فصلنامه مطالعات جنگ
سال سوم، شماره هشتم، بهار ۱۴۰۰
مقالهٔ پنجم از صفحه ۸۷ تا ۱۰۹

مصون‌سازی زیرساخت‌های سایبری کشور در برابر تهدیدهای آمریکا

دکتر محمد سپهری[۱]

دریافت مقاله: ۱۴۰۰/۰۱/۲۷ پذیرش مقاله:۱۴۰۰/۰۳/۰۳

چکیده

توسعه سامانه‌های سایبری در زندگی روزمره مردم و دولت ها، این فضای جدید را به صورت کاملا جدی و هدفمند به یکی از عرصه‌های جنگ و تقابل میان کشورها و دولت‌ها تبدیل نموده، بطوری که امروزه دفاع در فضای سایبری تبدیل به عرصه پنجم جنگ‌ها و تقابل تبدیل و مفهوم جدید سایبر در چارچوب های تهدیدهای متفاوت و متنوعی ظهور پیدا نموده است. مقاله حاضر به بررسی تهدیدهای مختلف فضای سایبری می پردازد و سوال اصلی مقاله، زیرساخت‌های سایبری را چگونه در برابر تهدیدهای سایبری آمریکا می‌توان مصون ساخت؟ و نتایج مقاله حاکی از راه کارهای هم‌افزایی منابع ملی در برابر تهدیدهای فضای سایبری جهت مقابله با تهدیدهای این حوزه می باشد و سپس با استفاده از جمع‌آوری اطلاعات بصورت اسنادی، راه کارهایی هم‌افزایی منابع به منظور کاهش آسیب پذیری و مقابله با تهدیدهای سایبری را ارائه می‌نماید.

واژگان کلیدی: دفاع سایبری، تهدیدهای سایبری، مصون‌سازی.

[۱] – عضو هئیت علمی دانشگاه پدافند هوایی خاتم الانبیاء(ص)

مقدمه

طی سال‌های اخیر، تهدیدات سایبری علیه جمهوری اسلامی ایران، جهش بی‌سابقه‌ای یافته و از روندی به‌شدّت فزآینده برخوردار بوده است. یکی از اصول تهاجم در هر فضای عملیاتی، اصل غافلگیری و متناظراً یکی از اصول دفاع، اصل پیش‌بینی حرکت بعدی دشمن است. بر این اساس، برآورد و پایش تهدیدهای سایبری کشور، در تمامی وضعیت‌های سایبری از صلح تا جنگ سایبری و اساساً به عنوان پیش‌نیاز تعیین سطح هشدار یا تعیین وضعیت سایبری کشور، در نظر گرفته شده است. فضای سایبر، اگرچه پس از زمین، دریا، هوا و فضا، به عنوان فضای پنجم نبردهای نظامی در نظر گرفته شده است، لیکن بواسطه برخورداری از تفاوت‌های عمده از قبیل تغییرات بسیار سریع، گسترده و مداومِ فضای سایبر، گمنامی کاربران در این فضا و بی‌مرزی حاکم بر آن، نسبت به سایر محیط‌های عملیاتی فوق‌الذکر، از ویژگی‌های منحصر به فردی برخوردار است. در این فضا، غافلگیری بسیار ساده‌تر از سایر فضاهای عملیاتی و پیش‌بینی، به مراتب مشکل‌تر از سایر محیط‌ها می‌باشد و پیش‌بینی انجام شده در خصوص فضای سایبر، از طول عمر به مراتب کمتری برخوردار است.

جنگ‌های امروزی و آتی بر علاوه بر فناوری‌های مختلف دفاعی بر مبنای فناوری‌های سایبری در حوزه فناوری اطلاعات و ارتباطات به منظور حمله و دفاع همه جانبه طرح‌ریزی و اجرا می‌گردد. دفاع همه جانبه از کشور مستلزم شناخت کافی از توانمندی‌های و فناوری‌های دشمن در تمامی حوزه‌های هوایی، فضایی، دریایی و زمینی و سایبری به عنوان بعد پنجم جهت مقابله با آنان می‌باشد. رشد سریع فضای سایبر بستری جدید و مهم در سیاست جهان است. هزینه پائین ورود، گمنامی و ناهمگون بودن در آسیب‌پذیری بدین معناست که بازیگران کوچکتر در فضای سایبر نسبت به حوزه‌های سنتی‌تر سیاست جهانی ظرفیت بیشتری برای اعمال قدرت سخت و نرم دارند. تغییرات بوجود آمده در اطلاعات همیشه تاثیر مهمی بر قدرت داشته‌اند، اما حوزه سایبر یک محیط مصنوعی جدید و غیرقابل پیش‌بینی است. ویژگی‌های فضای سایبر برخی از اختلافات قدرت بین بازیگران را کاهش داده و بدین ترتیب مثال خوبی از پراکندگی قدرت را که ویژگی سیاست جهانی در قرن حاضر است، به نمایش می‌گذارد. قدرت‌های بزرگ نخواهند تنوانست به اندازه حوزه‌هایی چون دریا، خشکی، هوا وفضا بر این حوزه مسلط شوند. نکته دیگری که فضای سایبر بر آن تاکید می‌کند این است که پراکندگی قدرت به معنای برابری قدرت یا جایگزینی دولت ها به عنوان قدرتمندترین بازیگران سیاست جهانی نیست. و سایبر بعد پنجم در جنگ‌ها شناخته می‌شود.

بیان مسئله و ضرورت و اهمیت تحقیق:

با توجه به اهمیت فناوری اطلاعات و ارتباطات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار فناوری اطلاعات، این بستر به یکی از نقاط بالقوه و بالفعل تهدید، آسیب‌پذیری و خطرآفرینی در جهان تبدیل شده است. ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند هم‌افزایی منابع در راستای تهدیدهای حوزه سایبری به منظور مصون‌سازی فضای سایبری کشور در برابر تهدیدهای این حوزه می‌باشد. بطوری که هم‌افزایی منابع در دفاع سایبری در برابر تهدیدهای مختلف سایبری، موجب کاهش آسیب‌پذیری و ایمن‌سازی شبکه فناوری اطلاعات و ارتباطات کشور، افزایش بازدارندگی و تولید قدرت سایبری، تداوم فعالیت‌های ضروری سایبری، ارتقاء پایداری زیرساخت‌های کشور در برابر تهدیدهای سایبری، بومی‌سازی و تولید نرم افزارهای اصلی و اساسی، تسهیل مدیریت بحران در زیر ساخت‌های کشور در برابر تهدیدهای سایبری و بومی‌سازی و تدوین الگو و مدل دفاع سایبری کشور می گردد. عدم هم‌افزایی منابع ملی در برابر تهدیدهای سایبری، باعث کاهش توان دفاع سایبری کشور در تمامی زیرساخت‌های حیاتی، حساس و مهم و موجب فلج سازی راهبردی بخش‌های مختلف فناوری اطلاعات و ارتباطات و شبکه ها و مراکز داده‌ها و تمامی بخش‌های رایانه‌ای و صنایع و تجهیزات وابسته به آن می‌گردد.

هدف اصلی تحقیق:

مصون‌سازی زیرساخت‌های سایبری کشور در برابر تهدیدهای سایبری آمریکا.

اهداف فرعی:

۱. تجزیه و تحلیل تهدیدهای سایبری موجود در زیرساخت‌های حیاتی، حساس و مهم کشور.
۲. الزامات مورد نیاز جهت هم‌افزایی منابع کشور در برابر تهدیدهای سایبری.

سئوال اصلی تحقیق:

زیرساخت‌های سایبری کشور را چگونه در برابر تهدیدهای سایبری آمریکا می‌توان مصون ساخت؟

سئوالات فرعی تحقیق:

۱. تهدیدهای سایبری موجود در زیرساخت‌های حیاتی، حساس و مهم کشور کدامند؟.
۲. الزامات مورد نیاز جهت هم‌افزایی منابع کشور در برابر تهدیدهای سایبری کدامند؟

نوع و روش تحقیق:

نوع پژوهش از نظر هدف کاربردی است و با توجه به این که برای اولین بار انجام می‌شود توسعه‌ای محسوب می‌شود و این تحقیق به روش موردی- زمینه‌ای انجام شده است.

روش گردآوری اطلاعات و تحلیل:

در این تحقیق برای جمع آوری اطلاعات از روش کتابخانه‌ای با استفاده از کتابخانه تخصصی و مطالعه اسناد و مدارک موجود و ابزار آن بررسی اسناد، مدارک، آرشیو، کتاب، اینترنت و استفاده از اطلاعات موجود در وبگاه‌ها می‌باشد.

مبانی نظری

فضای سایبر

رایانه‌های به هم متصل شده، سرورها، روترها، سوئیچ‌ها و کابل‌ها که زیر ساخت‌های حیاتی بوسیله آنها کار می‌کنند را فضای سایبر می‌گویند. یا به عبارتی فضای جنگ در جنگ سایبری، سرویس‌ها و شبکه‌های زیرساخت‌های اطلاعاتی در سطوح جهانی، ملی و دفاعی است. اینترنت، شبکه‌ها و سرویس‌های خدمات ارتباطی، شبکه‌های عمومی داده، شبکه‌های تجاری ماهواره‌ای ، شبکه‌های رادیویی و تلوزیونی و شبکه‌هایی از این دست، این فضا را تشکیل می‌دهد. کلیه عناصر و اجزای مورد استفاده در زیرساخت‌های اطلاعاتی شامل رایانه ها، اجزای شبکه، دیسک‌های فشرده، دوربین- ها، کابل‌ها، صفحه کلیدها عناصر شرکت کننده در جنگ‌های اطلاعاتی می‌باشند. (ابراهیم‌نژاد،۱۳۸۹: ۸۶)

زیرساخت‌های سایبری

دولت آمریکا، زیرساخت سایبری را به عنوان محیطی تعریف نموده است که امکانات اکتساب داده‌ها، ذخیره‌سازی داده‌ها، مدیریت داده‌ها، تجمیع داده‌ها، داده‌کاوی، مصورسازی داده‌ها، سرویس- های دیگر توزیع شده محاسباتی و پردازش اطلاعات که در سطح اینترنت و نه در یک موسسه خاص وجود دارند، تعریف نموده است.(K.F. Rauscher and V. Yaschenko, 2012:34)

زیرساخت‌های سایبری شامل:

۱. محیط سایبری: شامل ساختمان‌ها، مکان‌های آنتن‌های مخابراتی و فضا که مدار ماهواره‌ها در آن قرار دارد، کف دریاها که محل قرارگیری کابل‌ها می باشد .
۲. توان(قدرت): شامل برق، باتری‌ها، ژنراتورها می‌باشد.

۳. سخت‌افزار: شامل تراشه‌های نیمه هادی، کارت‌های الکترونیکی، تجهیزات انتقال سیستمی و نوری می‌باشد.
۴. نرم‌افزار: شامل متن برنامه‌ها، برنامه‌های اجرایی، برنامه‌های کنترل نگارش و مدیریت، پایگاه داده‌ها می‌باشد.
۵. شبکه و اتصالات: شامل گره‌ها، اتصالات، همبندی‌ها می‌باشد.
۶. محتوی: اطلاعات انتقالی از طریق زیرساخت، آمارها و الگوهای ترافیک می‌باشد.
۷. عوامل انسانی: شامل طراح ها، پیاده سازها، اپراتورها، کارمندان نگهداری می‌باشد.
۸. سیاست: شامل موافقت نامه‌ها، استانداردها، خط مشی و مقررات می‌باشد.

(WWW://en.wikipedia.org/wiki/Cyberinfrastructure, Visited: 2012-02-19)

جنگ سایبر[1]

استفاده از کامپیوترها به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت ترساندن و یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی و یا آرمانی انجام می‌گیرد و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل‌ونقل، ارتباطات، سرویس‌های ضروری مانند پلیس و خدمات پزشکی را هدف قرار می‌دهد و از شبکه‌های کامپیوتری به عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند. مفهوم سایبر در ابتدا در چارچوب‌ها و کارکردهای متفاوتی شکل‌گیری پیداکرده است. هر چند مفهوم اصلی دفاع، جنگ و امنیت سایبری در ارتش آمریکا شکل گرفته، اما با توجه به گذشت زمان و بوجود آمدن تحولات و پیشرفت‌ها در مفاهیم و تعاریف سایبری، جدای از کارهای نظامی که جزء کارکردهای اساسی و اصلی آن بوده، کارکردها و عملکردهای متفاوت و متنوعی بر آن افزوده شده‌است. از سوی دیگر مفاهیم و ابزارهای سایبری در زندگی روزمره مردم، این فضای جدید را به صورت کاملا جدی و هدفمند به یکی از عرصه‌های تقابل میان کشورها و قدرت‌های دنیا تبدیل کرده‌است. تا جایی که بسیاری از استراتژیست‌های جهان امروز جهان بر این عقیده‌اند که فضای جنگ سایبری، عرصه پنجم از تقابل و تهاجم میان قدرت‌های دنیا می باشد. بر همین اساس، در جدیدترین راهبرد اعلام شده توسط دولت آمریکا که در تاریخ پنجم ژانویه ۲۰۱۲ اعلام شد، شاهد تشکیل ساز و کارهای تهاجم و تدافع سایبری در سطح کلان در این کشور می باشیم. (جلالی،۹۱: ۱۱۳)

[1]- CYBER WARFARE

رسالت دفاع سایبری

تأمین و توسعه امنیت، ایمنی و پایداری در فضای تبادل اطلاعات کشور می‌باشد.

ماموریت دفاع سایبری

سیاست‌گذاری، هدایت، نظارت راهبردی و توسعه امنیت، ایمنی و پایداری فضای تبادل اطلاعات کشور و پشتیبانی از برنامه دستگاه‌ها و بخش‌های زیرساختی در جهت کاهش آسیب در برابر تهدیدات و جنگ از طریق ساماندهی و بکارگیری منابع و ظرفیت های ملی می باشد. (اسکندری، ۱۳۸۹: ۱۱۲)

تهدید سایبری

تعریف تهدید عبارت است از : "هر پیشامد یا رویدادی که پتانسیل واردنمودن ضربه‌ی خصمانه به فعالیت‌های سازمان (شامل ماموریت، وظایف، تصویر یا اعتبار)، سرمایه‌ها یا پرسنل سازمان از مسیر سامانه‌های اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر و یا ممانعت از ارائه خدمت را داشته باشد". در راهنمای ارزیابی مخاطرات موسسه ملی استاندارد و فناوری آمریکا [۲۱]، تهدید با عبارت "هرگونه پیشامد یا رویداد با پتانسیل ضربه متخاصمانه به عملیات سازمان، سرمایه‌ها، افراد، سازمان‌های دیگر یا کشور، با استفاده از یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء یا تغییر اطلاعات و یا ممانعت از سرویس"، تعریف شده است. در مستند مأموریت‌ها، ساختار تشکیلات و شرح وظایف قرارگاه دفاع سایبری کشور [۳۱] ، تعریف ارائه شده برای تهدید سایبری عبارت است از : "عامل خارجی با قابلیت وارد نمودن ضربه فاجعه بار امنیت، منافع و اقتصاد ملی، وجهه و روابط بین‌المللی، سلامت، ایمنی و اطمینان عمومی، باورهای دینی و ملی یا اداره‌ی امور کشور، از طریق تخریب یا ایجاد اختلال گسترده در عملکرد سرمایه‌های ملی سایبری کشور"

اشکال مختلف تهدیدهای سایبری بر علیه زیرساخت‌های کشور

تهاجمات سایبری اثر بخش به شکل های زیر انجام می شود :

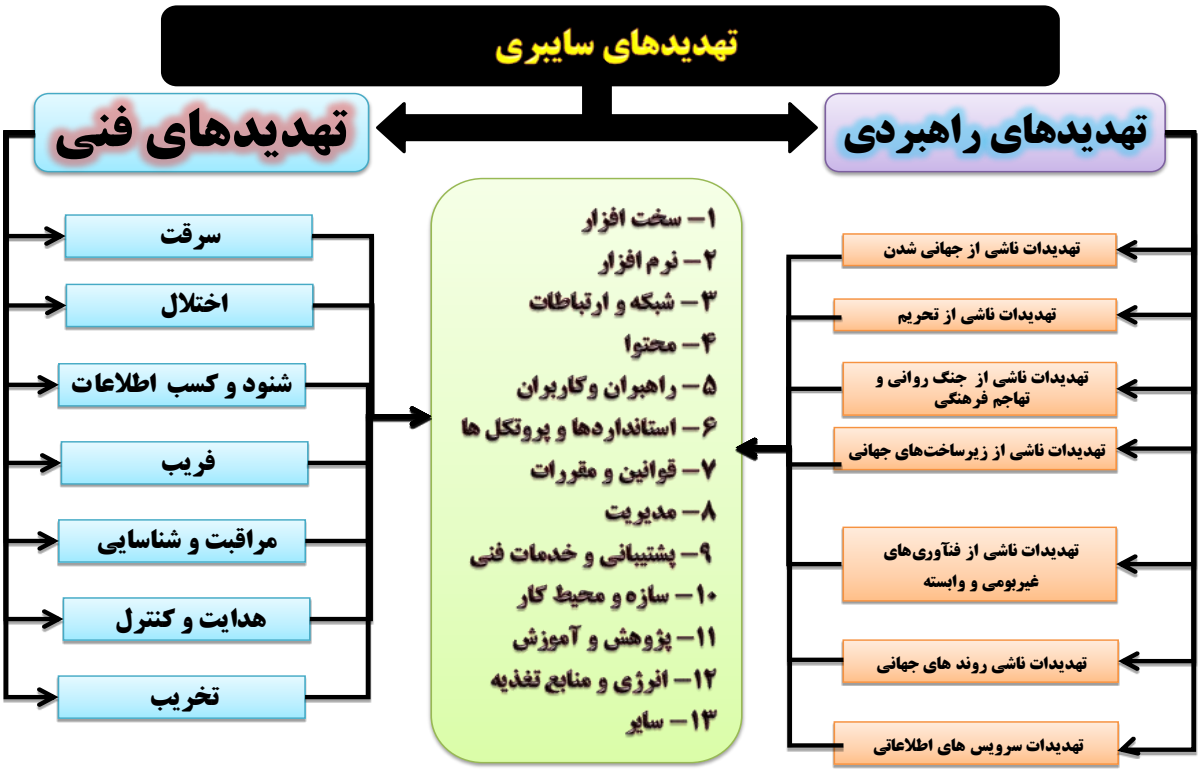
۱. توقف سرویس‌دهی زیرساخت: یکی از اولین تبعات یک تهاجم سایبری، توقف سرویس دهی است که می‌توان با اقدامات پیشگیرانه، آنرا به تاخیر انداخت.
۲. توقف زیرساخت: این حد از اثر بخشی تهاجم سایبری جایی است که خدمات رسانی و گردش امور زیرساخت متوقف شده و از کار می‌افتد.

۳. تخریب زیرساخت: این بخش از تهاجم، بیشتر از طریق بدافزارهای ویژه و خاصی انجام می‌گیرد که می‌تواند بخش مهمی از زیر ساخت را از بین برده و حتی تا انفجار و آتش سوزی ادامه یابد.

۴. تهدید امنیت ملی: در این بخش از تهدید، روش برخورد و شناسایی تهدید بسیار جدی و سریع بوده و دارای ویژگی‌های امنیتی و دفاعی می‌باشد. (جلالی، ۱۳۹۱: ۱۳۳)

تهدیدهای سایبری

تهدیدهای سایبری شامل تهدیدهای راهبردی و تهدیدهای فنی زیر می‌باشند:



شکل ۱- تهدیدهای سایبری بر علیه کشور (پورابراهیم:۱۳۹۲: ۱۶)

منشاء و ماهیّت تهدیدات سایبری خصمانه دشمن

در طرح قابلیت‌های مفهومی ارتش آمریکا برای عملیات در فضای سایبر طی سال‌های ۲۰۱۶ تا ۲۰۲۸ ، بازیگران تهدید، به هشت دسته‌ی دولت‌های سنّتی، افراد غیرنظامی، شرکت‌های چندملّیتی، سازمان‌های تبهکاری، تروریست‌ها، اتحادیه‌های هکری، هکرهای بدجنس(شیطان) و افراد بی‌توجّه و غیر بدخواه تفکیک شده‌اند. سند دکترین عملیات سایبری نیروی هوایی آمریکا (U.S

Secretary of the Air Force, 2010:14)، تهدیدات سایبری را از منظر منشاء تهدید، به دوازده دسته‌ی دولت‌ها (ارتش سایبری کشورها)، بازیگران چند ملّیتی، سازمان‌های تبهکاری، افراد یا گروه‌های کوچک و خودی‌ها، سنّتی، بی‌قاعده، فاجعه‌بار، مختل‌کننده، طبیعی و غیرمترقّبه طبقه‌بندی نموده است. طرح قدرت سایبری ناوگان دریایی در سال ۲۰۲۰ (U.S. Global Leadership, 2012: 14)، تهدیدات سایبری را از منظر بازیگران تهدید، به هفت دسته‌ی دولت‌ها، تروریست‌ها، اشخاص هکر، خودزن‌ها، گروه‌های سازمان‌یافته هکر دارای انگیزه سیاسی، خودی‌ها و سازمان‌های تبهکاری تفکیک نموده است. در گزارش تلاش‌های سایبری وزارت دفاع (**U.S ,2011: 6** Government Accountability Office)، تهدیدات سایبری از منظر منشاء تهدید به شش دسته‌ی سرویس‌های امنیتی کشورهای بیگانه، گروه‌های مجرم، هکرها، هکرهای دارای انگیزه سیاسی، خودی‌ها، تروریست‌ها تفکیک شده‌اند. جوزف نای در کتاب آینده‌ی قدرت(**جوزف اس. نای، ۱۳۹۰: ۳۲**)، بازیگران فضای سایبر را به سه دسته‌ی دولت‌ها، سازمان‌های دارای شبکه‌های بسیار پیچیده و شبکه‌های دارای ساختار ضعیف تفکیک نموده است، لیکن اشاره دارد که با توجه به تفاوت بسیار زیاد توان برخی دولت‌ها با سایر دول و همچنین اجزاء دو دسته‌ی دیگر، می‌توان تعداد این سطوح را افزایش داد.

در راهنمای ارزیابی مخاطرات موسسه ملی استاندارد و فناوری آمریکا (Computer Security Division,2012:17)، تهدیدات از منظر منشاء، به چهار دسته‌ی خصمانه، غیرمترقّبه، ساختاری و محیطی تفکیک شده‌اند. همچنین منشاء تهدیدات متخاصمانه به چهار دسته‌ی افراد، گروه‌ها، سازمان‌ها و دولت‌ها تفکیک شده‌اند. در مقاله مفاهیم پایه در جنگ سایبری(Lior Tabansky, 2011:3)، تهدیدات سایبری از منظر منشاء به هشت دسته‌ی هکرهای دارای انگیزه سیاسی، هکرها، نویسندگان بدافزار، گردانندگان شبکه‌های بات، مجرمین سازمان‌یافته، کارکنان، سرویس‌های امنیتی و تروریست‌ها تفکیک شده‌اند.

در کتاب جغرافیای سیاسی فضای مجازی (حافظ نیا، ۱۳۹۰: ۲۷)، تهدیدات سایبری خصمانه، در سه دسته با عناوین تهدیدات خارجی(از نوع تهدیدات نظامی، امنیتی با منشاء دولت‌ها و گروه‌های سازمان‌یافته)، تهدیدات تروریستی (با منشاء گروه‌های افراطی و تروریستی)، تهدیدات جنایی (جنایت‌کاران و مجرمان انفرادی یا گروهی) و تهدیدات داخلی یا درون‌مرزی (با منشاء درون‌کشوری یا درون‌سازمانی) تفکیک شده‌اند و از میان انواع فوق، دو نوع اوّل تهدیدات، به این دلیل که امنیت

ملی و زیرساخت‌های کشور مورد تهدید را هدف قرار می‌دهند، دارای ماهیت نظامی و دفاعی شناخته شده‌اند. همچنین مطرح شده است که فضای سایبر در سه حوزه‌ی ذیل، با جنگ ارتباط دارد:

الف – استفاده از ظرفیت‌های فضای سایبر برای عملیات نظامی در فضای واقعی

ب – تبدیل فضای سایبر به عرصه‌ی جنگ سایبری، از طریق تشکیل ارتش سایبری و ایجاد الگوی رزم در فضای سایبر

ج –استفاده از فضای سایبر برای عملیات و جنگ روانی

البته باید توجه داشت که بر اساس واژه‌نامه دوجانبه اصطلاحات حیاتی امنیت فضای سایبر روسیه و آمریکا، همچنین اسناد راهبردی مستقل ارتش آمریکا، از جمله راهبرد وزارت دفاع، برای عملیات در فضای سایبر، حالت دوم از سه حالت فوق، به عنوان تعریف جنگ سایبری، پذیرفته و شناخته شده است.(U.S Department of Defense ,201:33)

سطوح تهدیدهای سایبری علیه کشور ما

سطح فردی: هرگاه سطح تهاجم و تهدید علیه کشور، محدود به یک فرد خاص مانند هکر و یا متجاوز شود، سطح امنیت و تدابیر مقابله با آن بایستی متناسب با آن باشد. حیطه‌ی خطر در این سطح، بیشتر بخش‌های تدابیر مقابله با تهدید در این سطح، راه‌کنشی(تاکتیکی) می‌باشند.

سطح اجتماعی: هنگامی که تهاجم توسط یک گروه هکری انجام شود و یا امنیت سایبری بخشی از اجتماع به خطر بیفتد، می توان با اتخاذ تدابیر کارکردی و مهم، از بروز و پیشرفت آثار تهاجم سایبر سایبری پیشگیری نمود.

سطح امنیت ملی: در این سطح می‌تواند قدرتی در حد یک دولت به عنوان پشتیبان حمله شناخته شود. در این دسته ار تهاجمات، زیر ساخت‌های حیاتی کشور مورد هدف قرار می‌گیرد. در این سطح از تهاجم، حیطه ملی مورد هدف و تهاجم قرار گرفته و یا با حیطه‌بندی منطقه‌ای اما با تاثیری ملی می‌باشد. علی‌رغم این که نمونه‌ای از وقوع این تهدید تا سطح بین‌المللی تاکنون مشاهده نشده، اما باید توجه داشت که این موضوع به هیچ وجه محال و دور از ذهن نیست. با این ویژگی که منشاء تهدید ترکیبی بوده و زیر ساخت‌های بین‌المللی را هدف قرار دهد و تا سطح بین‌المللی نیز، سطح درگیری را ارتقا دهد. (جلالی، ۱۳۹۱: ۱۳۰-۱۳۴)

اهداف دفاع سایبری در برابر تهدیدات

۱. کاهش آسیب‌پذیری و ایمن‌سازی شبکه فناوری اطلاعات و ارتباطات کشور.
۲. افزایش بازدارندگی و تولید قدرت در حوزه سایبری.
۳. تداوم فعالیت های ضروری سایبری و ارتباطی کشور.
۴. ارتقاء پایداری زیر ساخت‌های سایبری کشور در برابر اقدامات و تهدیدهای سایبری.
۵. بومی‌سازی و تولید نرم افزارهای اساسی و پایه.
۶. تسهیل مدیریت بحران در زیر ساخت‌های حیاتی، حساس و مهم کشور در برابر تهدیدهای سایبری.
۷. بومی‌سازی و تدوین الگو و مدل دفاع سایبری بومی کشور. (جلالی:۱۳۰)

پدافندغیرعامل در تامین امنیت فضای تبادل اطلاعات

به هرگونه اقدام با هدف ایجاد اختلال، ناکارآمدی یا محروم سازی از منابع موجود در فضای تبادل اطلاعات، جنگ سایبر اطلاق می‌گردد. چنین عملیاتی بطور مشخص با اهداف تهدید امنیت و یا حفظ امنیت در ابعاد ملی انجام می‌پذیرد. جنگ سایبر دارای اهمیت روزافزون برای بخش‌های دفاعی و امنیتی، اقتصادی و تجاری، سیاسی، فرهنگی است. لازمه یک دفاع موفق در جنگ سایبر همانا بالا بردن سطح امنیتی عناصر درگیر است و این مهم جز با افزایش دانش در حوزه سایبر میسر نخواهد بود. بر اساس استانداردهای امنیتی قابل قبول، بطور خلاصه هر یک از عناصر درگیر در فضای سایبر، باید به اندازه ارزش خود حفاظت گردند. در غیر این صورت، انتخاب مکانیسم‌های دفاعی چندان بهینه نخواهد بود و بدون شک دارای هزینه‌های غیر ضرور است. بدیهی است آنهایی که قصد حمله داشته باشند تا دندان مسلح می‌شوند. پس باید ابتدا دارائی‌ها و عناصراصلی و اساسی اطلاعاتی اشیاء مهم در فضای سایبری را تعریف و تعیین نموده و براساس سیاست‌های کلان و با در نظر گرفتن تمامی تهدیدات، باید همه تمهیدات دفاعی را پی‌ریزی نمائیم.
(WWW.PAYDARIMELLI.IR 92/05/10)

روش‌های حملات سایبری

۱. روش حمله خاموش[۱]: این حملات شامل فعالیت‌هایی می‌شوند که در آنها بدون انجام هرگونه فعالیت ظاهری یا ایجاد تغییرات در سیستم‌های آسیب‌پذیر، به آنها نفوذ شده و منجر به سوء استفاده از منابع سیستم می‌گردد.

۲. روش حمله فعال[۲]: حملاتی هستند که به سامانه‌های کامپیوتری زیرساخت‌های حیاتی نفوذ می‌کنند و می‌توانند اطلاعات حساس را دستکاری می‌کنند و باعث بروز حوادث و فجایع ملی و جبران ناپذیر می‌گردند. از اهداف آنها می‌توان، از کار انداختن شبکه‌های خدماتی عمومی مثل شبکه برق، گاز و غیره و همچنین ایجاد وحشت و ترس در جامعه و کاهش میزان اعتماد به دولت و نظام را برشمرد.

انواع حملات در فضای سایبر

۱. **حملات تروریسم سایبری**: تروریست‌ها برای ایجاد اختلال، از فضای سایبر استفاده می‌کنند. این افراد در مقابل دولت‌ها قرارگرفته و برای رسیدن به آنچه می‌خواهند از هر ابزار ممکن استفاده می‌کنند. حملات سایبری دو دسته هستند یک دسته برای سرقت اطلاعات و دسته دیگر برای نفوذ به سیستم‌های کنترل صورت می‌پذیرد. دزدی و تخریب اطلاعات منجر به قطع خدمات می‌گردد و این شایع‌ترین شکل حمله اینترنتی و رایانه‌ای می باشد. (ابراهیم نژاد شلمانی:۱۳۸۹: ۳۰)

۲. **حمله انکار خدمات**: یک حمله انکار خدمات حادثه‌ای است که در آن یک کاربر یا سازمان از خدمات یک منبع که طبق معمول انتظار بهره‌گیری از آنرا دارند محروم می‌گردند. نوعا قطع سرویس به معنی ناتوانی موقت یک سرویس شبکه خاص مانند پست الکترونیکی از حضور یا قطع موقت تمام اتصال یا خدمات شبکه می‌باشد.

۳. **حمله توسط هکر**: بطور متعارف به اشخاصی که از دانش شبکه خود و سیستم‌های رایانه‌ای در جهت حصول دسترسی غیرمجاز به سامانه‌های رایانه ای بهره می‌گیرند. (همان: ۳۵)

۴. **جنگ اطلاعات**: جنگ اطلاعات را می توان نبردی در سطح اجتماع، از طریق وسایل اطلاعاتی و ارتباطی دانست.

۱_ THE SILENT KILLERS
۲_ ACTIVE

۵. **ویروس(بدافزار)**: یک برنامه خود تکثیر است که خودش را با ساختن نسخه‌های اجرایی متعدد از خود گسترش می‌دهد. ویروس رایانه‌ای دقیقا مانند ویروس بیولوژیک که خود را در سلول-های بدن میزبان تکثیر می‌کند، عمل می‌نماید. (همان: ۳۶)

۶. **جنگ شبکه‌ای و روش تحلیل شبکه اجتماعی**: جنگ شبکه‌ای یک حالت رو به پیدایش از جنگ است که در آن دست‌های عامل از یک ساختار شبکه‌ای متناسب با عصر اطلاعات برای سازمان، دکترین و استراتژی خود بهره می‌گیرند. یک از روش‌های مناسب برای بهره‌گیری، از افرادی که با مدیریت دانش آشنا هستند آن را بهتر درک می‌کنند، تحلیل شبکه اجتماع می‌باشد. در این تحلیل، جریان روابط بین افراد، گروه‌ها، سازمان‌ها و غیره اندازه‌گیری و به شیوه‌ای قابل فهم ترسیم می‌گردد. در این ترسیم، گره‌ها و خطوط به ترتیب نماینده افراد و ارتباطات می‌باشند. در واقع جنگ شبکه‌ای و روش تحلیل شبکه اجتماعی یک تحلیل ریاضی و یک تحلیل بصری از سیستم‌های انسانی پیچیده ارائه می‌دهد. بطور کاربردی‌تر، تحلیل شبکه‌های دانش تروریست-ها و شکست آنها نیازمند فرایندی متفاوت با ردیابی پیوند ارتباطی و هدف یابی آنهاست. آنچه نیاز است در واقع توجه به راه های انتقال یابی دانش می‌باشد.

۷. **مهندسی اجتماعی(مغز افزار)**: فرایندها و فناوری‌هایی هستند که برای همراه ساختن افراد با خواسته‌ها و تقاضاهای یک شخص بکار می‌رود تا آن شخص به اطلاعات بدون مجوز که محرمانه هستند، دسترسی پیدا کند. (همان: ۴۳)

ساختار و مراحل(مهندسی) یک حمله سایبری

۱. ابتدا یک هدف مشخص تعیین می‌شود که می‌تواند قسمتی از یک زیرساخت حیاتی مانند شبکه راه آهن، شبکه برق، شبکهٔ ATM و یا وب سایت‌های دولتی باشد سپس مهاجم‌ها شروع به جمع‌آوری اطلاعات می‌کنند.

۲. از طریق شبکه اینترنت، مقالات، مطالعات وب سایت‌های هدف، انجام آزمایش‌های تست نفوذ[۱] بر روی وب، شناسایی مؤلفه های تکنیکی هدف مانند سامانه عامل و جمع‌آوری اطلاعات از طریق مهندسی اجتماعی (توسط کارکنانی که در آن ساختار کار می‌کنند) می‌باشد.

۳. حملهٔ سایبر اتفاق می‌افتد. بعد از اینکه دسترسی حاصل شد، ممکن است که حمله تا مدتی نگه داشته شود. یا ممکن است که حمله موفقیت آمیز بوده و یا شکست بخورد و اگر حمله موفقیت

۱- PEN- TESTING

آمیز باشد، هکر آن را از طریق مالتی‌مدیا منتشر و یا ردپا و اثر خود را مخفی می‌کند. تحقیق و بررسی جهت حملات دیگر انجام می‌گیرد.

مراحل دفاع سایبری

همواره اشکال متفاوت دفاعی در برخورد با فعالیت‌های دشمن در یک فضای سایبر وجود دارد. در اینجا دو مرحله از مراحل دفاع بررسی می‌شود.

۱. **جلوگیری**[۱]: شناسایی راه‌های نفوذ، حمله و مقابله با آنها جهت افزایش ضریب امنیت، ایمنی و پایداری می‌باشد. از جمله روش‌های جلوگیری می توان به موارد ذیل اشاره نمود:

- **طراحی ایمن و پایدار سامانه‌ها**[۲]: در صورتی که امنیت جزو معیارها و اصول طراحی سامانه‌ها، قرار بگیرد، سامانه‌ها بسیار امن تر و ایمن تر و پایدارتر از قبل خواهند بود.
- **متوقف کردن حملات**[۳]: از دیگر راه‌های جلوگیری از حملات، متوقف نمودن آنها می‌باشد این روش از طریق استفاده از تجهیزات پیشرفته امنیتی و وضع قوانین لازم، میسر است.

۲. **مدیریت حادثه**[۴]**، محدود کردن خرابی‌ها**[۵]: روش‌های مدیریت حوادث و محدود نمودن اثار زیانبار حوادث، راه‌هایی هستند که با استفاده از آنها می‌توانیم اثر حملات صورت گرفته را در کمترین زمان کاهش دهیم.

۳. **تعیین آثار، نشانه‌ها و هشدارها:** وقتی حمله‌ای اتفاق می‌افتد، ابتدا در گام اول باید آثار و خطراتی که این حمله می‌تواند داشته باشد را شناسایی کنیم، زیرا با شناسایی آثار یک حمله می‌توانیم از پیامدهای حملات دیگر و خطراتی که ممکن است ایجاد شوند، جلوگیری کنیم.

۴. **ایمن و پایدار کردن سامانه‌ها**[۶]: جهت جلوگیری از نفوذهای بیرونی، ضروری است تا موانعی ایجاد کنیم. از قدیمی‌ترین موانع نفوذ، استفاده از کلمه عبور است که البته روش‌های جدیدتر، استفاده از تکنیک‌هایی مانند دیواره‌ی‌آتش و یا پروکسی سرورها[۷] است. البته همان‌طور که شیوه‌های رمزنگاری شکست خوردند، شیوه‌های جدید نیز می‌تواند منجر به شکست شوند. در مورد حملات فیزیکی نیز لازم است که ابتدا تمام حملات و نفوذهایی که می‌تواند انجام شود

۱- PREVENTION
۲- EMBED SECURITY INTO DESIGN
۳- BAN ATTACKS
۴- INCIDENT MANAGEMENT
۵- DAMAGE LIMITATION
۶- HARDEN THE SYSTEM
۷- PROXY SERVERS

را، شناسایی کنیم. مثلاً در مورد یک شبکه اطلاعاتی، باید راهبردهای فیزیکی مناسب جهت امن، ایمن و پایدار نمودن مراکز داده آن اتخاذ نمود.

۵. **خاموشی و تخصیص مجدد**[۱]: یک راه حل دیگر این است که سامانه به طور کامل یا به طور جزئی خاموش شود و دوباره تخصیص مجدد شود. سامانه‌ی که متوجه شود تحت یک حمله قرار دارد، باید موانع و دفاع‌هایی از خود را بنا نهد که شاید در مواقع عادی از آنها استفاده نمی‌کند و سعی کند قسمت‌هایی از سامانه را که مواجه با حمله شده‌اند، ایزوله کند. البته مراحل خاموش کردن و تخصیص دهی مجدد باید به صورت بلادرنگ[۲] و به سرعت انجام گیرد.

۶. **پشتیبانی**[۳]: نکتهٔ قابل توجه این است که باید همواره از اطلاعات جمع‌آوری شده، قبل از هر حمله‌ای پشتیبانی کنیم. این تاکتیک از طریق تهیه نسخه پشتیبان اطلاعاتی که ذخیره شده‌اند، به دست می‌آید. بسیاری از روش‌های دفاع، نیاز به این دارند که حالت صحیح سامانه قبل از حمله را، جهت تسهیل در بازیابی و تجدید مجدد بدانند. این روش برای مواقعی است که حملات براساس نقطهٔ شروع دقیق و مشخصی انجام می‌شود و پشتیبان‌ها به طور منظم گرفته می‌شوند. بسیاری از حملات موذیانه به کندی و بطور محرمانه، مشکلات زیادی را نسبت به زمانی که اطلاعات سالم بودند، ایجاد می‌کنند (یعنی در اینگونه از حملات ما زمان دقیق سالم بودن اطلاعات را نداریم و تاثیر حملات هنوز ایجاد نشده است). در این حالت، جهت ایجاد فضای سالم، سامانه‌های سازمان باید خودشان برنامه‌هایی برای تهیه نسخه پشتیبان داشته باشند. (ایزایران، ۱۳۹۰: ۱۷–۲۰)

فناوری‌های نوین حملات سایبری مورد استفاده آمریکا

جنگ اطلاعات و حمله سایبری و انجام جنگ شبکه محور[۴] در میدان نبرد سایبری و دیجیتالی یکی از مهمترین راهبردهای قرن ۲۱ آمریکا می‌باشد. طبق آماری که از فرماندهی دفاع سایبری در جهان منتشر کرد. روزانه ۵۵۰۰۰ ویروس در جهان تولید و منتشر می‌شود که از این میان برخی از آنها در حوزه مقابله با امنیت سایر کشورها به خصوص ایران بکار گرفته می‌شود. ویروس‌هایی همانند

۱- SHUTDOWN AND REALLOCATION
۲- REAL TIME
۳- BACKUP
۴- NETWORK CENTRIC WARFARE

استاکس‌نت[۱] برعلیه تاسیسات اتمی ایران از این قبیل بدافزار می‌باشد(WWW.MASHREGHNEWS.IR 91/02/12)

مهمترین موضوعات فضای سایبر در سند ۲۰۱۲ راهبردی آمریکا

- رویکرد راهبردی فضای سایبر: راهبرد آمریکا در حوزه فضای مجازی بین‌المللی بر این باور پایه‌گذاری شده است که فناوری های شبکه‌ای، پتانسیل نیرومندی برای آینده کشور ما و جهان دارند.
- **رویکرد نظامی فضای سایبر**: انصراف و ممانعت می‌باشد. آمریکا در حالی حق دفاع از دارایی‌های حیاتی را به عنوان سرمایه‌های ضروری خود محفوظ می‌داند، عوامل مخرب را منصرف و یا از عملکرد آنها ممانعت می‌کند. آمریکا به تقویت دفاع های شبکه‌ای و توانایی ما برای مقاومت و جبران اختلالات و سایر حملات، ادامه خواهد داد. در برابر آن دسته از حملات پیچیده‌ای که خسارت بار هستند، ما برنامه‌های واکنشی مفید و توسعه یافته‌ای را طراحی خواهیم کرد که به تفکیک و کاهش اختلال در دستگاه‌ها و محدودکردن تاثیرات در شبکه‌هایمان و تاثیرات متعاقب فراتر از اینها بپردازد. زمانی که مجوز صادر شود، آمریکا به اقدامات خصمانه در فضای مجازی پاسخ می‌دهد، درست همان‌طوری که در قبال هرگونه تهدید کشورمان واکنش نشان می‌دهیم. ما به منظور دفاع از کشور و هم پیمانان و شرکاء و منافعمان، حق استفاده از تمام ابزار دیپلماتیک، اطلاعاتی، نظامی و اقتصادی را مناسب و سازگار با قانون کاربردی بین‌المللی است، برای خود محفوظ می‌دانیم. در چنین اقدامی، هر زمانی که بتوانیم تمام گزینه‌ها را پیش از کاربرد فشار نظامی را بررسی خواهیم کرد و با دقت هزینه‌ها و خطرات واکنش در مقابل هزینه های عدم واکنش را سنجش خواهیم کرد.
- **ارتش سایبری**: آمادگی برای چالش‌های امنیتی قرن۲۱، نیاز فزاینده ارتش به شبکه‌های معتبر و ایمن را شناسایی و تعدیل خواهیم کرد. اتحاد نظامی فعلی را برای مقابله با تهدیدهای بالقوه در فضای سایبری ایجاد و افزایش خواهیم داد. (جلالی، ۱۳۹۱: ۱۱۴)

منابع تهدیدهای سایبری

تهدیدهای سایبری با منبع خارجی، گروه‌های خرابکار، هکرها، هکرهای سازمان یافته، عوامل ناراضی داخلی، گروه‌های تروریستی می باشد. (اسکندری، ۱۳۸۹: ۱۱۲)

۱- STUXNET

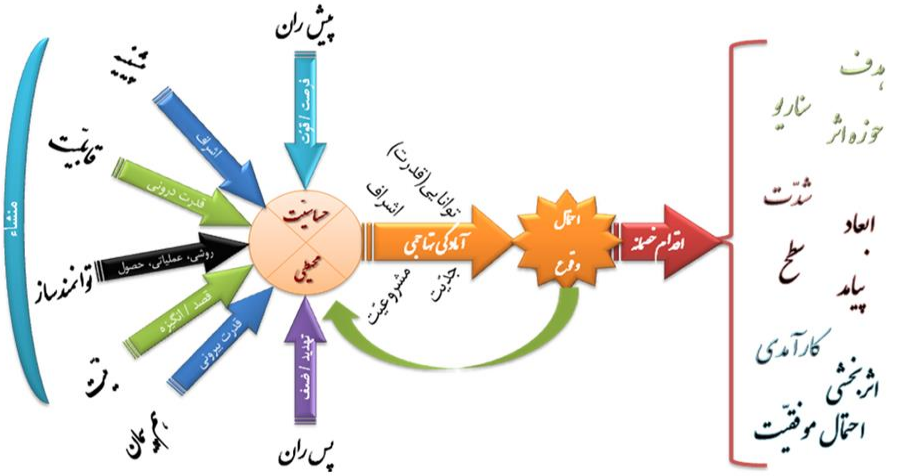
سطوح مختلف تهدید سایبری:

هر تهدید سایبری، دارای سطوح مختلفی از نفوذ گرفته تا بوجود آوردن تهدید ملی برای یک کشور هستند و طبعا برای دفاع در برابر این دست تهدیدهای، اقداماتی با سطوح مختلف درکشور وجود دارند که از اقدامات مدیریتی در سطوح پائین دستگاه‌ها گرفته تا تدابیر و اقدامات ملی رتبه‌بندی می‌شوند. حتی این موضوع می‌تواند به مناقشات بین‌المللی نیز برسد که تدابیر و راهبردهای متفاوتی نسبت به تهدیدهایی با مقیاس کوچکتر دارند. (همان : ۱۱۲)

شاخص‌های تهدید سایبری:

شاخص‌های تهدید در حوزه دفاع سایبری عبارتند از:

۱. دخیل بودن یک قدرت خارجی.
۲. تهدید امنیت ملی کشور.
۳. بوجود آمدن تهدید بر علیه زیرساخت‌های حیاتی و حساس کشور.
۴. مقیاس ملی و یا منطقه‌ای حوزه تاثیر تهدید بوجودآمدن تلفات و خسارات عمده اقتصادی در پی تهدید.
۵. هدف قرار دادن زیرساخت‌های حساس و حیاتی کشور. (ناظمی و همکار، ۱۳۸۵: ۱۶)



شکل۲- ویژگی‌های کلان تهدیدهای سایبری بر علیه کشور(خالقی،۱۳۹۲: ۸۰)

تجزیه و تحلیل

۱. فناوری اطلاعات و ارتباطات باعث ایجاد تحولات اساسی در جنگ شده است بطوری‌که بعضاً اندیشمندان دفاعی از آن با تعبیر انقلاب در امور نظامی یاد می‌کنند. علاوه بر آنکه جنگ‌های کلاسیک نیز متحول شده و پیشرفت‌های گسترده‌ای داشته‌است، سبک‌های ماهیتا نوینی از جنگ نیز در حال ظهور می‌باشد که مهمترین آنان جنگ سایبر می‌باشد. بنابراین سناریوهای متصور و متحمل در تهدیدهای سایبری بر علیه منابع ملی می‌تواند به شکل‌های زیر باشد:

الف– فلج‌سازی راهبردی

مدل تهاجم بصورت چند مرحله‌ای به حوزه‌های پولی و بانکی، انرژی، ارتباطات و ...می‌باشد و پیامدهای حاصله انهدام زیرساخت‌ها و امکانات کشور می‌باشد که هدف تهاجم سایبری، فلج‌سازی راهبردی حوزه سایبری و ضربه زدن به بخش‌های مختلف کشور از جمله بخش اقتصادی کشور می‌باشد.

ب– تهاجم سایبری به بخش اقتصادی کشور

ضربه به بخشی از دستگاه اجرایی کشور، بی‌نظمی در اجرای امور دولتی و خدمات عمومی می‌باشد که مدل کلی حمله سایبری، مقدمه‌ای برای تهاجم نظامی می‌باشد. و هدف این حمله راهبردی اغلب برای تکمیل سناریوهای دیگرحمله و با هدف ضربه به بخش اقتصادی کشور در حوزه دستگاه‌های اجرایی، بخش‌های عرضه خدمات عمومی می‌باشد.

۲. تهدید و جنگ سایبری را باید به اندازه و یا بیشتر جنگ فیزیکی مهم پنداشت بنابراین همانطور که در جنگ‌های فیزیکی هم‌افزایی همه منابع مادی و غیرمادی اعم از تجهیزات، سامانه‌ها، نیروی انسانی و سایر منابع جهت مقابله، دفع حمله و کاهش آسیب‌پذیری استفاده می‌شوند در جنگ سایبری هم هم‌افزایی منابع مورد نیاز و ضروری می‌باشد.

۳. فضای سایبری را می‌بایست جامع و کامل دانست که شامل کلیه عناصر فیزیکی و غیرفیزیکی، نیروی انسانی و تجهیزات می‌باشند که منابع مورد نیاز جهت حفاظت از آنها باید هم‌افزایی شوند.

۴. علی‌رغم خالص دانستن فضای سایبری، عامل انسانی نقش کلیدی و حساسی را دارد. مسلماً کشورهائی آسیب‌پذیرتر هستند که به شبکه‌های فناوری اطلاعات ناامن اتکای بیشتری دارند. پس داشتن شبکه فناوری اطلاعات بومی می‌تواند تهدیدهای حاصله را کاهش دهد.

۵. با توجه به گسترش روز افزون کاربری و کاربران فضای سایبری در ایران و وابسته شدن اکثر سامانه ها و خدمات به فضای سایبری، نیاز به افزایش توانمندی‌های بومی سایبری جهت مقابله و دفع تهدیدهای سایبری کشورمان بسیار محسوس است.

۶. توسعه امنیت، ایمنی و پایداری به موازات توسعه فضای سایبری در شبکه‌های ارتباطی و الکترونیکی با تأکید بر فناوری‌های بومی و ملی کشور می باشد که باید تمامی منابع مورد نیاز هم‌افزایی گردند.

۷. توسعه فرهنگ دفاع سایبری و ارتقاء دانش و شناخت مسئولین و کارشناسان حوزه ارتباطات و الکترونیک از تهدیدهای فضای سایبر و اقدامات پدافند غیرعامل در برابر آنها.

۸. ایجاد شبکه ملی اینترنت مبتنی برمولفه های امنیت، ایمنی، پایداری و متکی بر فناوری های بومی.

۹. نهادینه‌کردن ملاحظات دفاع سایبری و امنیت ملی در تعاملات و همکاری با کشورها و شرکت-های خارجی در حوزه فناوری اطلاعات و ارتباط.

۱۰. تشکیل مرکز پایش تهدیدهای سایبر و تشکیل مراکز واکنش سریع به تهاجمات سایبر[۱]

۱۱. پایش مستمر تهدیدهای سایبری در زیرساخت‌های حیاتی، حساس و مهم کشور و استفاده از ضد بدافزارهای بومی و هوشمند و پیشرفته و استفاده از نرم افزارهای بومی به منظور دفع و کاهش آسیب‌پذیری تهدیدهای سایبری.

نتیجه‌گیری

۱. نهادینه‌کردن اصول و ملاحظات پدافند غیرعامل در برابر تهدیدهای سایبری موجود در زیرساخت‌های حیاتی، حساس و مهم کشور نیازمند طرح‌های هم‌افزایی منابع ملی جهت مقابله، کاهش آسیب‌پذیری تهدیدهای فضای سایبری می‌باشد. که نیازمند سازماندهی، انسجام و هدایت راهبردی مجموعه‌های علمی، پژوهشی، آموزشی و صنعتی مرتبط با حوزه تخصصی سایبری در راستای تولید و توسعه دانش و فناوری‌های بومی و ملی مورد نیاز دفاع سایبری می‌باشد.

۲. الزامات و نیازمندی‌های هم‌افزایی منابع کشور در برابر تهدیدهای فضای سایبری کشور عبارتند از:

---

۱ (CERT) - Computer Emergency Reaction Team

الف– هم‌افزایی ایمن‌سازی:

تدوین سیاست‌ها، برنامه‌های ایمن‌سازی، دستوالعمل‌های اجرایی جهت هم‌افزایی منابع امری لازم و ضروری می‌باشد. در دفاع سایبر، کشور باید دارای راهبرد و قوانین و مقررات امنیت سایبر روشن و پیش گیرانه‌ای باشد. ایمن‌سازی شبکه‌های و سامانه‌های اطلاعاتی و برخورد جدی با خاطیان ملی و فراملی باید در دستور کار کلی قرارگاه دفاع سایبری کشور باشد. پیشرفت سیستم‌های اطلاعاتی و شبکه‌ای ملی و سازمانی به ویژه در حوزه زیرساخت‌ها، نویدبخش تهدیدهای نوین و جدی تر در آینده است. انتقال سیستم‌های اقتصادی، مالی، حقوقی، امنیتی و نظامی به روی شبکه‌ای ارتباطی و اینترنتی، علی‌رغم وجود محاسن فراوان می‌تواند پیامدهای خطرناکی را نیز به دنبال داشته باشد. باید راهبرد امنیت ملی، راهبرد دفاعی، راهبرد صنعت دفاعی، و راهبرد علوم و فناوری، تحقیق و توسعه از گرایش واحد و هم جهتی در زمینه جنگ و دفاع سایبری برخوردار باشند. توسعه توانمندی‌ها در این حوزه نیازمند نگاهی بلندمدت و آینده نگرانه است.

توسعه توانمندی‌های جنگ و دفاع سایبر، همچون شمشیر دولبه‌ای است که می تواند علاوه بر تهدید دشمن، علیه منافع ملی خود کشور نیز بکار گرفته شود. از نگاه کلی، جنگ اطلاعاتی و جنگ سایبر و دفاع، دارای دوره مشخصی نیستند، بلکه ماهیتی مستمر و فرصت طلبانه دارند. به همین جهت، نه می توان زمانی برای شروع و نه خاتمه آن در نظر گرفت. به علاوه شرایط ایده آل، امکان دستیابی به نتیجه مطلوب و بهینه را ممکن می سازد. دفاع سایبر نیز امری همیشگی است و باید همواره درحال آماده باش بود.

ب– هم‌افزایی علمی

ایجاد ساختارهای لازم و زیر ساخت‌های آموزشی و پژوهشی لازم و پیشرفته بومی در دانشگاه–های نظامی و غیرنظامی در کلیه مقاطع تحصیلی کارشناسی، کارشناسی ارشد و دکتری به منظور پایش مستمر و دفع تهدیدهای سایبری در حوزه‌های مختلف زیر ساخت‌های حیاتی، حساس و مهم کشور امری لازم و ضروری می‌باشد. که در این راستا تولید نرم افزارهای بسیار پیشرفته بومی و ضد بدافزارها و تولید سخت افزارهای بومی با تمام توانمندی‌های داخلی باید صورت پذیرد.

پ– الزامات فناورانه: استفاده از فناوری‌های زیربنایی و اساسی با استفاده از ظرفیت فناوری‌های بومی باید صورت پذیرد تا تولید زیرساخت‌های نرم‌افزاری و سخت‌افزاری فناوری‌های

ارتباطات و اطلاعات بومی و داخلی با استفاده از تمامی ظرفیت‌های علمی و پژوهشی داخلی انجام شود.

ت– هم‌افزایی عملیاتی

ارتقاء توانمندی عملیاتی کلیه سازمان‌ها و دستگاه‌های دولتی و غیردولتی به منظور مقابله و کاهش آسیب پذیری‌های سایبری در تمامی سطوح مختلف زیرساخت‌های حیاتی، حساس و مهم امری بسیار لازم و ضروری می‌باشد در این راستا باید مراکز پایش و واکنش سریع به تهاجمات سایبری در تمامی سازمان‌های دولتی و غیردولتی تشکیل گردد تا در کمترین زمان ممکن به احتمال حملات سایبری رخ داده را کشف و شناسایی کرده و اقدام لازم را بعمل آورند. این مراکز در حوزه نظامی باید جدای از مراکز عمومی یا خصوصی باشد بطوری که بخش دفاعی باید با پشتیبانی از چنین مراکز عمومی یا خصوصی، زمینه واکنش بهتر و همه جانبه تر را فراهم سازد.

ث– هم‌افزایی الزامات زیرساختی

زیرساخت مهمترین مقوله در زمینه جنگ و دفاع سایبر است. توسعه توانمندی‌های پایدار در حوزه فناوری برتر و فناوری اطلاعات، بدون وجود یک زیرساخت و بستر مناسب انجام نمی‌پذیرد. زیرساخت از ابعاد مختلفی فرهنگی و اجتماعی، اقتصادی، صنعتی، علوم و فناوری، دانش، فنی ارتباطات و شبکه‌ها، نهادها و قوانین برخوردار می‌باشد. بنابراین توسعه توانمندی‌های جنگ و دفاع سایبر در گرو توسعه صنعت و زیرساخت‌های فناوری اطلاعات و ارتباطات به ویژه صنعت نرم افزاری و خدمات شبکه‌ای می‌باشد. اگرچه امروز توسعه صنعت سخت افزار و نرم افزارهای پایه همچون سیستم عامل دیگر برای کشورهای تازه وارد به این حوزه، مقرون به صرفه نیست، اما همچنان ظرفیت‌های فراوانی در زمینه نرم افزار و خدمات شبکه‌ای وجود دارد. شاید یکی از مهمترین این حوزه‌ها، صنعت امنیت و خدمات امنیتی باشد. امروز می‌توان به کمک این صنعت، محصولات و خدمات مختلف موجود را ایمن نمود و محصولات درخور توجه‌ای روانه‌ی بازارهای جهانی نمود.

بنابراین با استفاده از هم‌افزایی ایمن‌سازی، علمی، عملیاتی و زیرساختی باعث مصون سازی مطابق الگوی زیر می‌گردد.

(برگرفته از مؤلفه‌های شکل‌دهنده‌ی نظام پدافند سایبری کشور)

پیشنهادها

به منظور کاهش آسیب‌پذیری و ایمن‌سازی شبکه فناوری اطلاعات و ارتباطات کشور، افزایش بازدارندگی و تولید قدرت سایبری، تداوم فعالیت‌های ضروری سایبری، ارتقاء پایداری ملی زیر ساخت‌های کشور، بومی‌سازی و تولید نرم افزارهای اصلی و اساسی و پایه و همچنین تسهیل مدیریت بحران سایبری در زیر ساخت‌های کشور، مدل لایه به لایه هم‌افزایی منابع به منظور دفاع سایبری زیر پیشنهاد می‌گردد:

- هم‌افزایی در لایه اجتماعی که شامل گروه‌ها، انجمن‌ها و شبکه‌هایی هستند که توسط انسان‌ها به عنوان کاربران فضای سایبری با اهداف علمی، فرهنگی، خبری، سیاسی، سرگرمی و غیره استفاده می نمایند.
- هم‌افزایی در لایه اطلاعاتی که شامل داده ها و اطلاعات تولیدشده، منتقل شده، دریافت‌شده، ذخیره شده، پردازش شده یا حذف شده در فضای سایبری می‌باشد که باید در برابر تهدیدهای سایبری مصون بمانند.
- هم‌افزایی در لایه کاربری و کاربردی که شامل نرم افزارهای کاربردی بومی و سرویس‌های مورد استفاده در فضای سایبری است.

- هم‌افزایی در لایه نرم‌افزاری که شامل تولید نرم افزارهای سیستمی و پروتکل‌های بومی مورد استفاده در زیرساخت‌ها و سیستم‌های فضای سایبری می‌باشد.
- هم‌افزایی در لایه سخت‌افزاری تجهیزات و لوازم الکترونیکی زیرساخت‌های بومی فضای سایبری می‌باشد.
- هم‌افزایی در لایه فیزیکی که شامل محیط فیزیکی مورد استفاده برای سیستم‌ها و زیرساخت-های فضای سایبری می باشد.

منابع

فارسی

- ابراهیم نژاد شلمانی، محمد ابراهیم.(۱۳۸۹). مقدمه ای بر جنگ سایبر و تروریسم سایبر جلد۱- بوستان حمید.
- اسکندری، حمید.(۱۳۸۹). دانستنیهای پدافندغیرعامل، بوستان حمید.
- پورابراهیم، علیرضا.(۱۳۹۲). پدافند ملی سایبر، دانشگاه عالی دفاع ملی.
- جلالی، غلامرضا.(۱۳۹۱). چهارگفتار در باب پدافندغیرعامل- انتشارات محدث.
- خالقی، محمود.(۱۳۹۱). ماموریت‌ها، ساختار تشکیلات و شرح وظایف قرارگاه پدافند سایبری کشور، مرکز پدافند سایبری کشور.
- خالقی، محمود.(۱۳۹۲). برآورد تهدیدات سایبری جمهوری اسلامی ایـران، قرارگاه پدافند سایبری مرکز پدافند سایبری کشور.
- موسسه ایزایران.(۱۳۹۰). پدافندغیرعامل در حوزه جنگ سایبر، موسسه اموزشی تحقیقاتی وزارت دفاع.
- ناظمی، امیر . قدیری، روح‌اله .(۱۳۸۵). آینده‌نگاری از مفهوم تا اجرا، مرکز صنایع نوین وزارت صنایع و معادن، تهران.
- نای، جوزف اس، ترجمه دکتر رضا مراد صحرایی.(۱۳۹۰). آینده‌ی قدرت، تهران.

انگلیسی

- Computer Security Division .(2012). IT Lab National Institute of Standards and Technology, Guide for Conducting Risk Assessment – NIST Special Publication 800-30 Revision 1.
- Lior Tabansky.(2011).Basic Concepts in Cyber Warfare, Military and Strategic Affairs.
- U.S Government Accountability Office.(2011). Defense Department Cyber Efforts.
- U.S Secretary of the Air Force.(2010).Air Force Doctrine Document 3-12 for Cyberspace Operations.
- U.S. Global Leadership.(2012). Navy Cyber Power 2020.
- WWW.PAYDARIMELLI.IR. 92/05/10
- WWW.MASHREGHNEWS.IR 91/02/12.