

دوفصلنامه علمی مطالعات قدرت نرم، سال نهم، شماره اول (پیاپی ۲۰)، بهار و تابستان ۱۳۹۸

صص ۱۷۲-۱۳۹

## بررسی نقش رسانه‌های نوین در گسترش تروریسم در عرصه بین‌الملل

نوع مقاله: پژوهشی

محمد برجلی زاده<sup>۱</sup>، علی جعفری<sup>۲</sup>، ناهید کردی<sup>۳</sup>

تاریخ پذیرش: ۱۳۹۸/۰۶/۲۷

تاریخ دریافت: ۱۳۹۸/۰۲/۲۱

### چکیده

فناوری‌های ارتباطی نوین به‌عنوان مهمترین دست‌آورد انسان قرن بیستم از طریق اتصال زیربناها و روبناها در حیات مادی و معنوی بشر، ظرف سه دهه، ابعاد گوناگون زندگی انسان معاصر را دستخوش تغییر و تحول کرده است. اینترنت و فضای مجازی علاوه بر تأثیرات بنیادین بر حوزه‌های فرهنگی، اجتماعی و اقتصادی جوامع مختلف ابعاد تهدیدآمیزی را نیز آشکار ساخته و زمینه انتقال منابع ناامنی از فضای واقعی به مجازی را فراهم کرده است. امروزه محیط‌های تهدیدآمیز علیه ملت‌ها و دولت‌ها به سرزمین محدود نمی‌شود و جهان مجازی نیز محیطی تهدیدزا به‌شمار می‌آید. سایر تروریسم یکی از مهمترین تهدیدات نوظهور است که با استفاده از قابلیت‌های اینترنت به فعالیت‌های خود بعد بین‌المللی داده است. با توجه به اهمیت مطالعات بنیادین در شیوه مواجهه با پدیده‌های نوظهور، این پژوهش با هدف شناخت نقش رسانه‌های نوین در ظهور و گسترش تروریسم در عرصه بین‌الملل، با استفاده از روش پیمایش و ابزار پرسشنامه محقق‌ساخته در سطح صاحب‌نظران و کارشناسان سراسر کشور اجراء شد. یافته‌ها نشان داد از میان پنج عامل مورد بررسی شامل: ماهواره، اینترنت، فضای مجازی، شبکه‌های اجتماعی و روزنامه‌نگاری سایر، عامل فضای مجازی در ظهور و گسترش و گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه بین‌الملل بیشترین نقش را ایفاء کرده است.

**واژه‌گان کلیدی:** رسانه‌های نوین، قدرت، فضای سایبر، تروریسم.

۱- دانشجوی دکتری علوم ارتباطات، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران.

۲- استادیار گروه علوم ارتباطات، واحد اردبیل، دانشگاه آزاد اسلامی، اردبیل، ایران. (نویسنده مسئول)

jafari.communication@gmail.com

۳- استادیار گروه علوم ارتباطات، واحد تهران شرق، دانشگاه آزاد اسلامی، تهران، ایران.



## مقدمه

تروریسم پدیده تازه‌ای نیست. بر اساس گفتمان مذاهب ابراهیمی، هابیل اولین قربانی تروریسم است. تروریسم بیشتر در فضا و شرایطی رخ می‌دهد که در آن قدرت به صورت ناعادلانه توزیع شده باشد (ناجی راد، ۱۳۸۷: ۷).

تروریسم سایبری پدیده‌ای است نوظهور که همزمان با تحول در حوزه فن‌آوری‌های نوین ارتباطی و اطلاعاتی و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت ایجاد شده است، به گونه‌ای که امروزه به‌عنوان یکی از چالش‌های مهمی که امنیت جهانی را تهدید می‌کند مورد توجه قرار گرفته است. اینکه تروریسم چگونه توانسته است تهدیدات خود را از فضای فیزیکی و جغرافیایی به فضای مجازی منتقل کند، به ظرفیت‌های کم‌نظیر و ساختار پیچیده اینترنت ارتباط دارد. تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند؛ این تهدیدها گستره وسیعی از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند. هزینه پایین بهره‌برداری از فن‌آوری رایانه‌ای همراه با اتصال گسترده به اینترنت و سهولت ایجاد یا به‌دست آوردن نرم‌افزارهای مخرب به ورود بازیگران جدید در عرصه‌های ملی و بین‌المللی منجر شده است. زمان محدود و سرعت بالای اقدام در فضای سایبر، شرایطی را برای انجام اقداماتی با خطرات و تأثیرگذاری بیشتر فراهم کرده است. این فناوری تهدیدکنندگان را برای عبور از محدودیت‌های مرزی به دستیابی به اهداف مورد نظر در هر نقطه‌ای از جهان قادر می‌سازد. بنابراین بدون توجه به مقوله قدرت و امنیت در قرن ۲۱، صحبت در باره پدیده تروریسم در فضای سایبر، مطالعه چگونگی رشد و گسترش فعالیت‌های تروریستی در سطح بین‌المللی بی‌نتیجه است. امروزه برای ارزیابی مقوله قدرت در سطح ملی و بین‌المللی توجه به عامل‌هایی چون، فن‌آوری، آموزش و رشد اقتصادی اهمیت یافته است. قدرت وابسته به فضای سایبری یکی از مهمترین زمینه‌های جدید در سیاست جهانی است که توانایی به‌دست آوردن نتایج بهتری را از طریق استفاده از منابع الکترونیکی در دامنه سایبری دارد (Nay, 2010: 4). افزایش سرعت فرایندها و

ساختارهای پیشرفته، وابستگی بیشتر به اینترنت را به همراه داشته و باعث شده سالانه میلیاردها دلار به اقتصاد جهانی اضافه شود. تجارت اینترنتی در سطح جهان در سال ۲۰۱۰ در حدود ۱۰ تریلیون دلار بوده و تخمین زده می‌شود این آمار در سال ۲۰۲۰ به ۲۴ تریلیون دلار برسد (خلیلی‌پور رکن آبادی و نورعلی‌وند ۱۳۹۱: ۲۲).

امروزه فضای سایبری به‌عنوان یکی از مهمترین منابع قدرت مورد توجه بازیگران دولتی برای دستیابی به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی است. توسعه جنبه‌های گوناگون خدمات رسانی در اینترنت از یک سو و گسترش فعالیت مهاجمان رایانه‌ای، سارقان و جاسوسان اطلاعاتی از سوی دیگر، حجم تهدیدها و آسیب‌های ناشی از این فناوری را به شدت افزایش داده است. این تهدیدها، امروزه علاوه بر اینکه روزبه‌روز گسترش می‌یابند و پیچیده‌تر می‌شوند، امنیت ملی کشورها و دولت‌ها را نیز به‌طور مستقیم تحت تأثیر قرار می‌دهند (میرمحمدی و محمدی لرد، ۱۳۸۷: ۳۶). اهمیت تهدیدات تروریستی در شبکه جهانی اینترنت به اندازه‌ای است که اداره اطلاعات ملی آمریکا که وظیفه هماهنگی بین ۱۶ سازمان اطلاعاتی آمریکا را بر عهده دارد، در گزارش فوریه ۲۰۱۰، تهدیدات سایبری را از مهمترین تهدیدات فراروی امنیت ملی این کشور ذکر می‌کند. بر اساس این گزارش موازنه قدرت در فضای مجازی به نفع کنشگران مخرب شامل دولت - ملت‌ها، شبکه‌های تروریستی و گروه‌های جنایی سازمان یافته و افراد در حال تغییر است (یزدان پناه، ۱۳۹۳).

ریچارد کلارک<sup>۱</sup> مشاور عالی ضد تروریسم آمریکا در سال ۲۰۱۰، ضمن اظهار عجز از ناتوانی آمریکا در جلوگیری از دستیابی تروریست‌ها به سیستم‌های رایانه‌ای این کشور، از این موضوع به‌عنوان فاجعه پرل هاربر الکترونیکی یاد می‌کند. گزارش‌های متعدد وال استریت ژورنال و نیویورک تایمز نظر کلارک را تأیید می‌کند. بنا به این گزارش‌ها از سال ۲۰۱۰ تا ۲۰۱۸ میلادی، به تأسیسات حیاتی ایالات متحده آمریکا شامل: کارخانه‌های برق،

1 Richard Clarke

صنایع سنگین، پیمان کاری‌های دفاعی و دانشگاه‌ها، بانک‌ها و سازمان سیا، صدها بار حمله شده است. در این عرصه تأسیسات حیاتی سایر کشورها مانند: تأسیسات هسته‌ای ایران در نطنز در سال ۲۰۰۷، برق و انرژی ترکیه در سال ۲۰۱۷ و تأسیات برق و انرژی ونزوئلا در سال ۲۰۱۸ از سوی تروریست‌ها تهدید و تخریب شده است. دایره تروریسم سایبری به سرعت در حال گسترش است، بعد از تروریسم دولتی، اقتصادی، صنعتی و زیستی، شاهد شکل‌گیری شاخه‌ای جدید تحت عنوان تروریسم مذهبی هستیم. تروریسم مذهبی با فعالیت سازمان یافته در فضای مجازی، ظرف مدت کوتاهی دایره نفوذ و سیطره خود را از سطح منطقه به سطح بین‌المللی گسترش داده است. گروه تروریستی سلفی و وهابی داعش بیشترین فعالیت‌های مالی، فرهنگی، تبلیغاتی، آموزشی و هدایت تیم‌های تروریستی خود را به‌طور گسترده در فضای مجازی سازماندهی می‌کند.

گسترش فعالیت‌های تروریستی در سطح جهان و تراکم گروه‌های تروریستی در محیط پیرامونی جمهوری اسلامی ایران نیز از جمله موضوعات مورد توجه این پژوهش است. در این پژوهش که با استفاده از روش پیمایش و پرسشنامه محقق ساخته اجرا شده، محقق در تلاش است به این پرسش اساسی پاسخ دهد که رسانه‌های نوین در گسترش تروریسم به‌عنوان یکی از کنشگران جدید در عرصه بین‌الملل چه نقشی دارند؟

### پیشینه تحقیق

میربد و همکاران (۱۳۹۸) در مقاله‌ای تأثیر تروریسم سایبری بر حقوق بین‌المللی را بررسی کرده‌اند. یافته‌های این پژوهش نشان می‌دهد؛ رسانه‌های نوین به‌ویژه اینترنت و فضای مجازی این امکان را برای تروریست‌ها فراهم کرده است که با حمله به زیرساخت‌های حیاتی دولت‌ها نظیر؛ حمل و نقل هوایی، سدها، نیروگاه‌های هسته‌ای و تولید برق، سیستم بانکی و مالی، ایجاد رعب و وحشت عمومی و تهدید و اجبار دولت‌ها به منافع مورد نظر دست یازند. نتایج این مطالعه نشان می‌دهد تروریسم سایبری ظرفیت تقویت و اجرای

انواع دیگر تروریسم نظیر؛ بیوتروریسم، اکوتروریسم، تروریسم هسته‌ای و انواع کلاسیک آن را دارد. تروریسم سایبری از قابلیت بالایی برای نقض قواعد حقوق بشر برخوردار است. بنابراین پرداختن به این موضوع و مبارزه همه‌جانبه با تروریسم سایبری در سطح بین‌المللی از اهمیت زیادی برخوردار است.

مطالعات آدمی و نکویی (۱۳۹۷) نشان می‌دهد رسانه‌های نوین علاوه بر کمک به پیشبرد ارزش‌های انسانی و پیشرفت صلح در جامعه جهانی، به ابزار گروه‌های رادیکال برای تبلیغ ارزش‌ها و اقدامات ضد بشری آنان تبدیل شده و خاورمیانه را به کانون اصلی بحران مبدل کرده است. یافته‌های این پژوهش نشان می‌دهد؛ گروه‌های تروریستی القاعده و داعش، بیشتر مراحل عضوگیری، ترویج خشونت، مشروعیت‌سازی و فراخواندن پیام‌های خود برای طرفداران و دشمنان را از طریق اینترنت و فضای مجازی انجام داده‌اند.

نتایج پژوهش سلطانی‌نژاد و همکاران (۱۳۹۵) حاکی است، متغیر قدرت بعد از جنگ سرد تحت تأثیر فناوری‌های نوین اطلاعاتی و ارتباطی دستخوش تغییر شده و مفهوم آن از حالت سخت‌افزاری به نرم‌افزاری تغییر یافته و اجزای مختلف قدرت را تحت تأثیر قرار داده است. همچنین در پرتو فضای مجازی، مفهوم قدرت ابعاد وسیع‌تری یافته است و در این میان، بعد فرهنگی و نرم‌افزاری آن تبدیل به مسئله محوری روابط بین‌الملل شده است و با هنجاری و اجتماعی شدن مفهوم قدرت، بازیگران و مرزهای جغرافیایی قدرت، منابع قدرت و گروه‌های هدف آن تحت تأثیر قرار گرفته‌اند.

تروریسم دولتی در فضای مجازی و راهکارهای مقابله با آن موضوع مقاله‌ای است که از سوی شاه‌علی و موحدیان (۱۳۹۱) مورد بررسی قرار گرفته است. به اعتقاد نویسندگان، تروریسم و یکی از شاخه‌های خطرناک آن یعنی تروریسم دولتی نیز از این تحولات تأثیرپذیرفته و پیدایش شبکه‌های اطلاع‌رسانی مانند اینترنت و شبکه‌های تلفن همراه به حامیان و سازمان‌دهندگان تروریسم دولتی امکان داده تا به شیوه‌های نوینی به اهداف خود جامعه عمل بپوشانند. در این مقاله ضمن بررسی معنا و مفهوم تروریسم دولتی در فضای

مجازی، انواع و جنبه‌های مختلف این پدیده و روش‌های مقابله با آن در داخل کشور و فضای بین‌الملل بررسی می‌شود.

امنیت در اینترنت و فضای مجازی از مقوله‌های مهم و پرچالش حوزه‌های فناوری ارتباطات و اطلاعات در عصر حاضر به‌شمار می‌رود. در این زمینه نورمحمدی (۱۳۸۹) پایان‌نامه دکترای تخصصی خود را به موضوع گسترش فناوری‌های اطلاعات و ارتباطات و تحول پدیده امنیت اختصاص داده است. یافته‌های این تحقیق بر این نکته تأکید دارد که دولت‌ها دیگر تنها کارگزاران تهدید در عرصه امنیتی جهانی نیستند، بلکه فناوری‌های اطلاعات و ارتباطات ظرفیت تهدیدآفرینی در گستره جهانی و ایجاد ناامنی در سطوح ملی و بین‌المللی را برای کنشگران غیردولتی فراهم ساخته‌اند.

نتایج مطالعات اریکسون و گیاکملو (۲۰۰۷) بر تحول در تهدیدهای امنیتی و ظهور تهدیدهای نوین مانند سایبر تروریسم و آسیب‌پذیری زیرساخت‌های حیاتی در برابر حملات سایبری در نتیجه تحولات دگرگونی‌های مداوم در وسایل اطلاعاتی و ارتباطاتی تأکید دارد. تهدیدات سایبری باعث شده است تا دولت‌ها از طریق مشارکت در وضع مقررات در سطح بین‌المللی و تدوین اصول، قواعد، هنجارها و رویه‌ها، امنیت زیرساخت‌های حیاتی را در برابر حملات بالا ببرند.

## ادبیات تحقیق

قدرت یکی از مفاهیم اصلی در روابط بین‌الملل بوده و دارای مفاهیم چندگانه است. با وجود مرکزیت مفهوم قدرت، هنوز درک کافی از آن صورت نگرفته است (آرندت<sup>۱</sup>، ۱۹۷۲: ۶۸). از این رو شناخت قدرت همواره یکی از دل‌مشغولی‌های اساسی محققان این رشته بوده است. به علاوه قدرت، مفهوم اساسی نظریه جدید سیاسی است و به عقیده برخی محققان، علم سیاست، کسب و حفظ قدرت سیاسی است (دودینگ، ۱۳۸۰: ۱۲۷). زمانی

<sup>1</sup>Arendt

که از قدرت در روابط بین‌الملل سخن می‌گوییم منظور، توانایی کنترل اذهان و اعمال انسان‌ها است. به عقیده مورگنتا<sup>۱</sup> تمام رفتار و اعمال بشر در اجتماع از قدرت سرچشمه می‌گیرد؛ از این رو قدرت در تمام شئون زندگی به نحوی از انحاء جلوه‌گر است و در ارکان اجتماعی، سیاسی، مذهبی و همچنین در تمام نهادهای داخلی و بین‌المللی به صورت‌های مختلف تجلی می‌کند (عامری، ۱۳۹۲: ۴۳۱ و ۳۶۹). از نظر «نای» قدرت قابلیت نفوذ در رفتار دیگران برای حصول نتایج دلخواه است. او رسانه‌های نوین را به‌عنوان ابزار اساسی قدرت معرفی می‌کند؛ ابزاری که قدرت را به قابلیت‌ها و توانایی‌های منحصر به فرد نفوذ در لایه‌های مختلف جامعه تجهیز می‌کند (نای، ۱۳۸۷: ۳۸). با آغاز قرن بیستم منابع قدرت تغییر کردند و ساختارها و شاخص‌های قدرت در قرن نوزدهم و ماقبل آن که بر عناصری چون میزان سلطه بر دریاها و خشکی‌ها، میزان جمعیت، وسعت مرزها و نیروی نظامی استوار بود در معرض تغییری دائمی قرار گرفت (آلبرس و پاپ، ۱۳۸۵: ۲۴۸). امروزه در ارزیابی قدرت بین‌المللی، عواملی همچون فن‌آوری، آموزش و رشد اقتصادی اهمیت بیشتری یافته است. با نگاهی به مولفه‌های قدرت در قرون گذشته روشن می‌شود که در هر دوره، منابع متفاوتی از قدرت به میزان کم یا زیاد نقش‌آفرینی کرده‌اند. «جیمز روزنا»<sup>۲</sup> از جمله اندیشمندانی است که دسته‌بندی مناسبی از منابع مهم قدرت در سده‌های مختلف ارائه کرده است. در گذشته، جمعیت، دانش، سلاح، زمین و ثروت مصادیق قدرت بودند. اما «در سه دهه اخیر، فناوریهای نوین ارتباطی شامل؛ شبکه جهانی وب و اینترنت به شکل گسترده‌ای ابعاد مختلف حیات بشری را تحت تأثیر قرار داده است» (نایار، ۱۳۹۴: ۱۳). بر این اساس، دولت‌ها، سازمان‌های ملی و فراملی، شرکت‌های بین‌المللی، گروه‌های سازمان‌یافته جنایی و تروریستی، تولیدکنندگان بدافزار و تسلیحات مجازی که به‌طور هدفمند و برنامه‌ریزی شده در فضای سایبر فعال هستند، ابعادی از قدرت محسوب

1 Morganthau

2 James N Rosenau

می‌شوند. جاسوسان رایانه‌ای و... کارایی جاسوس‌های رایانه‌ای ناپیدا و نامیرا که تنها با قرار گرفتن در اعداد غیرملموس صفر و یک در بستر مجازی شناور هستند و ویروس‌های رایانه‌ای که از هزاران موشک بالستیک مخرب‌تر، کم‌هزینه‌تر، کاربردی‌تر و مؤثرتر هستند، ابعاد دیگر قدرت در فضای سایبر به‌شمار می‌روند. به‌طور کلی ماهیت قدرت در قرن ۲۱ دچار تغییر اساسی شده است، شاهراه‌های اطلاعاتی، جهان امروز را به‌صورتی درآورده است که در آن، اطلاعات به‌مثابه قدرت به حساب می‌آید. صاحب‌نظران تأکید دارند عرصه قدرت از جمله حوزه‌هایی است که در عصر داده‌ها و اطلاعات شاهد تغییر و تحولات شگرف خواهد بود. برآیند این تحول، تغییر ماهیت قدرت از فیزیکی به قدرت سایبری است. شایان ذکر است موتورهای جستجوگر نظیر گوگل به‌عنوان گلوگاه اساسی برای دسترسی به اطلاعات و شبکه‌های اجتماعی نظیر فیس‌بوک به‌عنوان بستر تعامل ساکنان زمین، اطلاعات فردی و کاری، اجتماعی و... تمامی فعالان عرصه فضای مجازی را در اختیار دارند و فرصتی بی‌نظیر را در اختیار صاحبان این فناوری قرار می‌دهند و آنان را قادر می‌سازند تا بدون بهره‌گیری از ابزارهای قدرت گذشته نظیر قدرت تسلیحاتی و نظامی همراه با لشکرکشی‌های پرهزینه، آرایش سیاسی، فرهنگی و اقتصادی ملت‌ها و دولت‌ها را بدون حضور فیزیکی درهم ریخته و زمینه سقوط و ظهور رژیم‌های سیاسی را فراهم کنند.

ظهور و گسترش شبکه‌های اطلاعاتی، الکترونیکی و رسانه‌ای، تراکم زمان و مکان و به عبارت دقیق‌تر امواج جهانی شدن، نشانگر شروع دوران جدید و پیچیده‌تری در روابط بین‌الملل است. فناوری‌های نوین اطلاعاتی ارتباطی، که از اوایل دهه ۹۰ در مقیاس جهانی گسترش یافتند، موجب شتاب تغییرات نهادی، افزایش تعاملات بین‌المللی و تغییر مفاهیم اصلی علوم سیاسی و روابط بین‌الملل از جمله قدرت شده‌اند. شبکه جهانی اینترنت به دلیل ماهیت عملکرد فراکشوری و نیز قابلیت برقراری ارتباط و جابجایی اطلاعات، قدرت شهروندان را صرف نظر از قومیت، ملیت و مذهب و نژاد و زبان تا جایی افزایش داده که در تعارض با منافع حکومت‌ها و دولت‌ها دست به فعالیت‌هایی بزنند. سیمبر و امراللهی



(۱۳۹۴) معتقد هستند همانطوری که در جغرافیای واقعی، تهدیدها و فرصت‌ها و چالش‌هایی برای گروه‌های مختلف انسانی وجود دارد، در جغرافیای سایبر نیز عرصه این دسته از فعالیت‌ها منبع سخت‌افزاری و نرم‌افزاری را تحت الشعاع قرار می‌دهد. توجه به حیطه تهدیدها و آسیب‌ها در فضای سایبر در پنج سطح ۱. تهدیدات جهانی ۲. آسیب‌پذیری در سطح ملی ۳. تهدید تأسیسات زیربنایی ۴. تشکیلات اقتصادی بزرگ ۵. کاربران خانگی و تجارت‌های کوچک نشان می‌دهد گروه‌های تروریستی به‌واسطه بهره‌گیری از فناوری فضای مجازی از قدرتی برخوردار شده‌اند که می‌توانند با تهدید، تخریب تأسیسات زیربنایی، برانگیختن احساسات قومی، مذهبی، نژادی و ناسیونالیستی، گروه‌ها، اجتماعات بزرگ، حتی دولت‌ها و ملت‌ها را با مشکلات بزرگ مواجه نمایند. در مطالعات نوین امنیتی گفته می‌شود در شرایطی زندگی می‌کنیم که تهدیدات ملی مرتبط با امنیت تنها ناشی از وجود همسایگان متخاصم نیست، بلکه موضوعاتی مانند رکود اقتصادی، سرکوب سیاسی، کمبودها و نارسایی‌ها فرهنگی، تخریب محیط زیست، تروریسم فرامرزی، جنایات سازمان‌یافته بین‌المللی، بلایای طبیعی، بیماری‌های جهانگیر و مشکلات بهداشتی به تهدیدات بیرونی گذشته، اضافه شده‌اند.

### گستره تروریسم در اینترنت و فضای مجازی

تروریسم<sup>۱</sup>

در دایره‌المعارف فرانسوی مشهور لاروس، چنین آمده است که واژه «ترور»<sup>۲</sup> برگرفته از ریشه لاتین (Terreur) بوده که به معنای نظام یا رژیم وحشت است. کلیدواژه ترور هم این‌گونه تعریف شده است؛ ایجاد هراس در توده مردم یا گروهی از مردم به‌منظور در هم شکستن مقاومتشان؛ برقراری نظام یا فرایند سیاسی بر پایه این ترس، از طریق به‌کارگیری اقدامات حاد و خشونت‌بار (Larousse, 1964: 258). یکی از جامع‌ترین تعاریف

1 Terrorism

2 Terror

دانشگاهی از مفهوم تروریسم تعریف «آلکس. پ. اشمید»<sup>۱</sup> است. از منظر اشمید تروریسم شیوه اقدامات تکراری به منظور ایجاد دلهره و رعب و وحشت است که به دلایل سلیقه ورزی، جنایی و یا سیاسی توسط گروه‌های مختلف به کار گرفته می‌شود (schmid, 1993: 8). اما واژه سایبر تروریسم ابداع «کالین»<sup>۲</sup> است. به اعتقاد کالین، 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 (barry, 1997: 15-18). تروریسم انواع مختلفی دارد؛ تروریسم سیاسی، تروریسم اقتصادی، تروریسم فرهنگی و تروریسم سایبری را می‌توان از انواع آن برشمرد. شاید بتوان گفت که از جدیدترین نوع تروریسم در عصر حاضر، تروریسم سایبری است که در دهه ۱۹۸۰ توسط شخصی به نام کالین باری تعریف شد. بدین معنا که وقتی تروریسم و فضای مجازی با هم ترکیب شوند، دیگر از حمله‌های فیزیکی خبری نیست، حمله علیه رایانه‌ها و اطلاعات ذخیره شده است که به منظور ترساندن و مجبور کردن یک دولت و اتباع آن کشور برای اهداف سیاسی خاص صورت می‌گیرد.

### سایبر تروریسم / تروریسم مجازی

تروریسم سایبری یا مجازی، واژه‌ای است که اخیراً به ادبیات سیاسی جهان وارد شده است. تروریسم سایبری یا مجازی اعمال خشونت یا تهدید به آن در حمله به زیرساخت‌های حیاتی یک کشور با اعمال تخریب، ممانعت یا اختلال در داده‌ها، سیستم‌ها، شبکه یا مؤلفه‌های اطلاعاتی رایانه‌ای است که با ایراد خسارت یا صدمه و خسارت فیزیکی یا اطلاعاتی به اموال و اشخاص و ایجاد رعب و وحشت نموده و هدف از آن به زانو درآوردن دولت یا سازمان دولتی در جهت انگیزه‌های سیاسی و ایدئولوژیک و یا اجتماعی

1 Alex P. Schmid

2 Collin Barry

است (میرید و دیگران، ۱۳۹۸: ۲۲۷). سایر تروریسم<sup>۱</sup> را به‌عنوان نوعی جدید و متمایز از تروریسم به‌کار می‌برند، اما صحیح‌تر این است که آن را یک تاکتیک جدید تروریستی بدانیم. سایر تروریسم از جهت ماهیت بر همان اصولی استوار است که همه انواع تروریسم بر آن مبتنی است. به‌نظر می‌رسد نباید تروریسم سایبری را نوع جدید تروریسم به‌شمار آورد؛ زیرا سایر تروریسم در حقیقت مانند دیگر اشکال تروریسم است که در آن یک مؤلفه رایانه‌ای وجود دارد، لذا به‌نظر برخی حقوقدانان، سایر تروریسم روشی نوین برای اقدامات تروریستی است، نه نوع دیگری از تروریسم (عبدی، ۱۳۹۵). نخستین خطر جدی تروریسم سایبری در سال ۲۰۰۷ علیه وبسایت‌های دولت کشور استونی صورت پذیرفت. در آن زمان اشتراک نظر به‌دست داشتن دولت روسیه در این حمله بود (میرید و دیگران، ۱۳۹۸: ۲۲۵). در تهاجم سایبری سال ۲۰۰۷ علیه تأسیسات سایبری کشور استونی، در طی چند ساعت شبکه‌های اینترنتی بانکی از کار افتاد، انتشار تمامی روزنامه‌های محلی متوقف شد و ارتباطات دولتی مختل گردید. تداوم این حملات بیشتر وبسایت‌های مهم و اساسی استونی را از کار انداخت و باعث نافرمانی وسیع مدنی و آشوب گردید که طی آن ۱۵۰ نفر زخمی و یک تبعه روس کشته شد (شکلفورد، ۲۰۰۹). حمله به تأسیسات هسته‌ای ایران در سایت نطنز یکی از مهمترین حملات صورت گرفته علیه تأسیسات حیاتی یک کشور ارزیابی می‌شود؛ روزنامه نیویورک تایمز در مه ۲۰۱۰ با انتشار گزارشی افشا کرد: یکی از حملات سایبری که در چند سال گذشته توجه جهانیان را به خود جلب کرده است، حمله سایبری به تأسیسات هسته‌ای ایران است؛ این حمله به وسیله نرم‌افزاری به نام «استاکس نت»<sup>۲</sup> و با هدف نفوذ به تأسیسات هسته‌ای ایران از سال ۲۰۰۴ تا ۲۰۱۰ طراحی شد و قرار بود سرعت هزاران سانتریفیوژ را تغییر دهد و در تحقیقات هسته‌ای ایران اختلال ایجاد کند. شرکت لانگلد با آنالیز کدهای این بدافزار که ۲۰ برابر پیچیده‌تر از کدهای ویروسی دیگر

1 Cybernetic terrorism

2 Staks net

بود، اعلام کرد این اقدام تنها از قدرت سایبری آمریکا برمی آید. همچنین این شرکت اعلام کرد نشانه‌هایی از دخالت و نقش رژیم صهیونیستی نیز وجود دارد (عبدی، ۱۳۹۵). همچنین در این راستا می‌توان به دستیابی هک‌های اینترنتی به سیستم ارتباطی فرودگاهی در ماساچوست آمریکا در سال ۱۹۹۷ و ایجاد اختلال بین ارتباط برج مراقبت، خدمات فرودگاهی و هواپیماهای در حال پرواز اشاره کرد. دستیابی کارمند سابق صنایع مدیریت پسماند استرالیا به سیستم‌های رایانه‌ای آنجا و جاری ساختن هزاران لیتر فاضلاب در مزارع کوئینزلند برای تخریب محیط‌زیست نمونه دیگری از تروریسم سایبری است.

همچنین رایانه‌ای که از القاعده در افغانستان مصادره شد، حاوی نمونه‌هایی از یک سد بود که طراحان را قادر می‌ساخت تا سطح آسیب‌پذیری و تخریب سد را تخمین بزنند. دفتر فدرال ایالات متحده از موارد زیادی از نمونه‌های طراحی شده توسط القاعده که برای اهداف آنلاین و نظارت بر سیستم‌های تلفن اضطراری، ژنراتورها و دستگاه‌های مخابراتی، مخازن آب و سیستم توزیع، نیروگاه‌های اتمی و شبکه‌های مخازن سوخت برنامه‌ریزی شده بودند پرده برداشت (میربد و دیگران، ۱۳۹۸: ۲۳۰).

تروریسم در مرحله متاخر آن و در گذار به قرن بیست و یکم، از تروریسم بین‌المللی به تروریسم جهانی متحول شده و عامل این تحول، غیرسرزمینی شدن آن در روابط بین‌الملل است. عمده‌ترین متون مربوط به تروریسم و ابعاد فعالیت‌های آن در عرصه جهانی مربوط به برخی گروه‌های رادیکال در دنیای اسلام است. از جمله مهم‌ترین گروه‌های تروریستی دوره جدید که توانست بیشترین توجه مراکز رسانه‌ای و دانشگاهی را به خود جلب نماید القاعده است. گروه افراطی القاعده بعد از سقوط رژیم طالبان در اوایل دهه ۲۰۰۰، اجرای بسیاری از فعالیت‌هایش را به بستر اینترنت و فضای مجازی منتقل نمود. اکونومیست در سال ۲۰۰۷، گزارش داد: اینترنت وسیله‌ای عالی برای تبلیغات در اختیار گروه‌های جهادی قرار می‌دهد و آنها می‌توانند بدون سانسور حکومتی به بازدیدکنندگان فراوانی دست یابند (سیمبر، ۱۳۹۴: ۴۵).

القاعده بر خلاف ساختار سازمان‌های عصر مدرن (که از منطق ماشین پیروی می‌کنند) از یک سو با ایجاد روابط خانوادگی و از سوی دیگر با بهره‌گیری از فناوری‌های نوین، شکل جدیدی از سازماندهی را به‌منصه‌ظهور رسانده است که نه متعلق به سنت است و نه مدرن، بلکه متعلق به دورانی است که به پست‌مدرن شهرت دارد. در بین سازمان‌های تروریستی، داعش (دولت اسلامی شام و عراق) سازمان‌یافته‌ترین گروهی است که از فناوری‌های نوین ارتباطی و رسانه‌ای برای هدایت افکار عمومی بهره گرفته است (Ali, 2015: 10). داعش برای نشان دادن قدرت نظامی خود جدیدترین فیلم‌ها، اعلامیه‌ها و نشریات را در فضای مجازی، تالارهای گفت‌وگو و انجمن‌ها قرار داده و در شبکه‌های اجتماعی نظیر توئیتر، فیس بوک و گوگل پلاس بازنشر می‌کنند (Mahzam, 2015: 1). کرم‌های اینترنتی نمونه دیگری از تهدیدات سایبری هستند که در سالهای اخیر از سوی دولت‌ها، گروه‌ها و افراد مورد استفاده قرار گرفته و خسارات جبران‌ناپذیری به تأسیسات حیاتی سایر کشورها وارد کرده است. در سال ۲۰۱۲ کرم مخرب «استاکس‌نت»<sup>۱</sup> رایانه‌های صنعتی مورد استفاده در فرایند غنی‌سازی اورانیوم در سایت هسته‌ای نطنز را مورد حمله قرار داد و باعث خسارت فراوان در این سایت شد. در اواخر ماه مه ۲۰۱۲ رسانه‌های آمریکایی اعلام کردند که ساخت استاکس‌نت به صورت مستقیم به دستور اوباما رئیس‌جمهور آمریکا طراحی شده است. در تاریخ ۷ ژوئیه سال ۲۰۱۳ میلادی، «ادوارد اسنودن» در مصاحبه‌ای با اسپیکل اعلام کرد این بدافزار با همکاری مشترک آژانس امنیت ملی ایالات متحده آمریکا و اسرائیل ساخته شده است.

### چارچوب نظری تحقیق

در زمینه نقش رسانه‌های نوین در گسترش تروریسم سیاسی، فرهنگی و مذهبی و در راستای فهم پیوند و تأثیر ایدئولوژی‌ها و گفتمان‌های گوناگون و رسانه می‌توان به

---

1. Stuxnet

نظریاتی که تأثیر پیام را بررسی می‌کنند اشاره کرد. دسته نخست از این نظریات که به نظریه تزریقی مشهور هستند؛ بر این باورند که پیام‌های ارتباطی با عناوینی چون نظریه گلوله رسانه‌ای و ارتباط جمعی تأثیرات قدرتمند و یک‌سانی بر مخاطبان‌شان می‌گذارند (سورین<sup>۱</sup> و تانکارد<sup>۲</sup>، ۱۳۸۱). گویی این پیام‌ها کلمه‌به‌کلمه در ذهن مخاطب نقش می‌بندد و احساسات و کنش‌های مطلوب آن رسانه و ایدئولوژی حامی آن را در مخاطب ایجاد می‌نماید (عیوضی، ۱۳۸۸: ۱۶۳). ویژگی اصلی این نظریات این است که در آن سوژه یا مخاطب به صورت کامل در برابر پیام و ایدئولوژی رسانه‌ای منفعل در نظر گرفته می‌شود. دسته دوم نظریات تأثیر مستقیم و فعال رسانه‌ها بر مخاطبان را نفی نموده و در فرایند تأثیرگذاری بر عوامل واسطه‌ای تأکید دارند. کلاپر در اثر خود با عنوان «اثرات ارتباط جمعی» نظریه اثر محدود رسانه‌ها را صورت‌بندی می‌کند و اثر محدود رسانه را تابع خواست مخاطب قرار می‌دهد و برای مخاطب نقش فعال قائل است. نظریه استفاده و رضایت‌مندی نیز مخاطب را در مواجهه با رسانه و پیام‌های رسانه‌ای فعال در نظر می‌گیرد که فعالانه پیام‌ها را تحلیل می‌کند (بارکر<sup>۳</sup>، ۱۳۸۷: ۵۸۷). از نظر هال، مخاطب می‌تواند به قرائتی متفاوت از پیام دست یابد. علاوه بر این، رسانه‌ها پیام‌ها و تصاویر مشترک را میان مردمی به‌وجود می‌آورند که به جهت فضا و زمان بسیار از هم دورند و رسانه این پیام‌ها را در قالب بمباران‌های فرهنگی منتشر می‌کنند و طیف عظیمی از مخاطبان را فارغ از بعد مکانی تحت تأثیر قرار می‌دهند (هال<sup>۴</sup>، ۱۹۹۵: ۴۴۴). به علاوه در راستای بیان پیوند میان رویکردهای سلفی جهادی به‌مثابه ایدئولوژی و رسانه می‌توان به ادبیات نظری و لویی التوسر فیلسوف اجتماعی فرانسه اشاره کرد. از نظر آلتوسر کارکرد اصلی ایدئولوژی، سوژه‌سازی است «ایدئولوژی رابطه تخیلی افراد را با شرایط واقعی هستی‌شان بازنمایی می‌کند» (آلتوسر، ۱۳۸۶: ۵۷). در واقع می‌توان رسانه را به سان جان فیسک (۱۳۸۱) در

---

1 Severin

2 Tankard

3 Barker

4 Hall

راستای فرایند استیضاح و سوژه‌سازی مورد مطالعه قرار داد. به‌عنوان مثال می‌توان استدلال نمود که گروه‌های سلفی جهادی از طریق تبلیغات رسانه‌ای مسلمانان غیر جهادی را فرامی‌خوانند و یا استیضاح می‌کنند و ذیل این فراخواندن و تقبل مخاطب، آنان را در ایدئولوژی خود به‌سوژه تروریست جهادی تبدیل می‌کنند. در همین راستا می‌توان به عوامل نظری در کاربرد رسانه توسط گروه‌های سلفی جهادی اشاره کرد که به موجب آنها مخاطبان به‌سوی این گروه‌ها جذب می‌شوند. رسانه‌ها قادرند از طریق انتقال ارزش‌ها و رسوخ ایدئولوژی مسلط، نقش تأثیرگذاری را در شکل دهی به آگاهی عمومی ایجاد کنند و الهام‌بخش تفکر و رفتار اجتماعی سازگار با تفکر حاکم باشند (لال<sup>۱</sup>، ۱۳۸۹: ۲۹). همچنین رسانه‌ها با تصویرسازی و جهت‌دهی به تصویرهای ذهنی، به تولید و انتقال اطلاعات و معنا از طریق استفاده از نشانه‌ها (مانند تصویر و کارهای هنری) به‌عنوان ابزارهای سودمند انتقال نماد و حامل‌های معنایی مبادرت می‌ورزند (کوپلی<sup>۲</sup>، ۱۹۹۴: ۷). عمده بررسی‌ها نشان می‌دهد که سلفی جهادی‌ها در عرصه به‌کارگیری رسانه به‌طور مداوم دارای تطور و تحول هستند و به‌شیوه‌ای هوشمندانه در راستای جلب نظر و پیگیری اهداف خشونت‌آمیز خود توانسته‌اند از ظرفیت رسانه بهره‌برداری نمایند. بدین روی سنجش عملکرد رسانه‌های آنها همواره محل توجه حوزه مطالعات امنیت بین‌الملل بوده است.

یکی از کارکردهای مهم رسانه‌های نوین در عصر حاضر که مبتنی بر عنصر اطلاعات هستند تأثیر آن بر گفتمان‌های امنیتی (سخت‌افزارگرا و نرم‌افزارگرا) در نظام بین‌الملل است. جوزف نای<sup>۳</sup> در سال ۲۰۰۲ در مقاله‌ای با عنوان قدرت سخت و قدرت نرم در عصر اطلاعات ضمن برشمردن ویژگی‌های عصر اطلاعات و گسترش رسانه‌های جمعی و فردی برای انتقال و تبادل سریع و ارزان اطلاعات، معتقد است که به‌دلیل تفاوت گسترده‌بازیگران بین‌المللی و کشورها در زمینه‌های توسعه‌ای و تکنولوژیک همچنان ترکیبی از قدرت

1 Lal

2 Kopley

3 Joseph Nye

سخت، قدرت اقتصادی و قدرت نرم البته با میزان درجه متفاوت وجود دارد (نای، ۲۰۰۲: ۱۵۱-۱۵۳). او در سال ۲۰۰۴ از قدرت سومی یاد می‌کند، ترکیبی از دو قدرت نرم و سخت یا هوشمند که در سیاست خارجی دولت‌ها نقش راهبردی دارد (نای، ۱۳۹۲: ۲۹). نای در سال ۲۰۱۴ در مقاله‌ای با عنوان انقلاب اطلاعات و قدرت از اطلاعات و ارتباطات به‌عنوان یکی از منابع قدرت نرم بسیار مهم در فضای بین‌الملل یاد می‌کند که کنترل جریان اطلاعات و مدیریت آن علاوه بر تقویت قدرت باعث ورود بازیگران جدید غیر دولتی در صحنه معادلات جهانی شده است (نای، ۲۰۱۴). نگاه نای بر قدرت فناوری‌های نوین بر مبنای نگرش فرارنالیستی است که امروزه نمود آن در عملکرد دولت‌های قدرتمند جهانی قابل مشاهده است. اگرچه نگاه نای به قدرت سخت به‌عنوان یک نتولیرال ناشی از نگاه اندیشمندان رئالیست به حوزه قدرت، توانایی و عملگرایی است، اما وی نیم‌نگاهی هم به استفاده از منابع قدرت سخت، مانند اقتصاد به‌عنوان مکمل‌های توانایی محور و نرم‌افزارانه دارد.

قدرت هوشمند از سه بعد مادی، مجازی و معنوی تشکیل شده است؛ فناوری‌های حساس برای تولید و بازپروری مواد، ساخت و تبدیل کالاهای استراتژیک در حوزه‌های نظامی، زیست‌محیطی و اقتصادی منابع سخت افزاری ابزارهای مادی قدرت هوشمند هستند (فتاحی اردکانی، ۱۳۹۷: ۱۳۳-۱۳۰). ابزارهای مجازی قدرت هوشمند، شامل پردازش، ذخیره و انتقال اطلاعات است. تمامی مؤلفه‌های قدرت مجازی در حوزه‌های ارتباطات و اطلاعات، امکان بسیج و منعکس‌سازی قدرت هنجاری یک کشور در حوزه‌های جغرافیایی دوردست را فراهم می‌سازد (گلدبرگر، ۱۹۹۵: ۱۹). قدرت هوشمند از طریق عقلانیت ماهوی در صدد کنترل روح، احساس و درک جوامع دیگر است. البته هر یک از این مؤلفه‌ها نیازمند شاخص‌های معطوف به تأثیرگذاری و کنترل پویایی محیط درونی سایر



کشورها است (متقی، ۱۳۷۸: ۱۵). از نظر نای با توجه به ورود بازیگران جدید نظیر دولت‌ها، سازمان‌ها و شرکت‌های بین‌المللی و گروه‌های سازمان‌یافته تروریستی در محیط پر آشوب بین‌المللی، قدرت هوشمند توانایی راهبری و مدیریت دیگر منابع قدرت را در اختیار رهبران یک نظام سیاسی قرار می‌دهد. علی‌رغم تلاش‌های نای در اثبات و تبدیل‌شوندگی قدرت و عوض شدن ساحت اعمال قدرت‌ها و پیش‌بینی عدم کارایی منابع سنتی و سخت قدرت شاهد وقوع جنگ‌های ویرانگر و تلاش‌های دولت‌های قدرتمند همچون آمریکا و روسیه در به‌کارگیری فناوری‌های جدید برای نوسازی و تولید نسل جدید سلاح‌های هسته‌ای هستیم (فتاحی اردکانی، ۱۳۹۷: ۱۵۰). استفاده گسترده آمریکا از سلاح‌های پیشرفته نظامی مبتنی بر فناوری‌های ارتباطات و اطلاعات در لشکرکشی به خاورمیانه و استفاده از آنها در تخریب زیرساخت‌های حیاتی اقتصادی سوریه، عراق و افغانستان و ترور شخصیت‌های برجسته در این مناطق نظیر رویداد «ترور سردار سپهد قاسم سلیمانی فرماندهی نیروی قدس سپاه پاسداران انقلاب اسلامی ایران و سردار ابومهدی المهندس جانشین فرماندهی حشدالشعبی عراق در ۱۳ دیماه ۱۳۹۸ در فرودگاه بغداد» (خبرگزاری جمهوری اسلامی ایران، ۱۳۹۸)، ضمن تضعیف دیدگاه‌های خوش‌بینانه در تحکیم قدرت نرم به‌عنوان رویکرد مسلط در نزاع بین کشورها، نشان داد نسل نوین تسلیحات نظامی مبتنی بر فناوری‌های ارتباطی و اطلاعاتی در گفتمان‌های امنیتی و سیاسی نظام بین‌الملل نقش ایفاء می‌کنند.

### روش‌شناسی تحقیق

پژوهش حاضر از نظر کنترل شرایط پژوهش، یک بررسی پیمایشی به‌شمار می‌رود که با استفاده از پرسشنامه محقق‌ساخته در زمستان سال ۱۳۹۷ در سطح کشور اجرا شده است. جامعه آماری آن متشکل از نخبگان (اساتید رشته‌های علوم انسانی «نظیر ارتباطات، جامعه‌شناسی، علوم ارتباطات، روانشناسی، علوم سیاسی و ...»، مدیران، صاحب‌نظران و کارشناسان

خبره رسانه) است و حجم نمونه به روش نمونه‌گیری خوشه‌ای سیستماتیک بر اساس جدول مورگان ۳۷۹ نفر برآورد گردید و در راستای افزایش ضریب دقت، حجم نمونه به ۴۰۲ نفر افزایش یافت. این پژوهش به شیوه توصیفی-تحلیلی و با روش کمی صورت گرفته است. همچنین جهت تجزیه و تحلیل یافته‌های تحقیق از آماره‌های توصیفی (فراوانی، درصد، میانگین، انحراف معیار، واریانس) و آماره‌های تحلیلی (رگرسیون و تحلیل عاملی) استفاده گردید. در این تحقیق رابطه فناوری‌های نوین ارتباطی با تمرکز بر شبکه‌های ماهواره‌ای، اینترنت و فضای مجازی به‌عنوان متغیر مستقل با گسترش قدرت تروریسم به‌عنوان بازیگری جدید در عرصه بین‌الملل به‌عنوان متغیر وابسته بررسی شد. برای دست‌یابی به نتایج معتبر و امکان هرچه بیشتر مقایسه سنجه‌ها، جنبه‌های مختلف فناوری مانند: شبکه‌های ماهواره‌ای پخش صدا و تصویر، اینترنت، فضای مجازی، شبکه‌های اجتماعی تحت وب و موبایلی، وبسایت‌ها، بلاگ‌ها، موتورهای جستجوگر و روزنامه‌نگاری الکترونیک و نقش هریک بر متغیر تروریسم بررسی شد. پس از استخراج داده‌ها به کمک نرم‌افزار آماری SPSS نسخه ۲۲ نسبت به تجزیه و تحلیل داده‌ها اقدام گردید. پرسش‌نامه پژوهش حاضر حاوی ۳۰۱ پرسش است که براساس طیف لیکرت از بسیار کم تا بسیار زیاد (۵= بسیار کم، ۴= کم، ۳= تاحدودی، ۲= زیاد، ۱= بسیار زیاد) اندازه‌گیری شده است.

### یافته‌های تحقیق

اکثریت پاسخگویان، میزان تحصیلات خویش را در حد فوق لیسانس عنوان داشته‌اند (۶۱/۴ درصد). در عین حال ۲۵/۴ درصد نیز دارای مدرک تحصیلی لیسانس و ۱۳/۲ درصد دیگر نیز دارای مدرک تحصیلی دکترا هستند. اکثریت نسبی پاسخگویان، رشته تحصیلی خویش را علوم ارتباطات (۱۸/۹ درصد) و خبرنگاری (۱۸/۴ درصد) عنوان داشته‌اند. ضمن آنکه ۱۶/۹ درصد از آنان نیز پژوهشگری را به‌عنوان رشته تحصیلی عنوان نمودند. از نظر وضعیت استان محل خدمت شرکت‌کنندگان، (۱۶ استان)، اکثریت نسبی

پاسخگویان را شاغلین در استان تهران به خود اختصاص داده‌اند (۴۶/۸ درصد). همچنین شاغلین در استان‌های گیلان، هرمزگان و قزوین هر کدام به ترتیب با ۹ درصد، ۸/۵ درصد و ۶/۵ درصد، در رتبه‌های بعدی قرار گرفته‌اند. تحقیق حاضر در پی شناخت نقش فن‌آوری‌های نوین ارتباطی در گسترش قدرت تروریسم و ظهور گروه‌های تروریستی به‌عنوان بازیگرانی جدید در عرصه بین‌المللی است. نتایج حاصل از توصیف ویژگی‌های نمونه مطالعه نشان می‌دهد که بیشتر پاسخگویان (۶۰/۲ درصد) از نظر جنسیت، مرد هستند. ۶۰/۷ درصد پاسخگویان در گروه سنی ۳۰-۴۹ سال واقع شده‌اند. 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 داشته‌اند. اکثریت نسبی پاسخگویان ساکن استان تهران (۴۶/۸ درصد)، گیلان (۹ درصد)، هرمزگان (۸/۵ درصد) و قزوین (۶/۵ درصد) بودند. از نظر اکثریت پاسخگویان در حد متوسط به بالایی (زیاد)، رسانه‌های نوین بر گسترش تروریسم و ظهور گروه‌های تروریستی به‌عنوان بازیگرانی جدید در عرصه روابط بین‌الملل تأثیرگذار است.

### آزمون فرضیه تحقیق

رسانه‌های نوین در گسترش قدرت تروریسم و ظهور گروه‌های تروریستی به‌عنوان بازیگرانی جدید در عرصه بین‌المللی مؤثر است.

به‌منظور بررسی این فرضیه تحقیق و در راستای شناسایی مولفه‌های رسانه‌های نوین مؤثر بر گسترش قدرت تروریسم و ظهور گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه بین‌المللی از روش توصیفی و تحلیل عاملی استفاده شد که در ادامه نتایج تحلیل ذکر می‌شود.

### جدول شماره ۱. بررسی توصیفی گروه‌های تروریستی

مجموع عددی	آمارهای توصیفی			درصد					مولفه
	واریانس	انحراف معیار	میانگین	بسیار زیاد	زیاد	متوسط	کم	بسیار کم	
۱۴۶۸	۰/۷۸۰	۰/۸۸۲۹۷	۳/۷۲	۱۹/۸	۴۱/۱	۳۲	۶/۱	۱	شبکه‌های ماهواره‌ای
۱۵۰۶	۰/۶۳۵	۰/۷۹۶۷۲	۳/۸۴	۲۱/۴	۴۴/۹	۳۰/۱	۳/۶		فضای مجازی
۱۴۴۰	۰/۹۲۶	۰/۹۶۲۴۷	۳/۶۷	۲۱/۹	۳۵/۲	۳۲/۷	۸/۷	۱/۵	شبکه‌های اجتماعی
۱۳۷۲	۰/۸۲۴	۰/۹۰۷۴۹	۳/۵۰	۱۳/۸	۳۵/۷	۳۸/۸	۱/۲	۱/۵	اینترنت
۱۲۶۲	۰/۸۸۸	۰/۹۴۲۲۴	۳/۲۲	۷/۷	۳۲/۱	۳۷/۲	۱/۴	۲/۶	روزنامه نگاری سایر
۱۴۳۲	۰/۵۵۳	۰/۷۴۳۸۷	۳/۶۰	۹/۵	۳۶/۷	۳۷/۷	۵	۱	میانگین (جمع)

نتیجه آمار توصیفی در خصوص مولفه گروه‌های تروریستی نشان می‌دهد که میانگین پاسخ‌ها برای تمامی مولفه‌ها در حد متوسط به بالا (زیاد) است. در عین حال پایین‌ترین میانگین متعلق به روزنامه‌نگاری سایبری (میانگین پایین ۳/۲۲ و انحراف معیار ۰/۹۴۲۲۴) و بالاترین آن مربوط به فضای مجازی (میانگین متوسط ۳/۸۴ و انحراف معیار ۰/۷۹۶۷۲) است. در عین حال میانگین کلی مولفه گروه‌های تروریستی برابر با ۳/۶۰، انحراف معیار برابر با ۰/۷۴۳۸۷، واریانس برابر با ۰/۵۵۳ و مجموع عددی معادل ۱۴۳۲ است. با نظر به مطالب فوق، می‌توان چنین عنوان نمود که از نظر پاسخگویان در حد متوسط به بالایی (زیاد)، فن‌آوری‌های نوین ارتباطی بر ظهور گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه روابط بین‌الملل تأثیرگذار است. با توجه به تعدد جداول در روش تحلیل عاملی و محدودیت مقاله به ذکر دو جدول پایه و خروجی نهایی بسنده می‌شود.

### جدول شماره ۲. نتیجه آزمون بارتلت

شاخص کفایت نمونه توسط آزمون کایزر. مایر و اولکین		<b>.919</b>
آزمون کروی بودن بارتلت	تقریب کی دو	<b>14722,714</b>
	درجه آزادی	<b>820</b>
	ضریب همبستگی	<b>.000</b>

نتایج جدول شماره ۱، بیانگر نتیجه آزمون بارتلت که تقریبی از آماره کای دو است، نشان داده است، مقدار sig (ضریب همبستگی) آزمون بارتلت، کوچک‌تر از ۵ درصد است (۰/۰۰۰) و مبین این نکته است که تحلیل عاملی برای شناسایی ساختار، مدل عاملی، مناسب است و فرض شناخته شده بودن ماتریس همبستگی رد می‌شود. همچنین شاخص KMO با مقدار ۰/۹۱۹ در ابتدای این جدول آمده است و به دلیل آن، مقدارش نزدیک به یک است، تعداد نمونه (تعداد پاسخ‌دهندگان) برای تحلیل عاملی کافی است.

### جدول شماره ۳. تحلیل عاملی ماتریس اجزاء

گویه‌های تحقیق	۱	۲	۳	۴	۵	۶	۷	عامل‌ها:
								۱: فضای مجازی ۲. شبکه‌های اجتماعی تحت وب و موبایلی ۳. روزنامه نگاری سایبری ۴. شبکه‌های ماهواره‌ای (عام) ۵. اینترنت ۶. شبکه‌های ماهواره‌ای، فضای مجازی، شبکه‌های اجتماعی و اینترنت (دولت ایران) و ۷. شبکه‌های ماهواره‌ای (خاص).
ابزار تروریسم دولتی برای هدایت خشونت سازمان یافته است.	1	.245	.119	.074	.776	.230	.103	-.045
فضای مناسب برای دخالت تروریست‌ها در امور کشورها است.	2	.242	.157	.096	.806	.141	.169	.081
دامنه آسیب‌پذیری در شبکه‌های ماهواره‌ای بسیار گسترده است.	3	.090	.037	-.041	.216	.014	-.012	.689
در معرفی سازمان تروریسم به‌عنوان بعدی از قدرت نقش دارد.	4	.304	.202	.133	.740	.122	.060	.025

درجذب منابع مالی برای گروه‌های تروریستی نقش دارند.	5	.316	.289	.119	.725	.103	.060	.232
از منابع تروریست‌های مخالف جمهوری اسلامی ایران است.	6	.266	.239	.190	.783	.132	.016	.073
ایران در مقابل تروریسم از شبکه‌های ماهواره‌ای استفاده می‌کند.	7	.311	.252	.032	.661	.206	-.009	.206
تروریست‌ها از این فضا علیه تأسیسات حیاتی اقدام می‌کنند.	8	.162	.035	.229	.348	-.102	.538	-.055
دامنه آسیب‌پذیری عمومی در فضای سایبر بسیار گسترده است.	9	.685	.136	.076	.317	.286	.075	-.182
بستر مناسب برای تبلیغ عقاید و برنامه‌های تروریستی است.	10	.693	.214	.067	.393	.152	-.019	-.143
ابزار تروریسم دولتی برای هدایت خشونت سازمان یافته است.	11	.681	.206	.055	.348	.223	-.010	-.294
فضایی برای دخالت تروریست‌ها در امور داخلی کشورها است.	12	.781	.279	.180	.166	.186	.113	.119
در معرفی تروریسم به‌عنوان بعدی از قدرت نقش دارد.	13	.735	.255	.094	.227	.134	.115	.048
در جذب منابع مالی برای گروه‌های تروریستی نقش دارد.	14	.725	.308	.114	.109	.177	.059	.337
با برجسته‌سازی نماد وحشت در پیشبرد اهداف آنان موثر است.	15	.720	.208	.175	.274	.183	.103	.072
از این فضا برای تهدید علیه منافع کشور ایران استفاده می‌کنند.	16	.701	.222	.120	.223	.198	.127	.258
ایران از فضای مجازی برای مقابله با تروریسم استفاده می‌کند.	17	.652	.337	.149	.277	.108	.048	.038

ابزار توریسم دولتی برای هدایت خشونت سازمان یافته است.	18	.290	.115	.117	.071	.103	.789	-0.024
شبکه‌های اجتماعی بستر امن تبادل اطلاعات توریست‌ها است.	19	.353	.721	.127	.085	.194	.128	-0.104
برای جذب هوادار از سوی توریست‌ها می‌شود.	20	.296	.792	.168	.177	.145	.055	.013
بستر مناسب تبلیغ عقاید، اهداف و برنامه‌های توریستی است.	21	.241	.779	.190	.254	.137	-0.023	-0.136
ابزار قدرتمندی برای گسترش خشونت سازمان یافته است.	22	.232	.806	.195	.140	.182	.122	.083
در معرفی توریسم به‌عنوان بعدی از قدرت نقش دارد.	23	.195	.771	.159	.222	.275	.147	.058
با برجسته‌سازی نمادحشت در پیشبرد اهداف آنان موثر است.	24	.229	.750	.198	.204	.267	.057	.092
توریست‌ها از این بستر علیه منافع کشور ایران استفاده می‌کنند.	25	.280	.712	.115	.262	.248	.038	.167
استفاده از شبکه‌های اجتماعی راهبرد جمهوری اسلامی است.	26	.100	.452	.230	.189	.196	.623	-0.083
بستر مناسبی برای تبلیغ عقاید و برنامه‌های توریستی است.	27	.244	.383	.296	.120	.680	.035	.028
در جذب منابع مالی برای گروه‌های توریستی نقش دارد.	28	.189	.247	.325	.166	.650	.072	-0.040
ابزاری مؤثر برای جذب هوادار است.	29	.206	.303	.302	.136	.762	.044	-0.049
اینترنت فضای مناسب دخالت توریسم در امور کشورهاست.	30	.110	.100	.061	.091	.616	.070	-0.029

در معرفی سازمان تروریسم به عنوان بعدی از قدرت نقش دارد.	31	.230	.208	.371	.166	.721	.083	-0.001
سایت‌ها و وبلاگ‌ها ابزار گسترش خشونت سازمان یافته هستند.	32	.176	.151	.336	.184	.721	.171	.125
تروریست‌ها از این بستر علیه منافع ایران استفاده می‌کنند.	33	.252	.187	.328	.154	.661	-.057	.121
ایران از وبسایت و وبلاگ در تضعیف تروریسم استفاده می‌کند.	34	-.168	.015	.442	-.055	.200	.675	.119
در تحقق اهداف تروریسم دولتی در فضای سایبر نقش دارد.	35	.153	.167	.758	.167	.351	.036	-.011
در حمایت از برنامه‌های تبلیغاتی و عقاید تروریسم نقش دارد.	36	.132	.174	.726	.215	.363	.150	-.062
در معرفی سازمان تروریسم به عنوان بعدی از قدرت نقش دارد.	37	.095	.216	.820	.154	.235	.089	-.162
با برجسته‌سازی نماد وحشت در پیشبرد اهداف آنان موثر است.	38	.128	.158	.825	.084	.187	.188	.029
ابزار تروریسم دولتی برای هدایت خشونت سازمان یافته است.	39	.165	.154	.817	.075	.178	.161	.081
سلاح تبلیغی تروریسم علیه منافع جمهوری اسلامی ایران است.	40	.154	.238	.727	.107	.375	.074	-.040
ابزار ایران برای کاهش قدرت تروریسم در سطح جهانی است.	41	.003	.035	.695	-.076	.048	.510	.100

با توجه به نتیجه تحلیل عاملی روی ۴۱ متغیر مؤثر بر ایجاد گروه‌های تروریستی در عرصه بین‌المللی، هفت عامل زیر به عنوان عامل‌های اصلی شناسایی می‌شود.

۱- عامل فضای مجازی ۲- عامل شبکه‌های اجتماعی تحت وب و موبایلی ۳- عامل روزنامه‌نگاری سایبری ۴- عامل شبکه‌های ماهواره‌ای (عام) ۵- عامل موتورهای جستجوگر



(اینترنت) ۶- عامل شبکه‌های ماهواره‌ای، فضای مجازی، شبکه‌های اجتماعی و اینترنت (دولت ایران) ۷- عامل شبکه‌های ماهواره‌ای (خاص).

با نظر به نتایج تحلیل عاملی در جدول شماره ۳، در ارزیابی فرضیه تحقیق، چنین می‌توان انگاشت که با توجه به تجزیه و تحلیل اطلاعات فرضیه، (H1) مورد تأیید قرار گرفته و لذا فرضیه (H0) رد می‌شود. به عبارتی دیگر؛ هفت عامل شناسایی شده در بخش رسانه‌های نوین بر ظهور گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه بین‌الملل تأثیر گذارند. ضمن آنکه هفت عامل شناسایی شده، کمی بیش از ۷۳/۵ درصد از موضوع پژوهش را تبیین می‌کند. در عین حال از میان عوامل مورد بررسی، عامل فضای مجازی بیشترین سهم را در ظهور گروه‌های تروریستی به‌عنوان بازیگران جدید در عرصه بین‌الملل دارد.

## نتیجه‌گیری

پیدایش و گسترش فن‌آوری‌های نوین ارتباطی با آثار و تبعات زیادی در حوزه‌های سیاسی، اجتماعی، اقتصادی و... همراه بوده است که عمده‌ترین این آثار پیرامون موضوع تحقیق حاضر عبارتند از:

- ۱- گسترش حوزه نفوذ رسانه‌ها.
- ۲- ظهور و توسعه شبکه‌های اجتماعی.
- ۳- گسترش قدرت نرم از طریق فضای سایبری.
- ۴- تضعیف حاکمیت مرکزی و افول اقتدار دولت‌های ملی.
- ۵- گسترش قدرت مانور دولت‌ها در فضای سایبری.
- ۶- افزایش تهدیدات بین‌المللی.
- ۷- پیدایش ارتش‌های پنهان سایبری.
- ۸- گسترش قدرت تروریسم.

۹- ظهور گروه‌های تروریستی به‌عنوان بازیگرانی جدید در عرصه بین‌المللی.

۱۰- ظهور و توسعه نوع جدیدی از تروریسم؛ و ...

نتایج این مطالعه نشان داد رسانه‌های نوین بر گسترش قدرت تروریسم و ظهور گروه‌های تروریستی به‌عنوان بازیگرانی جدید در عرصه بین‌المللی تأثیرگذار است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و افراد با ورود به این فضا، زمینه تهدیدات سایبری را فراهم آورند. در این رابطه می‌توان به گروه افراطی القاعده اشاره کرد؛ از جمله سازمان‌های تروریستی که بعد از سقوط رژیم طالبان در اوایل سال ۲۰۰۰، اجرای بسیاری از فعالیت‌هایش را به بستر اینترنت و فضای مجازی منتقل نمود. همچنین گروه تروریستی داعش برای نشان‌دادن قدرت نظامی خود جدیدترین فیلم‌ها، اعلامیه‌ها و نشریات را در تالارهای گفت‌وگو و انجمن‌ها قرار داده و در شبکه‌های اجتماعی بازنشر می‌کنند. شواهد نشان می‌دهد با ورود به دهه دوم قرن بیست و یکم، تروریست‌ها اعم از دولتی و غیر دولتی بخش مهمی از فعالیت خود را به فضای مجازی منتقل کرده‌اند و با تحمل هزینه‌های پایین‌تر به نتایج قابل توجهی دست یافته‌اند.

مطابق یافته‌های جدول شماره ۳، از نظر پاسخگویان، فضای مجازی بستر مناسبی برای گسترش دامنه آسیب‌های عمومی، هدایت خشونت سازمان‌یافته از سوی دولت‌ها، دخالت سازمان‌های تروریستی در امور کشورها، معرفی سازمان‌های تروریستی به‌عنوان بعدی از قدرت، جذب کمک‌های مالی برای گروه‌های تروریستی به‌شمار می‌رود. بر این اساس، فضای مجازی، جایگزین فضای حقیقی و محیط مناسب برای فعالیت دشمنان علیه منافع جمهوری اسلامی ایران شده است و از سوی دیگر همین فضا فرصت مناسبی را برای دولت جمهوری اسلامی ایران فراهم کرده تا برای مقابله با تهدیدات تروریستی از آن بهره‌برداری نماید. این نتایج با نتایج مطالعات نورمحمدی (۱۳۸۹)، سلطانی نژاد (۱۳۹۵)، اریکسون و

گیاکملو (۲۰۰۷)، شاه علی و موحدیان (۱۳۹۱)، امراللهی (۱۳۹۴) و فتاحی (۱۳۹۰) همسو است.

نتایج تحقیق، مبین این نکته است که رسانه‌های نوین در گسترش قدرت تروریسم و ظهور گروه‌های تروریستی به‌عنوان بازیگرانی جدید در عرصه بین‌المللی نقش دارد. این رسانه‌ها با دگرگون کردن نوع تعاملات و ارتباطات، مفهوم قدرت را دگرگون ساخته‌اند؛ مفهوم قدرت از قدرت سخت به قدرت نرم یا از قدرت نظامی به قدرت فرهنگی و یا از قدرت اجبار به قدرت چانه‌زنی و هماهنگی تغییر یافته است. به عبارتی، گفتمان قدرت از حالت سخت به گفتمان نرم و فرهنگی یا اقناعی تغییر شکل داده است. گسترش قدرت تروریسم یکی از مباحث مهم در فضای سایبر است. تروریسم از جمله مفاهیمی است که به هنگام تعریف و مطالعه علمی، مناقشه برانگیز است و مطالعه آن در چارچوب بین‌رشته‌ای قرار می‌گیرد. لذا برای فهم و بررسی آن می‌بایست رویکرد بین‌رشته‌ای را به کار گرفت و آن را از دریچه علوم سیاسی، روابط بین‌الملل، حقوق بین‌الملل، روانشناسی، جامعه‌شناسی و مانند آن نگریست. تروریسم در مرحله متأخر آن و در گذار به قرن بیست و یکم، به تروریسم جهانی متحول شده و عامل این تحول، غیرسرزمینی شدن آن در روابط بین‌الملل است. جامعه‌شناسانی که روی گروه‌های تروریستی کار کرده‌اند، معتقدند که تروریسم بین‌الملل کنونی موج چهارم تروریسم در جهان و یا سوپر تروریسم است و از جمله ویژگی‌های متمایز کننده آن با سایرین استفاده گسترده از شبکه‌های مجازی و جذب افراد از سراسر جهان است. جان اریکسون و گیاکاملو اعتقاد دارند تحول و پیوند اطلاعات و فناوری به‌طور فزاینده‌ای دایره عملکرد شبکه‌های تروریستی را گسترش می‌دهد. در نظر دانش‌پژوهان روابط بین‌الملل و علوم سیاسی نیز گسترش فناوری‌های اطلاعات و ارتباطات عامل مهم تحول در مفهوم امنیت است. با تحول مفهوم امنیت، کشورهایایی چون ایالات متحده، اروپا، روسیه و چین، افرادی را در جهت کنترل، نظارت و تحلیل و تخمین ریسک‌ها و تهدیدات جامعه شبکه‌ای جهانی، استخدام می‌کنند. شورای مطالعات ملی

آمریکا بر این باور است که تروریست آینده بیش از آنکه با بمب تهدید کننده باشد با کیبورد تهدیدزا است. آنچه مسلم است؛ فضای مجازی (مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و سائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی) به‌عنوان جدیدترین پویا در تحول نظام سنتی بین‌المللی بستر ساز توسعه فعالیت‌های تروریسم بین‌المللی در شناسایی و عضویت، سازماندهی و تشکیلات و عملیات‌های تروریستی شده است. در جدیدترین و مهمترین موج تروریسم سایبری، این تروریست‌های تکفیری هستند که فضای مجازی را به‌عنوان گسترده‌ترین، ایمن‌ترین و راحت‌ترین عرصه فعالیت میدان گسترش فعالیت‌های ساختار شکنانه، فراحاکمیتی و ضد اقتدار بین‌المللی انتخاب کرده‌اند.

بررسی رویدادهای مختلف در دو دهه اخیر نشان می‌دهد، سهولت استفاده از روش‌های تروریستی در فضای مجازی و تنوع، مخفی بودن و کم‌هزینه بودن آن در مقایسه با روش‌های سنتی بر علاقه حامیان تروریسم مجازی دولتی برای استفاده از این روش برای مقابله با جمهوری اسلامی افزوده است. حمله سایبری به تأسیسات هسته‌ای ایران در نطنز، تداوم این حملات به شبکه‌های رایانه‌ای وزارت نفت و سپس وزارت علوم، تحقیقات و فناوری جمهوری اسلامی ایران نشان می‌دهد استفاده از زیرساخت‌های اینترنتی و فضای سایبر برای حمله به تأسیسات حیاتی کشور به شدت مورد توجه کشورهای متخاصم به‌ویژه آمریکا و اسرائیل است.

با نظر به یافته‌های تحقیق که بر نقش رسانه‌های نوین در ظهور و گسترش تروریسم در عرصه روابط بین‌الملل تأکید داشته و با نظر به اقدامات رو به تزاید تروریسم سایبری، موارد زیر پیشنهاد می‌شود:

- زیرساخت‌های فنی مقابله با حملات تروریستی در فضای سایبر ایجاد گردد.
- راهکارهای مقابله با آن در فضای داخلی و بین‌المللی مورد بررسی قرار گیرد.

- چگونگی دفاع از منافع کشور در محافل بین‌المللی با استفاده از ماده ۵۱ حقوق بین‌الملل که دفاع مشروع کشورها در موقعیت تجاوزات خارجی را مورد تأیید قرار می‌دهد بررسی شود.

- با توجه به اینکه فضای سایبر، بستر مناسبی برای انواع تروریسم اعم از اقتصادی، بیوتروریسم، نظامی با تخریب زیرساختهای حیاتی، تروریسم فردی و... است، ضرورت دارد نه تنها سازمان‌های دولتی به دانش و اطلاعات لازم برای مقابله با فعالیت‌های تروریستی مجهز شوند بلکه عموم مردم، خانواده‌ها، دانش‌آموزان و دانشجویان با جنبه‌های متفاوت تروریسم سایبری به صورت علمی و تخصصی آشنا شوند.

- نتایج مطالعات انجام شده در داخل و خارج از کشور تجربیات زی‌قیمتی هستند که نقش فناوری‌های نوین ارتباطی به طور خاص اینترنت و فضای مجازی را در تحولات سیاسی و اجتماعی و جابجایی دولت‌ها به خوبی آشکار می‌سازند. این تحولات بسیاری از کشورها را بر آن داشته تا در سیاست‌هایشان در مواجهه با فضای مجازی تجدید نظر کنند و با تدوین استراتژی جدید چگونگی بهره‌برداری از این ابزار را در حوزه‌های داخلی و خارجی مشخص نمایند. لذا با توجه به شرایط خاص جمهوری اسلامی ایران و تهدیدات مستمر ضرورت بازنگری و بهره‌برداری از تمامی ظرفیت‌های اینترنت و فضای مجازی در حوزه‌های سیاسی، اجتماعی، فرهنگی و اقتصادی و همچنین حفاظت از دست‌آوردهای معنوی انقلاب در مقابل جنگ نرم فرهنگی که رسانه‌های نوین ابزار مؤثر آن به شمار می‌روند، ضروری است.

- مدیریت آی.تی در کشور جمهوری اسلامی ایران کم‌وبیش نوپا بوده و تحت تأثیر جریان‌های سیاسی و عدم تمرکز مدیریتی و تصمیم‌گیری در مواجهه صحیح با جنبه‌های مختلف این پدیده از کشورهای دیگر عقب‌مانده است. از این رو بررسی بنیادی و سیستماتیک نقش فناوری‌های نوین ارتباطی در تغییرات و تحولات منطقه، همچنین بازنمایی و توصیف آثار مختلف این فناوری از زبان کارشناسان و دست‌اندرکاران در نقاط

مختلف کشور می‌تواند در تصمیم‌گیری‌ها و برنامه‌ریزی‌های کاربردی متولیان کشور، نقش سازنده‌ای ایفاء کند.

همچنین پیشنهاد می‌شود در گام اول با پذیرش مقوله اینترنت و فضای مجازی به‌عنوان ابزاری قدرتمند با قابلیت خلق تحولات و تغییرات در حیات بشر، زیرساخت‌های فعلی را در سطوح وسیع‌تر گسترش داده و زمینه دسترسی مردم در سراسر کشور به آن فراهم شود. در گام دوم برای جلوگیری از نفوذ بیگانگان نظیر وقایع انتخابات سال ۱۳۸۸ از سوی آمریکا و انگلیس کشور را به اینترنت ملی مجهز نمایند.

در گام سوم برای واکسینه کردن جامعه در برابر انواع تهدیدات سایبری، آموزش‌های عمومی و تخصصی را تحت عنوان سواد رسانه‌ای را از طریق رسانه‌ها، مدارس و دانشگاهها و عموم مردم توسعه ببخشند.

و در گام بعدی برای مقابله با جنگ نرم و تهاجمات مدون و برنامه‌ریزی شده دشمن به تقویت سازمانها و گروههای فعال داخلی در این عرصه همت گمارند.

## منابع

- (۱) آرایش، حسن؛ بابایی پهنه کلایی، سید حسین و فرضعلی سالاری سردری، فرضعلی (۱۳۹۷). «هجمه تروریسم؛ تاوان هویت تحول خواه نظام جمهوری اسلامی ایران»، فصلنامه راهبرد سیاسی، سال ۲، شماره ۶، پاییز، صص ۹۹-۱۱۵.
- (۲) 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 ۴، شماره ۱۳، صص ۳۲۵-۲۹۴.
- (۳) آلبرس، دیوید، پاپ، دانیل (۱۳۸۵). گزیده ای از عصر اطلاعات، ترجمه علی‌علی‌آبادی، رضا نخجوانی، تهران: پژوهشکده مطالعات راهبردی.
- (۴) آلتوسر لویی (۱۳۸۶). ایدئولوژی و سازو برگ‌های ایدئولوژیک دولت، ترجمه روزبه صدر آرا، تهران: نشر چشمه.
- (۵) بارکر، کریس (۱۳۸۷). مطالعات فرهنگی نظریه و عملکرد، تهران: پژوهشکده مطالعات فرهنگی و اجتماعی.
- (۶) امراللهی بیوکی، مهدی (۱۳۹۴). سلاح‌های سایبری، الگوهای جاسوسی، شنود و رصد، بررسی و پیاده‌سازی موردی در بدافزارهای بانکی، پایان‌نامه کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه قم.
- (۷) تافلر، الوین (۱۳۷۰). جابجایی قدرت، ترجمه شهیندخت خوارزمی، تهران: نشر نو.
- (۸) خلیلی پور رکن آبادی، علی و نورعلی وند، یاسر (۱۳۹۱). «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، فصلنامه مطالعات راهبردی، سال ۱۵، شماره ۵۶، صص ۱۶۸-۱۹۹.
- (۹) دودینگک، کیت (۱۳۸۰). قدرت، ترجمه عباس مخبر، تهران: نشر آشیان.
- (۱۰) روزنا، جیمز (۱۳۹۰). انقلاب اطلاعات، امنیت و فناوری های جدید، ترجمه علی‌رضا طیب، تهران: پژوهشکده مطالعات راهبردی.
- (۱۱) سلطانی نژاد، احمد؛ جمشیدی، محمد حسین و پوردست، زهرا (۱۳۹۵). «دگرگونی مفهوم قدرت در پرتو فناوری نوین اطلاعاتی-ارتباطی»، دوفصلنامه دانش سیاسی، سال ۱۲، شماره ۱، صص ۷۳-۹۸.
- (۱۲) سورین، ورنر؛ تانکارد، جیمز دبلیو (۱۳۸۱). نظریه‌های ارتباطات، ترجمه علیرضا دهقان، تهران: انتشارات دانشگاه تهران.
- (۱۳) سیمبر، رضا (۱۳۹۴). مقدمه ای بر تروریسم سایبری و امنیت دیجیتال، گیلان: انتشارات دانشگاه گیلان.
- (۱۴) شاه علی، احمد رضا و موحدیان، احسان (۱۳۹۱). «تروریسم دولتی در فضای مجازی و راهکارهای مقابله با آن»، فصلنامه رسانه، سال ۲۳، شماره ۲، صص ۲۵-۴۶.

- ۱۵) صدرپور، سید امیرحسین؛ جمشیدی، محمدحسین و اسلامی، محسن (۱۳۹۵). «بررسی ساز و کار نوین دیپلماسی عمومی بر مبنای نظریه قدرت نرم جوزف نای» دوفصلنامه مطالعات قدرت نرم، دوره ۶، شماره ۱، صص، ۱۵۲-۱۳۰.
- ۱۶) عامری، هوشنگ (۱۳۹۱). اصول روابط بین الملل، ویراست ششم، تهران: نشر آگه.
- ۱۷) عبدی، مهدی (۱۳۹۵). تروریسم سایبری علیه ایران. کنفرانس ملی شرق شناسی، تاریخ و ادبیات پارسی، پایگاه مرکز اطلاع رسانی جهاد دانشگاهی .
- <https://www.sid.ir/Fa/Seminar/ViewPaper.aspx?ID=۲۴۰۰۲>
- ۱۸) عیوضی، محمدرحیم (۱۳۸۸). «تأثیر رسانه‌ها بر رفتار انتخاباتی» فصل‌نامه پژوهش‌های ارتباطی، شماره ۱۶ دوره ۱، صص ۱۷۴-۱۵۷.
- ۱۹) فتاحی اردکانی، محسن، مسعودنیا، حسین و امام جمعه زاده، سیدجواد (۱۳۹۷). «تحلیل مفهوم قدرت و منابع تشکیل‌دهنده آن از دیدگاه جوزف نای» دوفصلنامه مطالعات قدرت نرم، دوره ۸، شماره ۱۸، صص، ۱۵۲-۱۳۰.
- ۲۰) فتاحی، محبوبه (۱۳۹۰). نقش آفرینی جمهوری اسلامی ایران و تروریسم در نظام بین‌الملل (بعد از ۱۱ سپتامبر)؛ راهبردها و رویکردها، پایان‌نامه کارشناسی ارشد علوم سیاسی، دانشگاه گیلان.
- ۲۱) فیسک، جان (۱۳۸۱). «فرهنگ و ایدئولوژی»، ترجمه مژگان برومند، فصلنامه ارغنون، وزارت فرهنگ و ارشاد اسلامی، شماره ۲۰.
- ۲۲) لال، جیمز (۱۳۷۹). رسانه‌ها، ارتباطات، فرهنگ: رهیافتی جهانی، ترجمه: مجید نکو دوست، تهران: روزنامه ایران.
- ۲۳) میربد، لیلا، سلیمی، صادق، نیاورانی، صابر و زمانی، سیدقاسم. (۱۳۹۸). «تروریسم سایبری، نقض حقوق بشر و آزادی‌های بنیادین» فصلنامه حقوق پزشکی، ویژه‌نامه حقوق بشر و حقوق شهروندی، شماره شش، صص، ۲۴۰-۲۲۴.
- ۲۴) 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.
- ۲۵) ناجی راد، محمدعلی (۱۳۸۷). جهانی شدن تروریسم، چاپ اول، تهران: دفتر مطالعات سیاسی و بین‌المللی وزارت امور خارجه.
- ۲۶) نای، جوزف (۱۳۸۷). قدرت در عصر اطلاعات، از واقع‌گرایی تا جهانی شدن، ترجمه سعید میرترابی، تهران: پژوهشکده مطالعات راهبردی.
- ۲۷) نای، جوزف (۲۰۱۰). قدرت نرم و دیپلماسی عمومی در قرن ۲۱، سخنرانی جلسه آغازین پارلمانی شورای انگلستان، ۲۰ ژوئن ۲۰۱۰، برگرفته از سایت استراتژیک رویو.



- ۲۸) نایار، پرامودکی (۱۳۹۴). درآمدی بر رسانه‌های نوین و فرهنگ‌های مجازی، ترجمه سعیدرضا عاملی و گوادرز میرزایی، تهران: انتشارات سروش.
- ۲۹) نورمحمدی، مرتضی (۱۳۸۹). گسترش فناوری‌های اطلاعات و ارتباطات و تحول پدیده امنیت، پایان‌نامه دکترای تخصصی، دانشگاه علامه طباطبائی.
- ۳۰) 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.
- 31) Ali, Mah- Rukh. (2015). ISIS and Propaganda: How ISIS Exploits Women, Reuters Institute for the Study of Journalism (University of Oxford).
- 32) Arendt, Hannah. (1972). "On Violence", in: Crises of the Republic, New York: Harcourt, Brace Jovanovich.
- 33) Barry, Collin. (1997). "The Future of Cyber terrorism", Crime and Justice International Magazine, Vol.13, :- Edward Snowden says motive behind leaks was to expose 'surveillance state'. From The [https://en.wikipedia.org/wiki/Edward\\_Snowden](https://en.wikipedia.org/wiki/Edward_Snowden), 4,1.
- 34) Eriksson, Johan and Giacomello, GiamPiero, International Relations and Security in the Digital Age: London, Rutledge, 2007, PP251.
- 35) Goldberger, Marnin. (1995). Reserch- Dokorate Programs, Washington, D.C, National Academy Press.
- 36) Hall, stuart (1995), The local and the global: globalization and
- 37) Ethnicity, Available at:
- 38) <http://depthome.brooklyn.cuny.edu/aod/Text/Hall.pdf>
- 39) Hare, Forrest (2010); "The Cyber Threat to National Security: Why Can't We Agree?" CCDCOE Publications, Tallinn, Estonia.
- 40) Kopley, T. (1994), Religious Education: Developing Primary Teaching Skills, London: Routledge.
- 41) Larousse, Pierre (1964), Grand Larousse encyclopédique en dix volumes, Paris Librairie
- 42) Mahzam, Remy. 2015. The Electronic Digitization of ISIS: Building a Multi- Media Legacy, S. Rajaratnam School of International Studies (RSIS).
- 43) Nye, J. S. 2002. Hard and Soft power hn a Global Information Age. In Mark Leonard (Ed), Re-ordering the world. London: The Foreign Policy Center.pp. 151-153.
- 44) Nye, J. S. 2004-a. Soft Power and Higher Education, Harward University: pp. 11-14.

- 45) Nye, Josephs. (2010); cyber power, Belfer center for science and international Affairs.
- 46) Nye, J. S. 2014. The Information Revolution and Power, Curent History. Vol. 113, No. 759: pp. 19-22.
- 47) Schmid, Alex P (1993), “The response problem as a definition problem”, In: “Western response to terrorism”, Alex Schmid and Ronald D.Crelinsten , London: Frank Cass & Co. Ltd.
- 48) Shackelford SJ. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. Berkeley J Int'l Law 2009; 27(192): 192-251. Available at: <https://www.scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368& context=bjil>. Accessed December, 2018.