فصلنامه علمی امنیت ملی
سال دوازدهم، شماره چهل‌وچهارم، تابستان ۱۴۰۱
مقاله دوازدهم از صفحات ۳۹۶-۳۶۱

مقاله پژوهشی: فضای سایبر و جهانی شدن گستره تهدیدات امنیتی

۲۰.۱۰۰۱.۱.۳۳۲۹۲۵۳۸.۱۴۰۱.۱۲.۴۴.۱۲.۳

علی جعفری[۱] و محمد برجعلی‌زاده[۲]

تاریخ دریافت: ۱۳۹۹/۰۲/۲۶ تاریخ پذیرش: ۱۴۰۰/۰۹/۰۲

چکیده

گذار از عصر انقلاب اطلاعات و ارتباطات و تحولات بنیادین در فضای سایبر، شبکه‌ها، منابع و تهدیدات امنیتی و تروریستی را از وضعیت محدود خارج ساخته و در ساختار نظام جهانی گسترش داده است. اهتمام پژوهش حاضر، شناخت میزان تأثیرپذیری تهدیدات امنیتی و تروریستی از فضای سایبر در محیط بین‌المللی است. این پژوهش با استفاده از روش‌های توصیفی – تحلیلی، پیمایش و با استفاده از ابزار پرسشنامه پژوهشگر ساخته صورت گرفت. برای تجزیه‌وتحلیل داده‌ها از آماره‌های توصیفی، رگرسیون چندمتغیره و تحلیل عاملی استفاده شد. جامعه آماری تحقیق شامل استادان، دانشجویان و کارشناسان رسانه است. حجم نمونه نیز بر اساس فرمول کوکران، ۳۸۴ نفر و برای افزایش ضریب دقت به ۴۰۲ نفر برآورد گردید. براساس یافته‌ها، متغیر فناوری‌های ارتباطی و اطلاعاتی در گسترش تهدیدات امنیتی و تروریستی در عرصه بین‌الملل نقش دارد. از منظر پاسخگویان اینترنت، شبکه‌های ماهواره‌ای فارسی زبان و شبکه‌های مجازی مهم‌ترین ابزار تهدید علیه منافع جمهوری اسلامی ایران به شمار می‌روند.

کلیدواژه‌ها: فناوری اطلاعات و ارتباطات، فضای سایبر، تهدیدات سایبری، امنیت ملی.

۱. استادیار پژوهشگاه مطالعات آموزش و پرورش، سازمان پژوهش و برنامه‌ریزی آموزشی، تهران، ایران. (نویسنده مسئول) Email: alijafari.researcher@gmail.com

۲. دانش آموخته دکتری علوم ارتباطات، دانشگاه آزاد اسلامی.

مقدمه و بیان مسئله

فناوری اطلاعات و ارتباطات با استفاده از ظرفیت فضای سایبر، مجموعه فعالیت‌های دولت‌ها و ملت‌ها را شبکه محور ساخته و از طریق فضای مجازی امکان گردآوری، تمرکز، جابه‌جایی و پردازش اطلاعات را در سراسر جهان فراهم کرده است (حافظ نیا، ۱۳۹۴: ۱). این فناوری با تأثیر بر ژئوپلیتیک و مناسبات دولت‌ها، ارتباطات سیاسی و تهدیدات امنیتی را در نظام جهانی گسترش داده است (یزدان‌پناه و کامرانی، ۱۳۹۳: ۲۶).

ویژگی‌های فناوری‌های نوین: سرعت بالا، سهولت دسترسی و ارتباطات شبکه‌ای جهانی، سایبر با حذف محدودیت‌های مرزی کنشگری افراد، گروه‌ها، سازمان‌ها و دولت‌ها در مقیاس بین‌المللی افزایش داده و امنیت ملی کشورها و دولت‌ها را تحت تأثیر قرار داده است (میرمحمدی و محمدی لرد، ۱۳۸۷: ۳۶).

جنبه‌های تهدیدآمیز فضای سایبر باعث شد، مرکز اطلاعات ملی ایالات متحده آمریکا، تهدیدات سایبری را در ردیف مهم‌ترین تهدیدات فراروی امنیت ملی اعلام نماید، موازنه قدرت در فضای مجازی به نفع کنشگران مخرب شامل دولت‌ها، شبکه‌های تروریستی و گروه‌های جنایی سازمان یافته و افراد در حال تغییر است (یزدان پناه و کامرانی، ۱۳۹۴: ۲۷).

این تهدیدات خصوصیات منحصر به فردی دارد، از یک‌سو، گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شود و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در این فضا کمک می‌کند تا بازیگران جدید به‌راحتی در عرصه جهانی فعالیت کنند. در این بین «ظهور گروه‌های غیر حکومتی به‌ویژه تولید شبکه‌ها و قطب‌های تروریستی که در تلاش برای پذیرش نظم مسلط بین‌الملل و چینش نظمی نوین و یا آنارشی بین‌المللی می‌باشند» تهدیدی مهم به شمار می‌روند (ذوالفقاری و کیانژاد، ۱۳۹۷: ۳۱).

تروریسم مذهبی از ابعاد جدید تهدید در فضای سایبر است. القاعده و داعش (دولت اسلامی شام و عراق) نمونه کاملی از تروریسم مذهبی‌اند که از طریق از فضای مجازی کانون‌های تهدید را از خاورمیانه به سراسر جهان سرایت دادند (آدمی و نکویی، ۱۳۹۷: ۲۹۶). نتایج

مطالعات نای[۱](۱۳۹۸)، روزنا[۲](۱۳۹۵)، آلبرتس و پاپ[۳](۱۳۸۵)، کاستلز[۴](۱۳۹۶)، ذوالفقاری و کیانژاد (۱۳۹۷) و نجفی علمی (۱۳۹۱) به‌اتفاق ظرفیت‌های رو به تکامل فناوری‌های نوین به‌ویژه فضای سایبر را در توسعه دامنه تهدیدهای امنیتی کلاسیک و ایجاد صورت‌های جدیدی از تاکتیک‌های پیشرفته جنگ سایبری شامل: سخت، نرم و هوشمند، تروریسم سایبری، جاسوسی سایبری و جرائم سایبری را مورد تأکید قرار داده‌اند. تغییراتی که از دیدگاه نای (۱۳۹۸)، بستر پهناوری را برای نقش‌آفرینی دولت‌ها، سازمان‌ها و شرکت‌ها در سیاست جهانی فراهم ساخته است و ادامه این روند در دهه ۲۰۵۰ میلادی می‌تواند به انتقال قدرت از غرب به شرق بیانجامد. این وضعیت، بهره‌گیری نظام سلطه از ظرفیت‌های تهدیدزای فضای سایبر در تخاصم با کشورها را به‌شدت افزایش داده است. علاوه بر این، تراکم گروه‌های تروریستی در خاورمیانه، تحرکات تروریست‌ها در نوار مرزی غرب و شرق کشور، تهدید زیرساخت‌های حیاتی کشور از طریق اینترنت و رشد فزاینده جرائم سایبری مؤلفه‌هایی هستند که اهمیت و ضرورت شناخت ظرفیت‌ها و مخاطرات حال و آینده فناوری سایبر را بیش از پیش آشکار می‌سازد.

گسترش فن‌آوری‌های نوین ارتباطی در قالب همگرایی شبکه‌های ماهواره‌ای با اینترنت و فضای مجازی بسیاری از معادلات و مناسبات جهان امروزی را تغییر داده است. فضای مجازی به‌عنوان شاهکار انقلاب اطلاعات و ارتباطات با فراهم کردن بستر واگذاری قدرت از حکومت‌ها به گروه‌ها، سازمان‌ها و افراد، زمینه رشد و ظهور رقبای جدیدی را در عرصه جهانی فراهم ساخته و تهدیدات سایبری را در ردیف مهم‌ترین مسائل فراروی امنیت ملی دولت‌ها قرار داده است. تغییر موازنه قدرت در فضای مجازی به نفع کنشگران مخرب به‌عنوان عنصری راهبردی و تعیین‌کننده در روابط بین‌الملل، اهمیت شناخت این پدیده را بیش از پیش آشکار می‌سازد. گستره تأثیر فضای سایبر در امور سیاسی، فرهنگی، اقتصادی،

---

۱. Nye Joseph
۲. James N. Rosenau
۳. Alberts David and Pope Daniel
۴. Manuels Castell

اجتماعی، صنعتی و نظامی کشورهای مختلف، همچنین توسعه غیر متوازن ICT در کشور تحت تأثیر مدیریت ضعیف و تحریم‌های اقتصادی و صنعتی از سوی نظام سلطه مؤلفه‌ای است که ضرورت بررسی بنیادی و نظام‌مند نقش فناوری سایبر در توسعه امنیت و کاهش تهدیدات امنیتی و بهره‌گیری از نتایج تحقیق در تصمیم‌گیری‌ها و برنامه‌ریزی‌های نهادهای مسئول را نمایان می‌سازد.

مقاله حاضر با تکیه بر نتایج مطالعات اسنادی و میدانی درصدد شناخت تهدیداتی است که فضای سایبر در توسعه و گسترش آن در سطح جهان نقش دارد. تهدیدات سایبری علیه منافع ملی جمهوری اسلامی ایران و میزان بهره‌مندی ایران از فناوری سایبر برای مقابله با تهدیدات در سویه‌های تحقیق مورد توجه قرار گرفته است. امکان سنجش همزمان نقش ابعاد فناوری‌های ارتباطی و اطلاعاتی (ماهواره، اینترنت و فضای مجازی و ابزارهای این فناوری‌ها مانند شبکه‌های اجتماعی تحت وب و موبایلی، روزنامه‌نگاری سایبر) مزیتی است که مطالعه حاضر را از مطالعات مشابه مجزا می‌سازد. با توجه به آنچه بیان شد پژوهش حاضر درصدد پاسخ به سؤالات زیر است؛

اول: آیا تحولات قدرت در عصر حاضر به تحولات فناورانه در حوزه ارتباطات و اطلاعات وابسته است؟

دوم: آیا فناوری‌های ارتباطی و اطلاعاتی در گسترش تهدیدات امنیتی نقش دارند؟

سوم: آیا فناوری‌های ارتباطی و اطلاعاتی در ظهور کنشگران جدید در عرصه بین‌الملل نقش دارد؟

چهارم: گسترش تهدیدات تروریستی و امنیتی علیه منافع ملی جمهوری اسلامی ایران و نحوه مقابله با آن بیشتر تحت تأثیر کدام یک از ابزارهای فناورانه است؟

۱. مبانی نظری

۱-۱. پیشینه پژوهش

جوزف نای (۱۳۹۸) نویسنده کتاب آینده قدرت، فرایند تغییر در منابع قدرت در قرن ۲۰ و ۲۱ را در پرتو سه منبع قدرت سخت، نرم و هوشمند بررسی کرد. از نظر نای

گسترش فنّاوری‌های اطلاعاتی و ارتباطی به‌ویژه فضای بیکرانه سایبر از طریق جهانی شدن شبکه‌ها فرصتی بی‌نظیر برای غرب به‌ویژه ایالات متحده فراهم کرده که به مدد آن قادر است جهان را مطابق نظم نوین مورد نظر اداره و کنترل نماید. از منظر نای نقش فناوری در دستیابی سایر دولت‌ها و سازمان‌ها و گروه‌ها به این بعد از قدرت، کلید ظهور کنشگران جدید در عرصه بین‌المللی است.

صیاد و همکاران (۱۳۹۹) در مقاله‌ای با عنوان تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات متحده آمریکا و جمهوری اسلامی ایران، تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی را بررسی کرده‌اند. از منظر نویسندگان استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای تهدیدات امنیتی (خرابکاری، اخلال، ترور، جاسوسی و...) هموار ساخته است. نویسندگان با اشاره به توجه کم متخصصان ایرانی به شناسایی تهدیدهای سایبری بر به‌روزرسانی راهکارهای مقابله با این تهدیدات تأکید کردند.

رامک و محمدی (۱۳۹۹) در پژوهشی با عنوان ارائه مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور به این نتایج دست یافتند؛ وابستگی روزافزون زیرساخت‌های حیاتی کشور به فضای سایبری مجازی، زمینه‌ساز افزایش آسیب‌پذیری ناخواسته کشور در برابر حملات و تهدیدهای سایبری شده است. نویسندگان با مرور تهدیدات دفاعی و امنیتی کشور از سال ۱۳۹۷ تا ۱۳۹۹ دفاع سایبری کشور با بهره‌گیری از همکاری‌های بین‌المللی تقویت شود.

نتایج تحقیقات محمدی منفرد و همکاران (۱۳۹۹) درباره تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران نشان داد؛ نظام سلطه در ادامه تقابل دائمی خود با جمهوری اسلامی ایران از ظرفیت فضای سایبر به‌طور فزاینده‌ای بهره‌برداری می‌نماید. بر اساس یافته‌ها، کاربردهای اجتماعی فضای سایبر در ایران برای امنیت ملی مخاطره‌آمیز است و از بین تهدیدات، حوزه انسانی و شناختی با ۳۸ درصد، اطلاعاتی با ۳۴/۵ درصد و حوزه فیزیکی و زیرساختی با ۲۷/۵ درصد به ترتیب در اولویت قرار دارند.

شبکه‌های تروریسم در ژئوپلیتیک نوین جهانی و راهبردهای مدیریت آن عنوان تحقیق ذوالفقاری پژوهشگر پسادکتری دانشگاه هاروارد (۱۳۹۷). بر اساس یافته‌ها، مدیریت تروریسم با رویکرد اقتصادی، ۱. از طریق کاهش منافع تروریسم با تمرکززدایی اقتصادی، دولت‌مداری و جامعه ۲. پراکندگی رسانه‌ای ۳. افزایش هزینه‌های فرصت تروریسم با کاهش هزینه‌های رویکردهای بدیل صورت می‌پذیرد. نگارنده رسانه‌ها را ابزار تروریسم برای اشاعه‌ی ترس و تعمیم مطالبات خود و دستیابی به نفوذ حداکثری معرفی می‌کند.

مطالعات آدمی و نکویی (۱۳۹۷) نشان می‌دهد رسانه‌های نوین، به ابزار گروه‌های رادیکال برای تبلیغ ارزش‌ها و اقدامات ضد بشری آنان تبدیل شده و خاورمیانه را به کانون اصلی بحران مبدل ساخته است. القاعده و داعش، بیشتر مراحل عضوگیری، ترویج خشونت، مشروعیت‌سازی و فراخواندن پیام‌های خود را از طریق اینترنت و فضای مجازی انجام داده‌اند.

روزنا (۱۳۹۵) مؤلف کتاب فناوری اطلاعات و سیاست جهانی؛ تغییر گستره قدرت و حاکمیت، معتقد است، سیاست جهانی متأثر از تحولات فناورانه جدید، مقدمات گذار به ابعاد و صورت‌بندی‌های نوینی از قدرت و حاکمیت در سیاست جهانی را فراهم کرده است. از نظر روزنا قدرت دو بعد دارد. بعد ابزاری قدرت در توانمندسازی دولت‌ها و ساختاری آن در شکل‌گیری ساختارها و تغییر رفتار انسان کاربرد دارد. روزنا به روندی فرا بین‌المللی بر استفاده از قابلیت‌های فناوری‌های اطلاعاتی برای تمرکززدایی قدرت و اقتدار از دولت‌ها تأکید می‌کند.

نجفی علمی (۱۳۹۱) در تحقیقی که با هدف بررسی روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر در جمهوری اسلامی ایران انجام داد، به این نتیجه رسید که قابلیت و ظرفیت سازگاری روند تحولی جرم در کشور، همگام و همسو با روند تحولات فضای سایبر، الگوی تهدید جرم (اهداف و راهبردها، نوع، ماهیت، فرآیند، گستره، محیط، آثار و پیامدها) را پیچیده کرده است. نجفی با اشاره به نشت اطلاعات، سرقت داده‌های حیاتی و آسیب‌پذیری شبکه‌های جامع اطلاع‌رسانی کشور، به عدم توجه

جدی متخصصان به ظرفیت‌های فضای سایبر و امکان خسارات سنگین به سامانه‌های حیاتی کشور هشدار می‌دهد.

آلبرتس و پاپ (۱۳۸۵) مؤلفان کتاب «گزیده‌ای از عصر اطلاعات؛ الزامات امنیت ملی در عصر اطلاعات» موضوعات امنیت ملی، سلطه و مدیریت اطلاعات، جنگ‌های اطلاعاتی، جنگ روانی، جنگ الکترونیکی، جنگ رخنه‌گری (هک) و... را بررسی کردند. از نظر آن‌ها رشد اینترنت، نگرانی‌های اساسی در پی داشته، اما ایالات متحده و دنیا می‌توانند با دسترسی به یک شبکه جهانی مقاوم در حوزه‌های تجارت، فرهنگ، آموزش و در قلمرو ترویج آزادی‌گرایی منافع ملی‌شان را محقق سازند.

غلام‌نیا و همکاران (۱۳۹۸) در پژوهشی کاربردهای نظامی اینترنت اشیاء را با تأکید بر مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران بررسی کردند. آن‌ها میزان بهره‌برداری از اینترنت اشیاء در مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران را با طرح‌های ارتش آمریکا در بخش‌های دفاعی و امنیت عمومی و شبکه‌های تلفن همراه مقایسه کردند. نتایج نشان داد، کاربرد اینترنت اشیاء در صنایع نظامی ایران در مراحل آغازین بوده و نیازمند توجه بیشتر است.

۲-۱. تعریف مفاهیم

فناوری‌های نوین ارتباطی: فناوری؛ از دو واژه یونانی «Techne» به معنای هنر و مهارت و «Logia» به معنای علم و دانش تشکیل شده است. فن‌آوری عبارت است؛ شاخه‌ای از دانش که با ایجاد و استفاده از ابزارهای فنی و ارتباط آن‌ها با زندگی، جامعه و محیط زیست، با موضوعاتی چون هنر صنعتی، مهندسی، علوم کاربردی و علم خالص روبرو است (مهدی‌زاده، ۱۳۹۲: ۳۱۷). این فناوری ترکیبی از فناوری‌های وسایل ارتباط جمعی، انفورماتیک و ارتباطات راه دورند که از آن‌ها به‌عنوان رسانه‌های جدید نیز یاد می‌شود(برجعلی زاده و همکاران،۱۴۰۰: ۴۳). «دیجیتالی بودن» «تعاملی بودن» و «دسترسی گسترده شهروندان» ویژگی‌های مشترک آن‌ها است (قاضی‌زاده، ۱۳۸۷: ۱۲-۱۳).

فناوری اطلاعات:[۱] بنا بر تعریف انجمن فناوری اطلاعات آمریکا[۲] عبارت است از «مطالعه، طراحی، توسعه، پیاده‌سازی، پشتیبانی یا مدیریت سامانه‌های اطلاعاتی مبتنی بر رایانه، به‌ویژه برنامه‌های نرم‌افزاری و سخت‌افزار رایانه» (براون[۳] ۱۳۹۷).

اینترنت: سامانه‌ای جهانی و از شبکه‌های رایانه‌ای به‌هم‌پیوسته است که از پروتکل برای ارتباط با یکدیگر استفاده می‌کنند. اینترنت دربرگیرنده منابع اطلاعاتی و خدمات گسترده‌ای است که برجسته‌ترین آن‌ها وب جهان‌گستر و رایانامه‌ها هستند. «چیپونزا» با اشاره به سازوکارهای تعاملی اینترنت تأکید می‌کند، اینترنت امکان تعامل و تبادل و اشتراک اطلاعات دو و چندجانبه را تحت وب و با استفاده از وبلاگ‌ها، ویکی‌ها، پادکست‌ها، ایمیل‌ها، گروه‌های مباحثه، اتاق‌های گفتگو، انجمن‌های گفتگو، فهرست‌های پستی، سیستم‌های ثبت پیام و پیام فوری فراهم می‌کند (چیپونزا، ۲۰۰۷: ۸۵-۶۱).

فضای سایبر:[۴] فضای سایبر یک مفهوم برای توصیف فناوری دیجیتال به‌هم‌پیوسته و گسترده است. لفظ مادرِ فضای سایبر، سایبرنتیک است که از یونانی باستان به معنای فرماندار یا راننده مشتق شده، واژه‌ای که نوربرت وینر برای کار پیش‌گامانه‌اش در مخابرات الکترونیک و علم کنترل به کار برد (برجعلی زاده، ۱۳۹۹: ۳۰-۲۹). فضای سایبر ارتباطات صورت گرفته مبتنی بر سیستم‌های مخابراتی را نیز شامل می‌شود. از نظر لیبیسکی به‌مثابه قلمروی جهانی در محیط اطلاعاتی و شامل: اینترنت، شبکه‌های ارتباط راه دور، سیستم‌های رایانه‌ای، پردازشگرها و کنترل‌کننده‌ها است (لیبیسکی، ۲۰۰۹: ۶). برخی فضای سایبر را با اینترنت و اشتباه می‌گیرند. برخی نیز آن را فضای مجازی معنا می‌کنند که این نیز اشتباه است، فضای سایبر اگرچه مجازی است به این معنا که در عالم واقعیت وجود ندارد، اما دقیقاً معادل virtual نیست. برای این منظور لازم است اشاره کنیم واژه virtual که مجازی ترجمه می‌شود، دو حوزه را پوشش می‌دهد، هم برای بیان آنچه که در جهان واقعیت

---

۱. Information Technology (IT)
۲. American Information Technology Association (ITAA)
۳. Michael Brown
۴. Cyberspace

وجود ندارد به کار می‌رود و هم در علوم کامپیوتر برای توصیف آنچه که توسط سیستم رقم می‌خورد کاربرد دارد.

فضای مجازی: ویتل فضای مجازی را مجموعه‌ای از فضای روانی و خیالی- مفاهیم و تعاملات شبکه‌ای شده و حالتی از اندیشه که توسط افراد به اشتراک گذارده می‌شود تعریف می‌کند. فضایی که در آن افراد در زمان و مکان جدا با ابزار فیزیکی از طریق شبکه‌ها به یکدیگر متصل‌اند (هانی، ۲۰۰۶: ۳۶-۳۵). به اعتقاد بندیکت: «فضای مجازی یک دنیای جدید و موازی است که با خطوط ارتباطی و کامپیوترهای جهان خلق و نگهداری می‌شود. دنیایی که در آن تردد جهانی دانش، رموز، سنجش‌ها، شاخص‌ها، سرگرمی‌ها و عاملیتِ دیگر انسانی شکل می‌گیرد» (بل، ۱۳۸۹: ۲۳-۲۲). هریک از عناصر فضای مجازی به‌عنوان مؤلفه‌های قدرت مجازی در حوزه ارتباطات و اطلاعات به شمار می‌آیند که امکان بسیج و منعکس‌سازی قدرت هنجاری یک کشور را در حوزه‌های جغرافیایی دوردست فراهم می‌سازد(فتاحی اردکانی و همکاران، ۱۳۹۷: ۱۴۷). تعامل در فضای مجازی از طریق سازوکارهای نوینی مانند شبکه‌های اجتماعی، وبلاگ‌ها، ایمیل، سایت‌های اینترنتی، اتاق‌های گفتگو (چت)، کنفرانس‌های ویدیویی، سیستم‌های ثبت پیام فوری، فهرست‌های پستی، انجمن‌های مباحثه و پادکست امکان‌پذیر می‌شود. هر کدام از این سازوکارهای ارتباطی، با توجه به ویژگی خود، سطح خاصی از تعامل را فراهم می‌کنند (خانیکی و بابایی، ۱۳۹۰: ۷۶-۷۹).

شبکه‌های اجتماعی مجازی: این شبکه‌ها زنجیره‌ای از ارتباطات و گره‌های شبکه اجتماعی هستند که با حضور غیر فیزیکی افراد در محل مجازی از طریق پیام‌رسان‌های مبتنی بر چت و ارتباط آنلاین، از طریق وب یا تلفن‌های همراه اجرا می‌شود (کاستلز، ۱۳۹۶: ۱۳-۱۰). جامعه شبکه‌ای از اتصال میلیون‌ها شبکه پویا و در حال افزایش تشکیل‌شده است. گره‌ها منابع مادی و غیرمادی را در درون شبکه به جریان می‌اندازند و حیات را تداوم می‌بخشند. آنچه که شبکه‌های اجتماعی مجازی را از شبکه‌های اجتماعی فیزیکی متمایز می‌سازد، نه بنیان‌های نظری آن‌ها، بلکه متفاوت بودن بستر و سازوکارهای ارتباطی و شیوه تعامل است(خانیکی و بابایی،۱۳۹۰: ۸۲). در این شبکه‌ها، افزون بر تعامل درون شبکه‌ای، تعامل‌های

برون شبکه‌ای نیز رایج است. این تعامل‌ها، نه تنها سرمایه اجتماعی و قدرت می‌آفرینند بلکه در ایجاد موج‌های اجتماعی و تأثیر بر واقعیت‌های محیط واقعی، نقش‌آفرین هستند. کنشگران در شبکه‌های اجتماعی، طیف وسیعی از افراد، گروه‌ها، شرکت‌ها و حتی کشورها را شامل می‌شود.

روزنامه‌نگاری سایبر: به روزنامه‌نگاری اطلاق می‌شود که به‌صورت الکترونیکی، تحت محیط وب در بستر اینترنت اجرا می‌گردد. روزنامه‌های الکترونیک، دارای هویت و ماهیتی متفاوت با روزنامه‌های چاپی هستند و لحظه‌به‌لحظه مهم‌ترین و تازه‌ترین تحولات داخلی و خارجی را در چارچوب خط‌مشی‌های تعیین‌شده برای روزنامه در محیط وب منتشر می‌سازند. ارائه هم‌زمان مطالب به‌صورت نوشتار، صوت و تصویر، دسترسی به بانک اطلاعات روزنامه، دریافت و ایفای نقش از طریق کامنت‌گذاری و تکمیل مطالب از سوی مخاطب ازجمله ویژگی‌های روزنامه‌نگاری الکترونیک است.

شبکه‌های ماهواره‌ای: ماهواره به دستگاه‌های ساخت بشر گفته می‌شود که به‌صورت عمدی به فضا فرستاده شده و در مدارهایی به گرد زمین یا سیارات می‌چرخند. شبکه‌های ماهواره‌ای امکانات و مزایای بسیاری همچون تنوع سرویس، انعطاف‌پذیری و استقلال از موانع طبیعی، سرعت عمل بالا و پوشش‌دهی وسیع فراهم می‌کنند که سایر روش‌های مخابراتی من‌جمله فیبر، کابل و یا مایکروویو زمینی قادر به ارائه آن‌ها نیستند (وبگاه سازمان فضایی ایران، ۱۳۹۵). این شبکه‌ها با سرعتی شگرف و بی‌اعتنا به مرزهای سنتی سیاسی، اجتماعی، فرهنگی و حقوقی، مجموعه‌ای از چالش‌ها و فرصت‌ها را فراهم می‌کنند. الیزابت روبینسون، رابرت پارک، هربرت بلومر و مایکل براون نیز تلویزیون‌های ماهواره‌ای را عامل تشدید بحران‌های ملی، همگون‌سازی فرهنگی، تحمیل و سلطه روابط نابرابر فرهنگی معرفی می‌کنند (حاجی محمدی و بیچرانلو، ۱۳۹۳: ۲۰).

امنیت[۱] به معنای آسایش خاطر، اطمینان، تأمین و مصونیت، ترکیبی است از دو واژه se به معنای جدا و curare به معنای مراقبت کردن، به عبارت بهتر چیزی را مورد مراقبت قرار

۱. Security

دادن است (نقبایی، ۱۳۹۱: ۱۶۲۷). امنیت به مفهوم کلی آزادی و رهایی از ترس و خطر و احساس ایمنی از هرگونه تهدید و یکی از نیازهای اولیه و اساسی انسان است. بوزان امنیت را موضوعی بین ذهنی و مبتنی بر تصمیم بازیگر می‌داند اما بر شناسایی آن در اجتماع تأکید دارد. درواقع این نظریه ترکیبی از رهیافت‌های مادی و سازه‌انگارانه می‌باشد که با توجه به ناتوانی مکاتب رئالیسم و ایدئالیسم در پیش‌بینی جنگ سرد در دهه ۶۰ میلادی، از سوی افرادی همچون باری بوزان و الی ویور ارائه گردید (صیاد و همکاران، ۱۳۹۹: ۳۰۰- ۲۹۸).

استفن والت[1] در چهارچوب مکتب واقع‌گرایی تدافعی ادعا می‌کند که مطالعات امنیتی بایستی بر روی پدیده جنگ که به‌وسیله قدرت‌های نظامی که تحت کنترل سیاسی بازیگران دولتی اداره می‌شوند تمرکز کند. در واقع نگاه واقع‌گرایان به پذیرش عناصر مکمل قدرت در چارچوب قدرت نظامی باعث شده است تا ابعاد گوناگون فضای سایبری در مطالعات این رویکرد جایگاه برجسته‌ای نداشته باشد اما در مقابل نوواقع‌گرایان در توسعه دستور کار مطالعات امنیتی، امنیت سایبری را مورد ملاحظه قرار داده‌اند، هرچند درباره‌ی چگونگی تأثیرگذاری واقعی حمله‌های سایبری بر امنیت فیزیکی دولت‌ها و ظرفیت نظامی‌شان اتفاق نظر ندارند (صیاد و همکاران، ۱۳۹۹: ۳۰۳). در مقابل این دو رویکرد، مکاتب لیبرالیسم و نئولیبرالیسم با تمرکز بر مطالعات گسترده پیرامون فنّاوری‌های نوین، استفاده از ابعاد پیشرفته این فناوری را در حوزه‌های نظامی مورد تأکید قرار داده‌اند.

امنیت ملی:[2] امنیت ملی از مشتقات امنیت است که در مرزهای جغرافیایی یا کشور به‌صورت امنیت داخلی (مصونیت بنیان‌های ایدئولوژیک مکتب حاکم و حفظ حاکمیت) و امنیت عمومی (حفظ حقوق و مصالح افراد، گروه‌ها و نهادهای اجتماعی) تعریف شده است (غرایاق زندی، ۱۳۹۰: ۲۸). از نظر بوزان و ویور امنیت ملی از مؤلفه‌های عینی، مانند مؤلفه‌های اقتصادی (تولید ثروت)، سیاسی (نهادهای مسلط در حوزه قدرت)، زیست محیطی (صیانت از فضای طبیعی) و نظامی (استحکامات دفاعی و هجومی و بازدارندگی

---

۱. Stephan Walet
۲. National Security

رقبا) تشکیل شده است و در صورت بروز تهدید برای هرکدام از این مؤلفه‌ها، دولت به‌عنوان بازیگر اصلی وارد عمل شده و با امنیتی کردن امور عادی، برای جلب منابع مالی و توجه اجتماعی مبادرت می‌کند (هلیلی و همکاران، ۱۳۹۷: ۱۸۱). در بسیاری از منابع، امنیت ملی با مصادیقی مانند استقلال، ثبات سیاسی و حفاظت از تمامیت ارضی و منافع ملی در برابر تهدیدات خارجی مرتبط است؛ از این‌رو تعریف امنیت ملی در هر کشور با توجه به منافع و ارزش‌های ملی، ایدئولوژی نظام سیاسی حاکم و نحوه تعامل با دیگر کشورها متفاوت است.

امنیت منطقه‌ای[۱]: نظریه‌ای در زمینه تبیین امنیت بین‌المللی است که ساختار آن با امنیت ملی کشورها و میزان تعامل آن‌ها در برقراری امنیت ارتباطی مستقیم دارد. اتحادیه‌های امنیت منطقه‌ای به‌عنوان الگوهای متمایز و پایدار تعامل امنیتی بین بازیگران تعریف می‌شوند (گوپتا، ۲۰۱۰). بوزان و ویور معتقدند که حتی منافع امنیتی قدرت‌های جهانی نیز اساساً ماهیتی منطقه‌ای دارند زیرا هنگامی که یک کشور اطراف کشور دیگری را مورد حمله و تهاجم قرار می‌دهد نه فقط امنیت ملی بلکه امنیت منطقه‌ای آن کشور به هم خورده است (بوزان و ویور[۲] ۲۰۰۳).

امنیت بین‌الملل[۳]: حالتی است که در آن قدرت‌ها در حالت تعادل و بدون دست‌یازی به قلمرو یکدیگر به سر برند و وضع موجود در خطر نیفتد. هرگاه یکی از قدرت‌ها از محدوده خود پا فراتر گذارد، از لحاظ قدرت (و یا قدرت‌های) مخالف، امنیت بین‌المللی در خطر افتاده است (آشوری، ۱۳۸۷: ۳۸).

امنیت سایبری[۴]: با ظهور فضای (دنیای) سایبری، کاربران یا همان شهروندان سایبری برای فعالیت نیاز به احساس امنیت دارند، همان‌گونه که در فضای فیزیکی و واقعی نیازمند برخورداری از امنیت هستند که این امنیت ابتدا با افزایش سطح آگاهی و دانش خود

---

۱. Regional security
۲. Weaver
۳. International Security
۴. Cyber Security

کاربران و سپس با کمک شرکت‌های امنیتی و مراجع قانونی و پلیس‌های سایبری فراهم می‌شود (داداندیش و کوزه‌گر کالجی، ۱۳۸۹: ۷۸).

تهدیدات سایبری: تهدیدهای سایبری به‌صورت وقایعی که به‌صورت طبیعی و یا توسط انسان (عمدی یا غیرعمدی) بر فضای مجازی تأثیرگذار باشد یا حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد تعریف شده است. تهدیدهای سایبری ویژگی‌های منحصربه‌فردی دارند. این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند که به دلیل تأثیرگذاری شگرف، عدم شفافیت عمومی، هزینه کم فناوری رایانه‌ای- اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب زمینه تعدد بازیگران در فضای سایبری را فراهم می‌کند. تهدیدکنندگان سایبری شامل: دولت‌های متخاصم، مزدوران سایبری یا گروه‌های تحت حمایت دولت‌ها، جاسوسان سایبری، تروریست‌های سایبری، مجرمین سازمان‌یافته سایبری و هکرهایی با انگیزه سیاسی هستند. در این زمینه، بیشترین نگرانی از ناحیه حملات سایبری سازمان یافته است که می‌تواند، لطمه‌های جبران‌ناپذیر بر زیرساخت‌های حیاتی کشورها وارد سازد (تقی‌پور و همکاران، ۱۳۹۷: ۲۰-۹).

ترور: به نوشته دایره المعارف فرانسوی لاروس، واژه‌ی «ترور»[1] برگرفته از ریشه لاتین (Terreur) بوده که به معنای نظام یا رژیم وحشت است (لاروس، ۱۹۶۴: ۲۵۸). کلید واژه ترور عبارت است از ایجاد هراس در توده مردم یا گروهی از مردم به‌منظور درهم شکستن مقاومتشان؛ برقراری نظام یا فرایند سیاسی بر پایه این ترس، از طریق به‌کارگیری اقدامات حاد و خشونت‌بار (علی بابایی،۱۳۸۴: ۱۸۸-۹۴).

تروریسم: تروریسم کاربرد نظام‌مند ارعاب یا خشونت پیش‌بینی‌ناپذیر بر ضد حکومت‌ها، مردمان یا افراد برای دستیابی به یک هدف سیاسی است. از منظر الکس پ. اشمید[2] تروریسم شیوه اقدامات تکراری به‌منظور ایجاد دلهره و رعب و وحشت است که به

---

۱. Terror
۲. Alex P. Schmid

دلایل سلیقه‌ورزی، جنایی و یا سیاسی توسط گروه‌های مختلف به‌کار گرفته می‌شود(برجعلی زاده و همکاران، ۱۳۹۸: ۱۵۲) اساساً تروریسم یک مفهوم نسبی است که درک تغییر واقعیات ژئوپلیتیکی بر چگونگی تفسیر کنش‌های خشونت‌آمیز بازیگران آن تأثیر می‌گذارد. در این پیوند شبکه‌های تروریسم را می‌توان برآیندی از پارادایم‌های «شکاف»[۱]، «نارضایتی و مطالبه‌گری»[۲]، «ایدئولوژی»[۳] و «فنّاوری»[۴] تلقی کرد. به بیان دیگر شبکه‌های تولید تروریسم برخلاف باور جاری بین‌الملل تنها با ابعاد ایدئولوژیک و اسلامی شناخته نمی‌شوند بلکه دارای وجوه دیگری نیز هستند. جدایی‌طلبی ملی‌گرا، سیاسی و دینی دیگر ابعاد شناخته شده تروریسم در جهان است (ذوالفقاری و کیانژاد،۱۳۹۷: ۳۲).

سایبر تروریسم: به‌طور کلی استفاده از ابزارهای دیجیتال و سامانه‌های کامپیوتری برای ایجاد خشونت و تهدید یا هر نوع عملیات خرابکارانه را سایبر تروریسم می‌نامند. به اعتقاد کالین[۵] تروریسم مجازی به حمله یا حملاتی اطلاق می‌شود که با برنامه‌ریزی قبلی و با اغراض سیاسی، توسط گروه‌های ضد دولتی خارجی یا مأموران مخفی خارجی، یا اشخاص حقیقی علیه سامانه‌های اطلاعاتی و ارتباطی، سامانه‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها انجام می‌شود (برجعلی‌زاده، ۱۳۹۹: ۱۰۸- ۱۰۶). در بین سازمان‌های تروریستی، داعش موسوم به (دولت اسلامی شام و عراق) از رسانه‌های نوین برای هدایت افکار عمومی به‌خوبی بهره گرفته (ماهرخ، ۲۰۱۵: ۱۰) و جدیدترین فیلم‌ها، اعلامیه‌ها و نشریات را در فضای مجازی، تالارهای گفت‌وگو و انجمن‌ها قرار داده و در شبکه‌های اجتماعی نظیر توییتر، فیس‌بوک و گوگل پلاس بازنشر می‌کنند (محزم، ۲۰۱۵: ۱).

---

۱. فقدان انسجام و یکپارچگی، اقلیت سازی، انشقاق‌های جامعه درونی و بحران‌های هویت

۲. سطح اشتغال پایین، سطح آموزش و تحصیلات پایین، محرومیت از حقوق سیاسی و دموکراتیک و تبعیض

۳. اعتقادات و باورها، جنبش‌های سیاسی و ارزش‌ها

۴. شبکه‌های اجتماعی، خانوادگی و جنایی، نهادها و ژئوپلیتیک آسیب‌پذیر و منازعه خیز، ناموازنه‌گری قوا، افراد تهدیدزا و افراد کاریزماتیک

۵Collin Barry

جنگ سایبری: امروزه با ظهور و معرفی الگوهای جنگ شبکه محور با معکوس کردن سیاست درگاه‌های ارتباطی گسترش یافته و همچنین مرتبط سازی دارایی‌های جنگی به مراکز فرماندهی موجب تغییر شکل رویکردهای نظامی قدیمی شده است (غلام‌نژاد و دیگران، ۱۳۹۸: ۱۴۵). در این جنگ، کشمکش اصلی برای تصاحب اطلاعاتی است که نقشی محوری دارد و به‌تدریج جای منازعاتی را خواهد گرفت که در گذشته بر سر دست‌یابی به مواضع جغرافیایی درمی‌گرفت. سرقت چندین ترابایت از اطلاعات برنامه‌های جنگنده‌های مشترک ۳۰۰ میلیاردی امریکا در سال ۲۰۰۹ نمونه کوچکی از جنگ سایبری است. این حادثه اوباما را بر آن داشت تا رسماً فضای سایبر به‌عنوان دارایی مهم ملی ایالات‌متحده و بر دفاع از آن تأکید نماید (خلیلی‌پور رکن‌آبادی،۱۳۹۱: ۱۹۹و۱۹۸).

هوش مصنوعی: از نظر جان مکارتی[1](۱۳۵۶) هوش مصنوعی «دانش و مهندسی ساخت ماشین‌های هوشمند» است. اصطلاحی برای توصیف ماشین‌ها یا کامپیوترهایی که فعالیت‌های شناختی وابسته به ذهن انسان را به‌خوبی انجام می‌دهند. باب ورک، یکی از پیشگامان فناوری هوش مصنوعی که تا سال ۲۰۱۷ معاون وزارت دفاع آمریکا بود بدون اشاره به پروژه خاصی می‌گوید: «هوش مصنوعی و یادگیری ماشین به شما کمک می‌کند سوزن را در انبار کاه پیدا کنید» (نایک، ۲۰۱۸). طبق پیش‌بینی‌ها هوش مصنوعی تا سال ۲۰۳۰، برای اقتصاد جهانی، حدود ۱۵ تریلیون دلار ارزآوری خواهد داشت. از نظر پوتین، رئیس جمهور روسیه، حکمرانی بر آینده جهان به میزان پیشرفت در استفاده از هوش مصنوعی بستگی دارد (قلی‌زاده و دیگران، ۱۳۹۷).

اینترنت اشیاء[2] فناوری اینترنت اشیاء یکی از فناوری‌های نوظهور است که امکان ارسال و دریافت داده‌ها بین اشیاء از طریق شبکه‌های ارتباطی را فراهم نموده و منشأ تغییرات بسیار در حوزه‌های مختلف از جمله نظامی است. اینترنت اشیاء با ترکیب دو عرصه دیجیتالی و فیزیکی، دسترسی به فناوری اطلاعات را گسترده‌تر می‌سازد و تغییرات

---

۱. John McCarthy

۲. Internet of things(IOT)

وسیعی را در چگونگی نظارت بر فعالیت‌ها از راه دور فراهم می‌کند (رمضانی و موحدی صفت، ۱۳۹۹: ۲۰۰- ۱۹۹). امروزه استفاده از حسگرهای پیشرفته در سامانه نظارت و شناسایی هواپیماهای بدون سرنشین، سامانه‌های ارتباطی ماهواره‌ای و کنترل در دستور کار سازمان‌های دفاعی قرار گرفته است. استفاده از این سامانه به‌طور بی‌سابقه‌ای، امکان دفاع موشکی بالستیک را برای ارتش آمریکا فراهم کرده است (غلام‌نژاد و همکاران، ۱۳۹۸: ۱۴۸-۱۴۵). حمله پهپادی ارتش آمریکا در سحرگاه جمعه ۱۳ آذرماه ۱۳۹۸ به خودرو حامل سپهبد قاسم سلیمانی و ابومهدی المهندس از فرماندهان بلند پایه ایران و عراق در فرودگاه بغداد(خبرگزاری جمهوری اسلامی، ۱۳۹۹) و حمله به خودرو محسن فخری‌زاده از دانشمندان هسته‌ای ایران در ۷ آذر ۱۳۹۹ با استفاده از فناوری هوش مصنوعی و اینترنت اشیاء صورت گرفت (سلطان‌زاده،۱۴۰۰).

جاسوسی سایبری: جاسوسی اینترنتی عموماً به کسب اطلاعات از طریق نصب نرم‌افزارها و ورود به رایانه شخصی افراد حین گردش آن‌ها در محیط وب تا زمانی که کاربر به شبکه جهانی وصل است اطلاق می‌شود. جاسوسی دیجیتال را از مهم‌ترین بزهکاری‌های عرصه دیجیتال عنوان می‌کنند. کشف اطلاعات دیگران و یا به‌کارگیری ابزارهای سایبری و ماهواره‌ای به‌منظور به دست آوردن اطلاعات عموماً با مقاصد مختلف انجام می‌شود (سیمبر،۱۳۹۴: ۸۷).

جرائم سایبری: جرائم اینترنتی می‌تواند نقض حق مالکیت معنوی، نقض حق اختراع، ربودن اسرار تجاری و غیره باشد. این جرائم، همچنین شامل حمله عمدی به رایانه‌ها به‌منظور مختل کردن آن‌ها و یا کپی از اطلاعات طبقه‌بندی شده می‌شود (خلیلی‌پور رکن‌آبادی و همکاران، ۱۳۹۱: ۱۷۳). جرائم یا تخلفات سایبری می‌تواند اشکال مختلفی از جمله موارد زیر را به خود اختصاص دهد:

بدافزارها:[۱] نوعی نرم‌افزار مخرب است که در آن می‌توان از هر فایل یا برنامه‌ای برای آسیب رساندن به کاربر رایانه مانند کرم‌ها، ویروس‌های رایانه‌ای، تروجان‌ها[۲] و نرم‌افزارهای

۱ Malware

۲ Trojan

جاسوسی[۱] استفاده کرد.

باج افزارها:[۲] نوعی بدافزار است که شامل یک مهاجم است که فایل‌های سیستم رایانه قربانی را قفل می‌کند. اختلال سایبری در شبکه سوخت آمریکا در دولت بایدن جدیدترین رویداد و نمونه از باج افزار است که با عنوان اولین چالش سایبری دولت بایدن خبرساز شد (رستم‌پور، ۱۴۰۰: ۲-۱).

فیشینگ:[۳] نوعی کلاهبرداری که در آن ایمیل‌های جعلی ارسال می‌شود که شبیه ایمیل از منابع معتبر است. با این حال، هدف از این ایمیل‌ها سرقت داده‌های حساس مانند کارت اعتباری یا اطلاعات ورود به سیستم است (پرهوده، ۱۳۹۸).

هکرها: اصطلاح «هک» به میانبر ایجاد شده در یک برنامه برای انجام سریع‌تر کار، اشاره می‌کند (دانشنامه رشد، ۱۳۹۹). هکرها کسانی هستند که سعی دارند به‌طور غیرقانونی به سایت‌های کامپیوتری دست یابند. از آزادی اینترنت سود برند، به مسائل خصوصی دست پیدا کنند، داده‌ها را تخریب و سیستم‌های کامپیوتری را تغییر دهند (خلیلی‌پور رکن‌آبادی و همکاران، ۱۳۹۱: ۱۷۴).

قدرت: قدرت به معنای توانایی، داشتن و توانستن است (معین، ۱۳۸۶: ۱۲۲۷) و در لاتین، معادل کلمه زور، برتری، نیرو و برگرفته از کلمه poss و معادل آن tobe able to است(نقبایی،۱۳۹۱: ۱۵۱۷). وبر قدرت را امکان تحمیل اراده خود بر رفتار دیگران تعریف می‌کند (راش، ۱۳۷۷: ۴۸). از نظر «نای» قدرت، قابلیت نفوذ در رفتار دیگران برای حصول نتایج دلخواه است (نای،۱۳۸۷: ۳۸). نای در تشریح قدرت نرم و لوازم اجرای آن از رسانه‌ها به‌عنوان مهم‌ترین ابزار قدرت برای «تضعیف کشور هدف»[۴] و دفاع از «منافع ملی»[۵] یاد

---

۱. Spyware

۲. Ransomware

۳. Phishing

۴. Target country

۵. National interest

می‌کند (نای، ۲۰۱۰).

قدرت سایبری: از دیدگاه دانیل کوهل (۲۰۰۹)، قدرت سایبری به معنای توانایی استفاده از فضای سایبر برای ایجاد برتری و تأثیرگذاری روی محیط‌های عملیاتی و از نظر نای (۲۰۱۱) مبتنی بر منابع اطلاعاتی فناوری‌های ارتباطی است. قدرت سایبری از مفاهیم نوظهور قدرت در سال‌های اخیر است. قدرت سایبری در بعد تهاجمی، برای تخریب زیرساخت‌های حیاتی و تأسیسات نظامی و هسته‌ای دشمن کاربرد دارد. در بعد تدافعی نیز نشان دهنده میزان آمادگی یک کشور در مقابله با بحران‌های سایبری و قدرت بازدارندگی است. این مفهوم در سطح کشور، اولین بار توسط امام خامنه‌ای(مدظله‌العالی) رهبری نظام جمهوری اسلامی ایران در حکم انتصاب اعضای شورای عالی فضای مجازی (در شهریور ۱۳۹۴) مورد توجه قرار گرفت. البته از نظر ایشان، قدرت سایبری باید همراه با برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای سایبر در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه باشد (هلیلی و همکاران، ۱۳۹۷: ۱۸۴ و ۱۷۵).

رابطه قدرت سایبری و امنیت ملی: فضای سایبر بستر مناسبی برای آزادی بیان، القای اندیشه‌ها و ایدئولوژی‌ها و اظهار وجود نهادها و سازمان‌های اجتماعی، اقوام و نژادها، ادیان و مذاهب و خرده فرهنگ‌ها است. امروزه در تمامی کشورها، علاوه بر توجه به منابع مادی قدرت سایبری (قدرت سخت)، رقابت و تلاش سرسختانه‌ای برای کسب و ترویج منابع غیرمادی قدرت از جمله فرهنگ، آرمان‌ها، ارزش‌های سیاسی (قدرت نرم) در حال انجام است که پیامدهای این اقدامات در قالب قدرت سایبری تجلی یافته است. فضای سایبر نوع جدیدی از تهدیدات، متفاوت با تهدیدات سنتی علیه امنیت ملی را به وجود آورده است. جرائم سایبری، جاسوسی سایبری، تروریسم سایبری و جنگ سایبری تهدیداتی هستند که منافع ملی کشورها را با چالش جدی روبرو ساخته است (هلیلی و همکاران،۱۳۹۷: ۱۸۶-۱۸۳).

۳-۱. چارچوب نظری پژوهش

فناوری‌های نوین با رسوخ به حوزه میان واحدهای نظام بین‌المللی به‌ویژه در بعد تهدیدها، جنگ‌ها و منازعات، بر پویش‌های جاری در درون و میان جوامع تأثیر نهاده‌اند. استفن والت در چارچوب مکتب واقع‌گرایی ادعا می‌کند که مطالعات امنیتی بایستی بر قدرت‌های نظامی که تحت کنترل سیاسی بازیگران دولتی اداره می‌شوند، تمرکز کند؛ بنابراین دستیابی به فناوری‌های نوین می‌تواند توزیع قدرت به‌ویژه قدرت نظامی در نظام بین‌الملل را تغییر دهد و شیوه‌های نوین منازعه و جنگ میان دولت‌ها را پدید آورد(نورمحمدی و طالبی آرانی، ۱۳۹۵: ۱۷۴-۱۷۱). واقع‌گرایان در برخی موارد تأثیر پیشرفت‌های فناورانه بر تعاملات میان دولت‌ها را می‌پذیرند و اعتقاد دارند، آنارشی بین‌المللی و فناوری‌های غالب دو شرط اساسی هستند که دولت‌ها مجبورند در بستر آن‌ها راهبردها را دنبال کنند (بوزان، ۱۹۸۷: ۷-۶).

از نظر مکتب کپنهاگ، دولت‌ها اگرچه در مطالعات امنیتی نقش محوری دارند، اما عرصه فضای سایبر به‌گونه‌ای است که بازیگران مختلف شامل: شرکت‌ها، دولت‌ها و اجتماعات را دربرمی‌گیرد. از نظر این مکتب، مسائل و تهدیدات امنیتی در زمینه‌های مختلف حتی اگر در سطح بازیگران فردی اجرا شود مهم هستند (هر[۱] ۲۰۱۰: ۲۱۴). از منظر لیبرالیست‌ها، دولت‌ها تنها کنشگران روابط بین‌الملل نیستند و به خاطر دگرگونی در سیاست بین‌الملل بستر مناسب برای ظهور شرکت‌های چند ملیتی، جنبش‌های اجتماعی، گروه‌های نفوذ و تروریست‌ها در نظام جهانی فراهم شده است. روزنا معتقد است تغییرات فناورانه زیربنای اصلی تغییرات گسترده و عمیق در نظام جهانی را تشکیل می‌دهد و ظهور موضوعات جهان گستر، قاچاق مواد مخدر و کاهش کارایی دولت ناشی از همین اثرگذاری است (روزنا، ۱۳۸۴: ۳۶۹-۳۵۷). مطالعه رفتار لیبرال‌ها در صحنه جهانی نشان می‌دهد فناوری‌های نوین صرفاً ابزار همکاری، دموکراتیک‌سازی و صلح نیستند، بلکه می‌توانند ابزار فریب، تبلیغ و ترور نیز باشند (نورمحمدی و طالبی آرانی، ۱۳۹۵: ۱۸۰-۱۷۸).

---

۱. Hare

سازه انگاران نظریه‌های واقع‌گرایی و لیبرالیستی را رویکردهایی مادی‌گرایانه تلقی می‌کنند. به اعتقاد ونت این دیدگاه‌ها می‌کوشند با ارجاع به نیروهای مادی صرف، مانند: سرشت بشر، محیط فیزیکی و مصنوعات فناورانه، تأثیرات قدرت، منافع، یا نهادها را توضیح دهند (ونت[1] ۱۳۸۴: ۱۶۲). یکی از رویکردهای سازه‌انگارانه، نظریه امنیتی ساختن است. امنیتی ساختن به این معنا است که یک تهدید امنیتی شناسایی می‌شود و از طریق کنش کلامی، آن موضوع در دستور کار سیاسی قرار می‌گیرد و به استفاده از زور، پنهان‌کاری و تجاوز به حریم خصوصی مشروعیت می‌بخشد (نورمحمدی و طالبی آرانی، ۱۳۹۵: ۱۸۲). در مجموع سازه‌انگاران اعتقاد دارند، فناوری به‌عنوان یک ساختار مادی بر فرایندهای سیاسی اجتماعی و اقتصادی تأثیر می‌گذارد اما این تغییرات نه فقط به فناوری بلکه به بافت اجتماعی هم بستگی دارد.

۴-۱. فرضیه‌های پژوهش

اصلی اول: فناوری‌های ارتباطی و اطلاعاتی در گسترش قدرت نقش دارد.

فرعی اول: فناوری‌های ارتباطی و اطلاعاتی در گسترش تهدیدات امنیتی نقش دارد.

فرعی دوم: فناوری‌های ارتباطی و اطلاعاتی در گسترش تهدیدات امنیتی علیه منافع جمهوری اسلامی ایران نقش دارد.

اصلی دوم: فناوری‌های ارتباطی و اطلاعاتی در ظهور بازیگران جدید نقش دارد.

فرعی اول: فناوری‌های ارتباطی و اطلاعاتی در ظهور تهدیدگران امنیتی در عرصه بین‌الملل نقش دارد.

فرعی دوم: فناوری‌های ارتباطی در ظهور سازمان‌های تروریستی در عرصه بین‌الملل نقش دارد.

---

۱. Wendt

۲. روش‌شناسی تحقیق

روش انجام این پژوهش پیمایشی است و هدف آن اکتشاف سازه‌های موضوع یعنی ابعاد، مؤلفه‌ها و شاخص‌ها است که با استفاده از روش توصیفی- تحلیلی صورت گرفته، همچنین برای دستیابی به نتایج موردنظر از مطالعات کتابخانه‌ای برای تکمیل ادبیات تحقیق و پرسش‌نامه محقق ساخته برای گردآوری اطلاعات بهره‌گیری شده است. جامعه آماری تحقیق؛ متشکل از اساتید دانشگاه، دانشجویان و کارشناسان رسانه است. با توجه به واحد سطح تحلیل، از میان استان‌های ۳۲ گانه کشور ۱۶ استان مشخص شد و حجم نمونه به روش نمونه‌گیری خوشه‌ای سهمیه‌ای براساس فرمول کوکران، ۳۸۴ نفر برآورد گردید و در راستای افزایش ضریب دقت، تعداد نمونه‌ها به ۴۰۲ نفر افزایش یافت. نمونه‌ها نیز از طریق روش نمونه‌گیری غیر احتمالی قضاوتی در دسترس انتخاب شدند. برای تجزیه و تحلیل یافته‌ها، از آماره‌های توصیفی (فراوانی، درصد، میانگین، انحراف معیار، واریانس) و از آماره رگرسیون چند متغیره و تحلیل عاملی برای فرضیه‌های اصلی و فرعی استفاده گردید. برای تعیین نقش متغیر مستقل، فناوری‌های اطلاعاتی و ارتباطی با ابعاد (ماهواره، اینترنت، فضای مجازی، شبکه‌های اجتماعی تحت وب و موبایلی و روزنامه‌نگاری الکترونیک) بر متغیر وابسته تحقیق؛ گسترش تهدیدات امنیتی و تروریسم و ظهور بازیگران جدید در عرصه بین‌الملل سعی گردید با استفاده از گویه‌های سنجش، میزان رابطه متغیرها محاسبه شود. در این پژوهش مطابق نظر لیبیسکی (۲۰۰۹) فضای سایبر به‌عنوان یک کل و اینترنت، فضای مجازی، شبکه‌های اجتماعی و روزنامه‌نگاری سایبر به‌عنوان اجزاء آن مورد توجه قرار گرفته و امکان سنجش و مقایسه تمامی ابعاد فناوری‌های ارتباطی و اطلاعاتی به‌طور هم‌زمان فراهم گردید. هدف از این اقدام ایجاد زمینه برای شناخت ظرفیت و قدرت نقش‌آفرینی هریک از این ابزارها در پدیده‌های پیرامونی است که برآیند آن می‌تواند در تصمیم‌گیری‌های راهبردی مسئولان کشور در مواجهه با جنبه‌های متفاوت تهدیدات سایبری تاثیرگذار باشد.

۳. تجزیه و تحلیل یافته‌ها

الف. یافته‌های توصیفی

تحقیق حاضر در پی شناخت نقش فناوری‌های ارتباطی و اطلاعاتی در گسترش تهدیدات امنیتی در عرصه بین‌المللی است. نتایج حاصل از توصیف ویژگی‌های نمونه مطالعه نشان داد، بیشتر پاسخگویان (۶۰/۲ درصد) از نظر جنسیت، مرد هستند. ۶۰/۷ درصد پاسخگویان در گروه سنی ۴۹-۳۰ سال قرار دارند. ۶۱/۴ درصد از پاسخگویان به لحاظ میزان تحصیلات، دارای مدرک تحصیلی فوق لیسانس هستند. اکثریت نسبی پاسخگویان، رشته تحصیلی خویش را علوم ارتباطات (۱۸/۹ درصد) و خبرنگاری (۱۸/۴ درصد) عنوان کردند. با توجه به سطح آماری تحلیل (۱۶ استان) بیشتر پاسخگویان ساکن استان‌های تهران (۴۶/۸ درصد)، گیلان (۹ درصد)، هرمزگان (۸/۵ درصد) و قزوین (۶/۵ درصد) بودند. نتایج آماره‌های توصیفی درباره نقش فن‌آوری‌های ارتباطی و اطلاعاتی بر متغیرهای گسترش تهدیدات امنیتی و تروریستی در سطوح جهانی بر میانگین پاسخ‌ها در حد متوسط به بالا (زیاد) دلالت دارد. در عین حال پایین‌ترین میانگین به ترتیب با (۳/۴۳) و (۳/۲۲) متعلق به روزنامه‌نگاری سایبری و بالاترین آن مربوط به فضای مجازی (۳/۸۸) و (۳/۸۴) است.

ب. یافته‌های استنباطی

در این پژوهش، آزمون فرضیه‌های اصلی تحقیق با استفاده از رگرسیون چند متغیره به روش همگانی بررسی شد و میزان تأثیر هر یک از ابعاد متغیر مستقل (فن‌آوری‌های ارتباطی و اطلاعاتی) بر تغییرات متغیر وابسته (گسترش قدرت و ظهور بازیگران جدید در عرصه بین‌الملل) مورد تجزیه و تحلیل قرار گرفت. بررسی داده‌ها نشان داد، ضریب رگرسیون چند متغیره به مقدار R = 0.531 بیش از ۹۹ درصد، (F = 88.617، Sig = 0.000) معنی‌دار است. ضریب تعیین به‌دست‌آمده R2 =0.525 است و بدین معنا می‌باشد که بیش از ۵۵ درصد از کل واریانس گسترش قدرت با متغیر فن‌آوری‌های نوین ارتباطی قابل پیش‌بینی می‌باشد و حدود ۴۵ درصد دیگر نیز به سایر متغیرها وابسته می‌باشد؛ اما در

خصوص مؤلفه ظهور بازیگران جدید، مقدار R=0.260 در سطح ۹۹ درصد، (F=27.585، Sig=0.000) معنی‌دار است. ضریب تعیین به‌دست‌آمده R2=0.251 بوده و بیش از ۲۵ درصد از کل واریانس ظهور بازیگران جدید در عرصه بین‌المللی از طریق فن‌آوری‌های نوین ارتباطی قابل پیش‌بینی می‌باشد و حدود ۷۵ درصد دیگر نیز به سایر متغیرها وابسته است.

به‌منظور بررسی فرضیه‌های فرعی تحقیق از روش تحلیل عاملی استفاده شد. آزمون تحلیل عاملی از چهار مرحله و چهار جدول تشکیل شده است که مهم‌ترین و کاربردی‌ترین بخش آن جدول ماتریس اجزاء یا ماتریس چرخشی است. به جهت پرهیز از طولانی شدن مطلب صرفاً جدول ماتریس چرخشی اجزاء برای مؤلفه تهدیدات امنیتی ارائه می‌شود.

نتایج تحلیل عاملی برای فرضیه فرعی اول به شناسایی تمامی ابعاد مورد بررسی و نقش‌آفرینی آن‌ها در گسترش تهدیدات امنیتی در عرصه بین‌الملل منجر شد. بر اساس یافته‌ها، اینترنت و فضای مجازی بیشترین سهم را در ایجاد تهدیدات امنیتی در عرصه بین‌المللی دارند؛ بنابراین نتایج، مبین تأیید فرضیه فرعی پژوهش است. همچنین استفاده از فضای سایبر در افزایش قدرت سخت و نرم جمهوری اسلامی ایران برای مقابله با تهدیدات امنیتی در سطح بین‌الملل نقش دارد.

جدول ۱. ماتریس عاملی نقش فناوری‌های ارتباطی و اطلاعاتی در گسترش تهدیدات امنیتی در عرصه بین‌الملل

گویه‌های سنجش	عامل‌های تحلیل: ۱. اینترنت و روزنامه‌نگاری سایبری ۲. شبکه‌های ماهواره‌ای (عام)۳. شبکه‌های اجتماعی تحت وب و موبایل ۴. شبکه‌های ماهواره‌ای، فضای مجازی، شبکه‌های اجتماعی، روزنامه‌نگاری سایبری و اینترنت (دولت ایران)۵. فضای مجازی ۶. روزنامه‌نگاری سایبری ۷. دسترسی آزاد به ماهواره و فضای سایبر (خاص)۸. فضای مجازی (خاص)							
	۱	۲	۳	۴	۵	۶	۷	۸
۱. ماهواره‌ها ابزارهای مهم جنگ نرم هستند	.۲۶۱	.۸۳۴	.۰۶۹	.۰۲۳	-.۰۳۱	.۰۷۴	-.۰۱۳	.۱۰۱
۲. ماهواره ابزار جنگ تبلیغاتی و روانی و تبلیغات است.	.۰۸۰	.۸۶۲	.۱۹۰	.۰۵۴	.۱۵۵	.۰۸۰	.۰۸۵	.۱۱۲

گویه‌های سنجش	عامل‌های تحلیل							
	۱. اینترنت و روزنامه‌نگاری سایبری ۲. شبکه‌های ماهواره‌ای (عام)۳. شبکه‌های اجتماعی تحت وب و موبایل ۴. شبکه‌های ماهواره‌ای، فضای مجازی، شبکه‌های اجتماعی، روزنامه‌نگاری سایبری و اینترنت (دولت ایران)۵. فضای مجازی ۶. روزنامه‌نگاری سایبری ۷. دسترسی آزاد به ماهواره و فضای سایبر (خاص)۸. فضای مجازی (خاص)							
	۱	۲	۳	۴	۵	۶	۷	۸
۳. بستر کم‌هزینه و فراگیر برای جنگ نرم است.	.۱۴۰	.۸۳۰	.۱۷۲	.۰۲۶	.۱۹۷	.۰۹۱	.۰۸۷	.۰۶۱
۴. سازمان‌ها و دولت‌ها برای تهدید استفاده می‌کنند	.۰۲۵	.۷۴۸	.۲۶۴	.۱۸۰	.۲۱۴	.۰۹۶	.۱۳۳	-.۱۰۰
۵. همگرایی از ماهواره ابزاری مخرب ساخته است.	.۱۳۶	.۶۸۲	.۲۴۷	.۱۴۶	.۳۶۰	-.۰۴۸	.۰۷۷	-.۱۸۸
۶. ابزار تهدید و تهاجم علیه کشورها است.	.۰۳۱	.۰۷۸	-.۰۳۱	.۰۱۰	-.۰۴۱	-.۰۷۲	.۹۲۰	-.۱۰۰
۷. قدرت نرم ایران را در سطح جهان افزایش می‌دهد	.۱۲۸	.۲۲۴	.۱۲۶	.۷۰۶	.۱۶۰	-.۰۲۶	.۰۶۲	-.۲۹۱
۸. ابزار مورد استفاده ایران برای مقابله با تهدید است	.۰۵۶	.۰۲۵	.۰۶۳	.۸۲۰	.۰۱۷	.۱۱۴	.۰۲۶	-.۰۴۲
۹. بستری کم‌هزینه و فراگیر برای جنگ نرم است.	.۲۱۴	.۴۷۹	.۰۹۹	.۰۶۸	.۳۱۲	.۱۹۸	.۰۹۰	.۵۷۲
۱۰. امکان تهدید از هر نقطه جهان را فراهم می‌کند.	.۱۴۳	.۴۷۵	.۱۵۸	.۰۴۶	.۴۷۵	.۲۷۳	.۱۹۰	.۳۸۷
۱۱. بهترین گزینه برای تخریب زیرساخت حیاتی است.	.۲۶۰	.۳۱۰	.۱۸۸	.۰۷۵	.۷۳۹	.۱۳۹	.۰۹۰	.۱۰۱
۱۲. دسترسی به اطلاعات از تهدیدات فضای سایبر است.	.۰۸۷	.۲۲۱	.۰۷۸	.۰۰۰	.۲۹۳	.۰۶۱	.۸۴۲	.۱۷۳
۱۳. صحنه اساسی تهدیدات آینده کشورها است.	.۲۴۵	.۳۷۳	.۱۶۸	.۱۶۰	.۷۴۲	.۱۲۳	.۰۷۸	.۰۷۱
۱۴. سازمان‌ها و دولت‌ها برای تهدید استفاده می‌کنند.	.۲۸۶	.۳۴۵	.۲۴۷	.۱۷۸	.۶۶۲	.۰۸۰	.۰۷۳	.۰۵۷
۱۵. قدرت نرم ایران را در سطح جهان افزایش می‌دهد.	.۱۸۸	.۱۱۲	.۱۴۲	.۶۹۷	.۴۱۰	-.۰۸۶	-.۰۶۱	-.۱۸۵
۱۶. ابزار مورد استفاده ایران علیه مقابله با تهدید است	.۰۶۶	.۰۸۳	.۰۳۷	.۷۸۶	.۱۴۴	.۰۰۱	.۰۷۳	.۲۳۲
۱۷. فیس‌بوک، توییتر و... ابزار کنترل شهروندان است.	.۳۰۸	.۰۸۷	.۶۰۲	.۰۳۲	.۱۸۴	.۰۱۸	-.۰۳۳	-.۱۳۵
۱۸. قدرت افراد و گروه‌ها را برابر دولت‌ها افزایش می‌دهد	.۲۹۶	.۲۱۱	.۵۵۸	.۱۲۵	.۱۴۹	.۰۹۷	.۱۲۹	.۲۹۴
۱۹. در تغییر اوضاع سیاسی کشورها اثرگذار است	.۲۹۵	.۲۲۸	.۶۳۲	.۰۹۱	.۱۹۱	.۲۹۹	.۰۰۱	.۰۶۹
۲۰. ابزار سازمان‌ها و دولت‌ها برای تهدید است	.۳۲۱	.۲۵۱	.۷۰۱	.۲۳۸	.۰۲۵	.۱۰۵	.۰۵۰	.۰۲۴
۲۱. ابزار جمع‌آوری اطلاعات برای امور نظامی است.	.۳۴۸	.۱۵۴	.۶۷۱	.۲۸۳	.۱۷۷	.۰۸۲	-.۰۸۰	.۰۰۳
۲۲. بستری کم‌هزینه و فراگیر برای جنگ نرم است.	.۲۵۳	.۳۲۲	.۵۹۳	-.۰۰۲	.۰۵۶	.۳۰۶	.۰۹۴	.۳۴۳
۲۳. فیس‌بوک، توییتر، ابزار کنترل شهروندان است	.۲۸۳	.۱۶۹	.۶۵۰	.۰۷۰	.۱۱۱	.۱۱۰	.۰۱۱	.۰۱۶
۲۴. ایران حضور مؤثر در شبکه‌های اجتماعی جهانی دارد.	-.۰۲۱	-.۰۱۰	.۳۹۴	.۶۳۹	-.۱۱۵	.۰۲۳	-.۰۵۳	.۱۴۷
۲۵. اینترنت ماهیت قدرت تغییر داده است	.۲۹۹	.۲۵۲	.۲۴۳	.۱۰۴	.۱۱۲	.۵۷۲	.۰۱۴	.۱۳۷
۲۶. دولت‌ها تهدید خود را از این طریق اعمال می‌کنند.	.۰۹۰	-.۰۳۱	.۱۷۴	-.۰۳۵	.۱۳۲	.۵۵۷	-.۰۵۴	.۰۰۰
۲۷. سایت و وبلاگ ابزار جمع‌آوری اطلاعات است	.۵۷۷	.۲۹۸	.۲۱۶	.۰۰۷	.۰۲۹	.۴۷۳	.۰۱۲	.۱۰۹

گویه‌های سنجش	عامل‌های تحلیل							
	۱. اینترنت و روزنامه‌نگاری سایبری ۲. شبکه‌های ماهواره‌ای (عام)۳. شبکه‌های اجتماعی تحت وب و موبایل ۴. شبکه‌های ماهواره‌ای، فضای مجازی، شبکه‌های اجتماعی، روزنامه‌نگاری سایبری و اینترنت (دولت ایران)۵. فضای مجازی ۶. روزنامه‌نگاری سایبری ۷. دسترسی آزاد به ماهواره و فضای سایبر (خاص)۸. فضای مجازی (خاص)							
	۱	۲	۳	۴	۵	۶	۷	۸
۲۸. در تغییر اوضاع سیاسی کشورها نقش دارند.	.۵۶۳	.۱۹۰	.۳۳۳	.۱۱۸	.۱۷۱	.۳۶۶	.۰۴۰	.۰۲۴
۲۹. سایت‌ها و وبلاگ‌ها ابزار ایران در جنگ نرم هستند	.۱۷۲	.۱۵۱	-.۰۶۴	.۳۲۸	-.۲۸۱	.۲۰۲	-.۰۴۸	-.۰۴۳
۳۰. ابزار مهم جمع‌آوری اطلاعات از شهروندان است	.۴۷۰	.۱۷۷	.۲۱۵	.۲۰۳	-.۰۵۸	.۴۳۱	-.۰۱۲	.۰۲۱
۳۱. اینترنت ماهیت قدرت را تغییر داده است	.۷۰۳	.۲۶۴	.۱۸۹	-.۰۰۵	.۱۰۶	.۳۰۲	-.۰۵۹	.۰۷۷
۳۲. ابزار سازمان‌ها و دولت‌ها برای اعمال تهدید است	.۷۵۲	.۱۵۸	.۲۵۹	.۱۱۴	.۱۱۶	.۱۲۵	.۰۷۹	-.۰۸۱
۳۳. سایت‌ها و بلاگ‌ها ابزار جمع‌آوری اطلاعات هستند	.۷۸۱	.۱۱۹	.۱۹۰	.۰۷۰	.۲۱۹	.۱۶۷	-.۰۰۳	-.۱۳۸
۳۴. در تغییر اوضاع سیاسی کشورها نقش دارند	.۸۱۰	.۰۶۳	.۲۲۱	.۱۰۴	.۲۰۷	.۱۷۵	.۰۴۲	-.۱۳۰
۳۵. ابزار مهم جمع‌آوری اطلاعات از شهروندان است.	.۸۷۶	.۰۹۹	.۱۵۷	.۰۹۵	.۱۶۸	.۰۹۷	.۰۰۲	-.۰۲۰
۳۶. در گسترش تهدید در فضای مجازی نقش دارد	.۱۸۸	.۰۶۸	-.۱۲۰	-.۰۰۱	-.۰۸۵	.۴۵۹	.۰۸۵	-.۴۴۷
۳۷. سلاح مهم اجرای عملیات روانی در جنگ نرم است	.۷۸۰	.۰۴۵	.۲۱۵	.۱۲۸	.۰۷۰	-.۰۵۵	.۰۹۴	.۱۸۷
۳۸. ابزار مناسب کنترل افکار عمومی است.	.۸۰۱	.۰۸۰	.۲۶۳	.۱۱۶	-.۰۲۴	.۰۱۵	.۰۵۷	.۱۳۰
۳۹. برای اقناع و تغییر نگرش افکار عمومی کاربرد دارد.	.۵۲۱	-.۱۱۶	.۰۷۵	.۶۲۴	-.۰۳۸	-.۰۵۲	-.۰۶۷	.۲۲۷

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
(برجعلی زاده، ۱۳۹۹: ۲۰۲)

در این پژوهش، پدیده تروریسم به‌عنوان یکی از ابعاد مهم تهدید سایبری بررسی شد. نتایج تحلیل عاملی نشان داد؛ تمامی ابعاد فناوری‌های ارتباطی و اطلاعاتی در ظهور گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه بین‌الملل نقش دارد اما بیشترین نقش به عامل فضای مجازی اختصاص دارد. یافته‌ها در خصوص ابعاد تهدیدزای فضای سایبر علیه جمهوری اسلامی ایران نشان داد؛ فناوری پخش برنامه‌های ماهواره، فضای مجازی و روزنامه‌نگاری سایبر به ترتیب ابزارهای مورد استفاده گروه‌های تروریستی برای

تهدید علیه امنیت ملی جمهوری اسلامی ایران است. ایران نیز با استفاده از فضای سایبر (شبکه‌های ماهواره‌ای، فضای مجازی، شبکه‌های اجتماعی و اینترنت) با ابعاد تهدیدآمیز تروریسم در سطح بین‌الملل مقابله می‌کند. از نظر پاسخگویان گروه‌های تروریستی در استفاده از ابزار روزنامه‌نگاری سایبر در صحنه بین‌المللی از جمهوری اسلامی ایران موفق‌تر عمل کرده‌اند.

۴. نتیجه‌گیری

در انطباق یافته‌های پژوهش حاضر با نتایج مطالعات پیشین و چارچوب نظری، مفروضات تحقیق مبنی بر نقش فناوری‌های نوین ارتباطی با پنج بعد ماهواره، اینترنت، فضای مجازی، شبکه‌های اجتماعی و روزنامه‌نگاری سایبر در گسترش قدرت و ظهور بازیگران جدید در عرصه بین‌الملل با محوریت تهدیدات امنیتی و تروریسم به‌درستی تبیین گردید. تجزیه و تحلیل داده‌ها نشان داد، فناوری‌های مدرن دارای ظرفیت جابجایی و گسترش قدرت هستند. آن‌ها این کارکرد را نخست از فضای حقیقی به فضای مجازی از طریق انتقال فعالیت‌های جامعه بشری به درون فضای بیکران جامعه شبکه‌ای محقق می‌سازند. دوم از طریق تأثیر بر عناصر تشکیل دهنده قدرت در جهان معاصر مانند دولت‌ها، سازمان‌های مافیایی و تروریستی، گروه‌ها، افراد و... به طرح انتقال قدرت کمک می‌کنند.

این یافته‌ها اگرچه نقش فناوری‌های نوین ارتباطی بر عناصر قدرت را مورد تأکید قرار داده‌اند اما این نکته را نیز آشکار ساخته که فناوری‌های مورد بررسی اگرچه دسترسی همگان به قدرت را تسهیل می‌کنند اما میزان تأثیرگذاری آن‌ها نسبت به یکدیگر کاملاً متفاوت بوده و این اثرگذاری با شرایط پیرامونی رابطه مستقیم داشته و ممکن است در جوامع مختلف صور و نتایج متفاوتی داشته باشد. یافته‌های پژوهش حاضر نیز با برجسته کردن نقش اینترنت و فضای مجازی در گسترش تهدیدات سایبری و تروریسم در جهان، مشخص کرد در وضعیت معاصر نظام بین‌الملل کدام‌یک از ابزارهای نوین فناوری ارتباطات و اطلاعات بیشترین نقش را در تغییرات و تحولات پدیده‌های امنیتی دارند. نتایج نشان داد جغرافیای امنیتی جمهوری اسلامی ایران نیز به‌عنوان کشوری مستقل، در حال

توسعه و تأثیرگذار در منطقه به‌شدت تحت تأثیر فضای سایبر با محوریت فضای مجازی است. در زمینه گسترش فعالیت کنشگران باید اذعان کرد؛ تمرکززدایی قدرت و اقتدار از دولت‌ها، نمادهای آشکاری از تغییرات در سیاست‌های جهانی است. یافته‌های پژوهش، مؤید برآیند این تغییرات و ظهور کنشگران جدید در حوزه بین‌الملل است. اگرچه نای (۱۳۹۸) بر این نکته تأکید داشت که فناوری اطلاعات فرصتی بی‌نظیر برای غرب، به‌ویژه ایالات متحده فراهم ساخته تا جهان را مطابق نظم مورد نظر اداره نماید اما بررسی‌ها نشان می‌دهد، فضای سایبر با فراهم ساختن امکان دسترسی دیگر دولت‌ها، سازمان‌ها، گروه‌ها و افراد، امکان مدیریت یکپارچه بر شبکه‌های جهانی را با چالش مواجه کرده است. مطالعات آدمی، نکویی (۱۳۹۷)، ذوالفقاری و کیانژاد (۱۳۹۷)، نیز رسانه‌های نوین را ابزار توسعه سازمان‌ها از جمله گروه‌های تروریستی عنوان می‌کند که از رسانه‌ها به نحوی مؤثر برای اشاعه ترس، تبلیغ ارزش‌ها و اقدامات ضد بشری بهره می‌گیرند. در بین رویکردهای جهانی، پارادایم لیبرالیستی قدرت از به‌کارگیری فناوری سایبر برای تکامل قدرت نظامی و اقتصادی و توسعه ارتباطات دمکراتیک به‌شدت حمایت می‌کند. آن‌ها ضمن پذیرش اصل کنشگری جهانی برای افراد، سازمان‌ها، شرکت‌ها و گروه‌های سازمان یافته جنایی و تروریستی، بر توسعه ساختارهای امنیتی فضای سایبر با همکاری دولت‌ها و سازمان‌های خصوصی تأکید می‌نمایند. مطالعه حاضر ضمن تعیین نقش فضای سایبر در تغییر پدیده‌های پیرامونی نشان داد، الگوی تأثیرپذیری سطوح ملی، منطقه‌ای و بین‌المللی در فضای سایبر یکسان نیست. درحالی که اینترنت و فضای مجازی در گسترش تهدیدات امنیتی در عرصه جهانی نقش دارد، امنیت ملی جمهوری اسلامی ایران متأثر از تمامی ابعاد فضای سایبر است. درباره‌ی مؤلفه نقش فناوری‌های ارتباطی و اطلاعاتی در ابعاد جهانی، نای (۱۳۹۸)، پراکندگی قدرت را زمینه‌ساز ظهور بازیگران جدید می‌داند. روزنا (۱۳۹۵)، آن را تسهیل کننده ظهور قدرت‌ها و حاکمیت‌های جدید می‌داند اما آلبرتس و پاپ (۱۳۸۷)، پیشرفت سلطه اطلاعاتی، جنگ‌های اطلاعاتی، جنگ‌های روانی، جنگ‌های الکترونیکی و جنگ‌های رخنه‌گری (هک) را نتیجه توسعه فناوری اطلاعات در قرن ۲۱

عنوان می‌کنند. در این زمینه بررسی‌های میدانی صیاد، رامک و منفرد (۱۳۹۹) نشان می‌دهد، قدرت‌های مسلط جهانی علی‌الخصوص آمریکا، حفظ و توسعه منافع ملی و بین‌المللی خود را از طریق گسترش تهدید، جنگ و ناامنی علیه کشورهای رقیب دنبال می‌کند. در خاورمیانه، محور مقاومت و به‌طور خاص جمهوری اسلامی ایران در کانون تهدیدات آمریکا و رژیم صهیونیستی و عربستان سعودی، دو هم پیمان راهبردی آمریکا قرار دارند. یافته‌های ذوالفقاری و کیانژاد (۱۳۹۷)، آدمی و نکویی (۱۳۹۷) و نجفی و علمی (۱۳۹۱)، حاکی است، سازمان‌های تروریستی با بهره‌برداری از فضای مجازی و شبکه‌های اجتماعی، نه تنها مراحل تبلیغ، عضوگیری، آموزش افراد و فعالیت‌های خود را جهانی ساخته‌اند، بلکه بر افزایش جرائم سازمان یافته سایبری در ج.ا.ایران، نیز تأثیر گذاشته‌اند.

شایان ذکر است، استفاده از فنّاوری به‌طور همزمان در قالب دو روی سکه‌ی جنگ و صلح، همواره سنت تاریخی غرب بوده است. نظام سلطه از ظرفیت‌های فضای سایبر علاوه بر تقویت بنیان‌های اقتصادی و توسعه دمکراسی کشورها، سیاست فریب، تبلیغ، جنگ و ترور را در دستور کار خود قرار داده است. در این زمینه می‌توان به مطالعات سازه‌انگارانه الکساندر ونت اشاره کرد. ونت معتقد بود، حکومت‌های لیبرالیستی به‌ویژه آمریکا با استفاده از ظرفیت رسانه‌های نوین و امنیتی کردن مسائل سیاسی تلاش می‌کنند، اقدامات غیرقانونی و اخلاقی مانند پنهان‌کاری، سانسور، سرقت اطلاعات و تجاوز به حریم خصوصی دیگران را تحت برنامه‌ها و اقدامات توسعه‌طلبانه مشروعیت ببخشند.

نکته: در مواجهه با تهدیدات بین‌المللی، شناخت گفتمان دوگانه غرب درباره‌ی فناوری‌های اطلاعاتی از اهمیت زیادی برخوردار است. فضای سایبر فضای امنیت و تهدید است. برای مقابله با تهدیدات این فضا، برخورداری از مدیریتی نظام‌مند، یکپارچه و هوشمند ضروری است. برنامه‌ریزی برای بهره‌برداری از این فناوری باید جامع و ساختارمند باشد. برای حفظ امنیت ملی، توجه به راهبر چهارگانه؛ توسعه دائمی طرح‌های پدافند غیرعامل- شناسایی پدیده‌ها و منابع تهدیدآمیز، - ترسیم آرایش دفاعی و خنثی کردن تهدیدات و راهبرد تهاجم از طریق رخنه و انهدام منابع تهدید ضروری است.

شناخت ویژگی‌ها، ظرفیت‌ها و آثار متفاوت اجزاء فضای سایبر و رابطه آن با پدیده‌های پیرامون در موفقیت اجرای برنامه‌های راهبردی و طرح‌های تاکتیکی بسیار تعیین کننده است. در این راستا، ۱. تمرکز زیرساخت‌های حیاتی فضای سایبر در مناطق مختلف و امن کشور ۲. مدیریت یکپارچه ۳. سیاست‌گذاری ۴. طراحی و برنامه‌ریزی منطبق با واقعیت‌های میدانی در ابعاد داخلی و بین‌المللی ۵. تعامل با صاحبان فنّاوری‌های نوین در جهان برای محقق ساختن اهداف توسعه در بخش‌های سیاسی، فرهنگی، اجتماعی، اقتصادی، صنعتی و نظامی توصیه می‌شود.

پیشنهاد

تغییرات و تحولات بی‌وقفه در ماهیت فناوری ارتباطات و اطلاعات و تأثیرگذاری آن بر تحولات جهانی، مؤلفه‌هایی هستند که در میزان موفقیت هر دولتی برای دستیابی به اهداف راهبردی نقش حیاتی دارند. در این راستا پیشنهاد می‌شود:

۱. وزارت ارتباطات و فناوری اطلاعات برای تکمیل و توسعه زیرساخت‌های اینترنتی مبتنی بر فناوری بومی، برای مبارزه کامل با تهدیداتی که حوزه‌های سیاسی و فرهنگی نظام جمهوری اسلامی را نشانه گرفته است، اقدام نماید.

۲. برای مبارزه فراگیر با ابعاد سیاسی و فرهنگی تروریسم در نظام جهانی از طریق وزارت ارتباطات و فناوری اطلاعات برای تکمیل زیرساخت‌های سایبری، فعالیت فراگیر رسانه‌ها و انتشار جهانی نشریه‌ها و روزنامه‌های الکترونی اقدامات لازم صورت پذیرد.

۳. سرعت بخشیدن به روند توسعه زیرساخت‌های فنی مقابله با حملات تروریستی در فضای سایبر از طریق وزارت ارتباطات و فناوری اطلاعات.

۲. وزارت علوم و تحقیقات با همکاری وزارت دفاع برای تقویت برنامه‌های پژوهش محور با رویکرد آینده‌پژوهی با هدف پیش‌بینی تحولات دائمی فناوری‌های نوین ارتباطی و اطلاعاتی در حوزه‌های مختلف به‌ویژه تهدیدات امنیتی برنامه‌ریزی نماید.

۳. از طریق وزارت امور خارجه برای استفاده گسترده از ظرفیت عظیم دیپلماسی نوین

رسانه‌ای برای دفاع از منافع ملی کشور کارسازی شود.

۴. وزارت امور خارجه با استفاده از ماده ۵۱ حقوق بین‌الملل که دفاع مشروع کشورها در موقعیت تجاوزات خارجی را محترم می‌شمارد با همکاری جمعی سایر کشورها کار مقابله با گسترش تهدیدات سایبری از طریق سازمان‌های منطقه‌ای و سازمان ملل متحد را پیگیری نماید.

۵. با توجه به رشد جنبه‌های متفاوت تروریسم در فضای سایبر مانند تروریسم هویت، مذهبی و ایدئولوژیک، نسل‌کشی، ترور دانشمندان، رهبران سیاسی و مقامات کشورها ضرورت دارد سازمان پدافند غیرعامل با همکاری رسانه‌ها و شهرداری‌ها برای آموزش و آگاهی شهروندان اقدام نمایند.

۶. بررسی بنیادی و سیستماتیک نقش فناوری‌های نوین ارتباطی در تغییرات و تحولات منطقه از سوی مراکز علمی و تحقیقاتی و استفاده از ایده‌های راهبردی در سیاست‌گذاری-های کلان نظام در دستور کار قرار بگیرد.

۷. وزارت فرهنگ و ارشاد اسلامی برای حل چالش ناهماهنگی بین متولیان مدیریت امور فناوری‌های نوین ارتباطی به‌ویژه اینترنت و فضای مجازی برای هدفمند کردن و اثربخش کردن تصمیمات راهبردی در این حوزه اقدام نماید.

۸. وزارت ارتباطات و فناوری اطلاعات با همکاری وزارتخانه‌های علوم، تحقیقات و فناوری و دفاع و پشتیبانی نیروهای مسلح زیرساخت‌های مورد نیاز برای توسعه برنامه‌های سیاسی، اقتصادی، فرهنگی، اجتماعی، صنعتی، علمی و نظامی با استفاده از فنّاوری‌های ارتباطی و اطلاعاتی نوین را فراهم نماید.

۹. برای مصون‌سازی و ایمن‌سازی دیتاهای داخلی ضمن اقدام برای افزایش قدرت نرم‌افزاری و سیستم‌های حفاظتی، کار تأسیس اینترنت داخلی با شدت بیشتر تداوم یابد.

۱۰. شبکه‌ای شدن و جهانی شدن فضای سایبر بر میزان تهدیدات امنیتی مانند تروریسم، تخریب منابع حیاتی و حساس، حمله نظامی، جاسوسی سایبری، حک کردن اطلاعات محرمانه سازمان‌ها و مردم در جهان افزوده است. جمهوری اسلامی ایران نیز

به‌عنوان کشوری باقابلیت‌های فراوان اقتصادی، نظامی و سیاسی در منطقه در معرض این تهدیدات قرار دارد؛ بنابراین پیشنهاد می‌شود وزارت دفاع و وزارت ارتباطات و فناوری اطلاعات برای حفاظت از سرمایه‌های ملی و حیاتی کشور، توسعه زیرساخت‌های اساسی در فضای سایبر و مطالعات گسترده برای تولید نرم‌افزارهای پیشرفته در حوزه سایبری را در دستور کار خود قرار دهند.

فهرست منابع ومآخذ

الف. منابع فارسی

- آدمی، علی و نکویی، سیداحمد (۱۳۹۷)، «نقش و جایگاه رسانه در راهبردهای گروه‌های سلفی جهادی و تأثیر آن بر خاورمیانه»، ***فصلنامه مطالعات رسانه‌های نوین***، سال چهارم، شماره ۳، صص، ۳۲۵-۲۹۱.
- اسدی، احمد (۱۳۹۹)، ***ترور شهید سلیمانی با سه پهپاد برخاسته از پایگاه آمریکایی عین السد در بغداد صورت گرفت***، وبگاه خبرگزاری جمهوری اسلامی. آدرس وبگاه:
https://www.irna.ir/news/۸۴۱۶۳۹۸۱
- آشوری، داریوش (۱۳۸۷)، ***دانش‌نامه سیاسی***، چاپ شانزدهم، تهران: نشر مروارید.
- آلبرس، دیوید و پاپ، دانیل (۱۳۸۵)، ***گزیده‌ای از عصر اطلاعات***، ترجمه علی علی‌آبادی، رضا نخجوانی، تهران: پژوهشکده مطالعات راهبردی.
- امام خامنه‌ای، سید علی (۱۳۹۷)، ***بیانات در اجتماع بسیجیان در ورزشگاه آزادی تهران***.
- برجعلی‌زاده، محمد؛ جعفری، علی و کردی، ناهید (۱۴۰۰)، «نقش فناوری‌های نوین ارتباطی در گسترش دیپلماسی در عرصه بین‌الملل (مورد مطالعه: استادان دانشگاه، کارشناسان و پژوهشگران رسانه)»، ***فصلنامه پژوهش‌های ارتباطی***، شماره ۱(پیاپی،۱۰۵)، صص ۶۵-۴۱.
- برجعلی زاده، محمد؛ جعفری، علی و کردی، ناهید (۱۳۹۸)، «نقش رسانه‌های نوین در گسترش تروریسم در عرصه بین‌الملل»، ***دو فصلنامه مطالعات قدرت نرم***، سال نهم، شماره اول (پیاپی ۲۰)، صص ۱۷۶-۱۴۳.
- برجعلی زاده، محمد؛ جعفری، علی و کردی، ناهید (۱۳۹۹)، «نقش فناوری‌های نوین ارتباطی در جابجایی قدرت در عرصه بین‌الملل»، ***دو فصلنامه دانش سیاسی***، دوره ۱۶، شماره ۲، (پیاپی ۳۲)، صص ۳۸۶-۳۶۱

- برون، مهرداد (۱۳۹۷)، ***فناوری اطلاعات***، تهران: ششمین کنگره بین‌المللی توسعه و ترویج علوم و فنون بین‌المللی.
- بل، دیوید (۱۳۸۹)، ***درآمدی بر فرهنگ سایبر***، ترجمه مسعود کوثری و حسین حسنی، تهران: انتشارات جامعه شناسان.
- پرهوده، لیلا (۱۳۹۸)، ***امنیت سایبری چیست؟*** وبگاه نکسترافاکتوری، ۱۴۰۰/۶/۲۲

https://www.nexterafactory.com/

- تقی پور، رضا؛ لشکریان، حمیدرضا و یزدانی چهربرج، رحیم (۱۳۹۷)، «الگوی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران»، ***فصلنامه امنیت ملی***، سال نهم، شماره ۳۴، صص، ۴۸-۸.
- حاجی محمدی، علی و بیچرانلو، عبدالله (۱۳۹۳)، ***رسانه‌های نوین و تحولات بین‌المللی***، تهران: مرکز پژوهش‌های صداوسیما.
- حافظ‌نیا، محمدرضا (۱۳۹۴)، ***جغرافیای سیاسی فضای مجازی***، تهران: سمت.
- خانیکی، هادی و بابایی، محمود (۱۳۹۰)، «تأثیر سازوکارهای ارتباطی اینترنت بر الگوهای تعامل کنشگران فضای سایبری ایران». ***فصلنامه علوم اجتماعی***، شماره ۵۶، صص، ۱۱۶-۷۳.
- خبرگزاری انا (۱۳۹۸)، ***سیطره هوش مصنوعی بر جنگ‌های آینده***/ به‌کارگیری میکروپهپادهای قاتل برای عملیات‌های تروریستی، نشانی سایت:

https://www.ana.press/news/447561

- خلیلی‌پور رکن‌آبادی، علی و نورعلی وند، یاسر (۱۳۹۱)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، ***فصلنامه مطالعات راهبردی***، سال پانزدهم، شماره ۵۶، ص ۱۹۹-۱۶۸
- داداندیش، پرویز و کوزه گر کالجی، ولی (۱۳۸۹)، «بررسی انتقادی نظریه مجموعه امنیتی منطقه‌ای با استفاده از محیط امنیتی منطقه قفقاز جنوبی»، ***فصلنامه راهبرد***، سال نوزدهم، شماره ۵۶، ۷۳-۱۰۷.
- دانشنامه رشد؛ شبکه ملی مدارس (۱۳۹۹)، ***مکرها کیستند؟*** وبگاه دانشنامه رشد. نشانی سایت:

http://daneshnameh.roshd.ir/mavara/mavara-index.php?page&SSOReturnPage=Check&Rand=0-

- ذوالفقاری، وحید و کیانژاد، سیده فاطمه (۱۳۹۷)، «شبکه‌های تروریسم در ژئوپلیتیک نوین جهانی و استراتژی‌های مدیریت آن»، ***دو فصلنامه سیاست و روابط بین‌الملل***، سال دوم، شماره دوم، صص، ۵۲-۳۱.

- رستم پور، محمد (۱۴۰۰)، «***اولین چالش سایبری دولت بایدن؛ اختلال سایبری در شبکه سوخت آمریکا***»، مرکز پژوهش‌های مجلس شورای اسلامی.

https://rc.majlis.ir/fa/report/show/1663669

- رمضانی، رسول و موحدی صفت، محمدرضا (۱۳۹۹)، «رتبه‌بندی تهدیدهای اینترنت اشیاء در محیط نظامی»، ***فصلنامه امنیت ملی***، سال یازدهم، شماره سی نهم، صص ۲۲۸-۱۹۹.
- روزنا، جیمز و سینگ، جیمز (۱۳۹۵)، ***فناوری اطلاعات و سیاست جهانی؛ تغییر گستره قدرت و حاکمیت***، ترجمه احمد سلطانی نژاد، تهران: انتشارات دانشگاه امام صادق (ع)، چاپ نخست.
- روزنا، جیمز (۱۳۸۴)، ***انقلاب اطلاعات، امنیت و فناوری‌های جدید***، ترجمه علی‌رضا طیب، تهران: پژوهشکده مطالعات راهبردی.
- زابلی زاده، اردشیر و وهاب پور، پیمان (۱۳۹۷)، «قدرت بازدارندگی در فضای معاصر»، ***دوفصلنامه رسانه و فرهنگ***، پژوهشگاه علوم انسانی، مطالعات فرهنگی، سال هشتم، شماره اول، صص ۷۴-۴۷.
- سلطان‌زاده، شادی (۱۴۰۰)، ***جزئیات جدید نیویورک تایمز از نحوه ترور شهید فخری زاده***، خبرگزاری ایسنا. نشانی وبگاه:

https://www.isna.ir/news/1400062720259

- سیمبر، رضا (۱۳۹۴)، ***مقدمه‌ای بر تروریسم سایبری و امنیت دیجیتال***، گیلان: انتشارات دانشگاه گیلان.
- شبکه‌های دینی، گزارش مانیتورینگ سیما (۱۳۹۰). نشانی سایت:

www.iribnews.ir/fa/news

- صیاد، محمدکاظم؛ امینی، آرمین و طاهری، ابوالقاسم. (۱۳۹۹)، «تهدیدات سایبری و اقدامات امنیتی در فضای مجازی، بررسی و رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران»، ***فصلنامه امنیت ملی***، سال دهم، شماره سی هشتم، صص ۳۹۳- ۳۳۰.
- غرایان زندی، داوود (۱۳۹۰)، ***سیاست‌گذاری امنیت ملی***، تهران: پژوهشکده مطالعات راهبردی.
- غلام نژاد، پژمان؛ غلامی، محمود و پورمکاری، علیرضا (۱۳۹۸)، «کاربردهای نظامی اینترنت اشیاء با تأکید بر مأموریت‌های نیروی هوایی ارتش جمهوری اسلامی ایران»، ***فصلنامه علوم و فنون نظامی***، سال ۱۵، شماره ۴۹، صص ۱۶۳-۱۴۲.
- کاستلز، مانوئل (۱۳۹۶)، ***شبکه‌های خشم وامید، جنبش‌های اجتماعی در عصر اینترنت***، ترجمه: مجتبی قلی پور، تهران: نشر مرکز.

- قاضی‌زاده، ضیاءالدین (۱۳۸۷)، ***فناوری اطلاعات و ارتباطات و مبانی نظام‌های اطلاعاتی***، تهران: موسسه چاپ و نشر امام حسین (ع).
- قلی زاده، میثم؛ حقیقی، مهدی؛ رضایی، علیرضا و قاسمی، ابراهیم (۱۳۹۷)، «***هوش مصنوعی نحوه‌ی عملکرد آن در امنیت دفاعی کشورهای پیشرفته و کاربرد و ضرورت آن در امور نظامی***»، کنفرانس بین‌المللی امنیت، پیشرفت و توسعه پایدار مناطق مرزی، سرزمینی و کلان‌شهرها، راهکارها و چالش‌ها با محوریت پدافند غیرعامل و مدیریت بحران، تهران، نشانی سایت: https://civilica.com/doc/876018
- فتاحی اردکانی، حسین؛ مسعودنیا، حسین و امام جمعه زاده، سیدجواد (۱۳۹۷)، «تحلیل مفهوم قدرت و منابع تشکیل دهنده آن از دیدگاه جوزف نای»، ***دوفصلنامه مطالعات قدرت نرم***، ۸(۱۸)، ۱۳۰-۱۵۲.
- معین، محمد. (۱۳۸۶)، ***فرهنگ فارسی***، تهران: جلد دوم، انتشارات نقره آبی.
- منفرد محمدی، محمد؛ نژادنوری، محمدمهدی و آقایی، محسن (۱۳۹۹)، «بررسی تهدیدات ناشی از کاربردهای اجتماعی فضای سایبر در جمهوری اسلامی ایران»، ***فصلنامه امنیت ملی***، سال دهم، شماره سی و ششم، صص ۲۴۲- ۲۱۳.
- مهدی زاده، سیدمهدی (۱۳۹۲)، ***انقلاب ارتباطات، همگرایی و تعامل***، سایت راسخون. نشانی سایت: http://www.rasekhoon.net/article/show ۲۷۶۹۰۷/
- میرمحمدی، مهدی و محمدی لرد، عبدالمحمود (۱۳۸۷)، ***سیاست و اطلاعات: مطالعه موردی ایالات متحده آمریکا***، تهران: موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.
- نای، جوزف (۱۳۹۸)، ***آینده قدرت***، ترجمه محمد حیدری و آرش فرزاد، تهران: انتشارات فیرزان.
- – نای، جوزف (۱۳۸۷)، ***قدرت در عصر اطلاعات، از واقع‌گرایی تا جهانی شدن***، ترجمه سعید میرترابی، تهران: پژوهشکده مطالعات راهبردی
- – نای، جوزف (۲۰۱۰)، ***قدرت نرم و دیپلماسی عمومی در قرن ۲۱***، سخنرانی جلسه آغازین پارلمانی شورای انگلستان. ۲۰ ژوئن ۲۰۱۰، برگرفته از سایت مشرق نیوز.
- نشانی سایت: https://www.mashreghnews.ir/news/۷۰۷۴/
- نایک، لیا (۲۰۱۸)، ***هوش مصنوعی برای ردیابی موشک؛ برنامه پنهانی پنتاگون***، خبرگزاری یورونیوز فارسی، بارگیری از وبگاه یورونیوز فارسی در تاریخ ۱۴۰۰/۷/۲. نشانی وبگاه: https://per.euronews.com/

۰۶/۰۶/ ۲۰۱۸/pentagon-in-search-of-ai-use-in-missile-defence- mechanisms

- نجفی علمی، مرتضی (۱۳۹۱)، ***روند تحولات فضای سایبر و نقش آن در تهدیدات ناشی از جرم در محیط سایبر در ج.ا.ا***، رساله دکترای جامعه‌شناسی، دانشگاه علامه طباطبایی، دانشکده علوم اجتماعی.
- نقبایی، سید رضا (۱۳۹۱)، ***دایره المعارف واژگانی ارتباطات***، جلد دوم، تهران: انتشارات آوینا.
- ونت، الکساندر (۱۳۸۴)، ***نظریه اجتماعی سیاست بین‌الملل***، ترجمه حمیرا مشیری، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات.
- هلیلی، خداداد؛ ولوی، محمدرضا؛ موحدی صفت، محمدرضا و باقری، مسعود (۱۳۹۷)، «قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر»، ***فصلنامه امنیت ملی***، سال هشتم، شماره بیست و نهم، صص، ۲۰۰-۱۷۳.
- یزدان پناه، کیومرث و کامرانی، احسان (۱۳۹۴)، «تروریسم در فضای مجازی و اثرات آن بر حوزه جغرافیای سیاسی»، ***فصلنامه انجمن جغرافیای ایران***، دوره جدید، شماره ۴۴، صص ۲۵- ۴۶.

ب. منابع انگلیسی

- Buzan, Barry; Wæver, Ole. (2003). Regions and Powers: The Structure of International Society. Cambridge, United Kingdom: The Press Syndicate of the University of Cambridge. pp. 6–20, ۴۱–۴۷, ۷۷–۸۲. SBN 0 521 81412 X.
- Buzan, B. (1987), An International to Sterategic Sudies: Military Thecnology and International Relations, New York: St. Martin Press.
- Chipunza, Linda Lorraine Cecilia. (2007). "What Men Say, How Women Say: An Exploration of the Interactional Mechanisms at Play in Management Meetings". PhD Thesis, University of South Africa.
- Gupta, M. (2010) Indian Ocean Region: Maritime Regimes for Regional Cooperation, London: Springer p 52. From https://en.wikipedia.org/wiki/Regional_security_complex_theory
- Hare, Forrest. (2010). "The Cyber Threat to National Security: Why Can't We Agree?" CCDCOE Publications, Tallinn, Estonia.
- Larousse, Pierre. (1964). Grand Larousse encyclopédique en dix volumes, Paris Librairie.
- Libiski, Martinec. Conguest in Cyber Space, National Security and formation War Fare London: Cambridge University Press, 2007.
- Mahrukh, Ali. (2015). ISIS and Propaganda: How ISIS Exploits Women, Reuters Institute forthe Study of Journalism (University of Oxford).
- Mahzam, Remy. (2015). The Electronic Digitization of ISIS: Building a Multi-Media Legacy, S. Rajaratnam School of International Studies (RSIS).

- Nye, Josephs. (2010). cyber power, Belfer center for science and international Affairs.
- Nye, J. S. (2011). The Future of Power, New York: Public Affairs.
- https://www.belfercenter.org/publication/cyber-power
- Waltz, K. (1979). Theory of International Politics, New York: Random house.