بررسی و بهره‌برداری از تکنولوژی جنگ اطلاعاتی بعنوان بعد پنجم در جنگ‌های نوین

مجید سلیمی

کارشناس– ستاد فرماندهی نیروی هوایی آجا

ایران – تهران

majid_salimi10@yahoo.com

چکیده

تحولات انجام شده در قرن حاضر بحدی سریع و گسترده بوده که واژه‌ها و مباحث جدیدی را در عرصه‌ها و امور مختلف وارد نموده است. این تحولات باعث شده که عامل زمان و مکان نیز تعریف جدیدی پیدا نموده است. در واقع باید گفت زمان انجام فرایندی کاهش یافته و صحنه عملکرد آن فرایند بسیار وسیع و فرا منطقه‌ای شده است. اصولاً جنگ اطلاعاتی و تکوین آن در نتیجه پیشرفت‌های سریع در تکنولوژی‌های اطلاعاتی و ارتباطاتی جدید همانند شبکه‌های الکترونیک و ظهور جامعه اطلاعاتی بروز کرده است. در جوامع اطلاعاتی معمولاً تمامی مبادلات اجتماعی، اقتصادی، سیاسی و فرهنگی ماهیتاً دیجیتال و وابسته به کامپیوتر شده است. لذا در یک تعریف ساده، جنگ اطلاعاتی عبارت است از استفاده از شبکه‌های الکترونیکی برای تخریب و یا از کار انداختن اطلاعات دیجیتالی و غیر عملیاتی کردن زیرساخت‌های اطلاعاتی که می‌تواند علیه یک جامعه یا نیروی نظامی تدارک دیده شود. در یک تقسیم‌بندی ساده دو گونه جنگ اطلاعاتی قابل تصور است: – NET WAR CYBERWARFARE – NETWAR یا جنگ شبکه‌ای: این نوع جنگ به جنگ‌های اطلاعاتی گفته می‌شود که بین افراد، جوامع و ملت‌ها جاری می‌شود و یا جهت‌گیری آن به سوی جامعه و اهداف غیر نظامی است. هدف این جنگ تخریب و فرو ریختن اندیشه‌ها و تصورات موجود در جامعه و جایگزین کرده انواع جدیدی به جای آنها می‌باشد. جنگ شبکه‌ای به دو صورت هدف‌گیری می‌شود. یکی افکار عمومی مردم و دیگری عقاید نخبگان. این قسم از جنگ طیف وسیعی از دیپلماسی، تبلیغات و مانورهای روانی و فریب با استفاده از رسانه‌های محلی و رخنه در شبکه‌های کامپیوتری و پایگاه‌های اطلاعاتی را شامل می‌شود. CYBERWARFARE : این نوع جنگ با هدف از هم گسیختن سیستم‌های اطلاعاتی و مخابراتی، سیستم‌های کنترل و فرماندهی، ارتباطات، خبرگیری و جاسوسی نیروهای دشمن و غیر عملیاتی کردن آنها در صحنه نبرد یا در غیر صحنه نبرد صورت می‌گیرد. دراین مقاله ضمن برشمردن ابزارهای نرم‌افزاری جنگ‌های اطلاعاتی، مواردی در خصوص کاربردها، عملکردها و مقابله با آنها ارائه می‌گردد.

کلمات کلیدی:

جنگ اطلاعاتی– CYBERWARFARE – NETWAR

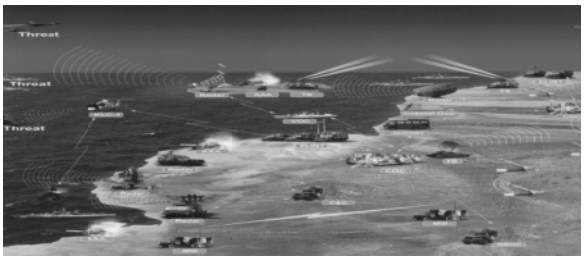
۱- مقدمه

در قرن ۲۱ و بالاخص سال‌های اخیر شاهد تحولات و پیشرفت‌های گوناگونی در مسایل نظامی بوده‌ایم. این تغییرات آنقدر سریع بوده است که مباحث متعدد و جدیدی را وارد عرصه نظامی‌گری نموده است.

از سوی دیگر واقعیت‌های صحنه نبرد موجب شده است که پارامترهای زمان و مکان تغییرات گسترده‌ای پیدا نمایند. از سویی زمان جنگ‌ها کاهش یافته و از طرفی هم صحنه نبرد وسیع و فرامنطقه‌ای شده است.

لزوم دستیابی به علوم و فناوری‌های نوین دفاعی در حوزه C4ISR ایجاب می‌نماید تا زمینه‌ها و بسترهای لازم بمنظور دستیابی مثمرثمر به تکنولوژی مدرن و پیشرفته در مفاهیم پیش گفته فراهم گردد. چنین ضرورتی اقتضاء می‌کند تا افزون بر ساز و کارهای متعارف، در زمینه توسعه و بسط و گسترش دانش بومی فرماندهی و کنترل اقدام گردد.

شکل(۱) یک میدان نبرد با انبوه شبکه‌ها و سامانه‌های فرماندهی و کنترل را نشان می‌دهد.



با توجه به اهمیت فناوری اطلاعات و ارتباطات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار IT این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است؛ که ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند به منظور مصون‌سازی این بستر از تهدیدات موجود درجهت حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین‌المللی را می‌طلبد.

۲- جنگ اطلاعاتی Warfare IW (Information)

برای جنگ اطلاعاتی، تعریف‌های مختلفی ارایه شده است که هر یک از منظر خاصی به رویارویی اطلاعاتی می‌نگرد، ولی تمام این تعریف‌ها رویکرد مشخصی را دنبال می‌کنند. به عنوان نمونه، به چند مورد زیر بسنده می‌گردد. جنگ اطلاعاتی:

الف) توانایی شنیدن، دیدن، داشتن درک صحیح از سامانه‌های فرماندهی و کنترل، شناسایی منابع اطلاعاتی و حسگرهای دشمن و در مجموع دست‌یابی به درک بهتر از استعدادهای دشمن به گونه‌ای که به برتری اطلاعاتی بیانجامد.[1]

ب) به کلیه اقداماتی اطلاق می‌شود که از طریق اثرگذاری بر اطلاعات و سامانه‌های اطلاعاتی دشمن و به منظور دست‌یابی به برتری اطلاعاتی، در راستای راهبرد نظامی یک کشور صورت پذیرد.[1]

پ) به عملیات‌های نظامی به غیر از جنگ‌های فیزیکی گفته می‌شود.[1]

ت) ایده‌ها و نظریه‌های مرتبط با اثرگذاری و روش تفکر انسان‌ها و از آن مهم‌تر، روش بهره‌گیری از اطلاعات برای دستیابی به اهداف ملی یک کشور نیز جنگ اطلاعاتی نام دارد. این اهداف ممکن است در زمینه‌های سیاسی، اقتصادی یا نظامی باشند.[1]

۳- ابزارهای نرم‌افزاری جنگ اطلاعاتی:

ویروس‌ها: ویروس‌ها برنامه‌هایی می‌باشند که قادر به تکثیر خود به برنامه‌های بزرگتر هستند. برنامه‌های ویروسی زمانی فعال می‌شوند که برنامه میزبان شروع به فعالیت کند و به دنبال آن ویروس خود را تکثیر می‌کند. ویروس‌ها در هر محیط کامپیوتری ساخته می‌شوند. پس تعجب‌آور نیست به مثابه جنگ‌افزارهای اطلاعاتی مورد استفاده قرار بگیرند. وقتی یک عامل، ویروس‌های کامپیوتری را به داخل شبکه کامپیوتر رخنه داده باشد در آن حالت شبکه هدف از کار می‌افتد و یا حداقل نارسایی‌های وسیعی در آنها ایجاد می‌شود.

کرم‌ها:

کرم‌ها یک برنامه مستقل هستند که خودشان را تکثیر می‌کنند و از یک کامپیوتر به کامپیوتر دیگر و اغلب بر روی شبکه‌ها می‌روند و بر خلاف ویروس‌ها برنامه‌های دیگر را تغییر نمی‌دهند. پیامدهای مخرب این جنگ افزار در دو زمینه قابل بررسی است: یکی نابودی منابع موجود اطلاعاتی در شبکه و دیگری تغییر شکل و انتشار در شبکه.

اسب تروا:

اسب تروا برنامه‌های هستند که در داخل سایر برنامه‌ها پنهان می‌گردند و برنامه خود را به اجرا در می‌آورند. اسب تروا می‌تواند خود را استتار کند و حتی در برنامه ایمنی شبکه قرار گیرند.

بمب منطقی:

بمب منطقی خود نیز یک نوع از اسب تروا می‌باشد که برای آزاد کردن ویروس‌ها و سیستم‌های تهاجمی دیگری استفاده می‌شود و می‌تواند بصورت یک برنامه مستقل که توسط برنامه‌نویس و طراح در سیستم جاسازی می‌شود، عمل نماید. کشورهای که در امر صادرات نرم‌افزار فعال هستند می‌توانند با نصب این بمب در نرم‌افزارهای صادراتی خود در شرایطی که با یک کشور درگیر جنگ می‌شوند با فعال کردن این بمب آثار بسیار مخربی همانند فرمت کردن دیسک‌ها و یا ارسال برنامه‌های کاربر نرم‌افزار به سازمان‌های جاسوسی خود را فراهم بیاورند.

درهای پشتی یا دامی:

این ابزار شامل سازو کارهای است که طراح نرم‌افزار آن را در زمان ساخت نرم‌افزار تعبیه می‌کند تا در زمانی که سیستم‌های حفاظت کامپیوتر به طور طبیعی فعالیت می‌کنند به طراح امکان می‌دهد تا به طور مخفیانه وارد سیستم شود. این مکانیزم در زمان جنگ اطلاعاتی قادر است سیستم‌ها و اطلاعات ذخیره شده در کشورهای خارجی را مورد کاوش و جستجو قرار دهد. این امر مهمترین مسئله و برنامه در استراتژی نظامی و منبعی برای فراهم آوردن اطلاعات حیاتی برای بخش جاسوسی است.

۴- جنگ اطلاعات در فضای مجازی Cyber Warfare

در بین جنگ‌های اطلاعاتی، این نوع رویارویی (در فضای مجازی) طیف بسیار وسیعی را در بر می‌گیرد که شامل تروریسم اطلاعاتی، تهاجم از طریق اختلال در منطق حاکم بر یک نرم‌افزار، شبیه‌سازی تمام عیار یک نبرد و جنگ گیبسون می‌باشد. جنگ اطلاعات به دلیل تخیلی و مجازی بودن آن در فضای مجازی، کمتر از انواع پیش گفته دارای مستندات و منابع قابل تعقیب می‌باشد. در تهاجم از طریق تغییر در مفهوم یا منطق حاکم بر یک نرم‌افزار، سعی می‌شود ماموریت یک نرم‌افزار به گونه‌ای تغییر داده شود تا نتایج نهایی، بر خلاف انتظار سامانه باشد. به عنوان مثال، با تزریق ویروس در سامانه ناوبری یک هواپیما می‌توان زمینه‌ی نمایش اطلاعات خطا (ولو به ظاهر طبیعی) مانند ارتفاع هواپیما از سطح دریا یا فاصله واقعی باند پرواز تا هواپیما را فراهم نمود.[1]

۴-۱- انقلاب در امور نظامی Revolution in Military Affairs

تحولات عظیم در فناوری‌ها به ویژه فناوری اطلاعات موجب ظهور چنان تغییرات اساسی‌ای در سازمان‌های نظامی شده است که از آن به عنوان انقلاب در امور نظامی، نامبرده می‌شود. این پیشرفت‌ها نه تنها باعث بروز ایده‌های نو و کاربردهای جدید در کلیه زمینه‌ها از جمله سامانه‌های اطلاعاتی، تسلیحات، فرماندهی و کنترل شده، بلکه تاثیرات قابل توجهی بر نظریه‌ها، روش‌های عملیاتی، تاکتیک‌ها و تفکرهای نظامی داشته است.[1]

۴-۲- جنگ فرماندهی و کنترل Command and Control Warfare

استفاده یکپارچه و هماهنگ از روش‌های جنگ روانی، فریب نظامی، امنیت در عملیات، جنگ الکترونیک و تخریب فیزیکی که به وسیله اطلاعات پشتیبانی شده باشند و قابلیت پیشگیری از دسترسی دشمن به اطلاعات خودی، اثرگذاری بر فرآیند گردآوری اطلاعات و کاهش کیفیت اطلاعات دشمن، از بین بردن سامانه‌های فرماندهی و کنترل حریف و دفاع از سامانه‌های خودی در گستره جنگ فرماندهی و کنترل قابل دست‌یابی می‌باشد. جنگ فرمان و کنترل شامل هر نوع عملیات در تمام سطوح رویارویی نظامی می‌باشد. بنابراین جنگ فرماندهی و کنترل می‌تواند ماهیت تدافعی و تهاجمی داشته باشد.[1]

۴-۳- جنگ نفوذگران رایانه‌ای Hacker Warfare

هدف این نوع جنگ اطلاعاتی، تهاجم به بخش غیرنظامی یک کشور است؛ چرا که تهاجم به بخش‌های نظامی در قالب روش‌های جنگ فرماندهی و کنترل صورت می‌پذیرد. در این نوع جنگ، سارقین اطلاعات یا نفوذگران رایانه‌ای اقدام به شناخت نقاط آسیب‌پذیر ساختار یک سامانه نموده و از ان نقاط، تهاجم خود را آغاز می‌کنند. زمینه‌های این تهاجم می‌تواند بسیار متنوع باشد. برای نمونه هدف از تهاجم ممکن است ساقط کردن یک سامانه، تعطیلی و توقف مکرر یک سامانه، ایجاد خطاهای اتفاقی در داده‌ها، سرقت خدمات (انجام مکالمات تلفنی رایگان، ورود و بهره‌برداری از اطلاعات پایگاه‌ها بدون پرداخت هزینه)، جعل هویت (استفاده از امضای دیجیتالی و یا کارت اعتباری دیگران)، گردآوری اطلاعات برای سرویس‌های امنیتی

(رمزشکنی و دستیابی به رمز ورود به پایگاه‌های نظامی و فروش این رمزها به سرویس‌های اطلاعاتی)، ارسال پیام‌های ساختگی غیرمجاز و دستیابی به اطلاعات شخصی افراد به منظور اخاذی از آنها باشد. در این رابطه از نرم‌افزارهای متعددی نیز بهره گرفته می‌شود. دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد چنین اقداماتی ازیک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و ازسوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد ضروری است این قبیل تمهیدات درمتن طراحی‌ها لحاظ گردند[1].

۵- اصول بکارگیری و گسترش در شبکه جنگ‌های اطلاعاتی:

در استراتژی‌های نوین نظامی بیشتر کشورهای توسعه یافته و پیشرفته، اصولی را در رابطه با بکارگیری و گسترش شبکه جنگ‌های اطلاعاتی پیش‌بینی و رعایت می‌کنند. این اصول در گذشت زمان‌های طولانی تکامل پیدا کرده و به دستورالعمل فنی، عملیاتی و بکارگیری و گسترش شبکه جنگ‌های اطلاعاتی بمنظور پشتیبانی مطلوب از وظایف دفاعی و امنیتی محوله، بدل شده است.

باید توجه داشت هریک از اصول عنوان شده در این مقوله نقش مهم و اساسی را در خصوص بهره‌برداری از شبکه جنگ‌های اطلاعاتی بیان می‌نماید و نمی‌توان بدون در نظر گرفتن ارتباط آنها با دیگری آنها را در نظر گرفت.[1]

۵-۱- سادگی:

با پیشرفت سامانه‌های فناوری اطلاعات و پیچیده‌تر شدن آنها، طراحان شبکه جنگ‌های اطلاعاتی باید حتی‌الامکان سادگی طرح‌های خود را حفظ نمایند چون طرح‌های ساده انعطاف بیشتری در برخورد با محدودیت‌های اعمال شده دارند.

علاوه بر اجرای طرح‌های ساده در شبکه جنگ‌های اطلاعاتی، باید سادگی و آسانی کاربری و عملیاتی شدن آنها از سوی طراحان مدنظر قرار گیرد. اجرای این مورد باعث اقدام مناسب در تغییرات موجود و پیش‌بینی نشده در صحنه عملیاتی می‌گردد.[1]

شکل زیر یکی از ابزارهای نفوذ اطلاعاتی با ارسال امواج کوتاه و بلند الکترونیکی موسوم به بمب الکترونیکی را نشان می‌دهد.

۵-۲- انعطاف‌پذیری:

شبکه سامانه‌های جنگ‌های اطلاعاتی باید بتواند به سرعت خود را با تغییرات و شرایط پیش‌بینی نشده صحنه نبرد هماهنگ نماید و پوشش شبکه با نیازهای مورد درخواست نیروهای مستقر در منطقه، تداوم یابد.

همچنین شبکه جنگ‌های اطلاعاتی باید تا حد ممکن برای انواع عملیات‌های محوله قابل بهره‌برداری باشد بنابراین شبکه موصوف به محض گسترش و عملیاتی شدن باید انعطاف‌پذیری مطلوبی را در مواجهه با وضعیت‌های مختلف داشته باشد و توانمندی اجرای همه انواع دستورات و درخواست‌ها را داشته باشد.

اگر برخی سامانه‌های موجود در شبکه جنگ‌های اطلاعاتی به تنهایی قادر به برآورد همه نیازهای درخواستی کاربران نبودند باید این انعطاف موجود باشد تا با ترکیب سایر تجهیزات و الحاق آنها به یکدیگر همه نیازهای شبکه پوشش داده شود.[1]

اصول اساسی در طراحی و بکارگیری شبکه جنگ‌های اطلاعاتی انعطاف‌پذیری عبارتند از:

۱) طراحی مناسب شبکه و زیر سیستم‌ها
۲) لایه‌های ارتباطی متعدد
۳) نیروی انسانی کارآمد
۴) ظرفیت مدارات بکارگیری شده
۵) دستورالعمل‌ها و پیوست‌های فنی و عملیاتی مناسب
۶) تمرین و رزمایش‌های متعدد
۷) رعایت استانداردهای موجود برای کاهش زمان بهره‌برداری و عملیاتی نمودن.

۵-۳- در برگیرنده همه نیازهای کاربران:

پیش‌بینی نیازهای جنگ‌های اطلاعاتی نیروهای مستقر در صحنه نبرد ممکن است با رعایت انعطاف‌پذیری شبکه مربوطه تا حد زیادی مرتفع گردد. فرماندهان درگیر در عملیات باید اطمینان داشته باشند که ستاد تخصصی مربوطه از همه نیازهای شبکه کنترل و فرماندهی آگاه بوده و زیرساخت‌های لازمه را تدارک دیده است.

۵-۴- قابلیت تعامل‌پذیری:

شبکه جنگ‌های اطلاعاتی و زیرسیستم‌های آن باید قابلیت تعامل‌پذیری را با سایر شبکه‌های فرماندهی وکنترل ازجمله سایرشبکه‌های سنسوری و شبکه‌های راهبردی و تجاری و .... داشته باشند.

ضرورت داشتن تعامل زمانی احساس می‌شود که لازم باشد اطلاعات بین این شبکه‌های منتقل گردد و علاوه بر مورد پیش گفته سامانه‌های جدید و مدرنی که به شبکه جنگ‌های اطلاعاتی وارد می‌شوند باید تعامل لازم را با سامانه‌های قدیمی داشته باشند.

۶- سوابق و اطلاعات ثبت شده جنگ‌های اطلاعاتی:

در جنگ‌های اطلاعاتی ریز مستندات این جنگها (نحوه عملیات، نتایج بدست آمده و آثار و تبعات و ...) باتوجه به ارتباط مستقیم با امنیت ملی کشورها بعنوان اسناد باسطح محرمانگی بالا تلقی گردیده و دولت‌ها مانع از فاش شدن آن‌ها می‌گردند.

یک جنگ اطلاعاتی و سایبری می‌تواند توسط یک دولت یا گروهی متخاصم و بمنظور ایجاد اختلال و یا صدمه زدن به زیرساخت‌های هدف طرح‌ریزی و اجرا شود. آنچه که تحت عنوان جرم سایبری شناخته می‌شود، در واقع می‌تواند بعنوان ابزارهای این نوع جنگ مورد استفاده و بهره‌برداری قرار گیرد[1].

از جمله جنگ‌های معروف و ثبت شده اطلاعاتی و سایبری می‌توان به موارد ذیل اشاره نمود:

- در سال ۱۹۸۰ میلادی طرح‌ریزی کره شمالی جهت آمریکا.
- سال ۱۹۹۴ در این سال به مراکز هوائی، تحقیقاتی نیویورک، انستیتو تحقیقات اتمی کره‌جنوبی و نهایتاً مرکزی علمی در لاتویا (از کشورهای تازه استقلال یافته شوروی سابق).
- سال ۱۹۹۵ حمله هکرهای روسی به Citybank آمریکا.
- سال ۱۹۹۹؛ حمله آمریکا به یوگسلاوی سابق و نفوذ به حساب‌های بانکی، قطع نمودن خطوط تلفن و تهدید مراکز سوخت‌رسانی و غذا.
- سال ۱۹۹۹؛ حمله آمریکا به صربستان در جنگ ۷۸ روزه و تهدید شبکه‌های کامپیوتری نظامی و اجتماعی.
- سال ۲۰۰۰؛ حمله هنگ‌کنگ به چین و تهدید مراکز انرژی، نظامی و بانک‌های چین.
- سال۲۰۰۱ حمله به مراکز خدمات امنیتی روسیه از سوی آمریکا.
- سال ۲۰۰۳ حمله چین به تایوان با بهره‌برداری از ویروس رایانه‌ای اسب تروآ.
- سال ۲۰۰۶ حمله رزیم اشغالگر قدس به حزب‌الله لبنان در جنگ ۳۳ روزه. (با تمهیدات صورت گرفته از سوی حزب‌الله این حملات به سرانجام نرسید.)
- سال ۲۰۰۸ حمله روسیه به اوستیای جنوبی و اخلال در عملکرد سایت‌های وزارت دفاع، امورخارجه، روزنامه‌ها و شبکه‌های رسمی و دولتی تلویزیونی با حملات مستمر DOS (Denial of Service). [1]

نگاه تحلیل‌گران به فناوری ارتباطات و اطلاعات، پس از موارد موصوف و مهمترین آنها شوک یازدهم سپتامبر ۲۰۰۱، دگرگون شد و در پی این دگرگونی، فرصت‌های جدید و پارادایم‌های نویی در مدیریت فاوا به عنوان محور تامین امنیت ملی، کشف و مطرح شدند. اکنون به جای ارائه‌ی تعریف دقیق از دشمن، نوع حمله و تمرکز روی یکایک رویدادها، مخاطرات و بحران‌های ضد امنیتی چه در سطح ملی یا در شبکه‌های فاوا، طیفی از همه‌ی انواع بحران‌های امنیتی و به جای رویکرد موردی و مقطعی، رویکردی سامان‌مند با تاکید بر تحلیل و مدیریت این طیف، مطرح شده است. با عنایت به موارد اشاره شده مهمترین پارامترها مورد نیاز در تامین امنیت ملی جهت عملکرد مطلوب در مواجه با تهدیدات جنگ‌های اطلاعاتی و نقش و سهم امنیت فناوری ارتباطات و اطلاعات در تامین این امنیت ملی بشرح ذیل ارائه می‌گردد:

این پارامترها عبارتند از:

- نوع موضوع امنیت
- فرهنگ امنیت

- خود ارزیابی حافظان امنیت ملی
- مدل تولید اطلاعات امنیتی
- رفتار عرضه کننده‌ی اطلاعات امنیتی
- شیوه‌ی کار و فعالیت مدیریت امنیت
- وضعیت مهار منابع اطلاعاتی و تشخیص هویت منبع
- قابلیت دستیابی امکانات
- رفتار بودجه‌ریزان و سرمایه‌گذاران روی امنیت

۷- نتیجه‌گیری:

با عنایت به مطالب اشاره شده در متن می‌توان اینگونه نتیجه گرفت که در جنگ‌های اطلاعاتی و سایبری، دشمن با دخل و تصرف غیر مجاز از طریق ورود و خروج، ذخیره، پردازش وکنترل داده‌ها و نرم‌افزارهای رایانه‌ای و ایجاد و وارد کردن ویروس‌های رایانه‌ای به زیرساخت‌های حیاتی، حساس و مهم کشور آسیب و صدمات قابل توجهی وارد نموده و باعث بروز بحران در نظام سیاسی، اجتماعی، اقتصادی، دفاعی، ارتباطی و فرماندهی و کنترل کشور می‌گردد.

نظر به گسترش شبکه‌های فناوری ارتباطات و اطلاعات در سطح جامعه و با توجه به لزوم انجام فرایندهای تولید و توزیع بسته‌های نرم‌افزاری مورد نیاز بصورت متمرکز در هر سازمان، وجود یک ساختار مناسب به منظور مدیریت این فرایند امری ضروری و اجتناب‌ناپذیرخواهد بود. دگرگونی‌های ناشی از جامعه‌ی اطلاعات، فرصت آخرین است و اغتنام فرصت‌ها، نیازمند جابجایی پارادایم‌ها، سیاست‌گذاری جدید و به موقع در زمینه‌ی فناوری ارتباطات و اطلاعات، تعیین سطح قابل قبول مخاطره، ایجاد اتاق فکر امنیت فناوری ارتباطات و اطلاعات، تاسیس پژوهشکده و آزمایشگاه فناوری ارتباطات و اطلاعات، تربیت تحلیل‌گران فناوری ارتباطات و اطلاعات و اتخاذ تصمیمات لازم برای افزایش انعطاف‌پذیری نهادهای امنیتی شفاف، مسئولیت‌پذیر، کارآ، قابل پیش‌بینی و راهبرد- محور است.

ساختار پیش‌بینی شده برای مدیریت این موضوع بایستی اهداف ذیل را مدنظر قرارداده تا در مواجه با تهدیدات منطقه‌ای و فرا منطقه‌ای بهترین عملکرد را اتخاذ نمایید:

- هماهنگی و ایجاد و وحدت رویه فناوری ارتباطات و اطلاعات
- تعیین معیارها و ضوابط لازم در طراحی، بهره‌برداری و تولید تجهیزات سخت‌افزاری و نرم‌افزاری فناوری ارتباطات و اطلاعات.
- حصول اطمینان از برقراری و استمرار امنیت رایانهٔ در سازمان با تهیه پایانه‌های بومی و امن.
- تعیین چارچوب و استانداردسازی در طراحی، ساخت و تأمین پایانه‌های بومی و امن با ویژگی‌های امنیتی و حفاظتی.
- تعیین خط‌مشی، همسوسازی و یکپارچه‌سازی در ساخت و تأمین سخت‌افزاری پایانه‌های بومی و امن سازمان.
- تأمین رایانه‌هایی با تجهیزات درونی کنترل امنیت.
- توجه به امنیت و مسائل مرتبط از ابتدا.
- شناخت و شناسائی تهدیدات منطقه‌ای و فرامنطقه‌ای.
- پیش‌بینی امنیتی در آینده.
- جداسازی بخش کنترهای دسترسی و امنیتی از بخش‌های دیگر سیستم.
- اعمال کمترین امتیازها در دسترسی‌ها.
- رعایت اصول امنیت شبکه.
- توجه و کنترل عوامل انسانی.
- ارتقاء ضریب امنیتی، شبکه‌های ارتباطی امن فناوری ارتباطات و اطلاعات.
- تامین امنیت بالا در آماده‌سازی و توزیع تجهیزات فناوری ارتباطات و اطلاعات.
- توجه به این امر که آموزش و فرهنگ‌سازی در حوزه امنیت ICT و تدوین اجرای سیستماتیک آن.

منابع:

[1] و[2]و[5]،[7]،[12]،[13] کتابچه جنگ سایبر – سازمان پدافندغیرعامل- خردادسال ۱۳۸۸

[3]،[4]،[8]،[1] کتابچه پدافندغیر عامل در حوزه جنگ سایبر – سازمان پدافندغیرعامل- خردادسال ۱۳۸۸

[6], [1]ISO/IEC 17799: Information Technology – Security Techniques - Code of Practicfe for Infromation Security Management (2nd edition), Feburary 2005.

[9], [11]Federal Information Processing Standards Publication, FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems, March 2006.