کنترل تروریسم سایبری با مدیریت مرزهای فضای سایبر راهبردی

محسن جان‌پرور،[1] ریحانه صالح‌آبادی،[2] سیروس احمدی[3]

چکیده

امروزه گسترش فضای سایبر سبب پیدایش مرزهای مجازی شده و از این جهت درک واقع‌بینانه از تهدیدهای امنیتی در گروی توجه به عوامل نرم‌افزاری است که حلقهٔ واسط محیط امنیتی کشورها و سخت‌افزارها به شمار می‌روند. یکی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی‌شدن، حوزه سایبری و تروریسم سایبری است. مقالهٔ حاضر درصدد بررسی تأثیر تروریسم سایبری بر مرزهای کشور است و از نظر هدف، کاربردی محسوب می‌شود. این مقاله به روش اسنادی و با استفاده از منابع کتابخانه‌ای با ابزار فیش‌برداری نوشته شده است. جمهوری اسلامی ایران با توجه به داشتنِ کاربران گسترده در فضای سایبر ازیک‌سو و دارابودنِ بدخواهان و دشمنان در فراسوی مرزهای کشور برای اینکه بتواند مسائل ناشی از بهره‌وری گروه‌های تروریستی در داخل را تا حد قابل‌توجهی کنترل کرده و کاهش دهد، نیازمند مدیریت مرزهای موجود و شناساندن این فضا به افراد و مسئولان، تقویت زیرساخت‌های بومی فضای سایبر و از همه مهم‌تر ایجاد فرهنگ لازم برای حضور در آن است.

واژگان کلیدی: *مدیریت مرز، فضای سایبر، تروریسم مجازی.*

---

1. استادیار دانشکده ادبیات و علوم انسانی دانشگاه فردوسی / janparvar@ferdowsi.um.ac.ir

2. دانشجوی دکتری دانشکده علوم انسانی دانشگاه تربیت مدرس / reyhane.salehabadi@gmail.com (نویسنده مسئول)

3. استادیار دانشکده ادبیات و علوم انسانی دانشگاه تربیت مدرس / sahmadi@modares.ac.ir

1. مقدمه

جهان امروز با سرعت بالایی در حال دگرگونی است و همه حکومت‌ها و کشورها در تکاپوی نوسازی و بهبود خود برای انطباق با این وضعیت جدید هستند. این تغییرات و دگرگونی‌ها به صورت‌های مختلفی حکومت‌ها را تحت تأثیر قرار داده و آن‌ها را در برخی زمینه‌ها دچار چالش کرده و در زمینه‌های دیگر، فرصت‌هایی فراهم آورده است. از جملهٔ این چالش‌ها گسترش زمینه تحرک و نقش‌آفرینی گروه‌های تروریستی و اقدامات تروریستی در سطوح محلی، ملی و منطقه‌ای است. توسعه و پیشرفت فناوری‌های اطلاعاتی و ارتباطی به گروه‌های تروریستی این امکان را داده است تا به‌سرعت و با سهولت از یک مکان به مکان دیگر حرکت کنند، به‌سادگی تبلیغ کرده و عضوگیری کنند، به توجیه اقدامات خود بپردازند، کارهای خود را بزرگ جلوه داده و ترس و وحشت را دامن بزنند.

این تغییرات سبب شده است تا اقدامات تروریستی طی دهه‌های اخیر وسعت جغرافیایی بیشتری یابد و با افزایش چشمگیر، ترس و وحشت حاصل از این اقدامات در میان عامه مردم رسوخ کند. حکومت‌ها برای جلوگیری از این اقدامات تروریستی، راهبردهای مختلفی را در پیش گرفته‌اند و به صورت‌های مختلف کوشیده‌اند با صرف هزینه‌های گسترده با پدیدهٔ تروریسم مقابله کنند. به نظر می‌رسد یکی از راهبردهایی که در این میان مغفول مانده و کمتر به آن توجه شده است، مدیریت مرزهای کشور در فضای سایبر است.

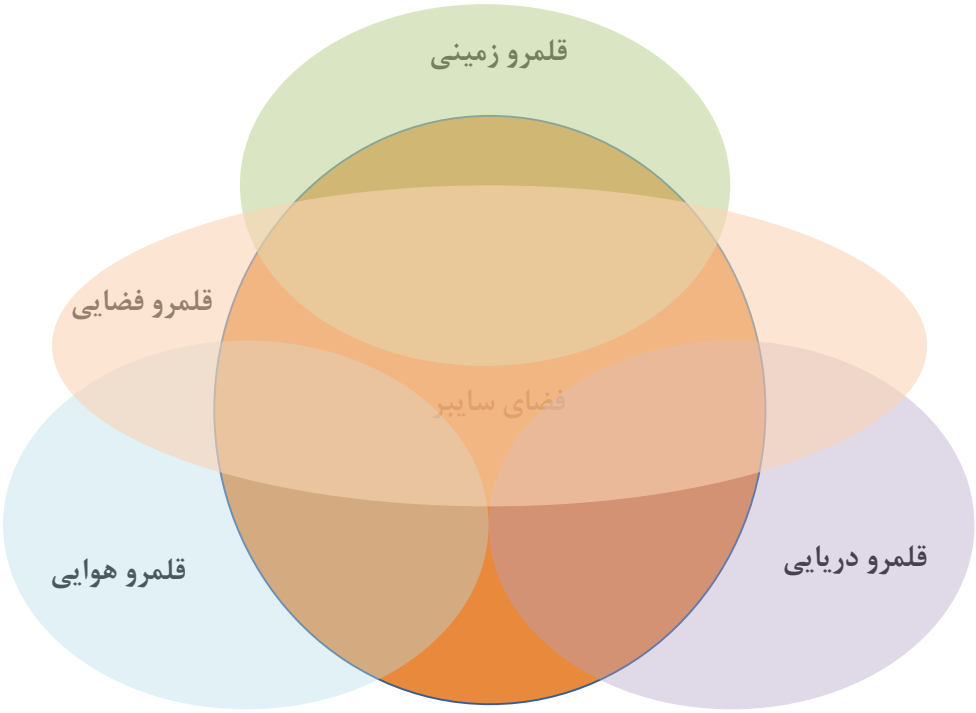
پرسش اصلی تحقیق این است که راهبرد مدیریت مرزهای فضای سایبر کشور در برابر تروریسم فضای مجازی چگونه باید تنظیم شود؟ مرزها از جمله پدیده‌های فضایی ـ جغرافیایی هستند که از جایگاه و اهمیت بالایی در برقراری امنیت در سطوح مختلف فردی، ملی و منطقه‌ای برخوردارند. یکی از کارکردهای اصلی مرزها که ناشی از ماهیت آن‌ها نیز هست، تأمین امنیت است. ازآنجاکه بیشترِ اقدامات و برنامه‌ریزی‌های گروه‌های تروریستی از فراسوی مرزهای کشور صورت می‌گیرد و از طریق مرزها وارد فضای داخلی کشورها می‌شود، با راهبرد مدیریت مرزها می‌توان به میزان قابل‌توجهی این اقدامات و حملات را کنترل کرد.

باید توجه داشت وقتی صحبت از مرز می‌شود، متأسفانه تنها مرزهای جغرافیایی به ذهن مسئولان می‌رسد؛ درحالی‌که باید توجه داشت تغییرات و تحولات صورت‌گرفته در عرصهٔ جهانی مانندِ پایان جنگ سرد، جهانی‌شدن و شکل‌گیری فضای سایبر، اشکال سنتی مرزها را دچار تغییر و دگرگونی کرده است. مرزهای سایبر، نوع جدیدی از مرزها هستند که در ارتباط با امنیت در برابر تروریسم‌ها شکل می‌گیرند. در این میان، سایبرتروریسم مانند دیگر اشکال تروریسم است که در آن مؤلفه‌ای رایانه‌ای وجود دارد. سایبر تروریسم روش نوین اقدامات تروریستی است نه نوع دیگر تروریسم. *مارک پلیت*، تعریفی از سایبرتروریسم ارائه کرده است که بر اطلاق این واژه بر حمله‌ای عامدانه با اهداف سیاسی اشاره دارد که علیه مدیریت سامانه‌های اطلاعاتی طراحی شده است و می‌تواند برای اهدافی که در وضعیت مخاصمه نیستند، عواقب جدی ایجاد کند (Foggetti, 2009: 366).

تروریست‌های سایبری به طور معمول، نقاط حساس و حیاتی جوامع را هدف می‌گیرند تا اساسی‌ترین ضربه‌ها را به دشمنان خود وارد کنند، و با استفاده از شبکه‌های اینترنتی که در دسترس همگان قرار دارند، اهداف و نتایج فعالیت‌های خود را در کوتاه‌ترین زمان در سطح جهان اطلاع‌رسانی کنند. دغدغهٔ اصلی تمامی مخاطبان این تئاتر وحشتناک، خسارت‌های سنگین و گاه جبران‌ناپذیر مالی و جانی است. حاصل تلاقی اعمال تروریستی سنتی و استفاده از تکنولوژی نوین مبتنی‌بر سیستم‌های رایانه‌ای، تروریسم سایبری است. اشخاص یا گروه‌های تروریستی سایبری با استفاده از امکانات نامحدود و حتی گاهی رایگان، می‌توانند فضای سایبر را در سرتاسر جهان با فشاردادن کلیدی به مخاطره بکشانند. همچنین با استخدام نیروهای متخصص در زمینهٔ فناوری اطلاعات، از جمله «نفوذگران»، «کرکرها» و «فریک‌ها» با انتشار بدافزارهای مخرب رایانه‌ای در عرض چند ثانیه، هزاران سیستم رایانه‌ای و مخابراتی را در جهان آلوده کنند؛ بنابراین محدودهٔ اقدام‌های تروریستی سایبری به اندازه‌ای گسترده است که در ارتکاب آن‌ها، رایانه هم نقش افزار دارد و هم نقش هدف یا موضوع. بر این اساس، با توجه به شرایط حاضر یعنی گسترش وسعت تحرکات گروه‌ها و اقدامات تروریستی در جهان و ازسوی‌دیگر شرایط ویژهٔ جمهوری اسلامی ایران به‌عنوان یکی از قربانیان تروریسم، درپیش‌گرفتنِ راهبردهایی برای کنترل تروریسم، اهمیت و جایگاه بالایی دارد. بر این مبنا در مقالهٔ حاضر تلاش شده است، راهبرد مدیریت مرزهای فضای سایبر مورد بررسی و تحلیل قرار گیرد.

کنترل تروریسم سایبری با مدیریت فضای سایبر راهبردی

شکل شماره 1. فضای سایبر به‌مثابه قلمرویی نوین



2. ادبیات و مفاهیم تحقیق

2-1. مرز

مرزها خطوطی هستند که حدود بیرونی قلمرو سرزمین تحت حاکمیت یک حکومتِ ملت‌پایه را مشخص می‌کنند. مرز عامل تشخیص و جدایی یک واحد متشکل سیاسی یا یک کشور، از دیگر واحدهای مجاور آن است (حافظنیا، 1385: 69). به بیان دیگر، مرز خطی است فرضی در فضا که جداکنندهٔ دو ملت، دو کشور و دو نظام حکومتی است. مرز در انتهای قلمرو حقوقی و قانونی یک دولت قرار می‌گیرد (مجتهدزاده، 1385: جزوه کلاسی). برای درک بهتر این مفهوم، می‌توان چند تعریف کلی از آن ارائه داد:

- خط فرضی در فضا که من را از شما، و یک کشور را از کشور دیگر جدا می‌کند؛
- خط فرضی که مصالح من را از شما، مصالح و منافع یک حکومت را از حکومت دیگر، و مصالح یک گروه را از گروه دیگر جدا می‌کند. در یک طرف خط مرزی مایملک و منافع من،

حکومت، گروه و در سوی دیگر مایملک دیگران قرار دارد؛

- همهٔ مرزها دو طرف دارند؛ طرف من و طرف تو، طرف یک حکومت و طرف یک حکومت دیگر. مرز، بخش ضروری برای هویت‌دهی و اعتباردهی به شخص، حکومت و گروه است؛
- الگوهای حکومتی در دو طرف مرز متفاوتند؛
- الگوهای برنامه‌ریزی و اقتصادی در دو طرف مرز با یکدیگر تفاوت دارند.

در مجموع می‌توان گفت، مرزها به صورت خطوط و دیوارهایی، زندگی، هویت، خانه، کشور، حکومت، منافع (ملی) وغیره ما را از دیگران جدا می‌کنند و به ما و آن‌ها اعتبار و هویت می‌دهند. با نگاهی به اطراف خود و مرزهایی که در اطراف وجود دارد می‌توان این موضوع را بهتر درک کرد (حافظ‌نیا و جان‌پرور، 1392: 32).

2-2. مدیریت مرز

مدیریت مرز اغلب به روش‌ها و فناوری‌هایی که به افراد، دولت‌ها و حکومت‌ها کمک می‌کند تا مسائل مرزی، رفت‌وآمد افراد و کالا، استفادهٔ بهینه از منابع مشترک وغیره را منطبق با قوانین و مقررات کشور انجام دهند، اشاره می‌کند. مدیریت مرز بیش از کنترل مرزی که گمان می‌شود مسئولیت رسیدگی به رفت‌وآمد افراد، کالاها، منابع مرزی وغیره را داشته باشد، با امنیت ملی کشور ارتباط دارد (Heinesson, 2009: 1). به عبارت ساده‌تر، «مدیریت مرز مکانیسمی برای تضمین امنیت مرزهای ملی و تنظیم حرکات قانونی در طول مرزها برای دستیابی به نیازهای متفاوت ملت از طریق ارتباط فرهنگی، اجتماعی، اقتصادی است که با مرزها فراهم می‌شود»؛ بنابراین واژه مدیریت مرز، واژه گسترده‌تری است که محدودهٔ کنترل امور اجرایی مرزها شامل اطمینان از حفظ حرمت آن‌ها را مشخص می‌کند (Pratt, 2001: 7). مدیریت مرزها را می‌توان تنظیم رابطه‌ای قائده‌مند و حساب‌شده دانست که بتوان تا حد امکان مرزهای کشور را در عرصه‌های مختلف باز گذاشت تا روابط، رفت‌وآمد افراد، کالاها، اطلاعات وغیره به‌راحتی در آن جریان داشته باشد، و ازسوی‌دیگر مرزها را تا آن اندازه بسته نگاه داشت که ناامنی‌ها، بی‌نظمی‌ها و سایر چالش‌ها و مسائل فراسوی مرزها نتواند وارد فضای کشور و جامعه شده و زمینهٔ بی‌نظمی و ناامنی را در کشور به وجود آورد (Janparvar & others, 2014: 61-62).

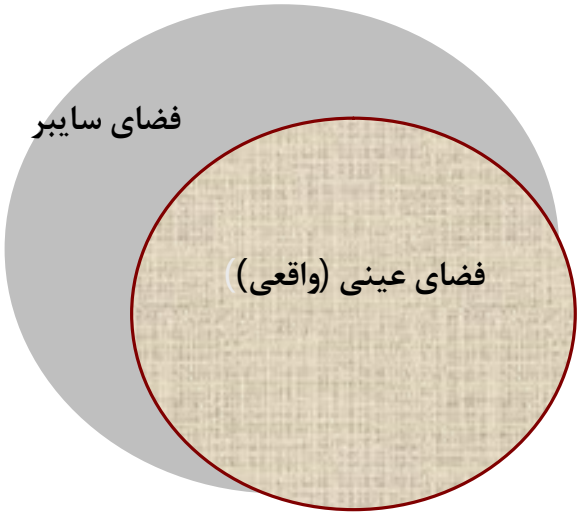
2-3. چیستی فضای سایبر

ویلیام گیبسون در رمان علمی ـ تخیلی «نورومونسر»[1] اصطلاح فضای سایبر را ابداع کرد (Gibson, 1984: 69). منظور از فضای سایبر، فضایی مجازی با ترکیبی از ده‌ها هزار رایانهٔ به‌هم‌پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سوییچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در سیستمی جامع فراهم می‌آورد (محمدی، 1389: 77). در بُعد چیستی، فضای سایبر از دیدگاه سخت‌افزاری، شبکه‌ای جهانی از کامپیوترهای به‌هم‌پیوسته است که کانال‌های ارتباطی پُرسرعتِ تارعنکبوتی را شکل داده‌اند و سریع‌تر از مصنوعات دیگر انسان، در حال گسترش است. اینترنت که نمایشی از فضای مجازی است، بستر هیجان‌انگیزی را ایجاد کرده است که قابلیت ارائه خدمات متنوع، سریع و جذاب دارد. ارتباطات سریع، قابلیت ارسال پیام، ارائه سرویس‌های ارتباطی، و تبادل اطلاعات با فرمت‌های مختلف از خدمات متنوع این ابرشبکه است (Mutula, 2007: 15).

از سوی برخی کارشناسان، فضای سایبری «تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی یا کاربران آن شکل می‌گیرد»، تعریف شده است (Sharp & Lord, 2011: 10). فضای سایبر به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون درنظرگرفتن جغرافیای فیزیکی گفته می‌شود (هاتف، 1386: 50). فضای سایبری محیطی غیرملموس و غیرفیزیکی است که با اتصال شبکه‌های ارتباطی یا مخابراتی به وجود آمده است. محتوای این فضا ناملموس و مجازی است که به آن داده گفته می‌شود و شامل صوت، تصویر، نوشته، سند و از این دست موارد است که ظرفیت انجام فعالیت‌های مختلف را دارد (آلبوعلی، 1392: 35). باید توجه داشت فضای سایبر چیزی جدا از فضای واقعی نیست، بلکه تحت تأثیر فضای واقعی به وجود آمده است که بر آن تأثیر متقابل می‌گذارد و از آن تأثیر می‌پذیرد (جان‌پرور، 1386: 56). روابط بین فضای واقعی و سایبر را می‌توان به صورت شکل شماره 2 نشان داد.

1. Neuromancer

شکل شماره 2. رابطهٔ بین فضای واقعی و فضای سایبر



منبع: حافظ‌نیا و جان‌پرور، 1392: 76.

2-4. تروریسم سایبری

این واژه نخستین‌بار از سوی *کالین باری* در دهه 1980 مطرح شد و بیشتر به معنای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره‌شده در آن‌هاست (قاسمی، 1394: 230). به گفتهٔ کانوی، تروریسم سایبری عبارت است از حملهٔ عمدی و آگاهانه با انگیزه‌های سیاسی به وسیله گروه‌های فروملی یا عوامل پنهانی علیه اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها که منتهی به خشونت علیه افراد غیرنظامی شود (Seddon, 2004: 20). تروریسم سایبری در واقع به طیفی از عملیات اطلاعاتی علیه موجودیت یک کشور گفته می‌شود که برای رسیدن به اهداف سیاسی انجام می‌گیرد (Theohary, 2015: 5). محدودهٔ اقدام‌های تروریستی سایبری به اندازه‌ای گسترده است که رایانه در جهت ارتکاب آن‌ها، هم نقش افزار و هم نقش هدف یا موضوع را دارد (فضلی، 1395: 5). به‌هرحال، امروز دنیای رایانه که در ارتباط با زندگی مردم است، دنیایی است که هر لحظه مورد تهدید تروریست‌هاست و این نگرانی از احتمال وقوع، هرچه بیشتر مردم جوامع را دچار ترس و وحشت می‌کند (طیب، 1382: 89). اقدام تروریست‌ها شامل افزایش منابع برای حمایت از عملیات‌های خود، برنامه‌ریزی عملیات، استفاده از ابزارهای در دسترس همانند Google Earth، فرماندهی و کنترل عملیات، انجام عملیات‌های نفوذی و آموزش به هواداران خود،

و استقرار وسایل انفجاری می‌شود (Starr, 2009: 18). ازسوی‌دیگر در تروریست سایبری زیرساخت‌های الکترونیکی، مقیاس بازی، وضعیت هویتی شهروندان، و نوع تصویرسازی از گفتمان رسانه‌ای نیز می‌تواند مهم انگاشته شود (Jarvis, 2017: 64). امروزه تروریسم سایبری افکار شهروندان را نیز تحت تأثیر قرار داده است؛ مانند اندیشه و بیان یک حمله تروریستی در فرودگاه یا تیراندازی در مرکز خرید وغیره. هدف امروزی تروریسم سایبری، نابودی روان شهروندان است (Gross, 2016: 288).

3. روش تحقیق

روش اصلی این تحقیق، با توجه به ماهیت نظری آن توصیفی ـ تحلیلی است. برای گردآوری و فیش‌برداری از اطلاعات کتابخانه‌ای و اینترنتی استفاده شده است. پرسش اصلی تحقیق این است که راهبرد مدیریت مرزهای فضای سایبر کشور در برابر تروریسم فضای مجازی به چه صورتی باید مورد توجه قرار گیرد؟ بر این اساس، تلاش شده است علاوه بر تصویرسازی درست از مرزها در فضای سایبر، به تشریح و تبیین چگونگی مدیریت مرزهای جمهوری اسلامی ایران در فضای سایبر برای کنترل تروریسم پرداخته شود. ازآنجاکه در بیشترِ حمله‌های تروریستی، منشأ و مبدأ ورود، سامان‌دهی، هدایت وغیره از فراسوی مرزهای کشور صورت می‌گیرد و برای ورود به کشور باید از مرزها عبور کند، مدیریت مرزها راهبردی کلیدی در این امر در نظر گرفته شده است.

4. یافته‌های تحقیق

4-1. مرزهای موجود در فضای سایبر

در دنیای کنونی، جهان از طریق شبکه اینترنت به‌شدت متداخل شده و فواصل دور، بسیار نزدیک و در جوار یکدیگر قرار گرفته است. این شبکهٔ جهانی، فرصت‌ها و امکانات زیادی را برای حکومت‌ها و ملت‌ها فراهم ساخته است؛ ولی نگرانی‌های فزاینده‌ای نیز در حفظ ارزش‌های حیاتی و امنیت ملی به وجود آورده است. شکل‌گیری فضای سایبر بر پایه اتصال شبکه جهانی اینترنت، به‌روشنی گویای این واقعیت است که ویرانگری و آسیب‌رسانی می‌تواند در یک لحظه، سراسر جهان را فرا گیرد. سوءاستفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی، آسایش عمومی و موجودیت جامعه را به مخاطره انداخته و تأثیرهای منفی زیادی بر زندگی افراد اجتماع تحمیل کند (وایلدینگ، 1379:

11). با توسعهٔ رسانه‌های الکترونیکی، در کنار جرایم سنتی یادشده، فرصت‌های تازه‌ای برای ایجاد ناامنی از سوی گروه‌های تروریستی فراهم شده است که قابلیت ارتکاب در محیط خارج از رایانه را ندارند مانندِ حملهٔ ویروس‌ها، ورود غیرمجاز به وب‌سایت‌ها و هک‌کردن آن‌ها، سرقت و سوءاستفاده از داده‌ها و خسارت‌زدن به رایانه‌ها. پیشرفت فناوری رایانه، شرایط و بسترهای مناسبی را برای سرقت اطلاعات (وایلدینگ، 1379: 29)، تکثیر نرم‌افزارهای غیرمجاز، سوءاستفاده از بازار سهام، تجاوز به حقوق مالکیت معنوی و مهم‌تر از همه تهاجم فرهنگی آماده کرده است (واسیلاکی، 1384: 19).

با توسعهٔ فضای سایبر، شبکه به دنیای «واقعی» متصل شده و واقعیت حقوقی، داخل فضای سایبر شده است؛ جایی که جنبه‌های مختلفی از مسائل مانند جنگ سایبری، تروریسم سایبری، حمله‌های سایبری، تشکیل ارتش سایبری، تشکیل پلیس سایبری، قوانین مالیاتی، حقوق مالکیت معنوی، تجارت الکترونیک و غیره در آن شکل می‌گیرد (Wilske, 2004: 3). ازسوی‌دیگر باید توجه داشت گروه‌های تروریستی بیشترین استفاده را از ظرفیت‌ها و پتانسیل‌های فضای سایبر برای دستیابی به اهداف خود یعنی تدارک اقدامات تروریستی، پشتیبانی اطلاعاتی، جذب نیرو وغیره برده‌اند. این بهره‌گیری سبب شده است تا مفهوم تروریسم مدرن مطرح شود. تروریسم مدرن نوع تازه‌ای از کشمکش است که از قرن نوزدهم به این سو، در صحنه‌های خشونت اجتماعی تولد یافته است. این شکل از تروریسم، در مقابل شکل سنتی، با توجه به نکات ضعیف ذاتی خویش، می‌کوشد تا رسانه به‌ویژه اینترنت را شبیه یکی از متحدان خود جذب کند. دیدگاهِ تروریست‌ها نسبت به ارتباطات و رسانه مانندِ سلاحی بالقوه است و تمایل دارند اقدامات و باورهای خویش را به وسیلهٔ آن برجسته سازند. در این راستا، *چرنیا. م باسیدن* معتقد است پوشش‌های خبری رسانه‌ها نقش نفوذپذیری در اشاعهٔ اهداف تروریستی دارند. او دلایل خود را بدین‌گونه بیان می‌دارد:

1. پوشش‌های خبری رسانه‌ها در بزرگ‌کردن و اهمیت‌دادن به تهدیدهای تروریست‌ها در ذهن افکار عمومی، نقش بسزایی دارند؛

2. رسانه ترس را پراکنده می‌سازد؛

3. رسانه تروریست‌ها را در انتخاب اهداف و به‌حداکثررساندن تبلیغات مورد نظرشان یاری می‌دهد (رهنورد، 1385: 905-903).

با پیشرفت فناوری، بسیاری از حکومت‌ها در دفاع سایبری در برابر ارتباطات الکترونیکی که از

مرزهای سرزمینی آن‌ها عبور می‌کنند، از طریق متوقف‌کردن یا قاعده‌مندکردنِ جریان اطلاعات، پاسخ داده‌اند (Johnson & Post, 2003: 4). حکومت‌ها سعی در گسترش و به‌روزکردن ابزارها و تکنیک‌های مدیریتی و نظارتی خود از طریق فناوری‌های نوین اطلاعاتی و ارتباطی می‌کنند و شکل‌های تازه‌ای از مدیریت و نظارت فضای سایبر کشور از طریق مدیریت بهینهٔ مرزهای موجود در این فضاها را شکل داده و گسترش می‌دهند (Vilken, 2001: 62). دولت‌ها می‌کوشند با استفاده از مدیریت مرزها بتوانند چالش‌ها و مسائل ناشی از تحولات فضای سایبر را بر فضای ملی و کشور خود کاهش داده و منافع و امنیت ملی را از طریق دفاع سایبری تأمین کنند. در این راستا، همچون فضای واقعی باید در برابر اقدامات و حملات تروریستی اقدامات کنترلی صورت گیرد تا بهره‌گیری این گروه‌ها از ظرفیت‌ها و پتانسیل‌های فضای سایبر کاهش یابد. از جملهٔ این راهبردها، مدیریت مرزهای موجود در فضای سایبر است که نقش مهمی در پیشگیری از بهره‌وری گروه‌های تروریستی دارد.

4-1-1. فیلترها

فیلتر اینترنتی یا نرم‌افزار کنترل محتوا، به معنای کنترل محتوا در فضای سایبر است که به نرم‌افزارهای کنترل محتوای مورد تقاضای کاربران اطلاق می‌شود. نرم‌افزار کنترل محتوا، ابزاری است که تعیین می‌کند کدام کاربر اجازهٔ مشاهدهٔ چه محتوایی را دارد. فیلترینگ می‌تواند در مواردی مانندِ دسترسی افراد به اطلاعات طبقه‌بندی‌شده در شرکت‌ها، سازمان‌ها، دسترسی غیراخلاقی، دسترسی به مطالبی در زمینه ترویج خشونت، استعمال مواد مخدر، الکل، قمار، دسترسی کارمندان یک اداره به اطلاعات یا برنامه‌های غیرضروری در محیط کار، دسترسی به مطالب سیاسی، دینی یا ضد دینی، امنیتی وغیره قابل‌استفاده باشد (http://forum.omegapars.com). کشورهای مختلف جهان برای اِعمال فیلترینگ در شبکه و فضاهای سایبر، سیاست متفاوتی را در پیش گرفته‌اند و هریک بنا به ملاحظه‌های خاص، خط قرمزهایی را در این فضا اِعمال کرده‌اند و مکانیسم‌های تعیین‌شده‌ای را به شهروندان ارائه می‌دهند. برای مثال، در این زمینه چین اعلام کرده است راهبردی برای تنظیم اینترنت و اِعمال حاکمیت و واپایش آن، به صورت «محو آنچه ناخواسته بوده و حفظ آنچه خوب است» دارد. حکومت چین معتقد است، اینترنت ابزاری برای کمک به تجارت است و تنها این بخش‌ها در اینترنت قابل‌اهمیت بوده و اطلاعات دیگر شامل حمایت مخصوص نخواهند بود. در واقع، چین به‌نوعی خواهان آن است تا تمامی اطلاعات، غیر از زمینه‌های تجاری را از دسترس خارج کند؛ بنابراین دسترسی به محتویات خارجی و نیز اطلاعات خارج از این

زمینه‌ها نیاز به اجازهٔ حکومت دارد. در این زمینه نیز دسترسی آزاد به اینترنت در داخل مرزهای چین، به تعداد اندکی از اشخاص انتخاب‌شده محدود بوده و بیشتر در ارتباط با استفاده‌های علمی و صنعتی از رایانه است (گوردون، 2006: 10). فیلترینگ اینترنت در ایران عبارت است از: اِعمال سانسور، محدودیت و نظارت ساختاریافته و هدفدار بر دسترسی به محتوای سایت‌ها و استفاده از سرویس‌های اینترنتی برای کاربران ایرانی. فیلترینگ در ایران براساس قوانین مصوب مجلس شورای اسلامی اِعمال می‌شود و طیف گسترده‌ای از سایت‌های اینترنتی، از پورنوگرافی گرفته تا سیاسی را شامل می‌شود (بدیعی، 1392: 308).

4-1-2. کدهای مخابراتی

همهٔ ما به قدرت و سرعتِ پردازش مخابرات وابسته‌تر می‌شویم، اما در واقع فضای نوین مخابرات فضای جهانیِ هموار و یکدستی نیست که پیام‌ها بدون هیچ‌گونه برخوردی بتوانند جریان یابند (جانستون، 1383: 4). پس از رادیو و تلویزیون، شناخته‌شده‌ترین دستگاه مخابراتی در دنیا، تلفن است. همزمان با پیشرفت‌های گوناگون مخابرات، موضوعات جدیدی از مسائل خط‌مشی ملی و جهانی پدیدار می‌شود. اتحادیه بین‌المللی مخابرات که بخشی از مسئولیت آن استانداردکردن مخابرات در سراسر دنیاست، از طریق انجمن مشاورهٔ بین‌المللی تلگراف و تلفن، برنامهٔ شماره‌گیری جهانی را طرح‌ریزی کرده است که در آن، به هر کشور، یک کد دو یا سه‌رقمی برای متمایزشدن از دیگر کشورها داده شده است. ایران نیز مانند همهٔ کشورهای جهان با گسترش دستگاه تلفن به‌عنوان شناخته‌شده‌ترین دستگاه مخابراتی مواجه بوده است؛ بدین‌ترتیب کدهای خاص مخابراتی که برای ایران در نظر گرفته شد، نوعی مرزبندی را ایجاد کرد که با شمارهٔ مخصوص مخابراتی مربوط به آن، محدودهٔ مرزی مشخصی شکل گرفته است (جان‌پرور، 1392: 111).

4-1-3. کارت‌های اعتباری

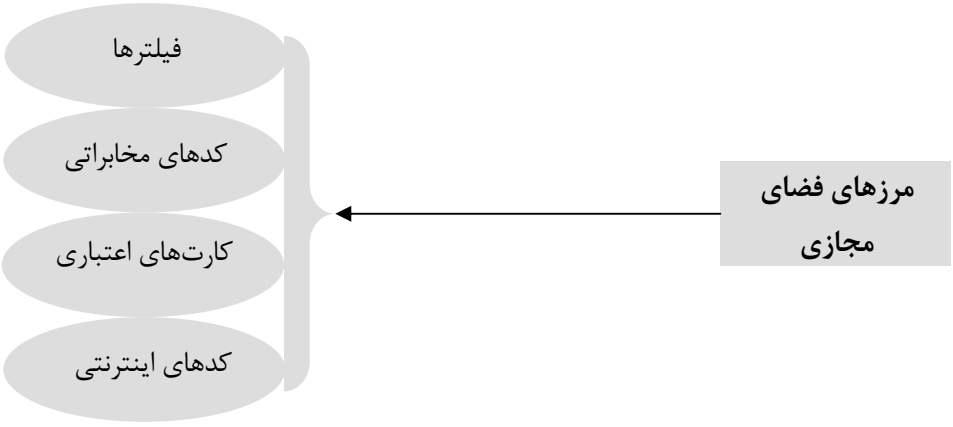
کارت‌های اعتباری تنها نوع کارت‌های پرداختی هستند که غیر از آسان‌سازیِ دریافت، پرداخت و تسریع در گردش پول از طریق پرداخت الکترونیکی، امنیت خریدار به دلیل حمل‌نکردنِ پول نقد، کاهش ریسک پذیرش پول تقلبی وغیره، وارد مقولهٔ اعتبار شده‌اند. پولِ روی کارت اعتباری از انواع تسهیلاتی است که بانک‌ها به صورت الکترونیکی به مشتریان می‌دهند. این نوع کارت‌ها محبوبیت خاصی در امریکا دارند و عمده کارت‌های صادره در این کشور از این نوع هستند. امروزه در کشور

ما نیز بانک‌ها اقدام به صدور انواع کارت کرده‌اند ولی تاکنون کارت اعتباری به شکل رایج آن در جهان، در کشور ما پیاده‌سازی نشده است (http: //novinbank.blogfa.com). در ایران به‌رغم پیشرفت در زمینه خدمات بانکداری الکترونیکی و ارائه کارت‌های اعتباری، به دلایلی مانند تحریم و ارائه‌نشدنِ سرویس‌های کارت اعتباری توسط شرکت‌های بین‌المللی و همچنین فرسودگی و کهنگی شبکه بانکی کشور، امکان ارائه سرویس مطلوب در داخل وجود ندارد.

4-1-4. کدهای اینترنتی

در راستای تحولات صورت‌گرفته در عرصهٔ فناوری‌های اطلاعاتی و ارتباطی و آسان و به‌صرفه‌شدن دستیابی، اینترنت به مهم‌ترین سامانه الکترونیکی در جهان تبدیل شده و این روند بسیاری از مردم جهان را به یکدیگر متصل کرده است. در راستای تکامل اینترنت و شکل‌گیری فضای رایانه‌ای، این فکر در میان کاربران ایجاد شد که سامانهٔ الکترونیکی اینترنت، فضایی بدون مرز است و هیچ قاعده، قانون و حاکمیتی ندارد، اما واقعیت چیز دیگری را نشان می‌دهد و آن این است که در این فضای رایانه‌ای، به هر کشور برای مجزاشدن از سایر کشورها، یک پسوند داده می‌شود که نشان‌دهندهٔ جدایی کشورها در این سامانهٔ الکترونیکی است. در ایران کدهای اینترنتی معمولاً با دامنه ir شناخته می‌شوند که در پایان همه آدرس‌های الکترونیکی علمی، ملی و پست‌های الکترونیکی خاص ایران آورده می‌شود (جان‌پرور، 1392: 113).

شکل شماره 2. مرزهای فضای مجازی



منبع: جان‌پرور، 1387: 151.

4-2. ویژگی‌های تهدید سایبری

سایبر پدیدهٔ نوینی است که در دهه‌های اخیر، هم‌زمان با تحول فناوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است؛ به‌گونه‌ای‌که امروزه چالش‌های مرتبط با تروریسم سایبری، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت نوین تهدیدها از سوی تروریست‌های سایبری و ویژگی‌ها و نمودهای منحصربه‌فردی است که شناخت آن را بسیار مهم و ضروری می‌نماید. تهدیدهای سایبری شبیه وقایعی است که به صورت طبیعی یا توسط انسان (عمدی یا غیرعمدی) بر فضای مجازی تأثیر گذاشته است، یا حوادثی که از طریق فضای مجازی عمل می‌کند، یا به نحوی به آن مرتبط باشد (رکن‌آبادی، 1391: 170). تهدیدهای سایبری ویژگی‌های منحصربه‌فردی دارند. ازیک‌سو، گسترهٔ وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و ازسوی‌دیگر، هزینهٔ اندک، تأثیرگذاری شگرف و فقدان شفافیت عمومی در فضای سایبری، موجب شده است تا بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تروریسم سایبری در مؤلفه‌های زیر خلاصه می‌شود:

4-2-1. تعدد بازیگران در فضای سایبری

هزینهٔ پایین فناوری رایانه‌ای، اتصال گسترده به اینترنت و آسانیِ ایجاد یا به‌دست‌آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هر کسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافتهٔ جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت‌ملت‌ها هستند (Charney, 2009: 5). آمار نیروی انسانی و تجهیزات طرفین درگیری، تأثیری در جنگ‌های سایبری نخواهد داشت، زیرا جنگ نامتقارن یا ناهمتراز است (صدرزاده، 1390: 367).

4-2-2. هزینهٔ پایینِ ورود، صرف زمان اندک و سرعت بالای اقدام

فضای مجازی، هزینهٔ جرایم ارتکابی را برای تروریست‌ها از نظر نتایج اقدامات و احتمال دستگیری و مجازات به شکل قابل‌ملاحظه‌ای کاهش داده است. با توجه به اهمیت هزینهٔ جرم برای تروریست‌ها، ماهیت فرامرزی فضای مجازی فرصت بسیار مغتنمی برای اقدامات تروریست‌ها در گسترهٔ جهانی است، چراکه با وجود دستیابی به اهداف مخرب پیش‌بینی‌شده، امکان به‌دام‌افتادن آن‌ها به حداقل می‌رسید. هر فرد برای انجام حمله سایبری تنها به یک رایانه، ارتباط اینترنتی و دانش فنی محدود در

زمینهٔ فضای سایبری نیاز دارد؛ در نتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینهٔ پایین می‌توان اقدامات خطرناکی را در مدت زمان اندک و با سرعت بالا انجام داد. البته انجام حمله‌های پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord & Sharp, 2011: 20-28).

4-2-3. ناشناس‌ماندن بازیگران و فقدان قابلیت ردیابی

اینترنت به شکل سیستمی نامتمرکز طراحی شده است و کاربران آن اغلب شناخته‌شده نیستند. همین ناشناختگی سبب می‌شود اثری از برخی حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند از جای‌جای دنیا، بدون هشدار و در عرض چند ثانیه و بی‌آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را هدف قرار دهند (جیستان، 1390: 249). به سبب ویژگی‌هایی که در ذات پروتکل‌های ارتباطی در فضای سایبر وجود دارد، در عمل شناسایی و ردیابی منبع اصلی حمله، بسیار دشوار و گاهی غیرممکن است. در حقیقت اگر در این زمینه، تشریک مساعی مرزهای سایبری را نادیده انگاریم، شناسایی غیرممکن است. برای مثال اگر به قالب سرآیند IP توجه کنید، خواهید دید که تغییر فیلد آدرس مبدأ و سپس تزریق بسته در شبکه، به‌سادگی و حتی توسط کاربران بسیار مبتدی امکان‌پذیر است؛ بنابراین مبدأ ناشناس و مبهم خواهد ماند (غروری و محمدی، 1390: 79).

4-2-4. تأثیرگذاری شگرف

ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجهٔ آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی ازدست‌دادن جان انسان‌ها شود، زیرا در این‌گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند (ابراهیمی، 1393: 11).

4-2-5. کمرنگ‌شدن نقش جغرافیا

ویژگی‌های بی‌همتای فناوری‌های اطلاعات و ارتباطات، تحولات بنیادینی را در قلمرو حیات بشری پدید آورده است که نخستین موردِ آن، جهان‌گیری گسترش این فناوری‌هاست. این ویژگی سبب شده است فناوری‌های اطلاعات و ارتباطات نفوذ جهان‌گسترانه‌ای به دست آورند و در گسترهٔ

جغرافیایی خاص و محدودی نگُنجند. به عبارت بهتر، فناوری‌های اطلاعات و ارتباطات تمامی مرزها را درمی‌نوردند و از جهان مرززدایی می‌کنند. این مرززدایی و کمرنگ‌کردن مرزهای سنتی، زمینهٔ آسان‌سازی حرکت هرچه آزادانه‌ترِ کالا، سرمایه و افراد را فراهم می‌کند (Everard, 2000: 62). فضای سایبری سرعت انتقال به سراسر جهان را در لحظهٔ کوتاهی فراهم کرده است؛ بنابراین تهدیدکنندگان قادر به فراتر رفتن از محدودهٔ جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند (Starr, 2009: 18).

4-2-6. ساختار فضای اینترنت

اینترنت، دامنه‌ای مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است. توانایی محدود برای جداکردن بازیگران و فعالیت‌های آن‌ها، و پاسخ مناسب به آن‌ها، ساختار تهدید را سخت‌تر کرده است (Charney, 2009: 5-6). اینترنت، دولت‌ها و شرکت‌های خصوصی را با فقدان اطمینان در قبال خطرهای فضای اینترنتی مواجه کرده است. این نبودِ قطعیت ناشی از پیچیدگی‌ها و فناوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است (Haller & Et al, 2010: 4).

4-3. بسترهای فراهم‌کنندهٔ سایبر تروریسم در جمهوری اسلامی ایران

4-3-1. ضعف در حوزه نیروی انسانی

فعالیت‌های محدودی در حوزه توسعه سطح دانش، آگاهی عمومی و اطلاع‌رسانی به عامهٔ مردم در کشور صورت گرفته است و فعالیت‌های انجام‌شده بیشتر موردی، محدود و کوتاه‌مدت بوده است. ضعف دانش و تجربهٔ امنیت سایبری در عامه مردم و کاربران عمومی رایانه و کارشناسان و کاربران تخصصی و همچنین مدیران بخش‌های رایانه و شبکه‌های رایانه‌ای، کارشناسان و مدیران امنیت سایبری، مدیران سطوح مختلف در سازمان‌های دولتی و خصوصی و همچنین مشاوران عالی، سیاست‌گذاران و قانون‌گذاران مشهود است. علاوه بر آن، تعداد محدودی از برنامه‌نویسان دربارهٔ امنیت رایانه و شیوهٔ تولید نرم‌افزارهای ایمن آموزش دیده‌اند. ضعف اطلاع‌رسانی گاه به اندازه‌ای بوده است که آگاهی کافی از خطرات و جدی‌بودن آن وجود نداشته و به این مقوله به چشم داستان علمی ـ تخیلی نگریسته می‌شود. گذشته از این، از نظر کمّی نیز تعداد کارشناسان و مدیران امنیت

سایبری در کشور محدود است و فعالیت قابل‌توجهی در آموزش و تربیت چنین کارشناسانی در سازمان‌ها مشاهده نمی‌شود. ازسوی‌دیگر، توان سازمان‌ها به‌ویژه سازمان‌های دولتی در جذب و نگهداری چنین کارشناسانی محدود بوده است. مهاجرت افراد صاحب دانش و تجربه به کشورهای بلوک غرب که سال‌هاست ادامه دارد، کشور را دچار آسیب‌پذیری دوچندان می‌کند. این موضوع سبب تقویت تسلط نرم‌افزاری این کشورها و افزایش فقر نرم‌افزاری در کشور خواهد شد.

4-3-2. ضعف صنعت نرم‌افزار

صنعت نرم‌افزار در کشور رشد محدودی داشته است و دارای عمق کافی نیست که بتواند ایجادکنندهٔ سطحی از تسلط نرم‌افزاری باشد. از دیدگاه اقتصادی، محدودیت بازار داخلی به علت رواج نقض حقوق پدیدآورندگان نرم‌افزار و محدودیت در دسترسی به بازارهای صادراتی ازیک‌سو و محدودیت در دستیابی به منابع مالی و بازار سرمایه ازسوی‌دیگر، زمینهٔ مناسبی را برای رشد اقتصادی تولیدکنندگان نرم‌افزار ایجاد نکرده است. ضعف در سطح دانش، تجربه و مهارت در جنبه‌های عمومی مدیریت، ضعف در بازاریابی و ضعف در کمیّت و کیفیت برنامه‌نویسان و محدودیت در همکاری‌ها و مشارکت با شرکت‌های خارجی توانمند، موجبات توسعه‌نیافتگی علمی و تجربی صنعت نرم‌افزار را فراهم کرده است.

4-3-3. تحریم‌ها

تحریم‌های وضع‌شده علیه کشور موانعی را در زمینهٔ توسعهٔ نرم‌افزار در کشور ایجاد کرده است. بروز مشکل در دریافت نرم‌افزارهای اصلی و دریافت خدمات پس از فروش و ضعف در امکان به‌روزرسانی نرم‌افزارها ازیک‌سو و رواج استفاده از نرم‌افزارهای غیراصلی به صورت فلّه در بازارهای نرم‌افزاری داخل کشور و دسترسی به نرم‌افزارهای مختلف از طریق محیط‌های به‌اشتراک‌گذاری فایل ازسوی‌دیگر، آسیب‌پذیری‌های خطرناکی را ایجاد کرده است که می‌تواند در صورت بروز حمله سایبری توسط دشمن، به‌راحتی قابل بهره‌برداری باشد. گفتنی است ارائه نرم‌افزارهای فلّه بدون هیچ‌گونه نظارت و بازبینی محتویات صورت می‌گیرد و در موارد زیادی آلوده به بدافزارهای خطرناکی هستند که خود یکی از راه‌های رواج آلودگی در کشور به شمار می‌روند.

تحریم‌ها در حوزه نرم‌افزار تناقضی را برای کشور به وجود آورده‌اند. ازیک‌سو در صورت

قانونی‌شدن الزام رعایت حقوق پدیدآورندگان نرم‌افزارهای خارجی، با توجه به تحریم‌ها و فروش‌نرفتنِ این نرم‌افزارها در داخل کشور، استفاده از این نرم‌افزارها غیرقانونی و ناممکن می‌شود و ازسوی‌دیگر در صورت خرید غیرمستقیم و با واسطه، امکان استفادهٔ مناسب از محصول خریداری‌شده از نظر نبودِ امکان برخورداری از خدمات پس از فروش و پشتیبانی فراهم نمی‌شود. ادامهٔ وضع موجود نیز علاوه‌بر آسیب‌پذیری‌های ناشی از استفاده‌نکردن از نرم‌افزار اصلی، به لحاظ استفاده تقریباً رایگان از این نرم‌افزارها بازار داخل را محدود و صنعت نرم‌افزار کشور را دچار ضعف و عقب‌ماندگی کرده است.

4-3-4. فضاسازی رسانه‌ای از طریق وبلاگ‌ها

وبلاگ این امکان را فراهم می‌کند تا فرد با بهره‌گیری از روابط شبکه‌ای، گسترهٔ وسیع و متنوعی از تعاملات را فارغ از محدودیت‌های مکانی، زمانی و فرهنگی ایجاد کند. وبلاگرها می‌توانند بدون هزینه و در کوتاه‌ترین زمان ممکن برای خود وبلاگ ساخته و اندیشه‌ها و آرای خود را پیرامون موضوعات و مسائل مختلف در دسترس یکدیگر قرار دهند؛ در جریان انتخابات دهم ریاست‌جمهوری، وبلاگ‌ها یکی از راه‌های برقراری ارتباط میان برخی معترضان داخلی با عناصر معاند نظام در خارج از کشور بودند. در همین زمینه نقش برخی از مراکز پژوهشی نیز اهمیت دارد. برای مثال، دانشگاه کلمبیای امریکا در چهارم و پنجم دسامبر 2008 (14 و 15 آذرماه 1387) سمیناری دوروزه با عنوان نقش بلاگرها در هماهنگی، ایجاد و گسترش جنبش‌های اجتماعی و اعتراضی در وبلاگ‌ها برگزار کرد. هدف اصلی این سمینار، آشنایی وبلاگ‌نویسان با آخرین روش‌ها و فنون وبلاگ‌نویسی برای هماهنگی و رهبری اعتراض‌های خیابانی بود؛ به‌طوری‌که بخشی از تحرکات براندازانهٔ مخالفان نظام در فضای مجازی پس از دهمین انتخابات ریاست‌جمهوری، از راهکارهای ارائه‌شده در این کنفرانس کپی‌برداری شده بود. وبلاگ یکی از مهم‌ترین ابزارهای نرم‌افزارگرایانه است که می‌تواند در راستای تضعیف امنیت اجتماعی از طریق شکل‌دهی به افکار عمومی و ترجیحات به‌ویژه در سطح منازعات قومی و فرقه‌ای به کار گرفته شود. گسترش وبلاگ‌ها در فضای وب با هدف تبلیغ علیه نظام و آرمان‌های آن، از جمله عوامل بسترساز تروریسم سایبری است (نورمحمدی، 1390: 142).

4-3-5. گسترش شبکه‌های اجتماعی

شبکه‌های اجتماعی آن دسته از محیط‌های جذب کاربران در فضای سایبری است که با فراهم‌کردن امکان اشتراک نظر و تبلیغ آزادی اعلام دیدگاه و بحث و مباحثه، بخشی از افراد جوامع مختلف را به صورت مجازی حول خود گرد آورده، آن‌ها را پیرامون محورهای مختلف (بسته به نوع جهت‌گیری و خط‌مشی مبنایی شبکه) شکل می‌دهد و از این مجرا، افکار و ایده‌ها بلکه رفتار آن‌ها را تحت تأثیر قرار می‌دهد. حجم وسیعی از اقصی‌نقاط جهان شامل کوچک‌ترین حوادث تا وقایع مهم در این سایت‌ها جمع‌آوری شده و به‌تدریج به منبع اطلاعاتی مهمی برای انجام عملیات جاسوسی و کسب اطلاعات از وضعیت سیاسی و اجتماعی کشورها تبدیل می‌شود. در واقع طبیعت شبکه‌های اجتماعی به گونه‌ای است که سبب ایجاد حمله‌های وسیع و سوءاستفاده‌هایی می‌شود که اطلاعات را برای دشمنان آشکار کرده و مسیری ساده برای خروج اطلاعات ایجاد می‌کند. ایالات متحده امریکا تحت عنوانِ دیپلماسی عمومی، فعالیت گسترده‌ای را برای ترویج استفاده از شبکه‌های اجتماعی دنبال کرد. نظامیان نیروی دریایی امریکا که با استفاده از شبکه‌های اجتماعی مانند «فیس‌بوک» و «توییتر» با خانواده و دوستان خود ارتباط برقرار می‌کردند، با ممنوعیت استفاده از شبکه‌های اجتماعی مواجه شدند. برخی از معروف‌ترین و پُرکاربردترین شبکه‌های اجتماعی فضای مجازی عبارتند از: مای اسپیس، فیس‌بوک، یوتوب، توییتر، دیلیکس و آوراستوری. گسترش شبکه‌های اجتماعی امروزه در ایران بستر مناسبی را برای ایجاد تروریسم سایبری فراهم کرده است (نورمحمدی، 1390: 143).

4-4. اهداف تروریسم سایبری در جمهوری اسلامی ایران

یکی از اهداف اصلی تروریسم نوین و جنگ نرم بیگانگان، تغییر در طرز تلقی و آمادگی روانی[1] و تقویت آیین ناهمنوایی[2] جامعه هدف است. واژهٔ آمادگی روانی به معنی آمادگی درونی بالفعل برای انجام عملی است مشاهده‌شدنی و به هر شیوه و وضعی است که یک شخص در برابر اشیای حائز اهمیت و ارزش، به خود می‌گیرد. از نظر *مینارد* آمادگی روانی عبارت است از آمادگی روانی درونی برای انجام عمل به شیوه‌ای خاص و به تجربهٔ یک موجود از وضع یا شرایطی وابسته است که باید با آن مقابله کند. آمادگی روانی از نظر ژرژ گورویچ این‌گونه تعریف شده است: مجموعه‌ها (بیشتر

1. Attitude
2. Non-Conformism

بالقوه تا بالفعل)، یا هیئت‌هایی اجتماعی که متضمن آمادگی‌های روانی، اعمالی حاکی از تنفر یا ترجیح، آمادگی‌های پیشین برای انجام عمل و بروز واکنش‌ها و گرایش‌هایی برای تقبل نقش‌های اجتماعی مشخص، منش جمعی و بالاخره چهارچوبی اجتماعی هستند که در آن نهادهای اجتماعی تجلی می‌کنند و مقیاس‌های خاص ارزشی پذیرفته یا طرد می‌شوند (آلن، 1366: 22).

همان‌طور که از تعریف آمادگی روانی برمی‌آید، تلاش گستردهٔ بیگانگان برای ایجاد حالت تنفر از هنجارهای پذیرفته‌شده و ارزش‌های موجود اجتماعی و دینی، یکی از اهداف اصلی ترویج سایت‌های پورنو، ضد دینی وغیره است. برای مثال، تغییر نگرش کودکان و نوجوانان نسبت به حیا و عفت و سایر هنجارهای اجتماعی، افزایش تعداد سایت‌ها و وبلاگ‌های حاوی مطالب کاملاً مستهجن و تصاویر غیراخلاقی در دستور کارشان قرار می‌گیرد. همچنین لطمه به خصلت رازداری افراد و تجاوز به حریم خصوصی دیگران در راستای ایجاد ناهمنوایی است که درنهایت به افرادی ضد ارزش‌ها و نظام سیاسی جامعه‌ای که در آن زندگی می‌کنند، تبدیل شوند.

درواقع ناهمنوایی تنها نفی همنوایی نیست بلکه مخالفت با آن نیز هست. هوادار این آیین کسی است که با عادات رایج و جاافتاده، عقاید پذیرفته‌شده و ارزش‌های مسلط در محیطی اجتماعی، مخالفت می‌ورزد. رفتار چنین فردی برخاسته از انگیزه‌های آگاهانه و مغایر با ویژگی‌های محیط اجتماعی پیرامون اوست که آن را قدیمی، کهنه و تنگ احساس می‌کند، یا آنکه از واکنشی مبتنی‌بر خویش مایه می‌گیرد که ویژگی آن طغیان، اعتراض و اختلاف رأی است. چنین شخصی (ناهمنوا) می‌تواند فردگرا، هرج‌ومرج‌گرا، کژآیین یا آنکه مبدعی ساده باشد. در حال حاضر، به عادت‌ها، عقاید و ارزش‌های رایج در جامعه با تمام قوا حمله می‌شود، از جمله حجاب، احترام به هنجارهای اجتماعی، عفت و حیا، جایگاه رفیع معنویات و اخلاق، اعتقاد به معاد و یکتاپرستی، احترام به شخصیت‌های سیاسی ـ مذهبی و مسئولان نظام، پرهیز از خشونت و پرخاشگری در محیط اجتماعی، پوشش‌های متناسب اجتماعی و مورد تأکید دین و غیره. حتی مشاهده شده است که به‌تازگی توسط سایت‌ها و وبلاگ‌های مورد حمایت مستقیم بیگانگان و به دنبال آن برخی مدیران وبلاگ‌ها (خواسته یا ناخواسته)، در قالب وبلاگ‌های عاشقانه و شکست عشقی، ارتباط آزاد دختر و پسر، اشاعهٔ ناامیدی و افسردگی، ارزش‌شمردن غم و اندوه برای جنس مخالف، و هیچ‌انگاری به طرز بسیار مرموز و زیرکانه‌ای برای تمام اقشار و سنین به‌ویژه نوجوانان و جوانان به شکل ارزش و مُد

مطرح می‌شود و سعی در ترویج حمله به تمام ارزش‌های اخلاقی جامعه دارند.

در این آیین فلسفی مطرود، به ناشناخت‌انگاری مطلق پرداخته می‌شود و واقعیتِ هر آنچه مردمان به‌عنوان موجود و دارای هستی می‌شمارند، انکار می‌شود. امروزه حتی با سیاست و ایدئولوژی مشخص و مدوّن، برای ترویج پوچ‌گرایی یا هیچ‌انگاری توسط سازمان‌های مخوف تبهکاری دشمنان اسلام، اقدام می‌شود که نابودی دین‌گرایی مسلمانان است. برای مثال، آن‌ها می‌خواهند از هر طریقی شیطان‌پرستی را رواج دهند، گاهی از انگیزه‌های صرف جنسی استفاده کرده، گاهی از مدل‌های ظاهری عجیب‌وغریب مو و لباس و گاهی از وبلاگ‌هایی استفاده می‌کنند که سخن از شکست در عشق دو جنس مخالف می‌گویند و به‌تدریج زمینه را برای احساس پوچی در مخاطبان ایجاد می‌کنند. کارشناسان با بررسی مطالب وبلاگ‌هایی که بیشتر در فواصل زمانی کوتاه روزآوری می‌شوند، پی خواهند برد که تعداد ایجاد وبلاگ‌های عاشقانه و دردودل‌های عشاق شکست‌خورده، حتی از وبلاگ‌های شرکت‌های سودجو با مقاصد مالی نیز بیشتر است.

4-5. کنترل تروریسم از طریق مدیریت مرزهای فضای سایبر

تمامی حکومت‌ها دارای اطلاعات دولتی محرمانه در شکل‌های مختلف (چاپی، صوتی، الکترونیکی یا تصویری) هستند که منبع استراتژیک اِعمال حاکمیت، اتحاد ملی، منافع ملی، اهداف ملی، مدیریت کشور به شمار می‌آیند. این اطلاعات در عمر حکومت‌ها به گونهٔ مؤثری کنترل و مدیریت می‌شوند و از جایگاه بالایی برای حفظ و نگهداری و امنیت برخوردارند. با پیشرفت‌های صورت‌گرفته در فناوری و افزایش حجم اطلاعات و نیازها برای استفاده از این فناوری در نگهداری و جابه‌جایی حفاظت از اطلاعات، موضوع تمامیت و محرمانگی اطلاعات دولتی را بیش از پیش به فناوری‌های نوین مانند اینترنت و فضای سایبر وابسته ساخته است. علاوه بر اطلاعات محرمانهٔ حکومتی که می‌تواند به صورت‌های مختلف مورد حمله و تجاوز گروه‌های تروریستی قرار گیرد و کشور را با مشکل مواجه سازد، می‌توان به دادن اطلاعات غلط و تهییج‌کننده و ایجاد شایعه در میان شهروندان و تحت تأثیر قراردادن آن‌ها برای کسب منافع شخصی، زیرِ سؤال‌بُردن امنیت کشور و شخصیت‌های سیاسی، استفاده از مسائل سیاسی و قومیتی در داخل و مانوردادن روی آن‌ها با هدفِ تحریک‌کردن شهروندان کشور علیه حکومت وغیره اشاره کرد.

این مسائل سبب شده است تا حکومت‌ها مرزبندی‌ها و قواعد و قوانین ویژه‌ای برای فضای

سایبر تعیین کنند و به صورت‌های مختلف به کنترل این فضا بپردازند (Janparvar & others, 2014: 71-72). در این میان، می‌توان با درپیش‌گرفتن راهبرد مدیریت مرزهای سایبری با شناختن و شناساندن آن به جامعه و مسئولان اجرایی و پُررنگ‌کردن مرزهای موجود در این فضا تا اندازهٔ قابل‌توجهی، مانع بهره‌گیری از ظرفیت‌ها و پتانسیل‌های موجود در این فضا توسط گروه‌های تروریستی شد.

جمهوری اسلامی ایران نیز با تهدیدهای نوینی در عرصه فضای سایبری روبه‌رو است که سرمنشأ تهدیدهای کاملاً جدیدی برای ایران است که تا دههٔ پیش وجود نداشته‌اند. مفهوم کلیدی در این رابطه، تهدید در فضای سایبر است که با جنگ‌های کلاسیک کاملاً متفاوت است. برای نمونه می‌توان به هجوم شدید کرم رایانه‌ای «استاکسنت» به رایانه‌های ایران اشاره کرد که علاوه‌بر اطلاعات سیستم‌های کنترل صنعتی و نیروگاهی و تأسیسات هسته‌ای، اطلاعات سیستم‌های خانگی را نیز به سرقت بُرد و حدود 60 درصد رایانه‌های ایرانی را آلوده ساخت. تحقیقات نشان داد این کرم بدین منظور طراحی شده تا سانتریفیوژهای ویژهٔ غنی‌سازی اورانیوم را مختل کند. پیچیدگی کرم نرم‌افزاری «استاکسنت» به اندازه‌ای بود که برخی از متخصصان از آن با عنوان «تروریسم سایبری» یاد کردند. به بیانی دیگر، گروه یا کشوری با هدف تخریب ساختارهای حیاتی کشور دیگر، این نرم‌افزار مخرب را نوشته و فعال کردند. هدف‌گیری این ویروس در راستای جنگ الکترونیکی علیه ایران اعلام شد تا اطلاعات مربوط به خطوط تولید را به خارج از کشور منتقل کند. حتی گفته شد این نخستین ویروس رایانه‌ای بود که با هدف ایجاد تغییرات فیزیک در جهان واقعی ساخته شده است. روزنامه نیویورک‌تایمز در سیزدهم خرداد 1391 در گزارشی فاش کرد باراک اوباما، رییس‌جمهور امریکا در نخستین ماه‌های ریاست‌جمهوری خود، مخفیانه دستور حمله‌ای سایبری با ویروس رایانه‌ای استاکسنت را علیه ایران صادر کرده است. این عملیات نخستین حمله سایبری پایدار امریکا علیه کشوری دیگر است که با استفاده از کدهای مخربی که با همکاری اسرائیل طراحی شده بود، انجام گرفت. امریکایی‌ها همچنین ویروس سارق اطلاعات به نام «دوکو» را برای سرقت اطلاعات از زیرساخت‌های حیاتی صنعتی و نفت و گاز ایران طراحی کرده بودند که گزارش شد در سال 2011 بخشی از صنعت ایران را هدف قرار داده بود.

به‌طورکلی باید گفت هزینهٔ کم ورود، ناشناس‌بودن، مشخص‌نبودن قلمرو جغرافیایی تهدیدکننده،

تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب شده است تا بازیگران اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد، به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری وغیره را ایجاد کنند. جمهوری اسلامی ایران نیز به دلیل آنکه محیط امنیتی آن بیش از آنکه دارای فرصت باشد، تهدیدهای بی‌شماری را دربردارد، همانند هر کشور دیگری نیازمند استراتژی جامعی برای مقابله با این مسئله در جهت تضمین امنیت و دستیابی به منافع حیاتی خود از جمله انرژی هسته‌ای است و لزوم برنامه‌ریزی و مقابله با این مسئله به‌عنوان یکی از مهم‌ترین تهدیدها و آسیب‌ها با توجه به اقدامات تخریبی علیه آن نظیر «استاکسنت» وغیره، ناگزیر می‌نماید (موسوی و همکاران، بی‌تا: 14-12).

براساس آمار مرکز مدیریت توسعه ملی اینترنت، حضور بیش از 60 درصد مردم ایران در فضای سایبر که 40 درصد آنان در گروه سنی 29-20 سال قرار دارند (http://www.bartarinha.ir)، زمینه را برای سوءاستفادهٔ گروه‌های تروریستی به منظور ترویج افکار و اهداف خود و جذب نیرو تا میزان قابل‌توجهی فراهم می‌آورد. در این میان، راهبرد مدیریت مرزهای فضای سایبر یعنی ایجاد شناخت، تقویت مرزها، ایجاد فرهنگ برای مسئولان اجرایی و مردم، مسائل و مشکلات ناشی از اقدامات تروریستی به‌ویژه تروریسم سایبری را برای کشور به حداقل می‌رساند.

به منظور مقابله با تروریسم سایبری، شاید اصلی‌ترین راهکار برای داشتن اینترنتی ایمن، اجرای طرح جامع امنیت ملی در حوزه سایبری باشد؛ طرحی که شبکه ملی اطلاعات نیز می‌تواند از اجزای آن باشد. در این طرح باید حوزه‌های آموزش عمومی، تقویت سیستم‌های دفاعی و توان مقابله و اجرای عملیات علیه مهاجم در هر سطح، مورد توجه قرار گیرد. همچنین نیاز است ملاحظه‌های مربوط به پدافند غیرعامل در تمامی طرح‌های مربوط به شبکه‌های ارتباطی و الزام دستگاه‌های اجرایی به استفاده از توان داخلی (تا حد امکان) مدنظر باشد. به نظر می‌رسد در این زمینه از نوعی ضعف دیپلماتیک رنج می‌بریم. یافتن راه‌های پیگیری حقوقی بین‌المللیِ حملات سایبری به ایران و همچنین تلاش برای سهیم‌شدن در مدیریت اینترنت جهانی از طریق حضور در مجامع مؤثر و مرتبط، اقداماتی است که نیازمند یک وزارت امور خارجه توانمند و متعهد است.

5. نتیجه‌گیری

با شکل‌گیری فضای سایبر و ورود به عصر اطلاعات و وابستگی‌هایی که در سطوح مختلف فردی تا کشوری به استفاده و ورود به فضای سایبر شکل گرفته است، بسیاری از نظریه‌پردازان مدعی ازبین‌رفتن مرز و مرزبندی و همچنین ناتوانی کنترل و مدیریت مرزی بین کشورها شده‌اند. این اشخاص مرزها را ازبین‌رفته و کنترل‌ناشدنی دانسته و در مفهوم‌سازی‌های نوین از جمله جهان بدون مرز، دهکده جهانی وغیره کوشیده‌اند. نقطهٔ اتکای این اشخاص، شکل‌گیری فضای سایبر و آزادی‌های بی‌مرز در این فضا برای افراد و ازبین‌رفتن کنترل و مدیریت حکومت‌ها و توانایی اثرگذاری و گذر از محدودیت‌های فضای واقعی بوده است، اما باید توجه داشت ظرفیت‌ها و پتانسیل‌های بالای فضای سایبر که به‌آسانی در اختیار افراد، گروه‌ها، قومیت‌ها، حکومت‌ها وغیره قرار گرفته است، به آن‌ها توانایی نقش‌آفرینی و قدرت‌نمایی در فضای سایبر را به منظور رسیدن به اهداف خود به صورت‌های مختلف داده است.

حکومت‌ها برای اینکه بتوانند در برابر این چالش‌های تازه که با شکل‌گیری فضای سایبر ایجاد شده‌اند، اقدامی کرده و تا حدودی آن‌ها را کاهش دهند، به صورت‌های مختلف سعی در کنترل و مدیریت این فضا داشته‌اند. از جمله این واکنش‌های دفاع سایبری تشکیل پلیس سایبر، ارتش سایبری، حقوق سایبر وغیره است، اما در این میان آنچه از اهمیت بالایی برخوردار است و می‌توان آن را گام نخست مدیریت فضای سایبر نامید که متأسفانه کمتر به آن پرداخته شده است، مدیریت مرزهای موجود در فضای سایبری است. باید توجه داشت فضای سایبر همان‌گونه که آن‌ها تصور می‌کنند، فضایی صاف و بدون مانع نیست، بلکه دارای مرزبندی‌ها، حقوق و قواعد و قوانین مختلفی است که با درجه‌های گوناگون از سوی حکومت‌ها در آن اِعمال می‌شود و حتی آزادترین کشورهایی که مهد آزادی تصور می‌شوند همچون ایالات متحده نیز این مرزبندی‌ها و موانع را در فضای سایبر اِعمال می‌کنند.

یکی از تهدیدهای نوین، سایبرتروریسم است که با توجه به تنوع و گستردگی گروه‌های تروریستی در محیط امنیتی جمهوری اسلامی ایران و برنامه‌ریزی نظام سلطه برای بهره‌گیری از ظرفیت‌های آنان به منظور بی‌ثبات‌سازی و ایجاد اخلال در نظم و امنیت عمومی، یکی از مهم‌ترین چالش‌های فراروی نظام است. در سال‌های اخیر تروریسم سایبری به یکی از چالش‌های اصلی

دولت‌ها به‌ویژه کشورمان تبدیل شده است. جمهوری اسلامی ایران که با دارابودن بیش از هفده هزار شهید ترور، یکی از قربانیان اصلی حمله‌ها و اقدامات تروریستی در سطح جهان است، از این قاعده مستثنی نیست و برای اینکه بتواند اقدامات تروریستی را در فضای کشور کنترل کند، نیازمند راهبردهای ویژه‌ای در این زمینه است.

راهبرد پیشنهادی تحقیق حاضر با عنوان مدیریت مرزها، گام نخستینِ کنترل تروریسم به صورت نظری است که در فضای جمهوری اسلامی ایران در مرزهای فضای سایبر مورد بررسی قرار گرفته است. ازآنجاکه شکل‌گیری فضای سایبر مخاطره‌های زیادی برای حکومت‌ها، گروه‌ها و حتی افراد به وجود آورده است و با توجه به قابلیت‌ها و ظرفیت‌های این فضا که روزبه‌روز بر گستردگی و بهره‌وری بیشتر آن افزوده می‌شود و به عرصهٔ نوین قدرت‌نمایی و نبرد بین حکومت‌ها، گروه‌ها و حتی افراد تبدیل شده است، اداره و کنترل فضای سایبر در قالب مدیریت سایبر در کشور شایستهٔ توجه بیشتری است. ظرفیت‌ها و پتانسیل‌های بالای این فضا امکان بهره‌برداری از سوی گروه‌های تروریستی برای دستیابی به اهداف خود مانندِ ضربه‌زدن به تأسیسات زیربنایی و حساس کشور، دسترسی و دستبرد به اطلاعات محرمانه در کشور، کسب اطلاعات، ایجاد رعب و وحشت، جذب نیرو وغیره در فضای کشور را به‌سادگی فراهم می‌آورد. بر این اساس، حکومت جمهوری اسلامی ایران با توجه به دارابودن کاربران گستردهٔ حاضر در فضای سایبر ازیک‌سو و دارابودن بدخواهان و دشمنان قسم‌خوردهٔ نظام در فراسوی مرزهای کشور ازسوی‌دیگر، برای اینکه بتواند مسائل ناشی از بهره‌وری گروه‌های تروریستی در داخل کشور را کنترل کرده و کاهش دهد، نیازمند راهبرد مدیریت مرزهای موجود در فضای سایبری یعنی شناساندن مرزهای این فضا به افراد و مسئولان، پُررنگ‌کردن مرزهای موجود، تقویت زیرساخت‌های بومی فضای سایبر، ایجاد شبکه‌های داخلی و از همه مهم‌تر ایجاد فرهنگ لازم برای حضور در فضای سایبر است.

فهرست منابع

1. آلبوعلی، امیر (1392)، *صلاحیت محاکم در جرایم سایبری*، چاپ اول، تهران: جنگل.
2. ابراهیمی، شهروز؛ جالینوسی، احمد؛ قنواتی، تیمور (1393)، «رویکرد دفاعی ـ تهاجمی جمهوری خلق چین در چهارچوب فضای سایبر»، *دوفصلنامه مطالعات قدرت نرم*، سال چهارم، شماره دهم، بهار و تابستان 1393.
3. بدیعی ازندهانی، مرجان؛ احمدی فیروزجائی، میثم؛ انصاری‌زاده، سلمان (1392)، «تبیین مفهوم مرز در فضای سیاسی ـ مجازی ایران»، *فصلنامه جغرافیا*، دوره جدید، سال یازدهم، شماره 36، بهار، صص 312-291.
4. بیرو، آلن (1966)، *فرهنگ علوم اجتماعی*، ترجمهٔ دکتر باقر ساروخانی (1366)، تهران: کیهان.
5. طیب، علیرضا (1384)، *تروریسم در فراز و فرود تاریخ*، تهران: نی.
6. فضلی، حسن؛ دهشیری، محمدرضا (1395)، «بررسی و تحلیل تروریسم سایبری با رویکرد پیشگیری وضعی»، *فصلنامه علمی تخصصی دانش انتظامی لرستان*، سال چهارم، شماره دوم.
7. درآنجلیز، جینا (1383)، *جرایم سایبر*، ترجمهٔ سعید حافظی و عبدالصمد خرم‌آبادی، دبیرخانه شورای عالی اطلاع‌رسانی.
8. خلیلی‌پور رکن‌آبادی، علی؛ نورعلی‌وند، یاسر (1391)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، *فصلنامه مطالعات راهبردی*، سال 15، شماره 2، تابستان 1391، مسلسل 59.
9. جان‌پرور، محسن؛ حیدری، طهمورث (1390)، «آسیب‌شناسی فضای سایبر بر امنیت اجتماعی»، *فصلنامه نظم و امنیت انتظامی*، شماره سوم، سال چهارم، پاییز 1390.
10. جان‌پرور، محسن؛ افشرد، محمدحسین؛ احمدی‌پور، زهرا؛ قصری، محمد (1392)، «تبیین مرزهای فضای رایانه‌ای و راهبرد مدیریتی آن‌ها»، *پژوهشنامه نظم و امنیت انتظامی*، شماره اول، سال پنجم، صص 120-99.
11. جیستان، ذبیح‌الله (1390)، *دفاع در برابر ابزار پنهان جنگ سایبری*. مجموعه مقالات نخستین همایش ملی دفاع سایبری، صص 256-247.
12. حافظ‌نیا، محمدرضا؛ جان‌پرور، محسن (1392)، *مرزها و جهانی‌شدن (با نگاهی کوتاه به مرزهای ایران)*، تهران: انتشارات پژوهشکده مطالعات راهبردی.
13. حافظ‌نیا، محمدرضا، کاویانی‌راد، مراد (1383)، *افق‌های جدید در جغرافیای سیاسی*، تهران: سمت.
14. حافظ‌نیا، محمدرضا (1385)، *اصول و مفاهیم ژئوپلیتیک*، مشهد: پاپلی.

کنترل تروریسم سایبری با مدیریت فضای سایبر راهبردی

15. رهنورد، حمید (1385)، «تروریسم، رسانه و افکار عمومی در امریکا»، *فصلنامه مطالعات راهبردی*، سال نهم، شماره چهارم، شماره مسلسل 34.
16. قاسمی، غلامعلی؛ باقرزاده، سجاد (1394)، «جایگاه حقوق بشر در مبارزه با سایبر تروریسم»، *مجله حقوقی بین‌المللی*، شماره 52.
17. عالی‌پور، حسن (1390)، «امنیت سایبر در سند چشم‌انداز 1404 چالش‌ها و راهکارهای حقوقی رویارویی با بزه‌های امنیتی سایبری»، *مجموعه مقالات نخستین همایش ملی دفاع سایبری*، صص 43-15.
18. غروری، ناصرحسین؛ محمدی، علی (1390)، «معرفی رویکردها و متدولوژی‌های طراحی و اجرای سناریوهای مقابله با تهدیدهای سایبری، *مجموعه مقالات نخستین همایش ملی دفاع سایبری*، صص 86-75.
19. صدرزاده، حبیب (1390)، «بعد هفت: فضای سایبر»، *مجموعه مقالات نخستین همایش ملی دفاع سایبری*، صص 374-365.
20. محمدی، مصطفی (1389)، *تأثیر فناوری اطلاعات بر جنگ*، پایان‌نامه کارشناسی‌ارشد روابط بین‌الملل، اصفهان، دانشکده حقوق و علوم سیاسی دانشگاه اصفهان.
21. موسوی، محمدرضا؛ حیدری، خدیجه؛ قنبری، علی (1390)، «تأثیر تهدیدهای امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن»، *مجموعه مقالات نخستین همایش دفاع سایبری*.
22. مجتهدزاده، پیروز، (1385)، *جزوه منتشرنشدهٔ درس نظریه‌ها و مفاهیم ژئوپلیتیک*، دانشگاه تربیت مدرس.
23. نمامیان، پیمان؛ سهراب‌بیگ، محمد (1391) «مبارزه با تروریسم؛ راهبردی مؤثر در تحقق صلح عادلانه جهانی»، *مطالعات راهبردی جهانی‌شدن*، دوره 3، شماره 6، بهار 1391، صص 114-77.
24. نورمحمدی، مرتضی (1390)، «جنگ نرم، فضای سایبر و امنیت جمهوری اسلامی ایران»، *فصلنامه راهبرد فرهنگ*، شماره شانزدهم، صص 145-128.
25. واسیلاکی، ایرینی (1381)، «جرم مالتی‌مدیا (چندرسانه‌ای): پیدایش پدیده‌شناسی و مسائل قانونی جرم فوق‌کامپیوتری»، ترجمهٔ محمدحسین دزیانی، *ماهنامه وکالت*، شماره 11.
26. Charney, Scott (2009), ***Rethinking the Cyber Threat A Framework and Path Forward***, Microsoft Corp, One Microsoft Way, Redmond, WA 98052-6399, USA.
27. Everard, J. (2000), ***Virtual states: the Internat and the boundaries of the nation-state***, New York: Routledge, p. 62.
28. Foggetti, Nadia (2009), "Cyber-terrorism and the Right to Privacy in the Third Pillar Perspective", ***Masaryk University Journal of Law and Technology***, Vol. 3.
29. GibsonWilliam (1984), ***Neuromancer***, US: Ace Books.
30. Gordon, Adv. b, ***the legal challenge of regulating the internet***, available at: www.geocities.com/athens/academy/5090/chapter 3, 4.
31. Gross, Michael L, Canetti, Daphna, Dana R. Vashdi (2016), "The psychological effects of cyber terrorism", ***Journal Bulletin of the Atomic Scientists***, Vol. 72, 2016-Issue 5.

32. Haller, John & Merrell, Samuel A. & Butkovic, Matthew J. & Willke, Bradford J. (2010), *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability*, Software Engineering Institute.
33. Heinesson (2009), *Accreditation and Border Management*, available at: www.kghborderservices.com
34. Janparvar, Mohsen (2014), "Border Management; as Strategy of States to Maintain Order and Security in the Country", *Geopolitics Quarterly*, Vol. 9, No. 4.
35. Jarvis, Lee, Macdonald, Stuart, Whiting, Andrew (2017), "Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat", *Access*, Vol. 2, Issue 1, February 2017, pp. 64-87.
36. Johnson, David & Post David G. (2003), *Law and border: role of law in cyberspace*, 48stan. 2r, b67, available at: www.cli.org/x0025-LBFIN.
37. Lord, Kristin M. & Sharp, Travis (2011), "America's Cyber future Security and Prosperity in the Information Age", *Center for a New American Security*, Vol. I.
38. Mutula, Stephen M. (2007), *Web Information Management*, UK: Cahndos Publication.
39. Peter W. (1998), *Wilson and others, Strategic Information Warfare Rising*, New York: Rand Corporation.
40. Pratt, Martin (2001), *Boundary-Making, Challenges & Opportunities*, IBRU. Durham University. UK.
41. Starr, Stuart H. (2009), "Towards an Evolving Theory of Cyber power", *National Defense University*, Center for Technology and National Security Policy.
42. The Provisions of Executive Order 12333 of Dec 4, 1981, United States Intelligence avtivities, http://www.archives.gov
43. Theohary, Catherine A.; Rollins, John W. (2015), "Cyberwarfare and Cyberterrorism", In: *Brief, Congressional Research Service*.
44. Vilken, P. (2001), The political economy of global communication and human security, Institute for strategic studies (In Persian).
45. http://shafaqna.com/persian/
46. http://revolution.pchi. ir/show. php?page=contents & id=13697
47. http://www.gerdab.ir/fa/news/427
48. http://www.bashgah.net/fa/content/show/15395
49. http://www.bartarinha.ir
50. http://forum. omegapars.com
51. http://novinbank. blogfa.com/post-40.aspx