نشریه علمی فقه، حقوق و علوم جزا
مقاله پژوهشی، سال هفتم، شماره ۲۴، تابستان ۱۴۰۱، صفحات ۱ تا ۲۰
تاریخ دریافت: ۱۴۰۱/۰۱/۱۵ – تاریخ پذیرش: ۱۴۰۱/۰۳/۱۲

سیاست جنایی مقابله با تروریسم سایبری

| مجید بادروح[۱]| کارشناس ارشد رشته حقوق جزا و جرم شناسی، دانشگاه آزاد واحد بوشهر.

چکیده

از تلاقی اعمال تروریستی و فضای سایبر، گونه ای نوپا و نوین از اعمال تروریستی تحت عنوان تروریسم سایبری پا به عرصه وجود نهاده است. یکی از تهدیدات امنیتی که همواره دولت‌ها و ملت‌ها را آزار داده، اقدامات تروریستی است که عمدتاً با پیامدهای بسیار زیانباری همراه هستند. بدیهی است زیرساخت‌های حیاتی و زیر بنایی جامعه از قبیل تولید و توزیع برق، منابع آب، صنعت گاز و نفت، سیستم‌های مخابراتی، خدمات بانکی و مالی، سیستم حمل و نقل و خدمات درمانی از بهترین اهداف محسوب می‌شوند که با توجه به رایانه ای و الکترونیکی شدن آنها، نه تنها ارتکاب اقدامات تروریستی را آسانتر نموده بلکه لطمات وارد شده بسیار سهمگین‌تر و جبران ناپذیرتر هستند. در عصر حاضر مطلوبیت‌ها و قابلیت‌های بی کران فضای سایبر از قبیل فراملی بودن، حجم بالای صدمات و خسارات، پنهانی و پوشیده بودن و تأمین راحت منابع مالی، انسانی و فعالیت‌های تبلیغاتی، توجه تروریست‌ها را به خود جلب نموده و منجر گردیده تا آنها خط مشی و اهداف خود را تغییر داده و از دنیای فیزیکی به فضای سایبر رو آورند؛ بطور طبیعی دولت‌ها و گروه‌های مخالف جمهوری اسلامی ایران نیز از این ابزار برای ضربه زدن به منافع و امنیت ملی استفاده می‌نمایند که در راستای پیشگیری و مقابله با تروریسم سایبری، اتخاذ سیاست‌گذاری‌های کلان در این حوزه ضروری می‌باشد. با عنایت به نوین بودن این پدیده علیه امنیت ملی، در حقوق کیفری ایران تعریف صریح و شفافی در خصوص این موضوع موجود نبوده و در ماده ۱۱ قانون جرایم رایانه ای، بدون ذکر عنوان تروریسم سایبری، مصادیق و محتوای بزهی پیش‌بینی گردیده که بسیار نزدیک به تروریسم سایبری بوده و به واسطه همین قصد خاص به خطر انداختن امنیت وآسایش عمومی است که ماده مزبور نزدیک به تروریسم سایبری معرفی شده است. اهمیت پیشگیری و مقابله با تروریسم سایبری از جرم‌انگاری آن کمتر نبوده و این مهم در گرو اتخاذ تدابیر فنی، اجتماعی و توسعه همکاری‌های بین‌المللی می‌باشد که نظر به وابستگی فزاینده زیرساخت‌های حیاتی جامعه به فضای سایبر، پیشرفت فناوری‌های رایانه‌ای و تهدیدات تروریسم، ضروری است با اتخاذ سیاست‌های کلان به ویژه تقویت و تشدید اقدامات امنیتی در سامانه‌های رایانه‌ای و مخابراتی، از هرگونه اخلال در سامانه‌های مزبور توسط تروریست‌های سایبری پیشگیری نمود. در این راستا این نوشتار، ضمن کمبود شدید منابع علمی و حقوقی به دلیل جدید بودن این پدیده، با عنایت به روش تحقیق توصیفی و تحلیلی، بر آن است تا با تبیین مفهوم تروریسم و فضای سایبر، ماهیت و مفهوم تروریسم سایبری را معرفی نموده و عناصر تشکیل دهنده این جرم نوین را بررسی و سپس سیاست‌های جنایی پیشگیری و مقابله با این پدیده را تشریح نماید.

واژگان کلیدی: تروریسم، فضای سایبری، تروریسم سایبری، زیرساخت‌های حیاتی.

---

[۱] نویسنده مسئول: majidba802@gmail.com

مقدمه

درباره سیاست جنایی تعاریف متعدد و متفاوتی از سوی نویسندگان ارائه گردیده است. بررسی مجموعه این تعاریف نشان می‌دهد که دامنه شمول این مفهوم، به تدریج دچار توسعه و گسترش فراوانی شده است. افزون براین، به نظر می‌رسد که گرایش نویسندگان سیاست جنایی به یکی از رشته‌های جرم شناسی، حقوق و جامعه‌شناسی در تعریف ارائه شده از سوی آنان تأثیرگذار بوده است.[۲] بررسی تحولات حقوق کیفری به خوبی نشان می‌دهد که حقوق کیفری تا چه میزان تحت تأثیر آموزه‌های کیفری قرار داشته است. آموزه‌هایی که به ترتیب در جهت جرم مداری (تحت تأثیر مکتب کلاسیک)، مجرم‌مداری (متأثر از مکاتب نئوکلاسیک و تحققی)، بزه دیده مداری (متأثر از تمایلات بزه دیده شناسی نخستین و حمایتی) و عدالت ترمیمی (بهره مند از مدل جامعوی در امر مبارزه با بزه) بوده است. این تحولات که در راستای عقلایی و نیز انسانی کردن مبارزه با بزه و بزهکاری صورت پذیرفت، زمینه باز شدن مفهوم سیاست جنایی را به تدریج فراهم نمود. مارک آنسل نخستین فردی است که تعبیری جدی از سیاست جنایی را ارائه کرده است. او سیاست جنایی را به معنای واکنش سازمان یافته جامعه در مقابل اعمال مجرمانه و ضداجتماعی دانسته است.[۳]

پذیرش نقش جامعه در کنترل جرم و توسعه شمول سیاست جنایی از قلمرو محدود جرم به حالت‌های خطرناک و انحراف، از نوآوری‌های آنسل در قلمرو توسعه مفهومی‌سیاست جنایی است. پس از او باید از نقش شاگرد او خانم دماس مارتی در توسعه و بسط حداکثری سیاست جنایی یاد نمود. او سیاست جنایی را به کلیه شیوه‌ها و روش‌هایی اطلاق نمود که هیأت اجتماع از طریق آن‌ها، پاسخ دهی به پدیده جنایی را سازمان می‌بخشد.[۴]

در واقع سیاست جنایی در تعریف رایج و کلی، به سیاست دولت در مقابله با پدیده مجرمانه گفته می‌شود. با این حال سیاست جنایی دارای تعاریف مختلفی است که عموماً در تعریف خاص معادل سیاست کیفری یعنی مقابله کیفری با جرم دانسته می‌شود ولی در تعریف عام به هر گونه اقدام مستقیم و مؤثر در رویایی با جرم و انحراف اطلاق می‌شود. یعنی نه تنها آسیب شناسی فراتر از شناخت جرم است، بلکه رفع آسیب نیز فراتر از کیفر است. از این نگاه، «سیاست جنایی، نخست علاوه بر جرم که یک مفهوم قانونی است به انحراف (کژروی)که یک مفهوم اجتماعی است نیز می‌پردازد. ۲- علاوه بر سرکوبی و مجازات بزهکاری، به پیشگیری از آن توجه دارد و ۳- علاوه بر اقدام‌های جزایی و نظام کیفری بر تدابیر و نظام‌های اجتماعی، فرهنگی، اخلاقی و... بر همه آنچه در بهداشت و پیشگیری اجتماعی از بزهکاری مؤثر است تکیه می‌کند و بدین سان سیاست جنایی

---

[۲] - حسینی، ، ۱۳۸۳، ص ۲۲

[۳] - می‌ری-(۱۳۸۰). دلماس مارتی، پیشین، ص ۲۳.

[۴] - حسینی، پیشین، ص ۲۸.

از مفهوم سنتی مضیق یعنی سیاست کیفری به سمت مفهوم موسع یعنی سیاست جنایی به معنای امروزی آن تحول می‌یابد.»[۵]

با این حال، در رویارویی با تروریسم سایبری، نه بر مفهوم خاص تأکید می‌شود و نه بر مفهوم میانی آن که از یک سو تنها به جرم اشاره می‌کند و از سوی دیگر علاوه بر تدابیر کیفری ماهوی و شکلی به تدابیر پیشگیرانه نیز نظر دارد، مدنظر است. در تروریسم سایبری با عنایت به حساسیت و اهمیت آن در امنیت ملی، باید پذیرفت که اقدامات کنشی و پیشگیرانه اهمیت بیشتری از اقدامات سرکوبگرانه دارند. از این رو در سال‌های اخیر نسبت به جرایم امنیتی، بر استراتژی‌های کنش گرا در برابر استراتژی‌های واکنش گرا، تأکید بسیاری گردیده است.

انواع جرم‌انگاری تروریسم سایبری

از دیدگاه جرم شناختی، جرم‌انگاری یا جرم تلقی کردن قانونی فعل و یا ترک فعل، فرآیندی است که به وسیله آن رفتارهای جدید، به موجب قوانین کیفری مشمول قانون جزا می‌شوند.[۶]جرم‌انگاری مهم ترین و آشکارترین دستاویز رویارویی با اعمال سرزنش پذیر یا مخاطره آور است.

جرم‌انگاری بازدارنده

منظور از جرم‌انگاری بازدارنده، پیش بینی رفتارهای جزئی یا مقدماتی به عنوان جرم است تا مانعی برای ارتکاب جرایم کلان تر یا مهم تر باشد. برخی از جرایم مقدماتی در فضای سایبر می‌تواند مورد توجه تروریست‌ها قرار بگیرد. این رفتارها هر چند فی نفسه جرم هستند ولی عموماً تروریست‌ها از طریق این رفتارها به اعمال تروریستی خود نزدیک می‌شوند. رفتارهای مقدماتی در واقع حکم جرم بازدارنده را نسبت به تروریسم سایبری پیدا می‌کنند. رفتارهای مطرح شده در این گفتار نسبت به تروریسم سایبری به عنوان جرم‌انگاری بازدارنده مطرح است، از این رو می‌توان از جرم‌انگاری مقدماتی نیز بهره برد و شامل دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه‌ای می باشد.

جرم‌انگاری ابزارمحور

جرم‌انگاری ابزار محور، دلالت بر حمایت کیفری از فضای سایبر دارد تا ابزار یا وسیله تروریست‌ها جهت انجام اقدامات تروریستی قرار نگیرد. جرم‌انگاری ابزار محور بر آن است تا دست تروریست‌ها را از یک وسیله پیچیده و پر امکانات دست کم در برابر انجام برخی رفتارها محروم سازد؛ وسیله ای که در سال‌های اخیر به شدت مورد توجه تروریست‌ها قرار گرفته است.

تبلیغات، افزایش سرمایه، انتشار اطلاعات، ارتباط امن، تأمین مالی، جنگ روانی افزایش سرمایه، گردآوری اطلاعات و جذب نیرو از جمله رفتارهایی هستند که تروریست‌ها از فضای سایبر به

---

[۵] - کریستین لازرژ، ۱۳۸۲، ص۱۴

[۶] - نجفی ابرند آبادی، ۱۳۷۷، ص ۷۶

عنوان ابزار جرم استفاده می‌کنند. دکتر پاکزاد از محققان جرایم رایانه‌ای در ایران، با بررسی قوانین ضدتروریسم برخی کشورها، معتقد است که تروریست‌ها از فضای سایبر برای انجام سه رفتار کلی و عمده بهره می‌برند: تبلیغ، تأمین و تهدید که در ادامه مورد تبیین قرار خواهند گرفت. تبلیغ به جنبه نرم‌افزاری تروریسم یا محتوای آن اشاره دارد که بر اساس آن تروریست‌ها با رفتارهای مختلفی سعی در پیشبرد محتوای اهداف تروریستی خود هستند. تأمین بیشتر به جنبه سخت افزاری یا تدارک نیروی انسانی و مالی می‌پردازد که به موجب آن تروریست‌ها از فضای سایبر برای تشکیلات خود و عملی کردن اهدافشان هم به دنبال نیروی انسانی‌اند، هم مال و هم اطلاعاتی و پشتوانه‌های معنوی.

جرم‌انگاری هدف‌محور

جرم‌انگاری هدف محور، سومین و مهم ترین تدبیر جرم‌انگاری در رویارویی با تروریسم سایبری است. این گفتار حاوی تحلیل انواع رفتارهای ضد فضای سایبر (حمله‌های سایبری) توسط تروریست‌ها است که از طریق سیستم‌های رایانه‌ای و اینترنت انجام می‌شود نمونه‌هایی از موارد یا تهدیداتی که در گذشته وقوع یافته اند یا ممکن است در آینده وقوع یابند آورده شده است. باید توجه داشت در همه این موارد این حمله در فضای سایبر و با استفاده از سامانه‌های رایانه‌ای انجام می‌شوند.

حمله‌های سایبری یا به تعبیر دقیق‌تر حمله‌های بر ضد فضای سایبر را می‌توان در قالب سه رفتار دید که در بیشتر حالات نیز در طول هم قرار دارند. رفتار نخست انتشار نرم افزارهای زیان آور به ویژه ویروس است که با توجه به ویژگی پخش سریع و ناگهانی نرم افزارهای مضر (بدافزارها) از آن‌ها به انفجار سایبری عنوان نموده‌ایم. رفتار دوم تخریب سایبری است که عمدتاً اشاره به از بین بردن یا از کار انداختن سامانه‌ها و شبکه‌های رایانه‌ای است. بدیهی است که تخریب و اختلال می‌تواند نتیجه انتشار نرم افزارهای مضر باشد و در واقع هر جا سخن از تخریب و اختلال به میان آورد می‌توان از ویروس‌ها و دیگر نرم افزارها نیز سخن به میان آورد. در بند دیگری به اخلال سایبری که دو رفتار ممانعت از دسترسی و اختلال در زیرساخت‌های حیاتی شامل آن می‌شود، مورد تبیین قرار می‌گیرد.

پیشگیری از تروریسم سایبری

پیشگیری در لغت به معنای جلوی وقوع چیزی را گرفتن، پیش دستی کردن و پیشی گرفتن و همچنین به معنای آگاه کردن، خبر چیزی دادن و هشدار دادن است.[۷]

۱-پیشگیری وضعی

پیشگیری وضعی به معنای تدابیری است که فرصت‌ها و مناسبت‌های ارتکاب جرم را از طریق ایجاد تغییرات در اوضاع و احوال خاصی که یک انسان متعارف در آن اوضاع و احوال ممکن است

---

[۷] - عمید، ۱۳۶۴، ص ۵۱۰

مرتکب شود، کاهش می‌دهد، کلارک پیشگیری وضعی از جرم را به عنوان اقدامات قابل سنجش و ارزیابی مقابله با جرم می‌داند که معطوف به اشکال خاصی از جرایم بوده و از طریق اعمال مدیریت یا مداخله در محیط بلاواسطه به شیوه‌ای پایدار و سیستماتیک منجر به کاهش فرصت‌های جرم و افزایش خطرات جرم می‌گردد.[۸]پیشگیری وضعی از جرم دارای قدمتی به درازای تاریخ است. زیرا انسان‌ها همواره برای مصون سازی خود از حملات دیگران اقداماتی را انجام داده و راهکارهایی را عملاً در نظر می‌گرفته اند. به موازات تکامل امکانات و پیشرفت‌های حاصل شده در علوم مختلف، پیشگیری وضعی نیز شکل فنی به خود گرفته است.[۹]

پیشگیری وضعی متضمن برهم زدن فرصت و وضعیت تحقق جرم است. پیشگیری وضعی در فضای سایبر متضمن پیش‌بینی تدابیر خاص و فنی است تا امنیت اطلاعات و سیستم‌ها تضمین شود. قابل ذکر است که تدابیر پیشگیرانه وضعی به اعتبار حمایت از هر ارزشی متفاوت است.

۲- سیستم‌های پیشگیری و مقابله با نفوذ[۱۰]

یکی از عملی ترین اشکال تروریسم سایبر، نفوذ به یک سیستم اطلاعاتی با مأموریت حساس، یا هر زیرساخت حیاتی دیگر و اعمال تأثیر مخرب بر دسترس پذیری، محرمانگی و صحت اطلاعات می‌باشد. با استفاده روزافزون از اینترنت در میان عموم، سازمان‌های بیشتری در حوزه تهدید حملات مختلف سایبری قرار می‌گیرند. بنابراین، سازمان‌ها برای محافظت ازسیستم‌های اطلاعاتی خود در چنین شرایطی، از راهکارهای مختلفی برای امنیت شبکه و رایانه بهره می‌گیرند. یکی از این راهکارها استفاده از سیستم‌های ممانعت و کشف ورود غیر مجاز (کشف نفوذ) می‌باشد. کشف نفوذ، فرایندی است شامل مراقبت و تحلیل وقایع حادث در یک رایانه‌ای و شبکه‌های ارتباطی به منظور کشف نشانه‌های نفوذ امنیتی.[۱۱]

سیستم‌های پیشگیری و مقابله نفوذ (IDS) یک نرم افزار، سخت افزار یا ترکیبی از هر دو برای شناسایی فعالیت‌های خصمانه نفوذگری است که از دیواره آتش، آنتی ویروس و دیگر تجهیزات امنیتی عبور کرده و وارد سیستم شده است. این سیستم‌ها به دو دسته سیستم‌های تشخیص نفوذ بر پایه ی امضا[۱۲] و سیستم‌های تشخیص بر پایه ناهنجاری[۱۳] تقسیم می‌شوند[۱۴]

---

[۸] - رز بنام، ۱۳۷۹، ص ۱۴۵

[۹] - ذاقلی، ۱۳۸۹، ص ۱۷۳

[10]- IDS

[۱۱]- لخ یانچوسکی، اندرو ام کلاریک ، ، ۱۳۸۹، ص ۵۶۸،

[12] -Signature Based IDS

[13]- Anomaly Detector

[۱۴] - معاونت حفاظت و امنیت هسته ای، اداره کل حفاظت اسناد و اطلاعات پایه، امنیت در فضای تبادل اطلاعات، مؤسسه فرهنگی- پژوهشی اشارات، ۱۳۹۰، ص۲۳۵

ب) امنیت داده‌ها

امروزه امنیت داده‌ها در شبکه‌ها و سیستم‌های رایانه‌ای یک مسأله مهم برای ادارت و شرکت‌های دولتی و سازمان‌های کوچک و بزرگ به خصوص دستگاه‌های حیاتی و زیربنایی است. تهدیدهای پیشرفته از سوی تروریست‌های فضای سایبر، کارمندان ناراضی و هکرها، رویکردی سیستماتیک را برای امنیت داده‌ها در شبکه‌ها و سیستم‌های رایانه‌ای می‌طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست بلکه یک ضرورت است.

۱- رمزنگاری

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی‌است و برای قرن‌ها بمنظور محافظت از پیغام‌هایی که بین فرماندهان، جاسوسان، عشاق و دیگران رد و بدل می‌شده، استفاده شده است تا پیغام‌های آن‌ها محرمانه بماند.[۱۵]

به رمز درآوردن برای امنیت داده‌ها در ذخیره سازی، انتقال داده‌های حساس و اعتبارسنجی قوی مورد استفاده قرار می‌گیرد. این قابلیت در سراسر محیط فناوری همانند سیستم عامل، نرم افزارهای کاربردی، سیستم‌های مدیریت فایل و پروتکل‌های ارتباطی قابل اجرا است. رمزنگاری را به عنوان کنترل پیشگیرانه و یا کنترل اکتشافی می‌توان استفاده نمود. کنترل پیشگیرانه برای حفاظت از افشاء داده‌ها و کنترل‌های اکتشافی برای کشف تغییرات غیر مجاز و مسئولیت پذیری داده‌ها استفاده می‌شود.[۱۶]

سازمان و نهادهای زیربنایی و حساس باید روش‌های قوی رمزنگاری را برای جلوگیری از افشاء مورد استفاده قرار دهند، تا به راحتی و با صرف هزینه زمانی کم اطلاعات آنان افشاء نشود.

۲- پنهان نگاری[۱۷]

پنهان نگاری به مخفی کردن یک داده سری یا محرمانه از تروریست‌های سایبر در فضای سایبر اطلاق می‌شود به طریقی که اشخاص بی اطلاع از وجود داده پنهانی نمی‌توانند آن را کشف کنند. «پنهان نگاری بر حسب داده‌های رایانه با جایگزینی داده‌های بی فایده یا استفاده نشده در فایل‌های منظم (مثل: تصاویر، فایل‌های صوتی یا اسناد) یا اطلاعات نادیدنی متفاوت، عملی می‌شود. این اطلاعات پنهان می‌توانند متن کشف، متن رمز شده یا حتی تصاویر باشند.»[۱۸] این روش برای سیستم‌هایی مفید است که می‌خواهند به هیچ وجه معلوم نشود که آنها اطلاعات محرمانه را فرستاده یا تبادل می‌نمایند؛ با روش رمزنگاری کلید عمومی، هر چند داده‌ها امن است، هر کسی که آن را ببیند، خواهد دانست آنچه که انتقال یافته، یک پیام رمز شده خصوصی است. با پنهان‌نگاری، حتی این واقعیت محرمانه نگه داشته می‌شود.

---

[۱۵] - قدسی، رهجو، ،ذوالقدر، ۱۳۸۷، ص۲۵۳

[۱۶] - کیان خواه ، ۱۳۸۹، ص ۸۰

[17]- steganography

[۱۸]- ابراهیم نژاد شلمانی، ۱۳۹۰، ص۱۱۷

ج) بدافزارها

امروزه، عموم مردم با ویروس‌های رایانه‌ای آشنایی دارند و آلوده شدن به یکی از انواع ویروس‌ها را حداقل یک بار تجربه کرده اند، اما اگر کمی‌حرفه‌ای تر به این مسأله نگاه شود، می‌توان دریافت که به کار بردن واژه ویروس برای تمام نرم افزارها و فایل‌های مخرب صحیح نیست؛ چرا که ویروس‌ها، تنهایکی از انواع نرم افزارهای مخرب یا بدافزارها به شمار می‌آیند و انواع دیگری همچون اسب‌های تروآ، کرم‌ها و ابزارهای جاسوسی همگی جزء بدافزارها هستند، که هر کدام به نوعی برای صدمه زدن به سیستم‌های رایانه‌ای، سرقت اطلاعات کاربران و تخریب داده‌ها طراحی شده اند.[۱۹]

بدافزار، نرم افزاری مخرب است. از عمده ترین بدافزارها که نیت تخریب و اختلال دارند و مورد استفاده تروریست سایبر قرار می‌گیرد، می‌تواند شامل موارد ذیل باشد:

۱. ویروس‌ها [۲۰]

۲. کرم‌ها [۲۱]

۳. ترآوا[۲۲]

د) کنترل دسترسی

کنترل دسترسی یا بررسی مجوز، بنیادی ترین و فراگیرترین مکانیزم امنیتی مورد استفاده امروز در سامانه‌های رایانه‌ای است. در سیستم‌های رایانه‌ای، ارائه مجوز به معنی تعیین دسترسی یک عامل به یک منبع می‌باشد. به بیان غیر رسمی این به این معنی است که "چه کسی چه کاری می‌تواند انجام دهد". با استفاده از کنترل دسترسی، محرمانگی و صحت اطلاعات حفظ شده و از دستیابی و تغییر فایل‌های حساس توسط هکرها و تروریست‌های سایبر جلوگیری می‌شود.

در سامانه‌های رایانه‌ای، کنترل دسترسی، مجوز انجام یک عملیات (مانند خواندن، نوشتن، اجرا، حذف، جستجو و غیره) توسط یک عامل (از قبیل فرایند، رایانه، کاربر انسانی و غیره) بر روی یک شیء (مانند یک جدول، یک فایل، یک سرویس، یک رکورد در بانک اطلاعات و بطور کلی هر منبعی در سیستم) را بر طبق یک سیاست کنترل می‌نماید. این مفاهیم در اغلب متون مرتبط با امنیت رایانه و کنترل دسترسی قابل مشاهده می‌باشند. سیاست‌های کنترل دسترسی، معرف حقوق دسترسی عامل در یک سیستم رایانه‌ای (براساس راهبرد امنیتی سازمان) می‌باشند. از این رو کنترل دسترسی، باعث ایجاد محافظت در برابر حملات داخلی و افشای اطلاعات در برابر تروریست‌های سایبر می‌گردد. با بهره گیری از یک مکانیزم صحیح بررسی مجوز دسترسی، اعضای غیرمجاز یا تروریست‌های سایبر قادر به دستیابی به ارزشمندترین اطلاعات سیستم نخواهد بود. کنترل دسترسی یک جنبه پر اهمیت از امنیت بوده و برای حفاظت از اطلاعات محرمانه و خصوصی در برابر دسترسی حمله‌کنندگان سایبری ضروری می‌باشد. درک کنترل دسترسی برای

---

[۱۹] - معاونت حفاظت و امنیت هسته ای، اداره کل حفاظت اسناد و اطلاعات رایانه، پیشین، ص ۱۶۳

[20]- Virus

[21]- Warms

[22] -Trojans

درک نحوه مدیریت امنیت اطلاعات اساسی می‌باشد. در طول دهه‌های گذشته مدل‌های مختلفی برای ارتقاء سطح محرمانگی، صحت دسترسی پذیری و انعطاف مدیریت اطلاعات معرفی شده است. این مدل‌ها، معیارهای مشترکی دارند که می‌تواند شامل ساخته شدن بر مبنای مدل‌های ریاضی رسمی(ماتریس، شبکه، و...)، تضمین مجموعه ای از خصوصیات (محرمانگی اطلاعات، صحت مبادلات، عدم تضاد مصالح و...) باشد. [۲۳]

هـ) نظارت سایبری

نظارت و کنترل به معنای دیده‌بانی فضای سایبر است. کنترل برخلاف دو تدبیر حفاظت و پالایش، صرفاً جنبه فنی ندارد و بلکه می‌تواند چهره انسانی نیز داشته باشد؛ یعنی برخی افراد همچون پلیس یا ارائه دهندگان خدمات اینترنتی یا حتی اشخاص و سازمان‌های غیردولتی در پی نظارت و کنترل مبادلات اینترنتی برآیند. بنابراین کنترل و نظارت را می‌توان پلیس سایبری نیز نام گذاشت. نظارت سایبری نهادهای امنیتی و پلیسی نخستین ومهم‌ترین راهکار کنترل تهدیدات اینترنتی و پیشگیری از حمله‌های سایبری است. یکی از طرق معمول کنترل سایبری که بیشتر ناظر به کنترل محتوا است، شنود یا دریافت اطلاعات است. شنود اگر به صورت غیرمجاز باشد فی نفسه جرم بوده و یکی از شیوه‌های مقدماتی برای انجام اقدامات تروریستی به حساب می‌آید ولی از نگاه دیگر نیز همین رفتار می‌تواند پادزهر یا واکنش پیشگیرانه تلقی شده و به عنوان راهکاری برای پیشگیری یا کشف تروریسم سایبری نیز به شمار آید. بنابراین از فن شنود بسته به امکانات وتخصص، دو گروه استفاده می‌کنند: تروریست‌ها و مجرمان سایبری و دولت‌ها. تروریست‌ها و مجرمان سایبری در معرض ارتکاب جرم شنود قرار می‌گیرند و دولت در معرض نقض حریم خصوصی افراد؛ به همین دلیل طبق ماده ۴۸ قانون جرایم رایانه‌ای شنود محتوای در حال انتقال ارتباطات غیر عمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود. طبق تبصره این ماده دسترسی به محتوای ارتباطات غیر عمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.[۲۴]

---

[۲۳] - یانچوسکی، لخ، ام کلاریک،اندرو، پیشین، ص۵۶۴-۵۶۵

[۲۴]- وزارت ارتباطات و فناوری اطلاعات (ICT) هرچند در برابر تروریسم سایبری تاکنون اقدام یا برنامه پیشگیرانه صریحی پیش بینی نکرده ولی نسبت به تأمین امنیت سایبری غافل نبوده است. بر این اساس مرکز تحقیقات مخابرات ایران در نظر دارد در راستای فعالیت آگاهی رسانی، پشتیبانی و امداد امنیت فضای تبادل اطلاعات و برای توسعه زیربخش‌های تخصصی مورد نیاز پورتال مرکزی WWW.ICTCERT.IR، ایجاد آزمایشگاه و گروه امداد تخصصی در زمینه اختلالات امنیتی مرتبط با هرزنامه‌ها در فضای تبادل اطلاعات کشور را درخواست کرده است. موضوع فعالیت، طراحی و ایجاد ازمایشگاه و گروه امداد فضای تبادل اطلاعات آپا در زمینه اختلالات امنیتی مرتبط با هرزنامه‌ها، شامل به کارگیری و اموزش پرسنل، نگارش آئین‌نامه‌ها، پیش بینی مسیرهای گردش کار، تشریح وظایف فردی و قسمتی، و همین‌طور تعیین تجهیزات موردنیاز، خریداری، نصب، راه اندازی این تجهیزات در محدوده زمانی مقرر، و مدیریت سازمان و نگهداری تجهیزات می باشد. ر.ک: www.irancert.ir

و) فیلترینگ

فیلتر یا پالایش داده‌ها از یک نظر همان حفاظت است ولی نه حفاظت داده‌ها و سامانه‌ها بلکه حفاظت کاربرها و مشترکین اینترنتی. به همین دلیل چون نمی‌توان همچون حفاظت از داده‌ها یا سامانه‌ها، دیوارهایی برای حفاظت کاربران کشید، پس باید اطلاعات را غربال کرد و محتویات مجرمانه و غیرقانونی را با تدابیر فنی پالایش کرد.[۲۵]

در دنیای رایانه واینترنت فیلتر دارای معانی و همین‌طور کاربردهای مختلفی است. فیلتر برنامه یا مجموعه‌ای از ویژگی‌های یک برنامه است که ورودی استاندارد یا مشخص شده را می‌خوانند، ورودی را به شکل مورد نظر تبدیل می‌کند و سپس خروجی را در مقصد استاندارد یا مورد نظر می‌نویسد. همین‌طور فیلتر الگو یا ماسکی است که داده‌ها از آن عبور داده می‌شوند تا اقلام مشخص شده کنار گذاشته شوند؛ به عنوان مثال فیلتری که در پست الکترونیکی یا بازیابی پیام‌های گروه خبری به کار برده می شود و به کاربران امکان می‌دهد تا پیام‌ها را از دسترس کاربران دیگر دور نگه دارند. اما از همه مهم‌تر بیشترین کاربرد فیلتر در ارتباطات است که در اینجا به سخت‌افزار یا نرم‌افزاری گفته می‌شود که برخی از عناصر یک سیگنال را عبور می‌دهد و مابقی را حذف یا به حداقل می‌رساند. به عنوان مثال در یک شبکه ارتباطاتی باید فیلتری طراحی شود تا فرکانس خاصی را عبور دهد اما از عبور فرکانس‌های بالاتر و پایین‌تر جلوگیری کند.[۲۶]

پیشگیری اجتماعی

بموجب پیش نویس لایحه پیشگیری از وقوع جرم در بند الف ماده یک این لایحه، پیشگیری اجتماعی عبارت است از تدابیر و روش‌های آموزشی، فرهنگی، اقتصادی و اجتماعی دولت و نهادها و سازمانهای غیر دولتی و مردمی‌در زمینه سالم سازی محیط اجتماعی و محیط فیزیکی برای حذف یا کاهش عوامل اجتماعی وقوع جرم. در واقع پیشگیری اجتماعی از جرم به معنای اتخاذ تمهیدات و تدابیر اجتماعی و عمومی برای فراهم نمودن بستری است که جرم ارتکاب نیابد یا میزان آن کاهش یابد. تدابیری از قبیل آموزش و اطلاع رسانی، ایجاد ضوابط رفتاری، مدیریت و کنترل از جمله راهکارهای پیشگیری اجتماعی در تروریسم سایبری اشاره گردیده که در ادامه مورد تبیین قرار می‌گیرد.

الف) آموزش و اطلاع رسانی

آموزش و اطلاع رسانی یکی از راه‌های اساسی برای پیشگیری از تهدیدات سایبری به خصوص تروریسم سایبری است. آگاهی و اطلاع رسانی و برنامه‌های آموزشی می‌توانند افراد به خصوص کارمندان را نسبت به خطرها و زیان‌های بالقوه سایبری، حساس و مطلع کند و به آن‌ها استفاده از فناوری‌ها و شیوه‌های امنیتی را آموزش دهد. «این برنامه‌ها می‌توانند در زمینه‌های آموزش امنیت فیزیکی و پرسنلی و همچنین امنیت فضای رایانه‌ها، مفید باشند. می‌توان کارمندان را در مورد

---

[۲۵] - بتول پاکزاد، پیشین، ص ۴۵۴

[۲۶] - فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت، کانون نشر علوم، ص ۳۰۳

مهندسی اجتماعی آگاه کرد و نحوی شناسایی و اجتناب از آن‌ها را آموزش داد. مدیران سیستم را می‌توان در امنیت اطّلاعات آموزش داد تا بتوانند به درستی، سیستم‌ها را پیکربندی و بر آن‌ها نظارت کنند. مدیران سیستم و دیگر کارمندان را می‌توان نسبت به مسئولیت‌هایشان در مورد اعمال و حوادث امنیتی آموزش داد.»[۲۷]همچنین می‌توان با ایجاد سایت‌های خاص، نسبت به آموزش عمومیو آگاهی شهروندان پرداخت.

اطلاع رسانی نسبت به تهدیدات سایبری، هم می تواند جنبه آموزشی داشته باشد و هم جنبه هشدار دهی.

در قوانین اخیر التصویب ایران، اطلاع‌رسانی اینترنتی به صورت کلی مورد تأکید قرار گرفته شده است؛ از جمله قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران مصوب ۱۳۸۳ به صورت پراکنده به ارزش اطلاع‌رسانی رایانه‌ای و اینترنتی اشاره کرده است.

ب) ایجاد ضوابط رفتاری

ضوابط رفتاری یا کدهای رفتاری، «مجموعه‌ای از قواعد است که بر پایه قبول مسئولیت‌ها یا انجام رفتارهای شایسته از سوی افراد یا سازمان‌ها است. ضوابط رفتاری شامل ضوابط اخلاقی و نیز ضوابط مقدس که مبتنی بر اندیشه‌های مذهبی و والا است، می‌شود.»[۲۸] می‌توان گفت در برخی زمینه‌ها ضوابط رفتاری همانند مقررات کیفری حائز اهمیت بوده و برخی از این کدهای رفتاری از سوی سازمان بین‌المللی نیز پیشنهاد گردیده‌اند.

به گفته لسیگ[۲۹]«چهار دسته از قواعد در فضای سایبر حاکم‌اند: قواعد قانونی، قواعد هنجاری، قواعد تجاری و قواعد فنی. در این میان به جهت اقتضائات فضای سایبر و حاکمیت فرهنگ آزاد در این فضا، باید قواعد قانونی به سمت قواعد هنجاری سوق داده شود.»[۳۰] ضوابط هنجاری در این نگاه نه تنها در مقام جایگزینی با قوانین هستند بلکه به جهت ماهیت آزاد گونه و کنترل‌ناپذیر چنین فضایی مناسب‌تر و کارآمدتر هستند؛ از این روست که به تدریج بحث «ضابط شهروند سایبری» نیز مطرح شده است.[۳۱] در سال ۱۹۹۰، کمیته خط مشی اطلاعات، رایانه و ارتباطات سازمان توسعه و همکاری اقتصادی، اقدام به تشکیل گروهی از کارشناسان جهت آماده سازی رهنمودهایی برای امنیت سیستم‌های اطلاعات کرد. این گروه متشکل از نمایندگانی از کشورهای عضو سازمان توسعه و همکاری، متخصصانی در رشته‌های حقوق، ریاضیات، علوم رایانه‌ای و نمایندگانی از بخش خصوصی بود. این گروه در طی یک دوره ۲۰ ماهه، شش بار تشکیل جلسه داد تا سرانجام نسخه نهایی گزارش خود را به نام «رهنمودهایی جهت امنیت سیستم‌های اطلاعات» برای تصویب به کمیته خط مشی ارتباطات مخابرات تحویل داد این رهنمودها در اکتبر ۱۹۹۲ توسط کمیته مذکور تصویب شد و در ماه نوامبر توسط ۲۴ کشور عضو سازمان همکاری و

---

[۲۷]- داروتی، ای دنینگ، ۱۳۸۸، ص ۴۷۰

[28] - http//en.wikipedia.org/wiki/code of conduct

[29]- Lawrence Lessig فعال آمریکایی در زمینه قانون زدایی از کپی رایت، علائم تجاری و مانند آن

[30]- http//en.wikipedia.org/wiki/code_and_other_laws_of_cyberspace

[31]- http//www.washburn.edu/ccc

توسعه پذیرفته شد. هدف، ارائه مبنایی برای توسعه و اجرای سازوکارها و شیوه‌هایی برای تسهیل امن ساختن اطلاعات بود.

ج) مدیریت و کنترل

از آنجا که ریشه‌های تروریسم در وضعیت سیاسی، اقتصادی، اجتماعی و فرهنگی جوامع نهفته است و بدون توجه به این علل و تلاش برای از بین بردن نابرابری‌ها در سطح ملی و جهانی نباید امیدی به پیروزی در مبارزه با تروریسم داشت، لذا توجه به توسعه همه جانبه و معیارهای حکمرانی و مدیریت مطلوب حائز اهمیت است.

اهمیت مدیریت و حکمرانی مطلوب در توسعه جوامع و رفع نابرابری‌ها در اعلامیه اجلاس جهانی برای توسعه اجتماعی در سال ۱۹۹۵ به خوبی منعکس شده است: «دموکراسی، حکمرانی و مدیریت شفاف و پاسخگو در همه بخش‌های جامعه، بنیان حیاتی و ناگزیر برای حقیقت بخشیدن به توسعه پایدار اجتماعی و انسانی است».

فضای سایبر و شکل‌گیری جامعه اطلاعاتی چالش‌ها ی جدیدی را در این خصوص ایجاد نموده است.زیرا از سویی این جهان جدید در انحصار دولت‌ها نیست، و از سوی دیگر دهکده جهانی با شهروندانی جهانی ایجاد نموده است که مفاهیم نابرابری را از درون مرزهای ملی فراتر برده و شهروندان آن درصدد دستیابی به برابری در سطح جهانی هستند. «اولین واحتمالاً آشکارترین مانع برای مفهوم شهروندی جهانی اشکال پیچیده سلسله مراتبی و نابرابری است که نظم جهان را تهدید می‌کند»[۳۲] . به همین لحاظ است که در جهت رفع این نابرابری که بخشی از آن ناشی از شکاف دیجیتال می‌باشد و تأمین دسترسی برابر به اطلاعات تلاش‌های گسترده جهانی صورت گرفته است. قطعنامه‌های متعدد سازمان ملل و تشکیل اجلاس‌های منطقه‌ای و جهانی درباره جامعه اطلاعاتی، اقدامات گروه هشت، اتحادیه بین‌المللی مخابرات و.... در این راستا قابل توجه می‌باشد.

نکته مهم، توجه به پیشگیری از جرم در جامعه اطلاعاتی است در اعلامیه فوق، از تمامی بازیگران جامعه اطلاعاتی خواسته شده از طریق فعالیت‌های مناسب و قانونی و اقدامات پیشگیرنده از استفاده نادرست از فناوری اطلاعات در ارتباطات اجتناب کنند و به ابعاد اخلاقی جامعه اطلاعاتی یعنی احترام به صلح و ارزش‌های بنیادی و اصولی شامل آزادی و برابری و.... توجه داشته باشند.[۳۳]

د) امنیت مهندسی اجتماعی

مهندسی اجتماعی مفهومی‌است که تمامی‌ترفندهای روانشناسی که افراد را در به خطر انداختن امنیت خود تشویق می‌کنند، در بر می‌گیرد.

---

[۳۲] - پیتر ویلکن، ۱۳۸۱، ص ۱۴۰

[۳۳] - همان، ص ۱۷۵ به بعد

برای انجام حمله ای از نوع مهندسی اجتماعی، مهاجم با بهره برداری از آسیب پذیری‌های رفتاری انسان‌ها، آن‌ها را فریب داده و متقاعد می‌کند که اطلاعاتی را در اختیار او قرار دهند یا کاری را انجام دهند. در این نوع حمله، فرد حمله کننده می‌تواند به کمک مهارت‌های اجتماعی خود با افراد ارتباط برقرار کرده و سپس به اطلاعات حساس سازمان دسترسی پیدا کند. به علاوه، روش‌های مهندسی اجتماعی می‌تواند به صورت رایانه‌ای نیز بکار گرفته شوند و کاربران را وادار نمایند که پیوست یک پست الکترونیکی را باز نمایند، دکمه ای را فشار دهند، در فرمی اطلاعات شخصی و محرمانه خود را وارد نمایند تا لینکی را دنبال نمایند.[۳۴]

روش‌هایی که در حمله‌های مهندسی اجتماعی به کار گرفته می‌شود، در هر حمله منحصر به فرد می‌باشد. اما در بیشتر موارد، وسیله و روش کلی استفاده شده در این حمله‌ها، مشترک است. از جمله این روش‌ها حضور در محل هدف می‌باشد در واقع تروریست‌های سایبری می‌توانند با جعل نمودن هویتشان، وانمود کنند که کارمند بخش پشتیبانی، تعمیرات و نگهداری یا غیره می‌باشند. سپس با تقلید نقش آن هویت جعلی، به راحتی وارد محیط مورد نظر خود شده و به جستجو در آن جا بپردازند. مهاجم می‌تواند در همین مرحله، به بخش‌های مورد نظر خود در سازمان زیربنایی و حیاتی نفوذ کرده و اطلاعات مورد نظر را به دست آورد، یا از اطلاعات حاصل از جستجوی خود برای کشف راه‌های نفوذ بعدی بهره جوید و همچنین داده‌ای رایانه‌ای را مختل یا از بین ببرد.

همکاری‌های بین‌المللی

در عصر حاضر لزوم و اهمیت همکاری‌های بین‌المللی در مقابله با جرایم رایانه‌ای بر کسی پوشیده نیست، لیکن موانعی بر سر راه این همکاری‌ها وجود دارند که باید رفع شوند. عملاً در غالب موراد، ارتکاب جرایم رایانه‌ای جنبه فراملی پیدا می‌کنند. در جرایم سنتی یک کشور می‌توانست به دلیل نادر بودن موارد از همکاری‌های بین‌المللی چشم پوشید، اما در شرایطی که امور حیاتی و روزمره آحاد جامعه به شبکه پیوند بخورد، دولت‌ها نخواهند توانست به دلیل فراهم نکردن شرایط همکاری بین المللی، از تعقیب مجرمان سرباز زنند؛ چرا که در غیر این صورت نخواهند توانست پاسخگوی جمع کثیری از بزهدیدگان باشند که به عنوان اساسی ترین حقوق، از دولت انتظار حمایت و دادخواهی دارند و به دادگاه‌ها مراجعه خواهند نمود.[۳۵]

از سوی دیگر عدم هماهنگی کشورها، سبب خواهد شد کشورها به دو قطب مخالف تبدیل شوند؛ برخی کشورها که در برخورد با جرایم رایانه‌ای ضعیف عمل می‌کنند به «بهشت جرایم رایانه‌ای» یا «پناهگاه جرایم رایانه‌ای» بدل خواهند شد و در مقابل کشورهایی که سطح برخورد مناسبی با

---

[۳۴] - معاونت حفاظت و امنیت هسته ای، اداره کل حفاظت اسناد و اطلاعات پایه، امنیت در فضای تبادل اطلاعات، مؤسسه فرهنگی- پژوهشی اشارات، ۱۳۹۰، صص ۱۴۲-۱۴۳

[۳۵] - اصل ۳۴ قانون اساسی جمهوری اسلامی‌ایران ذیل فصل مربوط به حقوق ملت مقرر داشته است: «دادخواهی حق مسلم هر فرد است و هر کس می‌تواند به منظور دادخواهی به دادگاههای صالح رجوع نماید ...»

جرایم رایانه‌ای دارند به «بهشت داده‌ها» یا «پناهگاه داده‌ها » بدل خواهند شد در نتیجه جریان آزاد اطلاعات بین این دو قطب دچار اختلال خواهد شد. [۳۶]

بسته به ماهیت تروریسم سایبری، به واقع باید اذعان داشت که مهم ترین چاره رویارویی با این پدیده، همکاری‌های بین‌المللی است. پدیده ای که مرز را نشناسد و مرتکبش خود را از اجرای قوانین داخلی کشورها دور ببینند، تنها با اجماع جهانی یا دست کم منطقه ای می‌توان پاسخی در خور به وی داد. از این رو شاید نسبت به هیچ پدیده ای به اندازه ی تروریسم سایبری، همکاری‌های بین المللی احساس نمی‌شود.[۳۷]

به لحاظ ویژگی‌های خاص تروریسم سایبری محققین سعی در ارئه الگو یا اصولی برای هر نوع همکاری بین المللی برای مقابله با آن داده اند که می‌توان به تحلیل مفصل لاکایسک[۳۸] از واکنش نسبت به جرایم سایبری و تروریسم سایبری اشاره نمود.

همکاری‌های بین المللی می‌تواند در سه سطح مطرح شود. در سطح نخست توافق دو یا چند کشور در مبارزه با تروریسم که بر خلاف دیگر پدیده‌های مجرمانه، در اینجا همسایه بودن شورها تأکید نمی‌شود. در سطح دوم، همکاری‌های در سطح منطقه ای که در این زمینه منطقه اروپا تأثیرگذارترین و موفق ترین کارایی را در مبارزه با تروریسم و تروریسم سایبری داشته است و در برابر منطقه آسیا هنوز نتوانسته بر صدور حتی یک سند ارشادی بین المللی در هر زمینه ای بویژه تروریسم اقدام کند. سطح جهانی که ناظر بر مشارکت همه کشورهای جهان به تعبیر حقوقی همه کشورهای عضو سازمان ملل متحد است. در بادی امر به نظر می‌رسد که فضای سایبر تنها با همکاری‌های یکدست و فراگیر جهانی، می‌تواند از شر تهدیدات تروریسم سایبری رهایی پیدا کند در ادامه به این سه سطح از همکاری‌ها اشاره می‌گردد[۳۹]:

الف) همکاری‌های دوجانبه

همکاری‌های دو جانبه در زمینه موضوعات حقوقی و امنیتی و به تبع آن تأکید بر استرداد مجرمین یکی از راهکارهای شناخته شده برای مقابله طرفینی با پدیده‌های مجرمانه است، که یا به جهت محل وقوع جرم یا متواری شدن متهم یا معماری‌های دیگر، لزوم همکاری بین المللی را مشخص می‌کند. این شیوه هر چند در برابر یک پدیده جهان مانند تروریسم سایبری، کمتر کارایی دارد و بیشتر در روابط دو یا چند کشور می‌تواند مؤثر واقع شود، ولی باید گفت در قاره آسیا که امکان شکل گیری اتحادیه به سختی قابل تصور است، توافق‌های دو جانبه یکی از راهکارهای مناسب و ابتدائی تلقی می‌گردد.

---

[۳۶] - حبیبی ، ۱۳۷۳، ص ۳۵۱.
- اولریش زیبر، ۱۳۸۳ ص ۱۹۸

[۳۷] - پاکزاد، ۱۳۹۰، ص ۵۴۴

[38]-Lukasik, 2005, pp.125-184

[۳۹] - پاکزاد، پیشین، ص ۵۴۷

ایران یکی از کشورهایی است که برای مبارزه با تروریسم و نیز جرایم رایانه‌ای بر توافقات دو جانبه تأکید دارد با آنکه قوانین داخلی دوباره تروریسم مبهم هستند ولی مقنن ایران نسبت به تهدیدات بین المللی تروریسم و نیز امکان فرار مرتکب بی اعتنا نبوده است؛ از این رو، مبارزه با تروریسم یا پیشگیری از آن در قوانین مرتبط با توافق نامه‌های دو جانبه ایران با سایر کشورها با تأکید و شفافیت بیشتری آمده است.

طبق قانون موافقتنامه امنیتی، انتظامی و مبارزه با مواد مخدر بین دولت جمهوری اسلامی‌ایران دولت جمهوری یونان مصوب ۱۳۷۹/۲/۲۷ مجلس شورای اسلامی،طبق بند الف ماده ۱، یکی از موارد همکاری در مقابله با تروریسم بین المللی و دیگر اعمال جناحی که ماهیت تروریستی دارند، است.

بر اساس قانون موافقت‌نامه همکاری امنیتی میان جمهوری اسلامی ایران و پادشاهی عربستان سعودی مصوب ۱۳۸۰/۴/۱۷ مجلس شورای اسلامی‌دولت ایران و عربستان با عنایت به روابط برادرانه اسلامی و دوستانه دو کشور و اهمیت مسایل امنیتی توافق کرده اند. بر اساس ماده ۱ این موافقت‌نامه، طرف‌های متعاهد در راستای تأمین امنیت و مقابله مؤثر با کلیه جرایم، به ویژه جرایم سازمان یافته و تروریسم، با انجام اقدامات شناسایی، پیشگیری و کشف جرایم و مبارزه با آنها در زمینه‌های زیر همکاری می‌نمایند:

۱- مبارزه با جعل اسناد دولتی، پول کارت‌های اعتباری و اسکناس و فروش غیر قانونی آنها و نیز جرایم اقتصادی از جمله تطهیر پول
۲- قاچاق اسلحه، مهمات و مواد منفجره
۳- قاچاق کالا و میراث فرهنگی
۴- تجاوز به جان، مال و تجاوز به عنف و اعمالب منافی عفت عمومی.

ب) همکاری‌های منطقه‌ای

در زمینه همکاری‌های منطقه‌ای چه در زمینه تروریسم و چه در زمینه جرایم رایانه‌ای، منطقه اروپا از همه مناطق جهان پیشتازتر است. در زمینه تروریسم، مناطق جهان در مبارزه با تروریسم یا پیشگیری از آن، اسنادی را پیش‌بینی کرده اند. در کنار قاره‌ها، مناطق فرو قاره‌ای مانند اتحادیه عرب (۱۹۹۸) و کشورهای آسه آن (۲۰۰۷) نیز دوباره مبارزه با تروریسم کنوانسیون‌هایی را تصویب کرده اند. همچنین باید به اقدامات آسه آن در مورد تروریسم سایبری نیز اشاره نمود. گروه کشورهای انجمن ملل آسیای جنوب شرقی که بیشتر با نام اختصاری آسه آن شناخته می‌شود تا کنون به طور خاص پنج سمینار در مورد تروریسم سایبری برگزار نموده‌اند. آخرین آن در سنگاپور در ۲۰۰۸ برگزار گردید. در این سمینار ضمن تأکید بر همکاری برای مبارزه با تروریسم سایبری، وزرا از تأسیس نشست مجازی متخصصین در زمینه تروریسم سایبری و امنیت سایبری استقبال

کردند و وزرای جمهوری کره و فیلیپین برای رهبری گروه در سال نخست اعلام آمادگی کردند.[۴۰] در زمینه جرایم رایانه‌ای، تنها در منطقه اروپا اقدام مؤثر انجام شده و آن هم تصویب کنوانسیون جرایم سایبر در سال ۲۰۰۱ در بوداپست است که به تصویب شورای اروپا رسید و از آن به بعد مبنای روابط میان اعضای شورا و سایر کشورهای جهان در مورد جرایم سایبری شد. این امر که مطابق اعلام این شورا این کنوانسیون طرح کنوانسیون سازمان ملل برای سایر کشورها نیز خواهد بود اهمیت دو چندان آن را می‌رساند[۴۱].

شورای اروپا در این کنوانسیون که به منزله یک قانون مؤثر برای مقابله با جرم‌های سایبری است، مبارزه با تروریسم سایبری را هنجارمند نموده است. مواد ۲- ۱۰ این کنوانسیون در بردارنده انواع جرم‌ها و مواد ۱۱-۱۳ نیز حاوی مقررات کلی مربوط همه جرایم با عنوان ضمانت اجراها و مسئولیت‌های تبعی است. جرم‌های مذکور در کنوانسیون تحت عناوین جرایم علیه محرمانگی، تمامیت و دسترس پذیری سیستم‌ها و داده‌های رایانه‌ای، جرایم ربوط به رایانه، جرایم مرتبط با محتوا با نقض حق نشر و حقوق مربوط به آن آمده است. به ویژه عنوان نخست هر چند به تروریسم سایبری اشاره نکرده است ولی جرایم مقدماتی تروریسم سایبری و نیز رفتارهایی که تنها با انگیزه سایسی چهره این پدیده را به خود می‌گیرند مانند تخریب و اخلال داده یا سامانه‌های رایانه‌ای را جرم دانسته است. این سند همچنین به مقررات شکلی و پیشگیرانه مرتبط با مبارزه با جرایم سایبری اشاره کرده است.

پیشرفته ترین سیستم همکاری‌های حقوقی بین المللی در کنوانسیون جرایم سایبری شورای اروپا در سال ۲۰۰۱، خصوصاً در فصل ۳ کنوانسیون، یافت می‌شود مثلاً ماده ۲۴ شامل مقررات استرداد مجرمین به دولت متبوعه است و در مواردی که در بردارنده جرایم خاص رایانه‌ای مطابق با ماده‌های ۲ الی ۱۱ است قابل اعمال می‌باشد، مشروط به آنکه مجرمین تحت قوانین هر دو طرف مربوطه قابل مجازات باشند. فصل ۳ نیز حاوی مقررات مشروح خاص رایانه‌ای برای همکاری متقابل است، از جمله همکاری در حیطه‌های حفاظت فوری از داده‌های رایانه‌ای ذخیره شده، افشای فوری داده‌های ترافیک حفظ شده، دسترسی به داده‌های رایانه‌ای ذخیره شده، جمع آوری فوری داده‌های ترافیک و شنود داده محتوا همچنین اصولی کلی را در رابطه با همکاری متقابل، محرمانگی و محدودیت در استفاده را فراهم می‌آورد و مسئله اطلاعات فوری را مطرح می‌سازد. ماده ۲۷ بند ۴ به کشور طرف درخواست امکان رد همکاری را در صورتی که آن خواسته در رابطه با جرمی باشد که طرف درخواست شونده، آن را جرمی سیاسی تلقی کند یا چنانچه احتمال دهد اجرای درخواست موجب لطمه زدن به استقلال، امنیت، نظم عمومی یا دیگر مصالح ضروری خواهد شد، می‌دهد.در هر حال برای مقابله بین المللی با تروریسم سایبری به ویژه در قالب توسل

---

[40]-htto//www.ioc.utokyo.ac.jp/~worldgpn/documents/texts/arf/2008724.OIE.html Singapore July 24, 2008 ASEAN

[۴۱] - پاکزاد، خرداد ۱۳۸۳، ص ۱۰۳

به جرم‌انگاری برخی رفتارهای ناقض هنجارهای سایبری، تا کنون تصویب کنوانسیون بوداپست راجع به جرایم محیط سایبری مهم ترین اقدام ماهوی و شکلی بوده است.
باید اشاره نمود که علاوه بر گسترش همکاری‌های دو جانبه، همکاری‌های جهانی در قالب رهنمودهای سازمان ملل متحد به ویژه قطعنامه‌ها خود تأثیر بسزایی در امر مقابله با تروریسم سایبری دارد، که در بند بعدی به آن پرداخته می‌شود.

ج) همکاری‌های جهانی

همکاری‌های جهانی در مبارزه با تروریسم بیشتر پیرامون کنوانسیون‌های سازمان ملل متحد درباره تروریسم و قطعنامه‌های شورای امنیت می‌چرخد. از دید اسناد بین المللی تروریسم دارای یک مفهوم عمومی است که مصادیق فراوان می‌تواند داشته باشد. رویکرد حقوقی مقابله با تروریسم بین المللی که در قالب کنوانسیون‌ها پروتکل‌های بین المللی تبلور یافته، کلی نگر نبوده بلکه مبتنی بر جرم‌انگاری و پرداختن به خشن ترین و رایج‌ترین مصادیق تروریسم بین المللی است، هر کدام از این اسناد مشتمل بر فهرست یا توصیفی عینی از جرایم ممنوعه است و اقداماتی مشخص را برای سرکوبی و مجازات آنها مقرر داشته است؛ « با اتخاذ چنین نگرش بخشی و عمل‌گرایانه‌ای، نظام ملل متحد توانسته است منظومه‌های حقوقی برای جلوگیری و مجازات بسیاری از اعمال تروریستی عرضه کند.[۴۲] اگر چه هر سند بین‌المللی به جرمی جداگانه مربوط می‌شود اما همه آنها ویژگی‌های مشترکی دارند از جمله: رویکرد موردی به جرم تروریسم بین المللی، مسئولیت کیفری که عموماً متوجه اشخاص حقیقی است،[۴۳] غیر سیاسی تلقی کردن جرایم تروریستی، اصل استرداد یا محاکمه[۴۴] و الزام دولت‌ها به همکاری با یکدیگر. کلیه این اسناد، دولت‌های عضو را ملزم می‌سازد که با یکدیگر، همکاری قضایی کنند.
همچنین طبق این اسناد، دولت‌های عضو ملزم اند جرایم فهرست شده، را در قوانین داخلی خود قابل مجازات بشناسند و صلاحیت اولیه و اصلی[۴۵] را درباره این جرایم (مانند جرایم ارتکابی در قلمرو خودشان یا توسط اتباعشان) اعمال کنند. وانگهی تمام دولت‌های عضو ملزم اند بر هر جرمی‌که متهم آن، متعاقباً در سرزمین آنها حضور پیدا کرده باشد، صلاحیت فرعی[۴۶] خود را اعمال نمایند.

---

[۴۲] -پترس غالی، ۱۳۸۴ ص، ۳۳۲

[۴۳]- از بین کنوانسون بین المللی مقابله با تروریسم « کنوانسیون بین المللی مبارزه با تأمین مالی تروریسم » به مسئولیت کیفری اشخاص حقوقی اشاره دارد . در ماده ۵ کنوانسیون مزبور مقرر شده است که اگر مدیر یا شخصی اداره کننده شخص حقوقی به اعتبار سمت و صلاحیت خود در شخص حقوقی مزبور مسئولیت کیفری، مدنی یا اداری داشته باشد . این مجازات می‌تواند شامل مجازات‌های مالی نیز باشد؛ ولی تا تحقق مسئولیت کیفری برای دولت‌ها به جهت اعمال تروریستی هنوز نیاز به تحولی در این زمینه وجود دارد.

۲-AUT dedere aut judicare .

۳. Primary jurisdiction .

۴. Secondary Jurisdiction .

تاکنون هیچ کنوانسیون خاصی تحت عنوان تروریسم سایبری تصویب نشده است. اما کنوانسیون های موجود در خیلی از موارد قابلیت اعمال در مورد تروریست سایبری را دارد.
از دیگر اسنادی که به تصویب مجمع عمومی‌سازمان ملل متحد رسید، «کنوانسیون بین المللی مبارزه با تأمین مالی تروریسم» است که در تاریخ ۹ دسامبر ۱۹۹۹ به تصویب مجمع عمومی رسید. کنوانسیون، سه تعهد عمده برای کشورهای عضو در نظر گرفته است:
۱- جرم‌انگاری تأمین مالی اعمال تروریستی در قوانین ملی خود.
۲- همکاری گسترده با سایر کشورهای عضو و ارائه معاضدت قضایی در موضوعات مربوط به کنوانسیون.
۳- وضع مقررات و الزامات مربوط به ایفای نقش مؤسسات ملی در کشف و گزارش دهی موارد اعمال تروریستی.[۴۷] هدف مهمی‌که در قالب اسناد مورد بحث دنبال شده است، هماهنگی بین المللی در قوانین شکلی و ماهوی در رویارویی با اقدامات تروریستی است.
همکاری‌های جهانی در مقابله با تروریسم سایبری به اسناد مذکور ختم نمی‌شود، بلکه اسناد و تصمیمات مشورتی و ارشادی متعددی راجع به تروریسم به ویژه پس از سپتامبر ۲۰۰۱ پیشنهاد شده است که مقابله با تروریسم سایبری را نیز می‌توان از لابه لای آنها جست. البته برخی از قطعه نامه‌های شورای امنیت در راستای پیشگیری و زمینه سازی یک فضای اطلاعاتی سالم تأثیر بسیاری در الگودهی به کشورهای عضو سازمان داشته است از جمله قطعنامه‌های ۲۰۵۷۲۳۹ دسامبر ۲۰۰۲ در مورد ایجاد فرهنگ جهانی امنیت سایبری ۴۵۵۶۳ دسامبر ۲۰۰۰ و ۱۹۵۶۱۲۱ دسانبر ۲۰۰۱ در مورد ایجاد مبانی قانونی مبارزه با سوء استفاده مجرمانه از فناوری‌های اطلاعاتی و ۴۵۳۷۰ دسانبر ۱۹۹۸ ـ ۱۵۴۴۹ دسامبر ۱۹۹۹ ـ ۲۰۵۵۲۸ نوامبر ۲۰۰۰ ـ ۲۹۵۶۱۹ نوامبر ۲۰۰۱ ـ ۲۲۵۷۵۳ نوامبر ۲۰۰۲ـ ۱۰ ـ ۱۶ هماهنگی در مورد پیشرفته‌ای در زمینه ارتباطات و اطلاعات در مورد امنیت بین المللی.

نتیجه گیری

فضای سایبر دنیای بی‌کرانی از امکانات و قابلیت‌های بی شمار است که بدون محدودیت در دسترس همگان قرار دارد و هرکس با هر انگیزه و هدفی می‌تواند از این موهبت بهره برداری کند. بی تردید تروریست‌ها هم خود را از این قاعده مستثنا نمی‌دانند. آن‌ها می‌توانند از امکانات بی شمار این فضا در جهت تحقق اهدافشان بهره‌برداری کنند. تروریسم سایبری، پدیده ای انکار ناپذیر و تأثیرگذار در حوزه سیاست جنایی بیشتر کشورهاست و از سوی دیگر تهدیدی جدی و نوین برای زمان حال یا خطری بزرگ برای آینده ای بسیار نزدیک است که تا حدودی تهدیدات و خطرات دیگر بر ضد امنیت ملی را تحت الشعاع قرار خواهد داد. عمق تهدید تروریسم سایبری در ورای ارتباط گسترده و تنگاتنگ زیرساخت‌های حیاتی کشورها با فضای مبادلات الکترونیکی یا

---

[۴۷] - طیبی فرد، ۱۳۸۴، ص ۲۷۱

همان فضای سایبر نهفته است و این زیرساخت‌ها در معرض شدیدترین و پیچیده ترین حمله‌ها قرار دارند. حقوق کیفری ایران، حتی نسبت به خود تروریسم نیز سرگردان بوده و موضع مشخصی ندارد ولی با این حال با بررسی قوانین و مقررات کیفری می‌توان به پذیرش پراکنده اعمال تروریستی سایبری از دید تقنینی صحه گذاشت. پیش از دانستن این که حقوق کیفری ایران چه از تروریسم سایبری اندوخته و چه میزان از آن را پذیرفته است باید برای بار دیگر به طور کلی به جلوه‌ها و رفتارهای تشکیل دهنده مجموعه جرایمی با عنوان تروریسم سایبری اشاره گردد. تروریسم سایبری در مفهوم موسع شامل همه انواع اقدامات تروریستی در فضای سایبر می‌باشد؛ اعم از آن که فضای سایبر وسیله یا پشتیبان اقدامات تروریست‌ها باشد و یا این که این محیط هدف و سیبل حمله‌های آنها قرار بگیرد.قانونگذار ایران، هنوز به طور راستین اقدام تروریستی را به عنوان یک بزه جداگانه و ناوابسته از دیگر بزه‌های امنیتی، پیش بینی نکرده است؛ از این رو نمی‌توان چشم داشت که اقدام تروریسم سایبری که خود گونه ای از اقدام تروریستی است، را در قانون‌های کیفری جای داده باشد. با این حال ماده ۱۱ قانون جرایم رایانه ای، بدون نام بردن از اقدام تروریستی یا تروریسم، بزهی را پیش بینی نموده که بسیار نزدیک به تروریسم سایبری است و آن اخلال رایانه ای همراه با قصد است و بواسطه همین قصد خاص است که ماده مزبور به تروریسم سایبری نزدیک است. برای پیشگیری و مقابله با تروریسم سایبری، ضرورت گسترش همکاری‌های بین المللی در عصر حاضر مسجل می باشد. در فضای سنتی و با شیوع تروریسم بین‌المللی، تقریباً بیشتر کشورها پذیرفته اند که مقابله با تروریسم جز با همکاری‌های بین المللی امکان پذیر نیست. این نکته در مورد تروریسم سایبری برجسته تر است و به علت اینکه فضای سایبری، مکان وقوع جرم است و این مکان نیز بدون مرز و بدون محدودیت است؛ امکان سرزمینی کردن مقابله با تروریسم سایبری وجود نداشته یا محکوم به ناتوانی و ناکامی است. رویارویی مؤثر در برابر اقدامات تروریستی سایبری مستلزم هماهنگ سازی حقوق کیفری ماهوی و شکلی کشورها، بهبود همکاری‌های بین المللی و اقدامات پیشگیرانه مانند حفاظت از زیرساخت‌ها و تأمین امنیت فضای سایبر دارد.

منابع و مراجع

ابراهیم نژاد شلمانی، محمد آشنایی با جنگ نرم، جلد یک، تهران، بوستان حمید، ۱۳۹۰، ص۱۱۷
اولریش زیبر، جرایم رایانه‌ای، ترجمه نوری، محمد علی، نخجوانی، رضا، بختیاروند، مصطفی، رحیمی‌مقدم، احمد، تهران، گنج دانش، چاپ اول، ۱۳۸۳ ص ۱۹۸
پاکزاد، بتول اقدام‌های سازمان‌های بین المللی و منطقه‌ای در خصوص جرم‌های رایانه‌ای، مجموعه مقالات همایش بررسی جنبه‌های حقوقی فن آوری اطلاعات، خرداد ۱۳۸۳، ص ۱۰۳
پترس غالی، سازمان ملل متحد و اقدامات جامع حقوقی برای مبارزه با تروریسم بین المللی، ترجمه دکتر سید قاسم زمانی، در کتاب « تروریسم » نشر نی، چاپ دوم، ۱۳۸۴ ص، ۳۳۲
پیتر ویلکن، اقتصاد سیاسی ارتباطات جهانی و امنیت انسانی، ترجمه مرتضی بحرانی، پژوهشکده مطالعات راهبردی، چاپ اول، ۱۳۸۱، ص ۱۴۰
حبیبی حسن ، منطق حقوقی و انفورماتیک حقوقی؛ تهران: اطلاعات، چاپ اول، ۱۳۷۳، ص ۳۵۱.
حسینی، سید محمد سیاست جنایی در اسلام و در جمهوری اسلامی‌ایران، انتشارات دانشگاه تهران، چاپ اول، تهران، ۱۳۸۳، ص ۲۲
داروتی، ای دنینگ، جنگ اطلاعات و امنیت، ترجمه: گروه مترجمان: جواد شیخ زادگان، محمودرضا روحانی، محمد علی حسین نژاد، تهران، مؤسسه فرهنگی هنری پژّوشکده پردازش هوشمند علائم، چاپ دوم، ۱۳۸۸، ص ۴۷۰
ذاقلی عباس ، قاچاق انسان در سیاست جنایی ایران و اسناد بین المللی، تهران، نشر میزان، چاپ اول، ۱۳۸۹، ص ۱۷۳
رز بنام، دنی و لوریسیو، آرتور و داویس، روبرت، پیشگیری وضعی از جرم، ترجمه رضا پرویزی، مجله حقوقی دادگستری، شماره ۳۲، ۱۳۷۹، ص ۱۴۵
طیبی فرد، امیر حسین مبارزه با تأمین مالی نرو در اسناد بین المللی، مجله حقوقی، شبکه ۳۲، ۱۳۸۴، ص۲۷۱
عمید، حسن فرهنگ فارسی عمید، تهران، انتشارات امیر کبیر، چاپ ششم، ۱۳۶۴، ص ۵۱۰
قدسی ابوالفضل ، محسن، رهجو، محسن، ذوالقدر، ضد تروریسم مجازی، موسسه تحقیقاتی و پژوهشی، چاپ اول، ۱۳۸۷، ص۲۵۳
کریستین لازرژ، درآمدی به سیاست جنایی، ترجمه علی حسین نجفی ابرند آبادی، نشر میزان، چاپ اول، تهران، ۱۳۸۲، ص۱۴
کیان خواه، احسان مدیریت امنیت اطلاعات، تهران، انتشارات ناقوس، ۱۳۸۹، ص ۸۰
لخ یانچوسکی، اندرو ام کلاریک ، مقدمه ای بر جنگ سایبر و تروریسم سایبر،جلد دوم، ترجمه: ابراهیم نژاد شلمانی، محمد، تهران، بوستان حمید، ۱۳۸۹، ص ۵۶۸،
معاونت حفاظت و امنیت هسته ای، اداره کل حفاظت اسناد و اطلاعات پایه، امنیت در فضای تبادل اطلاعات، مؤسسه فرهنگی- پژوهشی اشارات، ۱۳۹۰، ص۲۳۵
معاونت حفاظت و امنیت هسته ای، اداره کل حفاظت اسناد و اطلاعات رایانه، پیشین، ص ۱۶۳

می‌ری- دلماس، مارتی، ۱۳۸۱، نظام های بزرگ سیاست جنایی (مفاهیم و مدل ها)، ترجمه علی حسین نجفی ابرندآبادی، تهران، نشر میزان، چاپ اول.

نجفی ابرند آبادی علی حسین ، حمیدها شم بیگی، دانشنامه جرم شناسی، انتشارات شهید بهشتی، چاپ اول، تهران، ۱۳۷۷، ص ۷۶

Lukasik, S. J; Current and future technical capabilities. In.Ssofear,A.D & Goodman, S E.(Eds), the transnational dimension of cybercrime and terrorism Stanford, CA: Hoover Institution Press Publication, 2005, pp.125-184