فصلنامه دستاوردهای نوین در حقوق عمومی، سال اول،شماره چهارم،زمستان۱۴۰۱

اقدامات دولت در ایجاد امنیت سایبری

دکتر طیبه بلوردی [۱]، مطهره طیاری پوراحمدی [۲]

تاریخ دریافت: ۱۴۰۱/۰۹/۲۷ تاریخ پذیرش:۱۴۰۱/۱۰/۱۵

چکیده

امنیت یکی از ارکان مهم جامعه است. امروزه توسعه و گسترش تکنولوژی و فناوری‌ها سبب ایجاد تحول در مفهوم امنیت شده است. استفاده از فضای سایبری برای دستیابی سریع و موّثر به اهداف راهبردی، به ابزار جدید و مهمی برای تهدیدات و جنگ‌ها توسط دولت‌ها تبدیل شده است. تهدیداتی که علیه فضای سایبری یک کشور صورت می‌گیرد، خطرات جبران‌ناپذیری را برای دولت‌ها به وجود می‌آورد. فضای سایبری کشور ما نیز از این قاعده مستثنی نبوده، در چند سال اخیر شاهد موج حملات سایبری علیه زیرساخت‌های حساس کشور به ویژه در حوزه فناوری‌های هسته‌ای بوده است. نوشتار حاضر به بررسی اقدامات دولت در ایجاد امنیت سایبری می‌پردازد. نتایجی به دست آمده نشان می‌دهد، به دلیل اثرگذاری و گستردگی زیاد و سهولت و سادگی کاربرد و تنوع ابزارها و روش‌ها، وقوع تهدیدات سایبری قطعی است. بایستی با فرهنگ‌سازی، توسعه‌ی زیرساخت‌ها، تدابیر فنی مدیریتی یک تغییر بنیادین در فضای سایبری و ارتقای امنیت آن ایجاد کرد.

کلیدواژه‌ها: فضای سایبر، امنیت سایبری، دولت.

[۱] استادیار، گروه معارف، واحد سیرجان، دانشگاه آزاد اسلامی، سیرجان، ایران.(نویسنده مسئول)
t_balvardi90@yahoo.com
[۲] دانشجوی کارشناس ارشد، حقوق عمومی، واحد سیرجان، دانشگاه آزاد اسلامی، سیرجان، ایران.

مقدمه

عصری که در آن زندگی می‌کنیم را می‌توان عصر سایبری نام نهاد. از آن جهت که فناوری‌های نوین ارتباطی در زندگی و جامعه مدرن کنونی، نقش و جایگاهی بی‌بدیلی را به خود اختصاص داده‌اند تا جایی‌که تصور جامعه معاصر بدون آنها، بسیار دشوار به نظر می‌رسد، در حال حاضر شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی مانند اطلاع‌رسانی، ارائه خدمات، مدیریت وکنترل ارتباطات، از طریق سازوکارهای فضای سایبری انجام می‌پذیرد. تکنولوژی اطلاعات، صرفنظر از موقعیت جغرافیایی در تمام شئون زندگی وارد شده است، لیکن این رشد علیرغم مزایای خود جنبه‌های منفی هم دربرداشته است. بدین مفهوم که امکان رفتارهای ضد اجتماعی و مجرمانه در این فضا را به وجودآورده که پیش از این به هیچ وجه امکان‌پذیر نبوده‌است، زیرا نوع تهدیدها و ویژگی‌هایی که در این فضا انسان‌ها، جوامع و زیرساخت‌های هرنهادی را هدف قرار می‌دهند نیز با تهدیدهای روزمره دیگر بسیار متفاوت است. تهدید امنیتی در عصر ارتباطات و جهانی شدن برای کشورها از جمله تهدیدات حوزه سایبری دانست، جهانی شدن یکی از ابزارهای آن فناوری‌های سایبری می‌باشد در کنار فرصت‌های بی‌شماری که برای کشور ایجاد می‌کند، یک تهدید بسیار جدی است که عمدتاً خیلی به صورت جدی به آن پرداخته نمی‌شود. لذا نیاز است این موضوع، به طورمشخص بررسی گردد تا بتوان مناسب با آن اقدامات لازم به عمل آورد.

با توجه به نفوذ روز افزون فضای سایبری شامل اینترنت، شبکه‌های اجتماعی و... در معادلات بین‌المللی، توجه به ماهیت فضای سایبر به عنوان بستر اصلی اطلاعات کشور و اینکه امکان صدمه زدن از این راه بسیار محتمل می‌باشد، لازم است که نگاه ویژه به مسأله امنیت فضای سایبر مخصوصاً در سطح کاربردهای ملی شود، زیرا در آینده‌ای نزدیک زیرساخت‌های اصلی کشور در این فضا قرار خواهند گرفت و بروز هرگونه مشکل امنیتی باعث تهدید جدی در امنیت ملی کشور خواهد گردید. لذا بایستی امنیت فضای سایبر در کشور را ارتقاء دهیم و بتوانیم با تقویت فناوری‌ها و مکانیزم‌های امنیتی در بعضی موارد حتی مقابله به مثل نماییم و اقدامات لازم جهت ایجاد امنیت سایبری در کشور ایجاد شود. چالش امنیت در فضای سایبری در سازمان‌های بخش دفاع که متولی حفظ امنیت و دفاع از کشور در برابر تهدیدات مختلف هستند، بسیار جدی‌تر و اساسی‌تر است. در این امتداد، برابر سیاست‌های کلی خودکفایی دفاعی و امنیتی ابلاغی مجمع تشخیص مصلحت نظام در اواخر سال ۱۳۹۲، موارد مهمی همچون توسعه، خودکفایی، خلاقیت و نوآوری در تمام سطوح، ترویج نهضت نرم‌افزاری، ابعاد امنیتی و دفاعی، تولید و توسعه علوم و فناوری و تحقیقات دفاعی و امنیتی و حرکت در مرزهای دانش با تأکید بر روزآمدی و بومی‌سازی، دستیابی به فناوری‌های برتر مورد نیاز دفاعی و امنیتی حال و آینده با تأکید بر نوآوری و پشتیبانی از توسعه آنها، تأکید بر خودکفایی کشور در سامانه، کالاها و خدمات اولویت‌دار دفاعی و امنیتی توأم با بهسازی تجهیزات موجود و افزایش قابلیت و کارآیی آن، ممنوعیت تأمین نیازهای دفاعی و امنیتی از خارج کشور مگر در حد ضرورت قابل توجه هستند؛ بنابراین یکی از ملاحظات اساسی تحقق اهداف تعیین شده در سیاست کلی خودکفایی دفاعی و امنیتی، فناوری اطلاعات و ارتباطات و ضرورت تأمین امنیت فضای سایبری به عنوان شریان حیاتی بخش دفاع است. لذا پژوهش حاضر با هدف بررسی وظیفه دولت در ایجاد امنیت سایبری در حقوق موضوعه ایران می باشد.

۱- مفهوم امنیت سایبری

محیط مجازی مجموعه اطلاعاتی است که در رایانه ذخیره سازی شده و از طریق اینترنت به یکدیگر متصل هستند (Ploug 2009: 70) این در حالی است که شبکه یا نت دارای تعریف مخصوص به خود است، اینترنت مجموعه‌ای بسیار گسترده از رایانه‌های موجود

در شبکه‌های رایانه‌ای سراسر جهان است که از طریق خطوط ارتباطی به یکدیگر متصل شده و با استفاده از پروتکل‌های معینی به تبادل اطلاعات می‌پردازند. بسیاری از رایانه‌های موجود در عرصه اینترنت اطلاعات زیادی در خود ذخیره کرده و در مجموع حجم عظیمی از اطلاعات در اینترنت انبارشده است. اطلاعات موجود در اینترنت به روش‌های مختلفی ذخیره شده و در نتیجه با روش‌های گوناگونی قابل ارائه و انتقال هستند، صفحات وب یکی از راه‌های خاص ذخیره و ارائه اطلاعات در بین روش‌های متعدد ذخیره و ارائه اطلاعات در اینترنت هستند.

امنیت سایبری ریشه اصلی تکنولوژی‌ها، فرآیندها و شیوه‌های طراحی شده به منظور حفاظت از شبکه‌ها، ابزارهای دیجیتالی، داده‌ها و برنامه‌ها در مقابل حملات و خسارات و دسترسی‌های غیرمجاز می‌باشد. همچنین امنیت سایبری نقش مهمی در توسعه فناوری اطلاعات و خدمات اینترنتی بازی می‌کند. امن‌تر کردن فضای سایبر و حفاظت از کاربران برای توسعه خدمات دولت‌ها و حفظ امنیت کشورها در سطح داخل و بین الملل ضروری می‌باشد(جهان‌گشته؛ دامنی ،۱۰:۱۳۹۸).

«عبارت امنیت سایبری مجموعه ابزارها، سیاست‌ها، مفاهیم امنیتی، اعمال امنیتی، رویکردهای مدیریت بحران، اعمال، آموزش و فناوری‌های می‌باشد که در راستای در دسترس بودن، مورد اطمینان بودن و صحت اطلاعات می‌باشد که به منظور حفاظت از محیط سایبری و دارایی کاربران و سازمان‌ها به کار می‌رود. دارایی‌های کاربران و سازمان‌ها شامل خدمات زیربنایی، برنامه‌های کاربردی، سرویس‌های مخابراتی و کلیت اطلاعات ذخیره شده یا انتقال یافته در محیط سایبری می‌باشد. همچنین امنیت سایبری در راستای تضمین دستیابی و حفظ امنیت دارایی کاربران و سازمان‌ها در برابر خطرات امنیتی مربوط در محیط سایبری می‌باشد. امنیت سایبری نه تنها شامل مسائلی مانند حملات ویروسی و محرومیت از خدمات می‌باشد، بلکه مسائل انسانی از جمله تقلب درون سازمانی و مسائل حاکمیت ملی و بین المللی را نیز در بر خواهد گرفت. امنیت سایبری شامل یک سری پروتکل است که کاربران فضای سایبر برای اطمینان از اطلاعات ازICA۱۹ پیروی می‌کنند».(عسکری؛ مدیری،۱۳۹۹ : ۱۵)

۲- امنیت سایبری در حقوق ایران

«با توجه به اینکه فضای سایبر، فضایی بدون حدومرز است، بدیهی است که سیاست‌گذاری درحوزه داخلی، به تنهایی در تأمین امنیت راهگشا نخواهد بود، بلکه این فضا نیازمند یک سازوکار جهانی و بین‌المللی است. در واقع با پیشرفت فناوری، دولت‌ها نیازمند ایجاد تشکیلاتی هستند، که به صورت منظم و مستمر، با همکاری سایر دولت‌ها، در زمینه قواعد مربوط به فضای سایبر و تأمین امنیت سایبری، با توجه به نیاز جامعه خود را به روز کنند»(یاسمی‌نژاد،۱۱:۱۳۹) «جرایم سایبری به قدری پویا هستند که ارائه یک قانون و راهکار ملی، نمی‌تواند برای مدت طولانی کارآمد باشد»(خلیل‌زاده، ۴۳:۱۳۹۳). تهدیدات سایبری، ناقض حریم خصوصی اشخاص حقیقی و حقوقی است و امنیت ملی کشور را تهدید می‌کند. حریم خصوصی فضای سایبر، از جنس اطلاعات است و از طرق مختلف از جمله نفوذ به سیستم رایانه‌ای اشخاص، استفاده از روش‌های فریب، تارنماها و شبکه‌های اجتماعی نقض می‌شود. موجب مسئولیت کیفری و مدنی می‌شود.

قوانین و مقررات موضوعه این حوزه از جمله قانون مسئولیت مدنی مصوب ۱۳۳۹، متناسب با تهدیدات و حملات سایبری بازنگری شود. لوایح مرتبط با حقوق سایبری از جمله لایحه مسئولیت ارائه‌دهندگان خدمات هرچند مبانی و منابع تحقق مسئولیت مدنی، در دنیای واقعی و فضای سایبر مشترک هستند، و گروه‌های فعال در حوزه سایبری تبیین شود تا در هر مورد مشخص شود مسئولیت، چه زمان به صورت مجزا و چه زمانی اشتراکی است.

۳- انواع تهدیدها

تهدیدات از جهت شکل، هدف، موضوع، شدت، ماهیت و... قابل دسته‌بندی هستند. تهدیدات از جهت شدت و با توجه به موضوع به دو گروه سخت و نرم تقسیم می‌گردد.

۳-۱. تهدید سخت

در تهدید سخت هدف اصلی اشغال زمین و تهدید تمامیت ارضی کشورها، تخریب و حذف فیزیکی حریف و تصرف و اشغال سرزمین است. «هرگاه به موجب اقداماتی استقلال و تمامیت ارضی کشور در خطر (بالفعل یا بالقوه) هجوم نیروهای نظامی کشور دیگر با اتحادی از کشورهای خارجی با گروه‌های معارض مسلح داخلی قرار گیرد، تهدید سخت واقع شده است. تهدیدات سخت متکی به روش‌های عینی، فیزیکی، سخت‌افزارانه و همراه با رفتارها و اعمال خشونت‌آمیز، براندازی آشکار و با استفاده از شیوه اجبار و زور، حذف دفعی و اشغال سرزمین است. این تهدیدات عمدتاً عینی، محسوس و واقعی، همراه با عکس‌العمل‌های فیزیکی می‌باشد. ظهور این نوع تهدیدات عمدتاً مربوط به دوره استعمار کهن است که قدرت‌های استعماری با لشکرکشی، کشتار، اعمال زور و اشغال و الحاق سرزمین، اهداف خود را تأمین می‌کردند.» (ترابی، ۱۳۹۸: ۹۷).

۳-۲. تهدید نرم

در تهدید نرم فرهنگ، آرمان‌ها، هویت ملی و دینی مورد هدف است. مبنای تهدید نرم تأثیرگذاری بر انتخاب‌ها، فرایند تصمیم‌گیری و الگوهای رفتاری حریف و در نهایت سلب هویت‌های فرهنگی است. تهدیدات نرم پیچیده و حاصل پردازش ذهنی نخبگان، و اندازه‌گیری آن مشکل است. حوزه تهدید نرم، سلطه تام بر ابعاد اقتصاد، حکومت، اجتماع و فرهنگ است. که از طریق استحاله الگوهای رفتاری ملی در این حوزه‌ها و جایگزینی الگوهای نظام سلطه‌ای تهدید محقق می‌شود. با این نگاه، کلیه اقداماتی که موجب شود تا اهداف و ارزش‌های حیاتی یک نظام سیاسی (باورها و الگوهای رفتاری وزیرساخت‌های فکری، در حوزه فرهنگ و اقتصاد و سیاست) به خطر افتد، یا موجب ایجاد دگرگونی و تغییر اساسی در عوامل تعیین کننده هویت ملی یک کشور شود، تهدید نرم محسوب می شود. «در تهدید نرم، بدون منازعه و لشکرکشی فیزیکی، کشور مهاجم اراده خود را بر یک ملت تحمیل و آن را در ابعاد گوناگون با روش‌های نرم‌افزارانه اشغال می‌کند. تردید در زیر ساخت‌ها و مبانی فکری یک نظام سیاسی، بحران در ارزش‌ها و باورهای اساسی جامعه، بحران‌های پنج‌گانه سیاسی (هویت، مقبولیت، مشارکت، نفوذ و توزیع) در الگوهای رفتاری جامعه را می‌توان از مؤلفه‌های این تهدید نام برد. تغییرات حاصل از تهدید نرم، آرام، ذهنی، ماهوی، تدریجی و نرم‌افزارانه است. این تهدید همراه با آرامش و خالی از روش‌های فیزیکی و با استفاده از ابزارهای تبلیغات، رسانه، احزاب، تشکل‌های صنفی و قشری و شیوه القاء و اقناع انجام می‌پذیرد در حال حاضر جهانی‌سازی فرهنگ مترادف با مفهوم تهدید نرم تلقی می‌شود.» (نائینی، ۸۶،۱۳۸۶)

۴- توسعه امنیت نرم در محیط سایبر

ایمن‌سازی فضای مجازی به عنوان یکی از اصول راهبردی دولت‌ها برای ارتقای ضرایب امنیت داخلی و خارجی محسوب می‌شود. به طوریکه همسو با توسعه زیر ساخت‌های تدابیر حفاظتی و ایمنی مرزها و زیر ساخت‌های حساس نظیر نیروگاه‌ها، پادگان‌ها و مراکز و تأسیسات هسته‌ای، توسعه ضرایب امنیت شبکه نیز به عنوان یکی از دغدغه‌های اصلی کشورها در آمده است به طوری که امروزه مدیریت پیشگیری تهدیدات امنیت ملی در فضای مجازی به یکی از کار ویژه های مهم وزارت امنیت داخلی تبدیل شده است.

فناوری‌های نوین مشکلات و چالش‌هایی نیز برای امنیت ملی کشورها به وجود آورده که تهاجم سایبر، سرقت اطلاعات محرمانه، هک کردن سیاست‌های اینترنتی وزارت‌خانه‌ها و نهادها و نهادهای راهبردی نفوذی در شبکه های مالی و پولی و حساب‌های شخصی، هتک حرمت افراد و تهدید حاکمیت ملی از سوی اشخاص و گروه‌های سازمان یافته بین‌المللی از مهم‌ترین مصادیق آن است.

«گستره فضای مجازی در محیط امنیتی ملی با توسعه فناوری اطلاعات و ارتباطات و قرار گرفتن کشورها در دهکده جهانی افزوده شده و به غیر از لزوم حفظ و ارتقای امنیت فیزیکی مانند امنیت اقتصادی، فرهنگی، سیاسی، اجتماعی و مرزی و توسعه زیر ساخت‌های امنیت فضای شبکه نیز به یکی از پیش نیازهای توسعه انتظامی مطلوب در افق امنیت فضای شبکه نیز به یکی از پیش نیازهای توسعه انتظامی مطلوب در کشور تبدیل شده است»(وحیدپور، ۱۳۹۲: ۲۹).

۵- تأثیر تهدیدات سایبری بر امنیت ملی

« آنچه در مورد این تهدیدهای جدید قابل توجه است، این است که ویروس ها، کرم ها، جرم ها، هکرها و حملات اینترنتی، امروزه واقعیت مسلم و روزمره هستند. حملات مخرب مهم با تأثیرات گسترده، تهدیدهای سایبری را به عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جایی که ایالات متحده آمریکا اعلام کرده است که این حملات را به عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد.» مسائل مختلفی مانند: ارتباطات، بانکداری، مبادلات، تجارت الکترونیکی... در فضای سایبر سبب تخریب اطلاعات و در نتیجه ایجاد چالش در حوزه امنیت شده است. پس پایان یافتن جنگ سرد نه تنها سبب امن تر شدن جهان نشده است بلکه به وجود آمدن چنین چالش‌هایی، امنیت جهانی را با تهدید مواجه ساخته است. « حمله‌های مختلف مانند: محوریت هک (استفاده از قوه خلاقیت در یک مسئله یا پروژه برنامه‌سازی و همچنین تغییر رفتار یک برنامه کاربردی یا یک سیستم عامل از طریق تغییر دستورات و نه اجرای برنامه و انتخاب گزینه‌ها). و کرک (دستیابی غیر مجاز به یک شبکه از طریق گذشتن از اقدامات امنیتی است و متضمن تفسیر و درک اطلاعات رمز گذاری شده می‌باشد)، کرم‌ها، بمب منطقی (که سبب ایجاد خسارت، تغییر و تخریب در داده‌ها و یا برنامه‌های کامپیوتر می‌شود) جزء واقعیت‌های غیر قابل انکار می‌باشند. این حملات وسیع می‌تواند به عنوان تهدید جدی منافع ملی یک کشور را به چالش بکشاند. به طوریکه کشورهای مختلف، به برخورد فیزیکی با این حملات پرداخته‌اند و اسناد مختلفی در زمینه تأمین امنیت در فضای سایبر به تصویب رسیده است» (موسوی و همکاران، ۱۳۹۲: ۳۰)

۶- اقدامات دولت در ایجاد امنیت سایبری

۶-۱. تدوین بسته منسجم سیاسی برای مقابله با تهاجم شبکه‌ای

یکی از تهدیدات امنیت ملی، وجود برخی خلأهای تفنینی- نظارتی یا عدم حسن اجرای مناسب قوانین مصوب برای مقابله موثر بر جرائم امنیت ملی در فضای مجازی است.

۶-۱-۱. ایجاد شبکه اینترنت ملی

در بند ۴۴ سیاست‌های کلی برنامه پنجم توسعه بر ایجاد سامانه یکپارچه نرم افزاری- اطلاعاتی ارتقای سطح حفاظت از اطلاعات رایانه‌ای، توسعه علم فناوری‌های مرتبط با حفظ امنیت سامانه‌های اطلاعاتی و ارتباطی به منظور خیانت از فضای تبادل اطلاعات و مقابله با تخلفات رایانه‌ای تأکید شده که تحقق آن مستلزم شناسایی و آسیب‌شناسی تهدیدها در فضای سایبر است.

«با توجه به مبهم بودن عمق دامنه و نوع تحریم‌ها و همچنین فقدان ایمنی کامل شبکه فیبر نوری، توصیه می‌شود ایجاد اینترنت ملی، تنوع‌سازی ارتباط با شبکه جهانی اینترنت مانند ارتباط ماهواره‌ای و سیستم عامل ملی و نرم افزارهای کاربردی هر چه سریع‌تر عملیاتی شود تا عمق آسیب پذیری نظام از جانب جنگ های اطلاعاتی کاهش یابد ایجاد اینترنت ملی به مفهوم قطع ارتباط با خارج از کشور نیست. بلکه فقط بانک اطلاعات در داخل کشور نگهداری شده تا اگر دشمن ورودی‌های اینترنت را قطع کرد. بتوان سایت‌های داخلی را با حداقل مشکل مدیریت کرد.» (رضوی‌پور، ۱۳۹۷: ۳۳).

۶-۱-۲. تقویت ضریب ایمنی داده‌های راهبردی

در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه دستگاه‌های دولتی در سطح نامطلوبی قرار دارد که از دلایل آن می‌توان به فقدان زیر ساخت‌های فنی و اجرایی برای ایمن‌سازی فضای تبادل اطلاعات و فقدان نظام تحلیل و مدیریت مخاطرات امنیتی در محیط سایبری اشاره کرد. بنابراین هم‌زمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات، توجه به مقوله ایمن‌سازی فضای سایبر و مدیریت امنیت نظام اطلاعات به ویژه در ساختارهای استراتژیک نظام اطلاعات به ویژه در ساختارهای استراتژیک نظام از نیازهای حیاتی برنامه پنجم توسعه است. همچنین یکی از اهداف اصلی جنگ‌های سایبر، بهره‌گیری از بمب‌های الکترومغناطیس و نفوذ هکرها برای مختل سازی شبکه نرم‌افزاری داده استراتژیک که توصیه می‌شود با کاربست فناوری‌های نوین و یا میکرو فیلم‌های پشتیبان، ضریب ایمنی داده‌های راهبردی را افزایش داد. از طرفی هر چه بتوان با بهره‌وری مناسب از فنون جنگ اطلاعاتی قدرت تسخیر و چشم الکترونیک نیروهای مهاجم را مختل کرد ضریب آسیب‌پذیری بانک اطلاعاتی کاهش می‌یابد که موفقیت آن مستلزم توسعه تعامل ساختارهای عملیاتی و مراکز تحقیقات هوا و فضا است.(قهرمانی، ۱۳۹۷: ۵۹).

۶-۱-۳. بهره‌گیری مؤثر از ظرفیت فناوری‌های نوین در ساختار مدیریت بحران‌های امنیت اجتماعی

یکی از روش‌های توسعه مطلوب در سند چشم‌انداز، بهره‌گیری بهینه از ظرفیت فناوری و شبکه سایبر بوده است به طوریکه یکی از ابزارهای ارتقای مهندسی امنیتی کاربست فناوری‌های نوین مانند بیومتریک در ساختار امنیت ملی بوده و اهمیت آن در حدی است که

در ماده (۱۱۹) قانون برنامه چهارم توسعه بر لزوم ارتقای فناوری‌های نوین، هوشمند و نظام‌های اطلاعاتی در توسعه سامانه‌های دفاعی به ویژه سامانه‌های الکترونیکی، هوا فضا، دریایی و پدافند هوایی تاکید شده است. از مهم‌ترین مصادیق آن می‌توان به گسترش کاربست فناوری بیومتریک در توسعه نظام جامعه امنیت مرزی، تشکیل بانک اطلاعات مجرمان، صدور گذرنامه‌های بیومتریکی و پیشگیری از آسیب‌های اجتماعی اشاره کرد. سهولت کاربرد، سرعت عملکرد، هزینه کم، میزان پذیرش بالای کاربری، سطح امنیتی بالا، دوام و پایداری بالا از مهم‌ترین فرصت های توسعه کاربست دانش بیومتریک در ساختار امنیتی-نظامی و انتظامی است. به عنوان مثال، مهم‌ترین کاربردهای نهادینه‌سازی دانش بیومتریک در ساختار انتظامی- امنیتی برنامه پنجم عبارتند از: امنیت فضای سایبر، امنیت نظام مالی و پولی، افزایش اهمیت کارت‌های هوشمند، رأی‌گیری الکترونیکی، کنترل و نظارت دقیق‌تر، رفت و آمد مسافران در مبادی ورودی و خروجی کشور، صدور گذرنامه ها و شناسنامه‌های بیومتریکی، توسعه ضریب امنیت مرزی، تأیید سریع هویت و آمارگیری دقیق از بازماندگان، مجرمان و متوفیان در شرایط وقوع بحران های طبیعی، امنیتی و نظامی (نامی، ۱۳۹۲: ۹۰).

۷- ایجاد امنیت سایبری در حقوق

اقداماتی که برای تأمین امنیت سایبری انجام گیرد، بدین قرارند:

۷-۱. سیاست‌گذاری و تدوین استراتژی ملی برای مقابله با تهدیدات سایبری در حقوق

محیط سایبر و بایسته‌های مدیریت پیشگیرانه پلیس کشور در سند چشم‌انداز به منظور حداکثر بهره‌گیری و هم افزایی بهینه ظرفیت‌های نظام برای مقابله با آفندهای تهاجم شبکه‌ای، متولیان امر باید در سطح کلان که به ارتقای امنیت فضای سایبر منجر می‌شود را به عنوان یکی از اصول سیاست‌های انتظامی کلان کشور مورد توجه قرار دهند. در سطح خرد می‌توان با اتخاذ تدابیر و انجام نهادهای امنیتی لازم به ارتقای امنیت فضای مجازی کشور کمک کرد.

۷-۲. سیاست‌های راهبردی در حوزه حاکمیت سیاسی در فضای سایبر

۷-۲-۱. راه‌اندازی شبکه‌های اجتماعی بومی

لازم است یک نهضت وبلاگی در کنار شبکه‌های اجتماعی بومی راه‌اندازی شود؛ برای اینکه موج به وجود آمده از توان لازم برای ایجاد جریان‌سازی فکری، فرهنگی - سیاسی لازم برخوردار شود، اتاق فکری و مرکزی وجود داشته باشد که چنین موجی را هدایت و مدیریت کرده و انسجام و یکپارچگی لازم را ضمن خط دهی مناسب به آن فراهم سازد. «از این رو راه اندازی یک نهضت وبلاگی و ایجاد شبکه‌های اجتماعی بومی، می‌تواند به عنوان اولین گام در زنجیره تولید محتوا و جریان‌سازی فکری- فرهنگی نقش ایفا نماید. در قالب این نهضت وبلاگی می‌توان با مهندسی معکوس از شبکه‌های اجتماعی مجازی غیر بومی نظیر اینستاگرام، توئیتر و فیس‌بوک نیز بهره‌برداری نمود. در واقع تهدید شبکه‌های اجتماعی غیربومی را به فرصتی ارزشمند تبدیل کرد. از طرف دیگر این شبکه‌های اجتماعی می‌تواند به عنوان کانال بسیار مناسبی برای صدور پیام ایدئولوژیک مورد بهره‌برداری قرار گیرد. و بدین ترتیب این تهدید را به یک فرصت ارزشمند تبدیل نمود.» (صیفی، ۱۳۹۶: ۱۶).

۷-۲-۲. تولید محتوا در فضای سایبر

« در راستای اهداف مورد نظر تولید محتوای مناسب، از مهم‌ترین مقولات مرتبط با فضای سایبر تلقی می‌شود. فضای سایبر می‌تواند به مثابه یک رسانه و کانالی برای انتقال ارزش‌ها و مفاهیم مد نظر مورد استفاده قرار گیرد. از این جهت تولید محتوا در بستر فضای سایبر با توجه به طیف متنوع و گسترده مخاطبین از اهمیت بسیار زیادی برای شکل‌دهی به افکار عمومی و رساندن پیام و به تبع آن صیانت از حاکمیت سیاسی برخوردار خواهد بود». (صیفی، ۱۳۹۶: ۱۶).

۷-۲-۳. ارائه تصویری درست از تمدن و فرهنگ ایرانی- اسلامی

مسائل مربوط به اسلام هراسی، پیوندی اساسی با ایران هراسی پیدا کرده است. ظهور پدیده اسلام هراسی و تأثیر آن در سطح جهان، پروژه‌ای بود که نهایتاً توسعه مفهوم ترس و طراحی ایران هراسی را دنبال می‌کند. بدین ترتیب تصویرسازی از ایران تصویری غیرواقعی و مخدوش است. از این رو یکی از مهم‌ترین اقداماتی که در حوزه محتوایی و در بستر فضای سایبر برای مخاطبین خارجی لازم است، انجام پذیرد، معرفی واقعی فرهنگ و تمدن ایرانی- اسلامی است. «در این زمینه لازم است اهتمام ویژه داشته و شرایطی را در فضای سایبری کشور فراهم کنند که با ارائه تصویری درست و واقعی از ایرانی اسلامی، ذهنیت غلط ایجاد شده در افکار عمومی را اصلاح کنند. با معرفی فرهنگ اسلامی- ایرانی و مظاهر تمدنی آن در قالب هنر و سبک معماری خاص ایرانی اسلامی صورت پذیرد. بدین ترتیب با تولید محتوای مناسب برای مخاطب داخلی و خارجی ضمن صیانت از حاکمیت سیاسی، به تولید قدرت نرم در عرصه خارجی اقدام نمود.» (رضوی پور، ۱۳۹۷: ۵).

۷-۳.سیاست‌های راهبردی در حوزه زیرساخت‌ها

به منظور تأمین امنیت فضای سایبر در حوزه زیرساخت‌های راهبردی، می‌توان اقداماتی را در دو حوزه داخلی و بین‌المللی انجام داد.

۷-۳-۱. سیاست‌های راهبردی در بعد داخلی

۷-۳-۱-۱-فرماندهی سایبری در حوزه زیرساخت‌های راهبردی

برای تأمین امنیت فضای سایبر در برابر تروریسم سایبری، نیازمند به وجود یک فرماندهی متمرکز سایبری هستیم. این فرماندهی سایبری باید عهده‌دار دو وظیفه باشد:

یک: دفاع از زیرساخت های راهبردی: با توجه به اینکه در طول چند سال اخیر «شاهد حملات سایبری نظیر دو کو، استاکس‌نت، شعله و... بوده است و این حملات زیرساخت‌های حساسی در اقتصاد (وزارت نفت) و حوزه انرژی (نیروگاه هسته‌ای نطنز و بوشهر) را مورد هدف قرار داده‌اند. از این جهت حفاظت از زیرساخت‌های راهبردی کشور به عنوان اولویت اصلی این مرکز باید لحاظ گردد و رصد تهدیدات سایبری علیه زیرساخت‌های کشور و ایمن‌سازی زیرساخت‌های راهبردی کشور نسبت به تهدیدات زیرساختی به عنوان وظیفه اصلی این مرکز شناخته شود.» (طارمی، ۱۳۸۹: ۶۰).

دو: ایجاد توان بازدارندگی: «با ایجاد توان بازدارندگی دفاعی در حوزه فضای سایبر می‌توان تا حد زیادی امکان تهدیدات در این حوزه را کاهش داد. به عبارتی توان آفندی کشور در حوزه سایبری باید به حدی باشد که تضمین کننده بازدارندگی و توان دفاعی کشور باشد و قدرت پاسخگویی کشور به تهدیدات به گونه‌ای باشد که دیگران را از هرگونه فکر حمله سایبری به زیرساخت‌ها منصرف سازد». (طارمی، ۱۳۸۹: ۶۰).

۷-۳-۱-۲-پشتیبانی سایبری

فضای سایبر همچون سایر عرصه‌های دفاعی دارای نیازمندی‌هایی است که تأمین این نیازها می‌تواند در ارتقاء توان دفاعی در حوزه فضای سایبر مؤثر واقع شود. همانطور که وزارت دفاع نیازمندی‌های بخش دفاعی نظیر رادار، تفنگ، تانک و... را تولید می‌کند، در حوزه فضای سایبر نیز نیازمندی‌هایی وجود دارد که باید تأمین شود.

«اول. نظام جامع آموزش دفاع سایبری فضای سایبر و مقوله دفاع سایبری به عنوان یک حیطه بکر و جدید در علوم نظامی در حال مطرح شدن است. با توجه به اینکه کشور ما در چند سال اخیر نیز خطرات و تهدیدات این عرصه را به‌طور ملموس تجربه کرده است؛ تدوین یک نظام جامع آموزشی در کنار تهیه محتوای مناسب در حوزه دفاع سایبری ضرورتی اجتناب‌ناپذیر به نظر می‌رسد. نبود دانش تخصصی در این حوزه را باید آفتی دانست که می‌تواند در دراز مدت به‌صورت یک تهدید ظاهر شود.

دوم. حمایت‌های تکنیکی، فنی و زیرساختی: باید در حوزه پشتیبانی سایبری مورد توجه قرار گیرد. توان کشور در حوزه‌های زیرساختی، به قدری افزایش پیدا کند که نیاز زیرساخت‌های حیاتی کشور به سخت‌افزارها و نرم‌افزارها در داخل کشور و به شکل بومی مرتفع شده و وابستگی به خارج قطع شود. یکی از متولیان اصلی این حوزه وزارت ارتباطات و فناوری اطلاعات است که می‌تواند با بومی‌سازی در ارائه خدمات رایانه‌ای گام مهمی در حمایت‌های فنی و تکنیکی به منظور تأمین امنیت هر چه بیشتر فضای سایبر بردارد.» (باطنی؛ یزدان‌شناس، ۱۳۹۰: ۵۰).

۷-۳-۱-۳-شبکه ملی اطلاعات، موتور جستجوی و ایمیل بومی

راه‌اندازی شبکه ملی اطلاعات از چند جنبه ضروری به نظر می‌رسد. در راستای تبدیل شدن به یک جامعه شبکه‌ای، ناگزیر به ارائه خدمات الکترونیک بوده و از این جهت ایمنی اطلاعات مربوط به شهروندان اهمیت دو چندانی پیدا خواهد کرد. شبکه ملی اطلاعات در واقع زیرساخت اصلی خدمات دولت الکترونیک به شمار می‌رود و سه مشکل عمده هزینه خرید، سرعت گردش اطلاعات و تهیه پهنای باند و نهایتاً حفظ محرمانگی اطلاعات ,امنیت شبکه را مرتفع خواهد ساخت. « از دیگر مزایایی شبکه ملی اطلاعات این خواهد بود که خدماتی که در این شبکه ارائه می شود، با توجه به اشراف آژانس امنیت ملی بر اینترنت و رصد فعالیت کاربران در آن، لزومی ندارد که اطلاعاتی نظیر اطلاعات بانکی افراد که در داخل تولید، نگهداری و مورد استفاده قرار می‌گیرند از طریق این کانال پر خطر در دسترس قرار گیرد. شبکه ملی اطلاعات، یک شبکه داخلی است که پردازنده اطلاعات داخلی کشور خواهد بود و ایمنی بیشتری را تضمین خواهد کرد. قبل از راه‌اندازی اینترنت پر سرعت لازم است ایمنی شبکه و اطلاعات داخلی تأمین شود که با تحقق شبکه ملی اطلاعات میسر خواهد شد. ارائه خدمات رایانه‌ای نظیر موتور جستجوی و ایمیل بومی است. راه اندازی خدمات رایانه‌ای نظیر ایمیل و موتور جستجوگر بومی می‌تواند تا حد زیادی امنیت فعالیت و اطلاعات کاربران را در فضای اینترنت تأمین نماید. راه‌اندازی پست الکترونیک بومی موسوم به چاپار از سوی وزارت ارتباطات و فناوری اطلاعات، اقدام است که در این زمینه صورت پذیرفته است.» (یزدان‌فام، ۱۳۸۹: ۲۲).

۷-۳-۱-۴.سیستم عامل بومی

از اقدامات دیگر برای تأمین امنیت سایبری کشور، چه در حوزه ایمنی رایانه‌های شخصی و چه در حوزه کلان و دفاع سایبری، راه‌اندازی سیستم عامل بومی است. «امروزه کشورهای مختلفی نظیر انگلستان، چین، آلمان، کره و ژاپن به بومی‌سازی سیستم عامل خود اقدام نموده‌اند. مواردی چون عدم دسترسی به کد منبع این سیستم عامل، هزینه بالای خرید سیستم عامل ویندوز، مشکلات سیاسی احتمالی و از همه مهم‌تر ایمنی ناچیز آن برای رایانه‌های کاربران داخلی اعم از مراکز صنعتی و سازمان‌ها را که به محض اتصال به اینترنت اطلاعاتی ناخواسته وارد رایانه‌ها شوند و یا تخلیه اطلاعات به‌راحتی صورت پذیرد» (کریمی، ۱۳۹۰: ۳۸) را می‌توان به عنوان ضرورت طراحی و راه‌اندازی سیستم عامل بومی برشمرد در مجموع حمایت‌های فنی، تکنیکی و زیرساختی از مهم‌ترین مؤلفه‌ها در پشتیبانی سایبری به منظور تأمین امنیت سایبری به شمار می‌رود. به نظر می‌رسد مهم‌ترین راهکار در این زمینه بومی‌سازی است.« از آنجا که مقوله فضای سایبر دارای یک وجه امنیتی نیز هست، نهادهای فعال در این عرصه نظیر سازمان پدافند غیر عامل و وزارت دفاع نیز باید در پشتیبانی سایبری دخیل باشند و از طرفی در این حوزه باید از ظرفیت‌های موجود در مراکز دانشگاهی و علمی و پژوهشی و به منظور تولید نرم‌افزارهای بومی نهایت استفاده را برد.» (طارمی، ۱۳۸۹: ۶۳).

۷-۳-۲. سیاست‌های راهبردی در بعد خارجی

برنامه‌ها و اقداماتی که می‌تواند در بعد خارجی در تأمین امنیت و جایگاه سایبری کشور در محیط بین‌المللی مؤثر باشد.

۷-۳-۲-۱. ورود در جرگه قدرت‌های سایبری

با نگاهی به تاریخچه کشورهای غربی به راحتی می‌توان دریافت که تمدن غرب در مواجهه با تسلیحات مرتبط با فناوری های نوین ابتدائا به منظور شناسایی ابعاد مختلف تکنیکی، استراتژیکی این تسلیحات، از آنها استفاده نموده سپس به منظور جلوگیری از ورود و پیشرفت دیگر تمدن‌ها در حوزه دفاعی و تسلیحات مرتبط با فناوری‌های نوین، اقدام به تدوین نظام حقوقی- مدیریتی بین‌المللی می-کند.«نظیر آنچه در رابطه با نظام منع گسترش تسلیحات میکروبی، اتمی، شیمیایی و... مشاهده می‌کنیم. باید در نظر داشت که قوانین جنگی از قدیم الایام تحت یکسری معاهدات بین‌المللی همچون معاهده ژنو قرار داشته‌اند، با توجه به جدید بودن مقوله جنگ سایبری و ملاحظه این نکته که این نوع جنگ تحت هیچگونه معاهده‌ای قرار ندارد، لازم است توان سایبری خود را در مسیر رشد توان سایبری ایجاد شود، تقویت کرد.» (طیبی توکلی، ۱۳۹۳: ۲۳).

۷-۳-۲-۲.از انحصار در آوردن مالکیت اینترنت

امروزه اینترنت به یک پدیده بین‌المللی تبدیل شده است برخی کشورها خود را مالک اینترنت قلمداد می‌کند و از این فرصت به منظور نقض حریم خصوصی مردم و رصد تمامی دنیا بهره می‌گیرند. به نظر می‌رسد با یکسری تلاش‌های بین‌المللی حاکمیت اینترنت را از انحصار خارج نمود و آن را به‌صورت دوره‌ای در اختیار مجموعه‌ای از کشورها قرار داد. (طارمی، ۱۳۸۹: ۵۹).

نتیجه‌گیری

هر چند امنیت مفهومی ازلی است و ابدی نیز خواهد ماند، اما متناسب با زمینه اجتماعی و زمانه فکری همواره دست‌خوش تحول و دگرگونی بوده است. امنیت علاوه بر سیر مستمر و تکاملی که از جامعه بدوی آغاز و تا جامعه جهانی تداوم یافته برای تکوین و تکامل مفهومی خود نیازمند ناامنی و تهدید بوده و هر گفتمان حاصل رسیدن گفتمان قبلی به مرحله ناامنی بوده است البته این لزوماً معنی نمی دهد که با تکامل مفهوم امنیت، گفتمان‌های قبلی و ویژگی ها و مؤلفه های آنها به کلی از بین می روند بلکه به معنی پایان غلبه یک گفتمان در عین حفظ برخی ویژگی ها و مؤلفه های آن است. با توجه به عصر جدید مختصات امنیت گذشته دگرگون شده و با شکل‌گیری فضای مجازی مختصات امنیت و گفتمان‌های امنیتی دگرگون گردیده است و این دگرگونی را می‌توان از گذار فضای سنتی به فضای جدید یعنی فضای مجازی سایبر دانست. متناسب با پیچیده تر شدن روابط و شبکه‌های اجتماعی در عصر پست مدرنیته و خارج شدن این روابط از حالت‌های ساده اولیه که جنبه فیزیکی و محسوب داشت بر اهمیت افزایش امنیت شبکه و بررسی فرصت‌ها و آسیب‌های احتمالی آن بر ابعاد مختلف اقتصادی، فرهنگی و سیاسی افزوده شده که این خود ضرورت تبیین نظام جامع مدیریت نرم‌افزاری تهدیدات امنیت اجتماعی در فضای شبکه ای را دو چندان کرده و باید به عنوان یکی از بنیان های توسعه امنیت ملی مورد توجه متولیان امر قرار گیرد.

دولت علاوه بر تأمین امنیت منابع اطلاعاتی خود، باید متعهد باشد که مجموعه سیاست‌هایی را برای ایمن ساختن اطلاعات زیرساختی ملی خود تنظیم کند. این سیاست‌ها نقش مهمی در امنیت فناوری اطلاعات دارد با این حال تناقضی وجود خواهد داشت. آن این است که چهارچوب سیاست ملی باید به افزایش سطح امنیت کمک کند در اینجا نقش قوانین تعیین کننده‌اند و به بیان دیگر قوانین ضعیف دولتی بیش از آنکه سودی در پی داشته باشد ضرر به بار می‌آورد. فناوری به سرعت در حال تغییر است و تهدیدات رایانه‌ای جدید به دلیل همین تغییرات به وجود آمده در چنین وضعیتی از قوانین دولتی برای جلوگیری از گسترش شیوه‌های نوین استفاده می‌نند. جرایم رایانه‌ای و خلافکاری تدوین و ایجاد شده تا بهتر بتوانند معیارها و سیاست‌های امنیتی و تدابیر سازمانی به وجود آورند و در برابر تهدیدات فضای سایبر واکنش نشان دهند و سازمان ها را با یکدیگر هماهنگ نمایند. در سال‌های اخیر، دولت‌ها و سازمان‌های بین المللی بر امنیت سایبری تمرکز بیشتری نموده‌اند و از شرایط اضطراری آن کاملاً اطلاع دارند. حمله سایبری به احتمال قوی از جدی‌ترین چالش‌های امنیتی است که از طریق فضای مجازی به دولت‌ها تحمیل می‌گردد. مشابه با ابزارهای متعارف، از فناوری سایبری نیز می‌توان برای حمله به تشکیلات دولتی، موسسات مالی، زیرساخت‌های ملی، انرژی، صنعت، حمل و نقل و روحیه‌ی عمومی بهره جست. از مهم‌ترین راه‌های مقابله با تهدیدات سایبری:

- وضع قوانین و مقررات متعدد متناسب با شرایط بومی کشور است. با وضع قوانین می‌توان فعالیت کاربران را در شبکه مجازی سازمان‌دهی و نظارت و کنترل کرد.
- از آنجایی که نیروی انتظامی مسئولیت نظم در جامعه را دارد ایجاد و توسعه پلیس سایبر نقش مهمی در مقابله با تهدیدات در فضای مجازی ایفا می‌کند.
- دولت با کاربست فناوری‌های نوین و کاربست سازوکارهای تقنینی نظارتی برای مقابله موثر با تهاجم شبکه ای و تسهیل وتسریع زیرساخت‌های شبکه اقدام نماید.

- آسیب‌شناسی جنگ نرم و مقابله با آن از طریق تأسیس مرکز ملی هماهنگ کننده جنگ نرم در کشور، راه‌اندازی شبکه‌های رسانه‌ای جدید و اهمیت و توجه به مبانی قدرت نرم می‌تواند علاوه بر صیانت از حاکمیت سیاسی به بالابردن قدرت نرم در عرصه‌ی خارجی نیز اقدام نمود.
- تشکیل نهضت وبلاگی در کنار ایجاد شبکه‌های بومی در جهت جریان سازی فکری فرهنگی بسیار تأثیر گذار می‌باشد.
- تولید محتوای مناسب در فضای سایبر به عنوان یک رسانه برای انتقال مفاهیم و ارزش‌ها مورد استفاده قرار می‌گیرد.
- تولید نرم‌افزارهای اسکادای بومی، چون در بسیاری از صنایع و زیرساخت‌ها با نرم افزارهای کنترل صنعتی غیر بومی فعالیت می‌کنند و این مسئله خطر جدی تلقی می‌گردد و باعث انتشار ویروس‌ها بر روی سامانه‌های کامپیوتری می‌شود.
- ایجاد شبکه‌ی ملی اطلاعات که در واقع یک شبکه داخلی است که پردازنده اطلاعات داخلی کشور خواهد بود و ایمنی بیشتری را تضمین خواهد کرد.
- ارائه‌ی خدمات رایانه‌ای نظیر ایمیل و موتور جستجوی بومی که صرفنظر از بحث امنیت و محرمانگی اطلاعات فرصتی مناسب برای سایت‌های فارسی و تولیدکنندگان محتوای داخلی به شمار می‌رود .
- راه‌اندازی سیستم عامل بومی مشکلاتی چون هزینه بالا خرید سیستم عامل ویندوز، عدم دسترسی به کد منبع این سیستم عامل و ایمنی کم آن برای رایانه‌های کاربران داخلی را برطرف می‌کند.

منابع و مأخذ

۱. افتخاری، اصغر. ۱۳۸۲. استراتژی ملی برای تأمین امنیت در فضای مجازی، پژوهشکده مطالعات راهبردی.

۱. باطنی، ابراهیم؛ یزدان شناس، مهدی. ۱۳۹۰. نگاهی به شکل گیری دولت الکترونیک و چالش های فراروی آن، نشریه فقه حقوق.

۲. برون، مهرداد،۱۳۹۶. امنیت و دفاع سایبری،اولین کنفرانس ملی پدافند سایبری،مراغه

۳. پوراحمدی، حسین. ۱۳۸۴. انقلاب اطلاعاتی، ارتباطاتی جهانی شدن و تبیین نو از منابع قدرت، فصلنامه رهیافت‌های سیاسی و بین المللی.

۴. ترابی، قاسم. ۱۳۹۸. ضرورت ها و الزامات تدوین راهبرد سایبری کار آمد، فصلنامه مطالعات راهبردی، شماره ۳.

۵. جهانگشته، اسماعیل؛دامنی،فاطمه؛رئیسی،سلمان، ۱۳۹۸، بررسی اهمیت امنیت فضای سایبری، هشتمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات.

۶. حسینی، پرویز؛ ظریف‌منش، حسین. ۱۳۹۲. مطالعه تطبیقی ساختار دفاع سایبری دولت ها، فصلنامه پژوهش‌های حفاظتی امنیتی دانشگاه جامع امام حسین (ع)، شماره ۵.

۷. خلیل زاده، مونا. ۱۳۹۳. مسئولیت بین المللی دولت‌ها در برابر حمله‌های سایبری. تهران. انتشارات مجد.

۸. خلیلی‌پور رکن آبادی، علی؛ نورعلی وند، یاسر. ۱۳۹۱. تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی، شماره ۱۵.

۹. رضوی‌پور، فضل اله؛ فتحی، فرشته؛ نورمحمدیان، زهرا،۱۳۹۷. رابطه‌ی امنیت سایبری با تهدیدات سایبری، دومین کنفرانس ملی پدافند سایبری، مراغه.

۱۰. رضوی فرد، بهزاد؛ موسوی، سیدنعمت الله، ۱۳۹۵. مسئولیت کیفری در فضای سایبر در حقوق ایران، پژوهش حقوق کیفری سال پنجم، شماره شانزدهم.

۱۱. صیفی، بهنام،۱۳۹۶. بررسی مسئولیت کیفری متولیان امنیت سایبری در کشور ایران، اولین کنفرانس ملی پدافند سایبری، مراغه.

۲. طارمی، محمد حسین. ۱۳۸۹. فضای سایبر و آسیب ها و مخاطرات، اطلاع رسانی کتابداری ره آورد نور.

۱۲. طیبی توکلی، حسن. ۱۳۹۳. مجموعه قوانین و مقررات برنامه ۵ساله اول تا پنجم، مجمع مرکز تحقیقات استراتژیک.

۱۳. عسکری، مریم؛ مدیری، ناصر.۱۳۹۹. معماری خودارزیابی امنیت سایبری، چهارمین کنفرانس ملی پژوهشی کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی.

۱۴. علیوردی نیا، اکبر.۱۳۹۳. مدیریت پیشگیری از جرم در ایران. فصلنامه سایت های راهبردی کلان سال دوم شماره 5A-37:.

۱۵. قهرمانی افشار، نیوشا؛ کرامت میرشکارلو، یاسین،۱۳۹۷. جرم‌شناسی سایبری در پرتو دو مفهوم جرم و امنیت، اولین کنفرانس ملی پدافند سایبری، مراغه.

۱۶. موسوی، محمدرضا؛ حیدری، خدیجه؛ قنبری، علی. ۱۳۹۲. تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن، فصلنامه علمی مطالعات بین المللی پلیس، شماره ۱۴،

۱۷. نائینی، علی محمد، ۱۳۸۶. تهدید نرم ابعاد و ویژگی ها، مطالعات عملیات روانی، شماره ۱۶.

۱۸. نصری مشکینی، قدیر. ۱۳۸۵. سیاست‌گذاری امنیتی ایران در سه برهه، نشریه: اطلاع رسانی و کتابداری، ماه علوم اجتماعی.

۱۹. وحیدپور، حمید. ۱۳۹۲. لازمه وجود توانمندی های سایبری پدافندی و تهاجمی به عنوان عوامل بازدارندگی، ششمین کنگره انجمن ژئوپلیتیک ایران پدافند غیر عامل مشهد.

۳. ولی پور رزومی، حسین. ۱۳۹۱. گفتمان امنیت ملی، مؤسسه فرهنگی مطالعات ملی.

۲۰. یاسمی‌نژاد، عرفان؛ آزادی، اکرم؛ امویی، محمدرضا. ۱۳۹۰. فضای مجازی، امنیت اجتماعی، راهبردها و استراتژی‌ها، همایش ملی صنایع فرهنگی نقش آن در توسعه پایدار.

۲۱. یزدان فام، محمود. ۱۳۸۷. راهبرد امنیت ملی امریکا، پژوهشکده مطالعات راهبردی تهران.

۲۲. یزدان فام، محمود. ۱۳۸۹. امنیت نرم و چرایی آن شماره سوم سال ۱۲، فصلنامه مطالعات راهبردی.

23.Ploug,Thomas, *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal* Interaction, Ballerup Denmark, Springer pub: 2009.