فصلنامه مطالعات سیاسی
سال نهم، شماره ۳۴، زمستان ۱۳۹۵
صفحات: ۲۱۲-۱۹۹
تاریخ دریافت: ۱۳۹۵/۷/۱۵ ؛ تاریخ پذیرش نهایی: ۱۳۹۵/۱۰/۱۸

نقش تروریسم سایبری در تهدید علیه امنیت ایران و راه‌های پیشگیری از آن

فاطمه عظیمی*/ هادی خشنودی**

چکیده

تروریسم پدیده جدیدی نیست، تاریخ مشحون از اقدامات شوم تروریستی است که با انگیزه‌های گوناگون ارتکاب یافته و حیات انسان‌های بی‌گناه بی‌شماری را سلب نموده و حقوق، آزادی‌ها و امنیت مردم را به مخاطره افکنده است. امروز اما تروریسم از تهدیدی ملی به یک تهدید بین‌المللی تبدیل شده و خوف آن وجود دارد که با گسترش آن صلح و امنیت بین‌المللی به مخاطره افتد. با ورود به عصر اطلاعات، کیفیت و شرایط جنگ‌ها از پیچیدگی مفهومی و روشی بسیار زیادی برخوردار شده و جنبه‌های نوینی از درگیری در فضای سایبر شکل‌گرفته است. 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 می‌باشد.

کلید واژه‌ها

تروریسم، سایبر، تهدید، پیشگیری.

* عضو هیئت علمی دانشگاه پیام نور زنجان(نویسنده مسوول) Fatemeh.azimi1396@yahoo.com
** دکتری فقه و اصول از حوزه علمیه قم- مدرس حوزه و دانشگاه

مقدمه

تروریسم پدیده جدیدی نیست. تاریخ مشحون از اقدامات تروریستی است؛ اقداماتی که حیات انسان‌های بی‌گناهِ بی‌شماری را سلب نموده، بسیاری از افراد بشر را از حقوق و آزادی‌های اساسی محروم ساخته، روابط دوستانه فی‌مابین دولت‌ها را در معرض خطر قرار داده و تمامیت ارضی و امنیت دولت‌ها را به مخاطره افکنده است.

در عصر جدید، تروریسم از تهدیدی ملی به یک تهدید بین‌المللی مبدل گشته و هراس آن وجود دارد که با گسترش آن صلح و امنیت بین‌المللی به مخاطره افتد. در عصر جهانی‌شدن و تکنولوژی پیشرفته، دیگر تروریسم در مرزهای ملی یا منطقه‌ای محصور نمی‌ماند. تروریست‌ها همگام با روند جهانی‌شدن پیشرفت کرده‌اند اما هرگز در قید و بندهای بین‌المللی ناشی از آن گرفتار نشده‌اند. از آنجا که تروریست‌ها به بازیگرانی بین‌المللی تبدیل شده‌اند، می‌توانند تقریباً هر جا که بخواهند اقدامات تروریستی خود را ساماندهی کرده، به اجرا گذارند، از این‌رو هیچ منطقه، دولت یا ملّتی از اقدامات آن مصون نمی‌ماند.

تروریست‌ها با انگیزه‌های متفاوت ممکن است دست به اقدامات تروریستی بزنند. خطر آنگاه جدی‌تر جلوه می‌کند که امکان دستیابی گروه‌های تروریست و استفادهٔ آنان از سلاح‌های شیمیایی و میکروبی مورد توجه قرار گیرد، چنان که مجمع عمومی سازمان ملل متحد در سال ۱۹۹۵ با صدور قطعنامه‌ای آن را مورد توجه قرار داد. (U.N.G.A/Resolution/50/53, 1995)

اقداماتی در سطح جهانی توسط دولت‌ها و سازمان‌های بین‌المللی برای مقابله با این پدیدهٔ شوم صورت می‌گیرد ولی واکنش حکومت‌ها نسبت به پدیدهٔ نامیمون ترور اغلب ناهماهنگ و متشتت بوده است.

دولت‌ها و سازمان ملل متحد برای مقابله با تروریسم کنوانسیون‌های متعددی تصویب کرده‌اند، اما حق این است که به موازات پیشرفت تروریست‌ها و تبدیل شدن آنان به بازیگران بین‌المللی و فعالیت در قالب سازمان‌ها و مجموعه‌های هماهنگ، جامعه بین‌المللی باید اقدامات ضد تروریستی مؤثری را توسعه دهد که تجلّیات هر چه پیچیده‌تر و جهانی تهدیدهای تروریستی را مورد توجه قرار دهد. به نظر نمی‌رسد اقدامات یک جانبه یا حتی دو جانبه، برای مقابله با تهدیدی که جهانی است کافی باشد. برای محدود ساختن تروریست‌های بین‌المللی، همکاری و هماهنگی بین‌المللی ضروری است. اگر همچون رزالین هیگینز قاضی معروف دیوان

دادگستری بین‌المللی «تروریسم را چالشی برای حقوق بین‌الملل معاصر» (Rosalyn, 1999: 32 Higgins) بدانیم برای مواجهه با آن باید از ابزارهای مختلف بهره‌مند گردیم. در این مقاله ضمن تعریفی از مفهوم تروریسم، تروریسم سایبری، به راه‌های مقابله با این پدیده که ممکن است علیه جمهوری اسلامی ایران به وقوع بپیوندد، می‌پردازیم.

تروریسم

شاید نتوان هیچ تعریفی از تروریسم به دست داد که گونه‌های مختلف این پدیده را که در طول تاریخ تحقق یافته، پوشش دهد. دانشنامهٔ بریتانیکا تروریسم را به «کاربرد سیستماتیک ارعاب یا خشونت پیش‌بینی‌ناپذیر، بر ضد حکومت‌ها و افراد برای دستیابی به یک هدف سیاسی» تعریف می‌کند.(New The Encyclopedia Britannica, 1986: 213) اگر چه مهم‌ترین هدف و انگیزه تروریست‌ها در طول تاریخ هدف سیاسی بوده است، اما به نظر نمی‌رسد بتوان آن را در تعریف لحاظ کرد؛ چه آن‌که امروزه ترور ممکن است با اهداف و انگیزه‌هایی غیرسیاسی ارتکاب یابد، انگیزه‌ها تغییر یافته است. انگیزه‌های ایدئولوژیک یکی از انگیزه‌هاست. پاره‌ای از تروریست‌ها اقدامات تروریستی خود را برای کسب اعتبار و جلب توجه دیگران به آرمان خود نشان می‌دهند. تروریست‌های متأثر از افراط‌گری مذهبی، ممکن است، توجهی به کسب شهرت و قدرت سیاسی نداشته باشند.

شریف بسیونی تعریفی دیگر از تروریسم ارائه نموده است. به اعتقاد وی تروریسم عبارت است از رفتار اجبار آفرین فردی یا جمعی با به کارگیری استراتژی‌های خشونت، آمیخته با ارعاب که در برگیرندهٔ یک عنصر بین‌المللی یا هدف‌گیری شده ضد یک آماج تحت حمایت بین المللی است و هدف آن عبارت است از رسیدن به نتیجه‌ای قدرت طلبانه. (Bassioni, 1975: 45)

از تعریف بسیونی سه عنصر که به ماهیت رفتار، قلمرو اعمال و هدف آن مربوط است به دست می‌آید: رفتار اجبار آفرین و خشونت‌بار، عنصر بین‌المللی و هدفی با انگیزهٔ سیاسی. روشن است که رفتار اجبار آفرین اگر به شکل قانونی انجام پذیرد، مثلاً به قصد مقابله با حرکات خشونت‌آمیز و تروریستی صورت پذیرد عنوان تروریسم را به خود نخواهد گرفت. چنان‌که هدف دستیابی به قدرت سیاسی، باعث می‌شود جرایم سازمان یافته، تروریسم نامیده نشوند.

به رغم آن‌که در جرایم سازمان یافته، مرتکبان، گاه به شکل دهشتناکی مرتکب آدم کشی و رفتارهای خشونت‌بار و اجبار آفرین دیگر می‌شوند و با گسترش شبکه‌های جهانی چنین جرائمی در سطح بین‌المللی به وقوع می‌پیوندند، اما چون ملاحظات مادی انگیزه اصلی این جرایم است و در پشت این ارعاب و رفتارهای اجبار آفرین هدف سیاسی وجود ندارد، آن را به عنوان تروریسم نمی‌شناسیم.

تروریسم سایبری

تروریسم، به کارگیری خشونت علیه اشخاص، دولت‌ها یا گروه‌ها برای پیشبرد زورمندانه‌ی اهداف سیاسی یا عمومی است. سایبر تروریسم نیز در واقع همان تعریف را دارد با این تفاوت که این بار هدف، روی منابع موجود در فضای مجازی متمرکز است. امروزه سایبر تروریسم خطرناک‌تر از تروریسم سنتی است، این امر به دلیل رشد روزافزون ساختار اقتصادی و خدمات رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی می‌باشد. سایبر اقدامات برنامه‌ریزی شده و هدفمند با اغراض سیاسی و غیرشخصی که: «تروریسم را می‌توان این گونه تعریف کرد علیه رایانه‌ها، امکانات و برنامه‌های ذخیره شده در درون آن‌ها از طریق شبکه جهانی صورت می‌گیرد و هدف از چنین بررسی یک مصداق امنیتی از آسیب‌های اینترنتی، سایبر». اقدامی نابودی یا وارد آوردن آسیب‌های جدی به آن‌هاست تروریسم یا تروریسم مجازی است (صدوقی، ۱۳۸۰: ۳۱) واژه سایبر تروریسم نخستین بار از سوی کالین باری در سال ۱۹۸۰ مطرح شد و تعریف جامع‌تری از سوی خانم دوروتی دنینگ، استاد علوم رایانه‌ای دانشگاه جرج تاون ارائه شده است: «سایبر تروریسم بیشتر به معنای حمله یا تهدید علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن‌ها است که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود. در تروریسم کلاسیک، مواد منفجره و سلاح‌های گرم اصلی‌ترین ابزار تروریسم هستند. به گفته کانوی تروریسم سایبری عبارت است از حمله عمدی و آگاهانه با انگیزه‌های سیاسی به وسیله گروه‌های فرو ملی یا عوامل پنهانی علیه اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها که منتهی به خشونت علیه افراد غیرنظامی و سایر اهداف شود.(seddon, 2004: 20)

اما مهم‌ترین ابزار سایبر تروریست‌ها رایانه است. در واقع، آنها ترجیح می‌دهند به جای بمب از بایت استفاده کنند.

ویژگی‌های تروریسم سایبری

تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند. از یک سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌های زیر خلاصه می‌شود:

الف. تعدد بازیگران در فضای سایبری: هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هر کسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت– ملت هستند. (Charney, 2009: 5-6)

ب. هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام: هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در نتیجه، فضای سایبری شرایطی را فراهم کرده که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد. انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است.(Sharp, Lord, 2011: 20)

ج. ناشناس ماندن بازیگران و عدم قابلیت ردیابی: اینترنت به عنوان سیستم نامتمرکز طراحی شده و کاربران آن، غالباً شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند.(Sharp, Lord, 2011: 22)

د. تأثیرگذاری شگرف: ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات، اعتبار، اطلاعات حساس و حتی از دست دادن جان انسان‌ها شود، زیرا در این گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند.(Lord, 22 (Sharp, 2011:

ه. کمرنگ شدن نقش جغرافیا: فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند.(Starr, 2009: 18)

و. ساختار فضای اینترنت: اینترنت، دامنه 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 جدا کردن بازیگران و فعالیت‌های آنها، پاسخ مناسب به از سوی دیگر، ساختار تهدید را بسیار دشوارتر کرده است.(Charney, 2009: 5-6)

ز. پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری: احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. در نتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیر سایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند.(خلیلی‌پور رکن‌آبادی، نورعلی وند، ۱۳۹۱: ۱۷۱)

موانع تهدیدات امنیتی علیه ایران در قبال تروریسم سایبری

هم اکنون در مورد اینکه تأمین امنیت ایران در گرو پیگیری چه نوع اهدافی است، اختلاف نظر وجود دارد. در این زمینه دست کم پنج دیدگاه، سه دیدگاه درون‌گرا و دو دیدگاه برون‌گرا است. هرکدام از این دیدگاه‌ها تأمین و حفظ امنیت ملی را در گرو تعقیب و تحقق یکی از اهداف زیر می‌داند:

نظریه اول توسعه اقتصادی را مهم‌ترین هدف استراتژیک ایران می‌داند. تقابل ادعای توسعه اقتصادی از سوی راست سنتی و مدرن در مقابل توسعه سیاسی اصلاح‌طلبان از سال‌های ۱۳۶۸ به بعد معطوف به این نظر است. استدلال آبادگران نزدیک به راست سنتی وکارگزاران نزدیک به راست مدرن این است که مشکلات اقتصادی می‌تواند موجب نارضایتی مردم شده و با شدت یافتن آن نظام حکومتی با انفجار اقتصادی مواجه خواهد شد.

نظریه دوم تأکید خود را بر توسعه سیاسی و آزادی‌های مدنی گذاشته است. پس از برنامه‌های نوسازی صنعتی راست مدرن در سال‌های ۱۳۶۸ تا ۱۳۷۶، از سال ۱۳۷۶ اصلاح طلبان توسعه سیاسی را مبنای اقدام خود قرار دادند. براین اساس، آزادی‌های سیاسی و فعالیت احزاب و گروه‌ها در عرصه‌های فرهنگی، اجتماعی و سیاسی دارای اهمیت استراتژیک می‌باشد. به نظر این گروه، ایجاد خفقان انسان‌ها را کم مقدار و بیتوان می‌کند و لذا بسیار شدیدتر کشور

را دچار ضعف و التهاب کرده و بدین لحاظ بسیار سریع‌تر از مشکلات اقتصادی، مردم را خواسته یا ناخواسته بر ضد نظام می‌شوراند.

نظریه سوم حفظ ویژگی انقلابی و تجدیدنظرطلبی در نظام بین‌الملل را استراتژیک ترین هدف می‌داند و معتقد است تعدیل در اصول انقلابی باعث از دست رفتن و فروپاشیدن نظام برآمده از انقلاب اسلامی خواهد شد. این گروه، انقلاب و نظام ملی را از یکدیگر جدا و انقلاب را اصل می‌داند و حفظ این اصول انقلاب را به هر قیمتی ضروری می‌انگارد. گروهی از روحانیان سنتی، همراه با بخشی از نهادهای انقلابی- نظامی خواهان این هدف هستند.

سه دیدگاه فوق را می‌توان به نوعی «درون‌گرا» نامید. البته نظریه سوم پیامدهای خارجی فراوانی دارد، در حالی که دو نظریه اول با تأکید بر درون‌گرا می‌توان به‌نوعی تواناسازی درونی می‌تواند محیط بیرونی را در جهت اهداف داخلی بسیج کرده و به کار گیرد. برخلاف سه نظریه فوق، دو نظریه «برون‌گرا» نیز قابل اشاره است که به آنها می‌پردازیم.

نظریه چهارم حول محور مسائل خارجی است که در قالب تعریف سنتی از امنیت قرار می‌گیرد. این نظریه حفظ امنیت جمهوری اسلامی ایران را از لحاظ نظامی، مهم‌ترین مسئله برای نظام می‌داند و مدعی است که برای تأمین آن باید تمام منابع و برنامه‌ها را 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 نظر حمایت می‌کنند.

نظریه پنجم معتقد است که بزرگترین دشمن ایران، آمریکا 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 آمریکا درگیر شد. آشکار است که این نظریه نیز در چارچوب تعریف سنتی از امنیت می‌گنجد ولی نسبت به نظریه چهارم دایره محدودتری را نمایان می‌سازد. برخی از انقلابیون نظامی گرا و خواهانِ مبارزه پیگیر از این نظر پیروی می‌کنند.

با عنایت به دیدگاه‌های فوق نکته‌ای که مغفول مانده است این است که اکنون در فضایی قرار داریم که ابزارها و به تبع آن شاهد تغییر نوع نگاه به امنیت در دنیای جدید می‌باشیم. بنابراین به نظر می‌رسد که علی‌رغم تهدیدهای فوق، امنیت ملی و جانی انسان‌ها در خطر می‌باشد. از منظر امنیت ملی می‌توان گفت که در شرایط حاضر، دولت‌ها و ملت‌ها با زنجیره‌ای

از تهدیدات نامشخص در محیط‌های مجازی مواجهند که امنیت آنها را به چالش کشیده و ابزارهای سنتی تأمین کننده امنیت ملی دیگر توان مقابله با آنها را ندارند.(حسن بیگی، ۱۳۸۴: ۲۷۸)

بنابراین، باید گفت این یکی از نکات طنزآلود عصر کنونی است که صنعتی که برای حصول امنیت ملی طراحی شده است هم اینک ابزاری شده است که می‌تواند تهدیدآفرین شود. برای نمونه، همان‌گونه که فریدمن خاطرنشان می‌سازد: «ویروس رایانه‌ای lovebug در سال گذشته که توسط دو فیلیپینی ناراضی در اینترنت ریخته شد، ظرف ۲۴ ساعت ۱۰ میلیون رایانه را خراب و ۱۰ میلیارد 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 جهانی‌شدن کنونی است. این حادثه نشان دهندهٔ آسیب‌پذیری پرخطر ماست.(کالدول، ۱۳۸۲: ۳۴۱) بنابراین، جهانی‌شدن با شکل جدیدی که محیط امنیتی، بازیگران و قواعد بازی امنیت خارجی داده است، سرمنشأ تهدیدهای کاملاً جدیدی برای ایران است که تا دههٔ پیش وجود نداشته‌اند. مفهوم کلیدی در این رابطه، تهدید در فضای الکترونیکی و مجازی است که با جنگ‌های کلاسیک کاملاً متفاوت می‌باشند. برای نمونه می‌توان به هجوم شدید کرم به رایانه‌ای «استاکس نت» ایران اشاره نمود که علاوه بر اطلاعات سیستم‌های کنترل صنعتی و نیروگاهی و رایانه‌ای تأسیسات هسته‌ای، اطلاعات سیستم‌های خانگی را نیز به سرقت برد و حدود ۶۰ درصد رایانه‌های ایرانی را آلوده ساخت. تحقیقات نشان داد که این کرم برای این منظور طراحی شده که سانتریفیوژهای ویژه غنی‌سازی اورانیوم را مختل کند. پیچیدگی کرم نرم‌افزاری «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 نرم‌افزار مخرب را نوشته و فعال کردند که 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 اولین ویروس رایانه‌ای 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 استاکس نت را علیه ایران صادرکرده است. این عملیات در واقع نخستین حمله سایبری پایدار آمریکا علیه یک کشور دیگر است که با استفاده از کدهای

مخربی که با همکاری اسرائیل طراحی شده، انجام گرفته است. درست مانند عملیات کودتای ۲۸ مرداد ۱۳۳۲ که سازمان سیا برای اولین بار در یک تجربه برون‌مرزی دولت قانونی مصدق را سرنگون کرد و حکومت وابسته محمدرضا شاه را بار دیگر به مردم ایران تحمیل نمود.(بهشتی پور، ۱۳۹۱) آمریکایی‌ها همچنین ویروس سارق اطلاعات به نام «دوکو» را برای سرقت اطلاعات از زیرساخت‌های 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)

از این‌رو می‌توان گفت ساختار اینترنت اساساً، چالش‌های امنیتی برای دولت‌ها به وجود می‌آورد. اینترنت به‌عنوان یک سیستم نامتمرکز طراحی شده و کاربران آن غالباً شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حملات سایبری باقی نماند. این چالش باعث قدرتمندتر شدن بازیگران قوی و ضعیف می‌شود؛ چرا که ناشناخته بودن یک مزیت برای آن‌ها به حساب می‌آید. بنابراین، درحالی که تداوم این نوآوری فرصت‌های بیشتری برای استفاده مؤثر از اینترنت ارائه می‌کند، برخی نیز از همین مزیت برای حملات سایبری استفاده می‌کنند. امنیت سایبری، زمان‌بر و پرهزینه است و شرکت‌های رایانه‌ای برای عرضه سریع‌تر نوآوری‌های خود تحت فشار قرار دارند و همین امر باعث می‌شود فناوری‌هایی وارد بازار شوند که از امنیت کمتری برخوردار هستند. همین نکته، تهدیدات سایبری را از تهدیدات سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند و بازیگران آن را دولت-ملت هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است که امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید.

راه‌های پیشگیری از تروریسم سایبری

کارگزاری‌های انسانی، که آنها را تروریست‌های متخصص می‌خوانیم، و اندیشه آن در شکل دادن به «دانش سایبری مهاجم» بوده، نتایج و عواقب زیانباری را به دنبال داشته است. می‌دانیم که، آنچه انسان و دانش بشری را به سطح امروزی آن رسانده، چیزی جز آموزش نبوده است. در خصوص تهدیدهای سایبری، مراجع ذی‌صلاح تقریب از همان ابتدا به دنبال راهکارهایی از جنس آموزش بودند؛ حقوقدانان پیشگیری از وقوع جرم را بر ضمانت‌های اجرایی در برابر آن مقدم می‌دانند. با توجه به اهدافی که تروریست‌ها دنبال می‌کنند، در خصوص

بسیاری از آنها به هیچ وجه انواع ضمانت اجراهای سنگین کیفری، حتی اعدام، تأثیرگذار نیست و حتی می‌تواند موجب تشجیع و تحریک همراهانشان گردد. لذا با توجه به شرایط خاص حاکم بر این پدیدهٔ مجرمانه، اولین گزینهٔ کاملاً عاقلانه و منطقی، اتخاذ تدابیر پیشگیرانه از وقوع تروریسم است؛ هرچند اهمیت این مسئله نباید جایگاه ضمانت اجراهای کیفری را تحت‌الشعاع قرار دهد.(جلالی فراهانی، ۱۳۸۵: ۱۰)

در ارتباط با اقدامات پیشگیرانه علیه تروریسم سایبری، سه رکن اصلی این پدیدهٔ مجرمانه تروریست‌های متخصص، قربانیان اقدامات تروریست‌های متخصص و فضای سایبری، به عنوان بستر ارتکاب اقدامات تروریستی است. پیشگیری در فضای سایبری با عنایت به ارکان مذکور، الگوهایی دارد که از میان آنها، به ویژه طی نیم قرن اخیر، «پیشگیری وضعی» و «پیشگیری اجتماعی» به‌عنوان جامع‌ترین راهکارهای موفقیت‌آمیز از جرم مورد توجه قرار گرفته‌اند.(نجفی ابرندآبادی، ۱۳۸۰: ۷۴۸)

در عرصه بین‌المللی نیز، پیشگیری در وقوع جرائم مهمی نظیر جنایات سازمان یافته فراملی و فساد نیز به ترتیب در کنوانسیون‌های پالرمو و مریدای سازمان ملل متحد بر آنها تأکید شده است.

به طور خلاصه، در پیشگیری اجتماعی، هدف، از بین بردن «انگیزهٔ مجرمانه» است و به همین دلیل، به آن «پیشگیری بزهکار محور» گفته می‌شود. در اینجا راهکارهای اجتماعی، مانند رفع بیکاری و فقر که زمینه‌ساز شکل‌گیری انگیزه‌های مجرمانهٔ مالی و حتی قتل می‌شوند و همچنین «راهکارهای تربیتی و آموزشی» برای کودکان، به‌عنوان آسیب‌پذیرترین گروه سنی، هم از لحاظ بزهکاری و هم از لحاظ بزه دیدگی، در دستور کار قرار می‌گیرند.(نیازپور، ۱۳۸۲: ۱۳۸)

اما در پیشگیری وضعی، هدف، صیانت از بزه دیدگی بالقوه از طریق سلب «فرصت» و یا «ابزار» ارتکاب جرم است.(Shinder, 2002: 353) بسیاری از تدابیر امنیتی که در ساختمان‌ها، اتومبیل‌ها و نظایر آن به اجرا در می‌آید یا اینکه از خرید و فروش انواع سلاح‌های گرم و سرد جلوگیری می‌شود، در واقع پیشگیری وضعی از وقوع جرائم است.

با توجه به این توضیحات اجمالی، به نظر می‌رسد نحوهٔ پیاده‌سازی تدابیر پیشگیرانهٔ اجتماعی و وضعی در فضای سایبر روش نشده باشد. اگر واقعیات و شرایط خاص حاکم بر این فضا به خوبی به کاربران آن، که عمدتاً قشر جوان و نوجوان جامعه هستند، منعکس شود، از

شکل‌گیری و تحقق بسیاری از انگیزه‌های مجرمانه و درعین حال بزه دیدگی آنها پیشگیری خواهد شد. هم اکنون این مسئله تا حدی مورد توجه قرارگرفته که مباحث تخصصی از سوی صاحب‌نظران و سیاست‌گذاران این حوزه تحت عنوان «اخلاق سایبری» مطرح شده است. (جلالی فراهانی، ۱۳۸۵: ۶۵)

با این حال، ازآنجا که این فضا ماهیتی فنی دارد، دست اندرکاران بیشتر به دنبال اجرای «تدابیر پیشگیرانهٔ وضعی فنی» هستند که از نمونه‌های بارز آن می‌توان به انواع «فیلترها» و «تدابیر نظارتی» اشاره کرد که البته ناکارایی‌های این گونه ابزارها بر همگان محرز شده، اما به کارگیری آنها اجتناب‌ناپذیر است.(جلالی فراهانی، ۱۳۸۴: ۱۳۳) اما در خصوص کارآیی این تدابیر در مورد اقدامات تروریستی سایبری، روشن است که تدابیر پیشگیرانهٔ اجتماعی ماهیت تروریسم را هدف قرار می‌دهند و در این جهت می‌توانند از فضای سایبر به عنوان یک ابزار اطلاع‌رسانی و تبلیغاتی نیز استفاده کنند و البته تأکید ویژه‌ای بر این اقدامات در فضای سایبر داشته باشند. تدابیر پیشگیرانهٔ وضعی نیز عمدتاً بدون توجه به هویت مجرمان به کار می‌روند. برای مثال، هدف، پیشگیری از آلوده نشدن سیستم‌ها به انواع ویروس‌ها یا محتواهای مستهجن است و تفاوتی نمی‌کند مرتکب آنچه کسی است. البته برای برخی سیستم‌ها که در زیرساخت های حیاتی مستقر هستند و عمدتاً مجرمانی نظیر تروریست‌ها قصد تعرض به آنها را دارند، می‌بایست برنامه‌ریزی‌هایی ویژه صورت گیرد. همچنین برای اینکه از دسترس کاربران به محتواهای ارسالی از سوی تروریست‌ها جلوگیری شود، مانند انواع پیام‌های تحریک کننده و مخل آسایش عمومی، می‌بایست «فهرست‌های سیاه یا سفید» فیلترها به نحوی تنظیم شود که تمامی حوزه‌های مربوط را شناسایی و دسترس‌ناپذیر کنند.(جلالی فراهانی، ۱۳۸۵: ۱۰)

نتیجه‌گیری

با گسترش انقلاب‌های تکنولوژیک و اطلاعاتی و پیچیده‌تر شدن مناسبات اقتصادی و تولیدی در عصر جهانی شدن، از یک سو مفهوم قلمروزدایی مطرح شده است و از سوی دیگر تغییر ماهیت تهدیدهای امنیت و مفهوم مرز و حراست از آن را به مسئله‌ای 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 یک نتیجه‌گیری کلی می‌توان گفت هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب شده 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 و ... را به وجود آورند. جمهوری اسلامی ایران نیز به دلیل آنکه محیط امنیتی آن بیش از آنکه دارای فرصت باشد، تهدیدهای بی‌شماری را دربر دارد 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 می‌باشد و لزوم برنامه‌ریزی و مقابله با این مسئله به عنوان یکی از مهم‌ترین تهدیدها و آسیب‌ها با توجه به اقدامات تخریبی علیه آن نظیر «استاکس نت» و ... ناگزیر می‌نماید. لذا با اتخاذ یک روش و برنامه‌ریزی مناسب می‌توان این روند را معکوس نمود و مهم‌ترین کار ویژه امنیتی یک نظام، یعنی تبدیل تهدیدها به فرصت‌ها را صورت داد.

فهرست منابع

الف) منابع فارسی

احمری، حسین، کحلکی غلامرضا، رحیم پور اصفهانی، حامد (۱۳۹۵). «تحلیل سازه انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن»، **فصلنامه پژوهش های روابط بین الملل**، شماره ۱۹، صص ۳۳۳-۳۰۵.

بهشتی پور، حسن، «ضرورت اقدام حقوقی علیه حملات سایبری آمریکا» در http://www.khabaronline.ir/detail/218047/weblog/beheshtipour.

جلالی فراهانی، امیرحسین (۱۳۸۴). «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، فصلنامه تخصصی فقه و حقوق، شماره ۶، صص ۱۶۲-۱۳۳.

جلالی فراهانی، امیرحسین (۱۳۸۵). «تروریسم سایبری»، **فصلنامه تخصصی فقه و حقوق**، شماره ۱۰، صص ۱۱۲-۸۵.

جلالی فراهانی، امیرحسین (۱۳۸۵). **پیشگیری اجتماعی از جرایم سایبری راهکاری اصولی برای نهادینه سازی اخلاق سایبری**، تهران: انتشارات مرکز تحقیقات مخابرات.

حسن بیگی، ابراهیم (۱۳۸۴). **حقوق وامنیت در فضای سایبر**، تهران: موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر.

خلیلی پور رکن آبادی، علی، نورعلی وند، یاسر (۱۳۹۱). «تهدیدات سایبری و تاثیر آن بر امنیت ملی»، **فصلنامه مطالعات راهبردی**، سال پانزدهم، شماره دوم، شماره مسلسل ۵۶.

کالدول، دانیل (۱۳۸۲). «رابطه تهدیدها با امنیت در دنیای جهانی شده»، ترجمه مسعود آریایی نیا، **فصلنامه راهبرد**، شماره ۲۸، صص ۱۹۶-۱۶۷.

مرادعلی، صدوقی (۱۳۸۰). **فناوری های اطلاعاتی و حاکمیت ملی**، تهران: دفتر مطالعات سیاسی و بین المللی.

مک کین لای، رابرت، لتیل، ریچارد (۱۳۸۰). **امنیت جهانی**، ترجمه اصغر افتخاری، تهران: نشر راهبرد.

نجفی ابرندآبادی، علی حسین (۱۳۸۰). **تقریریات درس جرم شناسی**، تهران: دوره دکتری دانشگاه تربیت مدرس.

نیازپور، امیرحسن (۱۳۸۴). «پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم»، **مجله حقوقی دادگستری**، شماره ۴۵، صص ۱۵۹-۱۲۴.

ب) منابع انگلیسی

Charney, Scott (2009). "Rethinking the Cyber Threat A Framework and Path Forward", Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA.

Lord, Kristin M. & Sharp, Travis (2011). "America's Cyber future Security and Prosperity in the Information Age", Center for a New American Security, Volume I.

Rosalyn Higgins and M (1999). Flory; Terrorism and International Law, London and New York, Routledge.

Seddon, Embar (2004). "Cyber terrorism", Edited Alan Oday, Ash gate Publishing company.

Shinder, D (2002). Scene of the cyber forensics Hand book. Syngress publication.

Starr, Stuart H (2009). "Towards an Evolving Theory of Cyber power", National Defense University, Center for Technology and National Security Policy.

The New Encyclopedia Britannica (1986). vole 11, Micropaedia.