژی‌های دفاعی و امنیتی خود دنبال کرده است. وزارت دفاع آمریکا[1] واحدهای اختصاصی مانند آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی (دارپا) ایجاد کرده است که تحقیقات درزمینه هوش مصنوعی، علوم اعصاب و سایر زمینه‌های مرتبط را پیش می‌برند (DARPA,2009).

ایالات‌متحده یک زیست‌بوم قوی را برای توسعه علوم و فناوری‌های شناختی ایجاد کرده است. این مهم شامل ابتکاراتی مانند استراتژی آفست سوم است که بر بهره‌برداری از فناوری‌های نوظهور برای مزیت نظامی تأکید دارد (کلارک و همکاران، ۲۰۱۷). علاوه بر این، همکاری بین وزارت دفاع، دانشگاه و صنعت خصوصی، نوآوری را سرعت می بخشد و جریان ثابت راه‌حل‌های پیشرفته را تضمین می‌کند (دفتر وزیر دفاع، ۲۰۲۲). ارتش ایالات‌متحده به‌طور فعال در حال بررسی برنامه‌های مختلفی از قبیل استفاده از هوش مصنوعی برای تجزیه‌وتحلیل میدان نبرد، پیش‌بینی تهدید و حتی سامانه‌های تسلیحاتی خودمختار (کلارک و همکاران، ۲۰۱۷)، بررسی رابط‌های مغز و رایانه برای

1. .DoD

بهینه‌سازی برنامه‌های آموزشی و بهبود عملکرد سرباز (آزمایشگاه تحقیقاتی نیروی هوایی، ۲۰۲۳)، استفاده از الگوریتم‌های یادگیری ماشین برای شناسایی و مقابله با تهدیدهای سایبری به‌طور مؤثرتر (مجله نیروی هوایی، ۲۰۲۲) بوده است.

چین به‌عنوان بازیگر مهمی در استفاده از علوم و فناوری شناختی برای اهداف دفاعی و امنیتی ظاهرشده است. چین به‌طور فعال به دنبال ادغام علم مغز و هوش مصنوعی است. این شامل تحقیق در مورد علوم اعصاب برای درک نحوه عملکرد مغز و توسعه بالقوه رابط‌های مغز و رایانه[1] برای کاربردهای نظامی است (Ndu Press,۲۰۲۳). علاوه بر این، آن‌ها به‌شدت در توسعه هوش مصنوعی برای کاربردهای مختلف دفاعی سرمایه‌گذاری کرده‌اند (CSIS,۲۰۲۲). ارتش آزادی‌بخش خلق چین[2]، در حال بررسی و توسعه کاربردهای مختلف علوم و فناوری‌های شناختی از قبیل دست‌کاری تصمیم‌گیری دشمن و روحیه سربازان از طریق عملیات روانی و کنترل اطلاعات (Defence one، ۲۰۲۳)، استفاده از هوش مصنوعی برای تجزیه‌وتحلیل میدان نبرد، ارزیابی تهدید و سامانه‌های تسلیحاتی بالقوه خودمختار (IAR-Gwu,۲۰۲۲) و توسعه برنامه‌های آموزشی که از واقعیت مجازی، واقعیت افزوده و هوش مصنوعی برای افزایش عملکرد و تصمیم‌گیری سرباز استفاده می‌کنند (SCMP,2020)[3] است.

دولت چین توسعه علوم و فناوری شناختی را از طریق سرمایه‌گذاری‌های استراتژیک و ابتکارات سیاستی در اولویت قرار می‌دهد. این شامل ایجاد مؤسسات تحقیقاتی اختصاصی و تقویت همکاری بین بخش‌های نظامی و غیرنظامی است (CSIS,2022).

روسیه نیز به‌عنوان کشوری که تأکید زیادی بر نوسازی نظامی دارد، پتانسیل علوم و فناوری شناختی را برای کاربردهای دفاعی و امنیتی به‌خوبی تشخیص داده است. روسیه

1. BCIs
2. PLA
3. South China Morning Post

توسعه و استقرار وسایل نقلیه هوایی بدون سرنشین[1]، وسایل نقلیه زمینی بدون سرنشین[2] و سامانه‌های تسلیحاتی خودران را در اولویت قرار می‌دهد. این سامانه‌ها اغلب از هوش مصنوعی برای عملکردهایی مانند شناسایی هدف و تصمیم‌گیری استفاده می‌کنند (CSIS,2020). روسیه در حال بررسی و توسعه روزافزون کاربردهای نظامی مختلف علوم و فناوری‌های شناختی ازجمله استفاده از هوش مصنوعی و یادگیری ماشینی برای ایجاد اختلال در ارتباطات و سامانه‌های الکترونیکی دشمن (CNA,2022)، توسعه ابزارهای دفاع سایبری مبتنی بر هوش مصنوعی برای مقابله با حملات سایبری و حفاظت از زیرساخت‌های حیاتی، استفاده از واقعیت مجازی و واقعیت افزوده برای شبیه‌سازی واقعی آموزش نظامی (CNA,2022) است. دولت روسیه همچنین در مؤسسات تحقیقاتی سرمایه‌گذاری می‌کند و همکاری بین ارتش و دانشگاه را برای تسریع توسعه علوم و فناوری‌های شناختی برای اهداف دفاعی تقویت می‌کند (RAND,2022)

بهر حال میدان نبرد مدرن در حال دگردیسی است. درحالی‌که توانایی فیزیکی و مانورهای تاکتیکی همیشه مهم باقی خواهند ماند، ذهن انسان به‌عنوان یک مرز مهم در دفاع و امنیت ظاهرشده است. علوم و فن‌آوری‌های شناختی در حال بازتعریف چشم‌انداز هستند و جنگ را از یک نبرد تنومند به برخورد توانایی‌های شناختی تبدیل می‌کنند. در مقالات و منابعی که موردمطالعه قرارگرفته‌اند به پنج حوزه کلیدی پرداخته‌شده است که این پیشرفت‌ها آینده امنیت ملی کشورها را دستخوش تغییر قرار می‌دهد.

۱. ابر سربازان: افزایش عملکرد انسانی

سربازانی را با تمرکز بالا، انعطاف‌پذیری بهینه و توانایی پردازش اطلاعات با سرعت رعدوبرق تصور کنید. علوم اعصاب شناختی این دیدگاه را به واقعیت تبدیل می‌کند. تکنیک‌های عصب فناوری که توسط مؤسساتی مانند مؤسسه تعامل انسان و رایانه دانشگاه کارنگی ملون پیشگام شده است، تمرکز و توجه را افزایش می‌دهد، درحالی‌که دارپا نوید

1. UAV
2. UGV

رابط‌های مغز و رایانه را با یکپارچه‌سازی اطلاعات میدان جنگ در زمان واقعی و به‌طور مستقیم در درک سرباز می‌دهد. این پیشرفت‌ها می‌تواند منجر به افزایش تصمیم‌گیری، واکنش‌های سریع‌تر و بهبود اثربخشی رزم شود.

۲. تقویت ذهن: ایجاد انعطاف‌پذیری شناختی

در عصر اطلاعات غلط و مهندسی اجتماعی، ذهن انسان به یک هدف آسیب‌پذیر تبدیل‌شده است. با درک این موضوع، برنامه امنیت شناختی داخلی دارپا بر سامانه‌های مقاوم به دست‌کاری شناختی مستقرشده است به‌گونه‌ای که دارای قابلیت شناسایی آسیب‌پذیری‌ها در سامانه‌های اطلاعاتی از طریق منطق صوری و طراحی رابط‌هایی است که در برابر تاکتیک‌های مهندسی اجتماعی مقاومت می‌کنند. با تقویت ذهن سربازان و غیرنظامیان به‌طور یکسان، می‌توانیم جامعه‌ای مقاوم و غیرقابل نفوذ در برابر سلاح‌های موذیانه جنگ اطلاعاتی ایجاد کنیم.

۳. تسلیحات شناختی: تهدید احتمالی «جنگ شناختی»

اصطلاح «جنگ شناختی»[1] به دست‌کاری عمدی شناخت انسان برای مزیت نظامی اشاره دارد. گزارشی از سازمان علم و فناوری ناتو تصویری دل‌خراش از این تهدید نوظهور را ترسیم می‌کند. فناوری‌های پیشرفته مانند هوش مصنوعی و فناوری عصبی می توانند برای بهره‌برداری از تعصبات انسانی، انتشار اطلاعات نادرست و تأثیرگذاری بر رفتار در مقیاس بزرگ مورداستفاده قرار گیرند. شناخت و کاهش اثرات جنگ شناختی به اقدامات پیشگیرانه‌ای نیاز دارد ازجمله: برنامه‌های آموزشی، دستورالعمل‌های اخلاقی برای توسعه فناوری و همکاری بین‌المللی برای مبارزه با اطلاعات غلط تسلیح شده

٤. همجوشی انسان و ماشین: قدرت هوش گروهی

آینده جنگ ممکن است صرفاً انسانی یا صرفاً ماشینی نباشد. در عوض، گروه‌سازی انسان و ماشین – با استفاده از قدرت هر دو – در حال افزایش است. همان‌طور که ایوان

1. CogWar

کانیا (۲۰۱۹) در «ذهن در جنگ: پیگیری مزیت نظامی چین از طریق علوم شناختی و زیست‌فناوری» کاوش می‌کند، کشورهایی مانند چین به‌طور فعال درحال‌توسعه فناوری عصبی برای افزایش عملکرد سربازان و ادغام سامانه‌های هوش مصنوعی برای ارتقاء قدرت تصمیم‌گیری هستند. این رابطه همزیستی قابلیت‌های بی‌نظیری را ارائه می‌کند، اما همچنان سؤالات اخلاقی را در مورد نقش انسان در جنگ و پتانسیل پیامدهای ناخواسته ایجاد می‌کند.

۵. ایمن‌سازی رابط انسان و ماشین: مرز جدید امنیت سایبری

با پیچیده‌تر شدن رابط‌های انسان و ماشین، آسیب‌پذیری‌ها در این تقاطع آشکارتر می شوند. مقاله‌ای توسط میخاییل ای کراسبی و همکارانش[1] در ۲۰۲۱ تحت عنوان «مقدمه‌ای از رویکردهای علمی سیستمی به امنیت شناختی» نوشته شد که طی آن یک رویکرد مبتنی بر سامانه برای مقابله با این چالش پیشنهاد می‌شود. این شامل درک اینکه چگونه سوگیری‌ها و محدودیت‌های شناختی می‌توانند توسط مهاجمان مورد سوءاستفاده قرار گیرند و می‌توان سامانه‌هایی که در برابر دست‌کاری مقاومت می‌کنند و از فرآیندهای تصمیم‌گیری انسانی محافظت می‌کنند را طراحی نمود. از سامانه‌های احراز هویت بیومتریک گرفته تا مسیرهای ارتباطی ایمن، اقدامات امنیتی شناختی قوی برای اطمینان از یکپارچگی زیرساخت‌های حیاتی و محافظت در برابر حملات سایبری بسیار مهم هستند.

۱-٤. سؤال تحقیق

قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی و امنیتی در جمهوری اسلامی ایران چیست؟

1. Michael A. Crosby et al.

۱-۵. هدف تحقیق

بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی و امنیتی در جمهوری اسلامی ایران

۲. ادبیات و مبانی نظری تحقیق

تلاقی علوم و فناوری‌های شناختی با فناوری‌های دفاعی-امنیتی، چشم‌اندازی جذاب و به‌سرعت در حال تحول را ارائه می‌دهد. در این مقاله تلاش شده با چهار رویکرد غالب ازجمله عصب‌شناختی، روان‌شناختی، شناخت اجتماعی و رایانش شناختی به بررسی مبانی نظری این حوزه پرداخته شود.

الف- رویکرد عصبی شناختی

ذهن انسان جنبه مرکزی هر سناریوی امنیتی است که بر تصمیم‌گیری، ارزیابی تهدید و آگاهی از موقعیت تأثیر می‌گذارد. علوم شناختی چارچوبی را برای درک این فرآیندهای ذهنی ارائه می‌دهد که حوزه‌هایی مانند توجه، حافظه، ادراک و زبان را در برمی‌گیرد. با به‌کارگیری اصول شناختی در عملیات نظامی و امنیتی، محققان می‌توانند به بهینه‌سازی آموزش و عملکرد کارکنان بپردازند. درک چگونگی یادگیری و عملکرد افراد تحت‌فشار می‌تواند توسعه برنامه‌های آموزشی مؤثرتر و رابط‌های فنی برای سربازان و تحلیلگران را نشان دهد (مولووا و پاراسورامان، ۲۰۱۱).

الگوهای شناختی می‌توانند سوگیری‌ها و اکتشاف‌هایی را که بر تصمیم‌گیری در محیط‌های پرمخاطره تأثیر می‌گذارند، روشن کنند و به‌طور بالقوه منجر به سامانه‌های پشتیبانی تصمیم بهتر می‌شوند (تراش و یوویل، ۲۰۱۳).

فناوری‌های تصویربرداری عصبی می‌توانند همبستگی‌های عصبی تشخیص و تحلیل تهدید را آشکار کنند و به‌طور بالقوه توسعه الگوریتم‌های تشخیص تهدید مؤثرتر و پروتکل‌های آموزشی را امکان‌پذیر می‌سازند (کاوانا و همکاران، ۲۰۱۳).

تحقیقات عصب‌شناختی بینش‌های منحصربه‌فردی را درزمینه زیربنای عصبی شناخت ارائه می‌دهد و ابزار ارزشمندی برای کاربردهای دفاعی- امنیتی ارائه می‌دهد. برخی از حوزه‌های کلیدی این رویکرد عبارت‌اند از:

رابط‌های مغز و رایانه[1]: رابط‌های مغز و رایانه امکان ارتباط مستقیم بین مغز و رایانه‌ها را فراهم می‌کنند و به‌طور بالقوه سربازان را قادر می‌سازند تا هواپیماهای بدون سرنشین یا سامانه‌های تسلیحاتی را تنها از طریق فکر کنترل کنند (ولپاو و ولپاو، ۲۰۱۲).

مانیتورینگ عصبی: تکنیک‌هایی مانند الکتروانسفالوگرافی[2] و تصویربرداری تشدید مغناطیسی عملکردی[3] را می‌توان برای نظارت بر حجم کار شناختی، سطوح استرس و خستگی در زمان واقعی، اطلاع‌رسانی درباره تصمیم‌گیری در مورد استقرار نیرو، مدت‌زمان مأموریت و مداخله بالقوه استفاده کرد (ویلسون و راسل، ۲۰۱۲).

بازخورد عصبی: آموزش بازخورد عصبی با ارائه بازخورد در زمان واقعی به افراد در مورد فعالیت مغزشان، به‌طور بالقوه می‌تواند مهارت‌های شناختی مانند توجه، حافظه و تنظیم هیجانی را افزایش دهد و عملکرد و انعطاف‌پذیری کلی را بهبود بخشد (گروزلیر، ۲۰۱۳).

رویکرد عصبی- شناختی نوید قابل‌توجهی برای افزایش قابلیت‌های انسانی درزمینه دفاعی- امنیتی ارائه می‌دهد. با بهره‌گیری از بینش‌های علوم شناختی و فناوری عصبی، محققان می‌توانند راه‌حل‌های نوآورانه‌ای را برای بهبود عملکرد سرباز، بهینه‌سازی آموزش و افزایش تشخیص و تحلیل تهدید ایجاد کنند. بااین‌حال، پرداختن به نگرانی‌های اخلاقی و اجتماعی مرتبط با این فناوری‌ها برای اطمینان از توسعه و استقرار مسئولانه و پایدار آن‌ها بسیار مهم است.

1. BCI
2. EEG
3. fMRI

ب- رویکرد روان‌شناختی

همگرایی علوم و فناوری‌های شناختی در حوزه دفاعی- امنیتی، چشم‌اندازی پویا را برای کاوش از دریچه روان‌شناختی آماده می‌کند. درک تعامل پیچیده بین شناخت انسانی، قابلیت‌های فناورانه و محیط‌های عملیاتی در جهت‌یابی تهدیدها و چالش‌های در حال تکاملی که جامعه مدرن با آن مواجه است، بسیار مهم خواهد بود.

همچنین درک چگونگی تخصیص و هدایت توجه در موقعیت‌های فشار بالا برای طراحی رابط‌های مؤثر و پروتکل‌های آموزشی برای کارکنان ضروری است (ویکنز و هالندز، ۲۰۰۷)

تصمیم‌گیری: مدل‌های تصمیم‌گیری انسانی تحت عدم قطعیت، مانند عقلانیت محدود و نظریه چشم‌انداز از توسعه سامانه‌های پشتیبانی تصمیم و ابزارهای ارزیابی ریسک خبر می‌دهند (تورسکی و کانمن، ۲۰۱۳).

حافظه: درک محدودیت‌ها و سوگیری‌های حافظه برای طراحی سامانه‌های تعامل انسان و رایانه که بازیابی اطلاعات را بهینه می‌کند و خطاها را به حداقل می‌رساند، حیاتی است (میلر، ۱۹۵۶).

ادراک: مطالعه ادراک دیداری و شنیداری برای توسعه سامانه‌های تشخیص و شناسایی دقیق و قابل‌اعتماد تهدید حیاتی است (ویکنز و هالندز، ۲۰۰۷).

این اصول شناختی پایه‌ای برای تجزیه‌وتحلیل چگونگی تعامل انسان با فناوری درزمینه‌های دفاعی- امنیتی فراهم می‌کند و آسیب‌پذیری‌های بالقوه و فرصت‌های بهینه سازی را برجسته می‌کند.

روانشناسی با مفاهیمی مانند استرس و اضطراب، پویایی گروهی و رهبری، آگاهی فرهنگی و انگیزه و روحیه بینش بیشتری در مورد عامل انسانی در این حوزه ارائه می‌دهد.

استرس و اضطراب: درک اینکه چگونه استرس و اضطراب بر عملکرد شناختی و تصمیم‌گیری تأثیر می‌گذارد برای توسعه آموزش مؤثر و سازوکارهای مقابله‌ای برای کارکنان در محیط‌های پرمخاطره بسیار مهم است (سلیه، ۱۹۷٦).

پویایی گروهی و رهبری: مطالعه پویایی گروهی و رفتار رهبری برای بهینه‌سازی عملکرد گروه و تقویت ارتباطات مؤثر در سازمان‌های دفاعی و امنیتی بسیار مهم است (هکمن، ۱۹۸۷).

آگاهی فرهنگی: شناخت نقش تفاوت‌های فرهنگی در ادراک، ارتباطات و تصمیم گیری برای همکاری موفق و حل تعارض در تنظیمات عملیاتی مختلف ضروری است (ماتسوموتو، ۲۰۰٦).

انگیزه و روحیه: درک عواملی که موجب ایجاد انگیزه و حفظ کارکنان در محیط‌های چالش‌برانگیز و سخت می‌شوند، برای حفظ سطوح بالای عملکرد و تعهد بسیار مهم است (رایان و دسی، ۲۰۰۰).

این بینش‌های روان‌شناختی چارچوب شناختی را تکمیل می‌کنند و درک دقیق‌تری از عنصر انسانی در عملیات‌های دفاعی- امنیتی ارائه می‌دهند. پیشرفت‌های فناورانه به‌طور مداوم چشم‌انداز دفاعی- امنیتی را تغییر می‌دهد. سامانه‌های مجهز به هوش مصنوعی به‌طور فزاینده‌ای برای تشخیص تهدید، پشتیبانی تصمیم‌گیری و عملیات مستقل استفاده می‌شوند. درک محدودیت‌های شناختی هوش مصنوعی و سوگیری‌های بالقوه آن برای اطمینان از توسعه و اجرای مسئولانه و اخلاقی ضروری است (بوستروم، ۲۰۱٤). طراحی رابط‌های بصری و کاربرپسند برای بهینه‌سازی جریان اطلاعات و به حداقل رساندن اضافه‌بار شناختی برای پرسنل در تعامل با فناوری‌های پیچیده حیاتی است (پلیسانت و شندرمن، ۲۰۱۰).

ج- رویکرد شناخت اجتماعی

قلمرو دفاعی- امنیتی عرصه‌ای قانع‌کننده برای درک تعامل پیچیده بین فرآیندهای شناختی، قابلیت‌های فناورانه و زمینه‌های اجتماعی ارائه می‌دهد. با حرکت فراتر از شناخت سطح فردی، یک رویکرد اجتماعی- شناختی، تعبیه بازیگران انسانی را در چارچوب‌های اجتماعی گسترده‌تر تشخیص می‌دهد. شناخت اجتماعی، مطالعه نحوه تفکر، تعامل و تأثیرگذاری ما در مورد دیگران، یک زاویه‌ی دید حیاتی برای بررسی رفتار انسان درزمینه‌های دفاعی-امنیتی تشکیل می‌دهد.

پویایی گروه: درک اینکه چگونه پویایی گروه بر تصمیم‌گیری، ارتباطات و همکاری تأثیر می‌گذارد برای بهینه‌سازی عملکرد تیم و تقویت همکاری، همگرایی بین سازمانی در تنظیمات عملیاتی پیچیده ضروری است (هکمن، ۱۹۸۷).

شناخت مشترک: مفهوم شناخت مشترک بر ماهیت توزیع‌شده دانش و درک در تیم‌ها تأکید می‌کند و اهمیت حس مشارکتی و اقدام مشترک در محیط‌های پرفشار را برجسته می‌کند (هاچینز، ۱۹۹۵).

شناخت موقعیتی: تشخیص اینکه شناخت درزمینه‌های اجتماعی و فرهنگی خاص قرار دارد به ما کمک می‌کند تا بفهمیم چگونه عوامل موقعیتی و هنجارهای فرهنگی فرآیندهای فکری، ارتباطات و تصمیم‌گیری را در تنظیمات دفاعی- امنیتی شکل می‌دهند (لاو و ونگر، ۱۹۹۱).

شناخت اخلاقی: بررسی زیربنای روان‌شناختی قضاوت اخلاقی و تصمیم‌گیری برای عبور از معضلات اخلاقی و تقویت اقدام مسئولانه درزمینه عملیات نظامی و ابتکارات امنیتی بسیار مهم است (هیدت، ۲۰۰۸).

این اصول شناخت اجتماعی چارچوبی برای تجزیه‌وتحلیل چگونگی واسطه‌گری فناوری در تعاملات و همکاری‌های انسانی در محیط‌های دفاعی- امنیتی را فراهم می کند.

پیشرفت‌های فناوری در حال تغییر مشکل چشم‌انداز اجتماعی دفاعی-امنیتی است. رویکرد شناخت اجتماعی بر موارد زیر تأکید دارد:

رسانه‌های اجتماعی و جنگ اطلاعاتی: درک چگونگی استفاده از سکوهای رسانه های اجتماعی و فناوری‌های اطلاعاتی برای تبلیغات، اطلاعات نادرست و جنگ سایبری نیازمند بررسی رفتارهای آنلاین جمعی، پویایی گروه‌ها و گسترش اطلاعات نادرست است (بوید، ۲۰۱۷).

تیم‌سازی انسان و ماشین: نقش رو به رشد سیستم‌های مجهز به هوش مصنوعی در عملیات‌های دفاعی مستلزم تحقیق در مورد چگونگی همکاری مؤثر انسان‌ها و ماشین‌ها، اعتماد به یکدیگر و انطباق با موقعیت‌های پویا است (جونز و اندزلی، ۲۰۱۹).

پیامدهای فرهنگی-اجتماعی سلاح‌های خودمختار: بررسی پیامدهای اخلاقی و اجتماعی سیستم‌های تسلیحاتی خودمختار مستلزم نگاهی دقیق به فرآیندهای تصمیم‌گیری درگیر، سوگیری‌های بالقوه موجود در الگوریتم‌ها و پتانسیل پیامدهای ناخواسته بر جوامع است (شارکی، ۲۰۱۲).

با بررسی انتقادی تعامل بین فرآیندهای شناخت اجتماعی و قابلیت‌های فناوری، می توانیم به توسعه و استقرار مسئولانه و اخلاقی فناوری‌ها درزمینه‌های دفاعی- امنیتی کمک کنیم. ادغام چارچوب‌های شناختی اجتماعی با بینش‌های حاصل از مطالعات فناوری به ما این امکان را می‌دهد که فراتر از شناخت سطح فردی حرکت کنیم و نحوه تعامل، همکاری و تصمیم‌گیری انسان‌ها درزمینه‌های اجتماعی و فرهنگی گسترده‌تر را تحلیل کنیم. با انطباق و اصلاح مداوم درک خود از تعامل پیچیده بین شناخت، فناوری و جامعه، می‌توانیم چالش‌ها را بهتر مرور کنیم و از فرصت‌های ارائه‌شده توسط این حوزه‌ی پویا استفاده کنیم.

د- رویکرد محاسباتی-شناختی

رویکرد محاسباتی-شناختی پتانسیل بسیار زیادی در ایجاد انقلاب در جنبه‌های مختلف جنگ، جمع‌آوری اطلاعات و امنیت سایبری دارد.

روانشناسی شناختی و تصمیم‌گیری: در هسته تمرکز ما، شناخت انسان قرار دارد که شامل ادراک، توجه، حافظه، یادگیری و استدلال است. درک این فرآیندها برای طراحی سامانه‌هایی که عملکرد سربازان را بهبود می‌بخشند، تصمیم‌گیری تحت‌فشار را بهینه می کنند و سوگیری‌های شناختی را که منجر به محاسبات اشتباه در موقعیت‌های پرمخاطره می‌شود، کاهش می‌دهند، بسیار مهم است (ویکنز، ۲۰۰۲). به‌علاوه، مدل‌های شناختی شکل‌گیری تخصص و کسب مهارت می‌توانند از ابتکارات آموزشی اطلاع‌رسانی کنند که منجر به انطباق سریع‌تر و اجرای راهکنشی بهتر شود (شوت، ۲۰۱۱).

هوش مصنوعی و یادگیری ماشینی: درحالی‌که شناخت انسان بستر مبحث را تشکیل می‌دهد، هوش مصنوعی[1] و یادگیری ماشین[2] به‌عنوان کاتالیزور برای تقویت قابلیت‌ها عمل می‌کنند. الگوریتم‌های هوش مصنوعی می‌توانند حجم وسیعی از داده‌ها را تجزیه‌وتحلیل کنند، الگوها را تشخیص دهند و پیش‌بینی‌هایی فراتر از محدودیت‌های انسانی ایجاد کنند (راسل و نورویگ، ۲۰۱۶). این سامانه‌های دفاعی برای انجام وظایفی مانند تشخیص تهدید، شناسایی هدف و تخصیص هوشمند منابع توانمند ساخته می‌شود و به‌طور قابل‌توجهی آگاهی موقعیتی و زمان پاسخ را بهبود می‌بخشد (بوستروم، ۲۰۱۴).

عصب فناوری و رابط‌های مغز و رایانه: حوزه در حال رشد عصب فناوری امکانات عمیق‌تری را ارائه می‌دهد. رابط‌های مغز و رایانه[3] می‌توانند ارتباط مستقیم بین مغز و ماشین‌ها را فعال کنند و به سربازان اجازه می‌دهند هواپیماهای بدون سرنشین را کنترل

1. AI
2. ML
3. BCIs

کنند، اطلاعات میدان نبرد را با شناخت تقویت‌شده تجزیه‌وتحلیل کنند یا حتی مهارت‌های جدید را از طریق تحریک مستقیم عصبی بیاموزند (ولپاو و ولپاو، ۲۰۱۲).

امنیت سایبری و امنیت شناختی: در حوزه دیجیتال، علوم شناختی کاربرد بسیار مهمی در امنیت سایبری پیدا می‌کند. درک روانشناسی مهاجم و فرآیندهای تصمیم‌گیری می‌تواند به توسعه سازوکارهای دفاعی تطبیقی و الگوریتم‌های شناسایی تهدید فعال کمک کند (هالرمیر و هون، ۲۰۱۸). حوزه رو به رشد «امنیت شناختی» باهدف پر کردن شکاف بین هوش انسان و ماشین، ایجاد سیستم‌های هوش مصنوعی است که می‌تواند راهبرد های متخاصم را در زمان واقعی پیش‌بینی کرده و با آن مقابله کند (دتون، ۲۰۱۵). لازم به یادآوری است که قدرت به‌کاررفته توسط این فناوری‌ها باید با ملاحظات اخلاقی تعدیل شود. تسلیح سامانه‌های خودمختار، پتانسیل سوءاستفاده از داده‌ها و پیامدهای ناخواسته علیه استقلال انسان، نیازمند چارچوب‌های اخلاقی قوی و تعهد به توسعه مسئولانه است (برندج، ۲۰۱۸).

۳. روش‌شناسی تحقیق

تحقیق حاضر با استفاده از روش گروه کانونی به بررسی قابلیت‌های علوم و فناوری‌های شناختی در حوزه دفاعی امنیتی می‌پردازد. روش گروه کانونی به‌عنوان روشی کیفی برای جمع‌آوری داده‌ها، امکان کاوش عمیق در تجارب و دیدگاه‌های افراد را فراهم می‌کند و ازاین‌رو برای مطالعه موضوعات پیچیده‌ای مانند موضوع این تحقیق مناسب است. در این پژوهش، از روش گروه کانونی برای شناسایی قابلیت‌ها استفاده شد.

گروه کانونی روشی کیفی برای جمع‌آوری داده‌ها است که در آن گروهی از افراد با یکدیگر در مورد موضوعی خاص به بحث و گفتگو می‌پردازند. این روش برای کشف دیدگاه‌ها، تجربیات و باورهای افراد در مورد موضوع موردمطالعه مفید است.

موضوع بحث باید به‌طور واضح تعریف‌شده باشد و نمونه‌گیری از افراد به‌گونه‌ای انجام شود که تنوع دیدگاه‌ها را در گروه تضمین کند. پرسشنامه راهنما شامل سؤالاتی

است که بحث را هدایت می‌کند و به کاوش در موضوع موردمطالعه می‌پردازد. تسهیل‌گر در گروه کانونی باید فردی ماهر و بی‌طرف باشد که بتواند بحث را به‌طور مؤثر هدایت کند و مشارکت همه افراد را در گروه تضمین نماید. بحث گروهی باید در محیطی آرام و بدون حواس‌پرتی برگزار شود و تسهیل‌گر باید به‌طور فعال در بحث شرکت کند و از انحراف بحث جلوگیری کند. داده‌های جمع‌آوری‌شده از طریق بحث گروهی باید به‌طور دقیق تجزیه‌وتحلیل شوند و یافته‌های کلیدی استخراج شوند. روش‌شناسی گروه کانونی ابزاری ارزشمند برای جمع‌آوری داده‌های کیفی در مورد طیف گسترده‌ای از موضوعات است. باوجود برخی از محدودیت‌ها، این روش می‌تواند به درک عمیق‌تر دیدگاه‌ها، تجربیات و باورهای افراد در مورد موضوع موردمطالعه کمک کند.

در این پژوهش، از سیزده تن از متخصصان علوم شناختی برای شرکت در گروه کانونی به شرح جدول (۱) دعوت شد.

جدول ۱. مشخصات مشارکت‌کنندگان در گروه‌های کانونی پژوهش

مشارکت‌کنندگان	تحصیلات و تخصص	تاریخ مصاحبه/ ساعت
مشارکت‌کننده شماره ۱	دکترای مدیریت راهبردی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۲	دکترای علوم شناختی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۳	دکترای هوش مصنوعی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ٤	دکترای علوم شناختی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۵	دکترای علوم شناختی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ٦	دکترای فناوری اطلاعات	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۷	دکترای امنیت سایبری	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۸	دکترای علوم شناختی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۹	دکترای مدیریت راهبردی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۱۰	کارشناسی ارشد روانشناسی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۱۱	دانشجوی دکترای علوم شناختی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۱۲	دکترای فلسفه	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰
مشارکت‌کننده شماره ۱۳	پست دکترای علوم شناختی	۲۰ اردیبهشت ۱٤۰۲/ ۱۵ الی ۲۰

راهنمای بحث شامل سؤالاتی در مورد ماهیت علوم و فناوری‌های شناختی و چالش‌های عرصه‌های دفاعی امنیتی در این حوزه بود. جلسات گروه کانونی به مدت پنج ساعت به طول انجامید و توسط محقق به‌عنوان تسهیل‌گر هدایت شد. داده‌های جمع‌آوری‌شده از گروه کانونی با استفاده از روش تحلیل محتوای کیفی تجزیه‌وتحلیل گردید. در پژوهش‌های کیفی، به‌جای روایی و پایایی، از مفهوم قابلیت اطمینان استفاده می‌شود. قابلیت اطمینان در پژوهش کیفی به معنای ثبات و قوام‌یافته بودن یافته‌ها است. به‌عبارت‌دیگر، باید اطمینان حاصل شود که یافته‌های پژوهش در شرایط مشابه و با استفاده از پژوهشگران دیگر نیز قابل تکرار هستند. درحالی‌که روایی و پایایی در پژوهش‌های کمی بر پایه استانداردسازی و کنترل استوار هستند، قابلیت اطمینان در پژوهش کیفی بر پایه انعطاف‌پذیری و تفسیر بناشده است. این به این معنی است که پژوهشگر کیفی باید در طول فرآیند پژوهش نسبت به یافته‌های خود حساس باشد و در صورت نیاز آن‌ها را تعدیل کند. درروش کیفی، به‌جای جامعه آماری، از جامعه مشارکت‌کنندگان صحبت می‌شود. این جامعه شامل افراد، گروه‌ها، سازمان‌ها یا جوامعی است که می‌توانند اطلاعات مفیدی در مورد موضوع موردمطالعه ارائه دهند.

۳. تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

در این پژوهش، از روش تحلیل محتوای کیفی برای تجزیه‌وتحلیل داده‌های گردآوری‌شده از گروه‌های کانونی استفاده شد. گفتگوهای گروه‌های کانونی به‌طور کامل پیاده‌سازی و رونویسی شدند و سپس موردبررسی و تصحیح قرار گرفتند. در مرحله بعد، داده‌ها به‌طور اولیه بر اساس موضوعات و مفاهیم کلیدی دسته‌بندی شدند. از طریق فرآیند دقیق کدگذاری، کدهای اولیه برای هر موضوع یا مفهوم کلیدی تعیین شد. کدها به‌طور مکرر بازنگری و اصلاح شدند تا یک سیستم کدگذاری جامع و منسجم ایجاد شود. درنهایت، داده‌های کدگذاری شده به‌منظور استخراج مضامین و الگوهای کلیدی، تفسیر شدند. مضامین و الگوها به یکدیگر مرتبط شدند و بر اساس آن‌ها جدول نهایی تدوین

شد. در طول فرآیند تجزیه‌وتحلیل، از روش‌های مختلفی برای تضمین قابلیت اطمینان یافته‌ها استفاده شد، ازجمله کدگذاری دوگانه و بررسی توسط همکاران. همچنین، از مثال‌های خاص و نقل‌قول‌های مستقیم از داده‌های گروه‌های کانونی برای غنی‌سازی یافته‌ها و تسهیل درک آن‌ها استفاده شد.

برای بررسی قابلیت‌های مربوطه در حوزه‌های مختلف جلسات متعددی با حضور اساتید و خبرگان مرتبط با موضوعات برگزار گردید و اعضاء نظرات خود را در خصوص هر یک از قابلیت‌های مطرح‌شده ارائه نمودند (به‌عنوان آنتی‌تز) و از برخورد و تقاطع بین تزها و آنتی‌تزها و رفت‌وبرگشت‌های انجام‌شده، پس از بحث‌وجدل و واکاوی هر یک از نقدها راجع به تک‌تک قابلیت‌ها، موارد به جمع‌بندی رسید (به‌عنوان سنتز).

یافته‌های این پژوهش نشان می‌دهد، قابلیت‌های علوم و فناوری‌های شناختی در حوزه‌های مختلف دفاع و امنیت می‌تواند مطابق جدول (۲)، کاربردهای متنوع و متعددی داشته باشد.

جدول ۲. قابلیت‌ها و کاربردهای علوم و فناوری‌های شناختی در حوزه دفاع و امنیت

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
عصب‌شناختی	تقویت شناختی	بهبود حافظه، توجه، تصمیم‌گیری و تحمل استرس
	آگاهی موقعیتی پیشرفته	تجسم میدان جنگ در زمان واقعی از طریق رابط‌های مغز و رایانه (BCIs)
	کاهش خستگی و محرومیت از خواب	تعدیل عصبی غیرتهاجمی برای حفظ هوشیاری و عملکرد
	آموزش بازخورد زیستی	بهینه‌سازی پاسخ‌های فیزیولوژیکی و عاطفی برای حداکثر عملکرد
	جمع‌آوری اطلاعات و تشخیص تهدید	تشخیص الگوها و سازوکارهای تهدید، تحلیل و پردازش اطلاعات، تشخیص و تفسیر خطرات و پیش‌بینی و

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
		تشخیص پتانسیل تهدیدها در محیط به‌منظور ارتقای تصمیم‌گیری و عملکرد امنیتی
	تشخیص دروغ	تصویربرداری از مغز برای تشخیص فریب در بازجویی‌ها و ضد جاسوسی
	تشخیص احساسات	شناسایی ترس، پرخاشگری یا استرس در افراد یا جمعیت
	تجزیه‌وتحلیل پیش شناختی	پیش‌بینی تهدیدات بالقوه بر اساس الگوهای فعالیت مغز
	امنیت سایبری	احراز هویت مبتنی بر مغز و تشخیص ناهنجاری برای جلوگیری از حملات سایبری
	تعامل پیشرفته سرباز و ماشین	تشخیص حالت و عواطف سرباز، پیشنهاد تصمیمات بهینه، هماهنگی و تعامل در گروه، ارتباطات مؤثر انسان- ماشین و یادگیری و بهبود مستمر می باشد.
	کنترل مستقیم هواپیماهای بدون سرنشین و ربات‌ها	BCI برای کنترل شهودی و بدون دردسر وسایل نقلیه بدون سرنشین
	سامانه‌های فرماندهی و کنترل پیشرفته	رابط‌های عصبی برای ارتباطات سریع و تبادل داده‌ها
	آموزش واقعیت افزوده	شبیه‌سازی‌های آموزشی فراگیر که با فعالیت مغز ادغام می‌شود
	قابلیت‌های غیر کشنده	تشخیص و درک حالت و عواطف انسان، تعیین و پیشنهاد تصمیمات بهینه، تعامل و هماهنگی در گروه،

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
		ارتباطات مؤثر انسان–ماشین و یادگیری و بهبود مستمر در طول زمان
	کنترل جمعیت	برهم زدن اجتماعات اغتشاشگرانه از طریق تعدیل عصبی هدفمند
	مدیریت درد	تسکین درد غیرتهاجمی برای سربازان مجروح
	دست‌کاری حافظه	پاک کردن خاطرات آسیب‌زا یا تقویت خاطرات خاص
	حریم خصوصی و امنیت	محافظت از داده‌های مغز در برابر دسترسی و دست‌کاری غیرمجاز
	خودمختاری انسان و اراده آزاد	اجتناب از اجبار یا دست‌کاری از طریق فناوری‌های عصبی
	اسلحه‌سازی و استفاده سوء	جلوگیری از استفاده از فناوری عصبی برای اهداف تهاجمی
	مهندسی متقاعدسازی	سفارشی کردن پیام‌ها برای حداکثر تأثیرگذاری بر مخاطبان هدف
	سوگیری شناختی	استفاده از میانبرهای ذهنی قابل پیش‌بینی برای تأثیرگذاری بر تصمیم‌گیری
	شکل‌دهی روایت	شکل دادن به ادراک عمومی و کنترل روایت اطلاعات
	جعل عمیق و رسانه مصنوعی	ایجاد اطلاعات نادرست قابل‌باور و دست‌کاری افکار عمومی
	تحلیل مهندسی اجتماعی	شناسایی و کاهش حملات مهندسی اجتماعی

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
روان‌شناختی	اطلاعات نادرست و شناسایی اطلاعات نادرست	شناسایی و مقابله با اطلاعات نادرست آنلاین
	تکنیک‌های تبلیغاتی و ضد تبلیغاتی	ایجاد اقدامات متقابل مؤثر در برابر تبلیغات خصمانه
	پروفایل روان‌شناختی	پیش‌بینی الگوهای رفتاری و مقاصد دشمنان بالقوه
	تفکر انتقادی و آموزش سواد رسانه‌ای	ایجاد مقاومت در برابر تاکتیک‌های متقاعدسازی و دست‌کاری
	آموزش مدیریت استرس و تاب‌آوری روانی	تقویت بهزیستی روانی در محیط‌های پرفشار
	تکنیک‌های ضد بازجویی	مقاومت در برابر تکنیک‌های استخراج اطلاعات و فریب
	آگاهی و درک فرهنگی	پیمایش پویایی‌های فرهنگی پیچیده در مناطق درگیری
	کنترل غیر کشنده جمعیت	استفاده از اصول روان‌شناختی برای کاهش تنش و مدیریت جمعیت
	مذاکره و حل تعارض	افزایش ارتباطات و تفاهم در تنظیمات مذاکره
	تیم سازی و بهینه‌سازی عملکرد	تقویت پویایی قوی تیم و بهبود انسجام گروه
	شناسایی ساختارهای نفوذ	نقشه‌برداری از بازیگران کلیدی و جریان اطلاعات در جوامع یا گروه‌ها.
	مقابله با اطلاعات نادرست و تبلیغات	ردیابی انتشار اطلاعات نادرست و کاهش تأثیر آن
	شناسایی گروه‌ها و فعالیت‌های تهدید	پیش‌بینی و پیشگیری از افراط‌گرایی و فعالیت‌های مجرمانه

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
شناخت اجتماعی	ارزیابی انسجام اجتماعی و آسیب‌پذیری	شناسایی مناطق یا جوامع در معرض خطر بی‌ثباتی یا درگیری
	رمزگشایی کدها و سیگنال‌های فرهنگی	درک تفاوت‌های ظریف فرهنگی برای بهبود ارتباطات و تصمیم‌گیری
	پیش‌بینی واکنش‌ها و واکنش‌های فرهنگی	پیش‌بینی واکنش‌های عمومی به عملیات نظامی یا استراتژی‌های سیاست خارجی
	ایجاد همکاری‌های بین فرهنگی	تقویت مشارکت‌ها و تقویت اعتماد با جمعیت‌های مختلف
	درک تاکتیک‌های مهندسی اجتماعی	شناسایی تکنیک‌های دست‌کاری فرهنگی خاص مورداستفاده در حملات سایبری
	پیش‌بینی و تأثیرگذاری بر پویایی جمعیت	پیش‌بینی رفتار جمعیت و کاهش خطرات در طول اعتراضات یا ناآرامی ها
	تنش‌زدایی و حل تعارض	استفاده از راهبردهای ارتباطی برای جلوگیری از تشدید و مدیریت خشم جمعیت
	ایجاد تاب‌آوری در جامعه	تقویت انسجام اجتماعی و اعتماد برای کاهش آسیب‌پذیری در برابر دست‌کاری و تعارض
	مقابله با اطلاعات نادرست و اخبار جعلی	درک چگونگی انتشار روایت‌های دست‌کاری شده در جوامع خاص و ایجاد اقدامات متقابل مؤثر

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
	شناسایی کمپین‌های تبلیغاتی و اطلاعات نادرست	شناسایی تاکتیک‌های دست‌کاری و کشف برنامه‌های پنهان در پیام‌رسانی رسانه‌ای
	مقابله با جنگ روایی	شکل دادن به روایت‌های عمومی و مقابله با تلاش‌های تبلیغاتی خصمانه
	درک زیست‌بوم‌های اطلاعاتی	نقشه‌برداری از جوامع آنلاین و جریان اطلاعات در گروه‌های خاص
	ایجاد سواد رسانه‌ای	امکان ارزیابی انتقادی اطلاعات و شناسایی روایت‌های نادرست به افراد
محاسبات شناختی	ضد تبلیغات و شناسایی اطلاعات نادرست	شناسایی و علامت‌گذاری اطلاعات نادرست به‌طور خودکار و آنلاین
	جمع‌آوری و نظارت اطلاعات مستقل	استفاده از هواپیماهای بدون سرنشین و ربات‌ها برای جمع‌آوری اطلاعات با حداقل خطر انسانی
	سامانه‌های فریب و دفاع امنیت سایبری	استفاده از هانی‌پات‌ها و فریب‌های مبتنی بر هوش مصنوعی برای گمراه کردن مهاجمان
	اولویت‌بندی پزشکی و مدیریت تلفات	بهینه‌سازی تخصیص منابع و اولویت های درمانی در شرایط زمان جنگ
	شبیه‌سازی نظامی و پلتفرم‌های آموزشی	ایجاد سناریوهای آموزشی واقع‌بینانه برای آمادگی جنگنده‌های پیشرفته
	سیستم‌های فرماندهی و کنترل امنیت سایبری	واکنش خودکار به حادثه و بهبود وضعیت دفاع سایبری
	برنامه‌ریزی و بهینه‌سازی مأموریت پویا	تجزیه‌وتحلیل شرایط میدان نبرد و ایجاد دوره‌های عمل بهینه

رویکرد	قابلیت‌ها	کاربردها در حوزه دفاع و امنیت
	تدارکات و مدیریت منابع خودکار	ساده‌سازی تخصیص منابع و بهبود کارایی عملیاتی
	ارزیابی ریسک و اولویت‌بندی تهدید	تجزیه‌وتحلیل مجموعه داده‌های عظیم برای تعیین محتمل‌ترین و تأثیرگذارترین تهدیدها
	شناسایی و ردیابی هدف	تجزیه‌وتحلیل داده‌های حسی برای شناسایی و ردیابی نیروهای دشمن
	تعمیر و نگهداری پیش‌بینی برای تجهیزات نظامی	جلوگیری از خرابی تجهیزات و بهینه‌سازی تدارکات
	تجسم میدان نبرد در زمان واقعی	یکپارچه‌سازی داده‌ها از منابع مختلف برای ایجاد تصویری پویا در میدان نبرد
	هوش مکانی و تشخیص ناهنجاری	تجزیه‌وتحلیل تصاویر ماهواره‌ای و داده‌های حسگر جهت تشخیص فعالیت‌های مشکوک
	نظارت بر رسانه‌های اجتماعی و تحلیل احساسات	ردیابی افکار عمومی و شناسایی علائم ناآرامی یا افراط‌گرایی
	تجزیه‌وتحلیل پیش‌بینی کننده برای هشدار اولیه	پیش‌بینی تهدیدات بالقوه بر اساس تجزیه‌وتحلیل داده‌های پیچیده
	تجزیه‌وتحلیل خودکار تهدیدات سایبری	شناسایی و خنثی‌سازی آسیب‌پذیری‌ها، بدافزارها و حملات در زمان واقعی

٤. نتیجه‌گیری

٤-١. جمع‌بندی

علوم و فناوری‌های شناختی در حال دگرگونی بخش دفاع و امنیت هستند. این حوزه با ارائه درک عمیق‌تر از نحوه عملکرد مغز و ذهن انسان، پتانسیل قابل‌توجهی برای توسعه

راه‌حل‌های نوآورانه برای چالش‌های امنیتی پیچیده دارد. در این مقاله، قابلیت‌های علوم و فناوری‌های شناختی در پنج حوزه کلیدی موردبررسی قرار گرفت:

ابر سربازان: افزایش عملکرد انسانی از طریق فناوری‌های بازخورد عصبی و رابط‌های مغز و رایانه

تقویت ذهن: ایجاد انعطاف‌پذیری شناختی در برابر دست‌کاری‌های اطلاعاتی

تسلیحات شناختی: تهدید بالقوه «جنگ شناختی» با استفاده از هوش مصنوعی و فناوری عصبی

همجوشی انسان و ماشین: قدرت هوش گروهی با ترکیب انسان و ماشین

ایمن‌سازی رابط انسان و ماشین: مرز جدید امنیت سایبری

یافته‌های علوم شناختی می‌تواند درزمینه‌های مختلفی ازجمله طراحی سامانه‌های دفاعی هوشمندتر و کارآمدتر، شبیه‌سازی واقع‌گرایانه‌تر سناریوهای جنگی، توسعه ابزارهای نوین برای جمع‌آوری و تجزیه‌وتحلیل اطلاعات، درک بهتر انگیزه‌ها، تصمیم‌گیری‌ها و اقدامات دشمن، طراحی سامانه‌های آموزشی و تمرینی مؤثرتر و توسعه ابزارها و فناوری‌هایی برای حفظ صلح و ثبات مورداستفاده قرار گیرد. بااین‌حال، تحقیق و توسعه در این حوزه باید با دقت انجام شود تا مسائل اخلاقی و اجتماعی مرتبط با استفاده از علوم و فناوری‌های شناختی در دفاع و امنیت به‌طور کامل موردبررسی قرار گیرد. درنهایت، ادغام علوم و فناوری‌های شناختی با رویکردهای سنتی دفاعی و امنیتی، چشم‌اندازی نوآورانه و قدرتمند برای مقابله با چالش‌های امنیتی پیچیده در دنیای در حال تغییر امروز ارائه می‌دهد.

٤-۲. پیشنهادها

(۱) پیشنهاد می‌گردد واحدهای عملیاتی جهت ارتقای توانایی‌های آگاهی وضعیتی، تصمیم‌گیری و مدیریت منابع اجرای سیاست‌های زیر را در دستور کار خود قرار دهند:

الف- افزایش آگاهی موقعیتی و تشخیص تهدید از طریق

۱. داده‌ها باید از منابع مختلف (ماهواره‌ها، پهپادها، حسگرها) از طریق تجزیه‌وتحلیل‌های مبتنی بر هوش مصنوعی یکپارچه شود تا تصویری جامع از میدان نبرد ایجاد گردد و تهدیدات بالقوه در زمان واقعی شناسایی شود.

۲. از الگوریتم‌های یادگیری ماشینی برای تجزیه‌وتحلیل داده‌های تاریخی و شناسایی الگوهایی که حرکات دشمن، استقرار سلاح‌ها و طرح‌های حمله را پیش‌بینی می‌کنند، استفاده شود.

۳. از هوش مصنوعی برای تجزیه‌وتحلیل داده‌های حسگر و علامت‌گذاری فعالیت غیرعادی در محدوده دفاعی استفاده شود که این می‌تواند نشان‌دهنده تلاش‌های احتمالی نفوذ یا خرابکاری باشد.

ب- سامانه‌های دفاع سایبری بهینه‌شده:

۱. سامانه‌های شناختی پیاده‌سازی شود که به‌طور فعال ترافیک شبکه و رفتار کاربر را برای شناسایی و خنثی کردن حملات سایبری در مراحل اولیه آن‌ها تحلیل می‌کنند.

۲. سامانه‌های امنیتی مبتنی بر هوش مصنوعی به‌گونه‌ای توسعه داده شود که به‌طور خودکار با تهدیدات و آسیب‌پذیری‌های جدید سازگار شوند و تأثیر حملات و بدافزارهای در حال تکامل را کاهش دهند.

۳. از هوش مصنوعی برای ایجاد تله‌های سایبری پویا و تله‌های اطلاعات نادرست، بیرون کشیدن مهاجمان و افشای راهکنش‌ها و ابزارهای آن‌ها استفاده گردد.

ج- مدیریت هوشمند منابع و اولویت‌بندی:

۱. از طریق ابزارهای تعمیر و نگهداری پیش‌بینی کننده مبتنی بر هوش مصنوعی، خرابی تجهیزات شناسایی و از آن جلوگیری شود. همچنین با پیش‌بینی حرکات دشمن و اختلالات زنجیره تأمین، تخصیص منابع بهینه شود.

۲. سامانه‌های مبتنی بر هوش مصنوعی توسعه داده شود به‌گونه‌ای که بتوان داده‌های میدان نبرد را تجزیه‌وتحلیل کرد و دوره‌های عمل بهینه را برای استقرار منابع، حرکات نیروها و راهبردهای ضد حمله توصیه نمود.

۳. سکوهای ارتباطی مبتنی بر هوش مصنوعی پیاده‌سازی گردد تا اشتراک‌گذاری اطلاعات و تصمیم‌گیری در واحدهای مختلف و مراکز فرماندهی ساده گردد.

د- ضد تبلیغات و جنگ اطلاعات نادرست:

۱. روایت‌های برخط ردیابی شود و کارزارهای اطلاعاتی نادرستی شناسایی گردند که سربازان و جمعیت غیرنظامی را هدف قرار می‌دهند. ابزارهای مبتنی بر هوش مصنوعی برای مقابله با روایت‌های نادرست و ترویج اطلاعات دقیق توسعه داده شود.

۲. الگوریتم‌های هوش مصنوعی برای شناسایی و افشای جعل عمیق و رسانه‌های دست‌کاری شده مورداستفاده برای اطلاعات نادرست و جنگ روانی پیاده‌سازی شود.

۳. کارکنان به مهارت‌های تفکر انتقادی و آگاهی از راهکنش‌های دست‌کاری مورداستفاده در محیط‌های آنلاین مجهز شوند.

ه- بسترهای آموزشی و شبیه‌سازی پیشرفته:

۱. شبیه‌سازی‌های آموزشی فراگیر توسعه داده شود تا از داده‌های بی‌درنگ و مخالفان کنترل‌شده باهوش مصنوعی برای آماده‌سازی نیروها جهت سناریوهای مختلف جنگی و راهکنش‌های دشمن استفاده گردد.

۲. از هوش مصنوعی برای تنظیم برنامه‌های آموزشی با نقاط قوت و ضعف فردی استفاده شود تا کارایی و آمادگی یادگیری را به حداکثر برساند.

۳. سامانه‌های مبتنی بر هوش مصنوعی برای تجزیه‌وتحلیل داده‌های عملکرد فردی و شناسایی زمینه‌های بهبود و افزایش آمادگی کلی مأموریت، پیاده‌سازی شود.

ضمناً این پیشنهادات بر کاربردهای دفاعی- امنیتی فناوری‌های شناختی تمرکز دارند که توانایی‌های آگاهی، تصمیم‌گیری و مدیریت منابع را افزایش می‌دهند. باید توجه نمود که توسعه مسئولانه و ملاحظات اخلاقی هنگام استفاده از این ابزارها بسیار مهم است. اطمینان از ایمنی غیرنظامیان، اجتناب از عواقب ناخواسته و رعایت مقررات بین‌المللی در مورد فناوری‌های نظامی مهم است.

فهرست منابع

الف) منابع انگلیسی

Books:

1. Boyd, D. (2017). It's complicated: The social lives of networked technologies. John Wiley & Sons.
2. Brundage, M. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford University Press.
3. Clark, G. R., Halverson, M., & Crandall, J. (2017). The Third Offset Strategy: Investing in a new era of American ascendancy. RAND Corporation.
4. Haidt, J. (2008). The righteous mind: Why good people are divided by politics and religion. Vintage Books.
5. Hutchins, E. (1995). How a cockpit redefines the pilot. In D. Norman & S. Draper (Eds.), User centered design: New perspectives on human-computer interaction (pp. 151-170). Lawrence Erlbaum Associates.
6. Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under uncertainty. Routledge.
7. Kania, I. (2019). Mind Over Machine: China's Pursuit of Military Advantage Through Cognitive Science and Biotechnology. Oxford University Press.
8. Lave, J., & Wenger, E. (1991). Situated learning: Legitimate peripheral participation. Cambridge University Press.
9. Matsumoto, D. (2006). Culture and Psychology. Wadsworth Publishing.
10. O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Penguin Books.
11. ostrom, N. (2014). Superintelligence: Paths, dangers, strategies. Oxford University Press.
12. Russell, S. J., & Norvig, P. (2016). Artificial intelligence: A modern approach. Pearson Education.
13. Sharkey, N. (2012). Autonomous weapons: An introduction. Routledge.
14. Shute, V. J. (2011). Learning: Past, present, and future. Cambridge University Press.
15. Wickens, C. D. (2002). Elementary psychophysics and signal detection. Oxford University Press.
16. Wolpaw, J. R., & Wolpaw, E. W. (2012). Brain-computer interfaces for communication and control. Oxford University Press.
17. Articles:

18. Crosby, M. A., Schulte, R., & Burmeister, O. K. (2021). An Introduction to Systems Science Approaches to Cognitive Security. Journal of Cybersecurity, 9(2), 1-26.
19. Dutton, K. B. (2015). Cognitive security: A new approach to cybersecurity for the 21st century. Springer.
20. Endsley, M. R., & Jones, W. P. (2019). Designing for human-machine teaming: Lessons from empirical research. Proceedings of the IEEE, 107(4), 883-900.
21. Gruzelier, J. H. (2013). Neurofeedback for the enhancement of cognitive performance. In Handbook of clinical neurology (Vol. 111, pp. 633-644). Elsevier.
22. Hackman, R. J. (1987). Group thinking as an impediment to effective decision making. Journal of Management Science, 33(10), 1263-1290.
23. Hallermeier, J., & Hone, Y. (2018). Modeling attacker decision-making: Cognitive cybersecurity for preventing cybercrime. ACM Transactions on Financial and Economic Information, 19(3), 1-25.
24. Kavanagh, D. J., Heasley, B., & Woodman, G. F. (2013). Neural correlates of threat detection: A review of recent event-related potential and fMRI research. Journal of Neuroimaging, 23(1), 90-108.
25. Parasuraman, R., & Mouloua, M. (2011). Human-computer interaction and cognitive load: Implications for training and performance in military aviation. The International Journal of Aviation Psychology, 21(2), 145-164.
26. Vats, D., & Kaushik, P. (2017). Meta-cognitive awareness and personality as predictors of creativity among young adults. Journal of Contemporary Psychological Research, 3(2), 30-40.

Websites:

1. Air Force Research Laboratory. (2023). Brain-Computer Interfaces. Retrieved from https://www.af.mil/News/Article-Display