بررسی نقش اقدامات پلیس در پیشگیری از حملات سایبری با تأکید بر آموزه‌های پیشگیری وضعی

نوشین لقمانی،[1] مهدی رستمی خانقاهی[2]

فصلنامه علمی – تخصصی دانش انتظامی شرق استان تهران
سال دوم، شماره هشتم، زمستان ۱۳۹۴

از صفحه ۲۱ تا ۴۰

تاریخ دریافت: ۹۴/۰۴/۱۲
تاریخ پذیرش: ۹۴/۰۸/۱۱

چکیده

در سال‌های اخیر، استفاده فراگیر از رایانه و فناوری‌های مرتبط با آن، موفقیت‌ها و پیشرفت‌های فراوانی را برای جوامع بشری به ارمغان آورده است. علیرغم فواید انکار ناپذیر رایانه در زندگی بشر، همین حضور فراگیر موجب شد تا جرائم رایانه‌ای به عرصه‌های مختلف راه یابد. حملات سایبری شامل تروریسم و جنگ سایبری از این جمله جرائم رایانه‌ای است که از دهه ۹۰ میلادی در محافل علمی مورد بحث قرار گرفته است. امروزه حملات سایبری به یک معضل بزرگ برای بسیاری از کشورها تبدیل شده است تا جایی که در برخی موارد بحران‌های بزرگ سیاسی و امنیتی به همراه داشته و علاوه بر اشخاص، زیرساخت‌ها و پایگاه‌های نظامی آنان را مورد تهاجم قرار داده است. با توجه به خسارات هنگفتی که حملات سایبری بر جوامع تحمیل می‌کند، بسیاری از کشورها با وضع قوانین جدید، امکان تعقیب و مجازات مرتکبین حملات سایبری را فراهم آورده‌اند. قانون‌گذار کشورمان نیز با درک این ضرورت، در سال ۱۳۸۷ اقدام به تصویب قانون جرائم رایانه‌ای نموده است. اما علیرغم تمامی این تلاش‌ها، به دلیل ماهیت خاص حملات سایبری نسبت به حملات فیزیکی و مشکلاتی که پیرامون شناسایی و اجرای مجازات بر مرتکبین این جرائم وجود دارد، ضرورت پیش‌بینی اقدامات پیشگیرانه در مقابل این حملات، کاملاً احساس می‌گردد. لذا در این مقاله مهم‌ترین اقدامات پلیس کشورمان در پیشگیری وضعی از حملات سایبری مورد بررسی قرار گرفته است.

کلید واژه‌ها

سایبر، تروریسم، پلیس، پیشگیری.

۱- کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشگاه شهید اشرفی اصفهانی، ایمیل: Loghmaninooshin@yahoo.com
۲- کارشناس ارشد حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی واحد دامغان، ایمیل: Rostami.khanghahi@yahoo.com

۱- مقدمه

در دوره معاصر، گروه‌های مهاجم و کشورهای مخاصم به دنبال راه‌هایی ساده برای زدن ضربات سنگین هستند. از این رو، با استفاده از فضای سایبر زیرساخت‌ها، پایگاه‌ها و تأسیسات نظامی سایر کشورها را مورد تهاجم قرار داده‌اند. آنان چند سالی است که با به‌کارگیری فضای سایبر، هم هزینه انجام عملیات خود را کم کرده‌اند و هم تلفات انسانی کمتری داده‌اند. لذا بسیاری از کشورها خود را برای مقابله با این اقدامات خرابکارانه جدید که بسیار آسان‌تر از اقدامات فیزیکی به وقوع می‌پیوندد، آماده می‌کنند.

پیشینه مقابله با جرائم سایبری به دو دهه اخیر باز می‌گردد. در سال‌های اخیر، بسیاری از کشورها به اهمیت مقابله با جرائم سایبری پی برده‌اند و قوانین لازم را برای مقابله با آن تدوین نموده‌اند. قانون تروریسم بریتانیا در سال ۲۰۰۰ به تصویب رسید. ایالات متحده نیز که وجود تروریست‌های سایبری را بیش از هر کشوری احساس نموده بود، قانون امنیت و ضد تروریست و قانون پیشگیری از تروریسم را در سال‌های ۲۰۰۱ و ۲۰۰۵ به تصویب رساند. (Andrew, 2005: 6) در حقوق ایران نیز قانون‌گذار در ماده ۱۱ قانون جرائم رایانه‌ای مصوب ۱۳۸۷ برای اقدامات خرابکارانه سایبری، ضمانت اجراهایی به نسبت سنگین پیش‌بینی نموده است.

اما با توجه به گستردگی و پیچیدگی حملات در فضای مجازی و به دلیل تنوع ابزارهایی که در این فضا وجود دارد، شرایط مقابله با این جرائم در فضای سایبری با شرایط مقابله با آن در محیط فیزیکی بسیار متفاوت است. از این رو، صرف تدوین قوانین و اعمال مجازات برای جلوگیری و کاهش آسیب‌های وارده ناشی از اقدامات تروریستی سایبری، کافی نیست بلکه به‌موازات آن نیازمند اتخاذ تدابیر پیشگیرانه نیز هستیم. پیشگیری وضعی از تروریسم سایبری از جمله این اقدامات می‌باشد. پیشگیری وضعی، متضمن طراحی و مدیریت محیط بلا واسطه (صحنه و محل وقوع جرم) یا همان نظارت و تحت نفوذ در آوردن هر چه پایدارتر و سازمان‌یافته‌تر محل وقوع جرم است که به‌سوی شکل کاملاً خاصی از جرم نشانه می‌رود به‌گونه‌ای که زحمات و خطرات ناشی از اقدام برای ارتکاب جرم را افزایش داده و سود حاصله مورد نظر اکثر مرتکبین را کاهش می‌دهد.

با توجه به تغییر دائمی فناوری اطلاعات و ارتباطات و همچنین با در نظر گرفتن نقص و سکوت قوانین در مواجهه با این جرائم؛ پیشگیری وضعی از حملات سایبری امری ضروری به نظر می‌رسد. هدف از این تحقیق، مروری بر مسائل مرتبط با جنگ و تروریسم سایبری و ارتقای دانش و آگاهی پلیس و اعضای جامعه در حوزه ماهیت تهدیدات سایبری و مقابله با این حملات می‌باشد. بر این اساس، کوشش نموده‌ایم تا با روش توصیفی و به شیوه مطالعه کتابخانه‌ای، نقش به‌کارگیری اقدامات پیشگیرانه وضعی در پیشگیری از حملات سایبری را مورد تجزیه و تحلیل قرار دهیم.

۲- مفاهیم

۲-۱- پیشگیری وضعی

پیشگیری وضعی عبارت است از تغییر در موقعیت‌های خاصی که احتمال ارتکاب جرم در آن زیاد است به‌منظور دشوار و پر خطر کردن یا جاذبه زدایی برای کسانی که قصد ارتکاب جرم دارند. (گسن، ۱۳۷۶: ۶۰۷) پیشگیری وضعی، توانایی تمرکز بر روی یک جرم خاص، از هر نوع که باشد را دارد. این نوع پیشگیری با این فرض که هر یک از جرائم با یکدیگر تفاوت‌هایی دارند، جرائم خاص را مورد هدف قرار می‌دهد. (رزنبام، ۱۳۷۹: ۱۴۹) در پیشگیری وضعی فرض بر آن است که انسان اصولاً موجودی معقول و حسابگر است. انسان‌ها در همه زمینه‌ها، ناخودآگاه دست به محاسبه می‌زنند و مرتکب خطر شدید نمی‌شوند. بزهکاران نیز از این قاعده کلی مستثنا نیستند. بنابراین با بالا بردن هزینه‌های ارتکاب جرم می‌توان مجرمین را از ارتکاب جرم منصرف ساخت. (نجفی ابرندآبادی، ۱۳۸۱: ۵۷) پیشگیری وضعی، به شیوه‌های گوناگونی انجام می‌پذیرد. کلارک شیوه‌های پیشگیری وضعی را به چهار دسته اصلی تقسیم می‌کند. اول؛ شیوه‌هایی که مبتنی بر افزایش زحمت و تلاش مورد نظر برای دستیابی به هدف است. دوم، شیوه‌هایی که مبتنی بر افزایش خطرات مورد نظر برای ارتکاب جرم است. سوم؛ اتخاذ اقدامات به‌منظور کاهش منافع و دستاوردهای مورد انتظار از جرم. چهارم؛ حذف معاذیر یا از بین بردن عواملی که باعث تحریک یا تشویق افراد به ارتکاب جرم می‌شود.

پیشگیری وضعی همچون دیگر انواع پیشگیری، مورد نقد و بررسی‌های گوناگون قرار گرفته است. برخی معتقدند پیشگیری وضعی بزهکاری را از بین نمی‌برد بلکه تنها باعث

جابه‌جایی بزهکاری می‌شود که عبارت است از وقوع مجدد اعمال مجرمانه، پس از اعمال تدابیر پیشگیرانه‌ای که دشواری ارتکاب یک جرم خاص و یا ریسک دستگیر شدن را افزایش می‌دهد. (نجفی ابرندآبادی و هاشم بیگی، ۱۳۷۷: ۱۳۹) بنابراین، گرچه ممکن است در یک مقطع زمانی آمارها به ظاهر از کاهش نرخ جرائم خبر دهند ولی به زودی جرائم دیگری از همان نوع یا نوع دیگر به وقوع خواهد پیوست. در پاسخ به این ایراد باید گفت اولاً- لزوماً چنین نیست که پیشگیری وضعی از یک جرم خاص منجر به ارتکاب جرم دیگر از همان نوع یا نوع دیگر شود بلکه چه بسا با ایجاد مانع در برابر مجرم بالقوه، او اساساً از ارتکاب جرم منصرف شود. بنابراین اگرچه امکان جابه‌جایی وجود دارد اما چنین وضعی به‌ندرت تحقق پیدا می‌کند. ثانیاً- جرم شناسان با تحقیقات خود اثبات کرده‌اند که پیشگیری وضعی نه‌تنها باعث جابه‌جایی جرم نمی‌شود بلکه باعث پخش منافع می‌گردد، یعنی آماجی که مستقیماً مدنظر تدابیر پیشگیرانه نبوده‌اند نیز از خطر جرم رهایی می‌یابند و این یک مزیت برای پیشگیری وضعی است. ثالثاً- انتقال به جرم دیگر، خود مدت زمان ویژه‌ای را طلب می‌کند که در این مدت زمان، جامعه به‌نوعی هرچند موقت از شر مجرم آسوده می‌شود و می‌تواند به فکر تدابیر پیشگیرانه دیگری بیفتد که اساساً جرم را عقیم سازد. پیشگیری وضعی از نظر اخلاقی بهتر از سایر اشکال پیشگیری است زیرا سبب می‌شود زمینه بزه دیدگی مردم در اثر وقوع جرم از بین برود، وسوسه‌ها کاهش یافته و اسباب رنجش و ناراحتی کسانی که از این قواعد پیروی نمی‌کنند فراهم گردد. همچنین این نوع پیشگیری به لحاظ مشارکت دادن آحاد اجتماع، با اصل مردم سالاری نیز سازگارتر است. (حاجی ده آبادی، ۱۳۹۰: ۴۳)

۲-۲- جنگ سایبری

امروزه با پیشرفت جوامع بشری شیوه‌های جنگ نیز دستخوش تغییرات عمده شده است. جنگ سایبری به وضعیتی اشاره دارد که در آن عملیات نظامی بر اساس اطلاعات رایانه‌ای کنترل می‌شود و یا به‌منظور جلوگیری از عملیات دشمن برای ایجاد اخلال در ارتباطات و جلوگیری از دسترسی وی به اطلاعات تلاش می‌شود. در تعریف دیگر، جنگ سایبری به معنای استفاده از اطلاعات برای به حداقل رساندن سرمایه، جنگ‌افزار و نیروی انسانی مورد نیاز برای کسب پیروزی در جنگ است. این نوع جنگ، به خصوص برای صدور فرمان‌ها و کنترل میدان جنگ، جمع‌آوری هوشمندانه اطلاعات و پردازش و

صدور آن‌ها، ارتباط تاکتیکی، موقعیت‌یابی و در نهایت برای استفاده از سلاح‌های هوشمند که قادرند به صورت اتوماتیک و بر اساس اطلاعات دریافتی از ماهواره، علیه دشمن بجنگند، نیازمند تکنولوژی‌های مختلفی است. (ضیایی پرور، ۱۳۸۳: ۱۵) پیشرفت تکنولوژی اطلاعاتی و شبکه‌های رایانه‌ای باعث شد تا صنایع نظامی نیز از این مسئله تأثیر پذیرفته و به سمت رایانه‌ای‌تر شدن پیش روند. امروزه حتی صحبت از چیزی به نام «جنگ از راه دور» به میان می‌آید، جنگی که در آن فرماندهان و افسران، از نقطه‌ای بسیار دور، مستقیماً عملیات نظامی در یک منطقه جنگی را به دست گرفته و آن را هدایت می‌کنند. (همان: ۱۸) به همین دلیل، بسیاری حقوقدانان بر این باورند حملات سایبری می‌تواند وضعیت مخاصمه مسلحانه را به وجود آورد و از این حیث با حملات فیزیکی تفاوت ماهوی ندارد. (Brown, 2011: 71)

ویژگی اصلی جنگ‌های سایبری را می‌توان در اتکای روزافزون فعالیت‌های نظامی به پیشرفته‌ترین فناوری‌های ارتباطی - اطلاعاتی دانست. حذف عامل انسانی از عملیات خطرناک و دقیق جنگ، استفاده روزافزون از هواپیما و تانک‌ها و بالگردهای بدون سرنشین، حذف خونریزی از جنگ و کاهش تلفات با استفاده از سلاح‌هایی که قدرت هدف‌گیری دقیقی دارند و به‌طورکلی، حرکت در جهت دستیابی به سلاح‌هایی که با دقت کامل تنها یک هدف را نشانه می‌گیرند، اهمیت روزافزون فرماندهی عملیات ویژه و عملیات فضایی ارتش، جایگزینی نیروهای هوشمند و تعلیم دیده‌ای که بتوانند با مردمان و فرهنگ‌های گوناگون ارتباط بهتری برقرار کنند، همچنین تغییر در شیوه‌های جمع‌آوری و تجزیه و تحلیل اطلاعات و تغییر در فرآیند تصمیم‌گیری در عرصه‌های روابط بین‌الملل و نظامی تأثیر شگرف در تغییر شیوه‌های جنگ بر جای گذاشته که از نمودهای بارز تأثیر جنگ سایبری در صحنه نبرد است. (مرادی، ۱۳۸۹: ۴۴۳) «شبکه‌های ارتباطات دیتا و فناوری جدید انفورماتیک در حال ایجاد تحولات اساسی در نبردها هستند، به طوری که در حال حاضر تمامی تشکل‌های نظامی جدید روی فناوری انفورماتیک و ارتباطات سرمایه‌گذاری می‌کنند. دانستن همان‌طور که کلید اصلی برای تولید است، می‌تواند به کلیدی اصلی برای تخریب تبدیل شود و دقیقاً به همین دلیل، تعداد رایانه‌ها به‌زودی می‌تواند از تعداد توپ و تفنگ‌ها در ارتش‌های مدرن جهان پیشی بگیرد». (همان: ۴۴۳)

۲-۳- تروریسم سایبری

مجمع عمومی سازمان ملل متحد در قطعنامه سال ۱۹۸۴، تروریسم را این‌گونه تعریف می‌کند: «تروریسم، مجموعه فعالیت‌های مجرمانه و خشونت‌آمیزی است که گروه‌های سازمان‌یافته برای ایجاد رعب و وحشت انجام می‌دهند تا به این ترتیب، نیل به اهداف به‌اصطلاح سیاسی را میسر سازند». در حقوق ایران بر اساس ماده یک لایحه مبارزه با تروریسم که در سال ۱۳۸۲ از طرف دولت به مجلس شورای اسلامی ارسال شده، تروریسم این‌گونه تعریف شده است: «ارتکاب یا تهدید به ارتکاب جرائم و اقدامات خشونت‌آمیز از طریق به وحشت افکندن مردم جهت تأثیرگذاری برخط مشی، تصمیمات و اقدامات دولت جمهوری اسلامی ایران، سایر کشورها و سازمان‌های بین‌المللی، جرم تروریستی محسوب می‌شود». هرچند این تعریف در حد یک تعریف پیشنهادی به قوه مقننه ارزش دارد؛ در عین حال، با این اشکال اساسی روبرو است که صرفاً به عملیات تروریستی که با ترس و وحشت عمومی قصد تأثیرگذاری بر خط مشی دولت ایران یا سایر دولت‌ها را دارند توجه دارد. در حالی که ممکن است منظور تروریست‌ها از توسل به خشونت، یک هدف مذهبی یا ایدئولوژیک یا به دست آوردن منافع مادی و اقتصادی باشد.

بنابراین، تروریسم سایبری که حاصل تلاقی تروریسم و فضای مجازی است عبارت است از حمله یا تهدید به حمله علیه رایانه‌ها و اطلاعات ذخیره شده در آن‌ها؛ هنگامی‌که به‌منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود. (عباسی و هاشمی، ۱۳۸۹: ۶۲)

بر سر وجود یا عدم وجود تروریسم در فضای سایبری اختلاف‌نظر وجود دارد. اما اقدامات خرابکارانه‌ای که تا به حال از سوی تروریست‌ها در فضای سایبری صورت گرفت آن‌قدر گسترده و مخرب بوده که این باور را قاطعانه می‌رساند که تروریسم سایبری وجود دارد. یکی از نویسندگان در خصوص اقدامات خرابکارانه سایبری، عبارت سلاح‌هایی با تخریب بالا[1] را به کار برده است که با این سلاح می‌شود به هر کجا

1- Weapons of mass Destruction

حمله‌ور شد. این سلاح مخرب می‌تواند به سیستم‌های الکترونیکی و خطوط کنترل هوایی تأسیسات نظامی حمله‌ور شود. (Power and Forte, 2006: 4)

مهم‌ترین استفاده تروریست‌ها از فضای سایبر، استفاده از آن در جهت خرابکاری به‌طور مستقیم است.[۱] به‌عنوان‌مثال تروریست‌ها در حمله سایبری به نیروی هوایی آمریکا، توانستند ۱۷ روز حمله خود را ادامه دهند و نیروی هوایی را به حالت آماده‌باش درآورند. همچنین گروه تروریستی با نام گارد امنیتی یونیکس[۲] صد و یازده حمله سایبری علیه هند صورت داده است.[۳] (Nagpal, 2002: 3) اقدامات خرابکارانه سایبری گاهی در منازعات بین دو کشور هم دیده می‌شود. در آوریل ۲۰۰۱ هکرهای چینی و آمریکایی به مواضع سایبری هم حمله‌ور شدند. نتیجه این حملات در آمریکا این بود که سایت کاخ سفید قطع گردید همچنین سازمان عدالت قضایی کالیفرنیا دچار آسیب گردید. (Sheyri, 2005: 552) در همین سال صدام حسین اقدام به ایجاد ۱۰۰ وب‌سایت خرابکاری سایبری علیه آمریکا نمود. (Stohi, 2007: 6) در سال ۲۰۰۵ حملات سایبری علیه آمریکا تشدید شد و تروریست‌ها خسارات زیر بنایی را به تأسیسات نظامی این کشور وارد نمودند. حتی FBI هم مورد حملات تروریست‌های سایبری قرار گرفت. (Grake, 2007: 2) حملات سایبری علیه جمهوری استونی در سال ۲۰۰۷ میلادی که به مدت ۲۲ روز به طول انجامید، نمونه دیگری از این دست حملات بود. طی این حملات که توسط دولت روسیه صورت پذیرفت بسیاری از اطلاعات نظامی و سری استونی مورد هجوم قرار گرفت. این حملات در واکنش به تصمیم دولت استونی برای تبدیل بنای یادبود جنگ جهانی دوم دولت شوروی به گورستان نظامی، انجام گرفت. این اقدام با انتقاد جمع کثیری از سران روسی و همچنین اقلیتی از روس‌های مقیم در استونی مواجه شد و نهایتاً منجر به حملات گسترده سایبری از سوی روس‌ها شد. (martin, 2009: 1)

۱- در این نوشتار هم بیشتر بر این نوع استفاده تروریست‌ها تکیه شده است.

2- The Unix security Guards

۳- البته برخی معتقدند اقدامات خرابکارانه علیه کامپیوترها را فقط می‌توان به دو دسته فیزیکی (Physical) و مصنوعی (Semantic) تقسیم نمود. در حملات نوع اول، کامپیوترها با سلاح فیزیکی مثل بمب، نابود می‌شوند. اما در حملات مصنوعی، تروریست‌ها اقدام به پخش اخبار دروغین وسیع از طریق میل‌ها و وب‌سایت‌ها می‌کنند و از این طریق به اهداف خود می‌رسند. (Prichard, 2004: 28) البته این تقسیم‌بندی ناقص است و باید نوع سومی (حملات سایبری) وجود داشته باشد.

در حمله آمریکا به کوزوو نیز حملات سایبری از کشورهای صربستان، چین و روسیه به ناتو انجام گرفت. هرچند هکرها وارد اطلاعات محرمانه ناتو نشدند اما در اقدامات آن خلل وارد کردند. (Moly, 2009: 10) در سال‌های اخیر، تأسیسات هسته‌ای ایران نیز آماج حملات تروریستی سایبری بوده است. «دیوید آلبرایت» مدیر موسسه علوم و امنیت بین‌الملل، گفته است ایران در برابر حملات سایبری چندان ایمن نیست و برای محافظت از برنامه غنی‌سازی خود در برابر نرم‌افزارهای آلوده با مشکلات عدیده‌ای رو به رو خواهد بود. وی با اشاره به بدافزار «استاکس نت» گفت که حملات بعدی می‌توانند خشن‌تر باشند و در تأسیسات هسته‌ای حساس ایران انفجارهایی ایجاد کنند.[۱]

۳- تفاوت‌های عملیات سایبری در مقایسه با عملیات فیزیکی

مهم‌ترین تفاوت‌های عملیات خرابکارانه در فضای سایبر در مقایسه با عملیات فیزیکی عبارت است از:

الف- حملات سایبری در مقایسه با حملات فیزیکی تنوع فراوانی دارد. مهاجمین ابزارهای بسیار فراوانی برای ضربه زدن از طریق فضای سایبری دارند. هک کردن سیستم محافظ، اخلال در شبکه‌های مرکزی، تخریب اطلاعاتی صنایع و تأسیسات نظامی و ... از جمله روش‌هایی است که مهاجمین به‌راحتی می‌توانند با کمک فضای سایبری بکار ببندند.

ب- هرچند تنوع اقدام در حملات سایبری بسیار بالاست اما فقط افرادی می‌توانند به این اقدامات دست بزنند که بسیار حرفه‌ای باشند و آموزش کافی در این زمینه دیده باشند. (Souma, 2011: 79 & 80) بنابراین قید «حرفه‌ای» برای این نوع از مهاجمین بکار می‌رود. همچنین، هزینه حملات سایبری بسیار کمتر از حملات فیزیکی است. عوامل و عناصر نیز در فضای سایبر سهل‌الوصول‌تر و ارزان‌تر هستند.

ج- بر خلاف عملیات فیزیکی که مهاجمین در زمان و مکان معین به هدف خاص حمله می‌کنند، محدوده حمله در حملات سایبری بسیار وسیع است و این احتمال وجود دارد که یک حمله همه‌جانبه در هر منطقه صورت گیرد. (Ibid)

۱- به نقل از وب‌سایت گرداب؛ وابسته به مرکز بررسی جرائم سازمان‌یافته، کد خبر ۱۱۵۴۹، تاریخ انتشار ۲۴ تیر ۱۳۹۱.

د- تحقیقات در زمینه کشف حملات سایبری بسیار مشکل‌تر از حملات فیزیکی است. با توجه به ویژگی منحصر به فرد فضای سایبر، مهاجمین سایبری بعد از اقدامات خرابکارانه، به سرعت مخفی می‌شوند و یا آنکه اقدامات خرابکارانه را طوری طراحی می‌کنند که هیچ اثری از آن‌ها باقی نماند.

ه- تفاوت دیگر حملات سایبری در مقایسه با حملات فیزیکی؛ قابلیت طراحی، نتیجه‌گیری و اجرا از راه دور است. برای حمله سایبری نیاز به جا به جایی فیزیکی نداریم.

۴- معرفی برخی از ویروس‌ها و کرم‌های سایبری

تا به حال چندین ویروس و کرم با اهداف حملات سایبری شناسایی شده‌اند. از مهم‌ترین آن می‌توان به کرم نیمدا، ویروس آرورا و ویروس استاکس نت اشاره کرد که در ادامه به معرفی آن‌ها می‌پردازیم.

۴-۱- کرم نیمدا[1]

کرم نیمدا برای اهداف تروریستی طراحی شده و کامپیوترهای خانگی را هدف قرار داده بود. همچنین علاوه بر کامپیوترهای خانگی به ایمیل‌ها و وب‌سایت‌های دولتی نیز حمله‌ور می‌شد. این کرم اینترنتی از آسیب‌پذیری ویندوز استفاده می‌کرد و به سه روش اصلی منتشر می‌شد: ایمیل، وب و به اشتراک گذاشتن شبکه. تروریست‌ها با پخش این بدافزار خسارت فراوانی را برای دولت‌ها به وجود آوردند. مرکز اصلی خسارت، کشورهای انگلستان، آمریکا و هنگ‌کنگ بود. (Hinde, 2001: 69)

۴-۲- ویروس آرورا[2]

این ویروس مخرب برای اولین بار در سال ۲۰۱۰ ظاهر گشت و قربانیان زیادی در سرتاسر دنیا گرفت. این ویروس به‌راحتی از سطح دفاعی کامپیوترها عبور می‌کرد. کارشناسان عقیده داشتند که این ویروس تروریستی آن‌قدر خسارت به بار آورد که تروریست‌ها به تمام اهداف خود رسیدند تا اینکه بالاخره توسط یک نرم‌افزار از پای در

1- Nimda
2- Aurora

آمد. برخی کارشناسان این ویروس مخرب را یکی از پیچیده‌ترین بدافزارهای شناخته شده می‌دانند. (Willems, 2011: 17)

۴-۳- ویروس استاکس نت[1]

ویروس استاکس نت اولین بار در ماه جولای سال ۲۰۱۰ توسط شرکت زیمنس شناسایی شد. این بدافزار همان سال در سطحی وسیع از برزیل تا مصر انتشار یافت، ولی بیشترین میزان آلودگی با ۶۰ درصد در ایران گزارش شد. ویروس تروریستی استاکس نت به‌گونه‌ای طراحی شده بود که به محض اتصال کابل کامپیوتر، وارد مکان مورد نظر شده و نیازی به انتقال داده نبود و حتی با وصل کردن چاپگر و اسکنر هم منتقل می‌شد. کارشناسان عقیده دارند که این ویروس به یک دوازدهم از صنایع جهان وارد شده اما مهم‌ترین هدف آن برنامه هسته‌ای ایران بوده است. در خصوص اینکه آیا این ویروس تروریستی توانسته است به اهداف مورد نظر خود در ایران دست یابد یا خیر بین کارشناسان اختلاف‌نظر وجود دارد. (Ibid)

۵- پیشگیری وضعی از حملات سایبری

با توجه به ویژگی خاص فضای سایبری، امکان استفاده از تمامی راهکارهای پیشگیری وضعی در مورد تروریسم سایبری در اماکن و پایگاه‌های نظامی وجود نخواهد داشت و فقط برخی از آن‌ها قابل استفاده خواهد بود. در این قسمت راهکارهای پیشگیری وضعی که برخی کشورها اتخاذ کرده‌اند یا مورد توصیه دانشمندان قرار گرفته است بررسی می‌شود. پلیس فضای تولید و تبادل اطلاعات ایران با نام اختصاری پلیس فتا، به‌عنوان متولی تأمین نظم و امنیت در فضای سایبر باید با همکاری سایر نهادها این راهکارها را در کشورمان اجرایی نماید.

۵-۱- آموزش مقابله با حملات سایبری

آموزش مقابله با حملات سایبری یکی از مهم‌ترین و مؤثرترین عناصر پیشگیری از این‌گونه حملات است. کاربران اینترنت باید با شیوه استفاده صحیح از فضای سایبر به‌طوری‌که خطری آن‌ها و بخش مربوطه آن‌ها را تهدید نکند، آشنا باشند.

1- Stuxnet

(Ramsaroop, 2003: 12)مطالعات نشان داده است چنانچه کاربران به خوبی با استفاده صحیح از محیط سایبر آشنا شوند، خطر حملات سایبری تا ۸۰٪ کم می‌شود. (Grake, 2007: 6)کاربران باید از خطرات موجود آگاه شوند و انواع گروه‌های تروریستی سایبری، ابزارهای آن‌ها و راهکارهای پیشگیری از آن را بشناسند. به‌عنوان‌مثال باید بدانند که نباید به کامپیوترهای اداری حافظه خارجی وصل کنند یا اینکه نباید با این کامپیوترها ایمیل‌ها را چک کنند. (Willems, 2011: 18)

بر این اساس، افزایش آگاهی کاربران در خصوص خصایص امنیتی، تهدیدات، فرصت‌ها و رفتار مناسب در اینترنت، به امری ضروری و حیاتی تبدیل شده است. در این رابطه لازم است به این نکته مهم اشاره گردد که بقاء سیستم وابسته به امنیت سیستم‌ها در سمت دیگر بوده و حل مشکل سیستم به تنهایی کافی نخواهد بود و در این رابطه لازم است به تمامی کاربران در خصوص نحوه استفاده از کامپیوترهای خود با لحاظ نمودن پارامترهای ایمنی و امنیتی، آموزش‌های لازم و مستمر ارائه گردد. علاوه بر موارد فوق، لازم است به مصرف‌کنندگان محصولات نرم‌افزاری آموزش‌های خاصی در مورد نحوه تهیه و نصب نرم‌افزارهای ایمن ارائه گردد.

از جمله ابزارهایی که بدین منظور پیشنهاد شده است، سیستم جامع آخرین اطلاعات سایبری است. این سیستم، آخرین اطلاعات از چگونگی روش صحیح استفاده از فضای سایبر، آخرین اخبار از تروریست‌های سایبری و سایر اطلاعات مربوط به گروه‌های مهاجم و خرابکار را به‌تمامی کاربران ارائه می‌دهد. (Jones, 2002: 13) حملات سایبری هنگامی اتفاق می‌افتد که کاربران اینترنتی با عدم علم به حمله و عدم شناسایی شیوه‌های حمله، کارهایی را انجام دهند که در معرض آسیب اینترنتی قرار گیرند. بنابراین، اگر کاربران نسبت به این‌گونه حمله‌های اینترنتی آگاهی کامل یابند و درک کنند که حملات سایبری همانند حملات فیزیکی می‌تواند آسیب بسیار زیادی وارد کند، مهاجمین فرصت ارتکاب جرم پیدا نمی‌کنند. (گرکی، ۱۳۸۹: ۱۹۱)

۵-۲- بهبود امنیت در فضای سایبر

چنانچه در فضای سایبر امنیت به‌صورت کامل برقرار شود، دیگر مجالی برای فعالیت مهاجمین سایبری نخواهد بود. امنیت پروسه‌ای است که طی آن یک سیستم در مقابل

انواع مختلف تهدیدات داخلی و خارجی ایمن می‌شود. شناسایی بخشی که باید مورد حفاظت قرار گیرد، تصمیم‌گیری مواردی که باید در مقابل آن‌ها از بخش مورد نظر حمایت کرد، تصمیم‌گیری درباره چگونگی تهدیدات و مرور مجدد و مداوم پروسه و تقویت آن در صورت یافتن نقاط ضعف؛ از جمله مواردی است که برای ایجاد امنیت سیستم‌ها در فضای سایبر پیشنهاد می‌گردد.

علت افزایش حملات سایبری در مقایسه با حملات فیزیکی را باید ناشی از سهل‌انگاری دولت‌ها دانست. دولت‌ها در حفظ امنیت فیزیکی تلاش‌های خوبی انجام داده‌اند و از بسیاری از حملات جلوگیری کرده‌اند اما محیط سایبر را فراموش کرده‌اند تا اینکه مهاجمین و گروه‌های مخاصم برای ادامه فعالیت خود وارد این عرصه شدند، محیطی که در آن خطری آن‌ها را تهدید نمی‌کند. در حالیکه با افزایش خطرات قابل پیش‌بینی در این محیط، آنان جسارت کمتری برای انجام اعمال مجرمانه خواهند داشت. کارشناسان بر این باورند که امنیت فضای سایبر باید بهبود باید. برخی از تدابیر حفظ امنیت در فضای سایبر از قرار ذیل است:

۵-۲-۱- استفاده از سیستم‌های حفاظتی سایبری

یکی از اشتباهات دولت‌ها در زمینه بهبود امنیت در فضای سایبر این است که ابتدا از سیستم‌های حفاظتی جامعی استفاده می‌کنند اما به مرور زمان فراموش می‌کنند که این سیستم‌ها باید در هر دوره کامل‌تر از دوره قبل شود. سیستم‌های امنیتی سایبری باید مورد بازبینی قرار گیرند و خطرات بالقوه آنان سنجش شوند. بر حسب نوع اطلاعات در فضای سایبری و اینکه اطلاعات مربوط به چه بخشی باشد، نوع حفاظت متفاوت خواهد بود. (Ramsaroop, 2003: 16)

علاوه بر این، بسیاری از دولت‌ها اقدامات امنیتی نظیر استفاده از محصولات امنیتی و همچنین به روز رسانی سیستم‌های حافظتی را رعایت نمی‌کنند. در حال حاضر، حملات سایبری در حال گسترش است و هر سال نسبت به سال قبل حملات بیشتری انجام می‌پذیرد. برای مقابله صحیح با این حملات باید هر سال نسبت به سال قبل اقدامات دفاعی همه‌جانبه‌تری اتخاذ گردد. (Hinde, 2003: 19)

۵-۲-۲- اعمال تدابیر نظارتی در فضای سایبری

در فرآیند ارتکاب جرم، مجرمان به‌طورمعمول به دنبال اهداف آسیب‌پذیر و حمایت نشده هستند. پیشگیری وضعی از جرم، از گذشته تاکنون به شیوه‌های مختلفی اجرا می‌شده است. افزایش خطر دستگیری یا شناخته شدن مرتکب از طریق نظارت و کنترل، یکی از این شیوه‌ها است. (کوسن، ۱۳۸۴: ۳۲۴) اعمال تدابیر نظارتی در فضای سایبری، سختی ارتکاب جرم را افزایش و میزان ارتکاب حملات سایبری را کاهش می‌دهد. سیستم کلان مبارزه با جرم که از سوی پلیس اتخاذ می‌شود، چه در محیط فیزیکی و چه در فضای مجازی یکسان است و پلیس در پیشگیری از جرائم سایبری همان جایگاه خود را خواهد داشت. در واقع اقدامات پلیس برای پیشگیری از وقوع این جرائم، چیزی جز مبارزه وضعی و سیاست عام این نهاد در مقابله با سایر جرائم نیست اما آنچه باعث تفاوت در این دو حوزه می‌شود، ویژگی‌های منحصر به فرد جرائم سایبری است که شیوه‌های اجرایی خاص خود را به‌منظور تحقق این سیاست عام طلب می‌کند. (رضوی، ۱۳۸۰: ۱۳۴) پلیس فضای تولید و تبادل اطلاعات ایران یا پلیس سایبری ایران با نام فتا، از جمله واحدهای تخصصی نیروی انتظامی جمهوری اسلامی ایران است که سند راهبردی آن اسفند ماه سال ۱۳۸۷ به تصویب هیئت‌وزیران رسید. ایجاد امنیت و کاهش مخاطرات برای فعالیت‌های علمی، اجتماعی و اقتصادی، همچنین مراقبت و پایش از فضای تولید و تبادل اطلاعات به‌منظور پیشگیری از تبدیل شدن این فضا به بستری برای انجام جرائم سایبری؛ از جمله اهداف شکل‌گیری پلیس فتا است. این نهاد نقش مهمی در پیشگیری از حملات سایبری ایفا می‌کند. بر این اساس، می‌توان با استفاده بهینه از شهروندان؛ زمینه لازم برای آموزش نظارت در فضای سایبر به آنان جهت همکاری با پلیس فتا را فراهم و از این طریق از حملات سایبری پیشگیری نمود.

نظارت شبکه‌ای فنی نیز یک اقدام پیشگیرانه است که باید موردتوجه قرار گیرد. در نظارت شبکه‌ای فنی، ابزارها یا برنامه‌هایی بر روی سیستم نصب می‌شوند و کلیه فعالیت‌های شبکه‌ای کاربران، حتی ضرباتی که بر روی صفحه‌کلیدشان زده‌اند یا نقاطی را که به‌وسیله ماوس بر روی آن‌ها کلیک کرده‌اند ضبط می‌کنند. پلیس می‌تواند با بررسی این سوابق، موارد غیرقانونی را تحت پیگرد قرار دهد.

شایان ذکر است نظارت شبکه‌ای در صورتی مؤثر خواهد بود که کاربر بداند فعالیت‌هایش تحت نظارت قرار دارد، زیرا همان‌طور که می‌دانیم، نظارت مخفی فقط برای جمع‌آوری ادله علیه متهم به کار می‌رود و هیچ اثر پیشگیرانه‌ای ندارد. (جلالی فراهانی، ۱۳۸۴: ۱۴۴)

۵-۲-۳- لزوم صدور مجوز برای استفاده از اینترنت

اگرچه برای دسترسی به اینترنت و فضای سایبر، کنترل مرزی وجود ندارد اما می‌توان تدابیری در جهت محدود کردن دسترسی به آن‌ها اتخاذ نمود. افزایش تعداد کاربران ناشناس اینترنت، تعداد هدف‌ها و متخلفان را افزایش می‌دهد. حتی اگر ۰/۱ درصد کاربران اینترنت مرتکب جرم شوند، تعداد کلی مجرمان بیشتر از یک میلیون نفر خواهد بود. (گرکی، ۱۳۸۹: ۱۴۱) در این خصوص تلاش می‌شود بر اساس معیارهایی خاص، از ورود اشخاص ناشناس یا فاقد اعتبار جلوگیری شود. نمونه ساده این اقدام، به کارگیری گذرواژه است که در گذشته و اکنون جایگاه خود را حفظ کرده است. به این ترتیب، تنها کاربرانی حق بهره‌برداری از یک سیستم یا سایت را خواهند داشت که پس از طی مراحل شناسایی و کسب اعتبار لازم، گذرواژه مربوط را دریافت کنند. رمزگذاری روی داده‌ها (غیرقابل فهم یا غیر قابل خوانده شدن داده‌ها)، لایه سوکت های امن به‌عنوان استاندارد ایمنی و رمز عبور معتبر، جداسازی داده‌ها روی کامپیوترهای متعدد و تفکیک پایگاه داده‌ها (جدا نگهداشتن اطلاعات کاربران) روش‌های پیشرفته در ایمنی داده‌ها می‌باشند که می‌تواند از دستیابی هکرها به داده‌ها جلوگیری کنند. (حسن بیگی، ۱۳۸۸: ۱۶۵)

۵-۳- تشکیل ستاد ویژه در جهت گرفتن فرصت از مهاجمین سایبری

یکی از روش‌هایی که از وقوع حملات سایبری پیشگیری می‌کند، تشکیل کارگروه و ستادهایی است که در جهت حذف فرصت‌های خرابکاری تروریست‌ها فعالیت کنند. به‌عنوان نمونه، پس از سقوط شوروی، پروژه دفاع ملی در برنامه «دفاع هملند» مطرح گشت که بر اساس این پروژه، در مسئله امنیت باید یک باز تعریف صورت گیرد. یکی از جنبه‌های «دفاع هملند»، مقابله با تروریسم سایبری و دفاع همه‌جانبه‌تر بود. (Andrew, 2005: 822) با توجه به این پروژه، ستادهایی وظیفه بر قرار کردن امنیت در فضای سایبر را بر عهده گرفتند. این

ستادها از طریق سلب فرصت خرابکاری از تروریست‌های سایبری فعالیت می‌کنند. سازمان مرکزی پیشگیری ملی آمریکا[1] نمونه‌ای دیگر از مراکزی است که بر اساس قانون، یکسری اختیارات به این سازمان در فضای سایبر اعطا شده است. اختیارات این سازمان شامل کشف و پاسخ به جرائم سایبری، ارعاب خرابکاران سایبری و تحقیق و تفحص علیه خرابکاری‌های سایبری است. همچنین این سازمان وظیفه اعمال ضمانت اجراهای قانونی علیه مهاجمین سایبری را نیز بر عهده دارد. از دیگر اختیارات این سازمان می‌توان به حمایت از بخش‌هایی که در پروژه دفاع ملی همکاری می‌کنند، اشاره نمود. (Sans, 2011: 4) در حقوق ایران نیز تشکیل یک ستاد دائمی برای مقابله با حملات سایبری همانند ستادی که چندی پیش برای مقابله با ویروس «استاکس نت» شکل گرفت، لازم و ضروری به نظر می‌رسد.

۵-۴- طرح مسئولیت دفاع برای همه

یکی از اصول مهم و زیربنایی در پیشگیری وضعی از حملات سایبری این است که هر فرد، خود مسئول مراقبت از داده‌ها و پایگاه خویش باشد. (فهیمی، ۱۳۸۰: ۱۰۶) حتی برخی از کشورها با ایجاد این طرح، تمام اتباع کشور خود اعم از نظامی و غیر نظامی را مسئول مبارزه با تروریسم سایبری کرده‌اند. تا وقتی که کاربران اینترنت مسئول نباشد، به حفظ امنیت در فضای سایبر اهمیت نمی‌دهند. اما چنانچه یک طرح کلی همه افراد جامعه را موظف به رعایت و حفظ امنیت کند، نتیجه مناسبی به وقوع خواهد پیوست. (Ramsaroop, 2003: 2) استرالیا از جمله کشورهایی بوده است که افراد تبعه خود را به‌موجب قانون، موظف نموده است که ایمنی را در فضای سایبر رعایت نمایند. (Ellsmore, 2002: 18)

با طرح «مسئولیت دفاع برای همه»، هر فرد موظف است در وارد کردن پسوردها نهایت دقت را انجام دهد و از انجام کارهای مخاطره‌آمیز در فضای سایبر خودداری کند. زیرا با بی‌احتیاطی یک کاربر، ممکن است کلیه تدابیر امنیتی بی‌اثر گردد و مهاجمین سایبری به اهداف خود برسند.

1- Notional infrastructure protected center

۵-۵- ایجاد سپر دفاع سایبری

برخی از کشورها برای مبارزه و پیشگیری همه‌جانبه از حملات سایبری، اقدام به ایجاد سپر دفاع سایبری نموده‌اند. به‌عنوان نمونه، در اروپا از ۱۰ می ۲۰۱۰ سپر دفاع سایبری فعال گشت و بسیاری از کشورهای اروپایی در آن مشارکت نمودند. این طرح در آمریکا نیز با نام دفاع سایبری بین‌المللی پنتاگون[1] به وجود آمده است. هدف از شکل‌گیری سپر دفاعی در اروپا، پاسخ سریع به حملات سایبری بوده است. این سپر دفاعی برای سه هدف شکل گرفته است. الف– باید از اطلاعات حساس در فضای سایبر محافظت کند. ب- تمام اقدامات امنیتی و تمام اقدامات دفاعی ممکن را با استفاده از هر ابزاری به کار بندد تا مانع خرابکاری سایبری گردد. ج- باید در برابر حملات آینده تروریست‌ها و ابزارهای آنان مقاوم باشد و به روز شده باشد.

در حال حاضر طرح سپر دفاع سایبری در کشورهایی مانند استونی، سوئد و اسکاتلند اجرا می‌شود و وظیفه حفاظت از پایگاه‌ها و زیرساخت‌ها را به عهده دارد. البته برخی از کشورها مانند سوئد علاوه بر استفاده از سپر دفاع سایبری اروپایی، به‌طور اختصاصی اقدام به ایجاد چنین طرحی در سطح کشور خود کرده‌اند. (Ceers, 2010: 6 & 7)چین هم از جمله کشورهایی است که اقدام به ایجاد سپر دفاعی مشابهی در سطح کشور خود نموده است. اما نکته‌ای که کارشناسان به آن اشاره می‌کنند این است که تجربه نشان داده است ایجاد چنین سپر دفاعی به‌طور کامل امنیت را برقرار نمی‌کند. این طرح باید به همراه سایر اقدامات پیشگیرانه اجرا گردد. (Sauver, 2008: 60)

نمونه دیگر، فرماندهی سایبری آمریکا است که جزئی از آژانس امنیت ملی آمریکا[2] می‌باشد. فرمان تشکیل فرماندهی سایبری آمریکا توسط رابرت گیتس، وزیر دفاع آمریکا، در تاریخ ۲۳ ژوئن ۲۰۰۹ به فرماندهی استراتژیک ایالات متحده داده شد و در سپتامبر همان سال این نهاد شروع به فعالیت نمود. آژانس امنیت ملی آمریکا که وظیفه طراحی، خرید و نگهداری زیرساخت‌های ارتباطی وزارت دفاع را بر عهده دارد، برای چند دهه شبکه‌های وزارت دفاع را اداره می‌کند و قرار است پشتیبانی‌های لازم را از فرماندهی سایبری آمریکا به عمل آورد. هدف از تأسیس فرماندهی سایبری ایالات

1- Pentagon international cyber Defense
2- NSA

متحده آمریکا طراحی، رصد، ایجاد هماهنگی و اجرای عملیات مورد نظر آمریکا در فضای سایبر است. تأمین امنیت مداوم و دفاع از شبکه‌های اطلاعاتی و دفاعی پنتاگون و همچنین پشتیبانی از سایر اماکن نظامی در فضای سایبری نیز بر عهده این فرماندهی است. در مجموع می‌توان گفت این نهاد انواع حمایت سایبری از پنتاگون و منافع نظامی آمریکا را بر عهده دارد.

۶- نتیجه‌گیری

در دوره معاصر، مهاجمین و گروه‌های مخاصم با سوءاستفاده از سهولت ارتکاب جرم در فضای سایبری، اهداف مختلف را در بسیاری از کشورهای جهان مورد تهاجم قرار داده‌اند. آنچه از اتفاقات به وقوع پیوسته در سال‌های اخیر نتیجه‌گیری می‌شود اینکه اولاً- حملات سایبری شامل تروریسم و جنگ سایبری به‌واقع وجود دارد و ثانیاً- هر کشوری که بیشتر از فضای سایبر استفاده کند در مقابل حملات گسترده‌تر سایبری قرار دارد. در سال‌های اخیر، مراکز هسته‌ای و نظامی ایران نیز آماج حملات سایبری بوده است. اما علیرغم افزایش تعداد آمار این حملات؛ قانونمند شدن برخورد با آن، بسیار دیرتر از زمان مورد انتظار آغاز شد و قانون جرائم رایانه‌ای در سال ۱۳۸۷ به تصویب رسید. در دوره معاصر به‌موازات پیشرفت‌های حاصله در فناوری‌های رایانه‌ای، مهاجمین نیز از ابزارهای جدید بهره‌مند شده و حملات خود را به اشکال پیچیده‌تر و گسترده‌تر از قبل انجام می‌دهند. لذا صرف تدوین قوانین برای کاهش آسیب‌های وارده ناشی از اقدامات آنان کافی نیست بلکه اتخاذ تدابیر پیشگیرانه به‌ویژه پیشگیری وضعی از حملات سایبری ضروری به نظر می‌رسد.

با توجه به ماهیت خاص فضای سایبر نسبت به محیط فیزیکی، اقدامات پیشگیری وضعی از حملات سایبری در تمام ابعاد قابل‌اجرا نیستند اما برخی از روش‌ها از جمله آموزش شیوه صحیح استفاده از فضای سایبر به شهروندان، اعمال تدابیر نظارتی بر فعالیت‌های آنان در فضای سایبر، ایجاد سپر دفاعی و همچنین استفاده بهینه از شهروندان برای تشکیل ستاد ویژه در جهت گرفتن فرصت از مهاجمین سایبری؛ به‌خوبی و تا حد زیادی می‌تواند از اقدامات خرابکارانه سایبری بکاهد. لذا پیشنهاد می‌گردد پلیس کشورمان به‌منظور پیشگیری از حملات سایبری، با همکاری مقامات وزارت دفاع و پشتیبانی نیروهای مسلح، هر چه سریع‌تر ستاد دائمی برای مقابله با این‌گونه حملات را تشکیل دهد.

منابع

- جلالی فراهانی، امیرحسین، (۱۳۸۵)، «تروریسم سایبری»، مجله فقه و حقوق، شماره ۱۰.
- حاجی ده آبادی، محمدعلی، (۱۳۹۰)، «تقریرات جرم‌شناسی»، دوره کارشناسی ارشد دانشگاه قم.
- حسن بیگی، ابراهیم، (۱۳۸۸)، «حقوق و امنیت در فضای سایبر»، تهران، دانشگاه عالی دفاع ملی.
- رزنبام، دنیس و همکاران، (۱۳۷۹)، «پیشگیری وضعی از جرم»، مترجم رضا پرویزی، مجله حقوقی دادگستری، شماره ۳۲.
- رضوی، محمد، (۱۳۸۰)، «جرائم سایبری و نقش پلیس در پیشگیری از آن»، فصلنامه دانش انتظامی، شماره اول.
- ضیایی پرور، حمید، (۱۳۸۳)، جنگ نرم ۱: ویژه جنگ رایانه‌ای، انتشارات موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، تهران.
- عباسی، مهدی و هاشمی، تورج، (۱۳۸۹)، «نقش رسانه‌ای اینترنت در ناهنجاری‌های اجتماعی در فضای سایبری در میدان جنگ نرم»، ماهنامه مهندسی فرهنگی، شماره ۴۹ و ۵۰.
- فهیمی، مهدی، (۱۳۸۰)، «جرائم رایانه‌ای و روش‌های مقابله و پیشگیری از آن»، فصلنامه دیدگاه‌های حقوقی، دانشکده علوم قضایی و خدمات اداری، شماره ۲۳ و ۲۴.
- کوسن، موریس، (۱۳۸۴)، «نظارت ویدئویی؛ دلایل موفقیت و شکست»، مترجم شهرام ابراهیمی، مجله تخصصی الهیات و حقوق، شماره ۱۵ و ۱۶.
- گرکی، مارکو، (۱۳۸۹)، «جرائم سایبری: راهنمایی برای کشورهای در حال توسعه»، مترجم مرتضی اکبری، تهران، انتشارات نیروی انتظامی جمهوری اسلامی ایران.
- گسن، ریموند، (۱۳۷۶)، «روابط میان پیشگیری وضعی و کنترل جرم»، مترجم نجفی ابرندآبادی، مجله تحقیقات حقوقی، شماره‌های ۱۹ و ۲۰.
- مرادی، حجت اله، (۱۳۸۹)، قدرت و جنگ نرم؛ از نظریه تا عمل، نشر ساقی، تهران.
- نجفی ابرندآبادی، علی حسین، (۱۳۸۱)، «تقریرات جرم‌شناسی»، دوره کارشناسی ارشد مجتمع آموزش عالی قم.
- نجفی ابرندآبادی، علی حسین و هاشم بیگی، حمید، (۱۳۷۷)، «دانشنامه جرم‌شناسی»، تهران، انتشارات دانشگاه شهید بهشتی.
- A. Jonse, (2005), Cyber terrorism: fact or fiction, computer fraud & security.

- C. L. Martin, (2009), Cyber deterrence and Cyber war, United States, Published by RAND Corporation.
- E. Willems, (2011), Cyber terrorism in the processes industry, computer fraud & security.
- J. Prichard, and macdonald, Laurie, (2004), cyber terrorism, a study of the extent of coverage in computer security text books, journal of information technology Education, Vol 3.
- J. Sauver, cyber war, (2008), cyber terrorism and cyber Espionage, security programs manager.
- K. Ceers, (2010), Live five Exercises: Preparing for cyber war, journal of Homeland security and Emergency management, Vol 7.
- L. Andrew and A. jams, (2005), Cyber security and regulation in the United States, center for strategic and international studies, Washington.
- N. Ellsmore, (2002), Cyber terrorism in Australia, Tactical information control, Published by SIFT.
- N. Sheyri, (2005), Pattern of global cyber war and crime, a conceptual frame work, journal of international management.
- P. Grabosy, (2007), Requirements of prosecution service to deal with cybercrime, crime, law and social change.
- P. Ramsaroop, (2003), Cybercrime, cyber terrorism and cyber warfare, Health services organization unit.
- R. Moly, (2009), Cyber terrorism, Office for information security.
- R. Nagpal, (2002), Cyber terrorism in the context of globalization word, Congress on informatics and law Madrid.
- R. Power and P. Forte, (2006), Stalking cyber terrorists in sotiu-event report, computer fraud & security.
- S. Hinde, (2001), Incalculable potential for damage by cyber terrorism, computer security, Vol 20.
- S. M. Furhell and M. j. warren, (1999), Computer hacking and cyber terrorism: the real threats in the new millennium? Computer security, Vol 18.