نقش پلیس برای مقابله باچالش‌ها و تهدیدهای امنیتی در محیط سایبر

دریافت مقاله : ۹۰/۱۱/۲۳ پذیرش مقاله: ۹۱/۴/۱۱

مهدی شیرمحمدی[۱]

چکیده

احساس امنیت یکی از ابعاد اساسی مفهوم امنیت در معنای کلی آن است.پیش فرض اساسی مقاله حاضر نقش پلیس در تأمین و فراهم کردن امنیت فضای سایبردر ایران است.عملکرد این نهاد امنیتی انتظامی به اشکال گوناگون می تواند در فرآیند تولید و استمرار احساس امنیت سایبر مؤثر باشد.هدف تحقیق بررسی مهم‌ترین چالش‌های پیش رو و چگونگی شیوه بهتر کردن وتقویت عملکرد پلیس بر گسترش امنیت فضای سایبر است. در این پژوهش از روش توصیفی- تحلیلی استفاده شده است؛ علاوه بر این ارتباط معناداری بین مفاهیمی چون فضا، اطلاعات، امنیت و چالش ها به عنوان فرضیه لحاظ شده است.. بر این اساس فضای سایبر به دلیل اهمیت و جایگاه ویژه ای که از نظر تبادل اطلاعات پیدا نموده، مفهوم گسترده ای از امنیت و چالش را در خود نهفته است؛ بنابراین مفاهیم می توانند به عنوان مدلی در سایر فضا ها به کار گرفته شوند.

یافته‌های مقاله نشان می دهد که چالش ها در محیط سایبر در ابعاد گسترده و همه جانبه ای وجود دارند که سطوحی از امنیت اجتماعی، اقتصادی، فرهنگی و سیاسی را به چالش می‌کشند؛ بنابراین با توجه به اینکه تهدیدهای فضای سایبر[۲] در یک نگاه کلی با هدف جنگ نرم علیه نظام حاکمیت ملی کشور می باشد به همین منظور گسترش مفهوم امنیت شبکه از سوی پلیس و لزوم سیاست گذاری‌های منسجم از سوی قانونگذار و دستگاه‌های متصدی امری ضروری می باشد.

نتایج تجزیه و تحلیل داده ها نشان می دهد که توانمندی عملیاتی پلیس به تنهایی نمی تواند درگسترش امنیت فضای سایبر[۳]، اثر گذار باشد بلکه باید سیاست‌گذاری‌ها و قوانین حمایتی از سوی قانونگذار و دولت به منظور تخصصی کردن نقش ها و بالا بردن ظرفیت کارکرد سایر نهادها به‌ویژه پلیس[۴] صورت گیرد تا باعث بالا بردن افزایش امنیت فضای سایبری گردد.

کلید واژه ها

چالش‌ها/تهدیدهای امنیتی /محیط سایبر/ پلیس

۱- عضو هیئت علمی آموزش ناجا،کارشناس ارشد علوم سیاسی واطلاعات،مدرس دانشگاه علوم انتظامی

2-Challenges

3-Cyberspace

مقدمه

نظر به اینکه اینترنت یک شبکهٔ عظیم اطلاع‌رسانی و یک بانک وسیع اطلاعاتی است و در آینده نزدیک دسترسی به آن برای تک‌تک افراد الزامی لذا به نظر می‌رسد؛ بر این اساس، کارشناسان ارتباطات، بهره‌گیری از این شبکه را یک امر ضروری در عصر اطلاعات می‌دانند.

این شبکه به عنوان گستره ای همگانی که از هزاران شبکه کوچک‌تر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته و از طرف دیگر شرایط تبادل اطلاعات در این حوزه حائز اهمیت ویژه ای گردیده که در اثبات این موضوع طبق آخرین آمار بیش از شصت میلیون رایانه از تمام نقاط جهان در این شبکهٔ گسترده به یکدیگر متصل شده‌اند که اطلاعات بی‌شماری را در تمامی زمینه‌ها از هر سنخ و نوعی به اشتراک گذاشته‌اند. گفته می‌شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است (گنجی،علیرضا،۱۳۸۲ :۴).

این اطلاعات با سرعت تمام، در بزرگراه‌های اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود.

بدون شک، به دلیل اهمیت این موضوع است که حمایت از جریان آزاد اطلاعات، گسترش روزافزون فنآوری اطلاعات و بسترسازی برای اتصال به شبکه‌های اطلاع‌رسانی شعار دولت‌هاست، نه فقط به دلایلی که ذکر شد بلکه در عین حال تبادل آزاد اطلاعات، نگرانی‌هایی هم به همراه آورده است که عبارت‌اند از: گستردگی و تنوع اطلاعات آلوده روی اینترنت، انتشار تصاویر مستهجن، ایجاد پایگاه‌هایی با مضامین پورنوگرافی و سایت‌های سوءاستفاده از کودکان و انواع قاچاق در کشورهای پیشرفته صنعتی.

اهمیت بحران زایی فضای سایبر به‌خصوص در خاستگاه این شبکهٔ جهانی یعنی آمریکا، کارشناسان اجتماعی را به‌شدت نگران کرده، به گونه‌ای که هیئت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا نموده است. هشدار، جریمه و بازداشت برای برپاکنندگان پایگاه‌های مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده‌اند.این مهم باعث گردیده است تا نقش پلیس برای مقابله با پیامدهای منفی این گستره عظیم، مورد توجه قرار گیرد در ایران نیروی انتظامی جمهوری اسلامی نیز با ایجاد پلیس فتا(فناوری تبادل اطلاعات)سعی و تلاش دارد در جهت مدیریت این دسته از پیامدهای مرتبط اقدام نماید.

اهمیت و ضرورت

گستره مفهوم امنیت شبکه در پنج بعد سیاسی، اقتصادی، فرهنگی، اجتماعی و قضایی ریشه دوانده که فقدان بستر سیاستی منسجم برای مدیریت پیشگیرانه تهدیدهای احتمالی در فضای مجازی، می تواند،زیر بنای توسعه مطلوب انتظامی در افق ایران ۱۴۰۴را با چالش‌های جدی مواجه کند،از طرفی رفع خلاءهای قانونی،نظارتی و اجرایی مدیریت تهدیدهایی امنیت اجتماعی در فضای وب، زمانی دارای ضریب اثر بخشی بالایی است که از شش مشخصه همسویی با اسناد بالادستی،فرابخشی،کلان نگری، راهبردی، هدف محوری(انسجام فکری)و برنامه محوری(ثبات رویه ای)برخوردار باشد و هرگونه نگاه سطحی نسبت به تهدیدهای انتظامی–امنیتی کشور در محیط مجازی می تواند نطفه شکل گیری وقوع بحران‌های پنجگانه منزلت، مشروعیت، نفوذ، توزیع و مشارکت رادر سیاست‌های کلان انتظامی برنامه پنجم و سند چشم انداز، به وجود آورد (پای،۱۳۸۰ : ۲۰۸ و سیف زاده، ۱۳۶۸ :۱۷۳).

ایمن سازی فضای مجازی به عنوان یکی از اصول راهبردی دولت ها برای ارتقای ضرایب امنیت داخلی و خارجی محسوب می شود.به طوری که همسو با توسعه زیر ساخت‌های تدابیر حفاظتی و ایمنی مرزها و زیر ساخت‌های حساس نظیر نیروگاه ها،سدها،پادگان ها، مراکز و تأسیسات هسته ای، توسعه ضرایب امنیت شبکه نیز به عنوان یکی از دغدغه‌های اصلی کشورها درآمده است. به همین منظور کشورهای توسعه یافته، مانند ایالات متحده آمریکا،کمیته مشورتی ویژه ای را برای افزایش امنیت در فضای مجازی ایجاد کرده اند تا بتوانند با هماهنگی بین دو بخش خصوصی و دولتی امنیت فضای سایبر را فراهم کنند(افتخاری،۱۳۸۲ :۹)؛ به طوری که امروزه مدیریت پیشگیرانه تهدیدهای امنیت ملی در فضای مجازی به یکی از کارویژه‌های مهم وزارت امنیت داخلی تبدیل شده است(وایت و کالینز، ۲۰۰۶: ۳۷). طبق آمار، شرکت ها سالیانه حدود یک تریلیون دلار در زمینه تجهیزات،نرم افزار و خدمات فناوری هزینه می کنند و اگر مبالغ مربوط به هزینه خدمات مخابراتی را به این مبلغ اضافه کنیم رقمی معادل دو تریلیون دلار خواهد شد (گراه،۱۳۸۶ :۱۰۹).

در یک دیدگاه کلی به رغم وجود جنبه‌های مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبه‌رو ساخته است. از این رو به‌کارگیری فیلترها و فایر وال‌های[1] مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است.

اهمیت شناخت چالش‌ها و تهدیدهای فضای سایبر امری ضروری است و با وجود تبادل عظیم اطلاعات حیاتی ویا خصوصی از طریق اینترنت، باید دید اینترنت

۱-فایروال می‌تواند یک دستگاه سخت افزاری و یا یک برنامه نرم افزاری و یا ترکیبی از هردو باشد. یک فایر وال خوب می تواند جلوی دسترسی هکرها به‌داخل رایانه شما را بگیرد، در ضمن نمی گذارد هیچ‌گونه اطلاعاتی بدون اجازه شما از رایانه خارج شود. فایروال نمی تواند مستقیما جلوی حمله ویروس‌ها را بگیرد اما گاهی جلوی ویروس‌ها را برای ارسال ایمیل از یک رایانه آلوده می گیرد.

تا چه حد برای ارسال داده‌های حساس، مطمئن است و امنیت شبکه‌ها وقتی داده‌ها درآن جریان پیدا می‌کنند با چه راهکارهایی، کم هزینه می گردد.

تعریف مفاهیم

امنیت

مسئله امنیت (اعم از عینی و ذهنی) از جمله نیازهای اساسی بشر در طول تاریخ است که به گواه بسیاری از اندیشمندان قدمتی بسیار طولانی تر از مفهوم اجتماع و جامعه دارد.

انسان‌های اولیه، امنیت را به عنوان یکی از اساسی ترین ارکان زندگی در کنار نیاز به آب و غذا مطرح می کردند و دور از ذهن نیست اگر غارنشینی را به عنوان نماد قابل دفاعی از حرکت انسان‌های اولیه در مسیر رفع این نیاز عنوان کرد.

گذر زمان انسان ها را بر آن داشت تا زندگی در کنار یکدیگر را به عنوان یکی از بهترین راه‌های مؤثر در جهت حفظ امنیت خویش بپذیرند، ابتکاری که اگرچه تا حد زیادی توانست امنیت او را در مقابل بلایای احتمالی – بلایای طبیعی، حمله جانوران و درندگان و. .. تضمین کند اما به مرور زمان، خود دغدغه ای جدید برای انسان ها به ارمغان آورد.

انسان‌ها که با زندگی در کنار یکدیگر توانسته بودند پایگاه مناسبی در برابر خطرات احتمالی دیگر موجودات ایجاد کنند، به دنبال رشد جمعیت، نیاز به مالکیت زمین، تکاپو در مسیر آسایش و رفاه، تنوع طلبی، افزایش ابداعات و اختراعات و... خود، مخدوش کننده امنیت یکدیگر شدند. در ابتدا این درگیری ها حالت گروهی و قبیله ای داشت و یک قبیله برای غارت قبیله دیگر، امنیت اعضای آن را به مخاطره می انداخت اما با گذر زمان، رشد سریع جمعیت و تشکیل حکومت ها، امنیت نیز

وارد مرحله جدیدی شد و نیاز به طرح راهکارهای نوین در جهت افزایش امنیت به صورت چالشی عظیم در زندگی انسان پدیدار گشت.

در این دوران، نیاز به امنیت در دو فاز مجزای داخلی و خارجی قابل پیگیری بود، از یکسو حکومت ها موظف به حفظ امنیت شهروندان خود در مقابل تهاجم احتمالی بیگانگان بودند و از سوی دیگر، تعرض و تعدی قانون شکنان به حریم زندگی شهروندان، آنها را با مشکل روبه‌رو می ساخت و این مسئله، ایجاد نیروی خاص برای حفظ امنیت را الزامی می کرد.

اندک اندک با رشد صعودی شهرنشینی، افزایش انتظارات و خواسته ها و عدم توانایی گروه‌های قابل توجهی از مردم برای دستیابی به آمال و آرزوها، رشد بیکاری، افزایش معضلات و کجروی‌های اجتماعی و. ...، وضعیت امنیت بار دیگر با چالش روبه‌رو شد و اندیشمندان و صاحب نظران را برای ارائه راهکارهای عملی به تکاپو انداخت، تکاپویی که ماحصل آن خرد شدن واژه امنیت در مقوله‌های مختلفی از جمله نظامی، سیاسی، اقتصادی، اجتماعی و... بود.

از آنجایی که این پژوهش بر مفهوم امنیت اجتماعی تأکید دارد، از ورود به مباحث دیگر اجتناب نموده و بر بحث امنیت اجتماعی تمرکز می‌نماییم(تاجیک، محمدرضا،۱۳۷۷ :۱۲).

چالش‌های سایبری

در یک تحلیل گسترده‌تر در جهت نمایان‌تر شدن اهمیت موضوع، می توان این مسئله را مطرح کرد که فن‌آوری‌های نوین، مشکلات و چالش‌هایی را نیز برای امنیت ملی کشورها به وجود آورده که تهاجم سایبر،سرقت اطلاعات محرمانه،هک کردن سایت‌های اینترنتی وزارتخانه ها و نهادهای راهبردی، نفوذ در شبکه‌های مالی و پولی و حساب‌های شخصی، هتک حرمت افراد و در نهایت تهدید حاکمیت ملی

از سوی اشخاص و گروه‌های سازمان یافتهٔ بین المللی، از مهم ترین مصادیق آن است. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است؛ زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند، می‌تواند سلامت و امنیت جامعه را به خطر اندازد(جمال زاده. ۱۳۸۸ :۹).

تعریف جرم رایانه‌ای

تاکنون تعریف‌های گوناگونی از جرم رایانه‌ای از سوی سازمان‌ها، متخصصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این جرایم است.

جرم رایانه‌ای یا جرم در فضای مجازی (سایر جرایم) دارای دو معنی و مفهوم است. در تعریف مضیق، جرم رایانه‌ای صرفاً عبارت از جرایمی است که در فضای سایبر رخ می‌دهد. از این نظر جرایمی مثل هرزه‌نگاری، افترا، آزار و اذیت سوءاستفاده از پست الکترونیک و سایر جرایمی که در آنها رایانه به عنوان ابزار و وسیله ارتکاب جرم به‌کار گرفته می‌شود، در زمرهٔ جرم رایانه‌ای قرار نمی‌گیرند(گنجی، ۱۳۸۲ :۱۱).

در تعریف کامل تر، هر فعل و ترک فعلی که در اینترنت یا از طریق آن یا با اینترنت یا از طریق اتصال به اینترنت، چه به‌طور مستقیم یا غیرمستقیم رخ می‌دهد و قانون آن را ممنوع کرده و برای آن مجازات در نظر گرفته شده است جرم رایانه‌ای نامیده می‌شود. براین اساس این‌گونه جرایم را می‌توان به سه دسته تقسیم نمود: دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شوند. مانند سرقت، تخریب و غیره.

دسته دوم: جرایمی هستند که در آنها از رایانه به عنوان ابزار، توسط مجرم بـرای ارتکاب جرم استفاده می‌شود.

دسته سوم: جرایمی هستند که می‌توان آنها را جرایم رایانه‌ای محض نامیـد. ایـن نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیـای مجـازی بـه وقـوع می‌پیوندند اما آثار آنها در دنیای واقعی ظاهر می‌شود. ماننـد دسترسـی غیرمجـاز بـه سیستم‌های رایانه‌ای(محسنیان،۱۳۷۹ :۳۲).

طبقه‌بندی جرایم رایانه‌ای

طبقه‌بندی‌های مختلفی از جرایم رایانه‌ای توسط مراجع مختلف انجام گرفته است که مهم‌ترین آنها عبارت اند از:

۱- طبقه‌بندی اعمال مجرمانه (امپراطوری عثمانی پایگاه ارز)[1]

در سال ۱۹۸۳ «او.ای.سی.دی.بی» متعهد شد بر روی مطالعه امکان پذیری اعمال بین‌المللی و هماهنگی قوانین کیفری، به منظور حل مسئله جرم یا سوءاستفاده‌های رایانه‌ای مطالعه کند. این سازمان در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه‌ای، تحلیل سیاست‌های قانونی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو پرداخته و فهرست حداقل سوءاستفاده‌هایی را ارائه کرده بود که کشورهای مختلف باید با استفاده از قوانین کیفری، مشمول ممنوعیت و مجازات قرار دهند. بدین گونه اولین تقسیم‌بندی از جرایم رایانه‌ای در سال ۱۹۸۳ ارائه شد و طی آن پنج دسته اعمال را مجرمانه تلقی کرد و پیشنهاد کرد در قوانین ماهوی ذکر شود. این پنج دسته عبارت‌اند از:

1-Ottoman Empire Currency Database (OECB)

الف) ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که به‌طور ارادی با قصد انتقال غیرقانونی وجوه یا هر چیز باارزش دیگر صورت گرفته باشد؛

ب) ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌های رایانه‌ای و برنامه‌های رایانه‌ای که به‌صورت عمدی و به قصد ارتکاب جعل صورت گرفته باشند یا هرگونه مداخله دیگر در سیستم‌های رایانه‌ای که به‌صورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه‌ای و یا ارتباطات صورت گرفته باشد؛

ج) ورود، تغییر، پاک کردن و متوقف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای؛

د) تجاوز به حقوق انحصاری مالک یک برنامهٔ رایانه‌ای حفاظت شده با قصد بهره‌برداری تجاری از برنامه‌ها و ارائه آن به بازار؛

ه) دستیابی یا شنود در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور یا تخطی از تدابیر امنیتی و با هدف غیر شرافتمندانه و یا موضوع صورت گرفته باشد(محسنیان،۱۳۷۶ :۲۱).

گستره فضای مجازی در محیط امنیت 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 ومرزی، توسعه زیر ساخت‌های امنیت فضای شبکه نیز به یکی از پیش نیازهای توسعه انتظامی مطلوب در افق ۱۴۰۴ تبدیل شده است؛ از این رو دربارهٔ یک رویکرد آینده پژوهی کاربرد و یا ویژگی و ابعاد جنگ‌های شبکه ای با ذکر مصادیقی بررسی و در چارچوب ساختار امنیت ملی برنامه پنجم توسعه و سند چشم انداز، به مهم ترین تهدیدهای انتظامی –امنیتی و بایسته‌های سیاستی جمهوری اسلامی ایران، در برابر تهاجم شبکه ای اشاره می شود.

پلیس سایبر

اساس و بنیاد هر جامعه، چه کوچک و چه بزرگ، بر اصولی استوار است که بدون آنها شیرازه جامعه از هم گسیخته خواهد شد. گفته می شود مهم‌ترین این اصول، نظم و قانون است. جامعه مجازی نیز به همین صورت است. فضای سایبر در واقع محیطی مجازی برای فعالیت‌های اجتماعی است. مهم ترین ویژگی این فضا، استقلال از زمان و مکان است. با شکل گیری فضای سایبر، مرزها کمرنگ تر شده است و جهانی شدن در کلیه امور اجتماعی به وضوح دیده می شود. سرعت، ارزانی، بالا بودن کیفیت، نزدیکی و در دسترس بودن، شفافیت و تنوع از ویژگی‌های فضای سایبر است. در این فضا همان گونه که فعالیت‌ها سریع تر و دقیق تر انجام می‌شود، جرایم نیز پیچیده تر، سریع تر و کم هزینه تر انجام می شود. به عنوان مثال در دنیای واقعی، محیط فیزیکی محدودیت ها و موانع بزرگی را برای مجرمان و تبهکاران ایجاد می‌کند اما در فضای سایبر چنین موانع فیزیکی وجود ندارد. به دلیل ویژگی‌های خاص فضای سایبر، این فضا به قوانین کارآمد نیاز دارد. از سوی دیگر اجرای قانون نیازمند سیستمی است که بر فعالیت‌های شبکه نظارت کند و به تعقیب و دستگیری مجرمان در محیط سایبر بپردازد. به چنین سیستمی، «پلیس سایبر» می‌گوییم.

با توجه به این نکته که نیروی انتظامی مسئول برقراری نظم در جامعه است، این ارگان می تواند با در دست گرفتن ابتکار عمل و از دست ندادن فرصت ها، مسئولیت نظم و امنیت در این حوزه بزرگ اجتماعی را نیز بر عهده گرفته است.

از این رو در ایران نیز برای مقابله با این افراد، پلیسی به نام پلیس سایبر شکل گرفته که این پلیس در حال حاضر در معاونت آگاهی ناجا مشغول به فعالیت است (جمال‌زاده. ۱۳۸۸ :۱۱).

پیشینه تحقیق

در مورد زمان دقیق پیدایش جرم رایانه‌ای نمی‌توان اظهارنظر قطعی کرد. این جرم زاییدهٔ فناوری اطلاعاتی و انفورماتیکی است؛ بنابراین به‌طور منظم بعد از گذشت مدت کوتاهی از شیوع و کاربرد فناوری اطلاعات، باب سوءاستفاده نیز قابل طرح است. شیوع استعمال این فناوری و برابری کاربران آن حداقل در چند کشور مطرح جهان به‌صورت گسترده، امکان بررسی اولین مورد را دشوار می‌سازد. در نهایت آن چه روشن است اینکه در جامعه آمریکا رویس[1] موجب شد برای اولین بار اذهان متوجه سوءاستفاده‌های رایانه‌ای شود (مولانا،۱۳۷۹ :۴۸).

آلدون رویس حسابدار یک شرکت تجاری بود. چون به گمان وی، شرکت حق او را پایمال کرده بود، بنابراین با تهیه برنامه‌ای، قسمتی از پول‌های شرکت را اختلاس کرد. انگیزهٔ رویس در این کار انتقام‌گیری بود. مکانیزم کار بدین گونه بود که شرکت محل کار وی یک عمده‌فروش میوه و سبزی بود. محصولات متنوعی را از کشاورزان می‌خرید و با استفاده از تجهیزات خود از قبیل کامیون‌ها، انبار و بسته‌بندی و سرویس‌دهی، به گروه‌های فروشندگان عرضه می‌کرد. به دلیل وضعیت خاص این شغل، قیمت‌ها در نوسان بود و ارزیابی امور تنها می‌توانست از عهدهٔ رایانه برآید تا کنترل محاسبات این شرکت عظیم را عهده‌دار شود. کلیه امور حسابرسی و ممیزی اسناد و مدارک و صورت حساب‌ها به صورت اطلاعات ضبط شده در نوارهای الکترونیکی ثبت می‌شد.

رویس در برنامه‌ها، دستورالعمل‌های اضافی را گنجانده بود و قیمت کالاها را با ظرافت خاصی تغییر می‌داد. با تنظیم درآمد اجناس مبلغی را کاهش می‌داد و مبالغ حاصله را به حساب‌های مخصوص واریز می‌کرد. بعد در زمان‌های خاص چکی به

1.Aldon Roy

نام یکی از هفده شرکت جعلی و ساختگی خودش صادر و مقداری از مبالغ را برداشت می‌کرد. بدین ترتیب وی توانست در مدت ۶ سال بیش از یک میلیون دلار برداشت کند. اما او بر سر راه خودش مشکلی داشت و آن این بود که مکانیسمی برای توقف عملکرد سیستم نمی‌توانست بیندیشد. بنابراین در نهایت خود را به مراجع قضایی معرفی و به جرم خود اعتراف کرد و به مدت ده سال به زندان محکوم شد. از این جا بود که مبحث جدیدی به نام جرم رایانه‌ای مطرح شد(محمدی،۱۳۷۹ :۴۶).

موارد و روش ها

پلیس یک پدیده، کارکرد مشخصی دارد در مورد فضای سایبر، کارکرد پلیس حفظ امنیت در مقابل چالش‌های گسترده ای است که فضای سایبر مسبب آن است.در این میان کارکرد پلیس می تواند همراه با تحول در برخی پدیده ها متأثر شده و برای حفظ کارکرد مؤثر، نیازمند به تغییرات یا حمایت شود.

فضای سایبر: فضای سایبر به عنوان یک رویدادی است که در قرن بیستم سر بر آورده و بدلیل کلیت مفهومی که دارد ابعاد وسیعی از زندگی اجتماعی، سیاسی، اقتصادی و معنوی انسان ها مربوط شده و این ابعاد را تحت تأثیر قرار می دهد.ما در این مقاله به دنبال شناخت چالش‌هایی هستیم که فضای سایبر در حوزه امنیتی مسبب آن می شود و به دلیل اینکه موضوع امنیت فضای سایبر به طور عمده ای با کارکرد و نقش پلیس در جامعه گره خورده است شناخت ابعاد این تهدیدها و راه حل مهارشان از سوی نهاد پلیس، محور اصلی و روش اصلی تحقیق حاضر را در بر می‌گیرد که در یک عبارت می توان آن را روش ترتیب مسئله، علت و راه حل نامید.که به ترتیب شناخت مشکل و علت‌های وقوع آنها و راه حل‌های پیشنهادی از سوی محقق را شامل می شوند. بر این اساس نشان خواهیم داد که مفهوم امنیت در

فضای سایبر چه جایگاهی یافته است و این جایگاه را از طریق ترتیب موضوعی که از مفهوم امنیت ارائه خواهیم داد از نظر می گذرانیم. در ترتیب موضوعی چرایی اتفاق برخی چالش ها در فضای سایبر و تأثیرات ناشی از آنها بررسی می شود و بر این اساس روش ما روش توصیفی تحلیلی خواهد بود؛ چرا که چگونگی توصیف چالش‌های موجود در فضای سایبر می تواند ابعاد جدیدی را بر کارکرد نهادهای مسئول در این موضوع نمایان سازد؛ لذا ما کلیت و گسترش در مفهوم فضای سایبر را در لزوم تخصصی شدن کارکرد ها در زمینه شناخت و مهار این فضا تأثیر گذار می دانیم؛ بنابراین روش تحلیلی برای ارتباط بین این دو متغیر معنی پیدا می کند.

یافته‌ها

الف) امنیت شبکه‌های اطلاعاتی و ارتباطی

تعریف شبکه:

امروزه همهٔ انسان‌ها خواسته یا ناخواسته با فناوری وسیعی سرو کار دارند که در اصطلاح به آن شبکه گفته می‌شود. در تعریف ساده شبکه به مجموعه‌ای از دستگاه‌های رایانه از قبیل: Pad، device، router، switch،... گفته می‌شود که به نوعی با هم در ارتباط هستند. این ارتباط می‌تواند از طریق سیم، بی سیم، رادیو و... باشد.

اهمیت امنیت شبکه

چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن در اجتماع آینده پی برده باشیم، اهمیت امنیت این شبکه‌ها مشخص می‌گردد. اگر امنیت شبکه برقرار نگردد، مزیت‌های فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی

و نشریه‌های الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی قرار می‌گیرند. همچنین دستکاری اطلاعات- به عنوان زیربنای فکری ملت‌ها توسط گروه‌های سازماندهی شده بین‌المللی، به نوعی باعث مختل ساختن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود(باری،۱۳۸۷ :۳۵).

برای کشور ما که بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکت‌های خارجی تهیه می‌شود، بیم نفوذ از طریق راه‌های مخفی وجود دارد. در آینده، بانک‌ها و بسیاری از نهادها و دستگاه‌های دیگر، از طریق شبکه فعالیت خواهند کرد و جلوگیری از نفوذ عوامل مخرب در شبکه به‌صورت مسئله‌ای راهبردی درخواهد آمد که نپرداختن به آن باعث بروز خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایت‌های ایرانی ارسال شود و سیستم عامل‌ها در واکنش به این پیغام سیستم‌ها را خراب کنند و از کار بیندازند، به طورقطع ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد

نکته جالب اینکه بزرگ‌ترین شرکت تولید نرم‌افزارهای امنیت شبکه، شرکت چک پوینت است (گنجی،۱۳۸۲ :۸) که شعبهٔ اصلی آن در اسرائیل می‌باشد. مسئله امنیت شبکه برای کشورها، مسئله‌ای راهبردی است؛ بنابراین کشور ما نیز باید به آخرین فناوری‌های امنیت شبکه مجهز شود و از آنجایی که این فناوری‌ها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، پس می‌بایست محققان کشور این مهم را به‌دست بگیرند و در آن فعالیت نمایند.

ب-چالش‌هاوتهدیدهای امنیتی فضای سایبری:

مهم‌ترین شاخص‌های تهاجم سایبری با رویکرد افزایش هزینه‌های انتظام بخشی پلیس کشور در برنامه پنجم و سند چشم انداز عبارت اند از:

۱-سازمان دهی تنش‌های متراکم و گسترده با رویکرد تضعیف نظام امنیت اجتماعی و سیاسی کشور:

رصد تحرکات مخالفان نظام جمهوری اسلامی ایران قبل و بعد از دهمین دوره انتخابات ریاست جمهوری در فضای وب بیانگر برنامه ریزی شبکه ای هدفمند آنان، برای بحران سازی و ایجاد تنش‌های متراکم و گسسته در ساختار انتظامی کشور است.

تنش‌های اجتماعی متراکم، بخشی از جامعه را متأثر می سازند و کنترل آن برای پلیس کشور امکان پذیر است؛ در حالی که وقوع بحران‌های اجتماعی فراگیر در سطحی است که توانمندی‌های ناجا برای کنترل آن کافی نیست.

از طرفی رویکرد آمریکا پس از دهمین دوره انتخابات ریاست جمهوری ایران بر اساس دو رهیافت دولت ناکام و تهاجم نرم پایه گذاری شده به طوری که از یک طرف دولت دهم را در مدیریت کلان کشور ناکارآمد نشان می دهد و از طرف دیگر با گسترش کاربست آفندهای نرم افزاری برای پیشبرد دکترین (تنش از پایین، چانه زنی از بالا) برنامه ریزی می کند که با گسترش آشوب‌های اجتماعی می‌تواند هزینه‌های انتظام بخشی را افزایش دهد.

بحران‌سازی شبکه ای در قالب تهاجم نرم بیشتر بر قومیت ها، کارگران، دانشجویان، نخبگان، روزنامه نگاران و سرمایه داران متمرکز است؛ به طوری که دانشجویان، نخبگان و روزنامه نگاران با آفند تبلیغاتی نقض آزادی‌های مدنی و حقوق بشر؛ کارگران و دهک‌های متوسط و پایین جامعه از طریق بزرگ نمایی آسیب‌های اقتصادی و ناامنی شغلی، طیف سرمایه‌داران از طریق فقدان امنیت سرمایه‌گذاری و سرانجام گروه‌های قومی– فرقه ای با تبلیغ فقدان آزادی‌های مذهبی، نگاه تبعیض آمیز حاکمیت به آنها، بی توجهی دولت به توسعه استان‌های مرزی و تهییج ناسیونالیسم قومی در فضای سایبری تحریک می‌شوند.

به عبارتی، مهم‌ترین مختصات امنیتی تهاجم شبکه ای بر تنش افزایی چند بعدی[1] در پنج سطح قومی، فرقه ای، صنفی، دانشجویی و اجتماعی متمرکز شده که از مصادیق آن می توان به تأثیر شبکه‌های اجتماعی اینترنتی، مانند فیس بوک[2] و تویتر[3] در ایجاد، گسترش و انعکاس ناآرامی ها پس از دهمین دوره انتخابات ریاست جمهوری ۲۲ خرداد ۱۳۸۸ اشاره کرد و حتی دولت آمریکا با هدف تنش سازی‌های متراکم و گسترده از مدیریت سایت‌های اجتماعی، مانند تویتر، فیس بوک، یوتیوب[4] و فیلکر[5] درخواست کرد خدمات خود را بدون وقفه با تمرکز بر تحولات ایران ادامه دهند که خود بیانگر ارتباط تنگاتنگ محیط سایبر با امنیت ملی است(افتخاری، ۱۳۸۲ : ۱۵).

سایت‌های اجتماعی به سایت‌هایی گفته می شود که در آنها تولید محتوا و یا فعالیت کاربران از حالت یک طرفه بیرون آمده و کاربران در تولید محتوا، مشارکت فعال دارند و عقاید و نظریه‌های خود را در قالب متن و تصویر به اشتراک می‌گذارند.

شرکت جست و جو گر گوگل نیز برای تقویت ضریب نفوذ آفندهای شبکه ای، یک نرم افزار ترجمه انگلیسی به فارسی و بالعکس با هدف تسریع و تسهیل تبادل اطلاعات در وب سایت ها، وبلاگ ها و پیام‌های پست الکترونیک ایجاد و اقدام خود را با عناوین حمایت از دستیابی ایرانیان به اطلاعات، در شرایط افزایش محدودیت‌های رسانه ای توجیه کرد. زبان فارسی به عنوان چهل و دومین زبان در ترجمه آن لاین گوگل است(افتخاری، ۱۳۸۲ :۲۱).

1- Multi Dimension Maximizing
2- Facebook
3- Twitter
4- Youtube
5- Filker

مجلس نمایندگان و سنای آمریکا نیز همسو با آفندهای شبکه ای در ۱۹ ژوئن ۲۰۰۹ (۲۹ خرداد ۱۳۸۸) با صدور قطعنامه‌ای جمهوری اسلامی ایران را به دلیل اعمال خشونت علیه مردم معترض به نتیجه انتخابات ریاست جمهوری محکوم کرد. ۴۰۵ عضو مجلس نمایندگان به این قطعنامه رأی مثبت دادند.مهم ترین اهداف بحران سازی،در زمینه‌های سیاسی اقتصادی فرهنگی اجتماعی و ارزشی کشور از سوی مجرمان یا مهاجمان عبارت‌اند از:

۲-مشروعیت زدایی از نظام با شکاف سازی میان جامعه و سطوح حاکمیت؛

-به چالش کشاندن تعادل و انسجام تصمیم گیری‌های راهبردی با تفرقه افکنی و تضعیف انسجام فکری؛

-رویهٔ متولیان امر در مقوله‌های راهبردی؛

- بهره‌گیری از ترفند شایعه سازی با رویکرد به چالش کشاندن ثبات امنیت اجتماعی[1] و ایجاد ترس و رعب در جامعه، مانند شایعه ارتباط وقوع برخی زلزله ها در استان‌های جنوب شرقی با برخی آزمایش‌های هسته‌ای زیرزمینی، با هدف ناکارآمدسازی به وسیلهٔ تضعیف اعتماد مردم به نهادهای انتظامی، امنیتی و اطلاعاتی؛

-ایجاد بحران هویت با تضعیف وحدت ملی و تداعی شائبه نگاه تبعیض‌آمیز حاکمیت به اقلیت‌های قومی– فرقه ای؛

-تضعیف مقاومت ملی در شرایط بحران، از طریق افزایش سطح انتظارات و مطالبات جامعه؛

-امنیتی کردن مطالبات قومی – فرقه ای.

رصد گزاری ها و مراکز پژوهشی مخالف نظام در محیط‌های وب، بیانگر این است که مهم ترین اهداف آفندهای شبکه ای، ایجاد تنش‌های اجتماعی با ترفند تداعی شائبه نگاه تبعیض آمیز حاکمیت به آنان و تشویق ناسیونالیسم قومی است.

1- social security stability

ازراهکارهای مورد استفاده دشمنان برون مرزی، در جهت تأمین اهدافشان می توان به موارد زیر اشاره نمود:

۳-بهره گیری از ظرفیت مکمل دیپلماسی رسانه ای:

یکی از تدابیر مجریان تهاجم شبکه ای تأکید بر تهاجم رسانه ای به عنوان نقش مکمل آفندهای شبکه ای است؛ از این رو همسو با گسترش شبکه‌های اجتماعی مانند فیس بوک و تویتر شاهد افزایش رسانه‌های صوتی و تصویری مخالف نظام نیز هستیم. گسترش شبکه‌های تلویزیونی ماهواره‌ای مانند شبکه خبری بی.بی.سی فارسی[1] و صدای آمریکا[2] در این راستا قابل ارزیابی است.

۴- بهره گیری از ظرفیت نهادهای تقنینی:

یکی از شاخص‌های مختصات تهاجم شبکه ای حمایت نهادهای تقنینی و نظارتی کنگره آمریکا از آفندهای شبکه ای است که از مصادیق آن می توان به تصویب قانون قربانیان سانسور در ایران اشاره کرد که مجلس سنای آمریکا با اتفاق آرا در ۲۳ جولای ۲۰۰۹ (۱ مرداد ۱۳۸۸) آن را به تصویب رساند و به موجب آن مبلغ ۵۵ میلیون دلار با هدف شکستن فضای فیلترینگ و گسترش فضای اطلاع رسانی در ایران[3] اختصاص یافته است. سناتورهای دمکرات، باب کیسی و تد کافمن، سناتورهای جمهوری خواه، جان مک کین و لیندسی گراهام و سناتور مستقل جوزف لیبرمن[4] از طراحان این قانون بودند.

از مبلغ ۵۵ میلیون دلار، ۳۰ میلیون دلار آن برای گسترش برنامه و افزایش کارمندان رادیو اروپای آزاد (رادیو آزادی یا رادیو فردا)، شبکه خبری فارسی صدای آمریکا، خنثی سازی پارازیت‌های ماهواره ای[5] و بسته شدن پیامک‌های شبکه تلفن همراه،

1- british broadcasting corporation(BBC)farsi language programming
2- voice of Americas Persian news network
3- victims of iraninan censorship(voice)act
4- senators bob casey (D-PA).ted kaufman(D-DE).john McCain(R-AZ).lindsey graham(R-SC).joseph Lieberman(ID-CT)
5- satellite jam

افزایش وب سایت ها، حمایت از برنامه‌های فارسی بی.بی.سی و حمایت از سایت‌های اجتماعی مانند فیس بوک و تویتر و مبلغ ۲۰ میلیون دلار نیز برای رفع و دور زدن فیلترینگ در فضای سایبر اختصاص یافته است. در این طرح همچنین مبلغ ۵ میلیون دلار به وزارت امور خارجه اختصاص داده شده تا در زمینه تهیه گزارش از موارد نقض حقوق بشر در ایران به ویژه پس از دهمین دوره انتخابات ریاست جمهوری هزینه کند.

در این قانون دولت باراک اوباما ملزم شده فهرستی از شرکت‌هایی که به دولت ایران ابزار کنترل فضای اینترنت را فروخته اند، از پروژه‌های دولتی آمریکا کنار گذاشته شوند (رنجبران، ۱۳۸۹ :۱۳۴).

۵- بهره گیری از ترفندهای شایعه سازی مخرب:

از مهم ترین مختصات تهاجم شبکه ای، تمرکز آفندها بر ایجاد و ترویج شایعه‌های براندازانه و مخرب با هدف ایجاد تنش سازی و بی ثباتی در دو سطح گسسته و متراکم است. شایعه یعنی خبر یا اطلاع غیر موثقی که به صورت غیر رسمی مبتنی بر مشهودات و قول اجماع بوده و اعتبار خود را از تواتر و شیوع می گیرد (افتخاری، ۱۳۸۲ :۳۲).

ساختارهای شبکه ای مخالفان نظام جمهوری اسلامی ایران با شایعه سازی، به برنامه ریزی در محیط‌های شبکه ای و مجازی پرداخته و عمق راهبردی اقتدار نظام را در دو بعد داخلی و خارجی به چالش می کشانند. عمق راهبرد سیاسی در بعد داخلی عبارت است از راهبردی که بتواند زمینه پشتیبانی حداکثری و مستمر مردم را از سیاست‌ها و برنامه‌های نظام در داخل و خارج به دست آورد. مجریان تهاجم شبکه‌ای سعی دارند با بهره گیری از ترفند کاریکاتوریسم امینتی، اخبار واقعی را از طریق تصاویر مجازی تحریف و در راستای شکاف سازی میان سطوح حاکمیتی و جامعه و به تبع آن تضعیف اقتدار ملی برنامه ریزی کنند.

۶- بهره برداری ابزاری از ظرفیت گروهک‌های ضد انقلاب در فضای سایبر:
یکی از برنامه‌های گروهک‌های تروریستی مخالف نظام جمهوری اسلامی ایران، بهره‌گیری از فضای سایبر با هدف تنش‌افزایی، بحران‌زایی و شکاف‌زایی میان سطوح جامعه و حاکمیت است که از مصادیق آن می توان به موارد زیر اشاره کرد:
-بهره‌گیری منافقان از پیامک‌های تلفن همراه یا بلوتوث در راستای ناامن سازی فضای جامعه و یا شایعه سازی آنان مبتنی بر بیماری شدید رهبر فرزانه انقلاب؛
-ارتباط تلفنی با برخی مسئولان رده میانی و تلاش برای تخلیه اطلاعاتی آنان در فضای سایبر به ویژه در حوزه فعالیت‌های موشکی، هسته ای، امنیتی یا انتظامی؛
-رخنه در وبلاگ شخصی خبرنگاران و اعلام تمایل برای جذب هدفمند خبرنگار آزاد در محیط‌های مجازی (به عنوان مثال گروهک منافقان بدون افشای هویت خود با نفوذ در وبلاگ خبرنگاران، ارتباط دهی و ابراز تمایل برای همکاری با آنان، تلاش می کنند از آنها در راستای جمع آوری اطلاعات بهره برداری ابزاری کنند).
۷- تضعیف ثبات امنیت روانی جامعه:
یکی از شاخص‌های تهاجم شبکه ای دشمنان نظام جمهوری اسلامی ایران، تضعیف بنیان‌های اعتقادی و امنیت جامعه است که از مصادیق آن می توان به شایعه سازی در خصوص شیوه زندگی پیامبر اکرم (ص)، ایجاد و نشر تصاویر غیر اخلاقی و کلیپ با بلوتوث و تشکیک جامعه به قوانین مجازات اسلامی مانند احکام ارتداد، قصاص و سنگسار اشاره کرد.
۸- گسترش شیعه هراسی و هزینه افزایی ضرایب انتظام بخشی استان‌های مرزی:
تمرکز جنگ شبکه ای مخالفان نظام بر گستره افزایی آفندهای شیعه هراسی، مبین برنامه ریزی هدفمند تهاجم نرم برای تضعیف زیر ساخت‌های استان‌های مرزی جمهوری اسلامی ایران است که برخورداری اکثر این استان ها از موزاییک‌های قومی باعث می شود در صورت نبود بسته سیاسی منسجم، بستر شکل گیری برخی

تنش‌های فرقه ای در سر حدات و شهرهای مرزی فراهم گردد و هزینه‌های انتظام بخشی کلان کشور در برنامه پنجم توسعه، افزایش یابد. برخی شیوه ها و اهداف ایران هراسی و شیعه هراسی در ساختار تهاجم شبکه ای عبارت اند از:

*بهره گیری از بار منفی واژه ها، کلمات و مفاهیم حساسیت برانگیز در افکار عمومی (مانند نسبت دادن بنیاد گرایی به الگوی حکومتی جمهوری اسلامی ایران یا کاربرد مکرر کلمه ناکارآمدی ساختارها و کارگزاران نظام در وب سایت خبر گزاری‌های بین المللی)؛

*انعکاس چهره مخدوشی از هویت ایرانی– اسلامی (مانند نمایش فیلم فتنه در محیط‌های سایبر که گرت ویلدرس، نماینده مجلس و رهبر حزب ضد مهاجرت هلند،آن را ساخته است)، تداعی تصاویر خشنی از اهداف،ماهیت و دورنمای انقلاب اسلامی ایران؛

*انگاره سازی‌های هدفمند (تداعی شکلی و قرار دادن تصاویر کارگزاران نظام در کنار تصاویر افراد غیر محبوب در محیط‌های وب) (افتخاری، ۱۳۸۲ :۱۴).

محیط سایبر و بایسته های مدیریت پیشگیرانه پلیس کشور

به منظور حداکثر بهره‌گیری و هم افزایی بهینه ظرفیت‌های نظام برای مقابله با آفندهای تهاجم شبکه ای، متولیان امردر سطح نیروی انتظامی می‌توانند بااتخاذ تدابیر و ایجاد نهادهای امنیتی لازم به ارتقای امنیت فضای مجازی کشور کمک کنند. از طرفی در شرایطی که تهاجم نرم همسو با تهدیدهای نیمه سخت (گسترش احتمالی دامنه تحریم ها)به یکی از اولویت های دیپلماسی خصمانه مخالفان نظام جمهوری اسلامی ایران تبدیل شده، در نتیجه بر اهمیت تبیین پاداستراتژی[1] منسجم برای مهار آسیب های تهاجم سایبر افزوده شده است. مهم ترین تدابیری که می تواند ظرفیت

1- ipod strategy

مدیریت پیشگیرانه پلیس کشور را برای مقابله با جرایم انتظامی – امنیتی در فضای سایبر ارتقا دهد عبارت اند از:

*** بهره گیری از تجربیات سایر کشورها متناسب با شرایط بومی کشور:**

اهمیت مدیریت نرم افزاری فضای سایبر در ساختار انتظامی – امنیتی کلان سایر کشورهای توسعه یافته به حدی است که کشورهایی مانند ایالات متحده آمریکا، انگلیس و فرانسه که صاحب بسیاری از سرورهای محیط وب هستند، نظام مند کردن فضای سایبر را به عنوان یکی از اولویت‌های امنیت ملی خود تعریف کرده و برای سامان دهی چارچوب فعالیت کاربران در شبکه مجازی با تصویب قوه مسئول، قوانین متعددی را وضع کرده اند که مطالعه تطبیقی و بهره گیری از تجربیات آنان متناسب با شرایط بومی کشور، نه تنها می تواند ضرایب انتظام بخشی در سه سطح کلان شهری، استانی و ملی را ارتقا دهد بلکه موجب کاهش محسوس هزینه های مدیریت خرد و کلان پلیس کشور در سند چشم انداز شده و در عین حال باعث افزایش وحدت و امنیت اجتماعی در سطح جامعه می شود. به ویژه اینکه توسعه جهانی فناوری اطلاعات و ارتباطات و قرار گرفتن کشورها در دهکده ای جهانی بر اهمیت مهندسی انتظامی – امنیتی محیط های شبکه ای افزوده و ارتباط تنگاتنگی را با ضرایب اقتدار سنجی نظام به وجود آورده است.

جمهوری اسلامی ایران با بهره گیری از تجربیات سایر کشورها متناسب با شرایط بومی کشور نقش مهمی را در ارتقای امنیت فضای مجازی ایفا می کند.

***تدوین بسته سیاستی منسجم برای مقابله با آفندهای تهاجم شبکه ای:**

یکی از تهدیدهای امنیت ملی در برنامه پنجم، وجود برخی خلأهای تقنینی – نظارتی یا عدم حسن اجرای مناسب قوانین مصوب برای مقابله با جرایم امنیت ملی در فضای مجازی است؛ زیرا محیط های وب (اینترنت و پست های الکترونیکی)، مجازی (پیام های کوتاه تلفن همراه و بلوتوث) و رسانه ای (شبکه های ماهواره ای)

به دلیل ارتباط تنگاتنگ با اقشار مختلف جامعه از ظرفیت های قابل توجهی برای اثرگذاری و مدیریت رفتار جامعه برخوردارند و در صورت نبود پاداستراتژی منسجم می توانند ثبات امنیت اجتماعی را به چالش بکشانند. برخی راه کارهای کلان از سوی دولت و در حمایت از نیروی انتظامی در جهت به فعلیت رساندن راهکارهای ذکر شده عبارت‌اند از:

۱- ایجاد شبکه اینترنت ملی (اینترانت):

در بند ((۳-۴۴)) سیاست های کلی برنامه پنجم توسعه بر ایجاد سامانه یکپارچه نرم افزاری – اطلاعاتی، ارتقای سطح حفاظت از اطلاعات رایانه ای، توسعه علوم و فناوری های مرتبط با حفظ امنیت سامانه های اطلاعاتی و ارتباطی به منظور صیانت از فضای تبادل اطلاعات و مقابله با تخلفات رایانه ای تأکید شده که تحقق آن مستلزم شناسایی و آسیب شناسی تهدیدها در فضای سایبر است.اکثر سرورهای شبکه اینترنت در اختیار و کنترل ایالات متحده آمریکاست که در صورت تحریم رسانه ای، احتمال دارد تداوم خدمات رسانی[1] متوقف و نظام بانکی و اقتصادی مختل شود، به عبارتی با توجه به مبهم بودن عمق، دامنه و نوع تحریم ها و همچنین فقدان ایمنی کامل شبکه فیبر نوری[2]، توصیه می شود، ایجاد اینترنت ملی (اینترانت)، تنوع سازی ارتباط با شبکه جهانی اینترنت مانند ارتباط ماهواره ای و سیستم عامل ملی و نرم افزاهای کاربردی[3] 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 تمام ورودی های اینترنت را قطع کرد، بتوان سایت های داخل را با حداقل مشکل مدیریت کرد. از

1- Social Capita
2- Jean Jacobs
3- Reciprocity Trust

دوازده سرور موجود در محیط های وب، یازده سرور در آمریکا و یک سرور در کاناداست.

یکی از مجاری ارتباط جمهوری اسلامی ایران با شبکه جهانی اینترنت،اتصال با شبکه زیر ساخت دیگر کشورها به ویژه امارات و کویت است ولی در مقاطع زمانی به وسیله وقوع حوادث عمدی یا سهوی مانند برخورد لنگر کشتی ها به فیبر نوری ایران در فجیره امارات،اخلال‌هایی برای کاربران ایجاد شده است.

۲-تقویت ضریب ایمنی داده های راهبردی:

در حال حاضر وضعیت امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه دستگاه های دولتی در سطح نامطلوبی قرار دارد که از دلایل آن می توان به فقدان زیر ساخت های فنی و اجرایی برای ایمن سازی فضای تبادل اطلاعات و فقدان نظام تحلیل و مدیریت مخاطرات امنیتی در محیط سایبر اشاره کرد: بنابراین هم زمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات، توجه به مقوله ایمن سازی فضای سایبر و مدیریت امنیت نظام اطلاعات[1] به ویژه در ساختارهای راهبردی نظام از نیازهای حیاتی برنامه پنجم توسعه است.

همچنین یکی از اهداف اصلی جنگ های سایبر، بهره گیری از بمب‌های الکترومغناطیس[2] و نفوذ هکرها برای مختل سازی شبکه نرم افزاری داده‌های راهبردی بوده که توصیه می شود با کاربست فناوری های نوین و با میکروفیلم‌های پشتیبان، ضریب ایمنی داده های راهبردی را افزایش داد. از طرفی هر چقدر جمهوری اسلامی ایران بتواند با بهره وری مناسب از فنون جنگ اطلاعاتی، قدرت تمیز و چشم الکترونیک نیروهای مهاجم را مختل کند، ضریب آسیب پذیری بانک‌های اطلاعاتی کاهش می یابد که موفقیت آن مستلزم توسعه تعامل ساختارهای عملیاتی و مراکز تحقیقات هوا – فضا می‌باشد.

1- Information security management system(ISMS)
2- Electromagnetic Bomb

تصویب کنوانسیون جرایم رایانه ای و گزارش توجیهی آن در نوامبر ۲۰۰۱ و امضای آن از سوی سی کشور، تصویب قوانین مبارزه با این جرایم در قوانین داخلی و ایجاد واحدهای مبارزه با جرایم سایبر در ساختار پلیس این کشورها، تجهیز نیروهای پلیس به جدیدترین سخت افزارها و نرم افزارهای کشف این گونه جرائم و جذب و به کارگیری نیروهای متخصص برخی دیگر از مهم ترین اقدامات پیش روی پلیس کشور در فضای سایبر است (گنجی،۱۳۸۲ :۱۹).

۳- ایجاد زیر ساخت های تقنینی مناسب به منظور حمایت و صیانت از حقوق شهروندی:

مجریان تهاجم سایبر، عمق راهبردی اقتدار ملی را هدف قرار می دهند که به معنای مدیریت آفندهایی است که بتواند پشتیبانی حداکثری و تضمین شده مردم، کشورها و مجامع بین‌المللی را از سیاست‌ها و برنامه‌های دولت تضعیف کند. به همین منظور در برنامه پنجم توسعه باید به تدابیری توجه شود که به اقتدارافزایی ساختارهای حاکمیتی کمک می‌کند.

یکی از تدابیر پیش دستانه جمهوری اسلامی ایران برای مقابله مؤثر با تهاجم شبکه ای، تضعیف پیش زمینه های اثر بخشی سایبر است و از مهم ترین موارد آن می توان به حمایت نهادهای تقنینی و نظارتی در راستای رفع خلأهای قانونی برای حمایت و صیانت از حقوق اساسی ملت اشاره کرد که می تواند در دو حوزه زیر پیگیری شود:

الف) کاربست سازوکارها، تدابیر، اقدام ها و زیر ساخت های تقنینی – نظارتی لازم برای تسهیل و تسریع زیر ساخت های شبکه ای متناسب با حجم تهدیدهای سایبر در برنامه پنجم توسعه؛

ب) کاربست مؤثر سازوکارهای تقنینی – نظارتی برای صیانت از حقوق شهروندی و تحقق نظام مردم سالاری دینی در چارچوب قانون اساسی.

۴- توسعه زیر ساخت های مهندسی انتظامی– امنیتی دیجیتال:

استفاده از ابزارهای فناوری اطلاعات و ارتباطات برای تبیین، گسترش و ارتقای نظام امنیت اجتماعی با بهره گیری از فضای مجازی را مهندسی انتظامی سایبر می گویند که در واقع بخشی از فرآیند توسعه ضرایب انتظام بخش کشور است و تأثیر مثبتی بر امنیت افزایی ایفا می کند که منظور از آن، کاربست مناسب روش های پلیسی در فضای مجازی و شبکه اطلاع رسانی آنلاین به جامعه با مناسب ترین شیوه، کمترین هزینه و بالاترین کیفیت در حداقل زمان است که بتواند بستر تعامل پویا میان مردم، شبکه نخبگان و پلیس کشور را فراهم کند.

۵- ایجاد پلیس سایبر برای شناسایی و پیگرد مجرمان در فضای مجازی:

یکی از کاستی های پلیس کشور برای مقابله مؤثر با جرایم امنیت ملی در فضای سایبر، وجود سیاست های جزیره ای در حوزه مدیریت پیشگیرانه امنیت نرم است. در این راستا رفع خلأهای تقنینی، نظارتی و اجرایی- شکل گیری پلیس سایبر- در ساختار انتظامی کشور، نقش مهمی را در نظام مند کردن، اثر بخشی‌گسترش سیاست‌های پلیس کشور ایفا می کند.

سهولت فعالیت در فضای سایبر و نبود محدودیت دنیای واقعی در آن باعث شده تا جرایم ارتکابی انسان ها گسترده تر، پیچیده تر، سریع تر و کم هزینه تر شود. از این رو فضای مجازی، بستهٔ سیاستی خاص خود را می طلبد تا در قالب آن، تعقیب و دستگیری مجرمان در فضای مجازی صورت گیرد. لازمه این امر رفع خلأهای تقنینی – نظارتی، تربیت افراد متخصص، داشتن ابزارهای پیشرفته عملیات در فضای سایبر و همکاری مردم است. آمریکا، فرانسه، چین، هند و ژاپن از جمله کشورهایی هستند که در زمینه پلیس سایبر فعالیت می کنند. پلیس سایبر، وب یا شبکه، در حوزه مقابله پیشگیرانه با جرایم فضای سایبر، از قبیل نفوذ غیر مجازی خرابکاری اطلاعات و کلاهبرداری اینترنتی فعالیت می‌کند.

در معاونت آگاهی نیروی انتظامی ایران نیز بخشی برای مبارزه با جرایم رایانه ای ایجاد شده است. پلیس سایبر بخشی از توسعه فناوری اطلاعات در کشور است. با توجه به این نکته که نیروی انتظامی مسئولیت برقراری نظم در جامعه را دارد، گسترش وتوسعه پلیس سایبر می تواند نقش مهمی در تهدیدهای امنیت اجتماعی در فضای مجازی ایفا کند.

۶-بهره گیری مؤثر از ظرفیت فناوری های نوین، در ساختار مدیریت بحران های امنیت اجتماعی:

یکی از روش‌های توسعه انتظامی مطلوب، در سند چشم انداز، بهره‌گیری بهینه پلیس کشور، از ظرفیت فناوری شبکه سایبر است به طوری که یکی از ابزارهای ارتقای مهندسی امنیتی، کاربست فناوری های 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 فناوری های نوین، هوشمند و نظام های اطلاعاتی در توسعه سامانه های دفاعی به ویژه سامانه های الکترونیکی، هوا – فضا، دریایی و پدافند هوایی تأکید شده است. از مهم ترین مصادیق آن می‌توان به گسترش کاربست فناوری بیومتریک در توسعه نظام جامع امنیت مرزی، تشکیل بانک اطلاعات مجرمان، صدور گذرنامه‌های بیومتریکی و پیشگیری از آسیب‌های اجتماعی مجرمان سابقه دار اشاره کرد. مشخصات و کاراکترهای بیومتریکی عموماً به دو دسته بیولوژیکی و رفتاری[1] تفسیر می شوند.

-شاخص های بیومتریک بیولوژیکی مانند: اثر انگشت[2]، هندسه دست و کف دست[3]، اسکن شبکیه و عنبیه[4]، تحلیل دی.ان.ای[5] و شناسایی چهره؛

1- Physiological &Behavioral
2- Finger Print
3- Hand&Plam Geometry
4- Iris&Retina Recognition Iris&Retina Recognition
5- Deoxyribonucleic Acid(DNA)

-شاخص های بیومتریک رفتاری مانند: امضانگری، تایپ نگاری[1]، صورت نگاری، نحوه راه رفتن، بوی بدن، چهره نگاری سه بعدی، چهره نگاری حرارتی، شکل گوش، عروق لاله گوش، دستخط، اندازه گیری جمجمه، بافت پوست و بازتابش نور از آن و نحوه گرفتن اشیا با دست.

سهولت کاربرد، سرعت عملکرد، صحت عملکرد، هزینه کم، میزان پذیرش بالای کاربری، سطح امنیتی بالا، دوام و پایداری بالا، از مهم ترین فرصت های توسعه کاربست دانش بیومتریک در ساختار امنیتی- نظامی و انتظامی است.

به عنوان مثال، مهم ترین کاربردهای نهادینه سازی دانش بیومتریک در ساختار انتظامی – امنیتی برنامه پنجم، عبارت اند از:

-امنیت دسترسی فیزیکی (ارتقای ضریب امنیت دسترسی به محیط های راهبردی)؛

-امنیت فضای سایبر (ارتقای ضریب امنیت دسترسی به اطلاعات شبکه های نهادهای راهبردی نظام).

-امنیت نظام مالی و پولی (ارتقای ایمنی امنیت تراکنش های مالی و اعتباری).

-افزایش اهمیت کارت های هوشمند.

-رأی گیری الکترونیکی.

-کنترل و نظارت دقیق تر رفت و آمد مسافران در مبادی ورودی و خروجی کشور.

-صدور گذرنامه ها و شناسنامه های بیومتریکی؛ یکی از ابزارهای اتحادیه اروپا برای کنترل مهاجرت و پیشگیری از وقوع حوادث تروریستی است. ۲۷ کشور اروپایی، به صدور گذرنامه های بیومتریکی و حک یک تراشه الکترونیکی در یکی از صفحات گذرنامه که در آن تمام اطلاعات صاحب گذرنامه ذخیره شده، ملزم شده‌اند.

-تقویت نظارت نامحسوس در اماکن عمومی.

1-Typing Rhythm

- تشکیل بانک اطلاعاتی مجرمان و نظارت دقیق تر بر زندانیان آزاد شده، بزهکاران و یا مجرمان سابقه دار.
- توسعه ضریب امنیت مرزی.
- تأیید سریع هویت و آمارگیری دقیق از بازماندگان، مجرمان و متوفیان در شرایط وقوع بحران های طبیعی، امنیتی و نظامی.

۷- تقویت رایزنی پلیس کشور با سایر ساختارهای مرتبط با مدیریت امنیت فضای مجازی:

مدیریت انتظامی فضای شبکه- به عنوان یک موضوع فرابخشی- مستلزم هم اندیشی، همکاری و هم افزایی ظرفیت نهادهای متعدد بوده و لازم است پلیس کشور برنامه ریزی منسجمی را برای نحوه تعامل با سایر ساختارهای مرتبط تعریف کند. به عبارتی مدیریت انتظامی پیشگیرانه فضای وب نیازمند وجود راهبرد تصمیم گیری، میان ساختارهای حاکمیتی است و تصویب قوانین انتظامی صرف، به تنهایی برای ارتقای امنیت فضای سایبر کافی نیست.

اهمیت و جایگاه اصل یکپارچگی و همسوسازی سیاست‌گذاری‌ها در پیشگیری از وقوع تهدیدهای امنیت اجتماعی در فضای شبکه به حدی است که در کشور توسعه یافته‌ای مانند ایالات متحده آمریکا، بخشی با عنوان سازمان تأمین امنیت اجتماعی بنیان گذاشته شده و قسمتی از فعالیت خود را بر ارائه خدمات رفاهی و درمانی به سه طیف سال خوردگان، معلولان و بازماندگان بی‌سرپرست در فضای شبکه متمرکز کرده که نقش مهمی در ارتقای سطح رضایتمندی عمومی، پیشگیری از نارضایتی طیفی از اقشار جامعه و در نتیجه کاهش هزینه‌های انتظام بخشی کلان کشور ایفا می‌کند که این خود جلوه ای از مفهوم فرابخشی بودن مدیریت انتظامی و نقش تأثیر گذار سایر نهادها در فضای سایبر است.

۸- تدوین سند جامع امنیت شبکه در ساختار انتظامی کشور:

یکی از مؤلفه‌هایی که می تواند ضریب کارآمدی تدابیر پیشگیرانه برای مقابله با آفندهای نرم افزاری محیط سایبر را کاهش دهد وجود سیاست های جزیره ای در حوزه مهار تهدیدهای انتظامی – امنیتی در فضای شبکه است که در صورت نبود پاداستراتژی مناسب می تواند موجب پتانسیل شکل گیری بحران های اجتماعی شود. به عبارتی یکی از خلأهایی که چگونگی رفع آن باید در بازه های زمانی سند چشم انداز، مورد تأکید متولیان امر قرار گیرد، مهندسی نرم افزاری امنیت شبکه است که به مفهوم بررسی روش ها و ابزار واکسینه کردن نظام در برابر آفندهای ثبات امنیت ملی در محیط وب بوده و تحقق آن جز با تبیین منشور مدیریت راهبردی امنیت شبکه در ساختار ناجا میسر نیست.

۹- آسیب شناسی روابط عمومی ناجا، در ساختار مدیریت پیشگیرانه تهدیدهای امنیت ملی:

رسانه ها به دلیل اثرگذاری مستقیم در هنجارسازی و فرهنگ سازی، از ظرفیت بالایی برای پیشگری از وقوع بحران های اجتماعی برخوردارند. همچنین رسانه ها نقش مهمی را در نهادینه سازی فرهنگ خود کنترلی در جامعه و کاهش هزینه‌های انتظام بخشی ایفا می کنند؛ زیرا تقویت خود کنترلی، به ایجاد حالتی ثابت درون فرد، منجر می شود که طی آن بدون کاربست ابزار قهریه، به انجام درست وظایف و مسئولیت ها رهنمون می‌گردد(برزنویی،۱۳۸۶ :۱۵۳).

۱۰- تبیین طرح جامع حمایت شبکه ای ناجا از سرمایه های اجتماعی:

یکی از ریشه های شکل گیری تهدیدهای انتظامی، نبود نگاهی جامع، فرابخشی و راهبردی برای حراست از سرمایه های اجتماعی در ساختار امنیتی برنامه پنجم است. اصطلاح سرمایه اجتماعی[1] که تحت برخی شرایط قابل تبدیل به سرمایه اقتصادی

است، برای اولین بار در اثر کلاسیک جین جاکوب[۲]، به نام مرگ و زندگی در شهرهای بزرگ آمریکایی ۱۹۶۱ به کار رفت (اکبری،۱۳۸۳ :۲۳).

به‌طور خلاصه سرمایه اجتماعی، شبکه تعاملی در هم تنیده ای میان مردم، ساختارهای حاکمیتی و نهادهای مدنی است که زیربنای آن را اعتماد متقابل تشکیل می دهد و در نتیجه هر قدر ریشه های آن گسترده تر باشد به همان میزان ضریب وقوع بحران های اجتماعی کاهش می یابد؛ زیرا وجود اعتماد متقابل[۱] میان مسئولان و مردم، ضریب آستانه مقاومت ملی در برابر مؤلفه های بحران زا را افزایش می‌دهد.

تقویت نظارت همگانی ناجا در فضای سایبر، نقش مهمی در انسجام بخشی اعتماد جامعه به ساختار پلیس کشور ایفا می کند. به عبارتی حمایت های تقنینی، نظارتی و اجرایی در توسعه کمی و کیفی مرکز نظارت همگانی ناجا، نقش مهمی در پیشگیری از وقوع بحران‌های اجتماعی و پرهیز از نگاه تشریفاتی به این مرکز، که در سال ۱۳۷۹ تأسیس شد، ایفا می‌کند.

ارائه راهکارهایی برای مقابله با تهدیدهای سایبری

مدیریت نرم افزاری فضای شبکه، مستلزم ریشه یابی مؤلفه‌هایی است که می توانند پتانسیل ایجاد و گسترش نافرمانی مدنی یا وقوع آشوب‌های اجتماعی در سطوح خرد و کلان را فراهم کنند. به همین دلیل در این مقاله به مهم ترین چالش ها و راهکارهای فراروی مدیریت انتظامی مطلوب ناجا در فضای وب اشاره می‌شود (جمال زاده،۱۳۸۸ :۲۴).

1- Strength weakness opportunities&Threats(SWOT)

ردیف	چالش ها، موانع و کاستی ها	راهکارها
۱	– تبلیغ رسانه ای و سایبری سازمان‌های تروریستی فرقه ای (وابسته به وهابیت) در حلقه‌های پیرامونی جمهوری اسلامی ایران و افزایش ضریب احتمال شکل گیری تنش‌های اجتماعی در استان‌های مرزی به ویژه شهرهای برخوردار از موزاییک‌های قومی–فرقه ای؛ – برنامه ریزی هدفمند شبکه‌های وب مخالفان نظام جمهوری اسلامی ایران برای نفوذ، تبلیغ و ترویج برخی فرقه‌های الحادی مانند وهابیت، سلفی گری و بهائیت در استان‌های مرزی با رویکرد بستر سازی برای ایجاد و مدیریت آشوب‌های اجتماعی قومی –فرقه ای.	– توجه پلیس شبکه به رصد، شناسایی و خنثی سازی آفندهای تضعیف کننده وحدت ملی و تفرقه انداز میان شیعه و سنی؛ – مقابله با جریان‌های انحرافی و فرقه‌های الحادی در فضای مجازی؛ – لحاظ کردن تدابیر پیشگیرانه لازم برای توسعه زیر ساخت‌های امنیت شبکه در ساختار طرح جامع ارتقای ضرایب انتظامی استان‌های مرزی؛ – توسعه امنیت الکترونیک همسو با گسترش امنیت فیزیکی.
۲	–عدم بهره وری بهینه از ظرفیت فناوری‌های نوین در حوزه انسداد و نظارت بر امنیت مرزی.	– رفع خلأهای تقنینی، نظارتی و اجرایی توسعهٔ فناوری‌های نوین مانند فناوری بیومتریک در ساختار امنیتی ناجا با هدف انسداد، نظارت، کنترل دقیق سر حدات و همچنین تقویت نظارت بر ورود اتباع بیگانه.
۳	– نبود راهبردی منسجم برای حمایت زیربنایی ناجا از حقوق شهروندی در فضای سایبر.	– ایجاد ساز و کارهای مناسب برای تقویت نظارت همگانی بر فعالیت پلیس کشور در فضای وب با توجه با تأثیر بالای رضایتمندی عمومی در پیشگیری نرم افزاری وقوع بحران‌های اجتماعی؛ – توسعه برنامه‌های شبکه ای ناجا با رویکرد نهادینه سازی حمایت‌های مجازی پلیس کشور از چارچوب‌های حقوق شهروندی با رویکرد انسجام بخشی میان نیروی انتظامی و سرمایه‌های اجتماعی؛ – رفع خلأهای تقنینی– نظارتی برگزاری انتخابات رایانه ای؛

		– بهره گیری حداکثری از ظرفیت رسانه ای کشور برای آگاه سازی جامعه و متولیان ساختارهای انتظامی و امنیتی با مفاهیم حقوق شهروندی؛ – تعیین ساز و کارهای مناسب برای توازن بخشی میان سیاست‌های امنیتی ناجا و بنیان‌های حفاظت از حقوق اساسی جامعه مانند حقوق شهروندی.
۴	– نبود نقشه راهی منسجم برای نهادینه سازی زیرساخت‌های توسعه مهندسی انتظامی فضای سایبر در ساختار مدیریت پیشگیرانه تهدیدهای امنیت اجتماعی.	– نظارت بر حسن اجرای ابلاغیه مقام معظم رهبری راجع به سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه ای مورخ خرداد ۱۳۸۰ از سوی شورای انقلاب فرهنگی؛ – تدوین طرح اصلاح ساختار جامعه اطلاعاتی کشور (موضوع ماده (۱۲۴) قانون برنامه چهارم توسعه)؛ – حمایت‌های تقنینی – نظارتی از شکل گیری پلیس سایبر در ساختار انتظامی – امنیتی برنامه پنجم؛ – تبیین ساز و کارهای منسجم و بسترسازی مناسب برای تقویت فضای هم اندیشی ناجا با شبکه نخبگان در فضای وب؛ – الگوسازی امنیتی تهدیدها، فرصت ها، چالش ها و راهکارها در فضای سایبر، معروف به مدل خطی یا اسوات[1].
۵	– برنامه ریزی هدفمند شبکه‌های رسانه ای و مجازی مخالفان نظام جمهوری اسلامی ایران برای ایجاد و گسترش تهدیدهای امنیت اجتماعی در کلان شهرها. – نبود ساختار شبکه ای منسجم برای نظارت مؤثر بر اتباع بیگانه به ویژه افاغنه از رویکرد امنیت ملی و کلان شهری.	– تبیین طرح جامع امنیت شبکه ای کلان شهرها : * کنترل نامحسوس مجرمان سابقه دار؛ * تشکیل بانک جامع اطلاعات مجرمان سابقه دار؛ * توسعه اصول مهندسی انتظامی کلان شهرها در فضای وب؛ * بهره گیری بهینه از اطلاعات مردمی در فضای مجازی با رویکرد مدیریت پیش رویدادی آشوب‌های اجتماعی – منطقه ای؛ – سازمان دهی مجازی اتباع بیگانه در کلان شهرها

		و استان‌های مرزی؛ – تشکیل بانک جامع اطلاعات اتباع بیگانه؛ توسعهٔ سنسور اطلاعاتی گشت‌های پلیس اینترنتی با هدف کشف پیش دستانه جرایم رایانه ای؛ – رعایت ملزومات مهندسی امنیتی فضای سایبر در چارچوب طرح جامع ارتقای امنیت اجتماعی یا رفع خلأهای قانون جرائم رایانه ای؛ – ایجاد بانک اطلاعات مجرمان با هدف کنترل و نظارت مؤثر ناامنی‌های اجتماعی و نظارت دقیق تر بر بزهکاران و مجرمان سابقه دار.
۶	– در هم تنیدگی مؤلفه‌های مدیریت نرم افزاری فضای سایبر با متغیرهای امنیتی، سیاسی، فرهنگی، اقتصادی؛ – ضعف نگاه فرابخشی در حوزه ارتقای ایمنی و امنیت افزایی فضای سایبر، در سیاست‌های انتظامی کلان جمهوری اسلامی ایران.	– تبیین نظام جامع مدیریت نرم تهدیدهای امنیت اجتماعی با رویکرد حداکثر بهره وری بهینه از ظرفیت‌های نظام در فضای مجازی. – بهره گیری از فنون شبیه سازی رایانه ای برای پیشگیری از کاربست مدل آزمون و خطا در حوزه مدیریت بحران‌های امنیت اجتماعی.
۷	– نبود بسته سیاسی منسجم برای حداکثر بهره وری از ظرفیت بخش خصوصی در ساختار ایمن سازی و ارتقای امنیت فضای شبکه.	– تبیین منشور جامع فعالیت بخش خصوصی با رویکرد پیاده سازی اصل چهل و چهارم قانون اساسی، در ساختار مدیریت انتظامی کلان کشور (این رویکرد نقش مهمی در سرشکن کردن هزینه‌های مدیریت تهدیدهای امنیت اجتماعی و شکل گیری چارچوب‌های مدیریت مشارکتی ایفا می کند).
۸	– نبود سیاستی منسجم برای مقابله با پیش زمینه‌های وقوع آشوب‌های اجتماعی در فضای مجازی؛ – فقدان توسعه زیر ساخت‌های شبکه ای ناجا متناسب با نوع، جنس و حجم تهدیدها در محیط سایبر و در نتیجه آن کاهش توان نظارتی پلیس کشور برای پیشگیری یا مهار تهدیدهای نرم افزاری امنیت اجتماعی؛	– تدوین یا بازتولید نظام جامع فیلترینگ متناسب با آسیب‌های امنیت اجتماعی کشور؛ – آسیب شناسی گسترش وبلاگ‌های مخرب و تأثیر آن بر ضرایب امنیت عمومی، روانی و اخلاقی؛ – باز اندیشی دوره ای قانون مبارزه با جرایم رایانه‌ای به دلیل تنوع روزافزون ابزار و روش‌های مخرب و گستردگی فضایی روزافزون محیط‌های

	– گسترش پورنوگرافی (هرزه نگاری) در محیط سایبر، افزایش توزیع، نشر، خرید و فروش تصاویر، صوت ها یا متن‌های مستهجن و به دنبال آن تهدید امنیت اخلاقی در جوانان.	مجازی؛ – ریشه یابی و خنثی سازی آفندهای امنیت اجتماعی در محیط‌های شبکه ای؛ – توسعه گشت‌های اینترنتی پلیس کشور در فضای سایبر.
۹	– تمرکز بخشی از جنگ تبلیغاتی غرب برای تخریب وجهه ناجا در جایگاه افکار عمومی مانند شائبه سازی مبنی بر حمایت نیروی انتظامی از جریان سیاسی خاص در زمان رقابت‌های انتخاباتی با هدف بی اعتمادسازی بخشی از جامعه به پلیس کشور.	– ریشه یابی آسیب شناسی و خنثی سازی شایعه‌های مخرب در شبکه مجازی با رویکرد مدیریت رسانه ای تهدیدهای امنیت اجتماعی.
۱۰	– نبود بسته سیاستی منسجم برای بهره گیری حداکثری از ظرفیت رسانه ها در مدیریت امنیت اجتماعی؛ – تهاجم نرم افزاری غرب برای تهدید باورهای دینی، ارزش‌های حیاتی و الگوهای رفتاری در سه سطح دولتمردان، جامعه و نیروهای مسلح؛ – حمایت‌های تقنینی اتحادیه اروپا و آمریکا از گسترش رسانه‌های صوتی – تصویری ضد انقلاب با رویکرد گسترش نافرمانی مدنی، بحران سازی اجتماعی، مشروعیت زدایی از ساختارهای حکومتی و مخدوش جلوه دادن میزان مشارکت و نتایج آرای انتخاباتی.	– آگاه سازی جامعه با ابزار و شیوه‌های جنگ تبلیغاتی روانی غرب؛ – آسیب شناسی گسترش رسانه‌های صوتی – تصویری ضد انقلاب؛ – رصد تحرکات عوامل ضد انقلاب در فضای رسانه ای و سایبر. – حمایت‌های تقنینی – نظارتی مجلس شورای اسلامی برای مقابله با آفندهای جنگ روانی کنگره آمریکا.
۱۱	– عدم بهره گیری مناسب از ظرفیت‌های روابط عمومی ناجا در ساختار انتظام بخشی کشور.	– آسیب شناسی رسانه ای جمهوری اسلامی ایران در قالب مدیریت پیشگیرانه تهدیدهای امنیت اجتماعی؛ –آگاه سازی جامعه نسبت به آسیب‌های اجتماعی ازدواج رایانه ای.

جمع بندی و نتیجه‌گیری

وضعیت امنیت فضای تبادل اطلاعات کشور به ویژه در حوزه دستگاه‌های دولتی نیاز به تقویت دارد که از دلایل آن می‌توان به فقدان زیر ساخت‌های فنی و اجرایی برای ایمن سازی فضای تبادل اطلاعات و فقدان نظام تحلیل و مدیریت مخاطرات امنیتی در محیط سایبر اشاره کرد؛ بنابراین هم زمان با تدوین سند راهبردی امنیت فضای تبادل اطلاعات، توجه به مقوله ایمن سازی فضای سایبر و مدیریت امنیت نظام اطلاعات به ویژه در ساختارهای راهبردی 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 نرم افزاری داده‌های راهبردی بوده که توصیه می شود با کاربست فناوری‌های نوین و با نسخه های پشتیبان، ضریب ایمنی داده‌های راهبردی را افزایش دهیم.

مجریان تهاجم سایبر عمق راهبردی اقتدار ملی را هدف قرار می دهند که به معنای مدیریت آفندهایی است که بتواند پشتیبانی حداکثری و تضمین شده مردم، کشورها و مجامع بین المللی را از سیاست ها و برنامه‌های دولت تضعیف کند. به همین منظور در برنامه پنجم توسعه باید به تدابیری توجه شود که به اقتدارافزایی ساختارهای حاکمیتی کمک می کند.

یکی از تدابیر پیش دستانه جمهوری اسلامی ایران برای مقابله مؤثر با تهاجم شبکه ای، تضعیف پیش زمینه‌های اثر بخشی سایبر است و از مهم ترین موارد آن می توان به حمایت نهادهای تقنینی و نظارتی در راستای رفع خلأهای قانونی برای حمایت و صیانت از حقوق اساسی ملت اشاره کرد که می تواند در دو حوزه زیر پیگیری شود:

الف) کاربست سازوکارها، تدابیر، اقدام ها و زیر ساخت‌های تقنینی – نظارتی لازم برای تسهیل و تسریع زیر ساخت‌های شبکه ای متناسب با حجم تهدیدهای سایبر در برنامه پنجم توسعه؛

ب) کاربست مؤثر سازوکارهای تقنینی – نظارتی برای صیانت از حقوق شهروندی و تحقق نظام مردم سالاری دینی در چارچوب قانون اساسی.

در حوزه عملیاتی باتجهیز نیروهای پلیس، به جدیدترین سخت افزارها و نرم افزارها- برای کشف جرایم- همچنین جذب و به کارگیری نیروهای متخصص، می‌توان ازتهدیدهای امنیتی جلوگیری به عمل آورد. یکی از کاستی‌های پلیس کشور برای مقابله مؤثر با جرایم امنیت ملی در فضای سایبر وجود سیاست های جزیره ای در حوزه مدیریت پیشگیرانه امنیت نرم است. در این راستا رفع خلأهای تقنینی، نظارتی و اجرایی شکل گیری پلیس سایبر در ساختار انتظامی کشور نقش مهمی را در نظام مند کردن، اثر بخشی وگسترش سیاست های پلیس کشور ایفا می‌کند.

منابع و مآخذ

منابع فارسی:

۱- افتخاری، اصغر(۱۳۸۲)، **استراتژی ملی برای تامین امنیت در فضای مجازی**، تهران: پژوهشکده مطالعات راهبردی.

۲-اکبری، امین(۱۳۸۳)، **نقش سرمایه اجتماعی در مشارکت،بررسی تاثیر سرمایه اجتماعی بر مشارکت سیاسی و اجتماعی**، پایان‌نامه کارشناسی ارشد،تهران:دانشگاه علوم اجتماعی.

۳-برزنویی،محمد علی(۱۳۸۶).**مجموعه مقالات دومین همایش علمی تخصصی ناجا و نظارت همگانی**،(نظارت همگانی از منظر اسلام)،تهران.

۴-بوزان،باری (۱۳۷۸). **مردم،دولتها و هراس**. تهران: پژوهشکده مطالعات راهبردی.

۵-پای،لوسین(۱۳۸۵).**بحران‌ها و توالی‌ها در توسعه سیاسی**،ترجمه غلامرضا خواجه سروی،تهران:پژوهشکده مطالعات راهبردی.

۶-تاجیک، محمدرضا (۱۳۸۶). **قدرت و امنیت در عصر پسامدرنیسم**. گفتمان، شماره صفر.

۷-جمال زاده، ناصر(۱۳۸۹)، **ناجا و توسعه امنیت نرم**، تهران: مجلس شورای اسلامی.

۸-رابرت، ماندل (۱۳۸۷). **چهره متغیر امنیت ملی**. تهران: پژوهشکده مطالعات راهبردی.

۹-رنجبر، مقصود(۱۳۸۴). **ملاحظات امنیتی در سیاست خارجی جمهوری اسلامی ایران**. تهران: پژوهشکده مطالعات راهبردی.

۱۰-سیف زاده،سید حسین(۱۳۸۶).**نوسازی و دگرگونی جامعه**،تهران: سفیر.

۱۱-گراه،جعفری(۱۳۸۶)، **جنگ شبکه ای متركز**،ترجمه محمود فیروزی،فصلنامه مطالعات بسیج،سال دهم،شماره۳۴.

۱۲-گنجی،علیرضا(۱۳۸۲)، **امنیت شبکه:چالش ها و راهکارها**،مجله علوم اطلاع رسانی،دوره ۱۸،شماره ۳و۴.

۱۳-محسنیان‌راد، مهدی (۱۳۸۷)، **ارتباط جمعی در کشورهای اسلامی**. دانشگاه امام صادق، انتشار محدود.

۱۴-محسنیان‌راد، مهدی(۱۳۸۸). **انتقاد در مطبوعات ایران**. مرکز مطالعات و تحقیقات رسانه‌ها، انتشار محدود.

۱۵-محمدی، مجید (۱۳۸۹)، **سیمای اقتدارگرایی تلویزیون دولتی ایران**. تهران: جامعه ایرانیان.

۱۶-مولانا، حمید (۱۳۸۹)، **جریان بین‌المللی اطلاعات**. ترجمهٔ یونس شکرخواه. تهران: مرکز مطالعات و تحقیقات رسانه‌ها.

منابع لاتین:

17-Checkwick،william p.(2009).firewalls and internet security،washington،mips computer corporation.
18-Jim،miklaszewski(2011).the pentagon has been warning about a future war،washington D.C.
19-Libicki،martin c.(2009).conquest in cyberspace(2009)،the rand corporation،cambridge university press.
20-Milstein،sarah (2010).the twitter book،oreilly publications.
21-Westly،jody R.(2010).International Guide to Cyber security،American Bar Association privacy&computer Crime committee section of Science&technology.