چالش‌ها و چشم‌اندازهای امنیت در فضای مجازی

مهدی هاتف*

چکیده

از ابتدای زندگی بشر امنیت یکی از دغدغه‌های اصلی انسان‌ها بوده است، امروزه با گسترش اینترنت و فضاهای شبکه‌ای در کشورمان لزوم امنیت برای فعالیت در این فضاهای مجازی بیش از پیش احساس می‌شود. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، و نداشتن امنیت روانی و فرهنگی ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت و فضاهای مجازی واکنشی منطقی است، زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد. طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند، می‌تواند سلامت و امنیت جامعه را به خطر اندازد. برخلاف وجود جنبه‌های مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد هنجارشکن، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو به‌کارگیری روش‌ها و راه کارهای مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه جهانی اینترنت و فضاهای سایبر را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است.

در این مقاله ابتدا با عناوینی چون امنیت در فضای سایبر و جرائم رایانه‌ای و انواع آن آشنا می‌شویم، سپس به انواع فناوری‌های اطلاعات به طور کلی پرداخته و نمونه‌هایی از آن را ارائه نموده، در نهایت به آسیب شناسی فضای امنیت و اطلاعات در کشور می‌پردازیم و چالش‌ها و راه‌کارهای مقابله با این چالش‌ها را مرور می‌نماییم.

کلید واژه‌ها:

امنیت شبکه، جرائم رایانه‌ای، فناوری‌های امنیت اطلاعات

*. کارشناس دفتر تحقیقات کاربردی مع ط.ب.ب ناجا

مقدمه

مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دست‌یابی سریع و آسان به اطلاعات است. کنترل دست‌یابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای (خصوصاً اینترنت)، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی گردیده است.

در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند خود، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را اجرا نماید. نبود نظام مناسب امنیتی، بعضاً پیامدهای منفی و دور از انتظاری را به دنبال دارد. توفیق در ایمن‌سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس‌های امنیتی متعددی استفاده می‌گردد. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به موقع حملات، و واکنش سریع را داشته باشند. بنابراین می‌توان محور راهبردی انتخاب شده را بر سه مؤلفه حفاظت، تشخیص، و واکنش استوار نمود. حفاظت مطمئن، تشخیص به موقع و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت شود.

مقاله حاضر با توجه به این رویکرد به طبقه‌بندی فناوری‌های امنیت اطلاعات، براساس دو ویژگی خواهد پرداخت؛ اول مرحله خاصی از زمان که در هنگام تعامل فناوری با اطلاعات، عکس‌العمل لازم در برابر یک مشکل امنیتی، ممکن است به صورت کنشی یا واکنشی باشد، و دوم سطوح پیاده‌سازی نظام‌های امنیتی در یک محیط رایانه‌ای.

اهمیت و ضرورت امنیت در فضای مجازی

امنیت مجازی شاید به شکل قابل توجه آن، موضوع حیاتی برای کشورها باشد. چرا که شرط لازم برای تهدیدپذیری از دنیای مجازی، استفاده گسترده و اتصال به شبکه‌های الکترونیکی اطلاعات است و شرط کافی، دیجیتالی شدن تمامی سیستم‌ها و زیرساخت‌های اقتصادی، اجتماعی، سیاسی یک جامعه می‌باشد.

در عین حال نباید فراموش کرد که گسترش ارتباطات و انقلاب تکنولوژیکی، بسیاری از مسائل امنیتی را جهانی ساخته و شمال و جنوب در این زمینه دارای مسائل مشترکی هستند.

از طرفی دیگرتهدید، مفهومی نسبی و ذهنی است و درک آن به مؤلفه‌های گوناگونی بستگی دارد. تهدید در مفهوم گذشته دارای ویژگی‌های مشخصی بوده که می‌توان آن‌ها را این گونه برشمرد:

۱- عمدتاً با منشأ خارجی تصور می‌شد؛

۲- مبتنی بر قدرت نظامی بود؛

۳- متکی بر حضور فیزیکی دشمن بود؛

۴- آگاهی از تهدیدات، گسترده نبود؛

۵- دامنه تهدیدات محدود بود؛

۶- تهدیدات به راحتی قابل تشخیص بود؛

۷- در اکثر تهدیدات، دولت‌ها نقش مؤثری را ایفا می‌کردند .

اما در جهان امروز و در عصر جهانی شدن، به واسطه تغییرات تکنولوژی، مفاهیم نیز دستخوش تغییر و تحول شده‌اند. در شرایط نوین ویژگی تهدیدات به شرح زیر است:

- اکثر تهدیدات دولت محور نیستند. (این قبیل مخاطرات از عوامل و بازیگران ملی یا فرا ملی نشأت می‌گیرد.)
- این چالش‌ها، فضای جغرافیایی خاصی ندارند و تهدیدات متنوع، چندسویه و چندجهتی است و در سه سطح جهانی، منطقه‌ای و محلی قابل بررسی است.
- این تهدیدات را نمی‌توان تنها با اتکا به سیاست‌های دفاعی سنتی مدیریت کرد و مدیریت مؤثر مستلزم طیفی از رهیافت‌های غیرنظامی است.

مسلماً ترسیم یک گفتمان امنیتی خارج از مدار و حریم مفاهیمی چون قدرت، منافع، اهداف، مصالح، ارزش‌ها، تهدیدات و... دور از دسترس است.

به نظر می‌رسد لازم باشد در فضای مجازی این مفاهیم ابتدا مورد باز تعریف قرار گیرند و سپس به گفتمان امنیتی وابسته بدان پرداخته شود. اما در شرایطی که تمامی این مفاهیم خود بر ماهیت و شکلی دگرگون شونده و متلون اصرار می‌ورزند و بر مصداق‌های گوناگونی دلالت دارند این امر به راحتی امکان پذیر نیست.

اهداف تحقیق

- بررسی چالش‌های اساسی حوزه امنیت فضای مجازی؛
- شناخت مراکز دخیل و ذی نفوذ درحل مسائل حوزه امنیت فضای مجازی؛

- بررسی چشم انداز اولیه در صورت ادامه روند موجود؛
- بررسی چشم انداز مطلوب در حوزه امنیت مجازی؛

سؤالات تحقیق

- چالش‌های اساسی در امنیت فضای مجازی کدامند؟
- مراکز دخیل و ذی نفوذ در حل این مسائل کدامند؟
- چشم انداز اولیه در صورت ادامه روند موجود چه می‌باشد؟
- چشم انداز مطلوب در حوزه امنیت مجازی چیست؟
- اقدامات و راه حل‌ها چه می‌باشد؟

از این رو برای پاسخ به چنین سؤالاتی و جلوگیری از جرائم رایانه‌ای موجود و احتمالی در آینده ضروری است به بررسی امکانات و شرایط موجود، فرصت‌ها و تهدیدهای پیش رو پرداخته شود تا از این رهگذر به اقدامات و راه‌کارهای اساسی در زمینه فضای مجازی و سایبر دست یافت.

تعاریف واژگان

فضای سایبر[1]:

فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود.

امنیت سایبر[2]:

به امنیت فناوری اطلاعات، وابسته به سیاست دولت‌ها، امنیت سایبر می‌گوئیم. این اصطلاح عموماً توسط مؤسسه‌های دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با " امنیت اینترنت" است. هر دو عبارت به جوانب امنیت شبکه و اصول سیاستگذاری شبکه‌ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند.

---

1 .Cyberspace
2 .Cyber-Security

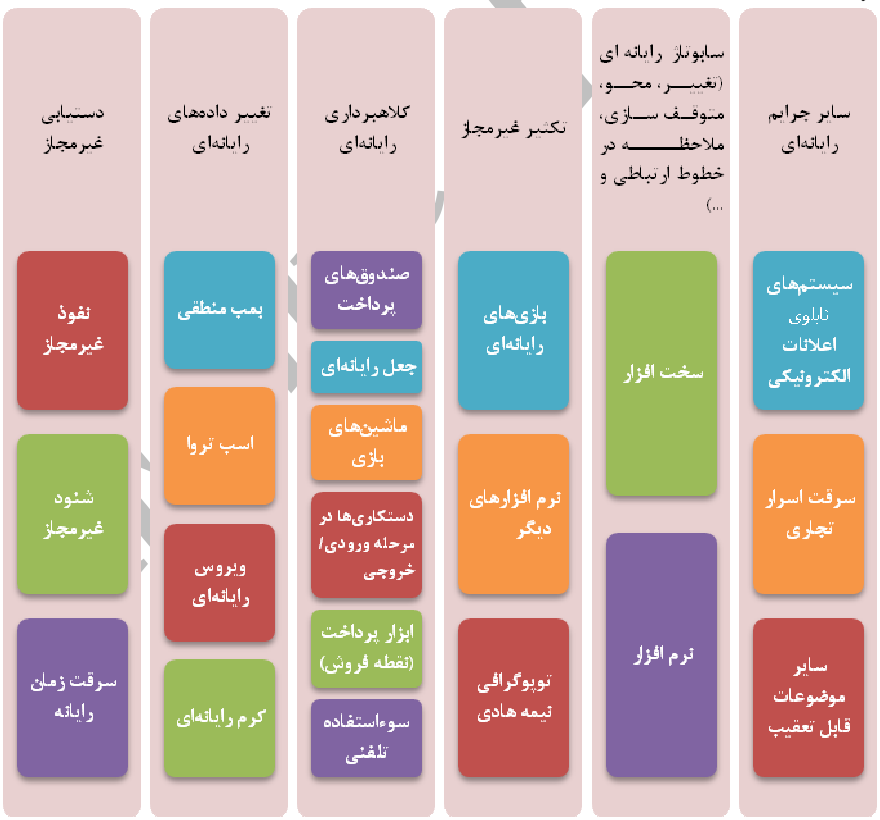
جرم رایانه‌ای :

جرم رایانه‌ای بر دو نوع است : در تعریف محدود (مضیق) جرمی که در فضای مجـازی (سایبر) رخ می‌دهد جرم رایانه‌ای است و بر اساس این دیـدگاه، اگـر رایانـه ابـزار و وسـیله ارتکاب جرم باشد آن جرم را نمی‌توان در زمره جرائم رایانه‌ای قلمداد کرد.

در تعریف گسترده (موسع) هر فعـل یـا تـرک فعلـی کـه « از طریـق»، یـا «بـه کمـک سیستم‌های رایانه‌ای» رخ می‌دهند جرم رایانه‌ای قلمداد می‌شود.

طبقه بندی جرائم رایانه ای:

سازمان پلیس جنایی بین المللی، جرائم رایانه‌ای را طبق نمونه‌ی ذیل طبقه بنـدی کرده است:



انواع متخلفین[1] (مجرمین اینترنتی):

روش‌های گوناگونی برای دسته‌بندی و بررسی مجرمین رایانه‌ای وجود دارد. این‌کار با یک دسته‌بندی ساده و معمولی تفاوت دارد. خیل فراوانی از متخلفان و جرائم رایانه‌ای پیش روی ما قرار دارند که از یک شوخی و تفریح شروع می‌شود و به فعالیت تروریستی بین‌المللی ختم می‌شود. روش‌های گوناگونی برای طبقه‌بندی مجرمین رایانه‌ای وجود دارد، ما آن‌ها را به سه دسته تقسیم می‌کنیم:

- نفوذکنندهٔ غیرمجاز؛
- مجرمین[2]؛
- خرابکاران[3]؛

این دسته‌بندی‌ها مقدار زیادی همپوشانی دارد. از منظری دیگر آن‌ها بر پایه انگیزه‌ها دسته‌بندی می‌شوند: انگیزهٔ اصلی نفوذ کنندهٔ غیرمجاز، دسترسی به سیستم یا داده‌هاست. انگیزهٔ اصلی مجرمین، دست‌یابی و انگیزهٔ اصلی خرابکاران، ایراد خسارت است. هر چند از مرتکبین هر سه گروه به عنوان مجرم نام‌برده می‌شود ولی طبقه‌بندی مجرمین بر دو رفتار اصلی مجرمانه متمرکز می‌شود: جاسوسی و کلاهبرداری.

اهداف در جرائم رایانه‌ای:

در عصر حاضر (خودکارسازی[4] و ارتباطات)، تقریباً هیچ سازمانی از جرائم رایانه‌ای مصون نیست. این بخش رایج‌ترین اهداف در جرائم رایانه‌ای را مورد توجه قرار می‌دهد:

- رایانه‌های نظامی و انتظامی ممکن است بوسیله سازمان‌های جاسوسی مورد هدف قرار گیرند.
- تاجرها ممکن است به‌وسیله رقبا مورد هدف قرار گیرند.

---

1. Offenders
2. Criminals
3. Vandals
4. Automation

- بانک‌ها و دیگر سازمان‌های مالی، ممکن است بوسیله جنایتکاران حرفه‌ای مورد هدف قرار گیرند.
- هر سازمان به ویژه دولت و رایانه‌های مربوط به شرکت‌های خدمات رسانی همگانی ممکن است به وسیله تروریست‌ها مورد هدف قرار گیرند.
- هر سازمان ممکن است به وسیله کارمندان ناراضی یا کارمندان اخراج شده خود مورد هدف قرار گیرند و در دانشگاه‌ها این اقدام توسط دانشجویان یا کسانی که قبلاً در آنجا کار می‌کردند انجام پذیرد.
- هر سازمانی ممکن است به وسیله رباینده‌گان مورد هدف قرار گیرد. در پاره‌ای از موارد مهاجمین برای مبارزات هوشمندانه‌تر این کار را انجام می‌دهند و در مواردی دیگر آن‌ها افراد ماهری هستند که برای ارضای خود این کار را انجام می‌دهند.

این بخش به انواع مختلف حملات رایانه‌ای از دستکاری حساب‌های بانکی و استراق سمع مکالمات گرفته تا برنامه‌ریزی جهت انجام هرگونه خرابکاری بوسیله ویروس‌ها می‌پردازد.

فناوری‌های امنیت اطلاعات

«امنیت اطلاعات»[1] به حفاظت از اطلاعات و به حداقل‌رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است. با توجه به تعاریف ارائه شده، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود. «**فن‌آوری**» به کاربرد علم، خصوصاً برای اهداف صنعتی و تجاری یا به دانش و روش‌های مورد استفاده برای تولید یک محصول گفته می‌شود.

---

1. Information Security

بنابراین «فناوری امنیت اطلاعات» به بهره‌گیری مناسب از تمام فناوری‌های امنیتی پیشرفته برای حفاظت از تمام اطلاعات احتمالی روی اینترنت اشاره دارد.

طبقه‌بندی (*INFOSEC*):

طبقه بندی ارائه شده در مقاله حاضر از فناوری‌های امنیت اطلاعات، در وهله اول براساس دو ویژگی پایه‌گذاری شده است:

براساس مرحله خاصی از زمان: بدین معنا که در زمان تعامل فناوری با اطلاعات، عکس‌العمل لازم در برابر یک مشکل امنیتی می‌تواند کنشگرایانه (کنشی)[1] یا واکنشی[2] باشد.

غرض از «کنشگرایانه»، انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می‌گردد که ما را در پیشگیری از وقوع یک مشکل کمک خواهد کرد (چه کار باید انجام دهیم تا ...؟).

غرض از «واکنشی» انجام عکس‌العمل لازم پس از وقوع یک مشکل خاص امنیتی است. در چنین مواردی به موضوعاتی اشاره می‌گردد که ما را در مقابله با یک مشکل پس از وقوع آن، کمک خواهند کرد (اکنون که ... چه کار باید انجام بدهیم؟).

براساس سطوح پیاده‌سازی نظام‌های امنیتی در یک محیط رایانه‌ای: فناوری امنیت اطلاعات را، خواه از نوع کنشی باشد یا واکنشی، می‌توان در سه سطح :

- سطح شبکه (*Network Level*)،
- سطح میزبان (*Host Level*)،
- سطح برنامه کاربردی (*Application Level*) پیاده‌سازی کرد.

بدین منظور می‌توان نظام امنیتی را در سطح شبکه و خدمات ارائه شده آن، در سطح برنامه کاربردی خاص، یا در محیطی که شرایط لازم برای اجرای یک برنامه را فراهم می‌نماید (سطح میزبان) پیاده کرد.

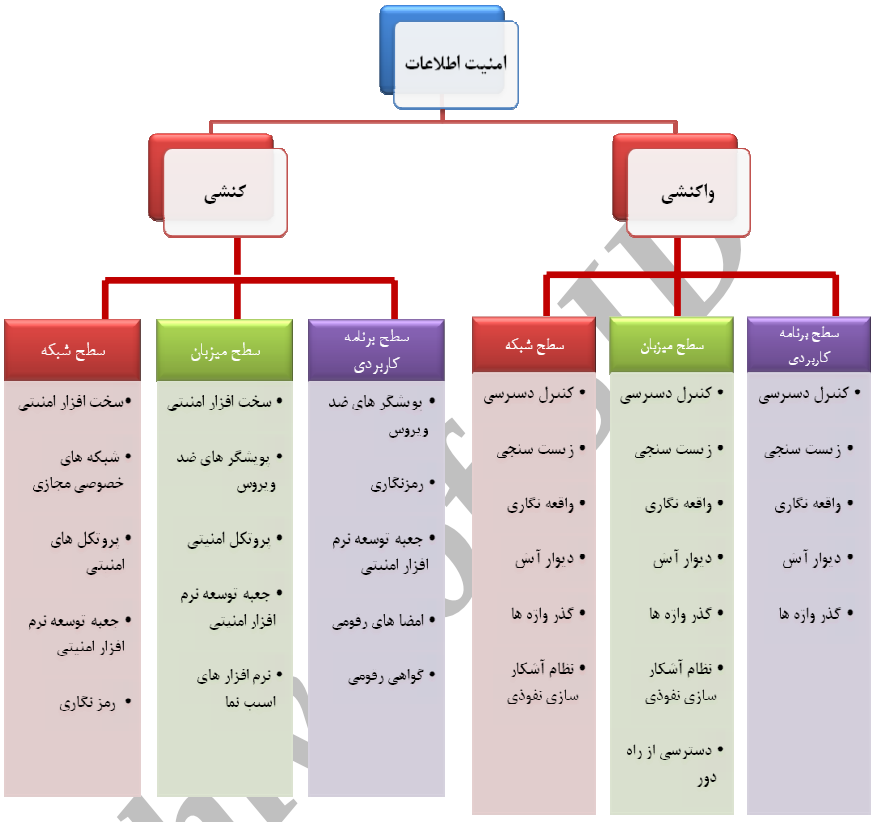
شکل شماره (۱)، شکل شماره (۲) و شکل شماره (۳) فناوری‌های امنیت اطلاعات را براساس دو ویژگی یاد شده ترسیم می‌نماید.

---

1. Proactive
2. Reactive

شکل شماره (۱): فناوری‌های امنیت اطلاعات کنش‌گرایانه

شکل شماره (۲): فناوری‌های امنیت اطلاعات واکنشی



شکل شماره (۳): فناوری‌های امنیت اطلاعات واکنشی و کنشی

آسیب شناسی و تأمین امنیت در فضای مجازی ایران

واژه‌هایی چون "تجارت الکترونیک"، "بانکداری الکترونیک"، "دولت الکترونیک" و از این دست، در حالی جسته و گریخته به گوش ما می‌خورند که سال‌هاست به صورت عملی و کاملاً طبیعی در بسیاری از کشورهای جهان در حال اجرا و بازدهی کلان هستند و علاوه بر برگشت سرمایه‌های هنگفت، موجب صرفه جویی‌های قابل توجه در منابع و ظرفیت‌های مختلف شده‌اند.

اما بسیاری از دولت‌ها و جوامع، خواسته و یا ناخواسته هنوز هم متوجه تغییر عظیمی که در مناسبات جهانی روی داده است نشده، و نپذیرفته‌اند که پیوستن آن‌ها به جمع جوامع اطلاعاتی پیشرفته، امتیازات بسیاری برای آن‌ها در پی خواهد داشت. علاوه بر این، حتی اگر اکنون درصد وسیعی از تعاملات تجاری، اداری و اجتماعی جهان به شکل الکترونیک انجام شده و سهم آن‌ها از این روند مطلوب و کارآمد، در حد صفر باشد و نیز اگر آمارهای معتبر و قابل استناد جهانی، آخرین رتبه‌های نفوذ روابط الکترونیک در میان جوامع را به آن‌ها اختصاص دهد، شاید باز هم کارآمدی فناوری اطلاعات را در فعالیت‌های کلان مدیریتی خود لحاظ نکنند.

متأسفانه، ادامه این روند و اصرار بر این نپذیرفتن، به کاهش محسوس بازدهی و افت قدرت تأثیرگذار این دولت‌ها و ملت‌ها در جامعه جهانی خواهد انجامید. چراکه تعاملات الکترونیکی و به طور خاص شکل کلان آن‌ها، بی گمان به روندی بی چون و چرا و غیر قابل اجتناب تبدیل خواهد شد.

به نظر می‌رسد که تلاش بسیاری از دولت‌ها برای کنترل دنیای الکترونیک، وجود مدیریت سنتی در ساختار اداری سیاسی و نیز عدم اعتنای توده مردم به روش‌های نوین تعامل با حکومت، از مهمترین دلایل عدم افزایش فعالیت‌های کلان الکترونیکی باشد.

هرچند عملکرد نهادهای دولتی و غیر دولتی، دارای تأثیر متقابل و قابل توجهی بر یکدیگر هستند، اما در میان کلیه نهادها و تشکل‌هایی که به شکل آنلاین و الکترونیک به فعالیت می‌پردازند، دولت‌های الکترونیک از مهمترین و بالاترین جایگاه برخوردار هستند. دلیل این مسأله نیز کاملاً واضح است. حجم قابل توجه، وسیع و متنوع تعاملات آن‌ها به شکل درون یا برون سازمانی، تأثیر عمده و گسترده‌ای را برکلیه ابعاد و شئون اجتماع خواهد داشت.

شاید بتوان گفت بارزترین مزیت استفاده از روش‌های نوین در فعالیت‌های کلان، افزایش سرعت رسیدگی به مشکلات و حل مسائل کلان کشورها و نیز صرفه جویی در منابع و ظرفیت‌های موجود است.

تجربه انجام موفقیت آمیز بسیاری از فعالیت‌های کلان تجاری، اداری، نظارتی و از این دست، به شکل الکترونیکی و آنلاین، توسط برخی از دولت‌ها، نشان داده که این شیوه مدرن قادر است علاوه بر افزایش بازده و سرمایه‌های برگشتی، از فرسایش قابل توجه نیرو ومنابع انسانی بکاهد.

برخی از مسئولان و صاحب نظران، به ویژه در حوزه قدرت و سیاست، ضعف امنیتی دولت‌های الکترونیک و آسیب پذیر بودن آن‌ها در برابر حملات مخرب آنلاین را به عنوان مانعی بزرگ برای تحقق آن می‌دانند، اما ...

باید گفت که تلاش و صرف هزینه در جهت تحقق و پیشبرد دولت الکترونیک، با توجه به مزایا و بازدهی فراوان آن در کوتاه مدت، خود پیش شرط لازم برای احساس نیاز به ایجاد امنیت در آن است. علاوه بر این، تجربه کشورهای پیشرو در این حوزه، استفاده از گواهی نامه‌های امنیتی موجود و نیز دسترسی آسان (البته برای کشورهای خارج از محدوده تحریم‌های جهانی) به فناوری‌های حفاظتی قدرتمند، تضمینی برای قدرت، قوت و استحکام لایه‌های امنیتی در تعاملات درون و برون سازمانی دولت‌های الکترونیک، محسوب می‌شوند.

از دیدگاه برخی از کارشناسان، تحقق دولت الکترونیک، مقدم بر بحث امنیت در آن است و کشورها باید تمام سعی خود را برای پرهیز از عواقب وخیم عقب ماندگی از جهان الکترونیک با تعاملات سریع، آسان و ارزان آن، بکار گیرند.

در نهایت، می‌توان فهرستی از موانع بزرگ و کوچک در راه تحقق و تأمین امنیت دولت‌های الکترونیک را در نظر گرفت. این موانع، که اغلب خواسته یا ناخواسته، به علل مختلف اجتماعی، سیاسی و فرهنگی و در طول زمان ایجاد شده‌اند با اعتماد و همکاری نزدیک میان دولت‌ها و ملت‌ها، ایجاد زیرساخت و بسترهای لازم و نیز توجه بیشتر به جهانی شدن (با حفظ ارزش‌ها و آرمان‌های فرهنگی، اجتماعی)، رفته رفته در کوتاه مدت از بین رفته و زمینه تحقق دولت‌های الکترونیک یکپارچه و یا مستقل، در سرتاسر جهان، ایجاد خواهد کرد.

از میان مهمترین موانع موجود، به‌ویژه در ساختارهای دولتی، می‌توان به موارد زیر اشاره کرد:

- مدیریت سنتی در بخش‌های مختلف دولت؛
- عدم توجه به‌کارگیری روش‌های نوین در تعاملات، رفتارها و ارتباطات درون سازمانی و برون سازمانی دولت؛
- عدم برنامه‌ریزی مدون برای فرهنگ سازی و آموزش در میان توده مردم برای افزایش اعتماد و اعتنا به تعاملات الکترونیکی؛

- عدم حمایت از کاربران دولتی یا غیر دولتی اینترنت از طریق فراهم کردن امکانات فنی و اطلاعاتی؛
- تلاش دولت‌ها برای کنترل و نظارت همه جانبه دنیای الکترونیک؛
- عدم وجود قوانین مدون و لازم الاجرا در بخش فعالیت‌ها و تعاملات الکترونیکی؛
- عدم توجه به امنیت به مفهوم واقعی کلمه در سیستم‌ها و شبکه‌های رایانه‌ای دولتی و غیر دولتی؛
- عدم وجود قانون کپی رایت در کشورها؛
- عدم توجه به جهانی شدن و ورود به دنیای مناسبات نوین با حفظ ارزش‌ها و آرمان‌های ملی؛

البته جوامع و توده مردم نیز با عدم اعتماد خود به روش‌های نوین، حضور غیرفیزیکی و غیر ملموس برای انجام فعالیت‌ها و پی‌گیری مسائل، ترجیح دادن روش‌های سنتی در تعامل خود با دولت برخلاف وجود ساختارهای لازم برای ارتباط الکترونیک و نیز عدم تمایل به استفاده از نرم افزارهای کامل، رسمی و ثبت شده برای تأمین امنیت لازم در فعالیت‌های تجاری، اداری و مالی خود، نشان داده‌اند که مانعی بزرگ برای تحقق امنیت دولت‌های الکترونیک محسوب می‌شوند.

به هرترتیب، باید پذیرفت که کشورهای در حال توسعه برای پیشرفت و ارتقاء همه جانبه خود، چاره‌ای جز ورود به دنیای یکپارچه الکترونیک، نخواهند داشت. هرچند ورود به این دنیا، صرف هزینه‌ها و منابع خاصی را می‌طلبد، اما مدت زمان اندک برای بازدهی قابل توجه، صرفه‌جویی‌های بسیار در منابع ملی و جهانی، ایجاد اتحاد، همدلی و همکاری نزدیک میان ملت‌ها و دولت‌ها و نیز عواقب ناخوشایند ناشی از طرد شدن از جامعه جهانی اطلاعات، روز به روز تمایل دولت‌ها را برای انجام تعاملات و فعالیت‌های الکترونیکی، افزایش می‌دهد.

چالش‌ها و موانع اساسی فراروی امنیت در فضای مجازی و اینترنت

در جریان سیاستگذاری برای امنیت فضای سایبر و اینترنت در کشور ما چالش‌ها و موانع جدّی وجود دارد. این چالش‌ها و موانع عبارتند از:

۱- فقدان راهبرد مشخص در زمینه توسعه الکترونیک و امنیت فضای مجازی؛
۲- فقدان متولی مشخص در حفاظت از داده‌های موجود در سامانه‌های نظامی، امنیتی، اقتصادی؛
۳- عدم وجود قانون کپی رایت و حفظ حقوق مادی و معنوی افراد در کشور؛
۴- فقدان سیاست ملی فضای سایبر، اینترنت و مخابراتی؛
- روشن نبودن سیاست‌ها در مورد گسترش اینترنت، تلفن همراه و مخابرات داده‌ها؛
- روشن نبودن میزان ظرفیت دولت در پذیرش مشارکت بخش خصوصی در وارد کردن و توزیع اینترنت؛

۵- فقدان سیاست روشن گمرکی در مورد مجاز یا ممنوع بودن واردات تجهیزات، دریافت و ارسال ماهواره‌ای برای خدمات اینترنت؛
۶- افزایش احتمال دستبرد اطلاعات محرمانه کشور و یا خرابکاری توسط بیگانگان؛
۷- افزایش جرائم پنهانی در فضای مجازی و حرفه‌ای شدن مجرمین با افزایش استفاده از شبکه‌های مجازی در دستگاه‌ها و نهادهای دولتی و خصوصی؛
۸- فقدان سیاست مشخص ملی در آموزش و اطلاع‌رسانی؛
- به رغم تشکیل شورای عالی اطلاع‌رسانی این شورا به سیاست‌گذاری تفصیلی و اعلام شده‌ای در زمینه‌ی اطلاع‌رسانی دست نیافته است. وجود مدعیان و متولیان متعدد در مدیریت ملی اطلاعات و عدم تفکیک وظایف آن‌ها موجب کندی و بلکه عقب‌ماندگی جدی ایران در تولید و سازمان‌دهی اطلاعات الکترونیک شده است. امروزه به علت عدم سازمان‌دهی اطلاعات علمی کشور، دسترسی به کتابخانه کنگره آمریکا بسیار ساده‌تر و مفیدتر از دسترسی به کتابخانه‌های ملی، مجلس و دانشگاه تهران است.

۹- فقدان سیاست‌های نظارتی و امنیتی مشخص در کشور ؛
- بایستی روشن شود که مسئول حفاظت از داده‌های موجود در سامانه‌های نظامی، امنیتی، اقتصادی کشور کیست؟
- چه سازمانی مسئول جلوگیری، پیشگیری و پیگیری حملات الکترونیکی و نقش امنیت سامانه‌های ملی است؟
- چه سازمانی متولی سیاستگذاری و تعیین موارد ممنوعه در تبادل داده‌ها است؟

– کدام سازمان مسئول نظارت بر کیفیت فرهنگی و محتوای سایت‌های تولیدشده و قابل دسترس در کشور است؟

چالش‌های پیش روی اینترنت در ایران:

- با نگاهی به وضعیت فعلی اینترنت در ایران در حال حاضر سیاست گسترش و افزایش ظرفیت تبادل بین المللی داده‌ها از سیاست‌های جاری دولت است و افراد، سازمان‌ها و شرکت‌ها به گونه‌ای نامحدود امکان دسترسی به سرویس دهندگان رسانه‌های جدید را دارند.برای دسترسی به اینترنت هیچگونه مجوز یا تاییدیه دولتی لازم نیست و هنوز سرویس دهندگان اطلاعات مربوط به مشترکان، کاربران و محتوای داده‌های تبادل شده را به سازمان‌های دولتی ارائه نمی‌دهند.
- هیچ قانون یا دستور العملی برای منع رمز گذاری محتوای داده‌های مبادله شده وجودندارد و هیچ قانونی نیز وجود ندارد که سرویس دهندگان را ملزم به کنترل محتوا نماید یا آنان را مسئول محتوای سایت‌های روی سرویس بداند از طرف دیگر خدمات اینترنت در ایران به سرعت ارزان شده و کافه‌های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوه تأسیس و نحوه اداره آن وجود ندارد.
- به نظر می‌رسد تهدید اصلی و بالفعل کشور در مورد اینترنت، فقدان گفتمان امنیتی در مورد این پدیده است. اینترنت که به طور بالقوه می‌تواند هم تهدید و هم فرصتی طلایی برای امنیت فرهنگی و سیاسی باشد، به وسیله‌ای برای فشار سیاسی و اقتصادی تبدیل شده است.
- برای تحلیل فرایند سیاستگذاری در مورد اینترنت در ایران، پاسخ به سؤالاتی در مورد آزادی بیان، کنترل جریان اطلاعات، قوانین مربوط و در یک بیان نظریه هنجاری حاکم بر رسانه‌های جدید ضروری است. این سؤالات به پنج حیطه اصلی قابل تحلیل است:

۱- حق ارتباط خصوصی؛

۲- حق ارتباط ناشناس؛

۳- حق رمزگذاری در ارتباط؛

۴- معافیت کانال ارتباطی از مسئولیت محتوا؛

۵- دسترسی عمومی و ارزان.

- با توجه به تحقیقات انجام شده نظریه حاکم بر رسانه‌های مرسوم در ایران در سال ۱۳۷۶، آمیزه‌ای از نظریه مسئولیت اجتماعی، توسعهٔ بخش و ایدئولوژیک بوده است. تغییرات سیاسی سال ۱۳۷۶ به بعد نقش نظریه مسئولیت اجتماعی را تقویت کرده است. ولی در مورد اینترنت وضع کاملاً متفاوت است و حاکمیت تئوری آزادی‌گرا بر دسترسی و انتشار از طریق اینترنت کاملاً ملموس است. تا اواخر نیمه اول سال ۱۳۸۰، دولت هیچ گونه نظارت و دخالت ملموسی در مورد آن نداشته است. زیرا:

- قوانین مربوط به مطبوعات که عمده‌ترین قانون در حوزهٔ محدودیت‌های آزادی بیان است و شامل گفتار روی شبکه نمی‌شود.
- افراد، سازمان‌ها و شرکت‌ها امکان دسترسی به سرویس دهندگان اینترنت را از طریق خطوط تلفن دارند.
- برای دسترسی به اینترنت هیچ گونه مجوز دولتی لازم نیست.
- دسترسی به اینترنت با پست یا پست الکترونیکی نیاز به هیچ گونه تائیدیه‌ای از طرف هیچ سازمان دولتی ندارد.
- هیچ دستورالعمل یا بخشنامه‌ای وجود ندارد که سرویس دهندگان را موظف کند اطلاعات مربوط به مشترکان، کاربران و محتوای داده‌های تبادل شده را به سازمان‌های دولتی ارائه دهند.
- هیچ قانون یا دستورالعملی برای منع رمزگذاری محتوای داده‌های مبادله شده وجود ندارد.
- هیچ قانونی وجود ندارد که سرویس‌دهندگان ملزم به کنترل محتوا نماید.
- هیچ سیاست و اقدام مشخصی در مورد سانسور یا بلوکه کردن سایت‌ها، گروه‌های مباحثاتی و آدرس‌های پست الکترونیکی وجود ندارد و ایران فاقد یک سیستم فیلترینگ ملی و مرکزی است.

- هیچ قانونی وجود ندارد که سرویس‌دهندگان را مسئول محتوای سایت‌های روی سرویس بداند.
- کافه‌های اینترنتی به سرعت در حال رشد است و هیچ قانون خاصی برای نحوه‌ی تأسیس و نحوه‌ی اداره وجود ندارد، این کافه‌ها تابع قانون اماکن عمومی هستند.

- خدمات اینترنت در ایران به سرعت ارزان شده است و دولت برای دسترسی‌های دانشگاهی یارانه قابل ملاحظه‌ای را پذیرفته است. سیاست گسترش فیبر نوری و افزایش ظرفیت تبادل بین‌المللی داده‌ها از سیاست‌های جاری دولت است.

مراکز دخیل یا ذی نفوذ در حل مسائل:

به مقوله امنیت در فضای مجازی می‌توان از دیدگاه‌های مختلفی پرداخت، می‌توان امنیت اخلاقی، فرهنگی، اقتصادی و یا حتی سیاسی را در آن بررسی نمود و یا از جنبه فنی به امنیت در فضای سایبر نگاه کرد، در این بخش سعی می‌کنیم سازمان‌ها و نهادهایی که در امنیت فضای مجازی از جنبه‌های گوناگون دخیل هستند را به اختصار بررسی نماییم.

شکل شماره (٤): مراکز دخیل و ذی‌نفوذ در امنیت فضای مجازی ایران

مجلس شورای اسلامی و مجمع تشخیص مصلحت نظام

مجلس شورای اسلامی و مجمع تشخیص مصلحت نظام با تصویب قوانین، اختصاص بودجه مناسب و ایجاد هماهنگی بین نهادهای مسئول، اساسی ترین نقش را در ایجاد امنیت و رهبری نهادهای دیگر بر عهده دارند.

وزارت ارتباطات و فناوری اطلاعات

با تامین نیازهای کاربران و ایجاد ساختار و بستر امن و مناسب فنی، از اصلی‌ترین نهادهای آماده سازی فعالیت در فضای مجازی به شمار می‌رود.

وزارت کشور

گستره فعالیت‌ها، بودجه، امکانات و زیر مجموعه‌هایی چون استانداری، فرمانداری، شهرداری و شوراهای شهر و اهمیت داشتن سیاست و رویکردی واحد در کشور خود بیانگر اهمیت این نهاد در برقراری امنیت و فرهنگ عمومی در سراسر کشور در فضای سایبر می‌باشد.

وزارت علوم، تحقیقات و فناوری و وزارت آموزش و پرورش

با توجه به این که افراد دوره طولانی از زندگی خود را در این نهادها می‌گذرانندآموزش روش‌ها، راه‌کارها، و قوانین زندگی در فضای مجازی و پژوهش در زمینه‌های پیشگیری و بالا بردن ضریب امنیت حرکت در این فضا راهبردی مؤثر در بالا بردن سطح آگاهی‌های عموم جامعه و افراد تحصیل کرده می‌باشد.

حوزه‌های علمیه

با ایفای بهتر و مؤثرتر نقش فرهنگی و دینی خود در راستای فرهنگ سازی اسلامی و دینی، با تولید و گسترش نرم افزارها، سایت‌ها و محصولات فرهنگی اسلامی جذاب و مطابق با ذائقه نسل جوان نقش بسیار مهمی در سالم سازی فضای اینترنتی و سایبر بر عهده دارد.

سازمان صدا و سیما

امروزه در جهان معاصر که به مثابه دهکده جهانی است ارتباطات نقش اول را در جوامع ایفا می‌کند. در این میان صدا و سیما نقشی اساسی در افزایش آگاهی‌های عموم مردم و فرهنگ فعالیت در جامعه مجازی را دارد.

وزارت فرهنگ و ارشاد اسلامی و سازمان تبلیغات اسلامی

تلاش در جهت گسترش فرهنگ اسلامی و دینی و هدایت افراد جامعه در مسیر صحیح و درست با افزایش آگاهی‌ها و تبلیغات خلاقانه و بررسی سایت‌ها و پورتال‌های موجود از لحاظ تطبیق با زندگی اسلامی و ایرانی و نشان دادن راه‌کارهای درست، در همین جهت می‌تواند نقشی محوری و ارشادی داشته باشد.

قوه قضائیه

قوه قضائیه در کنار نیروی انتظامی در برخورد با مجرمان و خلافکاران مسئولیت مستقیم دارد. این قوه با آموزش و تربیت و استفاده از قضات متخصص و کارآمد و آشنا با فضای سایبر و اینترنت نقش انکار ناپذیری در برقراری نظم و امنیت در جامعه مجازی را بر عهده دارد.

نیروی انتظامی

با توجه به گستره عملکرد و مسئولیت نیروی انتظامی به عنوان سازمانی که مسئولیت مستقیم برخورد با جرائم را بر عهده دارد با ظهور جامعه مجازی این مسئولیت نیز بر عهده کارکنان مسئولیت پذیر و ساعی این نهاد قرار داده شده که با آموزش و بکار گیری نیروهای متخصص و پلیس آگاه به فناوری‌های روز، همگام و هماهنگ با سایر سازمان‌ها به خصوص قوه قضائیه نقش انکار ناپذیر خود را در پیشگیری و مقابله با تهدیدات و جرائم در فضای سایبر ایفا کند.

چشم انداز اولیه در صورت ادامه روند وضع موجود

همانطور که گفته شد امنیت، یکی از مهمترین مسائل موجود در بحث فناوری اطلاعات و ارتباطات محسوب می‌شود که متاسفانه نه‌تنها با پیشرفت تکنولوژی‌های حفاظتی بهبود نیافته بلکه رو به وخامت نیز نهاده است. از این رو باتوجه به وضعیت کنونی خلق، انتشار و عملکرد سریع کُدهای مخرب و افزایش چشمگیر تعداد و تنوع عملیات و حملات تخریبی جاسوسی و کلاهبرداری و نیز افزایش تعداد مجرمین رایانه‌ای امنیت فضای مجازی بـه طـور گسـترده و روبه رشدی از بین رفته و مورد تهدید جدی قرار گرفته است و آزمایشگاه‌های امنیتی جهـان قادر به دریافت، تحلیل و بررسی تمام این بـدافزارها بـه منظـور ارائـه روش‌هـای پاکسـازی نخواهند بود.

این روند در کشور ایران با توجه به وضع موجود زیرساختارهای امنیتی و نیز عدم وجود قوانین و مقررات مناسب و همچنین توسعه و گسترش روز افزون و بدون برنامه اینترنـت و فضاهای مجازی در شرکت‌ها و سازمان‌های مختلف دولتـی و خصوصـی منجـر بـه کـاهش بیشتر امنیت و افزایش جرائم رایانه‌ایی در بُعد و اندازه‌های مختلف شده است.

بنابراین با توجه به جمیع مطالب گفته شده در فوق می‌توان چشم انداز امنیت در فضای مجازی ایران را در صورت ادامه روند موجود چنین بیان کرد:

- صدمه و خسارت غیر قابل جبران به اقتصاد ملی از طریق سرقت، تخریـب و حمـلات الکترونیکی و رایانه‌ای ؛
- کاهش امنیت فضای مجازی ایران و بالطبع عدم اعتماد و اطمینان مـردم بـه خـدمات الکترونیکی ارائه شده از سوی دولت و پلیس؛
- تخریب وجهه سیاسی و امنیتی کشور بوسیله هک شدن سایت‌های رسمی کشور؛
- کاهش اقتدار پلیس و افزایش هزینه‌های پلیسی با افزایش جرائم رایانه‌ای؛
- کاهش انگیزه مخترعان و نوآوران با از بین رفتن حقوق معنوی آن‌هـا بـه دلیـل عـدم وجود قوانین کپی رایت و عدم اجرای مجدانه این قوانین؛
- از بین رفتن امنیت و نقض حریم خصوصـی افـراد و سـازمان‌هـا بوسـیله فـاش شـدن اطلاعات محرمانه و شخصی کاربران ؛

- افزایش تعداد هکرها و خرابکاران و سارقان اینترنتی در فضای مجازی ایران بـه دلیـل عدم وجود زیرساختارهای امنیتی کامل و مناسب .

چشم انداز مطلوب

مهمترین مسأله در مقابله با جـرائم سـایبر مسـئولیت پـذیری دولـت در سیاسـتگذاری کارشناسانه و همه سو نگر برای تدوین سیاست‌ها، قوانین و مقررات مناسب حمایتی، هدایتی، نظارتی است. در این مسیر بهره‌گیری از تمام توان علمـی و اجرایـی کشـور، رویکـرد میـان رشته‌ای و میان بخشی ضروری اسـت. همچنـین تـدوین و اجـرای تـدابیر امنیتـی در قبـال تهدیدات گسترده ضرورتی اجتناب ناپـذیر بـرای سـازمان‌هـا و نهادهـای کشـور محسـوب می‌شود. تدابیر مناسب می‌توانند احتمال وقوع مخاطرات را به حداقل برسـانند، در صـورت وقوع آن‌ها میزان خسارت‌های وارده را در حد بسیار ناچیزی نگه دارنـد و قابلیـت واکـنش سریع و مؤثر بوجود آورند تا سازمان‌ها برای ترمیم خسارات از فراینـدهای از پـیش تعیـین شده استفاده کنند تا بهره‌وری و ایمنـی اطلاعـات افـزایش یابـد و کسـب و کـار بـا خیـالی آسوده‌تر تداوم یابد.

از طرف دیگر شرط موفقیت هر سیاستی اهتمام به آموزش خانواده و آموزش کودکان و نوجوانان، تربیت نیروی انسانی متخصص در مقابله با این جرائم و در نهایـت سـازمان‌دهـی جدید نیروی انتظامی و قوه قضاییه برای تأسیس پلیس سایبر و دادسرای جرائم سایبر است

با عنایت به مباحث فوق و باتوجه به این که در صورت انجام سیاستگذاری، برنامه‌ریزی و نظارت دقیق و کامل در خصـوص امنیـت فضـای سـایبر در کشـور و تعامـل و همکـاری مناسب میان تمامی نهادها، سازمان‌ها و بخش‌های دولتی و خصوصی در این زمینه مـی‌تـوان چشم انداز مطلوب امنیت فضای مجاز و اینترنت را این گونه ترسیم نمود:

- مسئولیت‌پذیری دولت در سیاستگذاری علمی، کارشناسانه و همه سو نگر و بهره‌گیـری از تمام توان علمی کشور، جهت تحقق بیشترین منافع و کمترین آسـیب‌هـا از صـنعت اینترنت در ایران؛
- جلوگیری از اثرات مخرب ارتباط با پایگاه‌های ضداخلاقی و مبتذل بـا ایجـاد و توسـعه سایت‌های مفید و درعین حال جذاب؛

- جلوگیری از نفوذ اطلاعات آلوده به شبکه‌های اطلاع‌رسانی و نیز جلوگیری از صدمات و خسارت‌های جبران‌ناپذیر از آلاینده‌های جسمی بر پیکر جامعه و کشور.

راه‌کارها و اقدامات مؤثر بر امنیت فضای مجازی و اینترنت

با توجه به این که با ایجاد مانع در توسعه فضای مجازی و اینترنت (همانند محدود کردن پهنای باند یا عدم توسعه خدمات نوین و ...) نمی‌توان جلوی تهدیدات را گرفت و بایستی همراه با توسعه صنعت و کاربری IT با مدیریت، تهدیدات و خطرات بالقوه و بالفعل امنیتی را کاهش و از وقوع آن جلوگیری کرد.

از این رو سه رویکرد در رویارویی با تهدیدات فضای سایبر و اقدامات غیر قانونی که امنیت و سلامت این فضا، با آن روبه‌رو است، متصور است :

جرم‌انگاری با توسل جستن به قانون که لازمه آن داشتن قانون جرائم رایانه‌ای و بسیاری از قوانین مکمل دیگر است، یکی از این رویکردهاست. از جمله رویکردهای دیگر ایجاد و اتخاذ تدابیر حفاظتی و کنترلی در قالب پیشگیری وضعی و آموزش کاربران و توانمندسازی در مقابل تهدیدات پیشگیری اجتماعی است؛ اما بهترین روش بهره‌گیری همزمان از این سه رویکرد است.

با توجه به مطالب و رویکردهای فوق راه‌کارها و اقدامات اساسی که می‌بایست در سیاستگذاری‌ها و برنامه‌های آتی کشور در مورد تأمین امنیت فضای مجازی و اینترنت در ایران در نظر گرفته شود به شرح زیر می‌باشد:

- تدوین و توسعه نظام نظارت و حفاظت امنیتی بر محتوای داده‌های مبادله شده با توجه به قانون امنیتی کشور و حفظ حریم عمومی و خصوصی که نقش اساسی در پیشگیری از گسترش فساد، تهدیدات امنیتی، رسوخ جاسوسی و خرابکاری الکترونیک و عملیات روانی خواهد داشت.
- ایمن‌سازی زیرساخت‌های حیاتی کشور و منابع ملی در قبال حملات الکترونیکی و ایجاد نظام مدیریت امنیت زیرساخت‌های حیاتی در دستگاه‌های مرتبط؛

- تامین سلامت و جلوگیری از مخاطرات ناشی از محتوای اطلاعات مبادله شده و تقویت صنعت الکترونیک و توسعه خدمات و محصولات؛
- توسعه و حمایت از تحقیق و ارتقاء سطح آگاهی دانش و مهارت‌های مرتبط امنیت فضای مجازی و شبکه‌های الکترونیکی؛
- توسعه و ارتقاء سطح همکاری‌های منطقه‌ای و بین‌المللی در زمینه امنیت فضای مجازی و شبکه‌های الکترونیکی شامل مسائل حقوقی، قضایی، انتظامی، کارت‌های اعتباری بانکی و غیره ؛
- تدوین و اجرای قوانین مورد نیاز و روزآمد در حوزهٔ ارتباطات شبکه‌ای به خصوص در موضوع حقوق تکثیر و مالکیت آثار فرهنگی و نرم‌افزارها و اطلاعات الکترونیکی که تأثیر قطعی در تشویق تولیدات و اختراعات بر روی شبکه دارد؛
- سیاستگذاری مناسب در توسعه اینترنت به طوری که توسعه مصرف یا باز تولید محتوای آن محدود نشده، بلکه به گسترش فرهنگ بومی و مذهبی و مقاومت فرهنگی کمک نماید و نیز به خلاقیت‌گستری مدد رسانده و موجبات خلاقیت‌زدایی را فراهم آورد؛
- تدوین و طراحی نظام تولید و سازمان‌دهی الکترونیک اطلاعات علمی، اداری و مالی براساس استانداردهای قابل تبادل در شبکه‌ها پیش از توسعه روز افزون اینترنت؛
- تدوین و تصویب و اجرای سریعتر قانون کپی رایت در کشور؛
- تحول در ساختار سازمانی ناجا با ایجاد جایگاه برای پلیس جرائم رایانه‌ای و اینترنتی به‌صورت حرفه‌ای جهت پیشگیری و مقابله با این نوع جرائم؛
- به‌کارگیری و آموزش نیروی انسانی متخصص و مجرب در زمینه مقابله با جرائم رایانه‌ای در ناجا؛
- ایجاد همکاری و هماهنگی قوی بین تمامی دستگاه‌ها و نهادهای دولتی و نظامی (کشوری و لشگری) جهت ایجاد امنیت فضای مجازی و جلوگیری از دوباره‌کاری‌ها و موازی‌کاری‌ها ؛
- توسعه و تجهیز امکانات و وسایل الکترونیکی و ارتباطی مدرن و جدید در ناجا جهت پیشگیری و مقابله با جرائم رایانه‌ای؛

- ایجاد ارتباط قوی با راهبرد مشخص بین نیروی انتظامی و قوه قضائیه، وزارت اطلاعات و مخابرات کشور. سایر دستگاه‌های مرتبط جهت پیشگیری و مقابله با جرائم رایانه‌ای؛
- اطلاع رسانی و ارتقاء آگاهی مردم در خصوص جرائم رایانه‌ای و قوانین و مقررات مربوطه؛

نتیجه گیری:

به نظر می‌رسد در حال حاضر تهدید اصلی کشور در مورد فضای مجازی، فقدان گفتمان امنیتی در مورد این پدیده است. فقدان دانش جامع‌نگر در مورد صورت مسأله و عدم وجود مطالعات سیاستگذاری مقایسه‌ای در کشور، حاکمیت روش آزمون خطا و اعمال سلایق فردی و سازمانی را به دنبال داشته است.

مسئولیت‌پذیری دولت در سیاستگذاری علمی، کارشناسانه و همه سو نگر و بهره‌گیری از تمام توان علمی کشور، شرط اصلی تحقق بیشترین منافع و کمترین آسیب‌ها از فضای مجازی در ایران است.

برای جلوگیری از اثرات مخرب ارتباط با پایگاه‌های ضداخلاقی باید به سمتی حرکت کنیم که سایت‌های مفید، جذابیت پیدا کند. یعنی ابتدا در حد توان باید در زمینه‌ی سایت‌های مفید و درعین حال جذاب سرمایه‌گذاری کنیم. از طرف دیگر هم باید موارد منفی را سد کنیم، یعنی از نفوذ سایت‌های مخرب، به این سو جلوگیری کنیم. چون در کشورهای غربی، مثل انگلیس، مسأله استفاده از سایت‌های مستهجن توسط دانش‌آموزان مدارس به صورت یک بحران درآمده است و آن‌ها به این نتیجه رسیده‌اند که دو راه در پیش رو دارند: بستن راه‌های دسترسی به اینترنت یا کنترل آن، در هر حال نیاز اساسی جوامع در حال رشد به دریافت اطلاعات مفید و سازنده را نمی‌توان نادیده گرفت. و این در حالی است که از تخریب مبانی اعتقادی و اجتماعی جامعه نیز می‌باید با حساسیت تمام جلوگیری کرد.

منابع

- خداقلی، زهرا (۱۳۸۲)، "***جرایم رایانه‌ای***"، انتشارات آریان، تهران.
- دیوید جی . آیکاو و همکاران (۱۳۸۳)، "***راه‌کارهای پیشگیری و مقابله با جرائم رایانه‌ای***"، مترجمان: اکبر استرکی و دیگران، دانشگاه علوم انتظامی، معاونت پژوهش.
- سادوسکای، جورج و همکاران (۱۳۸۴)، "***راهنمای امنیت فناوری اطلاعات***"، مترجمان: مهدی میردامادی و دیگران، تهران، دبیرخانه شورای عالی اطلاع رسانی.
- سایت اینترنتی روزنامه هموطن سلام.

- ***http://pandasoftware.com/***
- ***http://www.itiran.com/***
- ***http://www.websecurity.ir/***
- ***http://www.itlawseminar.net/***
- ***http://www.iranhackers.com/***