فضای سایبری و امنیت ملی جمهوری اسلامی ایران

محمدعابد عباسی[1]، مرتضی لطفی[2]

تاریخ دریافت: ۱۳۹۱/۰۳/۱۵
تاریخ پذیرش: ۱۳۹۱/۰۶/۱۹

چکیده

امروزه حفاظت و حراست از سرزمین ها، استراتژی ثابت تمامی ملت ها و نظام های سیاسی جهان است و به عنوان یک ارزش بنیادی متضمن ثبات و تداوم امنیت ملی است که بودن ترید این شاکله همواره در معرض تهدیدات متنوع و نوظهوریست که به طبع ابداعات و پیشرفت های علمی بشر دارای پیچیدگی ها و ابهاماتی می باشد که مبحث سایبری و پیامدهای مخرب این پدیده نوظهور مسأله ای شده که در سال های اخیر مورد توجه و دست مایه محققان و پژوهشگران این حوزه به ویژه نهادهای نظارتی و امنیتی قرار گرفته است. بنابراین یکی از محورهای اصلی تهدید امنیت در عصر ارتباطات و جهانی شدن برای کشورها و به خصوص ایران فضای مخرب رقابتی فرا منطقه ای سایبری و بحران های ناشی از آن است که نمونه بارز آن حمله رایانه ای به تاسیسات هسته ای و الکترونیکی ایران از طریق ویروس استاکس‌نت به عنوان نخستین حمله سایبری پایدار امریکا علیه یک کشور دیگر را اشاره نمود. بنابراین هیچ عنصری برای پیشرفت بشر و تکامل جامعه مهم تر از مفهوم امنیت نیست و به لحاظ نقش و جایگاهی که دارد مهمترین پارادایم روز دنیاست چرا که جبهه مقابل تروریسم سایبری امنیت ملی کشورهاست که با توجه به حوزه مفهومی آن مختص به یک قلمرو یا حوزه سرزمینی نیست و به عنوان تهدیدی جهانی محسوب می گردد.

واژگان کلیدی: *ایران، فضای سایبر، امنیت ملی، جهانی شدن.*

---

[1] کارشناس ادبیات و معاونت اجتماعی هنگ مرزی بانه.

[2] کارشناس ارشد علوم سیاسی و پرسنل وظیفه هنگ مرزی بانه.

مقدمه

تکنولوژی اطلاعات، صرف نظر از موقعیت جغرافیایی در تمام شئون زندگی وارد شده است، کمتر کسی باور می کرد که ایران در سال ۱۳۷۰ برای اولین بار توسط مرکز تحقیقات فیزیک نظری و ریاضیات به شبکه جهانی اینترنت متصل شد و اولین ارتباط ایران با اینترنت به طور موقت و از طریق اتریش و به وسیله پست الکترونیکی صورت گرفت، امروز کاربران آن به بیش از ۴۰ میلیون نفر برسد که قطعا همانند سایر محصولات عصر نو ارتباطات نگرانی هایی نیز به دنبال دارد به عبارتی هم سازنده است و هم مخرب، بدین مفهوم که امکان رفتارهای ضد اجتماعی و مجرمانه را به وجود آورده که پیش از این به هیچ وجه امکان پذیر نبوده و با روند رو به رشد این جرایم روبه رو هستیم. زیرا جرایم رایانه ای به دلیل ویژگی هایی که دارند، نسبت به سایر طرق ارتکاب جرایم، ارجح تر می باشند. اول آنکه شیوه ارتکاب آنها آسان است، با مبالغ اندک، خسارات هنگفتی وارد می نمایند، می توان بدون حضور فیزیکی در یک حوزه، این گونه جرایم را در فضای معین آن حوزه مرتکب شد، در آخر اینکه اغلب موارد غیر قانونی بودن آنها روشن نمی باشد. از سوی دیگر با پیشرفت تکنولوژی کامپیوتر راه های ارتکاب جرم فنی تر و تخصصی تر گشته و راه های مقابله با آن نیز دشوارتر می نماید. یکی از ویژگیهای فناوری اطلاعات به ویژه اینترنت، امکان ساماندهی و تدارک تهاجم سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده می باشد و به مهاجمان این امکان را می دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت های حیاتی می شود، با ایجاد ارتباط مخرب مانع از واکنش های دفاعی و یا ایجاد تاخیر در آنها می گردد (حسن بیگی، ۱۳۸۴ :۳). در دنیای امروز دیده می شود که برخی اقدامات تروریستی توسط دسترسی به اطلاعات حفاظت شده صورت می پذیرد و به نوعی

شکست های حفاظتی جبران ناپذیری را به دنبال می آورد. تروریست های اطلاعاتی می توانند به صورت غیرمجاز وارد سیستم های کامپیوتری امنیتی شوند، مثلاً با تداخل در سیستم ناوبری هوایی باعث سقوط هواپیما شده یا باعث قطع برق سراسری یا مسموم کردن منابع غذایی شوند (سلمانی زاده، ۱۳۸۰: ۲۰) .که شاخص آن حملات به تاسیسات نظامی و اخلال در این حوزه می باشد و به طور کلی آسیبهای امنیتی جدی ایجاد می کنند که می تواند منجر به ایجاد بحران های نوع حاد گردد.

بنابراین امروزه اهمیت و درک چنین فضایی در ارتباط با مفهوم امنیت ملی، از مهم ترین ادراکات ضروری برای جوامع مختلف است. توجه به این نکته مهم است که در دیدگاه‌های جدید درباره امنیت کل جامعه بشری از فرد گرفته تا بزرگترین نهادهای بین‌المللی می‌تواند منشا تهدیدات تلقی شوند. در پایان قرن بیستم ما به وضوح شاهد پایان جنگ سرد، انحلال نظام دو قطبی، سقوط کمونیسم و تغییر بازیگران اصلی روابط بین‌المللی بودیم. به اعتقاد (رابرت ماندل) از دیدگاه مفهومی، دگرگونی مزبور سه مرحله داشته: تهدید حاکمیت ملی، افزایش وابستگی متقابل جهانی و بالاخره فزونی کشمکش های بی‌نظم و هرج و مرج گونه (ماندل، ۱۳۷۹: ۲۶). این مقاله با بررسی رویکردهای داخلی امنیت ملی، به مفهوم امنیت در عصر جهانی شدن پرداخته و ضمن بررسی فضای سایبری تاثیر آن بر امنیت ملی جمهوری اسلامی را مورد بررسی قرار می‌دهد. در واقع فرض اصلی مقاله این می باشد که با توجه به تغییر ماهیت امنیت در عصر جهانی شدن و گسترش روز افزون ارتباطات مجازی ماهیت تهدیدات نیز دچار تغییر شده و در چنین فضایی آسیب پذیری جمهوری اسلامی ایران افزایش بیشتری یافته است و از این رو لزوم توجه و برنامه ریزی در مقابله و اقدام در فضای مجازی با توجه به اولویت های منافع ملی را ضروری می داند.

بیان مساله

جهانی شدن آمیخته ای از فرصت و تهدید امنیتی می باشد که با توجه به ساختار فرهنگی و ایدئولوژیکی هر کشوری، بهره وری آن تغییر کرده، از تهدید تا فرصت کامل، متغیر می باشد. از سوی دیگر بسته به تحرک و پیشرفت در ساخت فناوری و نهادهای جدید تکنولوژی، معمای حفاظتی به طور فزاینده ومسائل مرجع امنیتی به صورت گسترش یابنده، با هدف جلوگیری از انواع شکست های حفاظتی متعدد شده، از علایق فرد، موجودیت نهادهایی از قبیل گروه، جامعه و سازمان تا کشور را در بر می گیرد. مرجع امنیت و نهادهای تامین امنیت در هر یک از رهیافتهای نظری کدام است؟ در پاسخ به سوال باید امنیت را در رهیافتهای نظری و رویکرد اجرایی مختلف بررسی نمود: (سیف زاده، ۱۳۷۹، صص۲۱۳ و۲۲۵ و ۲۴۷).

۱- امنیت در رهیافت نظری و رویکرد باستان گرایان تامین فضیلت و حفاظت از حاملان آن می باشد.

۲- امنیت در رهیافت نظری و رویکرد اجرایی دنیای مدرن تامین قدرت انسانی و حاملان متخصص آن می باشد که البته نقدی اساسی می توان متوجه آن نمود که اگر چنین بود چرا جان میلیون ها انسان مدرن قربانی زیاده خواهی حاکمان و اندیشه های ایدئولوژیکی آنها طی دوجنگ جهانی شد.

۳- امنیت در دیدگاه پسا تجددگراها شامل نهادگریزی، اراده‌گرایی، معناجویی و لذت‌گرایی می باشد. بنابراین سایبر تروریسم در واقع نهاد گریزی را مبنای اقدام خود دنبال می کند و حوزه آسیب پذیری را در تهدید نهادها جسته است.

در هر دوره ای تهدیدات و نا امنی متوجه حوزه های خاصی بوده که از یک سو بسته به اولویت ارزش ها و دستاوردهای جدید بشری و از سوی دیگر قدرت توانایی تامین امنیت و امنیت سازی

برای آن حوزه تغییر می‌کرد. به عبارت دیگر اگر با افزایش توان نظامی در حوزه ای امنیت حاصل می شد حوزه دیگری که مغفول مانده و امکان تامین نبوده نشانه های فقدان امنیت آشکار می گردید که نمونه بارز آن در نظام مقدس جمهوری اسلامی ایران کم توجهی به فضای مجازی توسط نهادهای زیر ساختی و امنیتی می باشد به طوری که با افزایش روز افزون کاربران این فضای مجازی هیچ گونه ساختار فرهنگی و کنترلی و نظارتی برای آن در نظر گرفته نشد و از هر طرفی هر روز جرایم این حوزه در حال افزایش بود که به نوعی جرم افسار گسیخته تبدیل شد و وجود خلاءهای قانونی در برخورد با این جرایم خود مزید بر علت شد و نبود زیر ساختهای فرهنگی در ترویج مبانی سازنده و بسیار مفید اینترنت موجب بروز مشکلات اساسی شد که متاسفانه لایه های ضد اخلاقی و اجتماعی به عنوان اولین پیامد و در پی آن منتهی به ایجاد لایه های ضد امنیتی گشت. از آنجایی که همواره یکی از عوامل ایجاد نا امنی، تروریسم می باشد و هر جا عرصه را بر خود تنگ دیده است با ارائه تعریفی مجدد و بازنگری در شرایط و موقعیت خود اقدام خشونت بار خود را در محیط جدید امنیتی پی گرفته است ولی آنچه تقریبا ثابت مانده اقدام تهدیدی تروریستی می باشد. از نظر «مارتا کرنشاو» تروریسم ممکن است به عنوان گزینه ای مطلوب از سوی تمامی اعضا گروه تروریستی به دلایل سیاسی و استراتژیک مطلوب به نظر رسیده و انتخاب شود (Tosini, 2007: 664-681). در تبیین پدیده تروریستی نیز به همین مسأله اشاره می شود اما در این مرحله این سوال مطرح است که چرا برخی گروه ها از ابتدا برای نیل به اهداف خود به خشونت متوسل می شوند ولی برخی در فرایند تصمیم گیری به عنوان آخرین حربه به آن متوسل می شوند و برخی حتی در شرایط یکسان به دنبال راه های مسالمت آمیز هستند؟

«کرنشاو» عوامل متعدد از جمله شرایط مکانی، اندازه، شرایط زمانی و محیط بین المللی را در این موثر می داند (O'Connor, 2005). اما اهمیت تاثیر این موارد در مرحله بعد از اهمیت اهداف و معیارها، ایدئولوژی و میزان پای بندی اعضا به ایدئولوژی است. آنچه در این دست تحقیقات به ما کمک می کند آن است که گرچه روند حرکت عملی به سمت تروریسم درسطح «عقلانیت کنشی» قابل بررسی است اما ریشه های عمل تروریستی در عقلانیت نظری و ساختاری (منابع توجیه کننده نظری مثل آموزه های اسطوره ای و مذهبی) نهفته است[1]. نتیجه اینکه سایبر تروریسم باز تعریف محیط عملیاتی از سوی تروریستها می باشد و بیش از آنکه کنشی ضد امنیتی باشد اقدام و واکنشی به محدودیت های محیط عملیاتی می باشد و آسیب پذیری را مبنای تصمیم اقدام تروریستی خود قرار داده است.

روش تحقیق

برای پی بردن به جایگاه امنیت به عنوان زیر ساخت اصلی در شاکله هر نظام سیاسی و ظهور تروریسم سایبری به عنوان تهدیدی فراملی و جهانی و نیز با توجه به جایگاه حساس و ویژه ایران اسلامی در نظام بین المللی و دشمنی های آشکار و نهان غرب وشرق با این ملت ولایی و در پاسخ به این سوال که تروریسم سایبری چگونه می تواند بر امنیت ملی جمهوری اسلامی ایران تاثیر گذار باشد لذا با مطالعه کتاب ها و مقالات مرتبط و مشاوره با اساتید و هم اندیشی و تعمق در این زمینه موضوع به روش توصیفی - تحلیلی و با استفاده از ابزار کتابخانه ای مورد کنکاش و بررسی قرار گرفته که امید بهره وری آن می رود.

[1] Robert A. Pape, Strategies logical of suicide terrorism, American Political Review, Vol. 97, No. 3 2003.

تروریسم سایبری

تروریسم را به کارگیری خشونت علیه اشخاص، دولت ها یا گروه ها برای پیشبرد زورمندانه اهداف سیاسی یا عمومی تعریف می‌کنند. تروریسم در مفهوم رایج عبارت است از توسل به خشونت برای ایجاد رعب و هراس یا تهدید به آن. اصولا با توجه به سه عامل: «روش» که متضمن خشونت است، «هدف» که شامل شهروندان و دولت می شود و «قصد» که اشاعه ترس و تحمیل مقاصد سیاسی و تغییرات اجتماعی است، تروریسم تعریف می شود (Annamarie and Pat, 2005:157). سایبر تروریسم نیز در حقیقت همان تعریف را دارد، با این تفاوت که این بار هدف متمرکز روی منابع موجود در فضای مجازی است. این واژه نخستین بار از سوی «کالین باری» در دهه ۱۹۸۰مطرح شد و بیشتر به معنای حمله یا تهدید بر علیه رایانه ها، شبکه های رایانه ای و اطلاعات ذخیره شده در آنهاست، هنگامی که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می شود. به گفته (کانوی) تروریسم سایبری عبارت است از حمله عمدی و آگاهانه با انگیزه های سیاسی به وسیله گروه های فراملی یا عوامل پنهانی علیه اطلاعات، سیستم های رایانه ای، برنامه های رایانه ای و داده ها که منتهی به خشونت علیه افراد نظامی و غیر نظامی و سایر اهداف شود (Seddon, 2004: 20). سایبر تروریسم می تواند ابعاد داخلی داشته باشد یا شامل موارد بین المللی شود. سایبر تروریسم امروز خطرناک تر از تروریسم سنتی است به این دلیل که ساختار اقتصادی و خدمات رسانی بسیاری از کشورها مبتنی بر فناوری های اطلاعاتی و ارتباطی شده است. با این توضیحات می توان سایبر تروریسم را چنین تعریف کرد:« اقدامات برنامه ریزی شده و هدفمند با اغراض سیاسی و غیر شخصی که علیه رایانه ها و امکانات الکترونیکی و برنامه های ذخیره شده در درون آن ها از طریق شبکه جهانی صورت می گیرد و هدف از چنین اقدامی

نابودی یا وارد آوردن آسیب های جدی به آن هاست. سایبر تروریسم از ایجاد مزاحمت توسط خرابکاران رایانه ای آغاز می شود و تا مباحث مربوط به پیامدهای فاجعه بار حملات شیمیایی، میکروبی، تشعشعی و هسته ای را در بر می گیرد (فلمینگ و استول، ۱۳۸۴: ۱۵۶). درباره میزان خطرناکی این جرم، یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین المللی امریکا با اشاره به ادعای یک مقام رسمی سیا می نویسد: تروریست در فضای سایبر قادر است با یک میلیارد دلار هزینه و ۲۰ هکر شایسته، ایالات متحده را فلج کند. (والتر لاکور) یاد آوری می کند اگرچه هدف تروریست ها معمولا قتل سران سیاسی و گروگان گیری و...است اما صدمه ای که با حمله الکترونیکی به شبکه های رایانه ای وارد می آید ممکن است بسیار غم انگیزتر باشد و اثرات آن تا مدت ها باقی بماند (درآنجلیز، ۱۳۸۳: ۱۶). در واقع تروریستها صرف نظر از ماهیت و اهداف اقداماتشان نتایج بسیار زیان بار و گاه جبران ناپذیری به جای می گذارند. معمولا آنها نقاط حساس و حیاتی جوامع را هدف قرار می دهند تا اساسی ترین ضربات را به دشمنان خود وارد کنند و بهترین بهره برداری را از وضعیت موجود به عمل آورند که بی تردید زیرساختهای حیاتی و زیربناهای امنیتی از بهترین گزینه ها به شمار می آیند.

البته سهولت و کم هزینه بودن ارتکاب این اقدامات نیز از اهمیت قابل توجهی برخوردار است، لذا این گروه ها همواره به پیشرفته ترین ابزارها برای رسیدن به هدف شوم خود مجهز هستند. یکی از بهترین این ابزارها که به نظر می رسد تمامی ویژگی های مورد نیاز تروریست ها را در خود جمع کرده فضای سایبر است. «دنینگ» در تعریف آن می گوید: «تروریسم سایبری از همگرایی تروریسم و فضای سایبر به وجود آمده است. درک عمومی بر این است که به معنای تهاجمات و تهدید به تهاجمات غیرقانونی به رایانه ها، شبکه ها و اطلاعات ذخیره شده در آنها می باشد که به منظور ارعاب یا وادار کردن یک دولت یا مردم آن برای پیشبرد اهداف سیاسی یا

اجتماعی صورت می گیرد. به علاوه برای آنکه یک تهاجم، تروریسم سایبری تلقی شود باید منجر به اعمال خشونت علیه اشخاص یا اموال گردد یا حداقل آنقدر خسارات وارد آورد که منجر به وحشت گردد. تهاجماتی که باعث افشای اطلاعات به ویژه اطلاعات حساس و مهم از اماکن نظامی و امنیتی یا لطمه شدید اقتصادی می شوند، از جمله این موارد هستند.» (Walker, 2006:633). همان طور که برای مجرمان سازمان یافته، فضای نامتقارن مجازی و جنبه های پنهان آن می تواند یک منبع با ارزش باشد برای بازیگران غیر دولتی مانند سازمان های تروریستی و افراطی نیز جذاب است. هرچند شواهد قطعی وجود ندارد که گروه های تروریستی مانند القاعده از قابلیت یا از منابع لازم برای راه اندازی یک حمله اینترنتی برخوردار هستند.گروه های تروریستی به طور فزآینده ای به منظور انتشار پیام خود و بسیج حامیان از وب سایت و اینترنت استفاده می کنند. اینترنت گروه های مختلف را در کنار هم جمع می کند و مناقشه را برای شبه نظامیان و افراط گرایان تسهیل می کند که با تکنیک های اشتراک گذاری، پیام خود را گسترش دهند و با به کار گرفتن نیروهای لازم به موفقیت های برجسته ای دست پیدا کنند. علاوه بر این، تکامل تکنولوژی قابلیت ها را پیچیده می کند، اما اینها نسبتاً ارزان هستند مثل تلفن های هوشمند، نقشه های آنلاین و زیر ساخت های اینترنتی به عنوان اجزای مهم عملیات جنگی همراه با روش های دیگر مورد استفاده قرار می گیرند. پتانسیل استفاده از شبکه های اینترنتی و سیستم اطلاعات تلفن همراه و فناوری های هوشمند در تسهیل حملات تروریستی بسیار موثر هستند.

برای نمونه تمام شواهد و مدارک در بمب‌گذاری بمبئی در نوامبر ۲۰۰۸ (لشکر طیبه) از سیستم های 3G گوشی‌های هوشمند در کنار سلاحهای متعارف برای آماده‌سازی حمله به اهداف غیر نظامی استفاده‌کردند که قادر به ارتباط بین عاملان و ارائه راهنمایی های تاکتیکی به

افراد مسلح در حال حمله است. (Cornis, Livingstone, 2010:8). ممکن است تروریسم سایبری باعث آسیب رساندن به افراد شود اما همیشه هدف آن تحقق اهداف سیاسی، دینی و ایدئولوژیکی است. تا به امروز فعالیت‌های صورت گرفته در زمینه تروریسم سایبری، به میزان قابل توجهی غیر پیشرفته باقی مانده است. به دلیل آنکه فضای سایبری یک مکان مناسب برای تروریست‌ها است.

امنیت ملی در فضای جهانی شده

بدون تردید مقوله امنیت پیش نیاز برای حیات هر نظام سیاسی و اجتماعی است و دولت ها وقت و امکانات وسیعی را برای تامین آن صرف می کنند. مقوله امنیت به مثابه یک آرمان و واقعیت به عنوان یکی از حقوق اساسی مردم مطرح است و در نهایت فرآیند مجموعه ای از تعاملات و نیز تعاون و سازگاری بین اجزاء مختلف نظام اجتماعی است، امروزه نقش و اهمیت امنیت در پیشرفت هر جامعه ای تا بدان پایه است که آن را بستر و پیش نیاز هر گونه توسعه ای دانسته اند، خصوصاً در جوامع در حال توسعه که با انواع بحران ها و چالش های مستمر ناشی از عقب ماندگی و بی ثباتی ساختارهای مختلف سیاسی، اقتصادی، اجتماعی و غیره مواجه می باشند، امنیت نقش تعیین کننده و مهمی در ایجاد انواع توسعه ایفا می نماید (چلبی، ۱۳۸۵: ۲۵). با وجود پیشینه طولانی بحث های مربوط به امنیت، که همان طور که ذکر شد همزمان با خلق انسان متولد شد هنوز شاهد ابهام و پیچیدگی روز افزون و همچنین گسترش دایره امنیت هستیم. به عبارتی می توان گفت امنیت فضای مجازی از جمله دلایل اصلی پیچیدگی و گنگ بودن مفهوم امنیت ناشی از متغیر بودن مولفه های در بر گرفته از تغییر اوضاع و احوال زندگی بشری و ارزش های حاکم بر آن می باشد (مزدارانی، ۱۳۸۹: ۱۲). به

عبارت دیگر مفهوم امنیت در جوامع بدوی و غارنشین با مفهومی که انسان در عصر انقلاب صنعتی و سپس شروع جنگ های جهانی و در حال حاضر عصر جهانی شدن از عناصر امنیت در ذهن دارد تفاوت های بسیار بنیادین دارا است.

این پر رمز و راز بودن و فرو رفتن در هاله ای از پیچیدگی های تئوریکی، ایدئولوژیکی و روز مرگی امنیت تا جایی است که «باری بوزان» از نظریه پردازان برجسته در این حوزه معتقد است که هر کوششی برای درک مفهوم امنیت بدون آگاهی کافی از تناقضات و نارسایی های موجود در خود این مفهوم ساده اندیشانه است. مفهوم سازی امنیت هنگامی پیچیده تر می شود که آن را موضوعی بین رشته ای تصور کنیم که مورد توجه روانشناسان، جامعه شناسان و علمای علم سیاست قرار دارد. زیرا هر یک از دیدگاه خاص خود به بررسی موضوع می پردازند. افلاطون در کتاب سیاست معروف به جمهوری و در کتاب نوامیس معروف به قوامین، خواهان جامعه آرمانی (مدینه فاضله) که در آن همه ی مردم از امنیت اجتماعی برخوردارند می باشد، او معتقد است نباید گذاشت هم در فرد و هم در جامعه یکی از قوا بر دیگری پیشی گیرد زیرا هم در فرد و هم در جامعه تزلزل و انحطاط به میان خواهد آمد و امنیت ناپایدار خواهد شد. مفهوم امنیت مانند سایر مفاهیم اساسی و رایج در علوم انسانی نظیر صلح، عدالت و آزادی در معرض تفسیرها و تعبیرهای گوناگونی قرار دارد و در طول تاریخ بشری با تغییر و تحولات گسترده ای مواجه شده است و مکاتب متعددی نظریات خود را پیرامون این مفهوم ارائه کرده اند. (باری بوزان) آن را برابر با رهایی از تهدید تعریف می نماید و معتقد است امنیت در نبود مسأله دیگری به نام تهدید درک می شود (عبدالله خانی، ۱۳۸۳: ۱۳۵). از دید «آرنولد ولفرز» امنیت در یک مفهوم عینی به فقدان تهدیدها نسبت به ارزش های اکتسابی تلقی می شود و در یک مفهوم ذهنی بر اساس دلهره و نگرانی از به مخاطره افتادن ارزش ها و توانمندیهای لازم در کسب نتایج منصفانه

ارزیابی می شود (چگینی زاده، ۱۳۷۹: ۶۸). بنابراین یکی از دلایل پیچیدگی مفهوم امنیت و ماهیت ابهام‌آمیز آن چند وجهی و میان رشته ای بودن مفهوم امنیت است. وجوه و ابعاد مختلف امنیت را می‌توان در محورهای سیاسی، اقتصادی، نظامی، فرهنگی و زیست‌محیطی دسته بندی کرد (ماندل، ۱۳۷۹: ۸۳- ۷۱). حتی در آموزه های دینی نیز بر اهمیت امنیت تاکید شده از کلام الهی گرفته که بالغ بر ۷۰ آیه در بیان موضوع امنیت و پیامدهای آن (آیه ۸۲ سوره مبارکه انعام، آیه ۵۵ سوره مبارکه نور، آیه ۱۱۲ سوره مبارکه نحل) تا احادیث و روایات پیامبر (ص) و امامان معصوم (ع) و زیباترین آن حماسه همیشه جاوید عاشورا که نماد بارزی از جایگاه و اهمیت امنیت و تلاش برای دستیابی به آن می باشد. لذا گستردگی مفهومی و عمل این واژه و نقش کلیدی آن در بخش ها و حوزه های مختلف باعث شده تا صرف امنیت تنها مختص به یک قلمرو و یا محدوده خاص نبوده و فراتر رفته و جهان شمولی پیوسته و مستمری به خود گرفته باشد. قلمروهای گوناگون امنیت عبارت است از: امنیت فردی، ملی، منطقه‌ای و بین المللی. یکی از متغیرهای پیچیده و نو پدید که در قلمرو امنیت بین المللی مطرح است، مقوله جهانی شدن است. جهانی شدن در این زمینه به معنی فرایندهایی است که، به شکل گرفتن فضای جهانی واحد کمک می‌کند. بنابراین می توان گفت پیشرفت فن‌آوری ارتباطات، زمینه‌ساز جهانی شدن است. جهانی شدن دارای ابعاد مختلف و گوناگونی است. از نظر (مک گرو) جهانی شدن فرایندی چند بعدی است که دارای ابعاد و حوزه‌های مختلف اقتصادی، فرهنگی، سیاسی، اجتماعی و زیست‌محیطی است. از آثار جهانی شدن تغییر محیط بین المللی در نتیجه پیشرفتهای عظیم تکنولوژیک و تحولات گسترده در دانش ارتباطات است. برای نمونه، می‌توان به شکل‌گیری تجارت الکترونیکی به عنوان روشی نو در محاسبات اقتصادی اشاره کرد که شدیدا محیط اقتصاد بین المللی را در عرصه فعالیت های اقتصادی و سازوکارهای آن متحول ساخته و خود محصول

تغییرات در محیط بین المللی می‌باشد. از دیگر عوامل تغییر در محیط بین المللی، حرکت آزاد سرمایه، کالا، خدمات و همچنین اطلاعات است. عوامل مذکور از یک سو به عنوان آثار جهانی شدن محسوب می‌شوند و از سوی دیگر، موجبات بسط و گسترش جهانی شدن را فراهم می‌آورند. سازوکارهای شرایط نو موجب گشته که اهمیت عنصر ژئوپلیتیک بیش از پیش کاسته شود.

بنابراین در جامعه جهانی که اعضای آن شهروندان جهانی محسوب می‌گردند، چارچوب ملی به مبارزه فراخوانده می‌شود و این امر می‌تواند موجبات ناامنی برای واحدهای سیاسی باشد و بزرگترین مشکل از آنجا ناشی می‌شود که انسانها با ساختار تازه‌ای روبه رو می‌شوند که ضرورتاً ملی نمی باشد که به معنای جهانی کردن ناامنی است و این فرایندی است که کل جهان از جمله جمهوری اسلامی و نهادهای امنیتی با آن درگیر است. در واقع جهانی شدن، با شکل جدیدی که محیط امنیت خارجی، بازیگران امنیت خارجی و قواعد بازی امنیت خارجی داده است، سرمنشاء تهدیدهای کاملاً جدیدی برای ایران است که تا دهه پیش وجود نداشته اند. مفهوم کلیدی در این رابطه تهدید در فضای الکترونیکی است که با جنگ های الکترونیکی کلاسیک کاملاً متفاوت می باشند در این رابطه «اسویر لودگارد» یکی از شاخصه‌های اصلی فضای امنیتی جهان معاصر را در تولید انبوه ناامنی دانسته است. با این توضیح که زندگی انسان معاصر از حیث امنیتی بسیار آسیب‌پذیر می‌نماید و کشورهای در حال توسعه با هر قدمی که در راستای توسعه بر می‌دارند، به صورت مستقیم تهدید تازه‌ای را متوجه خود خواهند نمود (مک کین لای و لتیل، ۱۳۸۰: ۲۱). با عنایت به موارد فوق می توان یکی از محورهای اصلی تهدید امنیت در عصر ارتباطات و جهانی شدن برای کشورها را باید در حوزه سایبر و فضای مجازی مورد توجه قرار داد. بنابراین امنیت فضای سایبری به خاطر اتکای بیش ازحد تمامی بازیگران

فرهنگی، اقتصادی، سیاسی و مهمترین آن امنیتی به آن، بی تردید مقوله ای استراتژیک قلمداد می شود و به همین دلیل است که در ارزیابی از تهدیدات امنیت ملی و بین المللی، مفهوم امنیتی فضای سایبری، وارد اسناد پایه ای حفاظتی، امنیتی شده است. سندی که در اجلاس سران ناتو در نوامبر ۲۰۱۰ در لیسبون پرتقال به تصویب رسید، در این زمینه حائز اهمیت است. شایان ذکر است که ناتو از چندی پیش تعدادی از نخبگان امنیت ملی و سیاست خارجی را تحت رهبری آلبرایت وزیر خارجه پیشین امریکا گرد هم آورد تا به این سؤال پاسخ دهند که امنیت کشورهای عضو ناتو در آینده و دهه ای که در پیش است، چگونه و با تأثیر از چه منابعی مورد تهدید واقع می شود.

اکنون دیده می شود که گروه های تروریستی با استفاده از کامپیوتر و اینترنت، تروریسم را گسترش می دهند و با استفاده از اینترنت و وب سایت‌ها بسیاری برای استخدام و افزایش بودجه فعالیت هایشان و برای اهداف آموزش جهادی استفاده می کنند و راه هایی برای همکاری با یکدیگر و نوع جدیدی از تهدید را به وجود آورند که در آن از طریق ابزارهای قدرتمند برای جرایم اینترنتی و سرقت اطلاعات اماکن و اشخاص و یا منحل‌کردن سیستم‌های کامپیوتری که خدمات پشتیبانی از طریق اینترنت را انجام می‌دهندکه از جمله استفاده از چندین روش موثر برای اختلال در سیستم های کامپیوتری، حمله به شبکه های کامپیوتری با استفاده از کدهای مخرب، اختلال در سیستم پردازش و یا سرقت اطلاعات است (Nagre & Warade,2008 :8).

یافته های تحقیق

هم اکنون در مورد اینکه تامین امنیت ایران در گرو پیگیری چه نوع اهدافی است، اختلاف نظر وجود دارد. در این زمینه دست کم پنج دیدگاه، سه دیدگاه درون گرا و دو دیدگاه برون گرا است. هرکدام از این دیدگاه ها تامین و حفظ امنیت ملی را در گرو تعقیب و تحقق یکی از اهداف زیر می داند:

نظریه اول: توسعه اقتصادی را مهمترین هدف استراتژیک ایران می داند. تقابل ادعای توسعه اقتصادی از سوی راست سنتیومدرن در مقابل توسعه سیاسی اصلاح طلبان از سال های ۱۳۶۸ به بعد معطوف به این نظر است. استدلال آبادگران نزدیک به راست سنتی و کارگزاران نزدیک به راست مدرن این است که مشکلات اقتصادی می تواند موجب نارضایتی مردم گردیده و با شدت یافتن آن نظام حکومتی با انفجار اقتصادی مواجه خواهد شد.

نظریه دوم: تاکید خود را بر توسعه سیاسی و آزادی های مدنی گذاشته است. پس از برنامه های نوسازی صنعتی راست مدرن در سال های ۱۳۶۸ تا ۱۳۷۶، از سال ۱۳۷۶ اصلاح طلبان توسعه سیاسی را مبنای اقدام خود قرار دادند. بر این اساس، آزادی های سیاسی و فعالیت احزاب و گروه ها در عرصه های فرهنگی، اجتماعی و سیاسی دارای اهمیت استراتژیک می باشد. به نظر این گروه ایجاد خفقان انسانها را کم مقدار و بی‌توان می‌کند و لذا کشور را دچار ضعف و التهاب شدیدتر کرده و بدین لحاظ بسیار سریع تر به دلیل مشکلات اقتصادی مردم را خواسته یا ناخواسته بر ضد نظام می شوراند.

نظریه سوم: حفظ ویژگی انقلابی و تجدیدنظر طلبی در نظام بین الملل را استراتژیک ترین هدف می داند و معتقد است تعدیل در اصول انقلابی باعث از دست رفتن و فرو پاشی نظام بر آمده از انقلاب اسلامی خواهد شد. این گروه، انقلاب و نظام ملی را از یکدیگر جدا می داند و حفظ

اصول انقلاب را به هر قیمتی ضروری می‌انگارد. گروهی از روحانیان سنتی، همراه با بخشی از نهادهای انقلابی و نظامی خواهان این هدف هستند. سه دیدگاه فوق را می توان به نوعی «درونگرا» نامید. البته نظریه سوم پیامدهای خارجی فراوانی دارد، در حالی که دو نظریه اول با تاکید بر توانا سازی درونی می تواند محیط بیرونی را در جهت اهداف داخلی بسیج کرده و به کار گیرد. برخلاف سه نظریه فوق، دو نظریه «برون گرا» نیز قابل اشاره است که به آنها می پردازیم.

نظریه چهارم: محور این دیدگاه، مسائل خارجی است که در قالب تعریف سنتی از امنیت قرار می گیرد.این نظریه حفظ امنیت جمهوری اسلامی ایران را از لحاظ نظامی، مهمترین مسأله برای نظام می‌داند و مدعی است که برای تامین آن تمام منابع و برنامه ها را باید به یاری طلبید. این نظریه با تکیه بر حمله رژیم عراق به ایران، معتقد است که همیشه خطر جنگ وجود دارد و باید برای رفع هرگونه تجاوز خارجی، آمادگی نظامی بالایی داشته باشیم. بخش قابل توجه و اکثریت نیروهای نظامی به ویژه انقلابی، از این نظریه حمایت می کنند.

نظریه پنجم: معتقد است که بزرگترین دشمن ایران، امریکا و عوامل آن در منطقه چون اسرائیل و در سطح جهان چون کانادا است. بنابراین باید سعی نمود نه تنها در ایران و نه فقط در داخل کشورهای اسلامی، بلکه در تمام دنیا با امریکا درگیر شد. آشکار است که این نظریه در چارچوب تعریف سنتی از امنیت می گنجد ولی نسبت به نظریه چهارم، دایره ی محدودتری را نمایان می سازد. برخی از انقلابیون نظامی گرا و خواهان مبارزه، از این نظر پیروی می کنند. نکته ای که پنهان مانده این است که اکنون در فضایی قرار داریم که ابزارها و به تبع آن شاهد تغییر نوع نگاه به امنیت در دنیای جدید می باشیم. به نظر می رسد که علاوه بر تهدیدهای فوق، امنیت ملی و جانی انسانها در خطر می باشد. از منظر امنیت ملی می توان گفت در شرایط حاضر،

دولت ها و ملت ها با زنجیره ای از تهدیدات نامشخص در محیط های مجازی مواجه اند که امنیت آنها را به چالش کشیده و ابزارهای سنتی تامین کننده امنیت ملی، دیگر توان مقابله با آنها را ندارند (حسن بیگی، ۱۳۸۴: ۲۷۸). باید گفت این یکی از نکات طنزآلود عصر کنونی است، صنعتی که برای حصول امنیت ملی طراحی شده است هم اینک ابزاری شده که می تواند تهدید آفرین باشد. برای نمونه همان گونه که «فریدمن» خاطرنشان می سازد: «ویروس کامپیوتری lovebug در سال گذشته که توسط دو فیلیپینی ناراضی در اینترنت ریخته شد، ظرف ۲۴ ساعت تعداد ۱۰ میلیون کامپیوتر را خراب و ۱۰میلیارد دلار اطلاعات را در هفت قاره از بین برد. بحران موشکی کوبا معطوف به نظام جنگ سرد بود، اما ویروس فوق معطوف به کل سیستم جهانی شدن کنونی است. این حادثه نشان دهنده آسیب پذیری پرخطر ماست» (کالدول، ۱۳۸۲: ۳۴۱). بنابراین جهانی شدن با شکل جدیدی که محیط امنیتی، بازیگران و قواعد بازی امنیت خارجی داده است، سر منشاء تهدیدهای کاملاً جدیدی برای ایران است که تا دهه پیش وجود نداشته اند. مفهوم کلیدی در این رابطه تهدید در فضای الکترونیکی و مجازی است که با جنگ های کلاسیک کاملاً متفاوت می باشند. برای نمونه می توان به هجوم شدید کرم رایانه ای استاکس نت به رایانه های ایران اشاره نمود که علاوه بر اطلاعات سیستم های کنترل صنعتی و نیروگاهی و تاسیسات هسته ای، اطلاعات سیستم های خانگی را نیز به سرقت برد و حدود ۶۰ درصد کامپیوترهای ایرانی را آلوده ساخت. تحقیقات نشان داد که این کرم برای این منظور طراحی شد تا سانتریفیوژهای ویژه غنی سازی اورانیوم را مختل کند. پیچیدگی کرم نرم افزاری استاکس نت به حدی بود که برخی از متخصصان از آن به عنوان «تروریسم سایبری» یاد کردند. به بیانی دیگر گروه یا کشوری با هدف تخریب ساختارهای حیاتی یک کشور این نرم افزار مخرب را نوشته و فعال کردند که هدف گیری 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 اولین ویروس رایانه ای بود که با هدف ایجاد تغییرات فیزیک در جهان واقعی ساخته شده است. در این خصوص روزنامه نیویورک تایمز روز جمعه ۱۳ خرداد ۱۳۹۱ در گزارشی فاش کرد باراک اوباما، رئیس جمهور امریکا در اولین ماه‌های ریاست جمهوری خود، به طور مخفیانه دستور یک حمله سایبری با ویروس رایانه‌ای استاکس‌نت را علیه ایران، صادرکرده است. این عملیات در واقع نخستین حمله سایبری پایدار امریکا علیه یک کشور دیگر است، که با استفاده از کدهای مخرب طراحی شده با همکاری اسرائیل انجام گرفته است. درست مانند عملیات کودتای ۲۸ مرداد ۱۳۳۲ که سازمان سیا برای اولین بار در یک تجربه برون مرزی، دولت قانونی مصدق را سرنگون کرد و حکومت وابسته به محمد رضا شاه را بار دیگر به مردم ایران تحمیل نمود (بهشتی پور، ۱۳۹۱). امریکایی ها همچنین ویروس سارق اطلاعات به نام «دوکو» را برای سرقت اطلاعات از زیرساخت های حیاتی صنعتی و انرژی نفت و گاز ایران طراحی کرده بودند که در سال ۲۰۱۱ گزارش شد بخشی از صنعت ایران را هدف قرار داده بود (همان، ۱۳۹۱). می توان گفت ساختار اینترنت اساساً، چالش‌های امنیتی برای دولت‌ها به وجود می‌آورد. اینترنت به عنوان یک سیستم نا متمرکز طراحی شده و کاربران آن غالباً شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی حملات سایبری باقی نماند.

نتیجه گیری و پیشنهادها

با گسترش انقلاب های تکنولوژیک و اطلاعاتی و پیچیده تر شدن مناسبات اقتصادی و تولیدی در عصر جهانی شدن، از یک سو مفهوم قلمرو زدایی مطرح شده و از سوی دیگر تغییر ماهیت تهدیدهای امنیت و مفهوم مرز و حراست از آن را به مسأله ای حیاتی بدل ساخته است. بنابراین ویژگی جهانی و بدون مرز بودن این فضا با توسل به فناوری اطلاعات، امنیت ملی را با چالشی جدی مواجه کرده است. بنابراین به عنوان نتیجه‌گیری کلی می‌توان گفت هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدید کننده، تاثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب شده تا بازیگران اعم از دولت‌ها، گروه های سازمان یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی چون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و ... را به وجود آورند. جمهوری اسلامی ایران نیز چون محیط امنیتی آن بیش از آنکه دارای فرصت باشد، تهدیدهای بی شماری را در بر دارد همانند هر کشور دیگری نیازمند استراتژی جامعی برای مقابله با این مسأله در جهت تضمین امنیت خود و دستیابی به منافع حیاتی از جمله انرژی هسته ای می باشد و لزوم برنامه ریزی و مقابله با این مسأله به عنوان یکی از مهم ترین تهدیدها و آسیب ها با توجه به اقدامات تخریبی علیه آن نظیر استاکس نت و ... ناگزیر می نماید. زیرا با اتخاذ یک روش و برنامه ریزی مناسب می توان این روند را معکوس نمود و مهم ترین کار ویژه امنیتی یک نظام، یعنی تبدیل تهدیدات به فرصت ها را صورت داد.

راهکارها و مشکلات مقابله با تروریسم سایبری

ملاحظه می شود پس از جنگ جهانی دوم تهدیدات گسترده‌ای جهان را فرا گرفته و به تبع آن امنیت ملی کشورها به مخاطره افتاده است. این مسأله به ویژه در خلیج فارس که جنگ های فیزیکی و روانی در آن جریان داشت و تلاش دولت های این حوزه و نیز نیروهای فرا منطقه ای همواره به ایجاد طرح های امنیتی در راستای اهداف خود معطوف بوده و همانگونه که بررسی شد می توان اقدامات در فضای سایبر را در این زمینه مورد توجه قرار داد و از طرفی گسترش سریع اینترنت در کشورمان بدون توجه به آسیب های احتمالی آن منجر به ایجاد جبهه جدید و حمله به ایران اسلامی گشت که تمامی تئوریهای امنیتی و حفاظتی را دچار چالش قرار داد و می طلبد از فضای غبار آلود موجود نسیم های آرامش را ایجاد کرد و چتر احساس امنیت را بر امنیت موجود در جامعه انداخت. لازم به ذکر است برای اقدام در مقابل تهدیدهای امنیتی چند شاخص دارای اهمیت بسیاری می باشد و این عوامل درک سیستم را در برابر تهدیدهای امنیتی شکل می دهند که عبارتند از:

- دانش[1]: که مرتبط با شناخت افراد به تهدیدهای امنیتی می باشد و عواملی چون جدید بودن تهدید امنیتی، داشتن شناخت و فهم از تهدیدهای امنیتی در آن موثر است.
- تاثیر[2]: که مواردی چون مدت زمان شیوع تهدید، محدوده در برگیرنده تهدید امنیتی و اینکه در رسانه ها به آن پرداخته شده باشد را شامل می شود.
- شدت[3]: که مواردی چون آشکار شدن اطلاعات شخصی افراد به واسطه این تهدید و شدت خسارت های ناشی از تهدید امنیتی را شامل می گردد.

---

[1] Knowlege
[2] Impact
[3] Severity

- احتمال[1]: احتمال روی دادن و داشتن سابقه از تهدید امنیتی، یکی از عواملی است که باعث توجه بیشتر افراد به تهدید امنیتی می گردد.
- کنترل[2]: که با قابل کنترل بودن تهدید، امکان کاهش تاثیرات منفی آن و قابل جبران بودن خسارت های ناشی از تهدید مرتبط است.
- آگاهی[3]: که مرتبط با میزان آگاهی از وجود تهدید امنیتی است[4].

با توجه به عوامل فوق، به نظر می رسد ایران علاوه بر آنکه به دفاع همه جانبه در برابر این جنگ اعلام نشده علیه منافع ملی خود ادامه دهد، باید ابتکاراتی را در زمینه به جریان انداختن جنگ سایبری امریکا و متحدان آن علیه ایران در مجامع حقوقی بین المللی آغاز کند. بنابراین نمی توان از اقدامات سنتی برای پاسبانی امنیت ملی در فضای سایبر سود جست. زیرا به گفته (جانت رنو، دادستان امریکایی)، در فضای سایبر یک هکر نیازی به گذرنامه ندارد، زیرا در هیچ معبری بازرسی نمی شود. (Podgar, 2004: 97). اما در این خصوص چند مسأله وجود دارد که بیشتر، از ماهیت این نوع اقدامات ناشی می شود. واقعیت این است که اگر اقدامات تروریستی تحت شمول ضمانت اجراهای کیفری قرار گیرد باید تعاریف مشخص و دقیقی از آنها که عاری از هرگونه ابهام باشد، درقوانین کیفری انعکاس یابد. اما مجازی بودن این جرم و از سویی فرامرزی بودن فضای سایبری صرف نظر از مسائل دشواری که در حوزه آیین دادرسی به وجود آورده، قانونگذاران را با چالش های جدی رو به رو ساخته است. در واقع، سازمان ملل متحد به عنوان بزرگترین مرجع بین المللی از سال ۱۹۶۳ تاکنون درباره تروریسم سایبری و اقدامات تروریستی، سیزده سند بین المللی به تصویب رسانده است و جالب اینکه تنها در سه سند صراحتا به عنوان

---

[1] Possibility
[2] Controllability
[3] Awareness
[4] www.fa.wikibooks.org/wiki

تروریسم اشاره شده و در بقیه تنها مصادیق اقدامات تروریستی برشمرده شده است. این سه سند عبارتند از: کنوانسیون بین المللی برای جلوگیری از بمب گذاری تروریستی، کنوانسیون بین المللی برای جلوگیری از تامین مالی تروریسم و کنوانسیون بین المللی برای جلوگیری از اقدامات تروریستی هسته ای که متاسفانه ضمانت اجرایی چندانی نداشته و خروجی از آن مشاهده نگردیده است. پس از این موضوع باید به عنوان ابزارهای جانبی و حاشیه ای استفاده کرد. نکته شایان توجه از بعد حقوقی در فضای سایبر این است که چیزی به نام محل وقوع جرم معنا ندارد و نیز میزان قابلیت فنی مجریان قانون در شناسایی و ردیابی آثار مجرمانه الکترونیکی و کشف هویت مجرمان سایبری اهمیتی حیاتی دارد که مهمترین ثمره عملی این مسأله در استناد پذیری ادله الکترونیکی ظاهر می شود. نکته دیگر اینکه با توجه به فرامرزی بودن این جرم کشورها برای جمع آوری داده های به سرعت فناپذیر رایانه ای واقع در دیگر کشورها، تشریفات زمانبری را رعایت کنند که به هیچ وجه با شرایط حاکم بر این فضا سازگار نیست. البته باید به این موضوع توجه داشت که نسبت به این جرم به دلیل آثار و نتایج شدیدی که در پی دارد هر چند قوانین سخت گیرانه ای تصویب شود باز هم امکان بروز دارد، زیرا تعدد بازیگران در فضای سایبر، هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام و ناشناس ماندن بازیگران و عدم قابلیت ردیابی آنها چنین مزیت هایی را ایجاد نموده است، از این رو باید تا حد ممکن برنامه ریزی در محور سیاست های پیشگیریانه از آسیب و اقدامات حقوقی از طریق مراجع و سازمان های بین المللی و تدابیر نظارتی در این خصوص قرار گیرد و انجام اقدامات در جهت آموزش کافی استفاده کنندگان از این تکنولوژی و ارتقای سطح امنیت کامپیوتری، تدوین مقررات کافی و هماهنگ به خصوص از حیث مسئولیت کیفری و مجازات ها، همکاری و تعاون با مجامع بین المللی در زمینه حقوق ماهوی، شکلی و بین المللی و نیز همکاری با مجامع علمی

و دانشگاهی دنیا و تبادل افکار و تجربیات آنها می تواند در کاهش آسیب ها در این حوزه موثر واقع گردد. امیدواریم که دولت ها با تلاش در تحقق این موارد، از این چنین جرایم پیشگیری نمایند. زیرا مسأله اینجاست که نه می توان فناوری اطلاعات و ارتباطات الکترونیکی را کنار گذاشت و به یک جامعه عاری از آن تبدیل شد و نه امکان ریشه کنی هرگونه اقدام تروریستی علیه کشور وجود دارد. لذا تنها راه چاره جویی در جهت کاستن از تهدیدها یا عواقب اقدامات تروریستی سایبری در مفهوم موسع آن است. ذکر این موضوع ضرورت می نماید با توجه به سرعت چرخه تکنولوژی در جهان و لزوم بهره صحیح از این موهبت، ایجاد سیستم های نظارتی و حفاظتی در راستای جلوگیری از انواع شکست های حفاظتی امری اجتناب ناپذیر می نماید حال آنکه در نیروهای مسلح این موضوع دو چندان می باشد و به جرات می توان گفت هرگونه اتفاقی در این بخش جبران ناپذیر می باشد و ایجاد فیلترهای حفاظتی و امنیتی در این بخش کاملاً محرز و آشکار است.

فهرست منابع

- قران کریم.

- چگینی زاده، غلامعلی (۱۳۷۹). رویکردی نظری به مفهوم امنیت ملی در جهان سوم. مجله سیاست خارجی، سال ۱۴، شماره ۱.

- حسن بیگی، ابراهیم (۱۳۸۴). حقوق وامنیت در فضای سایبر، تهران، ابرار معاصر.

- درآنجلیز، جینا (۱۳۸۳). جرایم سایبر، ترجمه سعید حافظی و عبدالصمد خرم آبادی، دبیرخانه شورای عالی اطلاع رسانی.

- سلمانی‌زاده، محمود (۱۳۸۰). جنگ اطلاعات و امنیت، خبرنامه انفورماتیک، سازمان برنامه و بودجه کشور، شماره ۸۰، آذرودی.

- سیف زاده، حسین (۱۳۷۹). جهانی شدن، رهیافت های نظری و رویکرداجرایی نسبت به مسائل امنیتی در داخل، همایش امنیت عمومی و وحدت ملی، تهران، معاونت مطالعات و تحقیقات امنیتی وزارت کشور.

- عبداله خانی، علی (۱۳۸۳). نظریه های امنیت مقدمه ای بر طرح ریزی دکترین امنیت ملی (۱)، تهران: موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، چاپ نخست.

- فلمینگ، پیتر، استول، مایکل (۱۳۸۴). سایبر تروریسم: پندارها و واقعیت ها، ترجمه اسماعیل بقایی هامانه و عباس باقرپور اردکانی، در مجموعه تروریسم، گردآوری علیرضا طیب، نشر نی.

- کالدول، دانیل (۱۳۸۲). رابطه تهدیدها با امنیت در دنیای جهانی شده، ترجمه مسعود آریایی نیا، راهبرد، شماره بیست وهشتم، تابستان.

- ماندل، رابرت (۱۳۷۹). چهره متغیر امنیت ملی، ترجمه پژوهشکده مطالعات راهبردی، تهران.

- مک‌کین‌لای، رابرت، لتیل، ریچارد (۱۳۸۰). امنیت جهانی، ترجمه: اصغر افتخاری، تهران: راهبرد.

- بهشتی پور، حسن (۱۳۹۱). ضرورت اقدام حقوقی علیه حملات سایبری امریکا.

Annamarie, Oliverio, Pat, Lauderdale, (2005), "terrorism as deviance or social control", Sage Publication, London, Thousand Oaks and New Delhi.

Cornis, Paul & Livingstone, David & Clemente، Dave & Yorke, Claire (November 2010) "On Cyber Warfare", A Chatham House Report, www.chathamhouse.org.uk.

Nagre, Dhanashree & Warade, Priyanka,(2008) "Cyber Terrorism Vulnerabilities and Policy Issues "Facts Behind The Myth" http://www.andrew.cmu.edu/user/dnagre.

O'Connor, T, (2009), the criminology of terrorism: theories and models, Retrieved.from: http://faculty.ncwc.edu/toconnor/429/429lect02.htm.

Podgar, Ellen S, (2004), "Cyber crime: transnational or international", Wayne Law Review, vol.50.

Seddon, Embar, (2004), "Cyber terrorism", Edited Alan Oday, Ashgate Publishing Company.

Tosini, Domenico, (2007), Sociology of Terrorism and Counterterrorism: A Social Science Understanding of Terrorist Threat, Journal Compilation, Blackwell Publishing, Ltd.

Walker, cliver, (2006), "cyber terrorism.legal principle and law in the united kingdom", pen state law rev.110.no3.

www.ictna.ir/security/archive/32297

http://fa.wikibooks.org/wiki

http://www.khabaronline.ir/detail/218047/weblog/beheshtipour