جغرافیا (فصلنامه علمی ـ پژوهشی و بین‌المللی انجمن جغرافیای ایران)
دوره جدید، سال سیزدهم، شماره ۴۴، بهار ۱۳۹۴

تروریسم در فضای مجازی و اثرات آن بر حوزهٔ جغرافیای سیاسی

کیومرث یزدان‌پناه درو[۱] و حسن کامران[۲]
تاریخ وصول: ۱۳۹۳/۱/۲٤، تاریخ تایید: ۱۳۹۳/۳/۲۸

چکیده

نقش انکارناپذیر توسعه بشری در عرصه فناوریهای اطلاعاتی و ارتباطی را در کره زمین در عصر حاضر به‌هیچ عنوان نمی‌توان نادیده گرفت. فناوری‌های معرف به نرم‌افزارها امروزه تمام ابعاد زندگی بشری را در کلیه حوزه‌های جغرافیایی تحت‌تأثیر قرار داده است.تأثیر این روند جدید بر جغرافیای سیاسی نیز کاملاً مشهود بوده و جا را برای تحقیقات و پژوهش‌های گسترده در این حوزه فراهم کرده است، زیرا فناوری‌های بنیادین فضای مجازی، در فرهنگ، حیات اجتماعی، الگوهای تعاملی میان دولت‌ها و ماهیت تهدیدات نقش موثر و پراهمیت دارد و این بیانگر آن است که محیط تهدیدآفرین علیه امنیت ملی دولت‌ها دیگر محدود به جهان واقعی نیست، بلکه جهان مجازی نیز همپای جهان واقعی، محیطی تهدیدزا برای دولت‌هاست. در این میان یکی از مهمترین تهدیدات نوظهور، سایبر تروریسم است و با توجه به تراکم گروه‌های تروریستی معاند نظام در محیط پیرامونی جمهوری اسلامی ایران و افزایش نقش کنشگران غیردولتی در تهدیدآفرینی با بهره‌گیری از ظرفیت محیط مجازی، به همین منظور این نوشته بر آن است، ابعاد سایبر تروریسم و سناریوهای احتمالی آن را از منظر امنیت ملی مورد کنکاش و بررسی قرار دهد.

کلیدواژگان: فناوری اطلاعات و ارتباطات، سایبر تروریسم، تهدیدات سایبر تروریسم، امنیت ملی.

---

۱. استادیار جغرافیای سیاسی، دانشکده جغرافیا، دانشگاه تهران (نویسنده مسئول).
۲. دانشیار جغرافیای سیاسی، دانشکده جغرافیا، دانشگاه تهران.

مقدمه

امروزه جغرافیای سرزمینی کشورها به‌شدت تحت تأثیر فضای مجازی قرار گرفته‌اند. یکی از خطرناک‌ترین ابعاد فضای مجازی در حوزه جغرافیای سیاسی کشورها، موضوع تروریسم است. به‌صورت کلی در خصوص فضای مجازی که تبدیل به دنیای دوم ما انسانها در عصر حاضر شده است، می‌توان اینگونه نوشت که فضای مجازی یک دنیا فرصت و بی‌نهایت تهدید برای ملت‌ها و دولتها به ارمغان آورده است. صرف‌نظر از ابعاد اجتماعی – فرهنگی – سیاسی – امنیتی و سایبری این پدیده نو ظهور، تحلیل و ارزیابی آن از زاویه جغرافیای سیاسی نیز بسیار حائز اهمیت است. در این مقاله سعی شده با نگرشی ژئوپولیتیکی به این موضوع حساس نگریسته شود.

از طرفی نیز یکی از اهداف تروریستی شبکه‌های تروریستی حمله به اصول و ضوابط سنتی و دیرینه ملت‌های مستقل در لباس فضای مجازی است. اصول و ضوابط مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید سایبری به‌منظور حفظ و صیانت قلمرو سرزمینی و شبکه‌های درونی اطلاع‌رسانی، مخابراتی و رایانه‌ای از جمله مهمترین مباحثی است که در این مقاله از زاویه جغرافیای سیاسی مورد توجه قرار گرفته است.

در اینجا جا دارد از زحمات و همکاری دانشجوی مقطع کارشناسی‌ام، سرکار خانم مهتاب جعفری که در ویراستاری و تنظیم و ترتیب شکلی مقاله اینجانب را یاری دادند، تشکر و قدردانی نمایم.

بیان مساله

دنیا در حال گذار است. دستاوردهای علمی بشر که تحولات و دگرگونی‌های شتاب‌زا و شتاب‌زی را در ساخت‌های گوناگون زندگی بشر ایجاد می‌کنند، آثار و پیامدهای خود را بر حوزه‌های گوناگون حیات فردی، خانوادگی، اجتماعی، ملی، منطقه‌ای و بین‌المللی بر جای می‌گذارند و بخش‌های مختلف حیات انسان را دستخوش بسامدها و پیامدهای مختلف می‌سازند. یکی از مهمترین دستاوردهای بشر گسترش فزاینده فناوری اطلاعات و ارتباطات

است که به دگرگونی در ابعاد مختلف مولفه‌های اقتصادی، سیاسی، اجتماعی، فرهنگی و نظامی منجر خواهد شد (حسن‌بیگی،۱۳۸٤: ۲).

درست مانند جنگ جهانی اول که جنگ‌افزارهایی جدید و کارزاری نوین را برای قرن بیستم معرفی کرد، در حال حاضر نیز در عصری که در حال شکل‌گیری است، انقلابی در وضعیت جنگی برای قرن بیست‌ویکم به‌وجود می‌آید. در سراسر جهان، فن‌آوری اطلاعات به‌طور فزاینده‌ای در نظام‌های تسلیحاتی، زیرساخت‌های دفاعی و اقتصادهای ملی رواج یافته و نفوذ می‌کند. در نتیجه، فضای الکترونیکی- سیبرنتیکی به میدان نبرد و کارزاری نوین در عرصه بین‌المللی بدل می‌شود. در حالی که پیروزی‌های نظامی به فائق آمدن در رویارویی‌های فیزیکی سربازان و تسلیحات بستگی داشت، جنگ اطلاعاتی امروز با خراب‌کاری در کامپیوترها بوسیله‌ی مهاجمانی که از طرف بنگاه‌های خصوصی یا دولت‌ها اجیر شده‌اند، برپا می‌شود (آدامز،۱۳۸۰: ۲).

فناوری‌های نوین اطلاعاتی و ارتباطی، از جمله اینترنت این امکان را فراهم می‌کند تا کنشگران در بستر و محیط جدیدی به تعامل بپردازند که فضای مجازی(Cyberspace) نامیده می‌شود. نخستین بار ویلیام گیبسون (William Gibson) نویسنده داستان‌های علمی- تخیلی، در اثر خود باعنوان نورومنسر (Nouromancer) در سال ۱۹۸۲ واژه فضای مجازی را به کار برد (www.wikipedia.org).

فضای مجازی عبارت است از: مجموعه‌ای از ارتباطات بین انسان‌ها از طریق رایانه و و سایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی.

بارزترین ویژگی فضای سایبر، دسترس‌پذیر ساختن سریع و با حداقل هزینه کلیه اطلاعات آن‌لاین است. جالبتر اینکه اگر صاحبان منابع اطلاعات، رأسا یا به واسطه دیگران، به‌ویژه متصدیان شبکه‌های اطلاع‌رسانی رایانه‌ای با اجرای تمهیدات گوناگون سخت‌افزاری و نرم‌افزاری، سعی در تحدید این میزان دسترس‌پذیری داشته باشند، توفیق چندانی نمی‌یابند. به عبارت دیگر، تقریباً چیزی به نام تحدید دسترسی به اطلاعات در فضای سایبر معنا ندارد (جلالی فراهانی، ۱۳۸٤: ۳۱).

به عبارت دیگر، فضای مجازی، محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، در آن به‌طور زنده و مستقیم روی می‌دهد.

فناوری اطلاعات و ارتباطات این امکان را فراهم می‌کند که کنشگر همزمان در هر دو جهان واقعی و مجازی حضور داشته باشد و فراتر از حدود مکانی و زمانی محل استقرار خود به تعامل با سایبر کنشگران و تاثیرگذاری بر کنش‌های اجتماعی و سیاسی بپردازد.

در نتیجه محیط عملیاتی دولت‌ها در زمینه‌ها و ابعاد مختلف امنیتی، سیاسی، اقتصادی و اجتماعی دیگر محدود به جهان واقعی نخواهد بود، بلکه جهان مجازی که حاصل تعاملات و ارتباطات الکترونیکی کنشگران (اعم از دولتی و غیردولتی همچون افراد و گروه‌ها) از طریق اینترنت، ماهواره و تلفن همراه است، فرصت‌ها و تهدیدات نوینی را فراروی دولت‌ها قرار داده‌است. زیرا یکی از ویژگی‌های فناوری اطلاعات و بویژه اینترنت، امکان ساماندهی و تدارک تهاجم سازمان‌یافته از فواصل دور علیه اهداف از پیش تعیین شده است و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود یا ایجاد ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تاخیر در آن‌ها می‌گردد. در تهاجم از طریق شبکه اینترنتی حتی کشورهایی که به دلیل موقعیت جغرافیایی از بسیاری از تهاجم‌های فیزیکی مصون بودند دیگر در امان نخواهند بود (حسن‌بیگی،۱۳۸٤: ۳).

نقش فزاینده فناوری‌های بنیادین فضای مجازی در فرهنگ و حیات اجتماعی و تاثیرگذاری آن بر کیفیت و الگوهای تعاملی میان دولت‌ها و ماهیت تهدیدات (اهمیت یافتن تهدیدات نرم در مقابل تهدیدات سخت و امنیت نرم در مقابل امنیت سخت) بیانگر آن است که محیط تهدید آفرین علیه امنیت ملی دولت‌ها دیگر محدود به جهان واقعی نیست؛ بلکه جهان مجازی نیز همپای جهان واقعی، محیطی تهدیدزا برای دولت‌هاست که می‌تواند بوسیله کنشگران دولتی و غیر دولتی مورد بهره‌برداری قرار گیرد.

پیامی که در عرصه سیاست از طریق رسانه‌های الکترونیک منتقل می‌شود به اقتضای ماهیت رسانه و انباشت اطلاعات و داده‌ها صورتی ساده به خود می‌گیرد. افشاگری‌ها، بازگویی رسوایی‌های اخلاقی و مالی، برجسته کردن فقدان مشروعیت سیاسی در رقیب از موثرترین ابزار فعالیت سیاسی در این عرصه هستند (عباسی و هاشمی، ۱۳۸۹: ٥٦).

در این میان یکی از مهمترین تهدیدات نوظهور، سایبر تروریسم است که به واسطه کاربست فزاینده فناوری‌های اطلاعات و ارتباطات بوسیله دولت‌ها برای تسریع، افزایش کارایی و کاهش

هزینه‌ها در خدمت‌رسانی به شهروندان، اهمیت فزاینده‌ای یافته‌است؛ به گونه‌ای که حتی دولت‌ها نیز از سایبر تروریسم به‌عنوان ابزاری در الگوی تنازعی خود استفاده می‌کنند.

در این میان مهمترین کنشگران تهدیدزای فضای مجازی در بعد تروریسم در دو گروه عمده طبقه‌بندی می شوند. نخست: تهدید از ناحیه کنشگرانی که به یک کشور خارجی وابسته‌اند، از قبیل بخش‌های نظامی، سازمان‌های امنیتی و شرکت‌های که وابستگی زیاد به یک دولت دارند و تهدید؛ دوم: تروریست‌ها و گروه‌های افراطی که ممکن است به دولت خاصی وابستگی نداشته‌باشند، ولی در راستای اهداف خود به خرابکاری مبادرت ورزند.

با توجه به تراکم گروه‌های تروریستی معاند نظام در محیط پیرامونی جمهوری اسلامی ایران و افزایش نقش کنشگران غیردولتی در تهدیدآفرینی با بهره‌گیری از ظرفیت محیط مجازی، این احتمال وجود دارد که بخشی از دورنمای فعالیت‌های ایذایی این گروهک‌ها در فضای سایبر سازماندهی شود. به‌همین منظور بایسته است، ابعاد سایبر تروریسم و سناریوهای احتمالی آن از منظر امنیت ملی مورد کنکاش و بررسی قرار گیرد.

پیشینه تحقیق

در زمینه جایگاه فضای سایبری در انواع تهدیدات از جمله، جنگ نرم، تروریسم و... پژوهش‌های بسیاری انجام گرفته است که در اینجا به برخی از مهمترین آن‌ها اشاره می‌کنیم.

مهسا ماه‌پیشانیان در پژوهشی با عنوان: *گفتمان جنگ مجازی و رسانه‌های گروهی* معتقد است رسانه‌های گروهی می‌توانند شرایط جنگ را از طریق تبدیل و تخفیف مرگ در طی جنگ‌ها، شبیه‌سازی، مسافت‌سازی، فضیلت‌مند جلوه دادن جنگ، دگرگون‌سازی طبیعت جنگ، راه یافتن جنگ مجازی به‌همه صفحه‌های نمایشی، تلویزیون، رایانه، سینما تغییر دهند که اینترنت و تبلیغات نیز در تغییر شرایط جنگی و مجازی‌سازی موثر بوده‌اند (عباسی و هاشمی، ۱۳۸۹: ٥٦).

امیرحسین جلالی فراهانی در مقاله‌ای بنام تروریسم سایبری، شرح داده است که یکی از تهدیدات امنیتی که همواره ملت‌ها را آزار داده، اقدامات تروریستی است. وی یادآور شده زیرساخت‌های حیاتی از بهترین اهداف محسوب می‌شوند که با توجه به الکترونیکی شدن آن‌ها ارتکاب اقدامات تروریستی آسان‌تر شده، این نوشته جلالی فراهانی بر آن است که با تبیین

اجمالی مفهوم عام تروریسم سایبر به‌عنوان یک پدیده‌ی مجرمانه، راهکارهای حقوقی مقابله با آن و وضعیت کشورمان را بررسی نماید.

روش تحقیق

با توجه به اینکه هدف تحقیق حاضر، شناخت نقش، اثرات و کارکرد تروریسم در فضای مجازی از جمله اینترنت است، در راستای رسیدن به هدف ذکر شده، مطالعه‌ی مقالات و کتاب‌ها، بررسی سایت‌های مرتبط با موضوعات فضای مجازی، تروریسم، جنگ نرم و مشاوره با اساتید برجسته انجام شده و پس از تجزیه و تحلیل ویژگی‌های فضای مجازی از جمله اینترنت، به‌عنوان تسهیل‌کنندهی ایجاد چالش‌ها و ناامنی‌ها از سوی تروریسم برای دوات‌ها و جوامع هدف و همچنین، برای دستیابی به سازو کارهایی در جهت دفع فضای سایبر تروریسم، راهکارهایی ارائه شده و مورد بررسی قرار می‌گیرد.

مبانی نظری

فناوری نظامی و اقتصادی غالب هر عصری بر مولفه‌های ثبات‌بخش و بی‌ثبات‌کننده نظام بین‌الملل تاثیر می‌گذارند. بر همین اساس، تمرکز پژوهشگران عمدتاً بر فناوری‌های خاص و تاثیرات آن‌ها بر برآیندهای داخلی با بین‌الملل مانند تاثیر تسلیحات هسته‌ای بر اتحادها و به‌کارگیری زور (Waltz,1979:180-193)، دورنمای همکاری‌های بین‌المللی (Jervis,1978:167-214) تاثیر فناوری‌های اطلاعات و ارتباطات بر ظرفیت تعاملی نظام بین‌الملل (Buzan,2000:67-70) بوده است.

تعاملات انسانی و روابط میان کنشگران عضو نظام بین‌الملل همواره در یک بستر و بافت حادث می‌شود. ویژگی‌ها و مولفه‌های بنیادین هر بافتی، نقش مهمی را در شکل‌دهی و جهت‌دهی به رفتارها و نحوه تعامل میان واحدهای در حال تعامل اعم از فرد یا دولت ایفا می‌کند.

برخی از نظریه‌پردازان روابط بین‌الملل و علوم ارتباطات، روندها و تحولات جامعه انسانی، از جمله امور نظامی و ارتیاطات میان افراد را به گونه‌ای نظریه‌پردازی کرده‌اند که نقش مستقلی برای فناوری قائل شده‌اند و در همین راستا کوشیده‌اند نقش فناوری را در تحولات حوزه‌های

خاص از قلمرو فعالیت بشری مورد مطالعه قرار دهند. مارشال مک‌لوهان (Marshall Mc Luhan) استدلال می‌کند رسانه‌های هر عصر ماهیت جامعه آن عصر را تعیین می‌کنند. از دید مک‌لوهان، پیشرفت هر جامعه‌ای همزمان با رشد فناوری‌ها بوده‌است. جوامع انسانی از رسانه‌ها (فناوری) از حروف الفبا تا اینترنت، تاثیر پذیرفته و بر آن‌ها تاثیر نهاده‌اند. باری بوزان (Barry Buzan) در کتاب مقدمه‌ای بر مطالعات استراتژیک، استدلال می‌کند آنارشی بین‌المللی و فناوری‌های غالب، دو شرط اساسی هستند که دولت‌ها در بستر آن‌ها استراتژی را تدوین می‌کنند (Buzan,1987:66-67). وی معتقد است فناوری، یک ساختار ژرف و جهان‌گستر شبیه آنارشی است، ولی جدا از آن است. این ساختار نه یک بافت سیاسی، بلکه یا بافت فناورانه را ایجاد می‌کند که سیاست داخلی و بین‌المللی در درون آن عمل می‌کنند. از نظر بوزان، ساختار این بافت، الزام فناورانه، فرایند عام پیشرفت کیفی در فناوری است (Ibid:74). که بر گستره عملیات نظامی، سرشت تهدیدهای نظامی و پیامدهای توسل به زور تاثیر می‌نهد و دولت‌ها را مجبور می‌سازد به گونه‌ای رفتار کنند که به مسابقه تسلیحاتی شباهت دارد. روش‌ها، مهارت‌ها و ابزارهایی که کنشگران برای بقاء امنیت و یا تحقق هر هدف دیگری به‌کار می‌برند، زیربنای بافت فناورانه سیاست داخلی و بین‌المللی را تشکیل می‌دهند.

از آنجا که ما به تهدیدات سایبر تروریستی علیه امنیت کشورها توجه داریم، باید مباحث خود را بر فناوری‌های مرتبط با ظهور تهدیدات نوین، یعنی روش‌ها، ابزارها و مهارت‌هایی متمرکز سازیم که فرصت‌ها و محدودیت‌هایی را برای کنشگرانی از قبیل دولت‌ها و بازیگران غیردولتی ایجاد می‌کنند؛ روش‌ها و ابزارهایی که کنشگران برای اعمال تهدید علیه یکدیگر و الگوهای منازعه در سطوح مختلف به‌کار می‌برند. علاوه بر این ظهور فناوری‌های نوین که از سطح واحدها شروع می‌شود و بتدریج جهان‌گستر می‌شود، بر ابعاد سیاسی، اجتماعی و اقتصادی نظام سیاسی داخلی و بین‌المللی تاثیر می‌نهد. از دیدگاه واقع‌گرایی ساختاری، اهداف دولت‌ها و نیاز آن‌ها به توانمندی‌های نظامی، سیاسی و اقتصادی برای تحقق این اهداف کم و بیش تغییرناپذیرند. مادامی که آنارشی بین‌المللی وجود دارد، دولت‌ها به دنبال این توانمندی‌ها هستند. نوآوری‌های فناورانه بر انارشی بین‌المللی یا موجودیت و کارویژه‌های بنیادین دولت‌ها غلبه نکرده‌اند، اما برخی از نوآوری‌های فناورانه تاثیرات ژرفی بر برآیندهای سیاسی داخلی و

بین‌المللی داشته‌اند. از سال ۱۹٤٥ به بعد تسلیحات هسته‌ای سهم بسزایی در جلوگیری از جنگ میان قدرت‌های بزرگ داشته‌است. در همین راستا، گیلپین، استدلال می‌کند قوام و افول هژمون با تغییرات فناوری‌های نظامی و اقتصادی درهم تنیده شده‌است، چرا که اقتصادی که بتواند از رکود فناورانه رهایی یابد، قدرت جهانی آینده خواهد بود (Gilpin,1981:180). ظهور فناوری تسلیحات هسته‌ای در دهه ۱۹٤۰، در ایالات متحده آمریکا و متعاقب آن دستیابی اتحاد جماهیر شوروی به این فناوری، محیط بین‌المللی را متحول ساخت و موجب تغییر بین‌الملل از چند قطبی به دو قطبی و تحول استراتژی‌های نظامی از تهاجمی به بازدارندگی گردید.

این دو تحول، کاربست فناوری‌های اطلاعات و ارتباطات را در حوزه‌های نظامی، سیاسی و اقتصادی بوسیله کنشگران دولتی و غیردولتی امکان‌پذیر ساخت. روند شتابان گسترش و پراکندگی فناوری‌های اطلاعات و ارتباطات، جهان را در بستر بافت پسابین‌المللی یا پساوستفالیایی قرار داده است. این وضعیت بر تمامی ابعاد حیات بین‌المللی سایه افکنده و تمامی سطوح فردی، فروملی، ملی، منطقه‌ای و بین‌المللی را در نوردیده است. برهمین اساس، گسترش فناوری‌های اطلاعات و ارتباطات و کاربست آن در تمامی قلمرو حیات بشری، جایگاه فناوری را در حوزه‌های سیاسی، اقتصادی و اجتماعی برجسته ساخته‌است، به گونه‌ای که بافت فناورانه‌ای را پدید آورده‌است که روندها و پویش‌های عرصه داخلی و بین‌المللی از آن تاثیر چشمگیری می‌پذیرند. از انجا که هستی‌شناسی نظریه‌های متعارف روابط بین‌الملل بر مبنای جهان واقعی شکل می‌گیرد، در نتیجه بافت فناورانه بعنوان بستر پویش امنیت مورد بی‌توجهی قرار می‌گیرد. محیط بین‌الملل به جای بافت فناورانه می‌نشیند و دو کار ویژه انجام می‌شود: نخست اینکه عرصه بین‌المللی بستر امنیت است و دوم در برابر عرصه داخلی قرار داده می‌شود.

پایه استدلال پژوهش حاضر این است که نه نوع تعامل عرصه داخلی و بین‌المللی، بلکه، این بافت فناورانه است که پویش‌های امنیتی را شکل می‌دهد و هرچه فناوری در سطح وسیع‌تری گسترش یابد، بیشتر امنیت را دستخش دگرگونی می‌سازد. این مدعا بویژه درباره گسترش فناوری‌های اطلاعات و ارتباطات صادق است؛ چرا که فناوری‌های اطلاعات و ارتباطات با گسترش خود، جهان واقعی را درنوردیده‌اند و فضای مجازی را پدید آورده‌اند؛ البته به بیان صحیح‌تر، فضای مجازی را برجسته ساخته‌اند و بر تاثیرگذاری آن افزوده‌اند. بنابراین امنیت را

دیگر نمی‌توان با ویژگی‌های سنتی که بیشتر مبنی بر ویژگی‌های جهان فیزیکی است، تعریف کرد. چرا که فناوری‌های اطلاعات و ارتباطات، قوام‌بخش بافت فناورانه‌ای هستند که پویش‌های امنیتی در آن متفاوتی با ویژگی‌های جهان فیزیکی است. در این بافت فناورانه، مرزهای متصلب عرصه داخلی و عرصه بین‌المللی بسیار کمرنگ می‌شود. به‌طوریکه کنترل دولت‌ها بر جریان اطلاعات، ارز و کالا در طول مرزهای سرزمینی از بین می‌رود، چرا که بخش قابل توجهی از فعالیت‌های نظامی، اقتصادی و فرهنگی کنشگران غیردولتی در فضای مجازی و با بهره‌گیری از امکانات فناوری‌های اطلاعات و ارتباطات انجام می‌گیرد.

مفهوم امنیت ملی

پرداختن به مقوله امنیت ملی، با درک ۲ مفهوم امنیت و دولت عملی خواهد بود. در جغرافیای سیاسی، دولت فضای سیاسی سازمان‌یافته‌ای که حکومتی آن را اداره می‌کند و متشکل از سه عنصر (سرزمین، جمعیت و نظام سیاسی یا حکومت) است (کاویانی راد،۱۳۸۳: ٦٧١). دولت در تعریف مدرن آن محدود به یک سرزمین و حائز مجموعه‌ای از ویژگی‌های خاص از جمله فرهنگ خاص خودش است (مختاری،۱۳۷۹: ۲۵). امنیت مفهومی چند وجهی است و به همین جهت درباره معنای آن اختلاف نظر زیادی وجود دارد. تعریف‌های فراوانی از امنیت و امنیت ملی در منابع آمده است. بسیاری از این تعریف‌ها بر حفظ تمامیت ارضی یک کشور در مقابل تهدیدهای خارجی تاکید دارند، درحالی که چهره متحول جهان امروز، چارچوب‌های امنیت ملی را نیز دستخوش تحول ساخته‌است. عدم ثبات و سیال بودن شکلی و ماهوی امنیت ملی، همچنین ظهور مفاهیم جدیدی چون دولت‌های پیشامدرن و پسامدرن در کنار دولت‌های مدرن تعیین شده در معاهده وستفالیا، چهره‌ای پویا، سیال، نسبی، چند بعدی و پیچیده از مقوله امنیت ملی به تصویر می‌کشد (شریف،۱۳۸۷: ۱۲۳).

جهان وارد عصر تازه‌ای شده و انقلاب اطلاعات و ارتباطات، جوامع صنعتی را به سوی اطلاعاتی شدن سوق داده است. در عصر حاضر اطلاعات و ارتباطات منشأ قدرت محسوب می‌گردد (بیابان‌نورد،۱۳۸۳: ۱۲۱). از سویی جهانی شدن با تهدیدها و فرصت‌های خاص خود ظهور یافته‌است. بر همه جنبه‌های زندگی فردی و اجتماعی، از جمله ارتباطات و سیاست اثر

می‌گذارد. در این بستر متغیر، معادلات امنیتی نیز دستخوش تغییرات اساسی شده و عنصر اطلاعات، بعنوان عنصر نامحسوس قدرت و ارزش ویژه‌ای یافته‌است. تغییرات جدید، تهدیدات امنیتی جدیدی را در گفتمان امنیت ملی مطرح می‌سازد. تهدیدات جدید، ماهیتی اطلاعاتی را دارد و استراتژی‌های مقابله‌ای ویژه‌ای را می‌طلبد (شریف،۱۳۸۷: ۱۲۷). حال در تحلیل امنیت ملی انقلاب اطلاعاتی دو چهره دارد، یکی تهدید و دیگری فرصت. هیچ تغییری نه تهدید یکپارچه است. نه فرصت کامل، یعنی حالت توأمان و ترکیبی دارد. انقلاب اطلاعاتی اگرچه خطرات و تهدیدهای جدیدی را پیش روی تحلیل‌گران امنیت ملی گذاشته، فرصت‌های بی‌نظیری نیز در اختیار ملت‌ها قرار داده‌است (همان:۱۳۰).

سایبر تروریسم

حملات و تروریسم سایبری که در جهان مجازی همچون اقداماتی آشوب‌طلبانه در دنیایی واقع هستند، تروریسم سایبری که حاصل تلاقی و همگرایی دو واژه ترور و سایبر شکل گرفته‌است در عنوان عبارت اولی خود ترس و واهمه را گوشزد می‌کند و سایبر هم که همان فضای مجازی است و بر این اساس می‌توان گفت ایجاد هر نوع ترس و واهمه‌ای ازطریق فضای مجازی راتروریسم سایبری گویند (www.jahannews.com). تروریسم سایبری واژه‌ای است که این روزها وارد چهارمین دهه عمر خود شده و با گذر زمان به‌طور دائم با شیوه‌های غرب و پیچیده‌تر از قبل در دنیا رواج یافته است (www.teror.victims.com). تروریسم سایبری امروزه خطرناکتر از تروریسم سنتی است، به این دلیل که ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی شده‌است. تروریسم سایبری می‌تواند ابعاد داخلی داشته‌باشد یا شامل موارد بین‌المللی شود (www.tebyan.net).

به‌طور کلی تروریسم را اینگونه تعریف می‌کنند: **به‌کارگیری خشونت علیه اشخاص، دولت‌ها یا گروه‌ها برای پیشبرد زورمندانه اهداف سیاسی یا عمومی**. تروریسم مجازی به تاکتیک‌هایی اطلاق می‌شود که با هدف از کارانداختن زیرساخت‌های بحرانی یک کشور انجام می‌شود. عملیات تروریستی در فضای مجازی به حداقل زمان، هزینه و امکانات نیاز دارد. به‌علاوه اینکه خطر آن نیز کمتر است (حسن‌بیگی، ۱۳۸۸: ١٦٥). سایبر تروریسم (Cyber terrorism) در حقیقت

همان تعریف را دارد، با این تفاوت که این‌بار هدف متمرکز روی منابع موجود در فضای مجازی است. سایبر تروریسم می‌تواند ابعاد داخلی داشته باشد یا شامل موارد بین‌المللی شود. سایبر تروریسم امروز خطرناکتر از تروریسم سنتی است به این دلیل که ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی شده‌است.

فضای مجازی و تروریست‌ها

ویژگی‌های بی‌همتای فناوری‌های اطلاعات و ارتباطات، تحولات بنادینی را در قلمرو حیات بشری پدید آورده‌است. نخستین ویژگی بی‌همتای فناوری‌های اطلاعات و ارتباطات، جهان‌گیری گسترش این فناوری‌هاست. این ویژگی باعث گردیده‌است فناوری‌های اطلاعات و ارتباطات نفوذ جهان‌گسترانه‌ای به دست آورند و در یک گستره جغرافیایی خاص و محدود نگنجد. به عبارت بهتر، فناوری‌های اطلاعات و ارتباطات تمامی مرزها را درمی‌نوردند و از جهان مرززدایی می‌کنند. این مرززدایی و کمرنگ‌کردن مرزهای سنتی، زمینه تسهیل حرکت هرچه آزادانه‌تر کالا، سرمایه و افراد را فراهم می‌کنند (Everard,2000:63).

دومین ویژگی مهم و چشمگیر فناوری‌های اطلاعات و ارتباطات، کنترل‌ناپذیری و لجام‌گسیختگی آن است. گسترش فناوری‌های اطلاعات و ارتباطات به‌گونه‌ای است که در بسیاری از موارد حتی عاملان گسترش و زمینه‌سازان آن نیز نمی‌توانند آن را در کنترل خود درآورند (Cavelty,2008:10).

ویژگی سوم که پیوند تنگاتنگی با ویژگی دوم دارد و البته سایر ویژگی‌های فناوری‌های اطلاعات و ارتباطات را تحت‌الشعاع قرار می‌دهد، قاعده‌گریزی در این پدیده است. این ویژگی به علت ماهیت شبکه‌ای فناوری‌های اطلاعات و ارتباطات است که نوعی وضعیت غیرسلسله مراتبی و شبکه‌ای در عرصه‌ای که حضور می‌یابد، می‌آفرینند. این وضعیت غیرسلسله مراتبی، محیط سنتی و پویش‌های امنیتی آن را که نظام‌مند است نه شبکه‌ای، تحت‌تاثیر قرار می‌دهد (Gori,2006:81).

چهارمین ویژگی فناوری‌های اطلاعات و ارتباطات، که خصوصیتی بدیع و بدعت‌زا نیز به‌شمار می‌آید، ایجاد و گسترش جهان مجازی است. این ویژگی عرصه امنیت را دو جهانی ساخته

است: جهان واقعی و جهان مجازی. جهان واقعی همان عرصه سنتی امنیت است و جهان مجازی عرصه‌ای است که گسترش فناوری‌های اطلاعات و ارتباطات هر روز بر اهمیت و تاثیرگذاری آن می‌افزاید، به‌گونه‌ای که در حال حاضر رویدادهای جهان مجازی بر جهان واقعی سایه می‌افکند.

بدنبال افزایش اهمیت و تاثیرگذاری جهان مجازی، تهدیدهای مجازی نیز ظهور کرده و شدت گرفته‌اند. ظهور و شدت‌گیری تهدیدهای مجازی به وضعیتی شکل داده‌است که کنشگران موجود نمی‌توانند به‌طور کامل با آن‌ها مقابله کنند و در نتیجه کنشگران غیردولتی همچون گروه‌های تروریستی از این قابلیت و توانمندی برخوردار شده‌اند که ثبات و نظم بین‌المللی و امنیت ملی دولت‌ها را مورد تهدید قرار دهند (Cavelty,2008:10). بهره‌گیری گروه‌های تروریستی از امکانات فضای مجازی، نوع جدیدی از تهدید را پدید می‌آورد که سایبر تروریسم نامیده می‌شود. سایبر تروریسم هرگونه اقدام تروریستی است که در آن از سیستم‌های اطلاعاتی و فناوری‌های دیجیتالی بعنوان ابزار حمله و آماج حمله استفاده می‌شود. "دوروتی دنینگ"، سایبر تروریسم را اینگونه تعریف می‌کند: سایبر تروریسم حاصل همگرایی تروریسم و فضای مجازی است، سایبر تروریسم بمعنای تهاجم و تهدید به تهاجم غیرقانونی به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن‌هاست که به‌منظور ارعاب یا وادار کردن یک دولت یا مردم آن به پیشبرد اهداف سیاسی یا اجتماعی خاص صورت می‌گیرد (Hancock,2001:553).

اداره اطلاعات ملی آمریکا (Director of National Intelligence) که وظیفه هماهنگی ۱۶ سازمان اطلاعاتی آمریکا را برعهده دارد، در گزارش فوریه ۲۰۱۰ که به بررسی تهدیدهای امنیت ملی آمریکا می‌پردازد، تهدیدهای سایبری را از مهمترین تهدیدهای فراروی امنیت ملی آمریکا ذکر کرده‌است. در بخشی از این گزارش آمده‌است: هر چند تهدیدها و فناوری‌های مرتبط با فضای مجازی مدام در حال تغییر است، اما موازنه موجود به نفع کنشگران مخرب است. کنشگران مخربی که شامل دولت- ملت‌ها، شبکه‌های تروریستی، گروه‌های جنائی سازمان‌یافته و افراد است، از توانمندی ایجاد اختلال در فعالیت زیرساخت‌ها و دزدی اطلاعات محرمانه بخش‌های دولتی و خصوصی و تهدید امنیت ملی آمریکا برخوردار هستند.

پس از حوادث تروریستی۱۱ سپتامبر ۲۰۰۱، بوش با هدف مقابله با سایبر تروریسم، اصلاحیه قانون بدون مجوز شنود تلفنی (Wa,Tantless Wire-tapping Program) را امضا کرد که بر

اساس آن شرکت‌هایی که در حوزه جاسوسی داخلی (Domestic Spying) و یا زیر نظر آژانس امنیت ملی فعالیت می‌کردند، دیگر برای شنود تلفنی نیازی به اجازه دادگاه نداشته و از مصونیت قضایی برخوردار شدند. فعالان حقوق بشر به دلیل این که اجرای این قانون برخی آزادی‌های مصرح در اصلاحیه چهارم قانون اساسی آمریکا (Fourth Amendment to the U.S Constitution) را نقض می‌کند، با آن مخالفند. تنوع، پیچیدگی و لزوم مقابله با تهدیدها در فضای مجازی به حدی اهمیت‌یافته که رئیس جمهور ایالات متحده دفتر ویژه‌ای را در کاخ سفید باعنوان ناظر و هماهنگ‌کننده کاخ سفید در امنیت فضای سایبر(White House Coordinator to Oversee Cyber Security) برای خنثی‌سازی آسیب‌های ناشی از تهاجم هکرها به شبکه سایبر نهادهای فدرال ایجاد کرده است.

جدول۱: تهدیدهای سایبر تروریستی علیه زیرساخت‌های حیاتی

تهدید	توصیف
گروه‌های جنایی	گروه‌های جنایی با هدف کسب پول به سیستم‌ها حمله می‌کنند.
سرویس‌های اطلاعاتی خارجی	سرویس‌های اطلاعاتی خارجی از ابزارهای سایبر برای جمع‌آوری اطلاعات و فعالیت‌های جاسوسی استفاده می‌کنند.
هکرها	هکرها گاهی اوقات با هدف ایجاد چالش یا بدست‌آوردن حقوق در اجتماع هکرها به شبکه نفوذ می‌کنند.
جنگ اطلاعاتی	تعداد بسیاری از دولت‌ها برای توسعه دکترین، برنامه‌ها و قابلیت‌های جنگ اطلاعاتی تلاش می‌کنند تا از این طریق به توانایی اختلال در ارتباطات و زیرساخت‌های اقتصادی که از قدرت نظامی حمایت می‌کنند، دست‌یابند.
تهدید داخلی	سازمان‌های ناراضی داخلی، منبع اصلی جرایم رایانه‌ای هستند.
نویسندگان ویروس	نویسندگان ویروس‌ها، تهدیدهای جدی را برای شبکه‌های رایانه‌ای ایجاد می‌کنند.

میزان تهدیدآفرینی سایبر تروریسم علیه امنیت ملی کشورها به حدی است که ریچارد کلارک (Richard Clarke) مشاور عالی ضدتروریسم آمریکا در دوره جرج بوش و بیل کلینتون طی اظهاراتی در می ۲۰۱۰ اظهار داشت: آمریکا توانایی لازم برای مقابله با تلاش تروریست‌ها جهت

دستیابی به سیستم رایانه‌ای ایالات متحده را ندارد و این موضوع ممکن است به فاجعه پرل هاربر الکترونیکی (Electronic Pearl Harbor) در ایالات متحده منجر شود.

ویژگی‌های سایبر تروریسم

تروریسم فضای مجازی، نوع جدیدی از فعالیت‌های تروریستی است که کنشگران هدفمند بودن استفاده از ابزار تخریبگر فضای واقعی با حداقل امکانات تلاش دارند بیشترین صدمه را وارد کنند (حافظ‌نیا،۱۳۹۰:۲٦٦). با توجه به مطالب ذکر شده درباره سایبر تروریسم، می‌توان ویژگی‌های زیر را برای آن ذکر کرد: هدف قرار دادن تعداد بیشتری از مردم، استفاده از گروه‌های رایانه‌ای ناشناخته در سطح بین‌المللی، نداشتن محدودیت جغرافیایی، پنهان ماندن هویت، تبلیغ و عضوگیری بین‌المللی، گسترش دامنه تروریسم به مسائل مالی بانکی و اقتصادی و خدمات شهری. برخی از مهمترین ویژگی‌های فضای مجازی عبارتند از:

۱) **سیالیت مرز**: ویژگی فرامرزی فضای مجازی این امکان را فراهم می‌کند تا کنشگران فارغ از موانع و مرزهای موجود در دنیای فیزیکی، مقاصد و اهداف خود را پیگیری کند. سیالیت مرز و عدم توانایی دولت‌ها برای تسلط و کنترل کامل بر فضای مجازی، محیط مطلوبی را برای فعالیت گروه‌های تروریستی فراهم می‌کند.

۲) **کاهش هزینه جرم**: فضای مجازی هزینه جرائم ارتکابی را برای تروریست‌ها از لحاظ نتایج اقدامات و احتمال دستگیری و مجازات به نحو قابل ملاحظه‌ای کاهش داده‌است. باتوجه به اهمیت هزینه جرم برای تروریست‌ها، ماهیت فرامرزی فضای مجازی فرصت بسیار مغتنمی برای اقدامات تروریست‌ها در گستره جهانی است.

۳) **امکان وارد آوردن خسارات مالی، بدون رساندن آسیب‌های جسمی**: بیشتر اقدامات تروریستی در دنیای فیزیکی با آسیب‌دیدگی جسمانی افراد همراه است که این خود سازگاری چندانی با هدف جلب افکار عمومی و همنوا سازی آن‌ها با اهداف تروریستی ندارد؛ چرا که آسیب‌های جانی، حساسیت‌ها و واکنش‌های زیادی را علیه تروریست‌ها برمی‌انگیزند.

٤) **سهولت تدارک امکانات و عوامل مورد نیاز برای اقدامات تروریستی:** ماهیت اقدامات تروریستی در جهان فیزیکی به‌گونه‌ای است که برای ارتکاب آن‌ها باید به ابزارهایی متوسل شد که تدارک آن‌ها با مشکلات زیادی همراه است. اما فضای مجازی تمامی ابزارهای موردنیاز برای انواع اقدامات تروریستی مجازی را به‌صورت روزآمد و با کمترین هزینه در اختیار همگان قرار داده‌است. در فضای مجازی یک فرد قادر است با استفاده از یک رایانه و اتصال به اینترنت و برخورداری از مهارت کافی، خسارت‌های سنگینی را به هدف وارد کند.

٥) **امکان هماهنگی لحظه‌ای عملیات:** یکی از ابزارهای موردنیاز و حیاتی تروریست‌ها، وسایل ارتباطی پیشرفته است که از طریق آن‌ها، می‌توانند در کوتاهترین زمان و با کمترین مشکل از وضعیت یکدیگر آگاه شوند. فضای مجازی تروریست‌ها را قادر ساخته‌است با بهره‌گیری از انواع ابزارهای ارتباطات الکترونیکی، مانند پست‌الکترونیکی و تالارهای گفتگو به شکل مکتوب، صوتی و ویدئویی و به‌صورت زنده با یکدیگر ارتباط داشته‌باشند. البته مزیت برجسته این ابزارها که امکان بکارگیری بهینه را برای گروه‌های تروریستی فراهم می‌آورد، امکان رمزگذاری (Cryptography) محتوای ارتباطات الکترونیکی با ابزارهای بسیار پیشرفته است که احتمال رمزگشایی (Decryption) آن‌ها را بسیار ضعیف می‌گرداند؛ در نتیجه تروریست‌ها می‌توانند بدون نگرانی از دستیابی مجریان قانون به محتوای نامفهوم ارتباطات‌شان، براحتی به هماهنگی امور بپردازند.

٦) **انجام بهینه فعالیت‌های پولی و بانکی:** یکی از حوزه‌هایی که تقریباً به‌طور کامل تحت تاثیر فضای مجازی قرار می‌گیرد و روند توسعه و تکامل الکترونیکی شدن آن همچنان ادامه دارد، پول و بانکداری الکترونیکی است که شرایط را برای سوءاستفاده از خدمات پولی و بانکی فراهم کرده‌است. برای مثال گروه‌های جنایتکار سازمان‌یافته و تروریست‌ها که نیازمند مبادلات مالی‌اند و در عین حال با محدودیت‌های مالی بسیار مواجه می‌باشند، مجبورند درآمدهای مالی خود را شستشو(Money Laundering) کنند تا بتوانند از آن‌ها استفاده کنند.

گرایش فزاینده جوامع به بهره‌گیری از فناوری‌های اطلاعات و ارتباطات در امور اقتصادی و بانکداری، بستر مناسبی را برای اقدامات پول‌شویی در فضای مجازی فراهم کرده‌است؛ بگونه‌ای که پول‌شویی فیزیکی جای خود را به پول‌شویی مجازی (Cybre Laundering) داده‌است. همچنین امکان جذب کمک‌های مالی از سوی هواداران و حامیان نیز بسیار آسان شده‌است و امکان ارسال کمک‌های نقدی از هر جای دنیا در کمترین زمان ممکن فراهم گردیده‌است.

ترور مجازی

مهمترین مشکل که ترور مجازی را بسیار خطرناکتر کرده، شناسایی نشدن دقیق آن است. نه تنها مراکز قانون‌گذاری بلکه تروریست‌ها نیز هنوز تمامی جنبه‌های اقدامات خود را نمی‌شناسند. از همین روست آمریکا که خود بیشترین حملات اینترنتی را انجام می‌دهد، در مقابل هکرهای چینی که اهداف آمریکایی را هدف خویش قرار داده‌اند، همچنان ناتوان است. گروه‌های ملی برخی کشورها از جمله شرکت‌کنندگان در اجلاسWSIS و برخی نهادهای دیگر سعی در کنترل و برنامه‌ریزی برای مهار این پدیده دارند. یکی از سازمان‌های مذکور اینترپل است. در اروپا نیز از سال گذشته انجمن پیمان اروپا علیه جنایات مجازی تشکیل شده‌است که هر چند به آن صورت هم اروپایی نیست ولی اولین اقدام جدی در این زمینه به‌شمار می‌رود. برای مبارزه با این مسأله چندین را وجود دارد. اولین راه ارزیابی آسیب‌پذیری است. به‌عبارت دیگر این راه نوعی پیشگیری است ولی نه به‌عنوان ایجاد سد دفاعی بلکه رفع ضعف‌های موجود و پایین آوردن آسیب‌پذیری در صورت بروز حمله. راه دوم نوعی دیگر از پیشگیری است که در آن سعی می‌شود حملات احتمالی شناسایی و در مقابل آن پاتک زده شود. راه سوم پس از حمله قابل استفاده است، یعنی آمادگی برای بروز حمله و ترمیم اشکالات ایجاد شده پس از این مرحله.

راه‌های مقابله با سایبر تروریسم

متخصصان علم رایانه بهتر است که کاملاً با این پدیده باشند تا بتوانند با محافظت بیشتر از سیستم‌های تحت کنترل خود، از این پدیده و خسارات تابع آن جلوگیری کنند. در دنیای دیجیتالی امروزه با توجه به ازدیاد حملات تروریستی لزوم بررسی و تحقیقات در روش‌های مقابله بیش از پیش ضروری است. بهترین راهکار برای مقابله این است که نقشه و روش درستی برای اینکار داشته باشیم و در اولین گام اهداف روش‌های عملیاتی و منابع حمله‌کننده را بشناسیم. مشکل اساسی اینجاست که بسیاری از بخش‌های خصوصی و حتی دولتی از آسیب‌پذیری رایانه‌هایشان ناآگاه هستند، در حالیکه امروزه وابستگی به رایانه بیش از پیش به چشم می‌خورد و این ناآگاهی می‌تواند عواقب و خسارات جبران‌ناپذیری به همراه داشته باشد. مشکل دیگر در این مقوله که باید مورد توجه قرار گیرد. این است که چه کسی و از کجا به سیستم حمله کرده‌است. این مسأله بسیار مهم‌تر از بررسی خسارات وارده می‌باشد. کارشناسان به‌عنوان اولین پیشنهاد توصیه می‌کنند که از دیواره‌های آتش (Firewall) برای محافظت و ایزوله کردن سیستم‌ها نسبت به ارتباطات شبکه، در کنار مواردی از قبیل محافظت از کلمات عبور و اعمال امنیتی و محافظتی دیگر، استفاده شود.

در اینجا به تعدادی از راهکارها برای مبارزه با سایبر تروریسم اشاره می‌کنیم:

۱. تدوین استراتژی امنیتی برای حفظ امنیت شبکه‌های رایانه‌ای در کشور؛
۲. ارائه آموزش‌های لازم به نیروهای مرتبط با شبکه‌ها برای حفظ امنیت شبکه؛ از جمله مهارت‌های مهندسی اجتماعی؛
۳. بکارگیری نرم‌افزارها، ضد ویروس‌ها، دیواره‌های آتش در شبکه‌ها؛
٤. تعیین سطوح دسترسی به شبکه‌ها و سیستم‌های سایبری.

بدون شک یکی از پیچیده‌ترین ابزاری که تاکنون از آن برای اهداف تروریستی بهره برده شده‌است، اینترنت می‌باشد. تنها در دنیای اینترنت است که تروریست‌ها می‌توانند با هزارن نام مجازی و بدون این که ردی از خود بر جای گذارند، به پراکندن خشونت و علاقمندی‌های خود در این موضوع بپردازند. بخشی از این فعالیت‌ها آشکار و با اهداف خشونت‌طلبانه، تروریستی و

ضد دموکراتیک آن‌هاست. به‌طور طبیعی گروه‌های مخالف جمهوری اسلامی ایران نیز از این ابزار برای ضربه زدن به منافع ملی کشور استفاده می‌کنند.

نتیجه‌گیری

گسترش فزاینده کاربست فناوری اطلاعات و ارتباطات در زیرساخت‌های حیاتی همچون انرژی، حمل و نقل و بانکداری از یک طرف و دسترسی نامحدود و غیرقابل کنترل افراد به ابزارهای ارتباطی مانند اینترنت و ماهواره از یک طرف دیگر، منجر به شکل‌گیری فضای مجازی در کنار فضای واقعی در تعاملات بین دولت‌ها شده‌است. طبیعی است که در چنین فضایی مفهوم امنیت، چالش‌ها و تهدیدات متحول شده و بازیگران جدیدی مانند افراد، گروه‌های تروریستی و گروه‌های جنایی سازمان یافته، نقش و جایگاه مهمی را در پویش‌های امنیتی درون‌منطقه‌ای و بین‌المللی ایفا می‌کنند. با عنایت به توجه نظام سلطه بر بهره‌گیری از ظرفیت‌ها و قابلیت‌های فضای مجازی به‌منظور تنش‌سازی متراکم و گسترده قومی، فرقه‌ای، اجتماعی و ایجاد بی‌اعتمادی میان جامعه و حاکمیت و تهاجم شبکه‌ای تاکتیکی با هدف مختل‌سازی مدیریت امور جاری کشورها، سایبر تروریسم یکی از مهمترین تهدیداتی است که می‌تواند امنیت کشورها را با چالشی جدی مواجه سازد. علاوه بر این بهره‌گیری گروه‌های تروریستی از ویژگی‌ها و مزایای فضای مجازی و تلاش نهادهای تقنینی و اجرایی ایالات متحده برای حمایت از فعالیت‌های این گروه‌ها از یک طرف و حرکت شتابان کشور در جهت کاربست فناوری‌های اطلاعات و ارتباطات در زیرساخت‌های حیاتی و شبکه‌های اطلاعاتی و امنیتی کشورها موجب شده‌است، سایبر تروریسم تبدیل به یک تهدید جدی علیه امنیت ملی کشورها شود. در همین راستا بدیهی است کاهش آسیب‌پذیری‌ها و تقویت امنیت ملی در مقابل تهدیدات سایبر تروریستی، مستلزم انجام مطالعات و آینده‌پژوهی در خصوص تاثیر انقلاب اطلاعاتی بر امنیت ملی و تهدیدات فضای سایبر و ارتقای قابلیت‌های نهادهای دفاعی و امنیتی در بهره‌گیری از دانش و اطلاعات به‌عنوان سلاح استراتژیک در نبردهاست.

راهکارها و تدابیری که می‌تواند آسیب‌ناپذیری امنیت کشورها را در برابر تهدیدات سایبر تروریسم تقویت کند، عبارتند از:

- بومی‌سازی دانش امنیت شبکه و قطع وابستگی اطلاعاتی و فناورانه به دشمنان هر کشور.
- بهره‌گیری از فناوری‌های نوین در جهت هوشمندسازی زیرساخت‌ها و تاسیسات نظامی، تربیت نیروهای متخصص و کارآزموده برای بهره‌گیری از فناوری‌های نوین در نبردها.
- تلاش نهادهای تقنینی و اجرایی برای فراهم‌سازی شرایط لازم و مطلوب عملی با هدف تامین امنیت سیستم‌های اطلاعاتی و ارتباطی.

کتابشناسی

۱. بیابان‌نورد، علیرضا (۱۳۸۳)، انقلاب اطلاعات و مجازی‌سازی، فرصت‌ها و چالش‌ها، با مروری بر وضعیت پدیده اینترنت در ایران، فصلنامه عملیات روانی، ش ۲؛

۲. جلالی فراهانی، امیرحسین (۱۳۸۵)، تروریسم سایبری، فصلنامه فقه و حقوق، ش ۱۰؛

۳. جلالی فراهانی، امیرحسین (۱۳۸٤)، پیش‌گیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر، فصلنامه تخصصی فقه و حقوق؛

٤. حافظ‌نیا، محمدرضا (۱۳۹۰)، جغرافیای سیاسی فضای مجازی، تهران: سمت؛

۵. حبیبیان، علی‌اصغر (۱۳۸۸)، فضای مجازی از منظر تولید تهدید، مقاله منتشر نشده، تهران: دانشگاه عالی دفاع ملی؛

٦. حسن‌بیگی، ابراهیم (۱۳۸٤)، توسعه شبکه ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملی، فصلنامه مطالعات مدیریت بهبود و تحول، ش ٤۸؛

۷. حسن‌بیگی، ابراهیم (۱۳۸۸)، حقوق . امنیت در فضای سایبر، تهران: دانشگاه عالی دفاع ملی؛

۸. شریف، عاطفه (۱۳۸۷)، چالش‌های اطلاعاتی در گفتمان امنیت ملی، فصلنامه اطلاع‌رسانی و کتابداری، ش۱۹؛

۹. عباسی، مهدی، هاشمی، تورج (۱۳۸۹)، نقش رسانه‌ای اینترنت در ناهنجاری‌های اجتماعی در فضای سایبری در میدان جنگ نرم، فصلنامه علوم اجتماعی؛ مهندسی فرهنگی، ش ٤۹و۵۰؛

۱۰. کاویانی‌راد، مراد (۱۳۸۳)، امنیت ملی از منظر جغرافیای سیاسی، فصلنامه مطالعات راهبردی، ش ۷؛

۱۱. مختاری، مجید (۱۳۷۹)، گفتمان امنیت ملی، ج ۱، تهران: موسسه مطالعات سیاسی و فرهنگی اندیشه ناب؛

12. Buzan & Little, R.(2000), International Systems in World History: Remaking the Study of International Relations. London: Oxford University Press;

13. Buzan, B.(1987), An Lntroduction to Strategic Studies: Military Technology and International Relations. New/York: St.Martin Press;

14. Cavelty, M.D.(2008), Cyber-Security and Threat Politics: US efforts to secure the information age. New York: Routlefge;

15. Everard, J.(2000), Virtual states: the Internat and the boundaries of the nation-state. New York: Routledge;

16. Gilpin R.(1981), War and Change in World Politics. New York: Cambridge University Press;

17. Hancock, B.(2001), Cyber-Tracking, Cyber-terrorism. Computers and Security. Vol.20,No7,p.553;

18. http://www.tebyan.net/newindex.aspx?pid=226803;

19. **In: U. Gori &, I.Paparela. Invisible Threats; Financial and Information Technology Crimes Against National Securi, y. Netherlands: IOS Press;**
20. **Jervis, R.(1978), Cooperation Under the Security Dilemma. World politics. Vol.30,No.2pp.214-167;**
21. **Mesko,G.(2006), Perceptions of Security: Local Safety Councils in Slovenia;**
22. **Waltz, K.(1979), Theory of Intemational politics. New York: Random house;**
23. **www.en.wikipedia.org/wiki/Cyberspace;**
24. **www.jahannews.com/vdcbs9b59rhbz5p.uiur.html;**
25. **www.teror-victims.com/fa/index.php?Page=definition&UID=804350.**