امنیت ملی در فضای سایبر، فرصت ها و تهدیدها با تأکید بر استقرار دولت الکترونیکی

محمدرضا موحدی صفت[1]

چکیده

با ظهور فناوری های نوین اطلاعات و ارتباطات (ICT) در پایان هزارهٔ دوم مفهوم جدیدی به نام فضای سایبر (فضای مجازی) در پیش روی بشر قرار گرفته است که توانسته پیشرفت های خارق العاده ای را برای وی به ارمغان آورد. این فضا با توجه به ماهیت خود، مفهوم دهکدهٔ کوچک جهانی را متجلی نموده، به گونه ای که ارائه خدمات بین نظام های مختلف ملی و بین المللی در ساده ترین و سریع ترین وضعیت ممکن میسر گشته است.

با توجه به ماهیت فضای سایبر به عنوان بستر اصلی اطلاعات کشور و اینکه امکان صدمه زدن از این راه بسیار محتمل می باشد، لازم است که نگاه ویژه ای به مسأله امنیت فضای سایبر مخصوصاً در سطح کاربردهای ملی شود، زیرا در آینده ای نزدیک زیرساخت های اصلی کشور در این فضا قرار خواهند گرفت و بروز هر گونه مشکل امنیتی باعث تهدید جدی در امنیت ملی کشور خواهد گردید.

تحقیق حاضر ضمن معرفی ویژگی های فضای سایبر، وضعیت کشور را بر اساس آمارهای موجود مورد ارزیابی قرار داده و پس از بررسی مسأله امنیت فضای سایبر، به اولویت بندی در استقرار آن پرداخته است. همچنین دولت الکترونیکی به عنوان مهم ترین ره آورد فضای سایبر مورد بررسی قرار گرفته است.

کلید واژه

امنیت فناوری اطلاعات و ارتباطات، امنیت ملی، فضای سایبر، شبکه های رایانه ای، دولت الکترونیکی

---

[1] کارشناس ارشد رایانه – دانشگاه صنعتی امیر کبیر

❑ مقدمه

منظور از فضای سایبر یا فضای مجازی ترکیبی از ده ها هزار رایانه به هم پیوسته، سرویس دهنده ها، شبکه های ارتباطی، سویچها و کابل های فیبر نوری است که امکان ایجاد ارتباطات را در یک سیستم جامع فراهم می‌آورد.کارامد و سالم بودن فضای سایبر در اقتصاد و امنیت ملی کشورها از اهمیت ویژه ای برخوردار است. [1:5]

امنیت اطلاعات در محیط های مجازی و فضای سایبر به عنوان مهم ترین الزام در کاربری توسعه ای و فراگیر فناوری اطلاعات و ارتباطات می باشد. اگرچه امنیت مطلق در محیط های واقعی و محیط های مجازی امکان پذیر نیست، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی و متناسب با نیازها و سرمایه گذاری انجام شده باشد تقریباً در همه شرایط محیطی ممکن می باشد. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمان های دولتی و شرکت های خصوصی ضمن اعتقاد و اطمینان به طرف های گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند، نقش مورد انتظار خود را به عنوان گره ای مؤثر از این شبکه متعامل و هم افزار ایفا خواهند نمود.

اطمینان از ایمن بودن سرمایه های اطلاعاتی و تجهیزات زیرساختی کشور گذشته از ابعاد گسترده امنیت ملی، کلید قفل فرصت های بی شمار تجاری و غیر تجاری جدید اینترنتی است. آنچه مسلم است چالش امنیتی رودرروی کشور، عدم دسترسی به فناوری و یا عدم وجود محصولات امنیتی نیست، بلکه سیاست گذاری، فرهنگ سازی، مدیریت مناسب منابع موجود و نیز سازگاری آنها به گونه ای است که نیاز منحصر به فرد شبکه و فضای دیجیتالی کشور را تأمین کند. [4:37]

❑ بیان مسأله و ضرورت تحقیق

شالوده و بنیاد هر کشوری بر اساس مجموعه ای از زیرساختارهای حیاتی آن کشور در بخش های ارتباطات، دفاع، انرژی، حمل و نقل، کشاورزی، بهداشت و امور اقتصادی است که فضای سایبر به مثابه یک سیستم عصبی آنها را به هم مرتبط می سازد. [1:5]

استفاده از فضای سایبر که دستاورد فناوری های نوین اطلاعات است، اگرچه

برای کشورهای در حال توسعه به عنوان یک فرصت برای جبران عقب ماندگی های فناورانه نسبت به جوامع پیشرفته است، اما باید دقت نمود که همین فناورانه که ساخته دست این جوامع است، اگر درست مورد بهره برداری قرار نگیرد و حساسیت های امنیتی آن مورد توجه واقع نشود، خود می تواند به عنوان یک تهدید مهم به حساب آید.

امروزه اقدامات تروریستی فراوانی در فضای سایبر متوجه دولت هاست که از ویژگی های این حملات می توان به ناشناخته بودن و سرعت حملات مذکور اشاره نمود، و معمولاً این گونه حملات پس از وقوع مورد شناسایی قرار می گیرند. بنابراین با ایجاد یک راهبرد ملی در استقرار حداکثر امنیت در فضای سایبر می توان به کاهش آسیب‌پذیری کشور در مقابل حملات پرداخته و از بروز خسارت به زیرساخت های اطلاعاتی پایه و حیاتی و همچنین دارایی‌های ملی جلوگیری نمود.

این نکته نباید نادیده گرفته شود که امروزه انگیزه های زیادی برای مبارزه با نظام جمهوری اسلامی ایران که در طی دو دهه و نیم گذشته با چالش های اساسی روبرو شده، وجود دارد که موقعیت حساس کشور ایران در جهان اسلام و منطقه خاورمیانه و وجود متخصصان مجرب و رشد سریع فناوری در کشور از جمله عواملی است که دشمنان را ترغیب به خرابکاری می نماید و ساده ترین روش مبارزه با کشور ما سعی در عدم توسعه یافتگی و اختلال در زیرساختارهای حیاتی آن است که اجباراً باید در فضای سایبر قرار گیرند. شرایط پرتنش پیش رو و تحولات سریعی که در حال وقوع است ضروری می نماید که مدیریت کلان کشور از تمامی پتانسیل ها و امکانات موجود و نیز با پیش آگاهی نسبت به وقایع، درصدد طراحی راهبرد امنیت ملی در فضای سایبر برآید. [14:6]

نکته قابل توجه انکه امروزه تهدیدات نوینی در عرصهٔ جهانی ظهور کرده اند که با سیستم های واکنش سنتی قابل رفع نمی باشند و با توجه به توسعهٔ شگرف فضای سایبر چنین به نظر می رسد که کلیه کشورها دیر یا زود چنین تهدیداتی را تجربه خواهند کرد. بنابراین ایجاد یک سیستم واکنش ملی به تهدیدات بالقوه موجود در فضای سایبر یک ضرورت برای کشورهای توسعه یافته و همچنین برای کشورهای در حال توسعه که عموماً به عنوان مصرف کننده این فناورانه نوین می باشند خواهد

بود. [2:6]

تجاربی مانند واقعه ۱۱ سپتامبر نشان داد که در صورت وقوع هر تهدیدی از ناحیه فضای سایبر، دو اقدام باید به سرعت انجام شود. نخست ارائه یک واکنش مثبت جهت تحدید بحران و آماده کردن فضای مناسب برای مدیریت اوضاع و دوم، تهیه و اعمال سیاست هایی که بتواند مانع از تکرار وضعیت شود. با توجه به تخصصی بودن هر دو فعالیت، لازم است که گروه های کارشناسی تحلیل راهبردی، تحلیل تاکتیکی و آسیب شناسی فضای مجازی، کاملاً فعال باشند و با کمترین ریسک موجود و زمان محدود، بیشترین بهره را ببرند. [2:8]

همچنین باید توجه نمود که امنیت ملی در فضای سایبر بدون امنیت شبکه جهانی امکان پذیر نیست و هیچ کشوری نمی تواند نسبت به آنچه در سایر کشورهای حاضر در شبکه جهانی در حال وقوع است بی تفاوت باشد زیرا صدمات آن در صورت وقوع قابل انتقال به سایر کشورها است. بنابراین لازم است که بخش هایی از دولت مخصوصاً سرویس های اطلاعاتی – امنیتی به بازتعریف تقویت خویش در فضای سایبر بپردازند و برای انجام این بازتعریف نیازمند آشنایی با اصول و مدل های مختلف امنیت در فضای سایبر می باشند. [2:14]

❑ اهداف تحقیق

تحقیق حاضر برای پاسخ به سئوالات تحقیق، اهداف زیر را دنبال می نماید:

۱.تعیین عواملی که امنیت فضای سایبر را تهدید می کند.

۲.تعیین عواملی که امنیت فضای سایبر جمهوری اسلامی ایران را تهدید می کند.

۳.ارائه راهکارهای عملی جهت حفظ امنیت فضای سایبر در جمهوری اسلامی ایران

❑ سئوال اصلی تحقیق

تحقیق حاضر به دنبال دادن پاسخ به این پرسش است که "عوامل مؤثر بر حفظ امنیت فضای سایبر برای جمهوری اسلامی ایران کدام است؟" و در این ارتباط دو سئوال فرعی را می توان مطرح نمود:

▫ سئوالات فرعی تحقیق

۱. عواملی که عموماً امنیت فضای سایبر را تهدید می کند کدامند؟
۲. الزامات عملی برای حفظ فضای سایبر چیست؟

▫ فرضیهٔ تحقیق

به طور کلی در ارتباط با سئوالات تحقیق می توان فرضیه های ذیل را مطرح نمود:

۱. عوامل ساختاری و فرهنگی از مهم ترین عوامل تهدید کننده امنیت فضای سایبر می باشند.
۲. الزامات سخت افزاری (زیرساخت های مخابراتی، تجهیزات الکترونیکی) و الزامات نرم افزاری سواد الکترونیکی کاربران و قوانین فضای سایبر بر حفظ فضای سایبر مؤثر می باشند.

▫ روش تحقیق و ابزارهای جمع آوری داده ها

روش تحقیق حاضر از نوع اکتشافی است و از اسناد و مدارک موجود در شبکه جهانی اینترنت، کتب و مقالات به روش فیش برداری به عنوان مهم ترین ابزارهای جمع آوری اطلاعات در این تحقیق بهره برداری شده است. همچنین پس از جمع آوری اطلاعات، با استفاده از تحلیل فاصله، اطلاعات و داده های اکتشافی در محیط را مورد تجزیه و بررسی قرار می دهیم.

▫ مفاهیم و واژه های تحقیق

فضای سایبر : فضایی مجازی است که از ترکیب صدها هزار رایانه تحت شبکه های ارتباطی به وجود می آید. در این فضای مجازی سامانه های بسیاری به وجود آمده و با تعامل با یکدیگر عمل می نمایند. اینترنت به عنوان بزرگ ترین شبکه در فضای سایبر می باشد. امروزه اکثر زیرساخت های کشورها در قالب این فضا تعریف می شوند. [1:5]

امنیت ملی : یعنی در امان بودن و ایمن بودن یک ملت. بدیهی است یک ملت زمانی از امنیت برخوردار است که تمامی نیازها و ارزش های حیاتی آن از خطر تهدیدات مختلف و همه جانبه به طور نسبی در امان باشد. [7:69]

شبکه های رایانه ای : برای اتصال رایانه ها از شبکه ها استفاده می شود. این

شبکه ها در سه قالب شبکه های محلی، شبکه های شهری و شبکه های گسترده وجود دارند. شبکه های محلی به دلیل محدود بودن به عنوان ایمن ترین و شبکه های گسترده که در رأس آنها شبکه اینترنت قرار دارد به عنوان آسیب پذیرترین شبکه ها هستند. [6:113]

دولت الکترونیکی : دولت الکترونیکی دراصطلاح به استفاده از فناوری اطلاعات و ارتباطات درجهت ارائه اطلاعات و خدمات به شهروندان، بخش های اقتصادی، کارمندان دولت وسایر قسمت های دولتی اطلاق می شود که دارای مزایایی مانند کارامد نمودن مدیریت دولتی، ارائه بهتر خدمات دولتی به شهروندان و تعامل بیشتر با آنان، افزایش توان از طریق دسترسی به اطلاعات، سرعت و شفافیت بیشتر و گسترش فرهنگ خودمحوری در خدمات رسانی است. [8:1]

حقوق سایبری : این حقوق در دو حوزهٔ حقوق مدنی و حقوق تجاری قابل بررسی است. در حقوق مدنی مواردی همچون قراردادهای انفورماتیکی، ادله اثبات دیجیتالی، حقوق مالکیت فکری و پایگاه داده ها و در زمینه حقوق تجاری، ایجاب و قبول در مبادلات الکترونیکی، امنیت زیرساخت در رمزکردن پیام ها، استناد پذیری و حمایت از مصرف کنندگان وجود دارد. [9:166]

تهدیدات امنیتی فضای سایبر : زمانی می توان از فضای سایبر به عنوان پیوند دهنده زیرساخت های حیاتی کشور استفاده نمود که مسأله امنیت آن به طور کامل حل شده باشد. وجود هرگونه شکاف امنیتی در این فضا و همچنین در اجزایی که در این فضا عمل می نمایند، ضربات جبران ناپذیری را به کشور وارد خواهد کرد. [2:9]

امنیت شبکه های رایانه ای : با استفاده گسترده از شبکه های رایانه ای و اینکه همواره در خطر آسیب قرار دارند و هکرها و کراکرها همیشه درصدد نفوذ به شبکه و خرابکاری در آن هستند، برای داشتن فضای سایبر ایمن باید امنیت شبکه های ارتباطی را تا بالاترین حد خود افزایش داد. مزاحمان شبکه ها در دو گروه داخلی و خارجی تقسیم می شوند. [11:533]

جنگ اطلاعات : به کلیه اقداماتی اطلاق می شود که از طریق اثرگذاری بر اطلاعات و سامانه های اطلاعاتی دشمن و به منظور دستیابی به برتری اطلاعاتی در

راستای راهبرد نظامی یک کشور صورت پذیرد. [13:297]

▫ مبانی نظری (ادبیات تحقیق)

امنیت فضای سایبر و زیرساخت ها

در حوزه فناوری اطلاعات و ارتباطات، دو نوع امنیت برای یک کشور متصور است: امنیت زیرساخت های حیاتی و امنیت فضای سایبر که امنیت زیرساخت ها به عنوان یک اصل برای رسیدن به امنیت در حوزه فضای سایبر است و زمانی می توان در مورد امنیت در فضای سایبر بحث کرد که از امنیت زیرساخت ها مطمئن باشیم. بنابراین برای رسیدن به یک راهبرد در ارتباط با امنیت فضای سایبر باید مؤلفه های اصلی در امنیت زیرساخت ها را نیز مورد بررسی قرار دهیم. [19:3]

اگرچه زیرساخت های حیاتی یک کشور ممکن است در بخش های مستقلی فعال باشند، اما برای قرار گرفتن در فضای سایبر باید از لحاظ امنیتی دارای شرایط خاصی باشند تا با قرار گرفتن در این فضا برای خود و سایرین، مشکلات امنیتی به وجود نیاورند. نصب دیواره های آتش، اطمینان از شبکه بندی های داخلی، استفاده از تکنیک های مؤثر در رمزنگاری اطلاعات، اطمینان از عدم سرقت و نشت اطلاعات و هر گونه تهدید شبکه ای از وظایف اداره کنندگان این زیرساخت ها می باشد و پس از آنکه اطمینان لازم از امنیت آنها به وجود آمد می توان تمهیدات لازم را برای استقرار فضای سایبر یعنی ایمن سازی ارتباطی بین زیرساخت ها به وجود آورد.

بر اساس بیانیه های جهانی، ارتباطات، تولید نیرو، منابع نفت و گاز، بانکداری و امور اقتصادی، حمل و نقل، کشاورزی و دفاع از زیرساختارهای اصلی دولت به عنوان منابع هر کشوری هستند که هرگونه خدشه در عملکرد ویا حملات تروریستی علیه آنها باعث ضربه جبران ناپذیر دفاعی و اقتصادی می گردد. [20:4]

تهدیدات فضای سایبر

نشت اطلاعات، سرقت داده های حیاتی کشور و آسیب پذیری شبکه های جامع اطلاع رسانی به عنوان مهم ترین اشکالات امنیتی در این فضا می باشد که اگر از طرف حکومت توجه ویژه ای به آن نشود به عنوان یک تهدید جدی برای منافع پایه ای کشور تلقی می شود. وجود شبکه جهانی اینترنت که امکان دسترسی های مختلف را برای همه افراد در سرتاسر جهان میسر ساخته است، واقعیتی انکارناپذیر

است که به عنوان مهم ترین بستر فضای سایبر و مهم ترین عامل در امنیت ملی و زیرساخت های کشورهای توسعه یافته است که تهدیدات مجازی درون آن شکل گرفته و فعال می شوند.

ورود به دنیای جدید، قوانین خود را می طلبد، به قول "فرانسیس بیکن" حتی اگر نیازی به قانون احساس نمی کنیم ابتدا باید آن را بشناسیم و سپس آن را کنار بگذاریم. از طرف دیگر نبود زیرساخت های فنی قابل قبول نیز ما را در معرض خطرات بسیاری قرار داده است. هم اکنون غالب سایت های ایرانی روی سرورهای آمریکایی قرار دارند، همین موضوع برای امنیت اطلاعات ما یک بحران به شمار می رود. قراردادن سرور در داخل کشور نیز به وجود بسترهای مخابراتی قوی بستگی دارد، چیزی که در حال حاضر امیدی به آن نمی رود [3:3]

نمونه زیر، تهدیدی در فضای سایبر است که از سوی یک گروه خرابکاری در آمریکا اتفاق افتاده است:[3:1]

یک نهاد تروریستی اعلام می کند که شبکه برق شمال غربی اقیانوس آرام را به مدت ۶ ساعت از ساعت ۴ بعدازظهر قطع خواهد کرد و همین تهدید را هم اجرا می کنند، سپس همان گروه اعلام می کند مدارهای اصلی مخابرات بین شرق و غرب ایالات متحده را به مدت نصف روز از کار خواهد انداخت و همین کار را هم علیرغم کوشش های متخصصان جهت مبارزه علیه آنها انجام می دهد؛ سپس این گروه تهدید می کند سیستم کنترل ترافیک هوایی شهر نیویورک را از کار انداخته، مانع پروازها شده و مسیر پروازهای داخلی را منحرف می سازد و این کار را نیز انجام می دهد. تهدیدها به طور پیاپی ادامه یافته و با موفقیت اجرا می شوند که این نمایانگر توانایی دشمن برای حمله به زیرساخت های حیاتی یک کشور در فضای سایبر است. نهایتاً تهدید می کند که اگر فهرست خواسته هایشان برآورده نشود تجارت الکترونیک و سرویس کارت اعتباری را به وسیله چند صد هزار هویت ربوده شده در میلیون ها معامله تقلبی، از کار خواهد انداخت. حال هراس و آشوب و اغتشاش عمومی را پس از این تهدید تجسم کنید. [3:1]

عموماً تهدیدهایی که در فضای سایبر وجود دارد و می تواند باعث صدمه در زیرساختارهای کشور شود در۴ حوزه زیر قرار دارند :[15:4]

۱. کاربران خانگی که در زمان اتصال به شبکه می توانند با ورود به سامانه های موجود تهدیداتی را به وجود آورند. معمولا با توجه به آنکه اثر خاصی از آنها در شبکه ثبت نمی شود، شناسایی آنها دشوار می باشد.
۲. مؤسسات بزرگ مانند شرکت ها و دانشگاه ها که به بخش هایی از زیرساخت ها دسترسی دارند و انگیزه کافی در کارکنان و دانشجویان برای نفوذ به شبکه ها وجود دارد.
۳. بخش های مهم دولتی و موسسات ملی که بنا به اقتضا باید برخی از اطلاعات را به صورت اشتراکی در اختیار کاربران قرار دهند و خطر نفوذ از این ناحیه وجود دارد.
۴. کاربران شبکه اینترنت که با نفوذ به سرورهای موجود در زیرساختارها می توانند تهدیدی برای آنها به شمار آیند.

فضای سایبر و راهبردها

اکثر کشورهای توسعه یافته از جمله آمریکا برای تأمین امنیت در فضای مجازی خود، راهبرد های ملی خود را تدوین نموده اند که در کشور آمریکا سه هدف زیر مد نظر قرار داشته است: [1:5]

۱. از حملات فضای سایبر به زیرساخت های اساسی کشور ممانعت به عمل آید.
۲. زمینه های آسیب پذیری داخلی را که می توانند موضوع تهدیدات سایبر قرار گیرند، کاهش داده و از بین ببرند.
۳. در صورت وقوع حملات سایبر، ترتیبی اتخاذ شود تا خسارات وارده به حداقل رسیده و زمان بهبود شرایط کاهش یابد.

این راهبرد که پس از حادثه ۱۱ سپتامبر و با توجه به آسیب پذیری های جدی جامعه آمریکا ناشی از مخاطرات در فضای سایبر تدوین شده، به شرح زیر است : [2:6]

۱. طراحی یک سیستم واکنش ملی ویژه مقابله با تهدیدات در فضای سایبر؛
۲. طراحی برنامه واکنش در قبال تهدیدات و آسیب ها در فضای سایبر؛

۳. طراحی برنامه ارتقاء سطح آگاهی و مهارت عمومی برای فعالیت در فضای سایبر؛
۴. اهتمام به ایمن سازی جایگاه مجازی حکومت در شبکه ارتباطی؛
۵. ایجاد همکاری و همگرایی بین دو بخش امنیت ملی و امنیت مجازی بین المللی.

دولت الکترونیکی و فضای سایبر

دولت الکترونیکی، به عنوان مهم ترین کاربرد در استفاده از فضای سایبر است و با توجه به روند رو به رشدی که دارد، تا به حال با چالش های متعددی روبرو شده که مهم ترین آنها مسأله امنیت، عدم توانایی همه شهروندان در استفاده از خدمات، حفاظت از حریم خصوصی افراد، مقررات گذاری و مسایل حقوقی کاربران است. [18:3]

دولت الکترونیکی تمهیداتی را برای کارکنان دولت فراهم می کند که با در خدمت گرفتن فناوری اطلاعات و ارتباطات، بتوانند با دقت بیشتر، سریع تر و به صورت استاندارد وظایف محوله را به بهترین شکل انجام دهند اما بررسی این نکته که با استفاده از امکانات دولت الکترونیکی شهروندان بیشتری سرویس خواهند گرفت و یا فناوری در این زمینه به عنوان سد عمل می کند حائز اهمیت است. [18:4]

نوع نگرش به دولت الکترونیکی کاملاً با روال های سنتی متفاوت است. در روش های سنتی اطلاعات عموماً بر روی کاغذ نگهداری می شود و روش های ایمن سازی نقل و انتقال و نگهداری اطلاعات کاملاً مشخص و نسبتاً آسان می باشد اما در روش الکترونیکی که اطلاعات بر روی سرورها قرار می گیرند و به راحتی قابل نقل و انتقال به غیر هستند، مکانیزم نگهداری ایمن اطلاعات بسیار مهم و حیاتی است. دو اصلی که در این رابطه باید در نظر داشت عبارتند از: [21:4]

۱. قابلیت اعتماد: اطمینان از اینکه اطلاعات فقط در اختیار افراد و سیستم های مجاز قرار می گیرد. اطلاعات می تواند در حوزه های نظامی، اقتصادی و غیره محرمانه تلقی شود.
۲. در دسترس بودن : اطمینان از اینکه اشخاص دارای مجوز، بتوانند به اطلاعات مورد نظر خود در شبکه دسترسی داشته باشند.

اینترنت که به عنوان بستر اصلی ارتباطات دولت الکترونیک به شمار می رود، دارای نقاط ضعف فراوانی است که می تواند باعث بروز انواع خرابکاری ها در سرویس های ارائه شده در نظام دولت الکترونیکی گردد. وجود هکرها، سارقان و خرابکاران اینترنتی باعث شده که توجه به مسأله امنیت در استقرار دولت الکترونیکی برای هر کشوری حائز اهمیت گردد.

امروزه آمارها نشان می دهد که دولت ها با شتاب بسیاری در حال الکترونیکی شدن هستند و مزایای این حرکت به حدی زیاد است که کشورهای کمتر توسعه یافته نیز چاره ای جز پذیرش آن ندارند.[16:13]

با توجه به آنکه فناوری های مربوط به دولت الکترونیکی مخصوصاً در بخش ارتباطات عموماً از کشورهای توسعه یافته نشأت گرفته است، احتمال آنکه امنیت این سیستم ها دچار آسیب پذیری گردد و حتی سامانه های مستقر دچار نشت اطلاعاتی شوند بسیار زیاد است؛ که بر اساس آن امنیت ملی کشور دچار مخاطره می گردد. به عنوان نمونه وجود تجهیزاتی مانند مسیریاب ها و دیواره های آتش که کل سخت افزار آنها از خارج از کشور تهیه می شود می تواند به عنوان یک تهدید جدی تلقی شود.

امروزه موارد فراوانی از مسیریاب های شبکه مشاهده شده است که باعث نشت اطلاعات دولتی شده اند. برای نمونه آمریکایی ها یک سیستم بانکی را در کشور استرالیا پیاده سازی کرده بودند که یک نسخه از تراکنش های مهم عملیاتی را از طریق نشت اطلاعات به آمریکا ارسال می نمود.

همچنین به دلیل کاهش پهنای باند در کشور ما اکثر شرکت ها که برخی از آنها دولتی هم هستند از سرورهای اینترنتی که در کشورهای خارجی نصب می گردد، استفاده می کنند که از لحاظ امنیتی خود به عنوان یک تهدید جدی است.

وضعیت فضای سایبر در ایران

در بعد داخلی می توان گفت که تا قبل از سال ۱۳۸۰ تقریبا هیچ کار جدی که در ارتباط با ارائه راهبرد، برنامه ریزی و یا طرح ریزی منطقی در زمینه استقرار فضای سایبر و امنیت اطلاعات و یا حتی توسعه فناوری اطلاعات بوده باشد، وجود ندارد. در سال ۱۳۸۰ فهرستی از خط مشی های کلان در رابطه با چگونگی توسعه و

بهره برداری از شبکه های اطلاع رسانی رایانه ای توسط مقام معظم رهبری به دست اندرکاران در این زمینه ابلاغ گردید. در سال ۱۳۸۱ طرح توسعه و کاربری فناوری اطلاعات و ارتباطات کشور (تکفا) به عنوان اولین طرح در سطح ملی ارائه گردید.

تجربه های عمده ای که در ارتباط با فضای سایبر در کشور ما مورد استفاده قرار می گیرد عمدتاً برگرفته از کشورهای فنلاند و ایالات متحده آمریکا است. سند راهبردی کشور فنلاند در سال ۲۰۰۲ و کشور آمریکا در سال ۲۰۰۳ به تصویب رسیده است.[5:7]

یکی از الزامات اصلی در استفاده از فضای سایبر داشتن پهنای باند بالا در شبکه های ملی و بین المللی است و این درحالی است که پهنای باند متوسط استفاده شده در کشور ما بسیار پایین تر از سایر کشورهاست که باعث عدم ارائه سرویس های لازم بر روی این فضا می شود.

▫ تجزیه و تحلیل

اگرچه رشد توسعه فناوری در ارتباط با استفاده از فضای سایبر در ایران قابل توجه است، اما ضعف در زیرساخت ها و رشد بیش از حد این فناوری در کشورهای توسعه یافته باعث وجود شکاف دیجیتالی شده که برای حل این مشکل، دولت باید با عزم ملی و با سرعت هر چه بیشتر، برنامه های خود را در زمینه توسعه ساختاری فناوری اطلاعات تدوین و اجرا نماید.

در این بخش بر اساس تحلیل فاصله سعی شده که وضعیت ایران در مقایسه با سایر کشورها در موضوعات زیر مورد بررسی قرار گیرد:

۱. فاصله کاربری در شبکه سایبر؛
۲. فاصله ضریب نفوذ توزیع تجهیزاتی؛
۳. فاصله خدماتی؛
۴. فاصله دسترسی و زیرساخت؛
۵. فاصله تولیدات سخت افزاری و نرم افزاری؛
۶. فاصله فرهنگ بهره برداری و مشارکت اطلاعاتی.

۱- فاصله کاربری در شبکه سایبر

آمار منتشر شده توسط سایت www.internetworldstats.com میزان نفوذ اینترنت در کشورهای جهان را نشان می دهد که در جدول ۱ اطلاعات برخی از کشورها در پایان سال ۲۰۰۷ نشان داده شده است.

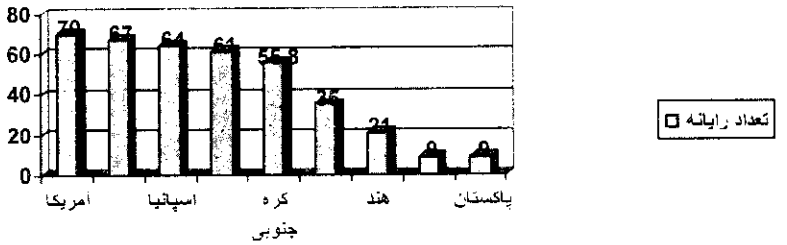
کشور	کاربران سال ۲۰۰۷	رشد از ۲۰۰۰ تا ۲۰۰۷	ضریب نفوذ در جمعیت	کشور	کاربران سال ۲۰۰۷	رشد از ۲۰۰۰ تا ۲۰۰۷	ضریب نفوذ در جمعیت
چین	۱۶۲,۰۰۰,۰۰۰	٪۶۲۰	٪۱۲	پاکستان	۱۲,۰۰۰,۰۰۰	٪۸۸۶۱	٪۷
هنگ کنگ	۴,۸۷۸,۷۱۳	٪۱۱۳	٪۶۸	امارات عربی	۱,۷۰۸,۵۰۰	٪۱۳۲	٪۴۳
هند	۶۰,۰۰۰,۰۰۰	٪۱۱۰۰	٪۵	اسرائیل	۳,۷۰۰,۰۰۰	٪۱۹۱	٪۵۱
اندونزی	۲۰,۰۰۰,۰۰۰	٪۹۰۰	٪۹	**ایران**	**۱۸,۰۰۰,۰۰۰**	**٪۷۱۰۰**	**٪۲۵**
ژاپن	۸۷,۵۴۰,۰۰۰	٪۸۵	٪۶۸	دانمارک	۳,۷۶۲,۵۰۰	٪۹۲	٪۶۹
قزاقستان	۱,۲۴۷,۰۰۰	٪۱۶۸۱	٪۹	آلمان	۵۰,۴۲۶,۱۱۷	٪۱۱۰	٪۶۱
کره جنوبی	۳۴,۱۲۰,۰۰۰	٪۷۹	٪۶۷	فرانسه	۳۲,۹۲۵,۹۵۳	٪۲۸۷	٪۵۴
مالزی	۱۴,۹۰۴,۰۰۰	٪۳۰۲	٪۵۸	آمریکا	۲۱۵,۰۸۸,۵۴۵	٪۱۲۵	٪۷۱

جدول ۱ – آمار کاربران اینترنت در برخی کشورها

اگرچه رشد اینترنت در کشور از وضعیت مناسبی برخوردار است، اما ضریب نفوذ اینترنت نسبت به اکثر کشورهای آسیایی در حد پایین قرار دارد. طبق این آمار متوسط ضریب نفوذ در آمریکا و کشورهای توسعه یافته اروپایی بیش از ۶۰٪ می باشد و این مهم ترین دلیل توسعه و استفاده کاربری از فضای سایبر است.

۲- فاصله ضریب نفوذ توزیع تجهیزاتی

در نمودار ۱ که بر اساس اطلاعات سایت www.orbicom.com می باشد، ضریب نفوذ دسترسی به رایانه در تعدادی از کشورها آمده است.



نمودار ۱ – ضریب نفوذ تجهیزات در کشورها

از از این جدول چنین استنباط می شود که نسبت تجهیزات توزیع شده در کشور ما نسبت به کشورهای توسعه یافته بسیار پایین است که این مسأله ضمن افت فرهنگ و سواد رایانه ای، امکان استفاده از خدمات ارائه شده در فضای سایبر را نیز کاهش می دهد.

۳- فاصله خدماتی

بر اساس گزارش های منتشر شده از واحد فناوری اطلاعات اکونومیست که در مورد میزان کارایی خدمات، به کارگیری سامانه ها و بررسی نقاط ضعف و قوت طرح های فناوری اطلاعات در کشورهای مختلف جهان است، ایران در رتبه ۶۹ قرار دارد. (جدول ۲)

این در حالی است که کشورهای دیگر حوزه خاورمیانه مثل امارات‌متحده عربی، ترکیه، عربستان سعودی، لبنان، مصر، پاکستان، قزاقستان و آذربایجان بالاتر از ایران قرار دارند.

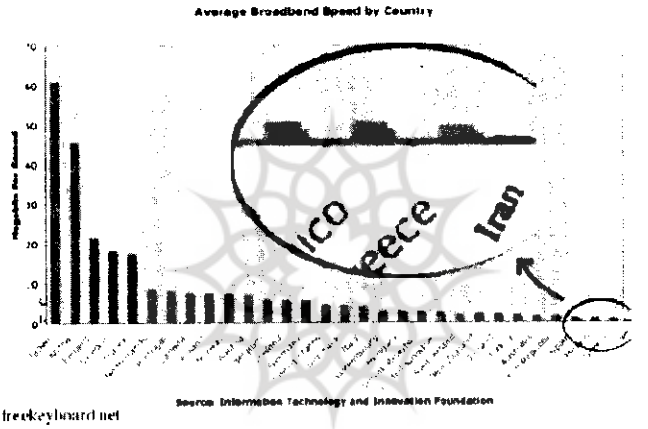
2007 e-readiness rank (of 69)	2006 rank	Country	2007 e-readiness score (of 10)	2006 score
1	1	Denmark	8.88	9.00
2(tie)	2	US	8.85	8.88
2(tie)	4	Sweden	8.85	8.74
4	10	Hong Kong	8.72	8.36
18	21	Japan	8.01	7.77
19	12	Germany	8.00	8.34
20	17	Belgium	7.90	7.99
21	16	Ireland	7.86	8.09
22	19	France	7.77	7.86
65	66	Vietnam	3.73	3.12
66	63	Algeria	3.63	3.32
67	62	Indonesia	3.39	3.39
68	68	Azerbaijan	3.26	2.92
69	65	Iran	3.08	3.15

جدول ۲

کشورهای هنگ کنگ، تایوان و ژاپن در آسیا دارای مقام نخست در ارائه فناوری ارتباطات و اطلاعات هستند و کشور آمریکا پس از کشور دانمارک در رتبه دوم قرار دارد. آنچه که باعث شده کشور دانمارک در جهان و یا کشورهای هنگ کنگ و تایوان در آسیا در مقام های نخست باشند، برتری آنها در زمینه ارائه آموزش‌های گوناگون فناوری، هزینه پایین برقراری مکالمات تلفنی، خرید و نصب تجهیزات لازم برای پیشبرد فناوری اطلاعات و ارتباطات و نیز اولویتی است که این دولت ها برای ICTدر سطح ملی قائل شده اند. البته با وجود آنکه آمریکا در رتبه دوم قرار دارد، در زمینه برخی شاخص‌ها مانند آمادگی تجاری و برتری در پژوهش‌های علمی پیشتاز است. [9:3]

۴- فاصله دسترسی و زیرساخت

بر اساس آمار سایت ITU1 ایران از لحاظ دسترسی و زیرساخت ارتباطی در جهان رتبه ۱۰۳ را داراست و همچنین بر اساس آمار سازمان بین المللی نوآوری فناوری اطلاعات ۲ ITIF میزان پهنای باند متوسط استفاده شده در کشور ۱۲۸ کیلوبایت می باشد. (نمودار ۲)



نمودار ۲ – پهنای باند مورد استفاده در برخی کشورها

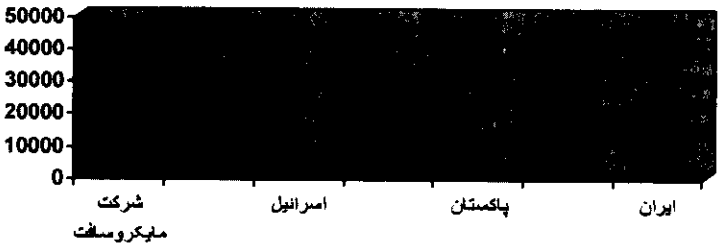
این میزان پهنای باند به هیچ وجه پاسخگوی ارائه خدمات مبتنی بر فضای سایبر نمی باشد و نمی توان سرویس های مورد نیاز را مخصوصاً در حوزه دولت الکترونیکی ارائه داد. نبود پهنای باند مناسب در کشور باعث شده که اکثر سازمان ها مخصوصاً سازمان های دولتی به سراغ میزبان های خارجی رفته و اطلاعات خود را بر روی میزبان های خارجی قرار دهند که از لحاظ امنیت به صلاح نیست.

۵- فاصله تولیدات سخت افزاری و نرم افزاری

در نمودار ۳ صادرات نرم افزاری تعدادی از کشورها و شرکت مایکروسافت آمریکا

1. International Telecommunication Union
2. Information Technology and Innovation Foundation

در سال ۲۰۰۶ مورد مقایسه قرار گرفته است:



نمودار ۳ – صادرات نرم افزار بر حسب میلیون دلار در سال ۲۰۰۶

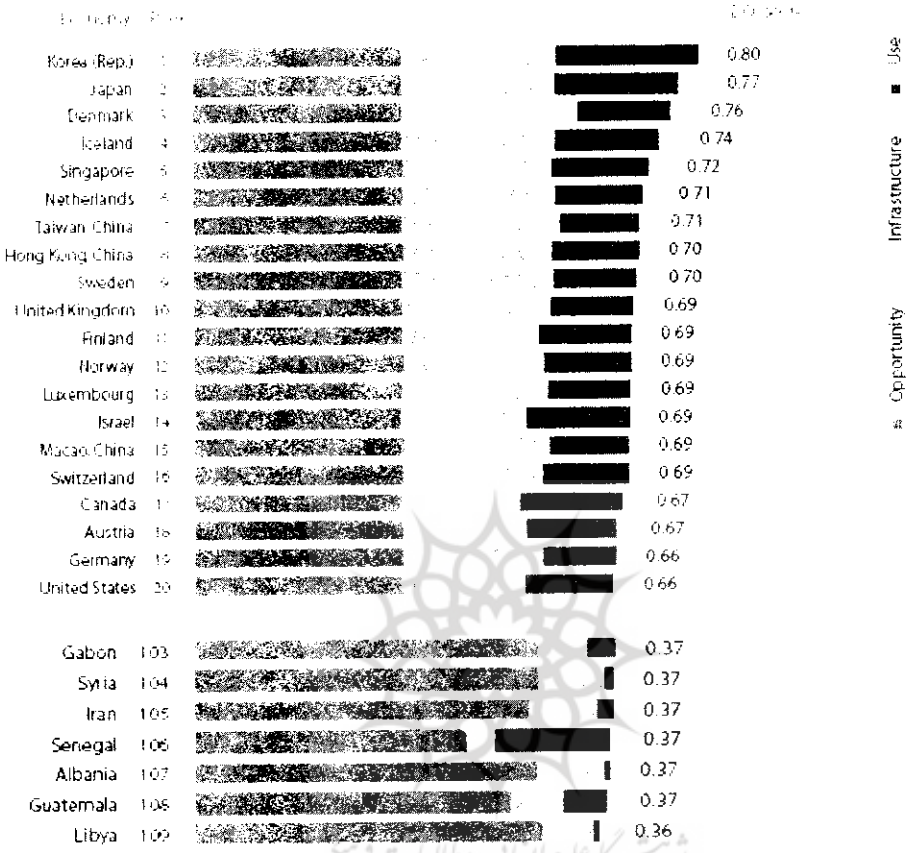
در زمینه نرم افزار که مهم ترین ملاک ارزشیابی آن صادرات است، وضعیت کشور ما مطلوب نیست که در این زمینه دولت با حمایت خود می تواند حامی صنعت نرم افزاری باشد.

در زمینه تولیدات سخت افزاری، کشور ما در وضعیت نامناسبی قرار دارد و تقریباً تمامی تجهیزات اصلی مورد نیاز رایانه ها از خارج از کشور تهیه می شود و هیچ گونه صادرات سخت افزاری وجود ندارد. در حالی که کشورهای آسیایی مانند مالزی، سنگاپور، تایوان، چین و هنگ کنگ به عنوان مهم ترین صادرکنندگان سخت افزار هستند.

۶- فاصله فرهنگ بهره برداری و مشارکت اطلاعاتی

سایت واحد ارتباطات جهانی[1] www.itu.com در گزارش سال ۲۰۰۷ میزان بهره برداری از فرصت های دیجیتالی را برای ۱۸۱ کشور جهان مورد بررسی قرار داده که بخشی از آن در نمودار ۴ مشاهده می شود:

1. International Telecommunication Union



نمودار ۴

رتبه ایران در بین ۱۸۱ کشور مورد مقایسه ۱۰۵ می باشد که از بسیاری از کشورهای منطقه مانند بحرین(۳۵)، امارات (۳۷)، قطر(۳۸)، ترکیه(۵۲)، کویت(۶۰)، عربستان (۷۵) و عمان(۸۱)، پایین تر می باشد. لازم به تاکید مجدد است که یکی از ابزارهای توسعه اقتصادی و داشتن فرصت های دیجیتالی استفاده از فناوری های موجود در فضای سایبر است که نیاز به عزم ملی دارد.

پاسخ به سوال اصلی

در ارتباط با فرضیه اول که عوامل ساختاری و فرهنگی را عامل تهدید در فضای سایبر می داند می توان به موارد ذیل اشاره نمود:

الف – عوامل ساختاری مرتبط

عوامل ساختاری زیر به عنوان مهم ترین تهدید کننده های فضای سایبر ایران شناخته می شوند:

۱. ضعف در ساختار مخابراتی به گونه ای که در حال حاضر اکثر ارتباطات مخابراتی کشور از طریق خطوط با پهنای باند کم صورت می گیرد. در حالی که در کشورهای توسعه یافته با استفاده از زیرساخت های مخابراتی مبتنی بر فیبر نوری سرعت متوسط را به بیش از ۱۰ مگابیت بر ثانیه رسانده اند. [12:1]

۲. نبود سازمان یا سازمان های تصمیم گیر مستقل برای مدیریت فضای سایبر در کشور به گونه ای که در حال حاضر مرجع واحدی در سطح ملی برای این مسأله وجود ندارد و تعدد نهادها باعث تعدد روش های اجرایی شده که از لحاظ امنیتی صحیح نمی باشد. در حالی که در کشورآمریکا بخش امنیت داخلی در سال ۲۰۰۲ به وجود آمد و مدیریت امنیت فضای سایبر بر عهده این نهاد گذاشته شد. [1:7]

موارد پیش گفته تأییدی است بر قسمت اول فرضیه اول که عوامل ساختاری به عنوان تهدید در فضای سایبر مؤثر می باشند.

ب- عوامل فرهنگی مرتبط :

در ارتباط با عوامل فرهنگی تأثیر گذار در امنیت فضای سایبر نیز می توان به موارد زیر اشاره داشت:

۱. وجود سایت های مخالف ارزش های مذهبی که تعداد آنها نیز بسیار زیاد می باشد و همچنین وجود فضاها و تالارهای گفتگوی مخالف این ارزش ها از عوامل تهدید کننده هستند و هدف آنها نیز بیشتر جوانان و اعتقادات آنها می باشد. به گونه ای که بر اساس آمارها ۲٪ مراجعات در دنیا و ۵٪ مراجعات در کشور ما به سایت های مخالف ارزش های مذهبی است و همچنین بیش از ۸۰٪ افرادی که در این فضای سایبر قرار می گیرند، تجربه اتصال به این گونه سایت ها را دارند که می تواند یک تهدید ملی در حوزه فضای سایبر تلقی شود.

۲. شایعه پراکنی و سرعت شایعه پراکنی در فضای سایبر و همچنین وجود

سایت هایی که دارای اندیشه های ضد نظام جمهوری اسلامی هستند می توانند به عنوان بستر نامناسب انتقال دیدگاه ها به مردم و علی الخصوص جوانان قرار گیرند که امروزه این مسأله به یک تهدید تبدیل شده است و این عوامل نیز تأیید کننده بخش دوم فرضیه اول می باشند.

در ارتباط با فرضیه دوم که الزامات سخت افزاری و نرم افزاری را عاملی مؤثر بر امنیت فضای سایبر می داند می توان به موارد ذیل اشاره نمود :

الف – الزامات سخت افزاری

وابستگی به تجهیزات پایه سخت افزاری که در زیرساخت های فناوری و ارتباطات کشور مورد استفاده قرار می گیرد به عنوان یک تهدید است. به عنوان مثال در حال حاضر شرکت ایزایران که پشتیبانی تجهیزات نیروهای مسلح را بر عهده دارد، تجهیزات مورد استفاده در فضای سایبر نیروهای مسلح مانند سوئیچ ها، مسیریاب ها و غیره را از شرکت های خارجی تهیه می کند که به عنوان یک تهدید جدی تلقی می شود.

ب- الزامات نرم افزاری :

۱- سواد الکترونیکی کاربران

دولت الکترونیکی تنها با وجود شهروند الکترونیکی محقق می شود و نبود برنامه ریزی صحیح، اثر مستقیم بر سواد دیجیتالی کاربران دارد. امروزه در کشورهای الکترونیکی اکثر خدمات دولت از طریق بالابودن سطح سواد الکترونیکی شهروندان ارائه می شود. بنابراین بالابردن سطح سواد دیجیتالی آحاد جامعه، مخصوصاً در مورد مدیران یکی از الزامات مؤثر در امنیت فضای سایبر است، زیرا زمانی شهروندان می توانند به صورت ایمن از فضای سایبر استفاده نمایند که آموزش های لازم را در این خصوص دیده باشند.[12:1]

۲- قوانین فضای سایبر

امروزه حقوق سایبری در ابعاد مدنی، تجارت، جزایی، بین الملل و فنی مطرح می شود و به تبع آن با ورود فناوری های نوین و گسترش روزافزون فضای سایبر مخصوصاً در بخش های ملی لازم است که موارد حقوقی آن نیز به صورت دقیق

معین گردد.[9:165]

البته مجلس شورای اسلامی حقوق مربوط به جرایم رایانه ای را در سال ۱۳۸۴ مورد بررسی قرار داده است اما باید توجه داشت که این قوانین باید در بازه های زمانی بسیار کوتاه بازنگری شوند.

در یک جمع بندی اجمالی می توان موارد ذیل را در پاسخ به سوال اصلی تحقیق مطرح نمود:

۱. *ایجاد نهادهای تصمیم گیر دولتی در بالاترین سطح :* کشور ما در حال پیمودن گام های اولیه در ارتباط با فضای سایبر می باشد و تا حد قابل قبولی در این زمینه پیشرفت داشته است و با رشد فزاینده ای در این بستر مجازی وارد شده و خدمات دولتی را به سمت الکترونیکی شدن پیش می برد. بنابراین لازم است که در بالاترین حد تصمیم گیری دولتی، نهادهای تخصصی ایجاد گردد تا مسأله امنیت فضای سایبر را به صورت ملی مورد بررسی قرار دهند.

۲. *بسیج بخش های غیردولتی :* برای نیل به امنیت در این فضا باید ضمن طراحی یک سیستم مدیریت بحران، به تجزیه و تحلیل داده ها و کشف تهدیدات در حال وقوع در این فضا پرداخت و این مسأله صرفاً از ناحیه اهتمام و برنامه بخش دولتی قابل تأمین نیست و برای این منظور بخش های غیردولتی و حتی کلیه مردم باید به نوعی بسیج شوند. [2:8]

۳. *نگرش تخصصی :* با توجه به آنکه فضای سایبر یک مفهوم جدید می باشد، نظام آموزشی و پژوهشی کشور باید سریعاً نسبت به آن واکنش نشان داده و پاسخ گوی این نیاز باشد. تاسیس رشته ها، دانشگاه ها، مؤسسات پژوهشی تخصصی در این زمینه ضرروری به نظر می رسد. [2:11]

۴. *بومی سازی فناوری :* با توجه به آن که وجود فناوری بومی در این زمینه می تواند منشاء خطرات و تهدیدات واقع گردد، با ترغیب نخبگان فناوری و قرار دادن فرصت های لازم به ایشان به این مهم اقدام نمود.

۵. *استقرار مقطعی و با برنامه :* فرهنگ سازی استفاده از فضای سایبر در کل جامعه و قراردادن زیرساخت های کشور به صورت برنامه ریزی های

کوتاه مدت، میان مدت و بلند مدت باید در برنامه اصلی دولت قرار گیرد. اضافه نمودن زیرساخت های اصلی کشور در فضای سایبر باید بر حسب اولویت و به صورت تدریجی صورت گیرد تا بازه های اطمینان در این زمینه به وجود آید. قرار دادن یک زیرساخت اصلی در فضای سایبر بدون بررسی همه جانبه امنیتی کاری نسنجیده بوده و تبعات جبران ناپذیری را دربر خواهد داشت.

۶. *ارتقای آموزشی*: ارائه یک برنامه آموزشی با هدف ارتقاء سطح دانش و آگاهی برای ایجاد امنیت ملی در فضای سایبر ضروری به نظر می رسد زیرا بسیاری از تهدیدات در این حوزه از ناحیه ضعف آگاهی و نبود مهارت لازم در بین مجریان و کاربران می باشد. [1:7]

۷. *برنامه ریزی کاهش تهدیدها*: ایجاد یک برنامه مشخص برای چگونگی کاهش و از بین بردن آسیب ها و تهدیدها در راستای تأمین امنیت ملی در فضای سایبر. در خصوص آسیب پذیری ها نیز باید به رشد فناوری ها، عدم کنترل مؤثر بر ابزارهای ارتباطاتی تازه و نداشتن تصویر روشن و قابل اتکایی از آینده اشاره داشت که این مسائل ما را در قبال امنیت فضای مجازی مردد می سازد.

۸. *تعاملات بین المللی*: برای ایجاد حداکثر ایمنی در فضای سایبر، ایجاد همکاری و انطباق لازم بین دو بخش امنیت ملی و بین المللی کاملاً ضروری است. در این فضا امنیت ملی و بین المللی، دو مفهوم مستقل از یکدیگر نیستند، بنابراین نمی توانیم نسبت به تهدیداتی که در خارج از فضای ملی اتفاق می افتند بی تفاوت باشیم. [1:8]

۹. *واکنش به تهدید در حداقل زمان ممکن*: یک سامانه واکنش مناسب برای تأمین امنیت فضای سایبر ملی ایجاد شود. با توجه به آن که تحولات در این حوزه سریع، عمیق و گسترده می باشد، ضروری است با همکاری بخش های خصوصی تمهیداتی به وجود آید تا واکنش های سیستم به صورت بی درنگ تعریف شود.[1:7]

❑ نتیجه گیری و پیشنهادها

تغییر نگرش دولت ها به استفاده از فضای سایبر و استفاده ازخدمات دولت الکترونیکی در عصر حاضر به عنوان یک اصل برای کشورهای توسعه یافته و همچنین یک راهبرد برای کشورهای کمتر توسعه یافته می باشد.

مسأله حائز اهمیت در این زمینه، امنیت این بستر ارتباطی است، به گونه ای که اگر این امنیت در بالاترین حد آن تامین نشود، استفاده از این فرصت به یک تهدید ملی تبدیل شده و صدمات جبران ناپذیری را به بار می آورد، زیرا راه های نفوذ به اطلاعات یک کشور و سعی در خرابکاری مخصوصا در بخش زیرساختارهای اصلی در این حوزه بسیار سریع تر و با آسیب پذیری خیلی زیاد امکان پذیر است.

تشکیل این کمیته ها، شناسایی عوامل غیر ایمن و شکاف های امنیتی در زیرساخت های اصلی کشور، مطالعه تطبیقی استقرار فضای سایبر در کشورهای توسعه یافته مخصوصا در کشورهای مسلمان مانند سنگاپور و مالزی، تعیین اولویت ها در استقرار فضای سایبر، ایجاد یک بستر ارتباطاتی ایمن، بومی سازی تجهیزات مورد استفاده در بخش های اصلی این فضا، توجه به تعاملات بین المللی در این زمینه، دادن آموزش های لازم به کلیه افرادی که به نحوی در این فضای مجازی قرار می گیرند، همگی از نکاتی هستند که باید مورد توجه مسئولین استقرار فضای سایبر در دولت واقع شود والا علاوه بر آنکه هزینه های بسیاری را بر دولت تحمیل می کند، باعث آسیب پذیری بخش های اصلی دولت مخصوصاً در ارتباط با زیرساخت های اصلی آن می گردد.

در سایه این اهداف و با رسیدن به یک فضای تعاملاتی ملی و بین المللی ایمن می توان به سه هدف اصلی توسعه، اقتدار و امنیت انسانی و اجتماعی بر طبق سند چشم انداز دست یافت.

با توجه به آنکه موضوع امنیت در فضای سایبر در ارتباط مستقیم با امنیت ملی کشور قرار دارد، دولت باید از طریق وزارت اطلاعات وظیفه برنامه ریزی راهبردی برای این مسأله را برعهده داشته باشد و از تخصص و توان موجود در شرکت های خصوصی و نهادهای غیردولتی (1NGO) نهایت استفاده را بنماید.

1. Non Government Organization

راهکارهای زیر در استقرار ایمن فضای سایبر توصیه می گردد.

۱. مسأله فضای سایبر و خطرات و تهدیدات آن در برنامه ملی امنیت کشور لحاظ شود.

۲. برنامه مدیریت بحران برای حملات احتمالی به زیرساخت های کشور در فضای سایبر تدوین شود.

۳. پروژه های تحقیقاتی به منظور یافتن راهکارها و امکانات جدید و کارامد برای تقویت امنیت داخلی تعریف گردد.

۴. همکاری مستمر بین بخش های دولتی و خصوصی به وجود آید، به گونه ای که بخش خصوصی توان مقابله با مشکلات امنیتی را دارا باشد و بتواند در زمان بحران ملی به کمک دولت بیاید.

۵. بومی سازی فناوری در بخش های مهم مانند دیواره های آتش ، تجهیزات شبکه ای مانند مسیریاب ها و غیره صورت پذیرد زیرا مهمترین عامل نشت و سرقت اطلاعات از کشورهای مصرف کننده فناوری از ناحیه تجهیزات واگذار شده به آن کشورها است.

همچنین در ارتباط با به کارگیری دولت الکترونیکی به عنوان مهم ترین ثمره استفاده از فضای سایبر و با توجه به مباحث مطرح شده می توان به این نتیجه رسید که برای استفاده امن و بهینه از سرویس های مربوط به دولت الکترونیکی باید گام های زیر توسط دولت برداشته شود: [17:10]

- ایجاد کمیته های تخصصی از نخبگان فناوری اطلاعات برای طرح ریزی راهبردی و هدایت پروژه ها؛
- زمانبندی با در نظر گرفتن اولویت در الکترونیکی کردن بخش های دولتی؛
- توجه به زیرساخت های اصلی کشور مانند آموزش و پرورش، ارتباطات، انرژی و غیره و سعی در ایمن سازی این زیرساخت ها به عنوان بخش های اصلی سامانه جامع دولت الکترونیکی؛
- آموزش شهروندان و عموم افراد جامعه برای دادن اطمینان به آنها در استفاده از سرویس های دولت الکترونیکی که برای این منظور

در ابتدا برخی از سرویس ها بـه هـر دو روش سـنتی و الکترونیکـی ارائه می گردد، سپس در یک زمانبندی مشخص بخـش سـنتی بـه تدریج حذف می گردد؛

- توجه کامل دولت به امنیت اطلاعات در دولت الکترونیکی مخصوصا در بخش های مربوط به مسائل اقتصادی و نظامی؛
- بومی سازی بسیاری از تجهیزات اسـتفاده شـده در زیرسـاختارهای مربوط به دولت الکترونیکی برای حصول اطمینـان از عـدم نـشت و سرقت داده ها مخصوصاً در بخش هایی که اطلاعات طبقه بنـدی و اسناد مهم مربوط به دولت و شهروندان نگهداری می گردد؛
- الحاق به کمیته های بین المللی از جمله کمیته فضای سـایبر اروپـا و همسان سازی راهبردهای خـود بـا سـایر کـشورها، مخـصوصاً در بخش های ارتباطی زیرا همان گونه که قبلاً عنـوان گردیـد امنیـت ملی در حد زیادی به امنیت بین المللی وابسته است.

❑ منابع :

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

۲. افتخاری، اصغر، ارکان پنج گانه استرانژی تأمین امنیت در فضای مجازی، پژوهشکده مطالعات راهبردی، ۱۳۸۲

۳. امنیت ملی در گروی امنیت اینترنتی– مقاله از سایت ITIRAN ، ۱۳۸۲

۴. امنیت فناوری اطلاعات در عصر دیجیتال ، شورای عالی اطلاع رسانی دولت، ۱۳۸۲

۵. بررسی فعالیت های داخلی و خارجی مرتبط با امنیت اطلاعات کشور – تهیه شده توسط مرکز تحقیقات مخابرات ایران – بهمن ۱۳۸۲

۶. پاک نظر، ثریا – دایره المعارف کامپیوتر – مؤسسه فرهنگی هنری دیباگران تهران – ۱۳۸۳

۷. تهامی سید مجتبی، امنیت ملی، دکترین و سیاست های دفاعی - امنیتی، جلد ۱، تهران، دانشگاه عالی دفاع ملی، چاپ سوم، دی ۱۳۸۰

۸. جراحی، محمدحسین - دولت الکترونیکی، فرصت‌ها، چالش‌ها و روند آینده – دانشگاه شهید بهشتی – مقاله ای از سایت itiran – ۱۳۸۳

۹. حسن بیگی، ابراهیم – حقوق و امنیت در فضای سایبر – مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر تهران – ۱۳۸۴

۱۰. سایت اینترنتی www.wefroum.com

۱۱. سلیمانی فرد، اکبر- آسیب پذیری شبکه های رایانه ای، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، تهران ، ۱۳۸۱

۱۲. فخار، سید محمد – کلیک روی دروازه های ایران الکترونیک – برگرفته از سایت www.aftab.ir- ۱۳۸۶

۱۳. فهیمی ، مهدی – جنگ های اطلاعات محور، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، فروردین ۱۳۸۱

۱۴. کلاهچیان، محمود – الگوی طراحی استراتژی امنیت ملی در جمهوری اسلامی ایران، پژوهشکده مطالعات راهبردی – ۱۳۸۳

15. Cyberspace - Threats and Vulnerabilities.
16. Darrell M. West - Global E-Government 2004 , Center for Public Policy Brown University Providence.
17. eGovernment in Germany – iDABC eGovernment Observatory – report of European Communities 2005
18. Government Information Quaterly 20 (2003) 389–394, 'E-government around the world, Lessons, Challenges and Future Directions'; Paul T. Jaeger and Kim M. Thompson (2003)
19. Matsuura, Jeffrey H. The Impact of National Infrastructure and Cyberspace Security Strategies on Legal Rights and Liabilities
20. Moteff, John. What Makes an Infrastructure Critical? - Congressional Research Service – 2003
21. Stephen Smith - Key Factors in E-Government Information System Security - 18th Bled eConference eIntegration in Action - Slovenia, June 6 - 8, 2005

راهنمای تهیه و ارسال مقاله های علمی پژوهشی

فصلنامهٔ مطالعات دفاعی‌استراتژیک دانشگاه عالی دفاع ملی ستاد کل نیروهای مسلح به منظور ارائه تازه‌ترین نظریه‌ها و یافته‌های علمی در حوزه‌های علوم دفاعی، امنیت ملی و مدیریت استراتژیک و همچنین به منظور تبادل و نشر افکار و اندیشه‌های بدیع، از اندیشمندان، صاحب نظران، دانش‌پژوهان، کارشناسان و دانشجویان مقطع دکتری دعوت می نماید تا با مدنظر قرار دادن نکات زیر، دانسته‌ها و یافته‌های خود را در قالب مقالات علمی- پژوهشی برای چاپ و انتشار در فصلنامه دانشگاه به آدرس اعلان شده ارسال نمایند:

❑ راهنمای تهیه مقاله

۱- مقاله در محیط نرم افزاری word ۲۰۰۲، (حاشیه از بالا ۲/۷، پایین ۷/۵۹، چپ ۴ و راست ۵ سانتی متر) در حدود ۲۰ صفحه روی کاغذ A۴ تایپ شود و چهار نسخه از مقاله به همراه دیسکت (فایل pdf&word)، به آدرس فصلنامه ارسال شود.

۲- مقاله‌های ارسالی باید دارای بخش‌های زیر باشد:

۱-۲- صفحه‌ی اول مقاله شامل: عنوان کامل مقاله، چکیده‌ی مقاله به زبان فارسی که نشان دهنده مسأله مورد بحث در مقاله، هدف آن، روش تحقیق و نتیجه‌گیری، مجموعاً حدود ۲۰۰ کلمه، همراه با واژه‌های کلیدی (حداکثر ۵ واژه)، نام نویسنده یا نویسندگان (نام نویسندهٔ عهده‌دار مکاتبات با علامت ستاره مشخص شود.) رتبه‌ی علمی، نام مؤسسه، دانشگاه و یا محل اشتغال، نشانی کامل نویسنده‌ی عهده‌دار مکاتبات شامل: نشانی پستی، شماره تلفن، نمابر و پست الکترونیکی.

۲-۲- صفحه‌ی دوم تا انتهای مقاله شامل مقدمه و متن که در آن به بحث و بررسی دربارهٔ مسأله واهمیت آن، مروری بر پیشینه‌ی موضوع، پرسش‌ها، یا فرضیه‌های پژوهش، روش تحقیق، فنون تجزیه و تحلیل اطلاعات و یافته‌های پژوهش پرداخته می شود و پس از نتیجه گیری و ارایه‌ی پیشنهادها در انتهای مقاله فهرست منابع و مآخذ آورده می شود.

۳-۲- چکیده انگلیسی مقاله که بر روی صفحه‌ای جداگانه همراه با عنوان مقاله، نام نویسنده یا نویسندگان، مرتبه علمی آنها، مؤسسه، دانشگاه یا محل اشتغال، ارسال می‌شود.

۳- ارجاعات در متن مقاله انجام می‌گیرد. برای این کار باید شماره مرجع در فهرست منابع مقاله و شماره صفحه مورد ارجاع در میان دو قلاب ذکر شود. این دو شماره با دو نقطه از هم جدا می‌شوند.[شماره صفحه: شماره مرجع]

۱-۳- در تمام ارجاعات از اعداد فارسی استفاده می‌شود[۲۱۴:۹].

۲-۳- استناد به متن کتب مقدس (قرآن، تورات، انجیل و...) و قوانین موضوعه در میان قلاب و بر اساس تقسیمات یا شماره‌های خاص آنها صورت می‌گیرد. [۲۱۴:بقره] [ماده ۸۶، بند ۳]

۴. یادداشت‌های نویسنده یا مترجم و توضیحات اضافی در پاورقی آورده می‌شود.

۵. معادل های واژگان فارسی یا زبان های دیگر در متن و بین دو کمان ذکر می‌شود.

۶- در پایان مقاله، منابع مورد استفاده در متن مقاله به ترتیب شماره‌ای که در داخل متن آمده، به شرح زیر آورده شود:

۱-۶- کتاب: نام خانوادگی، نام. (سال انتشار)/ نام کتاب با حروف ایتالیک، نام مترجم، محل انتشار، نام انتشارات.

۲-۶- مقاله: نام خانوادگی، نام نویسنده.(تاریخ انتشار)."عنوان مقاله داخل گیومه"نام نشریه با حروف ایتالیک؛ دوره (جلد)، محل انتشار.

۳-۶- موارد بدون نام، بدون تاریخ یا بدون محل نشر به ترتیب با عبارت: بی‌نا، بی‌تا و بی‌جا مشخص می‌گردد.

۴-۶- اگر کتابی دارای چند مجلد باشد تنها مجلداتی که بدان‌ها ارجاع شده فهرست خواهد شد؛ اما اگر مجلدات مختلف مورد ارجاع باشند باید مشخصات هر یک جداگانه فهرست شود.

۵-۶- بین شماره‌های مجلدات یا چاپ‌های یک اثر در فهرست منابع نباید فاصله باشد.

۶-۶- در فهرست منابع به‌ترتیب، ابتدا منابع فارسی سپس منابع عربی و پس از آن منابع انگلیسی، فرانسوی و آلمانی... ذکر می‌شود.

۶-۷- مؤلف می‌تواند منابعی را که در مقاله به‌طور مستقیم مورد ارجاع نبوده، اما در تهیه مقاله استفاده شده است، تحت عنوان کتاب شناسی پس از فهرست منابع ذکر کند.

۶-۸- در مورد گزارش‌ها و سایر منابع نیز اطلاعات کافی و کامل ارایه شود.

۷- مقاله‌ارسالی نباید در مجله‌های فارسی زبان داخل و خارج کشور چاپ شده باشد. همچنین نباید به صورت همزمان به مجله‌ی دیگر ارسال شده باشد.

۸- مجله از نشر مطلب با نام‌های غیره واقعی معذور است. لذا لازم است تصویر مدرک معتبری که حاکی از هویت واقعی ارسال کننده باشد ضمیمه مقاله گردد.

۹- درجه علمی یا مدرک تحصیلی نویسنده تنها پس از احراز، در مجله درج خواهد شد. بدین منظور فرد می‌تواند تصویر آخرین مدرک یا حکم درجه علمی خود را به همراه مقاله ارسال کند و مسئولیت آن با خود نویسنده می باشد.

۱۰- مقالات دانشجویان کارشناسی ارشد و مقالات برگرفته شده از پایان نامه‌های کارشناسی ارشد و دکتری تنها با تأیید آن توسط استاد راهنما پذیرفته می‌شود.

۱۱- فصلنامه در ویرایش مقاله‌ها، بدون تغییر در محتوای آن آزاد است.

۱۲- فصلنامه از پذیرش مقالاتی که موارد شکلی و ساختاری آورده شده در این راهنما در آن‌ها رعایت نشده باشد معذور است.

۱۳- مقالات رسیده عودت داده نمی‌شود.

❑ چگونگی تدوین "معرفی یا نقد کتاب، پژوهش یا پایان نامه ها"

۱- حجم نقد از ۷ صفحه‌ی A۴ بیشتر نباشد(هر صفحه ۲۵۰-۲۰۰ کلمه با قلم لوتوس ۱۳).

۲- معرفی کتاب یا پژوهش نباید بیش از یک چهارم آن را به خود اختصاص دهد.

۳- اولویت فصلنامه برای درج، معرفی یا نقد با کتب لاتین (انگلیسی)، گزارش پژوهش‌های میدانی و پایان نامه‌های دکتری می‌باشد.

۴- در نقد کتاب‌ها و نوشته‌ها رعایت سه گونه نقد ذیل ضروری است:

الف) نقد شکلی: شامل کاستی‌های چاپ، چارچوب، فصل‌بندی و سازماندهی مطالب.

ب) نقد روشی: شامل بررسی متدها، ابزارها، شاخص سازی، فرضیه‌ها، نمونه گیری و.....

ج) نقد محتوایی: در این بخش میزان توفیق یا عدم توفیق نویسنده، در دست یابی به اهداف و یافته‌های مورد نظر نویسنده، مورد نقد قرار می‌گیرد.

۵- معرفی و نقد با نرم افزار word۲۰۰۲ حروف چینی شده باشد(پس از پذیرش نقد، ارسال لوح فشرده یا دیسکت آن ضروری است).