سیاست جنایی اجرایی جمهوری اسلامی ایران در مقابله با تروریسم سایبری

امیرحمزه عرب پور[1]- محمدرضا شادمان فر[2]*

تاریخ دریافت: ۱۳۹۹/۰۵/۸- تاریخ پذیرش: ۱۳۹۹/۰۶/۱۲

چکیده:

فضای مجازی که اخیرا دنیا را به دهکده کوچکی تبدیل کرده محیطی معد ارتکاب جرایم است. اتصال به فضای سایبر بر دامنه پیچیدگی‌ها افزوده و مسایل اجتماعی نوینی را در رابطه با بزهکاران و بانیان نظام دادگری جنایی به وجود آورده است. هدف اصلی این مقاله شناسایی و تبیین پدیده کاملا جدی و خطرناک تروریسم سایبری، بیان عوامل تهدید زیرساخت‌های دولتی و صنعتی و ارائه راه کارهای اجرایی مناسب و پیشرفته دولت در پیشگیری و مقابله با تروریسم سایبری است. در نهایت پیرامون فضای سایبری در ایران و راه کارهای مقابله با تروریسم سایبری می‌توان به کلیه اقداماتی که قوه مجریه در راستای پیشگیری از تروریسم سایبری لحاظ نموده اشاره داشت، و بی تردید توسعه صنایع بومی با فناوری‌های نوین از جمله رایانش ابری و معماری سرویس‌گرا مهمترین عامل در ایجاد امنیت ملی در چنین شرایطی است.

واژگان کلیدی: سیاست جنایی، جرایم سایبری، سیاست جنایی اجرایی، تروریسم سایبری، پیشگیری

---

[1]- دانشجوی دکتری تخصصی گروه حقوق کیفری و جرم شناسی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران amirhamzeh.arabpour@yahoo.com

[2]- استادیار و عضو هیئت علمی گروه حقوق کیفری و جرم شناسی، دانشگاه آزاد اسلامی، واحد اصفهان (خوراسگان)، اصفهان، ایران: نویسنده مسئول

Mrsh23@gmail.com

مقدمه

همانطور که می‌دانیم، ماهیت علوم را اطلاعات تشکیل می‌دهد؛ عنصری که به دلیل اهمیت فوق العاده‌اش، عصر حاضر به آن نام گرفته است. (آنجلیز،۱۷:۱۳۸۳) به همین ترتیب، رشد هر حوزهٔ علمی به فرآوری و پردازش صحیح، دقیق و هرچه سریعتر اطلاعاتش وابسته است. لذا آنچه نیمهٔ دوم قرن بیستم را از دوره‌های پیشین متمایز کرده است، دستیابی بشر به یک پردازشگر بسیار سریع در عین حال مطمئن به نام «رایانهٔ الکترونیکی» است که سوئیچ اولین نمونه آن با نام کامپیوتر عددی الکترونیکی[1](ENIAC) در سال ۱۹۴۶ چرخانیده شد. (Casey,-2001:32) رایانه و اینترنت یک فناوری جدید است و مانند هر فناوری دیگری تا زمانی که استفاده از رایانه و اینترنت عمومیت پیدا نکرده بود هیچ پیش فرض درباره مزایا و مخاطرات احتمالی آن وجود نداشت. اما حالا به تدریج زوایای بسیاری از آن آشکار می‌شود. چند دهه ایست که رایانه و اینترنت همه گیر شده است و در مناسبات اجتماعی و فرهنگی، اقتصادی و سیاسی جای خود را یافته است به نحوی که در جوامع پیشرفته استفاده از آن به عنوان یک ضرورت مطرح شده است و روز به روز رسوخ سیستم‌های رایانه‌ای در اینترنت گسترش یافته است. (لک و عنایتی،۵۴:۱۳۹۵)

گسترش فزاینده «فناوری اطلاعاتی و ارتباطاتی» منجر به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. ویژگی‌های جوامع امروزی همچون «اقتصاد اطلاعاتی»، «فرهنگ مجازی»، «کاهش اهمیت زمان و مکان در تعاملات اجتماعی»، ویژگی متمایزی به هزاره سوم بخشیده که اصل بنیادین آن اهتمام محوری فرد در عرصه فعالیت‌های اجتماعی، سیاسی و اقتصادی با بهره گیری از ابزارهای نوین اطلاعاتی و ارتباطی است. در چنین فضایی که با عنوان «فضای مجازی»[2] توصیف می‌شود، تهدیدهای نوینی همانند: «جنگ مجازی»،«جنگ اطلاعاتی»[3]،«تروریسم سایبری»[4]،پدیده«هکرها»[5]،«واکرها»[6]، «کراکرها»[7] و «سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی» پدید آمده‌اند که می‌توانند امنیت ملی کشورها را با چالش جدی مواجش سازند. به علاوه، پیشرفت فنی در زمینه ارتباطات، موجب

[1]- Electronic Numerical Integrator and Computer
[2]- Cyberspace
[3]-Information warfare
[4] -Cyber terrorism
[5]- Hackers
[6]- Walkers
[7]- Crackers

ظهور قواعد حقوقی و به تبع آن، رفتارهای نوین فاصله گیر از هنجارها شده است که این موضوع، نه تنها اموال، بلکه اشخاص و دولت‌ها را نیز در بر می‌گیرد و آنها را تحت حمایت قرار می‌دهد. (جلالی فراهانی،۱۳۸۷: ۴۰-۴۱) یکی از این تهدیدات نوین، تهدیدات مربوط به تروریسم سایبری است که با توجه به تنوع و تعدد گروه‌های تروریستی در محیط امنیتی جمهوری اسلامی ایران و برنامه ریزی نظام سلطه برای بهره گیری از ظرفیت‌های گروه‌های تروریستی به منظور بی ثبات سازی و ایجاد اخلال در نظم و امنیت کشور، به یکی از مهمترین چالش‌های فراروی نظام مبدل گردیده است. با نگاهی به افزایش رخدادها و حمله‌های سایبری علیه بیشتر کشورهای توسعه یافته و بروز خسارات شدید در زیرساخت‌های حیاتی، می‌توان به فاجعه آمیز بودن نتایج حملات سایبری علیه سیستم‌های رایانه‌ای و دارایی‌های اطلاعاتی پی برد که تأثیرات شدیدی بر امنیت فیزیکی، اقتصاد ملی یا ایمنی همگانی خواهد گذاشت. طی سالیان اخیر دشمنان نظام ایران بخصوص ایالات متحده امریکا و اسرائیل با استفاده از قابلیت‌های فضای سایبر کوشیده‌اند ابعاد نوینی از جنگ نرم[1] و تروریسم سایبری را بر ضد کشورمان شکل دهند. لاکور معتقد است که تروریسم سایبری ممکن است برای تعداد کثیری از مردم بسیار ویران کننده تر از جنگ‌های بیولوژیک یا شیمیایی باشد. ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی در دسترس عموم، پنهان بودن و عدم شناسایی، کاهش هزینه‌های اقدامات تروریستی و نیز امکان تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده از ویژگی-های اقدامات تروریسم سایبری است که آن را به مقوله‌ای جذاب در بین عوامل و گروه‌های تروریستی مبدل ساخته است.(حسن بیگی،۱۳۸۴:۱۱)

سیستم جنای تقنینی، نمایانگر دیدگاه قانونگذار نسبت به موضوع جرم است. گرایش به تدابیر سرکوبگر کیفری یا اقدامات پیشگیرانه و اصلاحی ابتدا در سیاست جنایی تقنینی نمود پیدا می‌کند و موفقیت یا عدم موفقیت سیاست جنایی در دستیابی به اهداف خود به اتخاذ یک سیاست جنایی تقنینی منسجم و مناسب بستگی دارد. در همین راستا به جهت اهمیت تعیین مرجع و مقام مسئولی برای اجرای برنامه‌های پیشگیری، قوانین و مقررات مصوب موجود ایران را مورد بررسی قرار دادیم. هدف پژوهش حاضر بررسی رابطه میان ویژگی‌های وضعیت تقنینی با ارتکاب تروریسم سایبری در فضای مجازی، اقدامات تروریستی سایبری صورت گرفته علیه ایران در سالهای اخیر، موانع پیش رو در نظام حقوقی تقنینی ایران در برخورد با این دسته

[1] -Soft War

از جرایم و چالش‌ها و در نهایت ارائه پیشنهادات و راهکارهایی برای بهبود رویکرد سیاست جنایی تقنینی در قبال تروریسم سایبری است تا از این طریق هم درک صحیحی از چهره تغییر یافته تروریسم سنتی در فضای سایبر در عصر جدید فناوری اطلاعات حاصل آید و در عین حال سیاست تقنینی جمهوری اسلامی ایران مورد تحلیل و بررسی قرار گیرد.

مفهوم شناسی

پیشگیری واکنشی یا کیفری

پیشگیری واکنشی از نظر مانوی اقدامی پسینی است، پس از ارتکاب رفتار مجرمانه با استفاده از ابزارهای کیفری از رهگذر نظام عدالت کیفری اعمال می‌شود. این پیشگیری براساس اثری که بر جامعه و یا فرد بزهکار می‌گذارد، به دوگونه «پیشگیری واکنشی عام» و «پیشگیری واکنشی خاص» تقسیم می‌شود. پیشگیری واکنشی عام یک پیشگیری واکنشی جمعه مدار یا گروه مدار است که با مخاطب قرار دادن شهروندان از طریق رعب انگیزی و عبرت آموزی جمعی، به دنبال پیشگیری از بزهکاری نخستین افراد است. پیشگیری واکنشی خاص یک پیشگیری واکنشی مجرم مدار است که با اعمال کیفر بر فرد بزهکار و با رعب انگیزی و عبرت آموزی فردی، درصد پیشگیری از بزهکاران دوباره افراد است. (نیازپور،۱۳۹۱: ۱۷۲-۱۷۰)

این نوع پیشگیری که دارای قدمت طولانی در تاریخ بشر است، در جوامع گذشته به عنوان تنها راهکار مبارزه علیه جرم و مجرم تلقی می‌شد. پیشگیری کیفری که در مرحله بعد از ارتکاب جرم اعمال می‌شود، با استفاده از کیفر و مجازات که اثر آن رعب و وحشت در بزهکاران است، به اصلاح بزهکاران می‌پردازد. (رحیمی نژاد،۱۳۹۵:۱۱۰)

به طور کلی، پیشگیری واکنشی یا کیفری، ناظر به اقدام کیفری قبل و بعد از وقوع جرم است که با بهره گرفتن از ساز و کارهای نظام عدالت کیفری درصد کاهش نرخ بزهکاری است. رهیافت پیشگیری واکنشی، ارعاب انگیزی فردی، جمعی و عبرت آموزی می‌باشد تا از بزهکاری نخستین و بزهکاری دوباره افراد جلوگیری کند. (عباسی،۱۳۸۳:۶۳)

سیاست جنایی[1]

اصطلاح سیاست جنایی تولین بار توسط فوئرباخ به کار گرفته شد. وی سیاست جنایی را «مجموعه اقدامات سرکوبگر و کیفری می‌داند که دولت از طریق آنها در مقابل جرم، واکنش نشان می‌دهد». (لواسور،۱۳۷۲:۳۹۸)

[1]- criminal policy

کوش دانشمند فرانسوی (قرن۲۰) در تعریف سیاست جنایی می‌گوید: «یک علم کاربردی که هدف آن موفقیت عملی در سازماندهی عقلانی و مؤثر مبارزه با جرم است». (لازرژ،۱۳۸۱: ۱۳؛ رشادتی، ۱۳۸۷:۳۴۰)

سیاست جنایی از نظر لغوی به معنای تدبیر و تدبر چاره اندیشی برای پدیده مجرمانه که در قلمرو سیاست جنایی شامل انحراف و جرم می‌شود، آمده است. این تدبیر و تدبر ممکن است در قالب شیوه‌های مختلف رسیدگی و پاسخ‌های گوناگونی برای رویارویی با جرم با انحراف متصور و معمول شود. (نجفی ابرند آبادی،۱۳۷۹:۱۳)

دکتر جعفری لنگرودی در تعریف سیاست جنایی چنین می‌نویسد: « سیاست جنایی یعنی اتخاذ اصول و تدابیر لازم در برابر جرائم و دفع آنها و یا کاستن آنها». (جعفری لنگرودی،۱۳۸۷: ۱۲۲۱)

سیاست جنایی رشته‌ای ست که حسب یافته‌های فلسفی و علمی و طبق مقتضیات تاریخی کوشش می‌کند تا به تدوین« نظریه‌های کیفری و پیشگیری جرایم که در عمل مفید واقع گردد، بپردازد ». به اعتقاد وی، جرم معلول عوامل فردی و اجتماعی بوده و لذا سیاست اجتماعی و سیاست جنایی را از یک دیگر جدا کرده و تصریح نمود موضوع سیاست اجتماعی (پیشگیری اجتماعی) حذف کامل یا حداقل محدود ساختن شرایط اجتماعی جرم است، در حالی که سیاست جنایی در جایی که با بزهکار خاص سر و کار می‌یابد، نمایشگر مبارزه علیه جرم به وسیله تأثیر فردی علیه بزهکار است.(نوربها، ۱۳۷۰:۱۳۲)

مفهوم سیاست جنایی از بدو تولد خلقت تا به امروز تطورات و تحولات فراوانی را به خود دیده است به طوریکه نتیجه این فرایند، فربه تر شدن این اصطلاح از آغاز تا زمان کنونی شده است. بدین گونه که به طور کلی مفهوم سیاست جنایی از ابتدا تا اکنون به دوصورت متفاوت، از مضیق شروع شده و با رویکرد موسع به اوج رسیده است. آغازگر این اندیشه در سال ۱۸۰۳ میلادی، فویر باخپروفسور آلمانی است که با به کار بردن اصطلاح سیاست جنایی در کتاب حقوق کیفری خویش، برای اولین بار این اصطلاح را وارد قلمرو حقوق کیفری نمود، از دیدگاه او سیاست جنایی، شامل مجموعه شیوه‌هایی سرکوبی می‌شود که دولت از طریق آنها و با توسل به آنها علیه جرم واکنش نشان می‌دهد. (دلماس مارتی،۱۳۸۱:۲۳)

سیاست جنایی اجرایی

در تعریف سیاست جنایی اجرایی می‌توان گفت: سیاست جنایی اجرایی نوعی سیاست است که از سوی دولت و قوه مجریه به عنوان رکن اجرایی کشور جهت تطبیق و اجرای سیاستهای

اتخاذ شده توسط سیاست جنایی تقنینی، در پیش گرفته می‌شود. در مفهوم مضیق سیاست دولت یا قوه مجریه در زمینه کنترل جرم که ناظر بر چگونگی اجرای قوانین و رویه قضایی موجود است، سیاست جنایی اجرایی را تشکیل می‌دهد. (رضوانی،۱۳۷۷:۱۳۷۷۱۷)

در سطح بین‌الملل، با توجه به ساختار نظام‌های حاکم بر کشورها این مفهوم اجرایی است و به خوبی درک می‌شود که سیاست جنایی اجرایی ایران فراتر از دولت و قوه مجریه مورد استفاده در مفهوم مضیق می‌باشد. در نتیجه سازمانها و نهادهای وابسته به سایر قوانین در این بخش فعالیت دارند. نحوه اجرای تدابیر سرکوبگرانه یا پیشگیرانه علیه پدیده مجرمانه جایگاه خاصی در بین انواع سیاست جنایی دارد. (لازرژ،۱۳۷۵:۹)

تروریسم[1]

تروریسم از کلمه ترور مشتق شده است که از ریشه لاتین (ترس) به معنای ترساندن است. (کوشا،۱۳۸۹:۸) در عبارت کامل به معنای نظام وحشت و ترور تعریف می‌شود. تروریست کسی است که با کمک فعالیت‌های نظامی و هراس افکنی در تلاش برای پیش برد دیدگاه‌های خود است. در تعریف دیگر بر پایه دانشنامه بریتانیکا تروریسم به معنی"کاربرد سیستماتیک ارعاب یا خشونت پیش بینی ناپذیر بر ضد حکومت‌ها، مردمان یا افراد برای دستیابی به یک هدف سیاسی است. (طیب،۱۳۸۴:۲۱) تاریخ استفاده از کلمه تروریسم به زمان انقلاب فرانسه و اوایل حکومت جمهوری خواهان در زمان ژاکوب (۱۷۹۳-۱۷۹۴) باز می‌گردد. (سروش‌نژاد،۱۳۸۷:۵۷)

از دید حقوقدایان تعاریف زیادی برای تروریسم بیان شده است اما در عرصه‌هایی تعریف دقیق و یکسانی پیرامون تروریسم وجود ندارد و این مسئله بیشتر به جنبه سیاسی تروریسم بر می‌گردد تا جنبه حقوقی آن، حتی یکی از دلائل مخالفان عدم شمول تروریسم در صلاحیت دیوان کیفری بین‌المللی عدم تعریف مشخص و واضح از تروریسم بود. (قربان نیا،۱۳۸۳:۱۶۰)

تروریسم واژگانی است که ریشه در فرهنگ غرب دارد و از این رو در کتب قدیم اهل لغت به چنین واژه‌ای برخورد نمی‌کنیم. این واژه نخستین بار در سال ۱۹۷۶ و در متمم فرهنگ لغات فرهنگستان علوم فرانسه ظاهر شد و آن را وجود نظام یا رژیم وحشت معنا کرد. فرهنگ اصطلاحی دالوز تروریسم را اقدام سیاسی خشونت آمیز افراد یا اقلیت‌های سازمان یافته علیه اشخاص، دارایی‌ها و نهادهایی می‌داند که برای نیل به اهدافی نظیر کسب استقلال از یک دولت، سرنگونی رژیم حاکم و مبارزه علیه برخی جنبه‌های سیاسی یک دولت صورت می‌گیرد

[1]-terrorism

تروریسم سایبری[1]

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 ارایه شده است. «سایبر تروریسم بیشتر به معنای حمله یا تهدید علیه رایانه‌ها، شبکه های رایانه‌ای و اطلاعات ذخیره شده در آنها است، هنگامی که به منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیش برد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود. در تروریسم کلاسیک مواد منفجره و سلاح‌های گرم اصلی‌ترین ابزار تروریسم کلاسیک وجود دارند، اما مهمترین ابزار سایبر تروریست‌ها رایانه است. در واقع آنها ترجیح می‌دهند به جای بمب از بایت استفاده کنند. اساسی‌ترین روش‌های سایبر تروریسم عبارت است از هک کردن، ویروس‌های رایانه‌ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دستکاری اطلاعات و یا حامل‌های داده الکترونیکی. دلایل زیادی وجود دارد که سبب می‌شود سایبر تروریسم، برای تروریست‌ها جذاب باشد. (Barry, 1359)

کراساوین تروریسم سایبری را « استفاده از فناوری و اسباب اطلاعاتی به وسیله گروه‌ها و عوامل تروریستی» می‌داند. به تعریف استارک اشکالات متعددی وارد است از جمله اینکه:

اولا: پدیده تروریسم اصولا مورد توجه قرار نگرفته است و امکان دارد حمله مورد نظر استارک اصلا یک حمله تروریستی نباشد. در این تعریف هیچ قرینه‌ای که بر تفکیک تروریسم سایبری از جرم عادی دلالت کند وجود ندارد، چرا که به طور مثال ممکن است این حمله تجاوز به یک کارت خودپرداز بانکی و سرقت وجوه آن باشد؛ این پدیده را به هیچ وجه نمی‌توانیم یک عمل تروریستی قلمداد کنیم هرچند توسط گروهی تروریست واقع گردیده باشد. ثانیا؛ تروریسم سایبری زمانی مصداق دارد که بر علیه سازمان‌ها و سرویس‌های زیر بنایی و خدمات ضروری باشد. این تعریف به هیچ وجه بیانگر این امر نیست و شامل کلیه جریان‌های اطلاعاتی می‌گردد. ثالثا؛ به انگیزه و قصد مرتکب هیچ توجهی نشده است. (krasavin,2002:2)

امنیت فضای سایبر و زیر ساخت‌ها

در حوزه فناوری اطلاعات و ارتباطات، دو نوع امنیت برای یک کشور متصور است: امنیت زیر ساخت‌های حیاتی و امنیت فضای سایبر که امنیت زیر ساخت‌ها به عنوان یک اصل برای رسیدن به امنیت درحوزه فضای سایبر است و زمانی می‌توان در مورد امنیت در فضای سایبر

[1] -Cyber terrorism

بحث کرد که از امنیت زیر ساخت‌ها مطمئن باشیم. بنابراین برای رسیدن به یک راهبرد در ارتباط با امنیت فضای سایبر باید مولفه‌های اصلی در امنیت زیر ساخت‌ها را نیز مورد بررسی قرار دهیم. (Matsuura, 2003:3)

اگرچه زیر ساخت‌های حیاتی یک کشور ممکن است در بخش‌های مستقلی فعال باشند، اما برای قرار گرفتن در این فضا برای خود و سایرین، مشکلات امنیتی به وجود نیاورند. نصب دیواره‌های آتش، اطمینان از شبکه بندی‌های داخلی، استفاده از تکنیک‌های موثر در رمزنگاری اطلاعات، اطمینان از عدم سرقت و نشست اطلاعات و هرگونه تهدید شبکه‌ای از وظایف اداره کنندگان این زیرساخت‌ها می‌باشد و پس از آنکه اطمینان لازم از امنیت آنها به وجود آمد می-توان تمهیدات لازم را برای استقرار فضای سایبر یعنی ایمن سازی ارتباطی بین زیرساختها به وجود آورد. براساس بیانیه‌های جهانی، ارتباطات، تولیدنیرو، منابع نفت و گاز، بانکداری و امور اقتصادی، حمل و نقل، کشاورزی و دفاع از زیر ساختارهای اصلی دولت به عنوان منابع هر کشوری هستند که هرگونه خدشه در عملکرد و یا حملات تروریستی علیه آنها باعث ضربه جبران ناپذیر دفاعی و اقتصادی می‌گردد. (Moteff,2003:4)

امنیت شامل سه عنصر پایه‌ای است:۱- محرمانگی[1] ۲- یکپارچگی[2] ۳- در دسترس بودن[3]

محرمانگی: به این معنا که اگر داده‌هایی که در فضای سایبری در حال انتقال هستند، توسط مهاجمین خوانده شوند و محرمانه بودن آن نقض شود.

یکپارچگی: اگر در حین انتقال داده‌ها در فضای سایبری (به عنوان مثال در یک شبکه اطلاعات توسط مهاجمین دستکاری شده و تغییر داده شوند) به آن چیزی اضافه یا از آن کم شود.

در دسترس بودن: این نوع حملات با هدف خارج کردن منبع اطلاعاتی از سرویس به گونه‌ای که دیگر آن منبع قادر به ارائه سرویس به دیگران نبوده و نتواند تبادل اطلاعات درستی با کاربرانش داشته باشد، انجام می‌شود. (میرزایی ورزنه،۱۳۹۵:۲۰۱)

متاسفانه در نظام بین‌الملل دادگاه یا دیوانی مستقل که بتواند به جرایم ناشی از فعالیت‌های تروریستی رسیدگی کند، وجود ندارد. در بسیاری از کشورها هنوز قوانینی راجع به جرایم رایانه‌ای و اینترنتی تدوین نشده است و این موضوع یعنی وجود خلاءهای قانونی که نیروهای امنیتی را در مقابله با جرایم رایانه‌ای و اینترنتی، سردرگم نموده و توانایی واکنش به موقع و

[1]- Confidentiality
[2]-Integrity
[3]- Availability

مناسب را از آنان می‌گیرد. همچنین در این محیط نمی‌توان از اقدامات سنتی برای نظارت در فضای سایبری سود برد. زیرا به قول جانت رنو دادستان آمریکایی در فضای سایبر یک هکر نیازی به گذرنامه ندارد و در هیچ معبری بازرسی نمی‌شود. (Podgar & Wayne, 2004) .. در زمینه جرم انگاری تروریسم سایبر، در حقوق ایران با خلاء قانونی روبرو هستیم؛ قانون جرائم رایانه‌ای هم، اگرچه یکی از کاملترین قوانین در زمینه جرائم مربوط به فضای مجازی و رایانه‌ای است، لیکن در خصوص جرم انگاری تروریسم سایبر، صراحت ندارد. با این حال، برای رفع خلاء قانونی در حوزه جرم انگاری تروریسم سایبر، می‌توان برخی مواد مذکور در این قانون را، ملاک عمل قرار داد. به لحاظ مجازات کیفری مرتکبان و برخورد با این پدیده کیفری، از آنجا که حملات تروریستی سایبری، عمدتاً همان جرائم رایانه‌ای با اهداف خاص تروریستی می‌باشند، علاوه بر اقدام از بستر قانون جرائم رایانه‌ای، باید به طور مصداقی با اینگونه رفتارها، بر مبنای جرائم علیه امنیت و آسایش عمومی در قانون مجازات اسلامی و برخی دیگر مقررات و آئین نامه‌ها پیگیری و اقدام نمود. (مسعودی،۱۳۹۴:۱)

دولت با وضع قوانین ویژه، افراد را به رعایت و اتخاذ اقدامات و تدابیر و مقررات امنیتی لازم و اولیه ملزم می‌نماید. در واقع سیاست جنایی تقنینی، وظیفه قانون‌گذاری در یک کشور است که در کشور ما بر اساس قانون اساسی بر عهده مجلس شورای اسلامی و در موارد خاص بر عهده نهادهای دیگر گذاشته شده است. البته فرآیند قانون‌گذاری توسط مجلس انجام می‌شود اما در فرآیند تهیه و تنظیم یک پیشنویس قانونی تا تصویب آن، تحقیقات علمی، افکار عمومی، روشنفکران، گروه‌های فشار، سازمان‌های مستقل، احزاب و به ویژه رسانه‌های گروهی در آگاه سازی مردم، نحوه تصویب، نوع تصویب، مفاد قوانین آینده و ... نقش مهمی را بر عهده دارند. (باصری،۱۳۸۷:۳۶)

اقدامات قوه مجریه در راستای پیشگیری از تروریسم سایبری

با افزایش نگرانی حاصل از پیشرفت و درگیر شدن امور اجرایی کشور با فضای سایبر و خدمات الکترونیک، سازمان‌های متولّی فناوری اطلاعات و نهادهای امنیتی کشور، اقدام به تأسیس و راه اندازی مراکز متعدد به منظور مقابله با تهدیدات سایبری، به خصوص تروریسم سایبری، به منظور مقابله با تهدیدات و پیشگیری از بزه‌دیدگی ناشی از حملات تروریستی سایبری اقدام نموده‌اند. بی تردید تأسیس مراکز امنیتی و مقابله‌ای، یکی از راهکارهای افزایش خطرات ارتکاب جرم است که بزهکاران بالقوه را از اندیشه ارتکاب چنین جرایمی به دلیل وجود احتمال

دستگیری و ردیابی آنها باز می‌دارد. بنابراین در ذیل به بیان و توضیح مختصر نهادها و سازمان-های درگیر با تهدیدات سایبری و فعالیت‌های پیشگیرانه و مقابله‌ای آنها اشاره می‌گردد:

وزارت ارتباطات و فناوری اطلاعات

به عنوان اصلی‌ترین سازمان عهده دار علوم و فنون مرتبط با صنایع الکترونیک، مخابرات، ارتباطات رادیویی و رایانه‌ای در سال ۱۳۸۲ تأسیس گردید. با توجه به قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، عمده وظایف و اختیارات وزارت مذکور عبارت‌اند از:

«تدوین سیاست‌ها و ضوابط کلی در زمینه توسعه ارتباطات و فناوری اطلاعات، طراحی و تدوین نظام ملّی فناوری اطلاعات کشور، نظارت کلان بر فعالیت‌های بخش غیردولتی در امور مربوط به مخابرات، پست، پست بانک، خدمات هوایی پیام و فناوری اطلاعات، تدوین و پیشنهاد استانداردهای ملّی مربوط به ارتباطات و فناوری اطلاعات در کشور». (ماده سه قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، مصوب ۱۳۸۲)

اقدام وزیر ارتباطات و فناوری اطلاعات در ممنوع ساختن واردات نرم افزارهای امنیتی در بهمن ماه سال ۱۳۹۰، یکی دیگر از اقدامات این سازمان در ایمن سازی فضای سایبر و جلوگیری از سوءاستفاده و جاسوسی تولیدکنندگان خارجی در ارائه نرم افزارهای امنیتی است.

سازمان‌ها و نهادهای زیر مجموعه این سازمان، اقدامات شایان توجهی را در زمینه پیشگیری و اقدامات مقابله‌ای، به منظور مبارزه با تهدیدات سایبری از جمله تروریسم سایبری اتخاذ نموده‌اند. عمده‌ترین سازمان‌های زیرمجموعه وزارت ارتباطات و فناوری اطلاعات، عبارت‌اند از: سازمان تنظیم مقررات و ارتباطات رادیویی، شرکت ارتباطات زیرساخت، سازمان فناوری اطلاعات که در ذیل به تشریح اقدامات مقابله‌ای آنها پرداخته می‌شود.

- سازمان تنظیم مقررات و ارتباطات رادیویی

این سازمان، یکی از سازمان‌های وابسته به وزارت ارتباطات و فناوری اطلاعات است که با استناد به ماده هفت قانون وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات، در تاریخ ۱۳۸۲/۹/۱۹توسط مجلس شورای اسلامی تأسیس شده است. هدف از ایجاد این سازمان ایفای اختیارات حاکمیتی، نظارتی و اجرایی وزارت ارتباطات و فناوری اطلاعات در بخش تنظیم مقررات و ارتباطات رادیوئی است تا به عنوان نهاد نظارتی زمینه رقابتی شدن بازار ارائه خدمات مخابراتی و بالارفتن کیفیت خدمات ارتباطی را فراهم کند.

سازمان مذکور، یک نهاد مستقل قانون‌گذار و نظارتی است که یکی از وظایف آن تعیین نرخ و تعرفه استفاده از اینترنت است.

بر اساس یکی از نظریه‌های پیشگیری وضعی، که نظریه سبک فعالیت‌های روزمره نامیده می‌شود، هر اندازه کاربران در اینترنت حضور داشته باشند و مدت زیادی را در اینترنت به گشت زنی و وب نوردی بپردازند، احتمال بزهکاری و بزه‌دیدگی آنها بیشتر می‌شود. (Ngo & P-aternoster,2011:776) در این راستا یکی از راهکارهای حمایتی در خصوص جلوگیری از حملات سایبری و پشتیبانی از بزه‌دیدگان بالقوه و بالفعل این است که مدت حضور و استفاده کاربران را محدود کرد. افزایش تعرفه استفاده از اینترنت پرسرعت، نمونه‌ای از راهکارهایی است که در سال‌های اخیر توسط این سازمان اجرا شده است. این امر باعث تغییر الگوی کاربران در استفاده بهینه از اینترنت می‌شود، در نتیجه رایانه‌های کمتری به بدافزارهای رایانه‌ای آلوده می-شوند و به ندرت دچار حملات سایبری نیز خواهیم شد.

- شرکت ارتباطات زیرساخت

یکی از شرکت‌های زیرمجموعه وزارت ارتباطات و فناوری اطلاعات است. طبق اساسنامه شرکت ارتباطات زیرساخت، وظایف عمده این شرکت عبارت اند از: تهیه و تدوین طرح‌های جامع در خصوص شبکه‌های زیرساخت‌های ارتباطی بر اساس نیازهای موجود و تأمین کلیه نیازهای زیرساخت ارتباطی در قالب تهیه و تصویب دستورالعمل‌ها، ضوابط، معیارها و اعمال استانداردهای فنّی و تخصصی در خصوص تأسیس، توسعه، نگهداری و بهره برداری از شبکه‌های زیرساخت ارتباطی از عمده وظایف و فعالیت‌های این سازمان است. (ماده هشت اساس‌نامه شرکت ارتباطات زیرساخت، مصوب ۱۳۸۷)

با توجه به اینکه هر یک از وظایف فوق در راستای حفظ امنیت و محرمانگی و صحت و ایمن سازی فضای سایبر و جلوگیری از افزایش خطرات حملات سایبری و رخنه‌های ناخواسته تأثیر دارد، بنابراین در پیشگیری وضعی از تروریسم سایبری مؤثر واقع می‌شود.

- سازمان فناوری اطلاعات

این سازمان یکی از زیرشاخه‌های وزارت ارتباطات و فناوری اطلاعات است که با صدور توصیه نامه‌های امنیتی در خصوص ایمن سازی زیرساخت‌های اطلاعاتی و سامانه‌های فناوری اطلاعات و ارتباطات، از قبیل: تهیه نسخه پشتیبان از اطلاعات، کنترل دسترسی، کنترل درگاه‌های ورودی و خروجی، سیاست‌های امنیتی، حفاظت از اطلاعات، امنیت نرم افزار، امنیت شبکه، حفاظت در مقابل کدهای سیّار، به اقدامات پیشگیرانه و مقابله‌ای علیه تروریسم سایبری و ایمن سازی فضای سایبر کشور، جامه عمل می‌پوشاند.

- کارگروه مبارزه با ویروس‌های صنعتی جاسوسی

این گروه با عضویت وزارت ارتباطات، صنایع، سازمان پدافند غیرعامل، کمیته افتای وزارت ارتباطات و مدیران انجمن رمز ایران در سال ۱۳۸۹ تشکیل شد. در همین راستا گروه مذکور به منظور مقابله با کرم استاکس نت که تأسیسات صنعتی و به خصوص هسته‌ای کشور را مورد تهاجم قرار داده بود، پاک‌سازی و فعالیت‌های خود را در زمینه ایمن سازی سیستم‌های آسیب پذیر صنعتی و پیشگیری از حملات سایبری علیه این تأسیسات آغاز نمود و در راستای دیگر تهدیدات سایبری، اقدامات زیادی را انجام داده است.

قرارگاه دفاع سایبری

وظایف این قرارگاه، اعلام هشدارهای ملّی در برابر تهدیدات امنیتی کشور، ایمن سازی زیر-ساخت‌های کشور در برابر حملات سایبری و ایجاد توازن بازدارندگی در حوزه سایبری است. بر اساس قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی مصوب ۱۳۸۳، وظایف قرارگاه پدافند غیرعامل عبارت‌اند از:

«تبیین و برآورد تهدیدات و شناسایی دقیق تسلیحات دشمن از نظر زمان، حجم و منطقه عمل جهت ارائه به کمیته دائمی، هماهنگ سازی برنامه‌های پدافند غیرعامل و با توجه به میزان اثربخشی پدافند در هر نقطه و ارائه پیشنهاد به کمیته دائمی، ارزیابی عملیّاتی اولویت بندی مراکز تحت پوشش با توجه به برآورد تهدیدات و پیشنهاد به کمیته دائمی». (ماده شش آیین نامه بند ۱۱ ماده ۱۲۱ قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی، مصوب ۱۳۸۳)، از عمده فعالیت‌های این مرکز در جهت مقابله با تهدیدات سایبری و به تبع تروریسم سایبری به شمار می‌رود. (شیهان، ۵۴،۱۳۸۸)

سازمان پدافند غیرعامل

پدافند غیرعامل در حوزه‌های متفاوتی مشغول به انجام وظیفه است؛ اما در سال‌های اخیر رویکرد جدیدی به خود گرفته و حوزه فعالیت‌های خود را به فضای سایبر نیز گسترش داده است. پدافند غیر عامل اینگونه تعریف شده است: «مجموعه اقدامات غیر مسلحانه‌ای که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان‌ها و تأسیسات، تجهیزات و شریان‌های کشور در مقابل عملیّات خصمانه و مخرب دشمن می‌گردد». (آیین نامه اجرایی بند ۱۱ ماده ۱۲۱ قانون برنامه پنج ساله چهارم توسعه کشور، مصوب ۱۳۸۳)

مراکز تحت پوشش سازمان پدافند غیرعامل، شامل کلیه تأسیسات زیربنایی، ساختمان‌های حساس و شریان‌های اصلی و حیاتی کشور اعم از آنکه در دست مطالعه، اجرا و یا در حال

بهره برداری هستند و احتمال حملات نظامی دشمن علیه آنها وجود دارد، به این شرح سطح بندی می‌شود: مراکز حیاتی: مراکزی را شامل می‌شود که دارای گستره فعالیت ملّی هستند و وجود و استمرار فعالیت آن برای کشور حیاتی است و آسیب یا تصرف آنها به وسیله دشمن باعث اختلال کلی در اداره امور کشور می‌گردد. مراکز حساس: مراکزی که دارای گستره فعالیت منطقه‌ای هستند و وجود و استمرار فعالیت آنها برای مناطقی از کشور ضروری است و آسیب یا تصرف آنها به وسیله دشمن باعث بروز اختلال در بخش‌های گسترده‌ای از کشور می‌گردد.

مراکز مهم: یعنی مراکزی که دارای گستره فعالیت محلی هستند و وجود و استمرار فعالیت آنها برای بخشی از کشور دارای اهمیت است و آسیب یا تصرف آنها به وسیله دشمن باعث بروز اختلال در بخشی از کشور می‌گردد.

این سازمان در سال ۱۳۸۲، به طور مستقل آغاز به کار نمود و پروژه‌های مهمی در بخش مخابرات، صدا و سیما و هسته‌ای به انجام رسانده است. از نمونه اقدامات سازمان پدافند غیرعامل در زمینه ارتباطات و مخابرات کشور، می‌توان به راه‌اندازی چهار مرکز دفاع سایبری در عسلویه، خارک، بندر امام و اهواز و همچنین تأکید این سازمان برای انتقال میزبانی‌ها به داخل کشور و لزوم ایجاد یک مرکز داده ملّی اشاره کرد. (http://www.tabnak.ir) مستقل نمودن شبکه اطلاعات از تهدیدات خارجی، یکی از گام‌های مهم در ایمن نمودن فضای سایبر در مقابل تروریسم سایبری است.

پلیس فضای تولید و تبادل اطلاعات ناجا

پدیده تروریسم سایبری در حال حاضر به شکل گسترده تر و خطرناکتر، در سطحی بین-المللی و در اکثر کشورها به شکلهای گوناگونی ارتکاب می‌یابد که از آن به عنوان «اشکال نوین تروریسم» یاد می‌شود. (حیدرقلی زاده،۴۷:۱۳۹۲) و به حق میتوان گفت که تروریسم سایبری یکی از انواع تروریسم‌های دولتی و به معنای به کارگیری و حمایت از این پدیده از سوی یک دولت و یا یک نظام سیاسی است. (اچ کاریو،۱۳:۱۳۸۷) با توجه به توسعه روزافزون زیر-ساخت‌های فناوری اطلاعات و ارتباطات در کشور و افزایش کاربران و استفاده کنندگان از اینترنت و سایر فناوری‌ها، پلیس فضای تولید و تبادل اطلاعات ناجا موسوم به پلیس فتا به دنبال مصوبات کمیسیون افتا مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، در بهمن ۱۳۸۹ به دستور فرماندهی انتظامی تشکیل گردید. از جمله اهم وظایف پلیس فتا در راستای ایمن سازی فضای سایبر و مقابله با تهدیدات عبارت اند از: تأمین امنیت فضای تولید و تبادل اطلاعات کشور، صیانت از منافع، اسرار و اقتدار ملّی در فضای تولید و تبادل اطلاعات، فرهنگ

سازی، آموزش و رشد آگاهی‌های جامعه با محوریت فضای مجازی، حفظ زیرساخت‌های کشور در مقابل حملات الکترونیک و آسودگی خاطر شهروندان به انجام فعالیت‌های مبتنی بر فضای سایبر، حفظ حریم خصوصی و آزادی‌های مشروع و صیانت از هویت دینی، ملّی و ارزش‌های انسانی جامعه در افتا، از جمله اهداف عمده تشکیل پلیس فتا است. این نهاد با استفاده از نیروهای انسانی متخصص در فناوری اطلاعات، با رویکرد مقابله با جرایم از طریق پیش‌بینی، پیشگیری و کشف جرم اقدام می‌نماید. انکار مسئولیت ناشی از اقدامات تروریستی که مورد حمایت غیرمستقیم دولت و پلیس است، برای دولتها آسان و ردیابی اقدامات آنها اغلب دشوار و در عین حال مخفیانه که برای دستیابی به اهداف مورد نظر خود احزاب و گروهها را برای انجام فعالیت‌های تروریستی حمایت و تأمین مالی می‌کنند. (رئیسی، حیدرقلی زاده،۱۳۹۶: ۷۱) از جمله اقدامات انجام شده توسط پلیس افتا می‌توان به حمله سایبری اخیر به تأسیسات وزارت نفت اشاره نمود که در اسرع وقت در برای تحقیقات و ردیابی عاملان شروع به کار نمود و معلوم شد که (آی پی) حمله کنندگان، به کشور آمریکا تعلق داشته است و از طریق پلیس بین‌الملل این موضوع در حال پیگیری است.

انجمن رمز ایران

یکی دیگر از مؤسساتی که در زمینه مقابله تروریسم سایبری می‌تواند نقش بسزایی داشته باشد، انجمن رمز ایران است. انجمن رمز ایران یک موسسه علمی، غیرانتفاعی و غیرسیاسی است که به منظور گسترش و پیشبرد و ارتقاء علم و فناوری رمز و امنیت فضای تبادل اطلاعات و کمک به توسعه کمی و کیفی نیروهای متخصص و بهبود بخشیدن به امور آموزشی و پژوهشی در زمینه‌های مربوطه تأسیس شده است. (http://www.isc.org.ir) اهم فعالیت‌های مؤسسه مذکور عبارت است از:

ارائه خدمات آموزشی و پژوهشی و مشاوره، و همچنین ارزیابی و بازنگری طرح‌ها و برنامه-های محول یا مصوب و کمک به تدوین و توصیه استانداردها در زمینه علمی موضوع فعالیت انجمن، توسعه و ترویج فرهنگ استفاده صحیح از علم و فناوری رمز و امنیت ارتباطات و کامپیوتر و ارائه رهنمودهای حقوقی اجتماعی و اقتصادی مربوطه، برگزاری میزگردها و همایش‌های بررسی مسایل مبتلا به امنیت فضای تبادل اطلاعات کشور». (ماده پنج اساس نامه انجمن رمز ایران، مصوب ۱۳۸۶) در زمینه اقدامات انجمن به منظور پیشگیری از تروریسم سایبری، می‌توان به حمله صورت گرفته توسط کرم استاکس‌نت به تأسیسات هسته‌ای بوشهر اشاره نمود که با

همکاری نهادهای دیگر به مقابله با بدافزار مذکور و ایمن سازی سیستم‌های صنعتی آسیب پذیر تلاش نمود.

مرکز مدیریت توسعه ملّی اینترنت

مرکز مدیریت توسعه ملّی اینترنت (متما) به منظور بهره گیری هرچه بیشتر از مزایای فناوری اطلاعات، تحقق اهداف برنامه چهارم توسعه، تحقق بخشیدن به اهداف چشم انداز بیست ساله کشور و همچنین برای بالا بردن شاخص‌های آمادگی الکترونیکی کشور تأسیس شده است. از جمله وظایف اصلی این مرکز، تمرکز بر محافظت و توسعه فضای سایبر ملّی و تبدیل آن به محیطی پر نشاط جهت پیشبرد اهداف ملّی - مردمی، مدیریت مؤثر و پایدار منابع اینترنت، بهینه سازی و توسعه اینترنت و فعالیت‌های تحقیق و توسعه مربوط به منابع آدرس‌های اینترنتی نسل آینده شبکه، توسعه دامنه‌های IR و انجام سیاست‌های مربوط به رجیستری و تخصیص آدرس‌های آی پی، همکاری با مجامع بین‌الملل مربوطه و فعالیت‌های فرهنگی و آموزشی، شامل برگزاری دوره‌های آموزشی، سمینار و فعالیت‌های انتشاراتی، از اهداف عمده این مرکز است.

مرکز ملی داده ایران

مرکز داده[1] زیربنای اصلی فناوری اطلاعات و ارتباطات نوین را تشکیل می‌دهد. مرکز داده مجموعه‌ای عظیم از سیستم‌های سخت افزاری و نرم افزاری هستند که در تأسیسات کاملاً مجهز و پیشرفته قرار دارند که به منظور انجام خدمات مهمی از قبیل: انجام میزبانی وب، انواع خدمات دسترسی به شبکه اینترنت، انواع خدمات پشتیبانی سخت افزاری و نرم افزاری به‌کار برده می‌شوند. (جلالی فراهانی، ۱۳۸۵: ۵-۴)

اما آنچه در این میان از اهمیت زیادی برخوردار است، استفاده از مرکز داده به عنوان محل ذخیره سازی داده‌ها است. در بسیاری از تارنماهای دولتی و خصوصی، میزبانی وب، به سرور-های خارجی واقع در کشورهای اروپایی داده شده که نگرانی‌های زیادی را در خصوص حفظ امنیت اطلاعات به وجود آورده است. بدین منظور در سال‌های اخیر تلاش‌هایی به منظور ایجاد یک مرکز داده ایرانی و بومی صورت گرفته که مرکز ملّی داده ایران یکی از ثمره توجه مسئولان به این امر است. بنابراین تأسیس چنین مرکزی، اقدامی کاربردی در جهت امنیت اطلاعات سایبری در برابر تهدیدات حملات تروریستی سایبری است.

[1]-Data Center

گروه زیر ساخت شبکه و امنیت فضای تبادل اطلاعات

یکی دیگر از اقدامات کشورمان در زمینه ایمن سازی فضای سایبر و مقابله با تروریسم سایبری، راه اندازی گروه زیر ساخت شبکه و امنیت فضای تبادل اطلاعات است که فعالیت-های ارزنده‌ای را در این خصوص انجام داده است. اهمّ فعالیت‌های این گروه عبارت اند از:

«ارائه طرح جامع امنیت شبکه و اطلاعات با توجه به مصوبات، آیین نامه‌ها و قوانین و مقررات ابلاغی، تجزیه و تحلیل شبکه و تعیین مخاطرات امنیتی و ارائه راه حل آن، ارائه راه حل‌ها برای کاهش آسیب پذیری، تهدیدات و ریسک‌ها، طراحی ساختار مطمئن برای شبکه، حفاظت از دسترسی غیر مجاز به سرویس‌های شبکه، بازنگری در حقوق دسترسی کاربران، آگاهی رسانی به کاربران شبکه در خصوص روش‌های جدید نفوذ به سیستم‌ها و روش‌های مقابله با آن، نظارت بر خرید سخت افزار و نرم افزار به منظور انطباق با سیاست‌های امنیتی حفاظتی، بررسی و در صورت نیاز انتخاب خرید و تست نرم افزار ضد ویروس مناسب و کاراتر برای ایستگاه-های کاری به صورت دوره‌ای از عمده فعالیت‌های این گروه در راستای محافظت از فضای سایبر و تهدیدات موجود است.

همان طور که از وظایف و فعالیت‌های این گروه پیداست، راه اندازی گروه زیر ساخت شبکه و امنیت فضای تبادل اطلاعات اقدامی شایسته در جهت حمایت‌های تقنینی و فنّی از زیر-ساخت‌های اطلاعاتی است؛ لذا با گسترده نمودن حوزه فعالیت‌های این سازمان، می‌توان به ارتقای سلامت سایبری کشور و پیشگیری از تهدیدات تروریسم سایبری اقدام نمود.

مرکز تحقیقات مخابرات ایران

مرکز تحقیقات مخابرات ایران، قدیمی‌ترین مرکز پژوهشی در حوزه فناوری اطلاعات اصلی-ترین پایگاه تحقیقات در زمینه ارتباطات و فناوری اطلاعات در کشور است.

این مرکز با دارا بودن چهار پژوهشکده به عنوان پژوهشگاهی تحقیقاتی، قطب پژوهشی فناوری ارتباطات و اطلاعات محسوب می‌شود و نقش مهمی را به عنوان مشاور مادر در بخش فناوری اطلاعات و ارتباطات دارا است.

عمده فعالیت‌های پژوهشی این مرکز در خصوص اتخاذ تدابیر امنیتی و ایمن سازی فضای سایبر، پژوهشکده امنیت فناوری ارتباطات و اطلاعات است که در زمینه امنیت جامعه اطلاعاتی، فناوری امنیت شبکه، فناوری امنیت اطلاعات و سامانه‌ها، حقوق و مقررات ارتباطات و فناوری اطلاعات فعالیت می‌کند. علاوه بر اقدامات فوق، شورای عالی امنیت ملّی به کسب مشورت از متخصصان امر به تأسیس شورای عالی امنیت فضای تبادل اطلاعات کشور نموده است و هم‌چنین

اقدام شورای عالی انقلاب فرهنگی در زمینه صدور دستورالعمل‌هایی در خصوص نحوه ارائه خدمات شبکه‌ای، نمونه‌ای از اقدامات پیشگیرانه وضعی در زمینه مقابله با تهدیدات سایبری است. (https://www.ict.gov.ir)

گذشته از اقدامات نهادهای اجرایی که بیشتر در قالب پیشگیری اجتماعی مطرح شدند، تدابیر فنّی، بیشتر از هر راهکاری در مقابله با تروریسم سایبری مثمر ثمر واقع می‌شود. هر چند تدابیر دیگری همچون حمایت‌های تقنینی را نباید نادیده گرفت اما با توجه به متفاوت بودن بستر ارتکاب جرایم سایبری با جرایم دیگر، تدابیر فنّی و محدود کننده، بیشترین بازدهی را در این زمینه خواهند داشت. (موسوی، ۱۳۹۲: ۵)

در زمینه اقدامات تدابیر فنّی اتخاذ شده در سازمان‌ها و ادارات کشور به منظور مقابله با چالش‌های جدید فضای سایبر که به نوبه خود منجر به افزایش زحمات ارتکاب جرم می‌شوند که در ادامه توضیح می‌دهیم.

نصب و استقرار دیوار آتشین

دیوارهای آتشین یکی از کارآمدترین راهکارهای حفاظت و امنیت شبکه و سیستم‌های رایانه‌ای در مقابل حملات سایبری است. دیوار آتشین در اصطلاح علوم رایانه‌ای عبارت است از:

«یک سیستم ایمنی برای محافظت از شبکه یک سازمان در مقابل تهدیدهای خارجی همچون نفوذ گران که از شبکه‌های خارجی همچون اینترنت وارد می‌شوند. دیوار آتش که به طور معمول ترکیبی از سخت افزار و نرم افزار است، از ارتباط مستقیم کامپیوترهای عضو شبکه داخلی یا شبکه‌های خارجی و برعکس جلوگیری می‌کند». (شمس،۱۳۹۳:۴۰)

امروزه استفاده از دیوار آتشین در اکثر سیستم‌های بانکی و ادارات به منظور ممانعت از نفوذ و اجرای بدافزارهای غیرمجاز معمول است. در زمینه استفاده و به‌کارگیری دیوار آتشین مقررات گوناگونی تصویب شده است. از جمله مقررات مذکور، می‌توان به مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای اشاره نمود که "مخابرات و کلیه ایجاد کنندگان نقطه تماس بین‌المللی را موظف به حفاظت از شبکه‌های رایانه‌ای و مخابراتی به وسیله نصب و استقرار نقش دیوار آتشین نموده است." (ماده شش مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای، مصوب ۱۳۸۰) نقش دیوار آتشین، بستن درگاه‌های غیر ضروری، جداسازی و امنیت شبکه‌های داخلی در مقابل شبکه-های خارجی و ناامن است و به ترافیک داده، تنها از طریق درگاه‌های شناخته شده اجازه عبور می‌دهد. دیوار آتشین قادر به نظارت بر درخواست‌های دریافتی برای جلوگیری از دسترسی

حملات شناخته شده به سرور وب است. علاوه بر تشخیص نفوذ، دیوار آتش ابزار مفید برای جلوگیری از حملات و شناسایی اقدامات نفوذ در شبکه و یا در بدترین حالات، تشخیص منبع حمله است. دیوار آتشین دارای لیستی از قوانین مشخص شده فیلترینگ است و بر اساس لیست مذکور به جریان اطلاعات در شبکه اجازه عبور و مرور را می‌دهد. (خبیری،۱۳۹۱:۱۸۰)

به طور کلی این سیستم‌ها دو سیاست عمده را پیش می‌گیرند: امکان عبور به ارتباطاتی که به طور صریح منع نشده‌اند و جلوگیری از تمام ارتباطات و جریان‌ها مگر آنهایی که به طور صریح برای آنها مجوز دارد. سیستم‌های مذکور قابلیت این را دارند که در محیط‌هایی که به اینترنت هم وصل نیستند به فعالیت و محافظت خود از تهدیدات ادامه دهند. با توجه به حوزه فعالیت‌های تروریستی سایبری در زمینه‌های صنعتی و خدمات عمومی، می‌توان با به کارگیری این سیستم‌ها در مراکزی مانند: شبکه‌های گسترده انتقال برق یا استفاده آنها در تجهیزات کنترل خطوط مترو، در درجه اول از تهدیدات نفوذی به شبکه‌های آنان و در مراحل بعد از وقوع حوادث ناگوار و مختل شدن تأسیسات صنعتی جلوگیری نمود.

سیستم‌های تشخیص و پیشگیری از نفوذ

دیوارهای آتشین، ابزار کافی برای دفاع از شبکه یا سیستم‌های رایانه‌ای نیستند و نمی‌توانند در مقابل برخی حملات، از شبکه محافظت نمایند. بنابراین برخی از مدیران در کنار دیوار آتشین، سیستم‌های تشخیص نفوذ را نیز پیشنهاد می‌کنند. استفاده از سیستم‌های تشخیص نفوذ، در تصویب نامه برنامه توسعه تجارت الکترونیکی به منظور ایمن سازی تجارت الکترونیکی مورد تأکید قرار گرفته است. (ماده ۲۲ برنامه جامع توسعه تجارت الکترونیکی، مصوب ۱۳۸۴) هدف یک سیستم تشخیص نفوذ، جلوگیری از حمله نیست و تنها کشف و احتمالاً شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه‌های رایانه‌ای و اعلام آن به مدیر سیستم است. به طور معمول، بیشتر سیستم‌های تشخیص نفوذ در کنار دیواره‌های آتش و به صورت مکمل امنیتی برای محافظت از منابع اطلاعاتی در سیستم‌های رایانه‌ای و مخابراتی مراکز حساس و صنعتی مورد استفاده قرار می‌گیرند.

یکی دیگر ابزارهایی که در سیستم‌های رایانه‌ای و مخابراتی به منظور مقابله با تجاوز و ورود غیرمجاز استفاده می‌شود، سیستم‌های پیشگیری از نفوذ[1] است. در اغلب سازمان‌ها و ادارات به خصوص بانک‌ها و تارنماهای اطلاع رسانی دولتی، استفاده از اینگونه سیستم‌ها معمول است.

[1] -Intrusion prevention system

سیستم‌های پیشگیری از نفوذ ابزارهایی هستند که به منظور پیشگیری از وقوع حملات سایبری بر روی شبکه‌ها و سیستم‌های رایانه‌ای اقدام می‌کنند. به عبارت دیگر، "محافظت از سرمایه-های رایانه در مقابل درخواست‌های غیرقانونی و تهدیدهای بالقوه در سیستم عامل و جلوگیری از آلوده شدن به وسیله کدهای مخرب می‌شوند. تفاوت این سیستم‌ها با سیستم‌های تشخیص نفوذ در راهکارهای امنیتی است که قبل از درگیر شدن سیستم با تهدیدات و تحت تأثیر قرار گرفتن عملکرد سیستم، برای مقابله با نفوذ به کار گرفته می‌شوند."(JulianL,2016:5)

سیستم‌های تشخیص نفوذ و پیشگیری از نفوذ، مشخصات مشترک زیادی دارند؛ تفاوت کلیدی این دو تکنولوژی این است که سیستم‌های تشخیص نفوذ، تنها ترافیک آسیب رسان را تشخیص می‌دهند، اما سیستم‌های پیشگیری از نفوذ از ورود چنین ترافیکی به شبکه جلوگیری می‌کنند.

استفاده از برنامه‌های ضد ویروس

امروزه یکی از ملزومات اساسی سیستم‌های رایانه‌ای و مخابراتی، برنامه‌های ضد ویروس[1] هستند. انتشار بدافزارهای رایانه‌ای که به صورت روزانه در اینترنت وارد می‌شوند و نتایج زیان‌باری را در اثر آلوده شدن منابع رایانه‌ای باعث می‌شوند، ضرورت به‌کارگیری برنامه‌های ضد ویروس را به منظور ایمن نمودن سیستم‌های رایانه‌ای و مخابراتی هم در منازل و مراکز صنعتی و زیرساخت‌های اطلاعاتی روشن می‌سازد. البته ذکر این نکته الزامی است که امنیت قطعی و صد در صد وجود ندارد و هیچ برنامه ضد ویروسی نمی‌تواند به طور کامل امنیت داده‌های رایانه‌ای را تضمین کند. بنابراین استفاده از دیگر سخت افزارها و نرم افزارهای امنیتی در کنار یکدیگر به منظور ایمنی بیشتر لازم است. (مهدوی ثابت و همکاران،۱۳۹۶: ۱۰۰) عملکرد برنامه‌های مذکور اینگونه است که با قرارگیری در دستگاه‌های رایانه‌ای و مخابراتی، از ورود و اجرا شدن بدافزارهای مخرب جلوگیری می‌کنند و در صورت نفوذ به محو یا قرنطینه نمودن آنها اقدام می‌نمایند. بدین منظور استفاده از چنین برنامه‌هایی به منظور سخت‌تر کردن دسترسی به آماج تروریسم سایبری که زیرساخت‌های اطلاعاتی هستند و دستیابی به پیشگیری وضعی، کارایی به خصوصی دارند.

مستقل نمودن شبکه‌های کنترل و اداری

در محیط‌های صنعتی و خدماتی، می‌توان با مستقل نمودن شبکه‌هایی که کنترل منابع را

[1] -Anti Virus Program

در دست می‌گیرند، از دسترس پذیری و نفوذ در آنها جلوگیری نمود. مستقل کردن شبکه‌ها از اینترنت، یکی از شیوه‌هایی است که به تازگی در برخی پالایشگاه‌های کشور به منظور امنیت بیشتر تأسیسات و سخت‌تر کردن دسترسی به آماج جرم استفاده می‌شود. در این روش با استفاده از "دیوارهای آتشین دوتایی، استفاده از دیوار آتش به همراه مسیریاب و استفاده از دیوار آتش با دو پورت ساده بین شبکه کنترل و اداری تا حد زیادی از وقوع حملات ضد شبکه-های مذکور جلوگیری می‌شود." (غفار زاده و طباطبائیان، ۱۳۸۸: ۸-۷)

استفاده از پروتکل‌های رمزگذاری

استفاده از روش‌های رمزنگاری، نفوذگران و خرابکارهای حرفه‌ای به سادگی قادر خواهند بود اطلاعات رد و بدل شده توسط کاربران را شنود و مورد استفاده قرار دهند. (باطنی و یارجی آبادی،۱۳۹۰: ۴) بدین منظور مراکز مذکور برای ایمن نگاه داشتن داده‌های خود از روش‌های ذیل استفاده می‌کنند:

نخست، پروتکلHTTPS : برای انتقال ایمن اطلاعات در اینترنت از این پروتکل امن استفاده می‌شود. با استفاده از ویژگی‌های امنیتی این پروتکل، انتقال اطلاعات از قبیل فیل‌های متنی، گرافیکی و غیره رمزگذاری شده و اطلاعات با استفاده از درگاه (Port) امن منتقل می‌شود. (موسوی و سبزعلی گل، ۱۳۹۵: ۳۱۱) بنابراین با به‌کارگیری رمزنگاری اطلاعات، می‌توان به ایمن نگه داشتن اطلاعات حساس در پایگاه‌های زیرساختی استفاده نمود و از مورد تعرض قرار گرفتن داده‌های رایانه‌ای و مخابراتی توسط حملات نفوذگران و تروریست‌های سایبری جلوگیری نمود. در کشورمان از این پروتکل بر روی تارنماهای حساس مانند سیستم‌های پرداخت بانکی، پست الکترونیک یا تارنماهای مرتبط به صنایع کشور استفاده می‌شود.

دوم: پروتکل و گواهینامه دیجیتال SSL: امروزه از گواهی دیجیتال[1] به طور گسترده به منظور ایمن سازی تبادل اطلاعات رمز شده در اینترنت، به خصوص در پست الکترونیک استفاده می‌شود. گواهی دیجیتال از سوی مراجع صلاحیت دار ارائه دهنده گواهی دیجیتال، خریداری شده و مراجع مذکور با بررسی و ثبت اطلاعات مؤسسات و افراد، صحت گواهی‌های دیجیتال تارنماها یا افراد را بررسی کرده و به مرورگرهای اینترنتی اعلام می‌کنند. (موسوی و سبزعلی، ۱۳۹۰: ۳۷۶) واژه SSL، مخفف Secure Socket Layer است و در واقع، "عنوانی برای یک فناوری استاندارد و به ثبت رسیده برای ایجاد ارتباطات امن بین دو طرفی که خواهان استفاده

[1]-Digital Certificate

از این پروتکل هستند، استفاده می‌شود که در این صورت مرجع صادر کننده گواهی نامه تضمین می‌کند که اگر اطلاعات به سرقت برود باز هم قابل فهم برای فرد سارق نباشد." (باطنی و یارجی آبادی، ۱۳۹۰: ۴) استاندارد مذکور، یک استاندارد فنّی بوده و در حال حاضر توسط میلیون‌ها تارنما در سراسر دنیا مورد استفاده قرار می‌گیرد. گواهینامه‌های دیجیتال SSL، نیز ابزاری برای تأیید هویت و حفظ امنیت تارنماها هستند. گواهینامه‌های SSL که تنها برای شرکت‌ها و اشخاص حقیقی معتبر صادر می‌شوند، حاوی اطلاعاتی در مورد نام دامنه، شرکت، آدرس، تاریخ ابطال گواهینامه و همین طور اطلاعاتی در مورد صادرکننده گواهینامه هستند.

پالایش یا فیلترینگ

پالایش یا فیلترینگ یکی دیگر از ابزارهای مقاوم سازی فضای سایبر در مقابل تهدیدات است؛ هرچند که در نظر افکار جامعه، بیشتر جنبه اخلاقی یا سیاسی اجرای پالایش به ذهن خطور می‌کند. اما با استفاده از پالایش و مسدود نمودن منابع اطلاعاتی آلوده و خطرناک در اینترنت و جلوگیری از دسترسی شهروندان و دیگر مراکز به داده‌های خطرناک و نامعتبر، می‌توان از نفوذ بدافزارهای رایانه‌ای و انتشار آنها در فضای سایبری کشور جلوگیری نمود. (عباسی، ۱۳۹۱: ۲۰) متولی پالایش در ایران بر خلاف کشورهای دیگر نهادهای متعددی هستند. این امر منجر به سلیقه‌ای شدن و بروز مشکلات متعددی در پالایش و رفع پالایش تارنماهای اینترنت شده است. عهده دار فیلترینگ در کشور، کارگروهی با نام «تعیین مصادیق مجرمانه» است که این کمیته از ۱۲ نهاد و سازمان دولتی و عمومی تشکیل شده و مسئولیت فیلترینگ و رفع فیلتر را بر عهده دارد.

این کارگروه که مسئولیت آن بر عهده دادستان کل کشور است، نمایندگانی از وزارت خانه-های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، سازمان‌های تبلیغات اسلامی، صدا و سیما، فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی، یک نفر نماینده مجلس شورای اسلامی به انتخاب کمیسیون حقوق قضایی و تأیید مجلس شورای اسلامی داشته و به تصمیم گیری درباره پالایش یا رفع پالایش تارنماها می‌پردازند.

سیستم عامل قاصدک

یک سیستم عامل آزاد مبتنی برسیستم عامل لینوکس است که برای سازمان‌های دولتی و

خصوصی، مهندسان نرم افزار و شبکه، مهندسان عمران و راه و ساختمان، مدارس و مؤسسات آموزش عالی و مصارف شخصی و خانگی مورد استفاده قرار می‌گیرد. این سیستم عامل با داشتن مجموعه کاملّی از نرم افزارهای اداری و دفتری، نرم افزار های فنّی و مهندسی، مالتی مدیا، انیمیشن سازی و ابزارهای برنامه نویسی، جایگزین مناسبی برای محصول ویندوز مایکرو-سافت است و به مراتب دارای ایمنی بالا در مقابل تهدیدات سایبری است. در بسیاری از مواقع، نرم افزارهای تولیدی به گونه‌ای ساخته می‌شوند که خود به عنوان جاسوسی از آنها استفاده می‌گردد. بنابراین استفاده و به‌کارگیری محصولات داخلی تا حدودی از تهدیدات مذکور خواهد کاست. (http://www.ghasedak.ir)

نتیجه گیری

در خصوص سیاست جنایی اجرایی اتخاذ سیاست‌های پیشگیرانه مقتضی و متناسب با فضای سایبر نیز بسیار راهگشاست، هرچند ماهیت و ویژگی‌های این فضا، چالش‌های جدی در برابر اتخاذ تدابیر پیشگیرانه ایجاد کرده است؛ ولی باید دانست که اهمیت پیشگیری از تروریسم سایبری از جرم انگاری آن کمتر نیست. با این حال پیشگیری به ویژه پیشگیری وضعی بدون جرم انگاری، می‌تواند اقدامی ابتر و بلکه خطرناک باشد؛ از این رو پیشگیری وضعی در فضای سایبر تا زمانی که محدوده دقیق رفتارهای مجرمانه مشخص نشده است، پیشنهاد نمی‌گردد؛ زیرا سبب سوء استفاده متصدیان پیشگیری به ویژه دولت و محدود سازی آزادی‌های فردی در این فضا می‌گردد. اما انجام اقدامات فنی لازم برای تامین امنیت و بلکه تضمین اطلاعات و سامانه‌ها امری ضروری است. پیشگیری از تروریسم سایبری در گرو اتخاذ تدابیر فنی از یک سو و تدابیر اجتماعی از سوی دیگر است. در این میان بخش خصوصی و به ویژه ارایه دهندگان خدمات اینترنتی نقش به سزایی در پیشگیری آگاهانه و منطقی دارند؛ زیرا این نهادها به واقع به ارزش و جایگاه فضای سایبر آگاهند و پشتیبانان و راهبران جریان مبادلات اطلاعاتی به شمار می‌آیند؛ از این رو نباید تدابیر پیشگیرانه خارج از خواست و توانایی اشان نیز به آنها تحمیل کرد. با این حال پیشگیری از تروریسم سایبری بدون توجه و کمک موسسات تامین کننده اطلاعات و ارتباطات امکانپذیر نیست و اساساً تدابیر تامین امنیت فضای سایبر که عمده آنها در قالب پیشگیری از تروریسم سایبری است، در گرو پیش بینی نهادهای خاص است. در ایران، شورای عالی امنیت فضای تبادل اطلاعات با تصویب هیات وزیران پیش بینی شده است که وظیفه تامین امنیت فضای سایبر یا همان فضای تبادل اطلاعات در سطح ملی را داراست.

با این حال این نهاد را نمی‌توان مرجع اختصاصی و حتی عمومی پیشگیری از جرایم سایبری به ویژه تروریسم سایبری دانست زیرا این شورا برای تامین امنیت محیط تبادل اطلاعات که در معنایی بسیار گسترده از پیشگیری از تروریسم سایبری و جرایم سایبری است اقدام می کند و نسبت به این پدیده‌های مجرمانه برنامه مشخصی ندارد؛ از این رو پیش بینی نهادی که بتواند متولی امر پیش بینی مخاطرات احتمالی، پیشگیری از تروریسم سایبری و حتی واکنش سریع باشد، ضروری است.

لذا در کشورمان 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 کشور است. در این زمینه لازم است تدابیر تقنینی، قضایی و اجرایی ویژه‌ای در سطح ملی و بین‌المللی در نظر گرفته شود. بدیهی است برای حل این معضل باید راهکارهایی گوناگونی اساسی و زیربنایی در حوزه‌های مختلف طرح ریزی شود.

منابع فارسی

کتب

- آشوری، داریوش(۱۳۸۳)، **دانش نامه سیاسی**، تهران، انتشارات مروارید
- آنجیلیز، جینا دی، **جرایم سایبر**، ترجمه سعید حافظی و عبدالصمد خرم آبادی، دبیرخانه شورای عالی اطلاع، بی تا
- اچ.کاریو ف (۱۳۸۸)، **تروریسم دولتی و ایالت متحده آمریکا**، ترجمه رضا محمودی فقیهی، تهران، نشر دفتر مطالعات بین‌المللی مبارزه با تروریسم دانشگاه آزاد اسلامی، چاپ اول
- باصری، علی اکبر(۱۳۸۷)، **سیاست جنایی قضایی کودکان و نوجوانان در حقوق داخلی و اسناد بین‌المللی**، تهران، خرسندی
- پاکزاد، بتول (۱۳۸۸)، **تروریسم سایبری**، پژوهش منتشر شده در مرکز تحقیقات استراتژیک
- جعفری لنگرودی، محمد جعفر(۱۳۷۸)، **مبسوط در ترمینالوژی حقوق**، کتابخانه گنج دانش، تهران، چاپ اول، جلد سوم
- حسن بیگی، ابراهیم (۱۳۸۴)، حقوق و امنیت در فضای سایبر، تهران، موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار
- سروش نژاد، احمد (۱۳۸۷)، **دفاع مشروع: تعریف دفاع مشروع و جایگاه حقوقی آن**، انتشارات، دفتر مطالعات بین‌المللی مبارزه با تروریسم دانشگاه آزاد اسلامی
- سید علی موسوی، مجید سبزعلی گل(۱۳۹۵)، **مفاهیم پایه فناوری اطلاعات**، تهران، شرکت چاپ و نشر کتابهای درسی ایران
- شاملو احمدی، محمدحسین(۱۳۸۰)، **فرهنگ اصلاحات و عناوین جزایی**، جلد یک، اصفهان، نشر دادیار
- شیهان، مایکل (۱۳۸۸)، **امنیت بین‌الملل**، ترجمه سید جلال دهقانی فیروزآبادی، تهران، پژوهشکده مطالعات راهبردی
- طیب، علیرضا (۱۳۸۴)، **تروریسم**، تهران، انتشارات نشر نی
- کوشا سهیلا (۱۳۸۹)، **چالش‌های حقوقی پیشگیرانه و مقابله با تروریسم هسته‌ای**، انتشارات مرکز نشر آثار علمی دانشگاه مدرس
- لازرژ، کریستین، (۱۳۸۱)، **درآمدی بر سیاست جنایی**، ترجمه علی حسین نجفی ابرندآبادی تهران، میزان

- مارتی، میری دلماس(۱۳۸۱)، **نظام‌های بزرگ سیاست جنایی**، ترجمه، نجفی ابرند آبادی، انتشارات میزان

مقالات

- بهزاد لک، علی عنایتی(۱۳۹۵)، **رتبه بندی ارکان سیاست جنایی، جرایم سایبری**، فصل نامه پژوهش‌های اطلاعاتی و جنایی، سال یازدهم

- جلالی فراهانی، امیرحسین(۱۳۸۷)، **جنبه‌های حقوقی اقدامات کیفری بین‌المللی مجرمان قانون در قبال جرایم سایبر**، فصلنامه پیشگیری از جرم، شماره ۸

- رحیمی نژاد، اسماعیل (۱۳۹۵)، **دکترین احیای نفس و رابطه آن با عدالت ترمیمی**، نشریه علمی و پژوهشی نامه مفید، حقوق تطبیقی، شماره ۸۲

- زهره باطنی، افسانه یارجی آبادی(۱۳۹۰)، **امنیت در تجارت الکترونیک و راهکارهای ارتقاء آن**، اولین همایش منطقه‌ای رویکردهای نوین در مهندسی کامپیوتر و فناوری اطلاعات، رودسر، دانشگاه آزاد اسلامی واحد رودسر و املش

- شمس، احمد (۱۳۹۳)، **بررسی بنیادین انحراف‌های اجتماعی با تاکید بر نظریه تعامل‌گرا**، فصلنامه مطالعات توسعه اجتماعی ایران، دوره ۷، شماره ۱

- عباسی، مهدی (۱۳۸۳)، **اینترنت ابزار سیاست تروریسم مجازی**، نشریه فرهنگی و فناوری، سال اول، شماره سوم، دی و بهمن

- کابک خبیری، مارال دربندی (۱۳۹۱)، **حقوق بین‌المللی و مسئله تروریسم**، مطالعات روابط بین‌الملل، شماره۱۷

- قربان نیا، یاصر(۱۳۸۳)، **مواجه با تروریسم رویکرد نظامی سیاسی یا حقوقی**، نامه مفید، شماره ۴۳

- لواسور، ژرژ(۱۳۷۲)، **سیاست جنایی**، ترجمه دکتر علی حسین نجفی ابرندآبادی، مجله تحقیقات حقوقی، انتشارات دانشگاه شهید بهشتی، شماره ۵۵-۵۱

- میرزایی ورزنه، رضا (۱۳۹۵)، **کنفرانس پدافند غیر عامل در قلمرو فضای سایبر**، دانشگاه آزاد اسلامی واحد مراغه

محمد علی مهدوی ثابت، قاسم مرادی(۱۳۹۶)، **سیاست جنایی ایران در فضای سایبر**، فصلنامه مطالعات علوم اجتماعی، دوره ۳، شماره ۴

- نیازپور، امیرحسین(۱۳۹۱)، **مطالعه تطبیقی قابلیت تعیین ثمن در نظام‌های حقوقی ایران و انگلیس**، مجله حقوقی دادگستری، زمستان - شماره ۸۰
- نجفی ابرند آبادی، علی حسین (۱۳۷۹)، **در آمدی به جنبه‌های مختلف سیاست جنایی در قبال مواد مخدر**، مجموعه مقالات همایش بین‌المللی علمی

پایان نامه

- رضوانی، نعمت، (۱۳۷۷)، **سیاست جنایی تقنینی و قضایی بزه سرقت موضوع قانون مجازات اسلامی مصوب ۱۳۷۵**، پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه شهید بهشتی
- مسعودی، سیدمحسن(۱۳۹۴)، **بررسی و تحلیل مقررات کیفری ایران در حوزه مبارزه علیه تروریسم سایبر**، پایان نامه کارشناسی ارشد، دانشگاه فردوسی مشهد

English References

Book

- Podgar, Ellen S,(2004), **Wayne Law Review**, **Cyber crime**, transnational or international. vol.50
- Krasavin, serge(2002), **What is cyber-terrorism?**Sans Institute

Articles

-Barry, coLLin(1359), **Transnational Crime and Cyber Terrorism in International Law** 2003 strategies on
- Casey, Eoghan(2001),**Digital Evidence and Computer Crime**,Academic Press
- Moteff,john(2003), **What markes an In f restructure critical?** Congressional Research service
- Ngo, Fawn T, and Paternoster, Raymond (2010),**Cybercrime**
- **Victimization: An examination of Individual and Situational level factors**, International Journal of Cyber Criminology Vol 5 Issue1

Site

- Julian L. R.(2016), **SCADA Intrusion Prevention System**, Journal of Information, http://perso.telecom-paristech.fr/legrand/CI2RCO-conf/