استراتژی امنیت ملی تعاملی سازنده بر توسعه دانش سایبرنتیک در عصر جنگ سایبری

امین حسنوند[1]

[1]وکیل دادگستری و عضو کمیسیون پژوهش مرکز وکلای قوه قضائیه
amin_hasanvand@yahoo.com

چکیده

در قرن حاضر، عنصر «امنیت ملی» از ارزشمندترین و بالاترین ثروت‌هایی است که دولت‌ها همواره به دنبال آن می‌باشند و با تمام توان سعی در اثبات و ابقاء آن دارند. از شاخصه‌های مهم ثبات و پایداری هر حکومت امنیت ملی است و سخن گفتن از امنیت ملی مستلزم برخورداری از توسعه انسانی و توجه به جوانب مختلف سیاسی، فرهنگی و اجتماعی آن است. در عصر حاضر که به عصر اطلاعات و ارتباطات مشهور است یکی از ابزارهای پرقدرت و چالش‌برانگیز در امنیت هر کشور فضای مجازی است که می‌تواند به سهولت تهدیدات و زمینه‌های ناامنی ملل را فراهم آورد. بنابراین با توجه به جهانی‌شدن ارتباطات و اطلاعات و افزایش نقش فضای مجازی در زندگی مردم جهان، فضای سایبر یکی از منابع مهم کسب، حفظ و افزایش قدرت ملی به شمار می‌آید. از طرف دیگر، در راستای حفظ و ارتقای امنیت ملی جوامع، ضروری است تا عملکرد و تأثیرات فضای سایبر در زمینه‌های ایجاد یا سلب امنیت را مورد بررسی و تحلیل قرار داد تا تأثیرات مثبت و منفی بر جنبه‌های مختلف امنیت ملی را شناسایی نمود. پژوهش حاضر که به صورت توصیفی تحلیلی و در عین حال کتابخانه‌ای انجام شده است بر آن است که ضمن بسط مفهوم امنیت ملی، به بررسی مفهوم دانش سایبرنتیک و کاربرد آن در تعمیم دانش سازمانی و رابطه متقابل و معنادار سیبرنتیک و فرآیند مدیریت دانش می‌پردازد.

کلمات کلیدی: سایبرنتیک، امنیت ملی، فضای مجازی، مدیریت دانش.

۱ مقدمه

ابتدا به ساکن و قبل از ورود به بطن و بدنه موضوع پژوهش، تلاش نگارنده بر این است که عنصر امنیت ملی را به عنوان بازوان قدرت و سپر میدان نبرد معرفی و سپس استراتژی‌های موثر بر توسعه دانش سایبرنتیک را تجویز و تزریق نماید. امروزه امنیت ملی یکی از ارزشمندترین و بالاترین ثروت‌هایی است که دولت‌ها همواره به دنبال آن می‌باشند و با تمام توان سعی در ایجاد و حفظ آن دارند (حکیم، ۱۳۹۸: ۷). محرز است امنیت ملی به عنوان متغیر وابسته از موضوعات بسیار بزرگ روابط بین‌المللی محسوب می‌شود به طوری که بدون امنیت ملی زندگی با فروپاشی حکومت‌ها از بین خواهد رفت. گرچه این موضوع پیچیدگی‌های خاص خودش

را دارد و نظام‌های سیاسی مختلف بر اساس دیدگاه خود ابعاد متفاوت اقتصادی، نظامی، اجتماعی و فرهنگی یا سیاسی را تهدید یا تعیین کننده امنیت ملی و ضرورت زمان و تحولات در عرصه سیاست بین الملل نقش اساسی در تحول این نگرش‌ها داشته است طوری که اگر در مقطعی، ترس از حمله نظامی و قدرت تهاجمی دولت‌ها باعث تهدید ملی دولت‌ها می‌شد امروزه این مسئله تعدیل شده و ابعاد دیگر امنیت ملی اهمیت بیشتری یافته‌اند و در واقع از جنبه سخت افزاری به سمت عوامل نرم افزاری جهت پیدا کرده است (حاجی زاده، ۱۳۹۸: ۷). در حال حاضر با توسعه فضای سایبری، برقراری امنیت در این فضا به یکی از دغدغه‌های اساسی کشور ما تبدیل شده است. نو ظهور بودن این فضا به همراه سرعت بسیار بالای پیشرفت و توسعه فناوری‌های مرتبط با این فضا، کار کشورها و دولت‌ها را برای برقراری امنیت به چالش کشیده است. علاوه بر موارد ذکر شده، چالش‌هایی نظیر محدود نبودن فضای سایبری به مرزهای فیزیکی کشورها باعث شده تا برای برقراری کامل امنیت در این فضا نیاز به یک همکاری بین المللی قوی نیز وجود داشته باشد. فقدان قوانین و مقررات کامل در کشور در زمینه مدیریت امنیت سایبری، باعث ناشناس ماندن این فضا شده و کار را برای برقراری امنیت سایبری در کشور بیش از پیش چالش برانگیز کرده است (حاجی ملامیرزایی، ۱۳۹۸: ۱۳). طبق یک نقل قول معروف از کارشناسان امنیتی، نشت داده بالاخره اتفاق می‌افتد و هکرها راهی را خواهند یافت تا به سیستم‌های یک شرکت نفوذ کنند اما نکته با اهمیت، میزان خسارتی است که پس از این اتفاق به بار می‌آید. به عبارت دیگر، حمله سایبری و نشت داده، در دنیای کنونی گریز ناپذیر است و فقط با آمادگی قبلی و اتخاذ رویکردهای صحیح امنیتی می‌توان از میزان خسارت آن کاست (بلو و همکاران، ۱۳۹۹: ۶).

پس از ذکر مقدمه، نقشه راه این پژوهش در تفسیر مبسوط مفهوم امنیت ملی و مبانی نظری دکترین و تئوریسین‌های عرصه استراتژیک تبلور می‌یابد.

۲ طرح مطلب و بیان مسئله

به عنوان قاعده باید قائل به این نظر بود که در حال حاضر اگر جنگی صورت گیرد هیچ مشابهتی با جنگ‌های گذشته نخواهد داشت. در جنگ گذشته، جبهه ما مشخص بود لذا انتخاب تاکتیک‌ها و ابزارهای مبارزه کار سختی نبود. اما در جنگ‌های آینده این جبهه‌ها نامشخص و منشأ حملات نامعلوم است. امروزه با توجه به گسترش فناوری‌های نوین تهدیدات، مخابرات و نقاط رخنه پذیر متعددی به وجود آمده است که اغلب مورد غفلت قرار می‌گیرند به طوری که به منظور حفاظت از امنیت ملی و مقابله با دشمنان سایبری، نیازمند تقویت نیروهای خودی در این گستره و ارتقا توانمندی‌ها در جهت صیانت از فضای سایبر کشور می‌باشیم وانگهی حفاظت از سایبر کشور به عنوان یکی از شریان‌های اصلی اطلاعات در روزگاری که عصر اطلاعات لقب گرفته است به اندازه حفاظت از مرزهای روی نقشه برای هر کشوری حائز اهمیت است. باری، تضمین امنیت و آسایش همواره از بزرگ‌ترین دغدغه‌های حکومت‌ها می‌باشد؛ ضرورت پرداخت به این موضوع در هزاره‌ای که دشمن با استفاده از تمام امکانات ممکن، مترصد تجاوز و رخنه به منظور پیشبرد اهداف سوء خود می‌باشد، امری کاملاً محسوس و ملزوم است (سمیعی، ۱۳۹۷: ۱۰). مشهور است که مهم‌ترین وظیفه دولت‌ها در همه نظام‌های حکومتی، تامین دفاع و امنیت کشور است و لازمه تحقق این رسالت، سیاست دفاعی است تا منبع

قدرت ملی به نحو موثر و هماهنگ در این جهت استفاده شود. بدون شک سیاست دفاعی از اسناد راهبردی مهمی به شمار می‌رود که هدایتگر و راهنمای زمامداران حکومت و مدیران دفاعی و امنیتی در سکانداری ثبات و امنیت کشور است به خصوص در محیط پرچالش و متلاطمی چون غرب آسیا که در کانون اهداف راهبردی قدرت‌های جهانی قرار دارد و عنوان هارتلند فعلیِ جهان را به خود اختصاص داده است (ریاضی و همکاران، ۱۳۹۸: ۱۳). پس از طرح مطلب و بیان مسئله به منظور پیشبرد ماموریت جاری و با مشایعت عنوان پژوهش، لازم است که صبغه تاریخی و پیشینه استراتژی نظام حقوقی ایران در قبال تهدیدات سایبری بررسی و تحقیق را به طور گذرا در قالب یک بند تلخیص می‌نماییم.

۳ پیشینه و مبانی نظری تحقیق

فضای مجازی یا فضای سایر اصطلاحی است که نخستین بار توسط ویلیام گیبسون در داستان علمی تخیلی «نیورومانسر» به سال ۱۹۸۴ به کار برده شد و در سال ۱۹۹۰ واژه دنیای مجازی یا فضای مجازی کاربرد بیشتری پیدا کرده است و به کلیه فضاهای سه‌بُعدی اطلاق می‌شود. در این دوره استفاده از اینترنت، شبکه و مخابرات دیجیتال سریعاً در حال رشد بود و لفظ "فضای مجازی" می‌توانست بسیاری از ایده‌ها و پدیده‌های نوظهور را نمایندگی کند. لفظ ما در فضای مجازی، سایبرنتیک است که از واژه یونانی Kubernetes گرفته شده که «راننده» و «سکاندار» معنی می‌دهد و منشأ واژه «حکمران» است. این واژه توسط نوبرت وینر کمی پس از پایان جنگ جهانی دوم اختراع شد. او بعداً کشف کرد که واژه Cybernetique در حدود یک قرن پیش توسط امپر به معنای دانش اداره حکومت استعمال شده است (مرادی، ۱۳۹۹: ۱۷). با برش مختصری که از پیشینه تاریخی استراتژی امنیت ملی در فضای سایبر مطرح شد، اکنون به مطالعه موردی و کنکاش تحقیقات انجام شده در این حوزه می‌پردازیم و ماحصل سبق تحقیقات انجام شده در این حوزه را به صورت مختصر و گذرا مستند و رفرنس خواهیم کرد. یکی از مطالبات مبسوطی که در این حوزه به رشته تقریر درآمده است کتاب «پیشگیری از جرایم سایبری علیه امنیت ملی در ایران» نوشته محمد شکری است که ضمن ساختار شناسی فضای سایبر، به علت شناسی جرایم سایبر پرداخته و نهایتاً به بررسی روش‌های پیشگیرانه علیه جرایم اینترنتی در جمهوری اسلامی ایران می‌پردازد. در بخشی از کتاب پیشگیری از جرایم سایبری می‌خوانیم: فضای سایبر و اینترنت جدا از مرزهای جغرافیایی عمل می‌کنند و به اصولِ خطوطی که دولتمردان در طراحی نقشه‌های سیاسی رسم می‌کنن محدود نمی‌شود. این فضای بی پاسبان و رها که هر لحظه بر گستره آن افزوده می‌شود فرصت بسیار مناسبی را برای ارتکاب و اختفای جرایم سایبری به مرتکب اعطا می‌کند و در این فضا هیچ گونه چارچوب اخلاقی، ارزشی یا هنجار مشخصی برای مبارزه و درگیری وجود ندارد (شکری، ۱۳۹۹: ۴۸). در همین راستا مقاله‌ای با عنوان «امنیت ملی در فضای سایبر، فرصت‌ها و تهدیدها با تاکید بر استقرار دولت الکترونیکی» که توسط محمدرضا موحدی تقریر و تحریر شده است که ضمن معرفی ویژگی‌های فضای سایبر، وضعیت کشور را بر اساس آمارهای موجود مورد ارزیابی قرار داده و پس از بررسی مسئله امنیت فضای سایبر، به اولویت بندی در استقرار آن پرداخت و به این اعتقاد است که نشت اطلاعات، سرقت داده‌های حیاتی کشور و آسیب پذیری شبکه‌های جامع اطلاع رسانی به عنوان مهم‌ترین اشکالات امنیتی در این فضا می‌باشد

که اگر از طرف حکومت توجه ویژه‌ای به آن نشود به عنوان یک تهدید جدی برای منافع پایه‌ای کشور تلقی می‌شود (موحدی صفت، ۱۳۸۶: ۷). بدیهی است که با مطالعه کتب، مقالات و ابزار آلات علمی و عملی که آماس تجارب ادوار مختلف است می‌توان به نقطه نظری جامع به منظور توسعه دانش سایبرنتیک پرداخت.

۴ متدولوژی و روانشناسی تحقیق

تحقیق فرآیند رسیدن به سوال پژوهش است (سیابیدی، ۱۳۹۶: ۵). هدف از یک پژوهش، تکمیل پاسخ در ازای پرسش مطرح است، علی القاعده با طرح موضوع تحقیق، فرآیند پژوهش رسماً آغاز و انتخاب موضوع مهم‌ترین مرحله تدوین فرآیند پژوهش است. روش پژوهش حاضر کتابخانه‌ای (اسنادی) است که با بهره‌گیری از کتب، مجلات، اینترنت و اینترانت به بررسی، گفتگو و چاره اندیشی کنش فضای مجازی بر جهان متغیر کنونی می‌پردازد که اصل این کنکاش تزریق یک پژوهش مبسوط به عرصه فضای سایبر است.

۵ مفهوم شناسی و مبانی نظری

الف. استراتژی

مشهور است در دوران سخت، بهترین حمله دفاع خوب است (کالکینز، ۱۳۹۳: ۷). استراتژی واژه‌ی پیچیده‌ای است که بی نظمی گسترده‌ای ایجاد می‌کند. کتاب‌ها و آثار بیشماری وجود دارد که تلاش کرده‌اند تا با به کار گیری استراتژی در مسائل خاص، اسرار و پیچیدگی آن را آشکار سازند اما در بسیاری از موارد تنها مسئله را پیچیده‌تر کرده‌اند. در مقابل اگر به مفاهیم بنیادین استراتژی فکر کنیم مفهوم این واژه واضح‌تر خواهد شد. مسئله حیاتی که یک استراتژی را تعریف می‌کند این است که استراتژی مستلزم تعامل هوشمند و سازگارانه با دیگران یعنی دوستان، افراد و گروه‌های بی طرف و دشمنان است؛ اما باید توجه داشت که این تعامل اجتماعی نوع خاصی را دراد. هر یک از طرفین درگیر، به طور مستمر جایگاه، نیت و اقدامات خود را بر مبنای ادراکات و اقدامات سایر بازیگران اصلاح می‌کنند. در این خصوص دنیای راز آلود و پنهان نظریه بازی‌ها و حرف‌های مفیدی برای گفتن دارد. این تعاملات «اساساً موقعیت‌های چانه‌زنی هستند که در آن توانایی دستیابی یکی از طرفین، به اهداف، انتخاب‌ها یا تصمیمات سایر طرف‌ها بستگی دارد». (لیتون، ۱۳۹۸: ۲۵). در تعریف استراتژی پلان‌های متفاوتی از سوی اندیشمندان نظام استراتژی ارائه شده است که در این بخش از پژوهش ضمن ارائه دو تعریف جامع از استراتژی، نُه دیدگاه متفاوت از اندیشمندان شهیر این عرصه را مستند می‌کنیم. در تعریف نخست می‌خوانیم: «استراتژی فرضیه‌ای در مورد روابط علی و معلولی بین زنجیره‌ای از متغیرهاست که یک موقعیت بالقوه راهبردی را بالفعل می‌کند». در تعریف دوم آمده است: «استراتژی فرآیندی است جهت تعیین اهداف بلندمدت و راه رسیدن به آن هدف و منابعی که برای این کار تخصیص داده می‌شود». همانطور که اشاره شد عنصر استراتژی مفهومی بس گسترده و باز است که برای به تصویر کشیدن این مفهوم بسیط می‌توان نقشه راهی را ترسیم و به مخاطبان تحویل داد. در همین راستا به منظور شناسایی بیشتر این مفهوم به مبانی نظری اندیشمندان عرصه استراتژیک به طور مختصر گریزی می‌زنیم:

از دیدگاه:

- کاپلان:

استراتژی بدین معناست که سازمان چگونه می‌خواهد برای سهامداران، مشتریان و شهروندان ارزش آفرینی نماید. برای پیاده سازی استراتژی بایستی به بسیج دارایی‌های نامشهود پرداخت.

- فرد آر. دیوید:

هنر و علم تدوین، اجرا و تصمیمات وظیفه‌ای چندگانه که سازمان را قادر می‌سازد به اهداف بلندمدت خود دست یابد.

- جک واش:

استراتژی یعنی این که ما تصمیم‌های شفاف و دقیق در مورد نحوه رقابت با دیگران بگیریم.

- مایکل پورتر:

استراتژی یعنی اینکه کاری که دیگران انجام می‌دهند را با منابع کمتر انجام دهیم و کارهایی انجام دهیم که هیچ کس غیر از ما انجام نمی‌دهند.

- شرون اوستر:

استراتژی داشتن یعنی وقتی مجموعه تصمیمات ما دیده می‌شود بتوان الگوی خاصی را در آن مشاهده کرد.

- آلفرد دی چندلر:

استراتژی یعنی تعیین هدف‌های درازمدت در سازمان و آماده کردن برنامه‌های فعالیتی مناسب و تخصیص دادن منابع مورد نیاز برای تحقق این اهداف.

- هافر و شندل:

استراتژی یعنی فعالیت‌هایی که تامین کننده هماهنگی بین منابع داخلی و قابلیت‌های سازمان با فرصت و تهدیدهای محیط بیرونی است.

- هنری مینتزبرگ:

مفاهیمی چون استراتژی را نمی‌توان در قالب یک تعریف استراتژی آورد و برای آن باید تعاریف مختلفی را ارائه داد.

- گری پیسانو:

گری بیان می‌کند که استراتژی هیچ چیز به جز تعهد به یک الگوی رفتاری مشخص به منظور پیروی در یک رقابت نبوده و یک فرض اساسی منتج می‌شود که عبارتست از این که چه چیزی موجب پیروزی می‌شود (حاجی میر، ۱۳۹۶: ۷).

ب. امنیت ملی

«والتر لیپمن» محقق و نویسنده آمریکایی اولین کسی است که مفهوم امنیت ملی را به روشنی تعریف نموده است. وی می‌گوید: یک ملت وقتی دارای امنیت است که در صورت اجتناب از جنگ بتواند ارزش‌های اساسی خود را حفظ کرده و در صورت اقدام به جنگ، بتواند آن را پیش ببرد. «رابرت مک نامار» نیز می‌گوید: اگر امنیت دال بر وضعیتی باشد آن وضع حداقل نظم و ثبات خواهد بود. «ریچارد کوپر» نیز معتقد است که توان جامعه در حفظ و بهره گیری از فرهنگ و امنیت ملی است. تعریف دیگری که در این زمینه موجود است در چارچوب منافع ملی است. اگر منافع ملی را مجموعه منافع و اهدافی که دولت‌ها در پی کسب آن هستند بدانیم، حفظ و حراست از دستاوردهای منافع ملی بر عهده امنیت ملی خواهد بود. از سوی دیگر «رابرت ماندل» امنیت ملی را چنین تعریف کرده است: «امنیت ملی شامل تعقیب روانی و مادی و جزء مسئولیت‌های حکومت‌های ملی است تا از تهدیدات مستقیم خارجی نسبت به بقای رژیم، نظام شهروندان و شیوه زندگی شهروندان خود ممانعت به عمل آورند». با توجه به آنچه گفته شد می‌توان نتیجه گرفت که امنیت ملی به فرآیندی زیر اطلاق می‌گردد:

۱. حفظ تمامیت ارضی، حفظ جان و دین مردم، بقا و ادامه سیستم اجتماعی و حاکمیت کشور
۲. حفظ و ارتقا منافع حیاتی کشور
۳. فقدان تهدید جدی از خارج نسبت به منافع ملی و حیاتی کشور

اگر در تعاریف مزبور دقت شود می‌توان چنین برداشت شود که نقطه مشترک در تمام تعاریف فوق، بر ضرورت حفظ وجود خود متمرکز می‌باشد. به عبارت دیگر می‌توان امنیت را «حفظ ذات و صیانت نفس از اساسی‌ترین خطرات» خواند. باری، برخی از صاحبنظران حفظ خود یا «صیانت ذات و نفس» را در پنج مقوله زیر خلاصه نمودند:

۱. حفظ جان مردم
۲. حفظ دین، باورها و ارزش‌های مردم
۳. حفظ تمامیت ارضی
۴. حفظ نظام اقتصادی و سیاسی

۵. حفظ استقلال و حاکمیت کشور

پنج فاکتور فوق به عنوان جوهره امنیت ملی این پیام را دارد که تمامی کشورها، افراد و گروه‌ها و احزاب بدون توجه به گرایش‌ها، سلایق و اختلافات فردی و گروهی، طبقاتی، سیاسی و اجتماعی روی آن اتفاق نظر دارند (بیات، ۱۳۹۸: ۳۱).

ج. دانش سایبرنتیک

سایبرنتیک از جمله علومی است که در قرن بیستم پدید آمد و با رشد سریع خود توانست به علوم دیگر راه یابد. موضوع اصلی سایبرنتیک بررسی ماهیت کنترل در انسان، حیوان و ماشین است و لذا با زیست شناسی، روانشناسی، مکانیک، مهندسی، مدیریت و بسیاری علوم دیگر همبستگی دارد. سایبرنتیک توانسته به عنوان دانشی مستقل و در عین حال علمی بین رشته‌ای مطرح شود. در این علم به طبقه بندی و سازماندهی اطلاعات توجه زیادی می‌شود و از این رو در مدیریت اطلاعات و نیز در طراحی نظام‌های اطلاع رسانی از اهمیت ویژه‌ای برخوردار است (هوپ و همکاران، ۱۳۹۵: ۴). اگر بخواهیم علم و اصطلاح سایبرنتیک را که در حوزه علوم تجاری روزمره اندکی مجمل است را کالبد شکافی کنیم. باید گفت: سایبرنتیک علم میان رشته‌ای است که با سیستم‌های ارتباط و کنترل در موجودات زنده، ماشین‌ها و سازمان‌ها سر و کار دارد، یعنی سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی «کامپیوترها» است. از زمان هومر تا کنون لغت یونایی کوبرنانتیس معادل سکان‌دار بوده که معادل آن به انگلیسی سایبرنتس است که سایبر نیز بخشی از این کلمه است. اصطلاح سایبرنتیک نیز برگرفته از همین واژه یونانی است که نخستین بار توسط ریاضیدانی به نام نوربرت واینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. از نظر تئوری سایبرنتیک به مطالعه روانشناسی، هوش مصنوعی، علم اقتصاد، عصب شناسی، مهندسی سیستم‌ها و مطالعه سیستم‌های اجتماعی می‌پردازد. پیشوند «سایبر» که در مسائل مربوط به کامپیوتر به کار می‌رود بیشتر با انتقال پیام در اینترنت سر و کار دارد. به عنوان مثال لغت مرکب جنگ سایبر که در فرهنگ اصطلاحات جنگ‌های اطلاعاتی مترادف کلمه جنگ اطلاعاتی آمده است، به معنی جنگ از طریق شبکه‌های ارتباطی، علی الخصوص اینترنت می‌باشد. باری، انقلاب اطلاعات به گونه‌ای مفهوم نبرد را تغییر داد که پیش از این دیگر شاهد نبرد فرسایشی خونین نیروهای نظامی نخواهیم بود. در عوض، نیروهای کوچک و چالاکی که به اطلاعات بلادرنگ ماهواره‌ها و حسگرهای صحنه نبرد مسلح شده‌اند، با سرعت اعجاب آوری به محل‌های غیرمنتظره حمله می‌برند. مفروض است اطلاعات در حال تبدیل شدن به یک منبع استراتژیک می‌باشد و تواند خود را به عنوان یک عنصر با نفوذ و ارزشمند در عصر فراصنعتی، همانند نقش سرمایه و کار در عصر صنعتی، همانند نقش سرمایه و کار در عصر صنعتی مطرح کند (میرسمیعی، همان: ۳۱).

د. نبرد سایبری

بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری «عملیات سایبری» است که علیه منافع ملی سایبری کشورها انجام شده است و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی‌های این نوع از تهاجم‌های سایبری، برای آن است که دولت‌ها آن‌ها را جنگ علیه منافع ملی خود تلقی نمایند. جنگ سایبری با جنگ رایانه‌ای یا نبرد مجازی به نوعی جنگ اطلاق می‌گردد که طرفین در آن از رایانه و شبکه‌های رایانه‌ای به خصوص شبکه اینترنت به عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند. با توجه به این که جنگ‌های سایبری بعد از زمین، هوا، دریا و فضا، به بعد پنجم جنگ تبدیل شده است بنابراین جنگ سایبری، عبارتست از بهره‌برداری از ابزارها و شبکه‌های اطلاعاتی برای ضربه زدن به دیگران از طریق حمله مخفیانه به زیرساخت‌هاست. جنگ سایبری به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی مبتنی بر شبکه‌های رایانه‌ای دشمن در یک فضای سایبری است. چنین عملیاتی به طور مشخص و با اهداف نظامی، تجاری، سیاسی، مالی و ... انجام می‌گیرد.

نبرد سایبری در ساده‌ترین تعریف خود عبارتست از به کار گیری کامپیوترها برای حمله به زیرساخت‌های اطلاعاتی دشمن، در عین حفاظت از زیرساخت‌های اطلاعات خودی است. تهدیدات جنگ سایبری می‌تواند دامن‌گیر بخش‌های مختلف خصوصی و دولتی در هر کشور شود. سرقت اطلاعات راهبردی، اقتصادی، نظامی و ... یا تخریب و از کار اندازی سرویس‌ها و خدمات عمومی یا خصوصی می‌تواند نمونه‌ای از نتایج نبرد سایبری باشد. جنگ سایبری را می‌توان به صورت کلی تحت عنوان حمله عمدی به زیرساخت‌های اطلاعاتی دشمن از طریق استفاده از تکنیک‌های نفوذگری به کامپیوترها در عین جلوگیری کامل از انجام اقدامات مشابه از طرف دشمن تعریف نمود.

هـ. ژئوپلتیک امنیت سایبری

با رشد و توسعه فناوری و توسعه‌ی فضای سایبر که در رأی آن می‌توان به فراگیر شدن شبکه جهانی اینترنت اشاره کرد، فهم جغرافیای مربوط به این فضا و نیز رقابت‌های افراد، گروه‌ها، دولت‌ها و... در این فضا را می‌توان احساس نمود. در واقع علیرغم بی حد و حصر بودن فضای سایبر به لحاظ مکانی و تحلیل‌های فضایی می‌توان تلاشی را برای شناخت قلمرو سازی در این محیط پیشنهاد نمود و به تبع قلمروهایی که ساخته می‌شود می‌تواند، چه تأثیرات جغرافیایی گذاشته و یا بر تحولات ژئوپلتیک تاثیر بگذارد؟ پرداختن به این موضوع اولاً منجر به تعریف جغرافیایی و ظرفیت کارکرد ژئوپلتیکی از فضای سایبر خواهد شد و ثانیاً می‌تواند به تحلیل رقابت‌های مختلف سیاسی، اقتصادی، و اجتماعی که نمود آن در جغرافیای فیزیکی وجود دارد بیانجامد. (پاشایی و همکاران، ۱۳۹۹: ۷). در قرن حاضر، امنیت، بزرگ‌ترین چالشی می‌باشد که زیست بوم فناوری اطلاعات و ارتباطات با آن مواجه می‌شود و با گسترش فناوری‌های کوانتومی، بلاک چین و حمل و نقل هوشمند بر دامنه فراگیری آن افزوده خواهد شد به طوری که طی سالیان اخیر امنیت سایبری جزء پنج مخاطره مهم چسمانی شمرده می‌شود و به عنوان یک روند مهم بنا بر افزایش وابستگی سایبری نقش مهمی در معادلات بین المللی دارد (کمالی، ۱۳۹۸: ۷). چرا که امنیت سایبری یک عنصر اساسی برای تحقق اهداف

اجتماعی – اقتصادیِ اقتصادهای مدرن است (براهیماساتو، ۱۳۹۸: ۳).

از شاخصه‌های مهم پایداری و ثبات و حکومت، امنیت ملی است و سخن گفتن از امنیت ملی مستلزم برخورداری از توسعه انسان و توجه به جوانب مختلف سیاسی، فرهنگی، اقتصادی و اجتماعی آن است. دشمنان هر حکومت برای براندازی آن، از ابزارها و روش‌های مختلفی استفاده می‌کنند تا ثبات سیاسی، فرهنگی، اقتصادی و اجتماعی آن کشور را به چالش بکشند. از آنجا که امنیت کشورها در گرو کسب، حفظ و ازدیاد قدرت می‌باشد در عصر حاضر که به عصر اطلاعات و ارتباطات مشهور است یکی از ابزارهای پرقدرت چالش برانگیز در امنیت هر کشور فضای مجازی است که می‌تواند به سهولت تهدیدات و زمینه‌های ناامنی ملل را فراهم آورد. بنابراین با توجه به جهانی شدن ارتباطات و اطلاعات و افزایش نقش فضای سایبر در زندگی مردم جهان ژئوپلتیک امنیت و فضای مجازی ترسیم می‌نماییم. در بیان رابطه بین فضای مجازی و امنیت فرهنگی می‌توان اذعان کرد که فضای سایبر به عنوان مولود تعامل انسان با فناوری اطلاعاتی و ارتباطی، امکانات و الگوهای نوینی را برای تعاملات فکری و اندیشه‌ورزی فراروی جوامع عصر کنونی قرار داده است. اگرچه فضای سایبر بدون ارتباطات با واقعیات عینی و معمول در جوامع نیست اما به دلیل فضا، امکانات، زیرساخت‌ها، ابزارها، ویژگی‌های تعاملی و ذهنیت کاربران، گفتمان‌هایی که در آن شکل می‌گیرد ویژگی‌ها و ابعاد و سازکارهای مختص به خود دارد.

بنا به رویکرد «بلومر» بین گفتمان و تکنولوژی رابطه‌ای جداناپذیر وجود دارد. اکنون فناوری‌های اطلاعاتی و ارتباطی، با اثرگذاری بر ابعاد گوناگون ارتباطات، موجب پیدایش پدیده‌ای به نام «فرهنگ سایبر» شده است. در فضای سایبر، الگوهای نوین گفتمانی شکل گرفته است که دامنه و ماهیت آن ناشناخته مانده است. در این فضا به نوعی، موضوع ایجاد فضای کاملاً شخصی، به چالش کشیدن افکار و اندیشه، نضج گرفتن پاره فرهنگ‌های مجازی، تعامل بین فرهنگی، و قواعد گفتمانی مبتنی بر ارزش‌های فرهنگ سایبر مطرح است. کنشگران علمی، فرهنگی و اجتماعی نیز از اینترنت برای پیشبرد راهبردها و بسط الگوهای گفتمانی مورد نظر، از فضای سایبر سود می‌جویند. این مورد در چهارچوب وبلاگستان و شبکه‌های اجتماعی محیط سایبر انجام می‌شود. در حقیقت این باور خواهد بود که غیرقابل تطبیق بودن آنچه در فضای سایبر می‌گذرد با واقعیت بیرونی و وجود فاصله زیاد بین آن‌ها امری خطرناک می‌باشد و پیامدهای خطیری به دنبال دارد. روشن نبودن انواع ابعاد، الگوها، میدان پایداری، حوزه‌های گفتمانی، ماهیت‌های گفتمانی‌های فضای سایبر، از یک طرف و ساز و کارهایی که اینترنت در خدمت این گفتمان‌ها می‌گذارد، از نوع دیگر، موجب ناشناخته شدن قانون ماهیت گفتمان‌ها و فقدان دسترسی به نقشه روشنی از این فضا خواهد شد. به واقع، گفتمان‌های رایج در فضای سایبر و نیز ساز و کارها و ابزار اینترنتی آن، در ایجاد، توسعه و شکل دادن به دانش سهیم می‌باشند. باری، ابعاد تاثیر اینترنت بر شکل گیری و توسعه گفتمان در فضای مجازی در بسیاری از جوامع مانند ایران ناشناخته است و هویت و الگوهای این نوع گفتمان‌ها نیز ناشناخته مانده است. (حیدری و همکاران، ۱۳۹۸: ۱۱). یکی از مهم‌ترین نکات تحلیلی در زمینه ژئوپلتیک، واکنش ممکن نسبت به حمله سایبری یا روش مقابله با آن و همچنین شیوه درک این روش می‌باشد. به عنوان قاعده و اهرم بحث می‌توان گفت: ژئوپلتیک به روابط میان دولت‌ها و درگیری‌شان با جوامع جهانی و بزرگ‌تر اشاره می‌کند و تاکید ویژه‌ای را بر روی روابط میان جغرافیا و سیاست‌های دولتی دارد. عنصر ژئوپلتیک وظیفه خود را اختلال در گفتمان‌های ژئوپلتیکی

می‌داند؛ این حوزه نمی‌خواهد جغرافیای سیاسی را در مکان‌های مشخص مطالعه کند بلکه می‌خواهد پیش زمینه‌های سیاسی را از مناطق جغرافیایی مختلف ارائه نماید. از یک سو، دیپلماسی و سیاست خارجی به عنوان مسائل روشن فکرانه مطرح هستند که با پنهان کاری همراه خواهند بود. از سوی دیگر و به موازات وابستگی خاصی که به زبان مخصوص خودشان دارند گفتمان در زمینه‌ی امنیت و ژئوپلتیک، به شکل سنگینی به روایت‌های مشترک در زمینه‌ی مکان‌ها و هویت‌ها بستگی دارد (گیورا، ۱۳۹۸: ۵۱).

و. تروریسم سایبری

یکی از پدیده‌های مهم و بحث برانگیز بین المللی، منطقه‌ای و داخلی در دهه نخست سده بیست و یک و یکی از اساسی‌ترین معضل‌ها و چالش‌های جامعه جهانی در خصوص حقوق ملت‌ها و ثبات بین المللی مسئله تروریسم بوده است. در عصر ما، تروریسم از تهدید ملی به تهدیدی بین المللی و جهانی مبدل شده است و حتی این نگرانی وجود دارد که با گسترش آن صلح و امنیت بین المللی به مخاطره می‌افتد. در عصر جهانی شدن و پیشرفت فناوری، دیگر تروریسم در مرزهای ملی و منطقه‌ای محصور نمی‌ماند. تروریست‌ها همگام با روند جهانی شدن، پیشرفت کرده‌اند اما هرگز در قید و بندهای بین المللی ناشی از آن گرفتار نیامده‌اند. از این رو هیچ منطقه، دولت یا ملتی از اقدامات آن‌ها در امان نمی‌ماند. گروه‌های تروریستی با انگیزه‌های گوناگون دست به عملیات تروریستی می‌زنند و نگرانی از احتمال وقوع این گونه عملیات زمانی بیشتر می‌شود آنان از تسلیحات هسته‌ای، شیمیایی و بیولوژیک استفاده کنند. هرچند این تهدیدات در حال حاضر، به صورت بالفعل صلح و امنیت بین المللی را تخریب می‌کند باید اذعان کرد که تروریسم سایبری، تهدیدی بالقوه علیه جامعه بین المللی است که روش نوینی از اقدامات تروریستی به شمار می‌آید و نه گونه دیگری از تروریسم؛ چنان که مجمع عمومی سازمان ملل در سال ۱۹۹۵ با صدور قطعنامه‌ای این موضوع را مورد عنایت قرار داد. تروریسم سایبری که از جمله مصادیق جرایم تروریستی نوین است، زنگ خطری جدی برای تمام مردم دنیا و نیز دولت‌ها تلقی می‌شود. با وجود این، فرآیند برخورد با تروریسم سایبری به نسبت تروریسم کلاسیک و سنتی نه در سطح تقنینی و نه در سطح حمایت‌های اجتماعی، چندان قابل ملاحظه و توجه نیست. مشهور است تروریسم سایبری به مثابه تهدیدی نوین است که گروه‌های تروریستی از اینترنت برای اهداف گوناگونی همچون اطلاع رسانی، تبلیغات، جذب نیروی انسانی و جمع آوری اطلاعات استفاده می‌کند. شبکه اطلاع رسانی رایانه‌ای برای تروریست‌های اطلاع رسان، مطلوب به نظر می‌رسد؛ چرا که به دلیل متمرکز نبودن، کنترل یا محدودسازی آن دشوار است و امکان دستیابی را برای هر شخصی ممکن می‌سازد. با این حال به طریق دیگری هم می‌توان هم به عنوان یک ابزار مستقیم برای حمله و هم به عنوان یک صلاح مستقیم از فضای مجازی استفاده کرد (نمامیان، ۱۳۹۱: ۱۷ و ۱۴). باری، تروریسم سایبری به عنوان گونه‌ای جدید از تروریسم نشانگر آسیب پذیر بودن تابعان حقوق بین الملل در فضای سایبر است. اگر تروریست‌ها زیرساخت‌های یک دولت مانند حمل و نقل هوایی، سدها، نیروگاه‌های هسته‌ای و تولید برق، سیستم بانکی و مالی را با انواع بدافزارها مورد حمله قرار دهند و از این طریق باعث رعب و وحشت عمومی می‌گردند و با داشتن انگیزه‌های سیاسی یا ایدئولوژیک این اقدامات را در راستای اجبار دولت یا سازمان انجام دهند آنگاه تروریسم سایبری محقق می‌گردد. در حال حاضر جامعه جهانی بر سر تعریف جامعی از تروریسم به توصیفی دست نیافته‌اند و

حتی سند جامع الزام آوری نیز در این موضوع وجود ندارد اما این شکل از تروریسم به همراه دیگر گونه‌های نوینی چون بیوتروریسم، تروریسم هسته‌ای و اکوتروریسم ممکن است خسارت زیان بارتری نسبت به انواع کلاسیک تروریسم ایجاد کند. بنابراین می‌توان اظهار کرد که تروریسم سایبری تهدیدی علیه صلح و امنیت بین المللی است و در عین حال ناقض قواعد حقوق بشر در هر چهار نسل شناخته شده آن به شمار می‌آید (میربد و همکاران، ۱۳۹۸: ۲).

به عنوان طبقه بندی مفهوم و چیستی نبرد سایبری باید قائل و مشعو بر این باور بود که تروریسم سایبری امروزه به نگرانی‌های حقوقی و سیاسی بین المللی در زمینه تروریسم اهمیت دو چندانی بخشیده است. شکل فقدان تعریف موجود در تروریسم سنتی بر سر این نوع جدید از تروریست سایه افکنده و آن را با پیچیدگی‌های فزاینده‌ای همراه کرده است. از دیگر سوی، چالش‌های ذاتی فضای سایبر نیز مزید بر علت شده و این اصطلاح را به چالش برانگیزترین مباحث روز مبدل ساخته است. (میرعباسی و همکاران، ۱۳۹۵: ۱۷). چرا که بزرگ‌ترین خطر برای صلح و امنیت ملی و بین المللی شمرده می‌شود (شکری، همان: ۹۴). و نفوذگران یا افراد هکر، بارزترین بزهکاران فضای سایبر در زمینه نفوذ و رخنه در دیواره‌های امنیتی ایجاد شده در سیستم‌های رایانه‌ای هستند (حاجی رضایی، ۱۴۰۰: ۲۰).

۶ یافته‌ها و پیشنهادها

همان‌طور که پیش‌تر اشاره شد جامعه و مسائل امنیتی همزاد یکدیگر هستند و نمی‌توان جامعه‌ای را تصور کرد که فارغ از مسائل امنیتی و راهبردی باشد. شکل گیری دولت‌ها با بروز همین مسائل و بحران‌ها تعریف و تعیین یافته و جمهوری اسلامی ایران هم از این قاعده مستثنی نیست. کشور ایران در بیش از چهار دهه از عمر خود همواره با مسائل امنیتی و راهبردی متعدد داخلی و خارجی روبه‌رو شده است. برخی از این مسائل بنیان‌های وجود جمهوری اسلامی را هدف قرار داده و ضربات سنگینی را بر آن وارد آورده‌اند و برخی به بحرانی مزمن و مخاطره آمیز تبدیل شده است (قاضی زاده، ۱۴۰۰: ۷). در حال حاضر بسیاری از امکانات فنی و تکنولوژی‌های خارجی امروزی که در کشور مورد استفاده قرار می‌گیرد مربوط به سال‌ها قبل بوده که هم اکنون نزد ماست و هرچند معاونت پژوهشی وزیر علوم در مورخه ۲۴ مرداد ماه ۱۳۹۵ اعلام نمود که کشورمان از نظر رشد علمی رتبه سوم جهان را داراست ولی به نظر می‌رسد باید قدمی جهشی برداشته و سبقتی اساسی در علوم فنی بگیریم تا در زمینه‌های سایبری و ... بتوان مقابله کرد. لذا در قالب پیشنهاد، فعالیت‌های ملی و بین‌المللی در آینده بایستی بر موضوعات ذیل متمرکز شود:

الف. در زمینه‌های جدید حقوقی باید مطالعات تطبیقی و همکاری بین المللی بیش از گذشته گسترش یابد.

ب. علوم آکادمیک باید نقش بیشتری در پروسه‌های هماهنگ سازی حقوق ایفا کند.

ج. با توجه به فراملی بودن ماهیت جرایم سایبری، لزوم تعاون بین المللی در تدوین قوانین و تعقیب بین المللی مجرمین سایبری بسیار اهمیت می‌یابد.

و. مهم‌ترین ویژگی جرایم سایبری در جهانی بودن آن‌هاست که این ویژگی در گرو ماهیت فضای سایبر است. از این رو اگر نگوییم تنها راه ولی مهم‌ترین راهکار پیشگیرانه از جرایم سایبری، امنیتی همکاری‌های بین المللی است.

هـ. یکی دیگر از رموز موفقیت سیاست‌های هماهنگ دولت برای مدیریت فضای مجازی، افزایش قدرت سایبری از طریق دکترین و مفاهیم، تجهیزات، آموزش و توسعه و توانمند سازی کارکنان بخش‌های مختلف و مهم سازمان‌های اطلاعاتی و امنیتی برای شناسایی تهدیدات و مقابله با آن در فضای سایبر است (شکری، همان: ۱۶۳).

به هر حال صرفنظر از بسط و اطاله کلام، به عنوان پیشنهاد سازنده در راستای تقویت ماشینِ امنیت ملی کشور در فضای سایبری، اقدامات کشورهای پیشرو در زمینه امنیت سایبری را در قالب نمودار را در پنج بُعد اصیل ترسیم می‌نماییم (شکل ۱).

۷ نتیجه‌گیری

امروزه تروریسم سایبری به یکی از چالش‌های عمده نظام‌های حقوقی به خصوص نظام‌های کیفری تبدیل شده است. باری، بزه تروریسم دیگر از رویکردهای سنتی خود رنگ باخته و به سوی فناوری‌های نوین روی آورده است. از همین رو می‌توان گفت که زیرساخت‌های حیاتی و اطلاعاتی به عنوان عمده‌ترین بزه دیدگاه تروریسم سایبری، بیشترین جذابیت و مطلوبیت را برای تروریست‌های دارند. در حال حاضر، فضای سایبر حاصل پیشرفت تکنولوژی بشر در زمینه دیجیتال و علوم رایانه است بنابراین بایستی اظهار داشت که در عصری که ملاک و نژاد فکر برتر بر مدار ارضی دانش سایبرنتیک و گستره حدود و ثغور آن می‌چرخد امنیت مفهومی گیرا و چند بُعدی پیدا می‌کند پرده‌های محدودی واژه امنیت پاره و گدازه‌های آتشفشان عظیم واژگان امنیت بر دامنه و گستره آن فوران می‌کند. در نظم حقوقی کنونی بایستی از معنای تک پرِ امنیت که تمامیت جامعه را در آفند و پدافند تلخیص می‌کند رها شده و زنجیره‌های محدودیت و اسارت در قفس خودکامگی شکسته و جامعه را در مسیر ایمن کاشت. صرفنظر از تعبیر مضیق واژه امنیت در جنگ و میدان نبرد، باید قائل به این نظر بود که امنیت صرفاً در حوزه شلیک و گلوله خلاصه نمی‌شود بلکه یکی از مجاری رگه‌های مهم عنصر امنیت، در تامین آسایش مجازی در راستای القاء تفکرات سازنده در فضای واقعی است. کاربر مجازی باید در امن‌ترین فضای ممکن بتواند به دور از تهدیدات و سرقت‌های هکری یا سیاسی، تخم افکار نوین و متناسب با فرهنگ کنونی را در بطن جامعه کاشته و در اثنا کشمکش‌های مجازی آن را نگاه‌داری، پرورش و در گهواره قانون جامعه تزریق نماید. این مهم جز با تعاون و تعاملات سازنده با دنیای بیرون، شایسته گزینی متخصصین امر، تقنین بزه و تعقیب بزهکاران مجازی ممکن نیست.

شکل ۱: اقدامات کشورهای پیشرو در زمینه امنیت سایبری

مراجع

[۱] بیات، بهرام، نظریه‌های امنیت ملی، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۲] چگینی، حسن، نظام مدیریت استراتژیک، جلد اول، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۳] چگینی، حسن، نظام مدیریت استراتژیک، جلد دوم، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۴] حاجی رضایی، عسل، جایگاه تروریسم سایبری با نگاهی به اسناد بین المللی، نشر قانون یار، تهران، ۱۴۰۰.

[۵] حاجی زاده، قباد، امنیت ملی، نشر قانون یار، تهران، ۱۳۹۸.

[۶] حاجی ملامیرزایی، حامد، قوانین امنیت سایبری، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۷] حاجی میر، سید ابوالقاسم، نگاهی به مدیریت استراتژیک، انتشارات سخنران، تهران، ۱۳۹۶.

[۸] حکیم، حمید، غلامی، سعید، منصوری قوام آبادی، سهیلا، امنیت ملی و فضای سایبری، نشر پشتیبان، تهران، ۱۳۹۸.

[۹] حیدری، سعید بیگی، علی، تاثیر فضای سایبری بر امنیت از منظر حقوقی، اجتماعی و سیاسی، نشر فانوس دنیا، تهران، ۱۳۹۸.

[۱۰] ریاضی، وحید، دهقان، حسین، سیاستگذاری دفاع ملی، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۱۱] شکری، محمد، پیشگیری از جرایم سایبری علیه امنیت ملی در ایران، نشر قانون یار، تهران، ۱۳۹۹.

[۱۲] قاضی زاده، علیرضا، مسائل راهبردی امنیت ملی جمهوری اسلامی ایران، نشر پژوهشکده مطالعات راهبردی، تهران، ۱۴۰۰.

[۱۳] کریمی پاشا، سجاد، بردبار، مهرداد، مقدمه‌ای بر جغرافیای فضای سایبر، دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۱۴] کمالی، سید تقی، امنیت سایبری، انتشارات پشتیبان، تهران، ۱۳۹۸.

[۱۵] مرادی، سهیلا، قدسی، سید ابراهیم، نقش فضای سایبری در وقوع جرم، انتشارات ماهواره، تهران، ۱۳۹۹.

[۱۶] میرسمیعی، سید محمد، اصلی نژاد، مهدی، ماهیت نبرد سایبری، انتشارات پشتیبان، تهران، ۱۳۹۷.

[۱۷] بلو، الکس، برات اندرو، امنیت سایبر، مترجم کشت ورزه فاطمه، نشر راه پرداخت، تهران، ۱۳۹۹.

[۱۸] سانو، براهیما، راهنمایی بر توسعه استراتژی امنیت سایبری ملی، ترجمه چمندار، مهدی، فضلی، حسن، نشر ناقوس، تهران، ۱۳۹۸.

[۱۹] کلکینز، تیم، استراتژی دفاعی برند، ترجمه حیدرزاده، کامبیز، شجاعی، نیما، نشر شرکت چاپ و نشر بازرگانی، تهران، ۱۳۹۳.

[۲۰] گیورا، آموس، امنیت سایبری: ژئوپلتیک، قانون و سیاست، ترجمه موسوی، سید علی، نشر نسل روشن، تهران، ۱۳۹۹.

[۲۱] لیتون، پیتر، استراتژی بزرگ، ترجمه سلیمی، غلامرضا، نشر دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

[۲۲] لوهمان، ولفگانگ، مارکل هابرت، سایبرنتیک، نشر مینوفر، ترجمه رئیسی، سلیمه، تهران، ۱۳۹۵.

[۲۳] موحدی صفت، محمدرضا، امنیت ملی در فضای سایبر، مطالعات دفاعی استراتژیک، ۱۳۸۶، شماره ۳۰.

[۲۴] میربد، لیلا، سلیمی، صادق، نیاورانی، صابر، زمانی، سید قاسم، تروریسم سایبری: نقض حقوق بشر و آزادی‌های بنیادین، فصلنامه حقوق پزشکی، ویژه‌نامه حقوق بشر و حقوق شهروندی، ۱۳۹۸.

[۲۵] میرعباسی، سید باقر، کورکی نژاد قدایی، قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد، فصلنامه مطالعات حقوق عمومی، ۱۳۹۷.

[۲۶] نمامیان، پیمان، مواجهه با تروریسم سایبری در حقوق بین الملل کیفری، فصلنامه پژوهش‌های ارتباطی، سال بیستم، ۱۳۹۲.