پیشگیری از تأثیر فضای مجازی بر گسترش تروریسم سایبری

نگین برخورداری احمدی[1]، علیرضا سایبانی[2]

چکیده

در حال حاضر تروریسم در فضای مجازی به یکی از چالش‌های عمده نظام‌های حقوقی به خصوص نظام کیفری تبدیل شده است. تروریسم سایبری، با وجود نوظهور بودن خطرناک‌تر از تروریسم سنتی و کلاسیک است و تهدیدات آن برای امنیت ملی دولت‌ها به خطری بالقوه تبدیل شده است، این مقاله به روش تحلیلی- توصیفی به دنبال شفاف‌سازی هرچه بیشتر تاثیر فضای مجازی بر تروریسم و تبیین ویژگی‌های سایبر تروریسم بوده است. نتایج تحقیق نشان می‌دهد که باتوجه به قابلیت فضای سایبر، انجام جرائم تروریستی و تحقق اهداف حامیان تروریسم از حالت فیزیکی خارج گشته و جنبه سایبری به خود گرفته است که آسان‌تر، کم‌هزینه‌تر و مخفیانه‌تر است و مهمترین بهره‌گیری تروریست‌ها از شبکه جهانی ارتباطات، بین‌المللی کردن فعالیت‌های‌شان است. در این میان آنچه در وهله اول ضروری به نظر می‌رسد، پیشگیری از وقوع تروریسم سایبری به منظور حمایت از بزه دیدگان آن است.

واژگان کلیدی: پیشگیری از جرم، فضای مجازی، تروریسم

[1] دانشجوی دکتری حقوق جزاء و جرم‌شناسی، دانشگاه آزاد اسلامی، واحد بندرعباس N.barkhordari1996@gmail.com

[2] عضو هیات علمی گروه حقوق، استادیار دانشگاه آزاد اسلامی، واحد بندرعباس

مقدمه

همگام با توسعه روزافزون جوامع و گسترش امکانات برای بهبود زندگی اجتماعی، شاهد تغییر شیوه ارتکاب جرایم گوناگون در نظام اجتماعی هستیم. به این ترتیب مجرمان بالقوه به موازات با پیشرفت تکنولوژی، جرایم خود را براساس امکانات خلق شده، به روز می‌کنند. به این ترتیب از جمله جرایمی که بر این مبنا مطرح شده است، جرم تروریسم با توسل به فضای مجازی است. این دسته از عملیات تروریستی به صورت آسان‌تری نسبت به اعمال تروریستی سنتی واقع می‌شوند. از سوی دیگر به تجربه در چند سال اخیر مشاهده شده که این گروه از عملیات تروریستی خسارات بسیار شدیدتری را بر کشورها تحمیل کرده است. بطوریکه قانونگذاران در کشورهای مختلف کم و بیش به وضع مقرراتی در این زمینه پرداخته‌اند.

در واقع امروزه تکنولوژی اطلاعات، صرف‌نظر از موقعیت جغرافیایی در تمام شئون زندگی وارد شده است، لیکن این رشد علیرغم مزایای خود جنبه‌های منفی هم در بر داشته است. بدین مفهوم که امکان رفتارهای ضداجتماعی و مجرمانه را به وجود آورده که پیش از این به هیچ وجه امکانپذیر نبوده است و با روند رو به رشد این جرایم روبرو هستیم. زیرا جرایم رایانه‌ای به دلیل ویژگی‌هایی که دارند، نسبت به سایر روش‌ها ارتکاب جرایم مرجح می‌باشند. اول آنکه، شیوه ارتکاب آنها آسان است، با مبالغ اندک، خسارات هنگفتی می‌توانند وارد نمایند، می‌توان بدون حضور فیزیکی در یک حوزه فضایی معین در آن حوزه مرتکب اینگونه جرایم شد، دست آخر اینکه در اغلب موارد غیرقانونی بودن آنها روشن نمی‌باشد. از سوی دیگر با پیشرفت تکنولوژی رایانه، راه‌های ارتکاب جرم فنی‌تر و تخصصی‌تر شده و راه‌های مقابله با آن نیز دشوارتر می‌نماید. یکی از ویژگی‌های فناوری اطلاعات به ویژه اینترنت امکان ساماندهی و تدارک تهاجم سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده می‌باشد و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود، با ایجاد ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تأخیر در آنها می‌گردد. در دنیای امروز دیده می‌شود که برخی اقدامات تروریستی توسط دسترسی به اطلاعات حفاظت شده صورت می‌پذیرد. تروریست‌های اطلاعاتی می‌توانند به صورت غیرمجاز وارد سیستم‌های رایانه‌های امنیتی شوند، مثلاً با تداخل در سیستم ناوبری هوایی باعث سقوط هواپیما شوند و بطورکلی آسیب‌های امنیتی جدی ایجاد می‌کنند که می‌تواند منجر به ایجاد بحران‌های نوع حاد گردد.

بنابراین، امروزه اهمیت درک چنین فضایی در ارتباط با مفهوم امنیت ملی، از مهمترین 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 می‌توانند منشأ تهدیدات تلقی شوند. به عبارت دیگر از تلاقی اعمال تروریستی و فضای سایبر گونه‌ای نوپا از اعمال تروریستی تحت عنوان تروریسم سایبری پا به عرصه

وجود نهاده است. تروریسم در فضای سایبر، فرایندی است که در بر گیرنده اعمال یا تهدیدها، واکنش‌های عاطفی و آثار اجتماعی این اعمال یا تهدیدها و اقدامات ناشی از آنهاست. تروریسم در بستر فضای سایبر شامل کلیه عناصر بالا در یک محیط تکنولوژی بسیار متحول است که بر فرصت‌ها و منابع تروریستی تأثیر می‌گذارد. این تأثیرات، بطور مستقیم بر تاکتیک‌ها، هدف‌ها و سلاح‌های مورد استفاده تروریست‌ها اثر گذاشته و باعث بالا رفتن بحث درباره، نوعی تاکتیک تروریستی تازه به نام «تروریسم سایبری» شده است (چاووشی، ۱۳۸۷).

امکان ارتکاب جرم برای شهروندان اینترنت بسیار بیشتر از شهروندان دنیای واقعی است. در واقع «شناسایی جامع مخاطرات محتمل از ناحیه جرائم سایبری در ابعاد مختلف زندگی اجتماعی، پیش‌شرط قانونگذاری خوب و اجرای موفق قانون در این زمینه است» (جوان جعفری، ۱۳۸۵).

لذا به نظر می‌رسد جهت آشکار نمودن ضعف حمایتی زیرساخت‌های حیاتی و بنیادین جوامع، نشان دادن فقدان سیاست تقنینی و حمایت‌های لازم و عدم ارائه راهکارهای موثر در مقابل پدیده مجرمانه سایبر-تروریسم و همچنین توصیف پدیده تروریسم سایبری و نشان دادن آسیب‌پذیری جوامع در برابر پدیده مذکور، ضرورت بررسی و داشتن نگاه جرم‌شناسانه به این فضا امری اجتناب‌ناپذیر می‌باشد. با این وصف در این نوشتار سعی بر آن خواهد بود تا به راهکارهای پیشگیرانه از تاثیر فضای سایبری در گسترش تروریسم پرداخته شود.

۱- مفهوم و ماهیت تروریسم

کلمه «ارهاب» یا تروریسم، به معنی «ترس و ترساندن» است. مصدر آن «رهب» است. در فرهنگ لغات، وجه مشترک بین این کلمه و اکثر مشتقات کلمه «رهب»، به معنی ترس و ترساندن است. در زبان انگلیسی، اصل کلمه Terreur به فعل لاتینی Ters برمی‌گردد، و به معنی «ترساندن» یا «ترس و وحشت» است که بیشتر مشتقات آن حول همین معانی مشخص می‌چرخند. کلمه تروریسم در زبان فرانسه برای اولین بار در حوزه سیاسی بکار رفت. اگر به آن مراجعه کنیم، درمی‌یابیم که کلمه Terrour یا Terrorisme همان معانی گذشته را در بردارد. در لغت‌نامه دهخدا، تروریسم به معنای اصول حکومت وحشت و فشار (اصول حکومتی که در فرانسه حد فاصل سال‌های ۱۷۹۳ و ۱۷۹۴ حاکم بود) آمده است (مرادی، ۱۳۸۹).

در کتاب فرهنگ علوم سیاسی آمده است: «ترور، در لغت، در زبان فرانسه، به معنای هراس و هراس‌افکنی است و در سیاست به کارهای خشونت‌آمیز و غیرقانونی حکومت‌ها برای سرکوبی مخالفان خود و ترساندن آنها ترور می‌گویند و نیز کردار گروه‌های مبارزی که برای رسیدن به هدف‌های سیاسی خود، دست به کارهای خشونت‌آمیز و هراس‌انگیز می‌زنند، ترور نامیده می‌شود. همچنین ترور به معنای کشتار سیاسی نیز بکار

می‌رود. فرهنگ جامع سیاسی نیز بیان می‌کند که «ترور، به معنای ترس و وحشت است و در اصطلاح عام بیشتر به قتل‌های سیاسی گفته می‌شود که البته معنای واقعی این واژه نیست. همچنین آلن بیرو در فرهنگ علوم اجتماعی، ترور را به معنای حالت و یا احساس ترس دسته‌جمعی می‌داند که خشونت و کشتار بی‌حساب موجد آن است (آشوری، ۱۳۸۲).

«در زبان فارسی این کلمه به اصلی اطلاق می‌شود که در آن از قتل‌های سیاسی و ترور دفاع شود. در دیگر فرهنگ‌های فارسی نیز تروریسم به معنی لزوم آدم‌کشی و تهدید و خوف و وحشت در میان مردم، برای نیل به هدف‌های سیاسی؛ و یا برانداختن حکومت و در دست گرفتن زمام امور دولت، یا تفویض آن به دسته‌ی دیگری است که موردنظر می‌باشد. این عقیده معمولاً از ابزار اصلی فاشیسم، ماکیاولیسم و مکاتب مشابه می‌باشد».

به این ترتیب، پیش از هر چیز باید اقدامات تروریستی و عوامل آن بطور صحیح شناسایی شوند. این مسئله مستلزم شناسایی ابعاد گوناگون آن است. برای مثال، سازمان ملل متحد، بعنوان بزرگترین مرجع بین‌المللی، از سال ۱۹۶۳ تاکنون، درباره تروریسم و اقدامات تروریستی سیزده سند بین‌المللی به تصویب رسانده است و جالب اینکه تنها در سه سند صراحتاً بعنوان تروریسم اشاره شده و در بقیه تنها مصادیق اقدامات تروریستی برشمرده شده است. این سه سند عبارتند از: کنوانسیون بین‌المللی برای جلوگیری از بمب‌گذاری تروریستی (۱۹۹۷)[1]، کنوانسیون بین‌المللی برای جلوگیری از تأمین مالی تروریسم (۱۹۹۹)[2]، و کنوانسیون بین‌المللی برای جلوگیری از اقدامات تروریستی هسته‌ای (۲۰۰۵)[3] (حکیمی‌ها، ۱۳۸۵).

البته این سازمان در سال ۱۹۹۲ در یک تعریف غیررسمی که با استقبال گسترده دانشگاهیان نیز مواجه شد، چنین مقرر داشته است: «یک شیوه مشتاقانه-رغبت‌انگیز در ارتکاب خشونت مکرر توسط افراد، گروه‌ها یا دولت‌ها به صورت (نیمه) مجرمانه در جهت نگرش فکری خاص، مجرمانه یا سیاسی. در اینجا قربانیان اصلی خشونت، در مقایسه با آدم‌کشی، آماج اصلی محسوب نمی‌شوند».

بطورکلی، عناصر مشترک تشکیل دهنده تروریسم عبارتند از:

۱) سیاسی؛ ۲) روانشناختی؛ ۳) خشونت‌آمیز؛ ۴) پویا؛ ۵) مدبرانه؛ ۶) رسانه‌ای بودن.

۱) سیاسی: یک اقدام تروریستی، اقدامی سیاسی نیز محسوب می‌شود یا به منظور تأثیرگذاری سیاسی ارتکاب می‌یابد. کلوزویتز[4] به خوبی در اینباره اظهار داشته: «جنگ دنباله سیاست با ابزاری دیگر است».

---

[1] International Convention for the Suppression of Terrorist Bombing
[2] International Convention for the Suppression of the Financing of Terrorism
[3] International Convention for The Suppression of Acts of Nuclear Terrorism
[4] Clausewitz

۲) روانشناختی: نتایج پیش‌بینی شده اقدامات تروریستی، تأثیر روانشناختی به دنبال دارد. تروریست‌ها مخاطبان و نه قربانیان واقعی‌شان را هدف قرار می‌دهند. ممکن است مخاطب این اقدامات، همه مردم، بخش خاصی از جامعه (مانند اقلیت‌های قومی) یا نخبگان تصمیم‌ساز در جامعه سیاسی، اجتماعی یا نظامی باشند.
۳) خشونت‌آمیز: هدف از قهر و غلبه و تخریب، تاثیرگذاری است. حتی اگر نتایج یا خسارات به بار آمده نتیجه عملیات تروریست‌ها نباشد، تهدید یا خشونت بالقوه ایجاد شده تأثیر خود را خواهد گذاشت.
۴) **پویا:** گروه‌های تروریستی به تغییر و تحول و تحرکات سیاسی نیازمندند. اما از آنجا که دیدگاه‌های انتقادی شدیدی دارند، همواره سرسختانه‌ترین مواضع را اتخاذ می‌کنند.
۵) مدبرانه: تروریسم یک اقدام از پیش طراحی شده و هدفمند برای تحقق اهداف مشخص است، بطور منطقی بکار گرفته می‌شود و از تاکتیک‌های گزینشی خاصی برخوردار است و به هیچ وجه نمی‌توان آن را تصادفی دانست. برخورداری از امکانات و پشتیبانی‌های مستمر قدرتمند، این امکان را به تروریست‌ها می‌دهد تا یک برنامه‌ریزی حتی طولانی مدت برای خود داشته باشند.
۶) رسانه‌ای بودن: تروریست‌ها در جهت اهدافی که دنبال می‌کنند، عمداً بنحوی مرتکب اقدامات تروریستی می‌شوند یا تهدید به ارتکاب آنها می‌کنند که سریعاً در میان جامعه موردنظرشان انعکاس خبری داشته باشد و تأثیر دل‌خواهشان را بر مخاطبان بگذارد. مهم نیست چه کسی قربانی می‌شود یا چه میزان خسارات وارد می‌آید، بلکه میزان تأثیرپذیری مخاطبان از آنها حائز اهمیت است. لذا رسانه‌ها (خصوصاً فضای مجازی) ابزار قدرتمند و موثری برای تروریست‌ها محسوب می‌شوند (U.S. Army TRADOC,2004: 1-4).

۲- پیشگیری از وقوع تروریسم سایبری

برای اینکه اقدامات پیشگیرانه بطور سنجیده و صحیح به اجرا در آیند، لازم است سه رکن اصلی این پدیده مجرمانه براساس رهیافت‌های جرم‌شناختی مطالعه و بررسی و مطابق نتایج به دست آمده، راهکارهای پیشگیرانه مورد نیاز تدوین و اجرا گردند. این سه رکن عبارتند از:
۱) تروریست‌های سایبری؛ ۲) قربانیان اقدامات تروریستی سایبری؛ و ۳) فضای سایبر بعنوان بستر ارتکاب اقدامات تروریستی.

اما از میان الگوهای مختلف پیشگیری که به ویژه طی نیم قرن اخیر مورد نظریه‌پردازی و آزمون قرار گرفته‌اند، پیشگیری وضعی[1] و اجتماعی[2]، بعنوان جامع‌ترین راهکارهای موفقیت‌آمیز پیشگیری از جرم مورد توجه قرار گرفته است. کما اینکه برای پیشگیری از جرائم مهمی نظیر جنایات سازمان یافته فراملی و فساد اتخاذ و به ترتیب در کنوانسیون‌های پالرمو[3] و مریدای[4] سازمان ملل متحد بر آنها تأکید ویژه‌ای شده است.

۲-۱- پیشگیری وضعی از تروریسم سایبری

یکی از راهکارهای مهم برای پیشگیری از بزه دیدگی ناشی از تروریسم سایبری، پیشگیری وضعی است. این نوع پیشگیری در سال ۱۹۸۰، توسط «کرینش»، «می‌هیو» و«کلارک» در کشور انگلستان مطرح و توسعه یافته است. در تعریف پیشگیری وضعی آمده است: «کلارک پیشگیری وضعی از جرم را بعنوان اقدامات قابل سنجش و ارزیابی مقابله با جرم می‌داند. این اقدامات معطوف به اشکال خاصی از جرم بوده و از طریق اعمال مدیر، یا مداخله در محیط بلا واسطه به شیوه‌های پایدار و سیستماتیک منجر به کاهش فرصت‌های جرم و افزایش خطرات جرم که همواره مدنظر تعداد زیادی از مجرمین بوده است، می‌گردد».

این پیشگیری به وسیله دستکاری و تغییر موقعیت و محیط در فرآیند وقوع جرم به کاهش فرصت‌های ارتکاب جرم کمک می‌کند. از میان روش‌های مختلف پیشگیری از جرم، پیشگیری وضعی بهترین راهکارها را برای کاهش فرصت‌های ارتکاب جرم در جرایم سایبر و به تبع آن تروریسم سایبر پیشنهاد می‌کند. بنابراین به منظور کاهش فرصت‌های جرم، می‌توان از تقسیم‌بندی بیست و پنجگانه کلارک استفاده نمود. در این راستا راهکارهای پیشنهاد شده، در پنج گروه عمده جای می‌گیرند و به برخی از آنها که درباره موضوع مورد بحث در ارتباط هستند می‌پردازیم (نجفی ابرندآبادی، ۱۳۹۲):

۲-۱-۱- افزایش زحمات ارتکاب جرم

این رویکرد از پیشگیری وضعی سعی دارد با مشکل و سخت جلوه دادن آماج‌های جرم، بزهکاران بالقوه را از ارتکاب انواع بزه‌های مرتبط با تروریسم سایبری منصرف نماید و با قرار دادن موانعی در سر راه بزهکاران بالقوه، به خصوص در محاسبه عقلانی، مزایای قابل پیش‌بینی از ارتکاب جرم را کمتر نشان داده و با استفاده از تکنیک‌های افزایش زحمات ارتکاب جرم باز دارد.

[1] Situational Prevention
[2] Social Prevention
[3] United States Convention Against Corruption (2000)
[4] United States Convention Against Transnational Organized Crime (2003)

۱) فنون سخت‌تر کردن هدف: در این تکنیک سعی می‌شود، با بکارگیری راهکارهای متفاوت در زمینه تقویت آماج‌های بالقوه جرم، بزهکاران مذکور را در هدف‌گیری و انتخاب آنها به منظور دسترس غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم، و سوء استفاده از دستگاه‌ها بعنوان بستر جرم ممانعت شود.

۲) فنون محدود کننده دسترسی: در این تکنیک‌ها سعی می‌شود از دسترسی نفوذگرهای تروریستی به منابع شبکه، تأسیسات مختلف مبتنی بر فناوری‌های اطلاعاتی جلوگیری نمود. از جمله راهکارهای عملی عبارت‌اند از: (جلوگیری از ورود یا ارسال برخی داده‌های غیرمجاز یا غیرقانونی از طریق نصب سیستم‌ها و برنامه‌های خاص بر روی گره‌های دسترسی به شبکه که شامل رایانه‌های شخصی، مسیریاب‌ها[1]، سیستم‌های ارائه دهنده خدمات شبکه‌ای و ایجاد کنندگان نقطه تماس بین‌المللی) (جلالی فراهانی، ۱۳۸۴).

۳) فنون کنترل کننده ورودی‌ها و دسترسی به اهداف در اماکن: این راهکار سعی دارد با مشکل کردن دسترسی افراد تروریست به اهدافی که در مکان‌های خاصی وجود دارند، اقدام نماید. در بسیاری از موارد افراد و گروه‌های تروریستی با رخنه در افراد و کارکنان مراکز دولتی و مجاور با سیستم‌های حساس صنعتی یا نظامی سعی در انجام عملیات‌های تروریستی دارند. بنابراین سازوکارهای حفاظتی مانند تعبیه دوربین‌های مداربسته، سیستم‌های نظارتی (مانیتورینگ) یا استفاده از پردازشگرهایی که با اثرانگشت یا شبکه چشم اجازه ورود به مراکز حساس را صادر می‌کنند، برای جلوگیری از نفوذ چنین اشخاصی ضروری است. همچنین حافظه‌های قابل حمل که با اتصال آنها به سیستم‌ها امکان انتقال بدافزارها به آنها امکانپذیر می‌شود، استفاده از پوشش مخصوص در مکان‌های حساس به منظور تفکیک اشخاص غیرمجاز، استحکام مراکز داده با استفاده از مصالح بتنی و فولادی به منظور نفوذ افراد غیرمجاز و همچنین بکار بردن فناوری‌های ویژه به منظور جلوگیری از نفوذ امواج الکترومغناطیسی به دستگاه‌های حساس، به ویژه بمب‌های الکترونیکی که قادر است در فواصل صد متری با انتشار امواج مغناطیسی دستگاه‌های رایانه‌ای را منفجر نمایند. بکارگیری اصول معماری ساختمان در مراکز حساس، به خصوص در مکان‌هایی که سرورها در آن قرار دارند، استفاده از سیستم‌های تشخیص نفوذ فیزیکی در مکان‌های خلوت و همچنین اتاق‌های رایانه و تجهیزات مخابراتی، از جمله راهکارهای پیشگیری وضعی است.

۴) محصور کردن دسترسی به ابزارهای تسهیل کننده جرم: دیگر از رویکردهای پیشگیری، ابزارها و تسهیل کننده‌هایی هستند که برای ارتکاب جرم لازم بوده یا باعث تحریک و تشویق بزهکار به ارتکاب بزه می‌شوند. کنترل و محدود کردن دسترسی شامل تدابیری می‌شود که طی آن چگونگی و نحوه برقراری ارتباط بین کاربران و سیستم‌های رایانه‌ای و مخابراتی کنترل می‌شود و هدف از این تدابیر، جلوگیری از دسترسی غیرمجاز

[1] Router

افراد به منابع اطلاعاتی است. نمونه‌ای از اقدامات محدود کننده دسترسی عبارتند از: اعطای حق دسترسی محدود به کاربران نسبت به برخی داده‌ها، امکانات یا دستگاه‌های خاص به افرادی که برای انجام کار خود به آن نیاز دارند و استفاده اشتراکی از آنها ممنوع گردد. در این راستا با تدوین سیاست‌هایی از جمله افزایش نرخ تعرفه‌های دولتی توسط سازمان تنظیم مقررات و ارتباطات رادیویی کشور، درخصوص ارائه خدمات اینترنتی پر سرعت به شرکت‌ها، اپراتورها و خدمات دهندگان به خصوص شرکت‌های خصوصی، بکارگیری پالایش توسط دولت یکی دیگر از اقدامات عملی در ایمن نگه داشتن فضای سایبر است. در حوزه ادارات دولتی و مراکز مهم و زیرساخت‌های حیاتی، تعیین و تخصیص شناسه کاربری برای هر کارمند در محیط‌های اداری و مکان‌های حساس می‌تواند از گشت‌زنی‌های بی‌مورد و خطرناک کارمندان در فضای اینترنت جلوگیری نمود.

۵) انحراف جهت اعمال مجرمانه: از طریق این روش می‌توان با ایجاد فاصله بین تروریست‌های بالقوه و آماج‌هایی که جذابیت فراوانی برای این دسته از افراد دارند، به منظور پیشگیری از وقوع عملیات‌های تروریستی در فضای سایبر جلوگیری نمود. در محیط اینترنت و تارنماهای گوناگون به خصوص شبکه‌های اجتماعی که از انواع قشرهای جامعه در آن حضور دارند، با استفاده از بنرهای تبلیغاتی می‌توان به موضوعاتی نظیر قبیح جلوه دادن اعمال افرادی که به سرقت اطلاعات و دسترسی به داده‌های شخصی و یا دولتی می‌نمایند اقدام نمود و با استفاده از این امکانات نسبت به گردآوری افرادی که دارای قابلیت‌های بالقوه در زمینه ارتکاب اعمال تروریستی سایبری هستند، جهت بکارگیری آنها در مراکز آموزشی دانش‌های مرتبط با رایانه به منظور منحرف نمودن این افراد نسبت به عملیات‌های مخرب جلوگیری اقدام نمایند.

۲-۱-۲- افزایش خطرات قابل پیش‌بینی ارتکاب جرم

یکی از آورده‌های پیشگیری وضعی تشدید و افزایش خطرات قابل پیش‌بینی برای ارتکاب جرم خاصی است. با پیش‌بینی این تمهیدات، بزهکاران جسارت کمتری برای انجام عملیات مجرمانه خواهند داشت. درخصوص تروریسم سایبری و آماج بالقوه جرم، یعنی زیرساخت‌های اطلاعاتی کشور، بکارگیری روش‌هایی که بزهکاران را متقاعد سازد که در صورت اقدام به اعمال مجرمانه منفعتی برای آنها در بر نخواهد داشت و احتمال دستگیری و ردیابی آنها وجود دارد. افزایش خطرات جرم چهار تکنیک را در بر می‌گیرد:

۱) کنترل مبادی ورودی و خروجی‌های اماکن عمومی؛

۲) تدابیر نظارتی؛

۳) شناسایی؛

۴) کنترل نامحسوس.

۲-۱-۳- تقویت محافظت از آماج جرم

هدف این سری از تکنیک‌ها تقلیل منافع و مزایای حاصل از ارتکاب بزه است. زمانی که بزهکاران منفعتی برای ارتکاب بزه نداشته باشند دست به اقدامات خطرناکی چون اختلال در شبکه‌های زیرساختی نمی‌نمایند. راهکارهای کاهش سود و زیان ارتکاب جرم شامل:

۱) تقویت محافظت از آماج جرم: از جمله راهکارهای تقویت آماج جرم به منظور مقابله با سایبر تروریسم عبارت است از: جداسازی و تفکیک شبکه‌های داخلی از اینترنت و فضای بیرون به منظور غیرقابل دسترسی بودن داده‌های شبکه برای دیگران. در مراکز حساس و حیاتی لازم است تمام رایانه‌ها و تجهیزات شبکه پلمپ شده و شماره‌گذاری شوند، تا افراد غیرمجاز حق باز کردن بدنه رایانه‌ها و تجهیزات شبکه را به هر منظوری نداشته باشند. امنیت فیزیکی نیز از جمله اقدامات موثر در تقویت محافظت از آماج جرم می‌باشد.

۲) استفاده از یاری‌گر دوگانه: به معنی استفاده از یک شبکه دیگر در کنار شبکه اصلی به منظور کم‌رسانی به دستگاه اصلی در زمان تحمل بار اضافی و همچنین در مواقعی که شبکه اولیه دچار اختلال شده یا بطورکلی مختل شده باشد.

۳) ایجاد مکان امن برای تأسیسات: اقداماتی نظیر استقرار تجهیزات در ساختمان‌های اختصاصی به منظور تأمین ایمنی بیشتر و نصب دوربین‌های مداربسته برای محافظت بیشتر از قرارگیری تأسیسات رایانه‌ای و مخابراتی.

۴) استفاده از ارتباطات بی‌سیم: نفوذگرها به آسانی از طریق امواج الکترومغناطیسی منتشر شده در محیط می‌توانند خود را بعنوان عضویی از شبکه تلقی کرده و از این طریق به شنود اطلاعات در حال انتشار اقدام نمایند. بنابراین تا آنجایی که ممکن است باید از ارتباطات سیمی برای برقراری ارتباط بین تأسیسات رایانه‌ای و مخابراتی استفاده نمود.

۵) تعیین منابع تغذیه متعدد: به منظور پشتیبانی از نیروی برق شبکه، در نظر گرفتن منبع تغذیه‌های متعدد در مواقعی که بر اثر حملات سایبری مخرب، شبکه با اختلال یا فقدان برق مواجه است ضروری می‌باشد.

۶) تمهید راهکارهایی به منظور مقابله با عوامل محیطی: اینگونه راهکارها برای جلوگیری از اختلال کلی در شبکه، مقابل عواملی از قبیل: بلایای طبیعی و آتش سوزی می‌باشد. امنیت فیزیکی با مستحکم نمودن مکان‌های قرارگیری منابع تغذیه و تأسیسات شبکه‌ای از دستیابی خرابکاران به سیستم‌های رایانه‌ای و مخابراتی جلوگیری می‌نماید. زیرا تروریست‌های سایبر می‌توانند با اتصال حافظه‌های قابل حمل به تأسیسات رایانه‌ای، اقدام به انتشار بدافزارهای رایانه‌ای و آلوده نمودن آنها نمایند. بطور کلی راه‌حل اساسی، نصب سیستم پشتیبان برای کل شبکه الزامی می‌باشد.

۲-۱-۴- کاهش یا حذف منافع قابل پیش‌بینی از جرم

این راهکار سعی دارد با از بین بردن سود ارتکاب بزه، بطورکلی قصد ارتکاب جرم را بیهوده جلوه داده و به طبع آن بزهکار را از انجام عملیات اجرایی جرم منصرف نماید. نمونه‌هایی از این اقدامات شامل: بکارگیری مکانیسم‌های «رمزگذاری» در سطوح مختلف می‌باشد. در این روش با بکارگیری نرم‌افزارهایی اطلاعات رمزگذاری شده و فرستاده می‌شود و شخص گیرنده نیز با استفاده از روش مزبور به رمزگشایی اطلاعات اقدام می‌کند. استفاده از سیستم‌های تشخیص نفوذ و پیشگیری از نفوذ نیز از راهکارهایی است که بزهکار را از انجام بزه منصرف می‌نماید.

۱) کاهش جذابیت امکانات جرم؛

۲) کاهش عوامل محرک در ارتکاب جرم.[1]

۲-۱-۵- از بین بردن معاذیر[2] توجیه کننده برای عقلانی جلوه دادن جرم

براساس این راهکار، اقدامات قابل تصور در مورد تروریسم سایبری و فضای سایبر شامل: پایش رها کننده یا رها کننده کنترل شده می‌باشد. نمونه‌ای از این اقدامات از قبیل نصب تراشه‌های (VChip) بر روی سیستم های رایانه به منظور کنترل فعالیت‌های سیستم عامل و جلوگیری از دسترسی به منابع آن می‌باشد.

۲-۲- پیشگیری اجتماعی از تروریسم سایبری

۲-۲-۱- شاخصه‌های پیشگیری اجتماعی از تروریسم سایبری

۱) همه‌جانبه بودن

رایانه در برخی موارد نه تنها ابزاری برای وقوع جرم است و از آن در انجام عملیات مجرمانه استفاده می‌شود بلکه می‌تواند در قالب محیط اعمال جرم نیز مورد استفاده قرار گیرد. تروریست‌های سایبری از هر جا می‌توانند وارد شوند و اقدامات خرابکارانه خود را انجام دهند. بنابراین قبل از اقدام به هرگونه پیشگیری اجتماعی در این خصوص باید این اقدامات در مقیاس وسیع صورت گیرد (Denning, 2005).

۲) اختصاص بودجه مناسب برای پیشگیری اجتماعی

باتوجه به همه‌جانبه بودن این اقدامات و همچنین گستردگی در برنامه‌های پیشگیری، این لزوم احساس می‌شود که باید بودجه‌ای مناسب برای آن پیش‌بینی گردد البته باتوجه به حجم وسیع خسارات به وقوع

[1] Reducing the Provocations
[2] Removing Excuses

پیوسته توسط تروریست‌های سایبری که تا حدی در این مقاله به آن اشاره شد، لزوم اختصاص بودجه‌ای مناسب معقول به نظر می‌رسد.

بطورکلی، در پیشگیری اجتماعی، هدف، از بین بردن انگیزه مجرمانه[1] است و به همین دلیل، به آن پیشگیری بزهکارمحور[2] گفته می‌شود. در اینجا راهکارهای اجتماعی، مانند رفع بیکاری و فقر که زمینه‌ساز شکل‌گیری انگیزه‌های مجرمانه مالی و حتی قتل می‌شوند و همچنین راهکارهای تربیتی و آموزشی[3] کودکان، بعنوان آسیب‌پذیرترین گروه سنی، هم از لحاظ بزهکاری و هم از لحاظ بزه‌دیدگی، در دستورکار قرار می‌گیرند (نیازپور، ۱۳۸۲: ۷۴). اما در پیشگیری وضعی، هدف، صیانت از بزه‌دیدگی بالقوه از طریق سلب فرصت[4] و یا ابزار[5] ارتکاب جرم است (Shinder, 2002).

۲-۲-۲- آموزش بزه‌دیدگان بالقوه در مقابل تروریسم سایبری

آموزش بزه‌دیدگان بالقوه در مقابل تروریسم سایبری یکی از مهمترین و موثرترین عناصر پیشگیری از تروریسم سایبری است و کاربران اینترنتی، کارمندان دولتی و بخش خصوصی باید از شیوه استفاده صحیح از فضای سایبر بطوری که خطری آنها و بخش مربوطه آنها را تهدید نکند، آگاه باشند (Ramsaroop, 2003). مطالعات نشان داده است چنانچه کارمندان بخش خصوصی و دولتی و کاربران خانگی به خوبی به استفاده صحیح از محیط سایبر آگاه شوند، خطرات تروریسم سایبری تا ۸۰ درصد کم می‌شود (Grake, 2007). کاربران باید از خطرات موجود آگاه شوند و انواع گروه‌های تروریستی سایبری، ابزارهای آنها و راهکارهای پیشگیری از آن را بشناسند. بعنوان مثال باید بدانند که نباید به کامپیوترهای شرکت حافظه خارجی وصل کنند، یا اینکه نباید با کامپیوترهای شرکت ایمیل‌ها را چک کنند (Willems, 2011). یکی از ابزارهایی که بدین منظور پیشنهاد شده، سیستم جامع آخرین اطلاعات سایبری است. این سیستم به تمامی کارمندان آخرین اطلاعات را از چگونگی روش صحیح استفاده از فضای سایبر، آخرین اخبار از تروریست‌های سایبری و سایر اطلاعات را ارائه می‌دهد. کارمندانی که خارج از شرکت هستند نیز این اخبار از طریق آدرس الکترونیکی دریافت می‌کنند (Jonse, 2005). حملات سایبری هنگامی جواب می‌دهد که کاربران اینترنتی با عدم علم به حمله و عدم شناسایی شیوه‌های حمله کارهایی را انجام دهند که در معرض آسیب اینترنتی قرار گیرند اگر کل جامعه نسبت به اینگونه حمله‌های اینترنتی آگاهی کامل یابند و درک کنند که تروریسم سایبری

[1] Criminal Motivation
[2] Criminal-based Prevention
[3] Developmental-based Crime Prevention
[4] Opportunity
[5] Tool

همانند تروریسم فیزیکی می‌تواند آسیب بسیار زیادی وارد کند، تروریست‌ها فرصت ارتکاب جرم پیدا نمی‌کنند. ارائه برنامه‌های آموزش عمومی، آموزش در مدرسه، کتابخانه‌ها، مراکز IT و دانشگاه‌ها و مشارکت در آموزش‌های خصوصی- عمومی از جمله راه‌هایی است که باید در اموزش کاربران مورد استفاده قرار گیرد (گرکی، ۱۳۸۹).

۲-۲-۳- تشکیل ستاد ویژه در جهت گرفتن فرصت از تروریست‌های سایبری

یکی از روش‌هایی که فرصت خرابکاری را از تروریست‌های سایبری می‌گیرد، تشکیل کارگروه و ستادهایی است که در جهت حذف فرصت‌های خرابکاری تروریست‌های فعالیت کنند. بعنوان نمونه پس از سقوط شوروی، پروژه دفاع ملی در برنامه (دفاع هملند) مطرح گشت که براساس این پژوه در مسئله امنیت باید یک باز تعریف صورت گیرد. یکی از جنبه‌های (پروژه هملند) مقابله با ترویست‌های سایبری و دفاع همه‌جانبه‌تر بود (Andrew, 2005). باتوجه به این پروژه، ستادهایی وظیفه برقرار کردن امنیت در فضای سایبر را برعهده گرفتند این ستادها از طریق سلب فرصت خرابکاری از تروریست‌های سایبری فعالیت می‌کنند.

۲-۲-۴- ایجاد سپر دفاع سایبری

برای مبارزه و پیشگیری همه‌جانبه در مقابل تروریست‌های سایبری، برخی از کشورها اقدام به ایجاد سپر دفاع سایبری نموده‌اند بعنوان نمونه در اروپا از۱۰ می۲۰۱۰ سپر دفاع سایبری فعال گشت و بسیاری از کشورهای اروپایی در آن مشارکت نمودند همانند این طرح نیز در آمریکا با نام دفاع سایبری بین‌المللی پنتاگون به وجود آمده است هدف از شکل‌گیری سپر دفاعی در اروپا، پاسخ سریع به حملات سایبری بوده است این سپر دفاع برای سه هدف شکل گرفته است:

۱) باید از اطلاعات حساس در فضای سایبر محافظت کند؛

۲) تمام اقدامات امنیتی و تمام اقدامات دفاعی ممکن را با استفاده از هر ابزاری بکار بندد تا مانع خرابکاری سایبری گردد؛

۳) باید در برابر حملات آینده تروریست‌ها و ابزارهای آنان مقاوم باشد و به روز شده باشد.

اما نکته‌ای که کارشناسان به آن اشاره می‌کنند این است که تجربه نشان داده است ایجاد چنین سپر دفاعی بطور کامل امنیت را برقرار نمی‌کند طرح سپر دفاع سایبری باید به همراه سایر اقدامات پیشگیرانه اجرا گردد (Sauver, 2008).

تشکیل گروه‌های مردمی در جهت مبارزه با تروریسم سایبری دو مزیت مهم برای دولت‌ها به همراه دارد اول اینکه هزینه جاری دولت در راه مبارزه علیه تروریسم سایبری کاهش می‌یابد و دوم اینکه با تشکیل چنین گروه‌هایی، طرح و مسئولیت دفاع ملی برای همه بنحوه فزاینده‌تری اجرا خواهد شد.

بنابراین در میان انواع پیشگیری در نقش و تاثیر توسعه فضای مجازی در گسترش تروریسم، پیشگیری وضعی مناسب‌ترین راهکار است. لذا در کشورمان علاوه بر نیاز تخصیص قواعد خاص جزایی در این باره، تدابیر پیشگیرانه نیز در قالب سیاست‌های امنیتی و تدابیر کارآمد فنی لازم می‌باشد. بنابراین درخصوص پیشگیری از بزه‌دیدگی، کاربران خانگی و شبکه‌های زیرساختی بعنوان عمده‌ترین بزه‌دیدگان این بزه باید تدابیر پیشنهادی از جمله: بکارگیری سیستم‌های تشخیص نفوذ و پیشگیری از نفوذ، مستقل نمودن شبکه‌های کنترل و اداری، استفاده از دیوار آتشین نرم‌افزاری و سخت‌افزاری، اجباری نمودن استفاده از پست الکترونیکی بومی، تصویب قوانین صریح و روشن با مجازات‌های معین درخصوص مقابله با تروریسم سایبری و اتخاذ یک نقطه‌نظر مشترک از نظر حقوق جزای بین‌الملل در تدوین کنوانسیون جامع درخصوص تهدیدات فضای سایبر از جمله تروریسم سایبری از راهکارهایی هستند که به بهبود شرایط کنونی هم در کشورمان و هم در سطح بین‌الملل کم خواهند کرد.

به نظر می‌رسد نحوه پیاده‌سازی تدابیر پیشگیرانه اجتماعی و وضعی در فضای سایبر روشن شده 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 در عین حال بزه‌دیدگی آنها پیشگیری خواهد شد. هم اکنون این مسئله تا حدی مورد توجه قرار گرفته که مباحث تخصصی تحت عنوان اخلاق سایبری[1] از سوی صاحب‌نظران و سیاستگذاران این حوزه مطرح شده است. با این حال، از آنجا که این فضا ماهیتی فنی دارد، دست‌اندرکاران بیشتر به دنبال اجرای تدابیر پیشگیرانه وضعی فنی هستند که از نمونه‌های بارز آن می‌توان به انواع فیلترها اشاره کرد که البته ناکارآیی‌ها و تدابیر نظارتی اینگونه ابزارها بر همگان محرز شده، اما بکارگیری آنها اجتناب‌ناپذیر است (جلالی فراهانی، ۱۳۸۵).

اما درخصوص کارآیی این تدابیر در مورد اقدامات تروریستی سایبری، روشن است که تدابیر پیشگیرانه اجتماعی ماهیت تروریسم را هدف قرار می‌دهند و در این جهت می‌توانند از فضای سایبر بعنوان یک ابزار اطلاع‌رسانی و تبلیغاتی نیز استفاده کنند و البته تأکید ویژه‌ای بر این اقدامات در فضای سایبر داشته باشند. تدابیر پیشگیرانه وضعی نیز عمدتاً بدون توجه به هویت مجرمان بکار می‌روند. برای مثال، هدف، پیشگیری از آلوده نشدن سیستم‌ها به انواع ویروس‌ها یا محتواهای مستهجن است و تفاوتی نمی‌کند مرتکب آن چه کسی است. البته برای برخی سیستم‌ها که در زیرساخت‌های حیاتی مستقر هستند و عمدتاً مجرمانی نظیر تروریست‌ها قصد تعرض به آنها را دارند، می‌بایست برنامه‌ریزی‌های ویژه‌ای صورت گیرد. همچنین برای اینکه از دسترس کاربران به محتواهای ارسالی از سوی تروریست‌ها جلوگیری شود، مانند انواع پیام‌های تحریک

[1] Cyber Ethics

کننده و مخل آسایش عمومی، می‌بایست فهرست‌های سیاه یا سفید فیلترها بنحوی تنظیم شود که تمامی حوزه‌های مربوط را شناسایی و دسترس‌ناپذیر کنند.

۳- راهکارهای حقوقی مقابله با تروریسم سایبری

بی‌تردید معضل به واقع جهانی تروریسم که تقریباً تمامی دولت‌ها و ملت‌ها را به جنگ طلبیده و همواره لطمات بالقوه و بالفعل گوناگونی را به آنها وارد آورده، مستلزم اتخاذ تدابیر جدی است تا علاوه بر مقابله موثر با سیاستگذاران، برنامه‌ریزان و عوامل تروریستی، از وارد آمدن لطمات جانی و مالی بسیار جلوگیری گردد.

یکی از منطقی‌ترین و صحیح‌ترین راهکارهای مقابله با تروریسم که حتی می‌تواند زیربنای شایسته‌ای برای دیگر راهکارها نیز باشد، بسترسازی حقوقی از طریق وضع قوانین و مقررات موردنیاز است. باتوجه به اینکه ماهیت اقدامات تروریستی مجرمانه است و در واقع قانون‌نویسان و قانونگذاران با یک پدیده مجرمانه مواجه‌اند، لذا بسترسازی حقوقی برپایه قوانین کیفری صورت می‌گیرد. همانطور که ملاحظه شد، قانونگذاری کیفری راجع به تروریسم، سابقه‌ای نسبتاً طولانی دارد. اما از آنجا که نتایج و عواقب اینگونه اقدامات بسیار زیانبار و وحشتناک است، مراجع ذیصلاح تقریباً از همان ابتدا به دنبال پیشگیری از وقوع آنها بوده‌اند. زیرا باتوجه به اهدافی که تروریست‌ها دنبال می‌کنند، درخصوص 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 باتوجه به شرایط خاص حاکم بر این پدیده مجرمانه، اولین گزینه کاملاً عاقلانه و منطقی، اتخاذ تدابیر پیشگیرانه از وقوع تروریسم است؛ هرچند اهمیت این مسئله نباید جایگاه ضمانت اجراهای کیفری را تحت‌الشعاع قرار دهد.

مقابله کیفری با پدیده مجرمانه تروریسم، فرایندی است که از دو رکن اصلی تشکیل شده است:

۱) حقوق جزای ماهوی (جرم‌انگاری) و ۲) حقوق جزای شکلی (آئین دادرسی کیفری).

۳-۱- حقوق جزای ماهوی تروریسم سایبری

درخصوص پدیده تروریسم بعنوان یک پدیده مجرمانه، یک مانع بزرگ در این راه وجود دارد و آن اینکه اگر قرار است اقدامات تروریستی تحت شمول ضمانت اجراهای کیفری بعضاً سنگین و حتی جبران‌ناپذیری مانند اعدام قرار گیرند، باید تعاریف مشخص و دقیقی از آنها که عاری از هرگونه ابهام باشد، در قوانین کیفری انعکاس یابد.

همچنین فرامرزی بودن فضای سایبر، صرف‌نظر از مسائل دشواری که هر حوزه آئین دادرسی کیفری وجود آورده و در قسمت بعد به آن اشاره خواهد شود، قانونگذاران کیفری را نیز با چالش‌هایی جدی مواجه کرده است. طبق اصول اساسی کیفری اصل بر اجرای قوانین جزایی هر قلمرو سرزمینی کشورهاست، مگر موارد

استثنایی که به آن تصریح شده باشد (ماده ۳ قانون مجازات اسلامی ۱۳۷۰). حال چگونه می‌توان این قوانین را در مورد جرایمی قابل اجرا دانست که به قلمرو سرزمینی محدود نیستند. علاوه بر این، زمانی دشواری چاره‌جویی راجع به اینگونه مباحث محرز می‌گردد که ملاحظات اجتماعی، سیاسی، فرهنگی و اقتصادی کشورها برای جرم‌انگاری پدیده‌های خاص، سایبری نیز مورد توجه قرار گیرد (کاشیان، ۱۳۸۴: ۷۵).

این عدم اجماع بر سر عناوین مجرمانه و به تبع آن جرم‌انگاری متحدالاشکل برای مبارزه با جرایم سایبری به خوبی در اسناد بین‌المللی، منطقه‌ای و بین‌الدولی که تاکنون تدوین و منتشر شده نیز مشهود است بارزترین آن کنوانسیون اروپایی جرایم سایبر[1] است با اینکه اکثریت اعضای این کنوانسیون را کشورهای عضو شورای اروپا تشکیل می‌دهند و آنها نظام حقوقی مشابهی دارند، اما تنها ۹ عنوان مجرمانه از بیش از ۲۰۰ عنوان مجرمانه سایبری که تاکنون شناسایی شده در این سند منعکس شده و از میان این ۹ عنوان تنها هرزه‌نگاری کودکان[2] با حق شرط[3] مواجه نشده است. به این ترتیب، به نظر می‌رسد تکلیف عناوین مجرمانه بسیار خاص و در عین حال حساسی مانند تروریسم سایبری روشن شده است البته برخی کشورها سعی کرده‌اند بنحوی این حوزه را فتح باب کنند. برای مثال در بخش اول قانون تروریسم بریتانیا[4] مصوب ۲۰۰۰ چنین آمده است:

۱) در این قانون، تروریسم به معنای ارتکاب یا تهدید به ارتکاب اعمالی است که:

الف) تحت شمول بند ۲ قرار گیرند؛ ب) ارتکاب یا تهدید به ارتکاب به منظور تاثیرگذاری بر دولت یا ارعاب مردم یا بخشی از آنها باشد و پ) ارتکاب یا تهدید به ارتکاب به منظور پیشبرد اهداف سیاسی، مذهبی یا ایدئولوژیکی باشد.

۲) اعمالی که تحت شمول این بند قرار می‌گیرند عبارتند از: ... ث) اقداماتی که برای ایجاد اختلال یا قطع جدی یک سیستم الکترونیکی ارتکاب می‌یابند (Walker, 2006).

شایان ذکر است با وجود اینکه کشورها هنوز بطور گسترده به تروریسم سایبری در مفهوم خاص آن در قوانین جزایی نپرداخته‌اند، اما ماهیت این اقدام که همانا تخریب یا آسیب‌رسانی به داده‌ها و سیستم‌های رایانه‌ای است، از جمله مصادیق اولیه جرایم رایانه‌ای به شمار می‌روند که اغلب راجع به آن قوانین کیفری را تصویب رسانده‌اند و به نظر می‌رسد با لحاظ کیفیات مشاهده فعلا می‌تواند پاسخگوی نیازهای تقنینی باشد، ولی در آینده نزدیک با روند رو به رشد حملات تروریستی سایبری در سراسر جهان عملاً نیاز به قوانین خاص بروز خواهد یافت در مورد جرایمی که به تمامیت داده‌ها و کارکرد سیستم‌های رایانه‌ای لطمه وارد آورند کنوانسیون جرایم سایبر چنین اشعار می‌دارد:

[1] European Convention on Cybercrime
[2] Child Pornography
[3] Reservation
[4] United Kingdom Terrorism Act

ماده (۴) ایجاد اختلال در داده‌ها: ۱- هریک از اعضا باید بگونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم براساس حقوق داخلی خود، هر نوع صدمه زدن، پاک کردن، خراب کردن، تغییر یا قطع داده‌های رایانه‌ای را که بطور عمدی و بدون حق انجام می‌شود جرم‌انگاری کنند ۲- اعضا می‌توانند حق جرم‌انگاری افعال مندرج در بند یک را در جایی که صدمه شدیدی وارد شده اعمال کنند.

ماده ۵ ایجاد اختلال در سیستم‌ها: هریک از اعضا باید بگونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم براساس حقوق داخلی خود، هر نوع ایجاد اشکال جدی عمدی و بدون حق را که در عملکرد سیستم رایانه‌ای در اثر وارد کردن، انتقال، صدمه زدن، پاک کردن، خراب کردن، تغییر یا متوقف کردن داده‌های رایانه‌ای به وجود می‌آید جرم‌انگاری کند.

شایان ذکر است قانونگذار ما با این مفهوم بیگانه نیست و در لابلای بعضی قوانین کیفری موجود نمونه‌هایی را ملاحظه کرد که نمونه بارز ان ماده (۶۸۷) قانون مجازات اسلامی مصوب ۱۳۷۰ است هرچند این مقرره عام قانونی است و تنها اقدامات تروریستی را در بر نمی‌گیرد لذا نمی‌تواند مبنای مناسبی برای مقابله جدی و اختصاصی به معضل تروریسم باشد.

به همین دلیل در سال ۱۳۸۲ لایحه‌ای با عنوان (لایحه مبارزه با تروریسم) در دولت هشتم تنظیم و به مجلس شورای اسلامی اراده گردید که تاکنون به دلایل نامعلومی مسکوت مانده است. همچنین کشورمان بعنوان یکی از اعضای سازمان ملل متحد، تاکنون به پنج سند از اسناد مصوب این سازمان راجع به تروریسم پیوسته و مطابق آنها تعهداتی را پذیرفته است ولی هنوز هیچ یک از آنها جنبه قانونی نیافته‌اند، البته چهار سند راجع به تروریسم هوایی است. سازمان کنفرانس اسلامی نیز در مورد تروریسم درسال ۱۹۹۹ کنوانسیون مبارزه با تروریسم بین‌المللی را به تصویب رسانده است (حکیمی‌ها، ۱۳۸۵).

۳-۲- حقوق جزای شکلی (آئین دادرسی کیفری)

اولین مسئله‌ای که به هنگام طرح مباحث کیفری باید در مورد آن تعیین تکلیف کرد، تعیین مرجع ذیصلاح قضایی است در این زمینه اولین قاعده‌ای که مورد توجه قرار می‌گیرد. صلاحیت دادگاه محل وقوع جرم است رعایت این قاعده در بسیاری موارد منجر به رعایت اصل سرزمینی کشورها در امور کیفری نیز می‌شود در مواردی هم که جرایمی حالت فرامرزی پیدا می‌کنند، قواعدی نسبتاً مورد اتفاق میان کشورها وضع شده تا در اعمال صلاحیت کیفری فرامرزی[1] مشکل خاصی به وجود نیاید. اما در فضای سایبر، اولین و بدیهی‌ترین مسئله این است که چیزی به نام محل وقوع جرم معنا ندارد در جرمی مانند نشر ویروس یا تصاویر مستهجن

[1] Extraterritorial Jurisdiction

کودکان، هر سیستم رایانه‌ای در سراسر جهان می‌تواند محل وقوع جرم تلقی گردد. بالطبع هنگامی که نمی‌توان به این قاعده بدیهی تمسک کرد، مشکلات پیش‌روی دیگر قواعد محرز خواهد بود.

پس از صلاحیت کیفری، نوبت به فرایند اجرایی محاکم به همراه مجریان قانون برای تعیین تکلیف پرونده‌های مفتوح می‌رسد که عموماً از آن بعنوان کشف علمی جرایم یاد می‌شود و همانطور که شاهد هستیم در اثر پیشرفت علوم در حوزه‌های مختلف، این شاخه از علوم جنایی نیز با تحولات شگرفی مواجه شده است اما مسئله‌ای که فضای سایبر بطور خاص برای این شاخه به وجود آورده به ماهیت کاملاً فنی آن مربوط می‌شود. مسلماً برای شناسایی عوامل جرمی که در فضای سایبر ارتکاب می‌یابد و به تبع اثبات جرم باید وارد این فضا شد لذا میزان قابلیت فنی مجریان قانون در شناسایی و ردیابی آثار مجرمانه الکترونیکی و کشف هویت مجرمان سایبری اهمیت حیاتی دارد (Casey, 2002). مهمترین ثمره عملی این مسئله در استنادپذیری ادله الکترونیکی[1] ظاهر می‌شود.

باتوجه به آسیب‌پذیری بالای داده‌های الکترونیکی، برای اینکه بتوان نزد محاکم به آنها بعنوان ادله محکمه-پسند استناد کرد، مجریان قانون باید ضوابط پیچیده‌ای را رعایت کنند. البته وجود حساسیت‌های خاص در مورد برخی حوزه‌های سایبری نیز مجریان قانون را با مشکلات بسیاری مواجه ساخته است. نمونه بارز آن جمع‌آوری داده‌های شخصی و شنود ارتباطات الکترونیکی است که دغدغه‌های حقوق بشری بسیاری را برانگیخته است و به همین دلیل، در اسناد مربوط به این مسئله توجه ویژه‌ای شده است. برای مثال در ماده (۱۵) کنوانسیون جرایم سایبر، از کشورهای عضو خواسته شده اقدامات این حوزه را با رعایت اسناد و قوانین حقوق بشری انجام دهند.

همچنین برخلاف تصور عموم، فرامرزی بودن این فضا نه تنها کمکی به توسعه ارتکاب عمل مجریان قانون نمی‌کند، بلکه در بسیاری موارد مجبورند برای جمع‌آوری داده‌ها به سرعت فناپذیر رایانه‌ای از سیستم‌های رایانه‌ای واقع در دیگر کشورها، تشریفات زمان بری را رعایت کنند که به هیچ وجه با شرایط حاکم بر این فضا سازگار نیستند. به دلیل وجود اینگونه مسائل حیاتی، در تمامی اسناد بین‌المللی و منطقه‌ای که تا به حال راجع به جرایم سایبر تدوین و منتشر شده، به مجریان قانون توجه ویژه‌ای شده است. نمونه بارز آن کنوانسیون سایبر است که بیش از دو سوم مقررات آن به این حوزه اختصاص یافته است (کنوانسیون اروپایی، ۲۰۰۱).

با اعتقاد به نیاز مبرم به این سیاست جنایی مشترک بعنوان یک اولویت برای حمایت از جامعه در برابر جرایم سایبر، با اقداماتی از قبیل تصویب قوانین مناسب و گسترش همکاری‌های بین‌المللی و با اگاهی از

[1] Admissibility of Digital Evidence

دگرگونی‌های اساسی که در اثر دیجیتالی شدن همگرایی و ادامه جهانی شدن شبکه‌های رایانه‌ای به وجود آمده است.

در مجموع در این زمینه می‌توان اظهار داشت که با گسترش انقلاب‌های تکنولوژیک و اطلاعات و پیچیده‌تر شدن مناسبات اقتصادی و تولیدی در عصر جهانی شدن، از یکسو 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 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. بدیهی است برای حل این معضل باید راهکارهای گوناگون اساسی و زیربنایی در حوزه‌های مختلف طرح‌ریزی شود. آنچه در اینجا مورد تاکید قرار گرفته، بسترسازی حقوقی از منظر حقوق کیفری و جرم‌شناسی است هرچند باید در این زمینه به یک نکته اساسی توجه داشت و آن اینکه از انجا که کلیه راهکارهای مبارزه با تروریسم بطور اعم، و مبارزه با تروریسم سایبری بطور اخص، با یکدیگر ارتباط دارند و بر یکدیگر تاثیر گذارند. لازم است پیش از هر چیز راهبردهای کلان مبارزه با تروریسم باتوجه به مصالح و مقتضیات داخلی و عنایت به شرایط بین‌المللی تدوین شود و زمینه اجرای گسترده آن فراهم گردد تا تحقق اینگونه اقدامات بنیادین مسیر گردد.

نتیجه‌گیری

پیشرفت تکنولوژی و تحولات عصر حاضر بسیاری از مفاهیم سنتی حقوق کیفری را با چالش مواجه ساخته است. از جمله اینکه فضای مجازی و تبادل اطلاعات این فرصت را به خاطیان عرصه اجتماعی داده تا اعمال تروریستی خود را با آسانی با استفاده از این فضا متحول سازند.

براساس آنچه در این مقاله مورد بررسی قرار گرفته است می‌توان گفت که:

۱) در واقع نقش عمده فضای مجازی و فناوری رایانه بیش از همه، افزایش گزینه‌هایی است که گروه‌های تروریست برای رشد در اختیار دارند. از سوی دیگر، با پیشرفت تکنولوژی، راه‌های ارتکاب جرم فنی‌تر و تخصصی‌تر شده و راه‌های مقابله با آن نیز دشوارتر می‌نماید. یکی از ویژگی‌های فناوری اطلاعات به ویژه اینترنت امکان ساماندهی و تدارک تهاجم سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده می‌باشد و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود، با ایجاد ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تأخیر در آنها می‌گردد. از دلایل روی آوردن تروریست‌ها به فضای سایبری می‌توان به موارد زیر اشاره نمود، بی‌حد و مرز بودن، سرعت خیره کننده مبادلات در محیط سایبر، و به تبع

آن، سرعت ارتکاب جرایم سایبر، و امکان فرار بسیار سریع مرتکب از صحنه جرم مجازی، امکان اختفاء و یا حتی امحاء آثار و دلایل جرم، ابزار و تجهیزات قابل دسترس، ارزان بودن، دسترسی سریع و عدم نظارت کافی در این فضا، باعث شده که بزهکاران از دنیای فیزیکی روی برگردانده و به دلایل مختلف از جمله شکست آنها در اقدام به عمل مجرمانه در دنیای فیزیکی، عدم اعتماد به نفس در دنیای واقعی و دیگر عواملی که ممکن است ریشه در مباحث روانشناسی داشته باشد، به فضای سایبر کشیده شوند.

۲) بدیهی است برای حل این معضل باید راهکارهای گوناگون اساسی و زیربنایی در حوزه‌های مختلف طرح-ریزی شود. آنچه در اینجا مورد تأکید قرار گرفته، بسترسازی حقوقی از منظر حقوق کیفری و جرم‌شناسی است. هرچند باید در این زمینه به یک نکته اساسی توجه داشت و آن اینکه از آنجا که کلیه راهکارهای مبارزه با تروریسم بطور اعم، و مبارزه با تروریسم سایبری بطور اخص، با یکدیگر ارتباط دارند و بر یکدیگر تأثیرگذارند، لازم است پیش از هر چیز راهبردهای کلان مبارزه با تروریسم باتوجه به مصالح و مقتضیات داخلی و عنایت به شرایط بین‌المللی تدوین شود و زمینه اجرای گسترده آن فراهم گردد تا تحقق اینگونه اقدامات بنیادین میسر گردد.

ضرورت سیاستگذاری کلان در این حوزه، زمانی عینیت بیشتری می‌یابد که دریابیم تروریسم از آن ماهیت محدود چند دهه پیش خود خارج شده و با به خدمت گرفتن فناوری‌های نوین گوناگون نظیر فضای سایبر، انرژی هسته‌ای، مواد بیولوژیکی و شیمیایی و مانند آن، حوزه‌های بین رشته‌ای را با چالش جدی مواجه ساخته است. عدم توجه به این مسئله بسیار مهم باعث می‌شود قوانین و مقرراتی که بطور مجزا در هریک از این حوزه‌ها به تصویب می‌رسند، برای مثال قوانین و مقررات راجع به امنیت فضای سایبر از یکسو و قوانین و مقررات مبارزه با تروریسم از سوی دیگر، نتوانند آن رابطه لازم و بایسته را با یکدیگر برقرار کنند و عملاً نتیجه مورد انتظار محقق نگردد. به عبارت دیگر تصویب قوانین صریح و روشن با مجازات‌ها معین درخصوص مقابله با تروریسم سایبری و اتخاذ یک نقطه‌نظر مشترک از نظر حقوق جزای بین‌الملل در تدوین کنوانسیون جامع درخصوص تهدیدات تروریستی در فضای سایبر از راهکارهایی هستند که به بهبود شرایط کنونی هم در کشورمان و هم در سطح بین‌الملل کمک خواهند کرد. لذا علاوه بر نیاز تخصیص قواعد خاص جزایی در این باره، تدابیر پیشگیرانه نیز در قالب سیاست‌های امنیتی و تدابیر کارامد فنی لازم می‌باشد. در نهایت به دلیل اینکه در تروریسم سایبری، جرم فاقد محل وقوع می‌باشد، این جرم عموماً فرامرزی بوده و تهدیدی مستقیم علیه منافع و امنیت ملی کشورها است. در این زمینه لازم است تدابیر تقنینی، قضایی و اجرایی ویژه‌ای در سطح ملی و بین‌المللی در نظر گرفته شود.

فهرست منابع

فارسی:

۱- آشوری، داریوش (۱۳۸۲)، **دانش‌نامه سیاسی**، تهران: انتشارات مروارید.

۲- جلالی فراهانی، امیرحسین (۱۳۸۴)، «پیشگیری وضعی از جرائم سایبری در پرتو موازین حقوق بشر»، **مجله فقه و حقوق**، س۲.

۳- جلالی فراهانی، امیرحسین (۱۳۸۹)، **کنوانسیون جرائم سایبری و پروتکل الحاقی آن**، چ۱، تهران: انتشارات خرسندی.

۴- جوان جعفری، عبدالرضا (۱۳۸۵)، «جرائم سایبر و چالش‌های نوین سیاست کیفری»، **مجموعه مقالات همایش جهانی شدن حقوق و چالش‌های آن**، مشهد، دانشگاه فردوسی.

۵- چاوشی، محمدصادق (۱۳۸۷)، «بررسی تحلیلی تروریسم سایبری در نظام کیفری»، **پایان‌نامه کارشناسی‌ارشد، حقوق جزا و جرم‌شناسی**، دانشگاه قم.

۶- حکیمی‌ها، سعید (۱۳۸۵)، «تروریسم در حقوق ایران و اسناد بین‌المللی»، **رساله دکتری حقوق کیفری و جرم‌شناسی**، دانشکده علوم انسانی دانشگاه تربیت مدرس.

۷- عالی‌پور، حسن (۱۳۸۳)، «کلاهبرداری رایانه‌ای»، **مجله پژوهش‌های حقوقی؛ موسسه مطالعات و پژوهش‌های حقوقی شهر دانش**، ش۶.

۸- فضلی، مهدی (۱۳۸۹)، **مسئولیت کیفری در فضای سایبر**، چ۱، تهران، انتشارات خرسندی.

۹- کاشیان، علیرضا و دیگران (۱۳۸۴)، **راهبری اینترنت (مشارکت فراگیر)**، دبیرخانه شورای عالی اطلاع‌رسانی.

۱۰- گرکی، مارکو (۱۳۸۹)، **جرائم سایبری: راهنمایی برای کشورهای در حال توسعه**، مترجم: مرتضی اکبری، تهران، انتشارات نیروی انتظامی.

۱۱- مرادی، حجت‌اله (۱۳۸۹)، **قدرت و جنگ نرم**، چ۳، تهران: نشر ساقی.

۱۲- نجفی ابرندآبادی، علی‌حسین (۱۳۹۲)، **درباره سن و علوم جنایی، دیباچه در: مبانی پیشگیری اجتماعی رشدمدار از بزهکاری اطفال و نوجوانان**، چ۱، تهران: نشر میزان.

لاتین:

13- Andrew, Lewis and jams, autorms (2005). *Cyber security and regulation in the United States*, center for strategic and international studies Washington.

14- Casey, Eoghan (2002). *Digital Evidence and Computer Crime*, Academic Press.
15- Denning, Dorothy (2005). *Is cyber- terrorism coming?* Marshall Institution.
16- Grake, Marco (2007). Cyber terrorism, chao communication camp.
17- Jonse, Andrew (2005). Cyber terrorism, fact or fiction, computer fraud & security.
18- Ramsaroop, peter (2003). Cybercrime, cyber terrorism and cyber warfare, technology and health services Delivery health services organization unit.
19- Sauver, Joe (2008). Cyber war, cyber terrorism and cyber Esionage, security programs manager.
20- Shinder, Debra Littlejohn (2002). *Scene of the Cyber Crime, Computer Forensics Hand Book*, Syngress Publication.
21- U.S. Army TRADOC; A Military Guide to Terrorism in the Twenty-first Century (2004).
22- Walker, Clive (2006). Cyber-terrorism: Legal Principle and Law in the United Kingdom, *Penn State Law Rev 110*, No. 3.
23- Willems, Eddy (2011). Cyber-terrorism in the processes industry, computer fraud security.