معرفی رویکردها و متدولوژی‌های طراحی و اجرای سناریوهای مقابله با تهدیدات سایبری

ناصر حسین غروی[۱]، علی محمدی[۲]

[۱] دانشجوی دکتری، دانشگاه جامع امام حسین(ع)

تهران، ایران

n_gharavi@ihu.ac.ir

[۲] پژوهشکده مطالعات راهبردی و امنیت ملی، دانشگاه عالی دفاع ملی

تهران، ایران

a.mohammadi@sndu.ac.ir

چکیده

مقابله با تهدیدات سایبری به معنی حفاظت از مالکیت مادی و معنوی اطلاعات با ارزش در حوزه اقتصاد، سیاست و نظامی به صورت دیجیتال (نرم افزاری)، در برابر سرقت، جعل، تحریف، ازکاراندازی و هر نوع سوء استفاده است. بنابراین حفاظت از اطلاعات و داده‌ها در برابر این تهدیدات، بدون آنکه اختلالی در رشد و نوآوری و توسعه ایجاد شود، یک مسئله مهم به شمار می‌رود. درحال حاضر این موضوع بطور فزاینده‌ای تبدیل به یک مسئله مهم مدیریتی شده است، بطوریکه امروزه مقابله با تهدیدات سایبری یکی از جدی‌ترین چالش‌های امنیت ملی و اقتصادی برای دولت‌ها محسوب می‌شود. در این مقاله محورهای بحث روی دو موضوع متمرکز شده است. اول شناخت تهدیدات و دوم راه‌کارهای مقابله با آنها. لذا ابتدا در رابطه با مسایل فنی، به الگوی جنگ اطلاعاتی، اهداف و مشخصات عملیات، محدوده عملیاتی، نیازمندیهای یک عملیات سایبری، ویژگی‌های جنگ‌های سایبری نسبت به سایر انواع جنگ ها به خصوص در زمینه فعالیت های نرم افزاری و شبکه‌ای و اینترنت پرداخته می‌شود. سپس به تشریح شناخت نقاط آسیب پذیر، تدابیر فنی وپدافند های موجود، ابزارها و بطور خلاصه روش‌های مقابله با تهدیدات پرداخته می‌شود.

کلمات کلیدی:

فضای سایبری، تهدیدات سایبری، دفاع سایبری، شبکه، اینترنت، نفوذگری، امنیت اطلاعات

۱- مقدمه

آنجا که اصولاً امنیت امری نسبی و نه مطلق است، مقابله با تهدیدات سایبری به منظور از بین بردن و محو کامل آنها، امر غیرممکنی می‌باشد. بنابراین حفاظت از اطلاعات و داده‌ها در برابر این تهدیدات، بدون آنکه اختلالی در رشد و نوآوری و توسعه ایجاد شود، یک مسئله مهم به شمار می‌رود. مقابله با تهدیدات سایبری به معنی حفاظت از مالکیت مادی و معنوی اطلاعات با ارزش در حوزه اقتصاد، سیاست و نظامی به صورت دیجیتال (نرم افزاری)، در برابر سرقت، جعل، تحریف، ازکاراندازی و هر نوع سوء استفاده است. درحال حاضر این موضوع بطور فزاینده‌ای تبدیل به یک مسئله مهم مدیریتی شده است، بطوریکه امروزه مقابله با تهدیدات سایبری یکی از جدی‌ترین چالش‌های امنیت ملی و اقتصادی برای دولتها محسوب می‌شود. بعبارت دیگر حفاظت از مرزهای مجازی (Virtual Network Perimeters) به اندازه حفاظت از مرزهای روی نقشه، برای هر کشوری دارای اهمیت است.

ورود به هر موضوعی ابتدا به شناخت آن نیاز دارد. معرفی راه‌کارهای مقابله با تهدیدات سایبری، قبل از هر چیز مستلزم شناخت خود تهدیدات است. بنابراین در این مقاله ما محورهای بحث خود را روی دو موضوع متمرکز می‌کنیم: اول شناخت تهدیدات و دوم راهکارهای مقابله با آنها.

۲- تهدیدات سایبری

ترکیبی از دو عامل پیشرفت تکنولوژی و فعالان بدخواه، کار حفاظت از اطلاعات و فرآیندهای سایبری را پیچیده می‌سازد. سه نکته مشترک به این امر کمک می‌کند:

۱) جابجایی ارزشها: امروزه بطور فزاینده ای ارزشهای مادی و معنوی در فضای سایبری مبادله می‌شود و این امر خواه نا خواه توجه طمعکاران را بخود جلب می‌کند.

۲) سیستم‌های باز: امروزه نیاز به دسترسی به فضای مجازی به طور فزاینده‌ای در حال گسترش است (چه در بخشهای دولتی و چه خصوصی)، و این توسعه غالباً از طریق همان دستگاه‌های قابل حملی انجام می‌گیرد که در زندگی روزمره استفاده می‌شود، مانند تلفن همراه. چنین وسایلی درحالی که امکان ارتباط را افزایش می‌دهند، همزمان انواع تهدیدات امنیتی جدید را نیز دربردارند: هنگامی که هکرها دستگاهی را رمزگشایی یا کرک کنند، برای بدافزارها یک مسیر ورود آسان به کل شبکه ایجاد کرده‌اند.

۳) پیشرفت، توسعه و پیچیدگی تکنولوژیکی تهدیدات: حمله و دفاع همیشه دو روی یک سکه بوده‌اند، اما اگر قدرت یکی بر دیگری افزونی یابد، سکه همیشه به همان رو فرود خواهد آمد. فعالیت‌های بدخواهانه روز بروز در حال پیچیده‌تر شدن هستند. سازمان‌های حرفه‌ای جرائم رایانه‌ای، هکرهای سیاسی و گروه‌های تحت حمایت دولت‌های رقیب به لحاظ تکنولوژی پیشرفته‌تر شده‌اند و در برخی موارد از مهارت‌ها و منابع تیم‌های امنیتی شرکت‌ها پیش افتاده‌اند. هکرها در ازای هر دستگاهی که مورد نفوذ قرار دهند پول کلانی دریافت می‌کنند. در نتیجه، در ۵ سال گذشته حملات هدفمند و پیچیده‌تر شده‌اند. امروزه ردیابی ویروس‌ها بسیار مشکل تر شده است. اغلب این ویروس‌ها اطلاعاتی را می‌دزدند که سود مالی داشته باشد.

۲-۱- برخی از مفاهیم اولیه

برای تفهیم جنگ و تهدیدات سایبری، ابتدا باید فضای سایبری و عناصر آن را ادراک نمائیم. بنابراین ابتدا ببینیم اصولاً سایبر (Cyber) به چه مفهوم است. سایبر، پیشوندی برای اسامی متعدد و متنوعی است که همگی بر اساس توسعه روز افزون رایانه پدید آمده اند. ضمناً اغلب عناصر درگیر با اینترنت با این پیشوند قابل تشریح می‌باشند.

فضای سایبری (Cyber Space)

اولین اصطلاح، فضای سایبری است که استعاره‌ای برای تشریح سرزمین غیرفیزیکی، متشکل از سیستم های کامپیوتری و زیرساخت‌های ارتباطی می‌باشد. در فضای سایبری نمی‌توان بوئید یا شنید (توسط حواس رایج)، ولی این گستره نیز دارای عناصر و اشیاء (object) خاص خود است: فایل ها، پیغام‌های الکترونیکی، عکس‌ها و ... . این فضا دارای مدل های انتقالی و حمل نقل نیز می‌باشد. برخلاف فضای حقیقی، سیر و گشت در این سرزمین بدون هیچ گونه

حرکت فیزیکی مقدور است، تنها با حرکت موشواره یا فشردن کلیدی در صفحه کلید [1].

جنگ سایبری

جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم های اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی دشمن (اطلاعات، پروسه های مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای) در یک فضای سایبری است. چنین عملیاتی به طور مشخص با اهداف نظامی، تجاری، سیاسی، فرهنگی و غیره انجام می‌پذیرد. بنابراین باید دارای ارزش افزوده و به اصطلاح بهره برداری از عناصر دشمن باشد، همانطوریکه هر نوع جنگ دیگر نیز در نهایت به سوء استفاده از منابع دشمن ختم خواهد شد. جنگ سایبری دارای اهمیت روز افزون برای مراکز نظامی، سرویس های جاسوسی، اطلاعاتی، سری و دنیای تجارت است ولی در مجموع هر دو دیدگاه نظامی و غیرنظامی را باید مدنظر داشت.

۲-۲- محدودهٔ عملیاتی

برای فضای سایبری نمی توان محدوده جغرافیائی تصور نمود. بنابراین جنگ سایبری نیز دارای مرز نیست. ولی باید توجه داشت که این تجسم به علت مقایسه مستقیم فضای سایبری با دنیای حقیقی است و در عمل فضای سایبری نیز دارای مرز است. محدوده عملیات سایبری بسیار گسترده است، از تولید پارازیت مخابراتی گرفته تا عملیات روانی، از تغییر صفحات وب یک سایت گرفته تا بمباران ایمیلی. ولی نهایتاً هدف اصلی تهدیدات، منابع اطلاعاتی هستند، به نحوی که امنیت ملی دشمن مورد مخاطره قرار گیرد. بنابراین بستر عملیات سایبری همانا زیرساخت‌های اطلاعاتی می‌باشند. محدودهٔ عملیات سایبری به طور مشخص در حدود منابع دشمن است ولی می‌تواند دربرگیرندهٔ اشیاء خود حمله کننده نیز باشد و یا در محدوده سایبری دیگر عوامل وابسته یا غیر وابسته باشد. برای تفهیم بهتر به این سناریو دقت کنید: حمله کننده‌ای قصد دارد اقدام به دزدیدن اطلاعات دشمن و فروش آنها به شخص ثالث نماید. وی از طریق یک کانال واسط به دشمن نفوذ می‌کند و نهایتاً اطلاعات نیز از همان کانال منتقل می‌شوند. سناریوی فوق دقیقاً نظیر نمونه حقیقی است که برای منابع اطلاعاتی ایالات متحده آمریکا محقق گردید و در آن حمله کنندهٔ برزیلی، اطلاعات را به طور غیرمستقیم با واسطه اشیاء دیگر به جمهوری شوروی سابق می‌فروخت.

در مورد محدوده عملیاتی باید این نکته را مدنظر داشته باشیم که با انتخاب نادرست محدوده عملیات، بروز مشکل در محدوده سایبری خود حمله کننده نیز محتمل است. این به علت نزدیکی و تداخل مرزهای سایبری است. تصور کنید که حمله کننده سایبری مبادرت به تهاجم به یک سایت اینترنتی می‌نماید و نهایتاً موجب پایین آمدن کارآیی آن سایت می‌گردد، ولی هدف از پائین آمدن سایت، انهدام (crash) سرور اصلی بوده است و یکی از سرورهای محدوده جغرافیائی حمله کننده به طور ناخواسته در محدود عملیاتی بوده است. این مشکل به ویژه با انتشار و نامتمرکز بودن خدمات ثبت دامنه، میزبانی فضای وب، ثبت آدرس اینترنتی و ارائه پهنای باند بسیار محتمل و رایج است.

بعنوان نمونه هایی از محدوده‌های عملیات سایبری، می‌توان از موارد ذیل نام برد:

- اشیاء بسترساز شبکه (روترها، سوئیچ ها، ماهواره ها).
- عناصر وب (سایت‌های وب، پایگاه‌های اطلاعاتی مبتنی بر وب)
- ایمیل بعنوان رایج ترین عنصر گذشته و حال در فضای سایبری

۲-۳- چه کسانی تهدید می کنند

تهدیدات سایبری از طرف چند گروه می‌تواند بوجود آید. اول از طرف هرکرهای نوجوان و آماتور که بعنوان تفریح و سرگرمی اینکار را شروع می‌کنند ولی پس از مدتی خود تبدیل به یک تهدید کننده و سوء استفاده کننده حرفه‌ای تبدیل می‌شوند. دوم از سوی کارمندان ناراضی یا اخراجی که برای ضربه زدن به سازمان و اثبات ناکارآمدی آن صورت می‌گیرد، گروه سوم کسانی هستند که اطلاعات حساس را منتشر می‌کنند و مالکیت معنوی آن را در اختیار رقبا قرار می‌دهند و یا اینکه در کلاهبرداری‌های آنلاین شرکت می‌کنند تا منافع مادی و غیر مشروع خود را براحتی تامین کرده باشند. گروه چهارم کسانی هستند که با مقاصد سیاسی (دیپلماتیک) یا نظامی دست به اینکار می‌زنند. خطرناک‌ترین تهدیدات از جانب این گروه وجود می‌آید زیرا علیرغم آنکه بسیار قوی، مؤثر و حرفه‌ای عمل می‌کنند، درصورت

لزوم کمترین ردپا را از خود بجا می‌گذارند و شما ممکن است تا مدتها متوجه سوء استفاده‌ای که از این ناحیه از شما می‌شود، نگردید. این حمله کنندگان از لحاظ توانایی و اهداف تکنیکی در قالب‌های زیر دسته بندی می‌شوند [8]:

۱) گروه نفوذگران کلاه سفید (White hat hackers): هر کسی که با دانش خود بتواند از سد موانع امنیتی یک شبکه بگذرد و به داخل شبکه راه پیدا کند اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند. هکرهای کلاه سفید متخصصین شبکه‌ای هستند که سوراخ‌های امنیتی شبکه را پیدا می‌کنند و به مسئولان گزارش میدهند.

۲) گروه نفوذگران کلاه سیاه (Black hat hackers): به این گروه کراکر (Cracker) هم میگویند. این افراد آدم هایی هستند که با دانشی که دارند وارد کامپیوتر قربانی خود شده و به دستکاری اطلاعات و یا جاسوسی کردن و یا پخش کردن ویروس و غیره می‌پردازند.

۳) گروه نفوذگران کلاه خاکستری (Gray hat hackers): شاید سخت ترین کار توصیف حوزه عمل این گروه از نفوذگرهاست. به این نفوذگرها بعضاً whacker هم میگویند، این گروه از نفوذگرها حد وسط دو تعریف گذشته هستند.

۴) گروه نفوذگران کلاه صورتی (Pink hat hackers): این افراد آدم های کم سوادی هستند که فقط با چند نرم افزار به خرابکاری و آزار و اذیت بقیه اقدام میکنند.

۳- الگوی کلی جنگ سایبری

در یک مدل واقع گرایانه با توجه به محدوده عملیات جنگ سایبری، خواهیم دید که الگوی آن اعم از جنگ‌های سنتی شبکه‌ای و الکترونیکی خواهد بود. در واقع یک جنگ سایبری از سه بخش عمده **جنگ شبکه‌ای، جنگ رایانه‌ای و جنگ فرماندهی و کنترل** تشکیل شده است. حوزه‌های اصلی جنگ شبکه‌ای عبارتند از: جنگ‌های چندرسانه‌ای، فرهنگی، دیپلماتیک، اقتصادی، روانی و ... . جنگ رایانه‌ای معمولاً در محیط اطلاعاتی محلی یا جهانی رخ می‌دهد و هدف آن تسلط (آگاهی یا تخریب) بر اطلاعات است. در این مدل مهمترین بخش، جنگ فرماندهی و کنترل است که جنگ الکترونیک (جنگال) یا جنگهای فیزیکی مرسوم، تنها زیر بخش‌هایی از آن محسوب می‌شوند. این بخش از اجزای زیر تشکیل شده است: جنگ الکترونیک، فریب نظامی، عملیات روانی، امنیت اطلاعات، تخریب فیزیکی، تخریب غیرفیزیکی[2] .

در این مدل نحوه عملکرد همان حمله و دفاع رایج است و دارای مولفه‌های زیر است:

انگیزه: بدون شک، حمله کننده باید دارای انگیزهٔ مشخص مستقیم یا غیر مستقیم باشد . درغیر این صورت، مراحل بعدی دارای بستر و پایه منطقی نخواهند بود.

هدف: با توجه به انگیزه، محدوده عملیات مشخص میگردد. این همان چیزی است که آن را هدف می‌نامیم. هدف ممکن است به بزرگی و گسترهٔ شبکه توزیع نیرو در یک کشور باشد و یا به کوچکی یک سیستم در یک شبکه محلی باشد. در اینجا بزرگی و کوچکی هدف مهم نیست، بلکه ارزش هدف تعیین کننده است. در عملیات سایبری، یک هدف که در شکل فیزیکی بسیار کوچک است می‌تواند دارای ارزشی بزرگتر و بیشتر از کیلومترها خاک داشته باشد.

جمع آوری اطلاعات: هر عملیاتی، چه فیزیکی و چه سایبری باید با آگاهی صورت پذیرد. بدون اطلاعات فقط نیرو و منابع از دست میرود، ضمن آنکه احتمال ردیابی و شناسائی برای دشمن افزایش میابد. کسب اطلاعات از عناصر سایبری دشمن به عنوان مهمترین بخش از عملیات سایبری مورد توجه است. از دید کارشناسان، جمع آوری اطلاعات از اهداف سایبری به مفهوم انجام ۵۰ درصد از کل عملیات است. در اینجا اطلاعات به مفهوم هر جنبه از هدف است که به نحوی با ایمنی سایبری آن در ارتباط باشد: بلوک ها و آدرس های اینترنتی/اینترانتی (IP Addresses) ، اسامی دامنه های عمومی و خصوصی، سرویسهای مبتنی بر پروتکل اینترنت (TCP/IP)، معماری سیستم ها و شبکه ها، مکانیسم های امنیتی و کنترل دسترسی، سیستم های شناسائی و ردیابی، شماره های تلفن، مکانیسم های تصدیق و ... . جمع آوری اطلاعات شامل شناسائی، وارسی و کنکاش می‌شود.

نقاط ضعف: وقتی اطلاعات حمله کننده درباره ماهیت سایبری هدف کامل شد، این مرحله آغاز می‌شود. این بخش ساده ترین قسمت عملیات است. با دانستن مشخصات هدف، تعیین عیوب سخت افزاری و نرم افزاری چندان دشوار نبوده و فقط زمان لازم است. اگر دشمن به چنین مرحله‌ای برسد، انجام حمله قطعی است.

نفوذ: پس از تعیین نقاط ضعف و با در نظر گرفتن اطلاعات به دست آمده و با آگاهی از مکانیسم های ردیابی، عملیات سایبری در جهت نفوذ به هدف آغاز می‌شود. این مرحله، اگرچه بخش پایانی عملیات است ولی زمان بیشتری را به خود اختصاص میدهد زیرا دارای قسمت‌های متعدد است.

۴- ویژگی های جنگ های سایبری

جنگ فیزیکی با جنگ سایبری از برخی جهات کاملاً شبیه هم هستند. مثلاً انگیزه اصلی در هر نوع جنگ قاعدتاً تصاحب منابع است و لذا هدف وارد آوردن ضرر و زیان به دشمن خواهد بود. در حقیقت فلج نمودن دشمن بدون در اختیار گرفتن منابع آن چندان معقول به نظر نمی رسد. بهترین روش برای شناخت ویژگی‌های جنگ سایبری این است که تصور و تجسم فیزیکی را از میان برداشته و صرفاً سایبری تفکر نمائیم. برای این منظور ویژگی دیگر انواع جنگ ها را در کنار ویژگی‌های جنگ سایبری بررسی می‌کنیم:

حمله از راه دور: اولین تفاوت جنگ سایبری با دیگر انواع جنگ ها و بخصوص جنگ فیزیکی ، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور یا اصطلاحاً به شکل remote است. برای حمله سایبری نیازی به حرکت فیزیکی ندارید و طبیعی است که این موضوع از متفاوت بودن منشا فضای سایبری و فضای حقیقی ناشی می‌گردد. درفضای سایبری سربازها و نقاط حمله می‌توانند در تمام دنیا پخش شوند.

دشواری در شناسایی و ردیابی: به سبب خصائصی که در ذات پروتکل های ارتباطی در فضای سایبری وجود دارد، عملاً شناسائی و ردیابی منبع اصلی حمله، بسیار دشوار و گاهی غیرممکن است. در حقیقت اگر در این خصوص، تشریک مساعی مرزهای سایبری را نادیده بانگاریم، شناسائی غیرممکن است. بعنوان مثال اگر به قالب سرآیند IP توجه نمائید خواهید دید که تغییر فیلد آدرس مبداء (یا همان Source Address) و سپس تزریق بسته در شبکه به سادگی و حتی توسط کاربران بسیار مبتدی مقدور است. بنابراین مبداء ناشناس و مبهم خواهد ماند.

محدودیت در انتقال: به سبب وابستگی فعلی فضای سایبری به پروتکلهای ارتباطی موجود، انتقال و عوامل وابسته به آن (نظیر سرعت، حجم، کیفیت، اعتبار و ...) با چالش محدودیت در این پروسه روبرو هستند. TCP/IP همچون چسبی تمام اینترنت را به هم متصل نموده است ولی این چسب دارای نواقص و محدودیت هایی است.

تهدید متوجه هر سه جنبه امنیت است: در جنگ فیزیکی، حمله کننده سعی در تهدید جنبه های فیزیکی زندگی انسان دارد. در جنگ سایبری، تهدید یکی از سه جنبه ایمنی اطلاعات، (یعنی: محرمانگی (Confidentiality)، صحت و تمامیت (Integrity) و در دسترس بودن (Availability))، موجب تهدید عنصر سایبری و اشیاء مرتبط با آن می‌گردد.

اندازه هدف: بزرگی و کوچکی هدف در جنگ‌های فیزیکی فوق العاده با اهمیت است. ولی در جنگ های سایبری، بزرگی عناصر با بزرگی فیزیکی آنها قابل فهم و مقایسه نیست و باید اندازه سایبری آنها را مدنظر داشت. در جنگ های فیزیکی به دنبال تخریب مناطق جغرافیائی بزرگتر هستند، ولی در جنگ سایبری باید اهداف مهم و اساسی (از نظر سایبری و نقش آنها در این فضا) را هدف قرار داد. این اهداف ممکن است از نظر فیزیکی بسیار ناچیز باشند ولی نقش بزرگی در فضای سایبری ایفا نمایند.

انتشار حمله: هدایت و راهبری حملات فیزیکی که از چندین محل آغاز میگردند بسیار دشوار است ولی حمله سایبری می‌توانند به سادگی از چندین منبع / کانال صورت پذیرد. نظیر حملات سایبری DDos، DRDos و Mini- DDos که بسادگی و تاثیرگذاری زیاد از چندین - صد / هزار / ده هزار - نقطه قابل اجرا هستند.

هزینه: بدون شک هزینه جنگ حقیقی از جنگ سایبری بیشتر است و این خصوصیت بارز فضای سایبری است که عوامل و عناصر سهل الوصول تر و ارزان تر هستند.

مسئولیت پذیری: از آنجائی که قوانین مدون، مشخص و مورد توافق بین المللی برای مبارزه و ایجاد دعاوی سایبری وجود ندارد، کشورها به سادگی از زیر بار مسئولیت حملات سایبری خود شانه خالی می‌کنند [3].

راهبری ساده: راهبری و هدایت جنگ سایبری به مراتب ساده تر از جنگ های حقیقی است. گاهی با فشار یک کلید و یا اشاره به یک شیء سایبری می‌توان آن را در موقعیت حمله و یا دفاع قرار داد، نیروها را گسترش داد یا عقب نشینی نمود.

شروع و پایان: شروع و پایان مشخصی برای این گونه جنگ ها وجود ندارد. زیرا به سبب عوامل درگیر در جنگ که همگی دارای

ماهیت سایبری هستند (یا می‌توانند باشند)، عملاً شروع و خاتمه یـا مجازی است و یا فوق العاده متعدد.

۵- راه‌های مقابله با تهدیدات سایبری (پدافند جنگ سایبری)

اکنون که فضای سـایبری، محـدوده عملیـات و ویژگـی‌هـای جنـگ سایبری معرفی و بررسی گردیـد، بـه روش‌هـای مقابلـه بـا آن مـی-پردازیم. برای این منظور ابتدا به شناخت نیازمندی‌ها و ابزار و سـلاح این جنگ پرداخته و بر این اسـاس روش‌هـای مقابلـه بـا آن معرفـی خواهد شد. لازم بذکر است که وقتی صحبت از یک عملیات سایبری می‌کنیم منظور هر دوجنبه حمله و مقابله با حمله (دفاع) مـی‌باشـد زیرا این هر دو دوروی یک سکه هستند.

۵-۱- نیازمندی‌های یک عملیات سایبری

عملیات سایبری دارای ملزومات خاص خود است که عبارتند از: توان انسانی متخصص و تجهیزات مورد لزوم. البتـه اولـین نیـاز، حضـور و اتصال در این فضا است که ما آنرا مفروض می‌گیـریم. بعبـارت دیگـر اشیائی که در فضای سایبری حضـور نداشـته باشـند، عمـلاً از گزنـد حمله مصون هستند و نیز خود مبادرت به حمله نمی نمایند [4].

اولین نیاز، توان نیروی انسانی متخصص استکه در آن کیفیت بیش از کمیت دارای اهمیت اسـت. در حقیقـت تعـداد نیـروی انسـانی یـک عملیات سایبری ملاک نیست، بلکه متدهای مورد اسـتفاده ایشـان و نحوه عملکرد آنها مدنظر است. درهر صـورت، نیـروی انسـانی راهبـر عملیات سایبری است. از طرح ریزی و جمع آوری اطلاعات گرفته تـا تحلیل و اجرای حمله. به طور مشخص، اولین تـوان تخصصـی مـورد نیاز در یک عملیات سایبری (آفند یا پدافنـد)، دانـش شـبکه اسـت. سرباز سایبری باید بداند که بستر ارتباطی چگونه عمـل مـی‌نمایـد و مدیوم شبکه دارای چه خصوصیات ذاتی است (در مـورد اینترنـت بـا تمام گستردگی آن، نقطه اتکـاء پروتکـل TCP / IP اسـت). دومـین قابلیت مهم، شـناخت اجتماعـات مختلـف اسـت، بـه عبـارت دیگـر، سـربازان سـایبری بایـد بـه نـوعی مهندسـان اجتمـاعی (Social Engineer) باشند. آمـار و ارقـام مسـتند حـاکی از آن هسـتند کـه مهندسی اجتماعی اکنون بالاترین تهدید فضـای سـایبری محسـوب می‌گردد زیرا به شکل بسیار ظریفی بر تعامل بین این فضـا و محـیط فیزیکی تکیه دارد.

دومین نیاز توان تجهیزاتی است. مسلماً تجهیزات عام یـک عملیـات سایبری، همانا عناصر رایج و عمومی فضـای سـایبری هسـتند، ولـی برای انجام حرکات خاص باید دارای تجهیزات خاص بود یا به عبارت دیگر باید عناصر خاصی از فضای سایبری را در دست داشت.

۵-۲- ابزار و سلاح های جنگ سایبری

سلاح جنگ سایبری، مخلوطی از دانش و تجهیزات است. مسـلماً دانش تخصصی بالاترین اثر را دارد ولی بدون شک ابـزار نیـز لازم است. در مورد استفاده از ابزار باید به این نکتـه توجـه شـود کـه ابتدا باید تکنیک طراحی گردد و سـپس ابـزار آن تولیـد گـردد و برعکس عمل نشود. با حضور در بزرگراه اطلاعاتی نظیر اینترنـت، بسیاری از ابزارها، بدون صرف وقت زیـادی در دسـترس هسـتند، ولی که نحوه استفاده از آنها و زمینه دانـش مهـم اسـت. معمـولاً ابزارهای جنـگ هـای سـایبری را میتـوان در اجتمـاع نفـوذگران (Hacker Community) یافت.

اگـر بخـواهیم سـلاح و ابزارهـای سـایبری را دسـته بنـدی نمـائیم می‌توانیم دسته بندی زیر را در نظر بگیریم [5]:

ابزارهای شناسایی: عموم سـلاح هـای شناسـائی در خـود فضـای سایبری وجود دارند. قاعدتاً اهداف سهل الوصـول تـر دارای و هویـت سایبری مشخصی بوده و می‌توان آنها را به سادگی تعقیب نمـود. بـه نمونـه هـای کلـی ایـن ابزارهـای توجـه نمائیـد: اطلاعـات عمـومی، موتورهـای جسـتجوی دامنـه‌هـا، ثبـات دامنـه و آدرس اینترنتـی، تکنیک‌های Trace Routing ، ابزارهای شناسائی DNS و ابزارهـای شناسائی شبکه و همبندی آن.

ابزارهای وارسی: وارسی هدف، همانند کوبیدن به دیوارها برای پیدا کردن درب ها و پنجره هاست. سرباز سایبری بـا اقـدامات قبلـی بـه لیستی از شبکه‌ها و آدرس های IP دست خواهد یافت و می‌دانیم که این تکنیک ها، اطلاعات ذی قیمتی را برای وی فراهم خواهند نمود. با سلاح های وارسی باید سیستم های زنده و فعال (alive) و آنهایی را که از طریق اینترنت قابل دسترسی هستند را مشـخص نمـود. بـه نمونه‌های عـام از ایـن ابزارهـا عبارتنـد از: انـواع جـاروب کننـده هـا (Sweep) و انواع وارسی کننده های پورت های TCP وUDP. بایـد توجه داشت که وقتـی از ابزارهـای وارسـی اسـتفاده میشـود، اولـین ردپاهای حاکی از یک حمله قریب الوقوع، ثبت می‌گردد. تکنیک‌های

وارسی پنهان و بدون صدا در این بخش ، از اهمیت بالائی برخوردارند [6].

ابزارهای کنکاش: سلاحهای کنکاشگر عموماً در خود سیستم عاملها وجود دارند. این ابزارها مبادرت به بیرون کشیدن اطلاعات خاص سیستم عامل و شبکه، نظیر عناصر کاربری و نرم افزارهای موجود، می‌نمایند. نمونه‌هایی از این ابزارها عبارتند از: ابزارهای کنکاش در کاربران و گروه های فعال و غیرفعال یک سیستم عامل، ابزارهای کنکاش در سیاست‌های حاکم بر OS ها و ابزارهای ربودن و گرفتن نشانه‌ها (banner).

ابزارهای نفوذ: همانطور که قبلاً هم اشاره شد، با دارا بودن اطلاعات کافی از هدف، تکنیک و ابزار نفوذ چندان دور از دسترس نیست. این ابزارها به دو نوع سایبری و سایبری/ فیزیکی تقسیم می‌شوند.

سلاح های پنهان: گاهی برای نفوذ مجدد به یک هدف سایبری لازم است تمام مراحل کنکاشگرانه تکرار شود. برای این منظور حمله کننده مبادرت به جا دادن سلاح های پنهان می‌نماید تا بعداً بتواند اینکار راتکرار کند. برخی از ابزارهای مربوطه عبارتند از: انواع ویروس ها و کرم ها، انواع اسب های تروا و نقاط پنهان در سیستم‌های عامل.

جنگ افزارهای حملات Dos : گاهی اوقات هدف از حمله سایبری نفوذ نیست بلکه از کاراندازی و ممانعت از سرویس اشت که در این صورت استفاده از متدها و ابزارهای حملات Dos معمول است.

سلاح مهندسی اجتماعی: برای بهره‌برداری از عیوب کاربران، شناخت ایشان لازم است و این شناخت بر اساس کنکاش در جامعه دربرگیرنده آنها میسر می‌گردد. این پروسه Social Engineering یا مهندسی اجتماعی نام دارد. شیوه کلاسیک اجرای چنین حملاتی با جازدن اشیاء به جای اشیاء دیگر مورد اعتماد در مجموعه هدف است.

مهندسی اجتماعی نیازی به استفاده از رایانه ندارد و سلاح‌های مهندسی اجتماعی، بخش ابتدائی از فناوری‌های پیشرفته فضای سایبری محسوب می‌گردند [7].

در انتهای این بخش، توجه شما را به این مطلب جلب می‌کنیم که اولاً در بین تمام سلاحهای سایبری، سلاحی که قابلیت اتوماتیزه شدن را دارد، دارای ارزش بیشتری نزد سربازان سایبری است و ثانیاً اغلب سلاح های سایبری، به دنبال تائید و جلب اعتماد هدف خود هستند و این خصوصیت بارزی از فضای سایبری است که هر عنصری تحت شرایط خاص می‌تواند خود را به جای شیء دیگری جا بزند. ساده‌ترین نماد چنین عملی، حدس زدن کلمه رمز شیئی است که به شما تعلق ندارد.

۵-۳- نقاط آسیب پذیر در جنگ‌های سایبری

در هر نبردی بدون شک نقاطی آسیب پذیرتر هستند که دارای درگیری بیشتری در فضای نبرد هستند. در حقیقت میزان آسیب‌پذیری، ارتباط مستقیم با میزان تماس دارد. ولی به طور مشخص، در فضای سایبری، عناصر تنها (مانند سیستم‌های Stand – alone ، شبکه‌های خصوصی و ...) در مقایسه با فضاهای عمومی (مانند اینترنت، وب و ...) امن‌تر هستند.

۵-۴- روش‌های مقابله

حال که ملزومات جنگ سایبری بررسی شد، به روش‌های مقابله می‌پردازیم. بهترین دفاع در جنگ سایبری بالا بردن سطح ایمنی عناصر درگیر است. ولی سوال اساسی این است که چه سطح از ایمنی برای اشیاء سایبری لازم است؟ آیا تمام عناصر دارای ارزش یکسان امنیتی هستند؟ آیا باید هر عنصری را در حد توان ممکن حفاظت نمائیم؟

به طور خلاصه می‌توان گفت که هر یک از عناصر درگیر در فضای سایبری، باید به اندازه ارزش خود حفاظت گردند. در غیر این صورت، انتخاب مکانیسم‌های دفاعی چندان بهینه نبوده و دارای هزینه‌های سرسام آورخواهد بود.

۵-۴-۱- تاکتیک‌ها

برخی از عوامل هستند که نقش سیاست‌گذاری و تعیین کننده دارند و اغلب برای مدت‌های طولانی ثابت بوده و تغییر نمی‌کنند. ما از آنها بعنوان تاکتیک یاد می‌کنیم. برخی از آنها عبارتند از:

- به کارگیری مدلهای جدید و بروز امنیت سایبری بر پایه نیازمندی‌ها
- امنیت سایبری باید در سطوح ارشد مورد توجه قرار گیرد.
- نگاه کاربران به امنیت بعنوان یک امر اعتقادی باشد نه یک امر پیرایشی
- به جای «پیشبرد تکنولوژی» به فکر «پشتیبانی از خود» باشید.
- حفاظت از اطلاعات به جای حفاظت از محیط

- اقدامات لازم برای اطمینان از امنیت سایبری

۵-۴-۲- تکنیک ها

۱) امنیت فیزیکی یا تدابیر فنی:

امنیت فیزیکی طیف وسیعی از تدابیر را دربر می‌گیرد که استقرار تجهیزات در مکان‌های امن و به دور از خطر نفوذگران، تنها یکی از این تدابیر است. در بررسی امنیت فیزیکی و اعمال آن، ابتدا باید به خطراتی که از این طریق شبکه را تهدید می‌کنند، نگاهی داشته باشیم. سپس می‌توان به راه حل ها و ترفندهای دفاعی در برابر آنها پرداخت. برخی از تدابیر مهم فیزیکی بشرح زیرند [11]:

افزونگی در محل استقرار شبکه: منظور ایجاد سیستمی کامل و مشابه شبکهٔ اصلی (چه از بعد تجهیزات و چه از بعد کارکرد) در حال کار است. شبکهٔ ثانویهدر محلی که می‌تواند از نظر جغرافیایی با شبکهٔ اول فاصله‌ای نه چندان کوتاه داشته باشد برقرار می‌شود. با استفاده از این مکانیسم، علاوه بر آنکه در صورت رخداد وقایعی که کارکرد هر یک از این دو شبکه را مختل می‌کند (مانند زلزله)، می‌توان از شبکهٔ دیگر به طور جایگزین استفاده کرد، در استفاده های روزمره نیز در صورت ایجاد ترافیک سنگین بر روی شبکه، حجم ترافیک و پردازش بر روی دو شبکهٔ مشابه پخش می‌شود تا زمان پاسخ به حداقل ممکن برسد.

توپولوژی (همبندی) شبکه: طراحی توپولوژیکی شبکه، یکی از عوامل اصلی است که در زمان رخداد حملات فیزیکی می‌تواند از خطای کلی شبکه جلوگیری کند. لذا در این مقوله سه توپولوژی اصلی را بررسی می‌کنیم.

توپولوژی دنباله‌ای (سری) : در این توپولوژی با قطع خط تماس میان دو نقطه در شبکه، کل شبکه به دو تکه منفصل تبدیل شده و امکان سرویس دهی از هر یک از این دو ناحیه به ناحیه دیگر سلب می‌شود.

توپولوژی ستاره: در این توپولوژی، در صورت رخداد حمله فیزیکی و قطع اتصال یک نقطه از سرور اصلی، سرویس دهی به دیگر نقاط دچار اختلال نمی‌گردد. ولی از آنجایی که سرور اصلی در این میان نقش محوری دارد، در صورت اختلال در کارایی آن (بر اثر حمله فیزیکی)، ارتباطات کل شبکه دچار اختلال می‌شود، با در نظر گرفتن افزونگی برای سرور اصلی می‌توان از احتمال رخداد چنین حالتی کاست.

توپولوژی مش: در این توپولوژی که (در حالت فول مش) تمامی نقاط ارتباطی با دیگر نقاط در ارتباط هستند، هر گونه اختلال فیزیکی در سطوح دسترسی منجر به اختلال عملکرد شبکه نخواهد شد، هرچند که زمان بندی سرویس دهی را دچار اختلال خواهد کرد. پیاده سازی چنین روش با وجود امنیت بالا، به دلیل محدودیت های اقتصادی، تنها در موارد خاص و بحرانی انجام می‌گیرد.

محل های امن برای تجهیزات: در تعیین یک محل امن برای تجهیزات دو نکته باید مورد توجه قرار بگیرد: اول یافتن مکانی که به اندازه کافی از دیگر نقاط مجموعه متمایز باشد ، به طوری که هر گونه نفوذ در محل آشکار باشد. دوم آنکه محل موردنظر در داخل ساختمان یا مجموعه‌ای بزرگتر قرار گرفته باشد تا تدابیر امنیتی به کار گرفته شده برای مجموعهٔ بزرگتر خود بخود برای امن سازی محل اختیار شده نیز به کار گرفته شده باشد. در مجموع رعایت اصول زیر نیز به این امر کمک می‌کند: محدودسازی دسترسی به تجهیزات شبکه بروشهای فیریکی مانند قفلها و مکانیزم های دسترسی دیجیتالی به همراه ثبت زمانها و استفاده از دوربین‌های پایش در ورودی محل های استقرار تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه‌های داده.

انتخاب کانال ارتباطی امن: هرچند که امروزه زمان حملهٔ فیزیکی به شبکه های کامپیوتری، آنگونه که در قدیم شایع بوده، گذشته است و در حال حاضر تلاش اغلب نفوذگران برای به دست گرفتن کنترل یکی از سرویس دهنده های شبکه معطوف شده است، ولی گونه‌ای از حملات فیزیکی کماکان دارای خطری بحرانی است. عمل شنود بر روی سیم های مسی، چه از نوع هم محور و چه زوج‌های تابیده، هم اکنون نیز از راه های نفوذ به شمار می‌آیند. در حال حاضر، امن‌ترین روش ارتباطی در لایه فیزیکی، استفاده از فیبرهای نوری است. در این روش به دلیل نبود سیگنال های الکتریکی، هیچ گونه تشعشعی از نوع الکترومغناطیسی وجود ندارد، لذا امکان استفاده از روش‌های معمول شنود به پایین ترین حد خود نسبت به استفاده از سیم مسی در ارتباطات می‌شود [12].

منابع تغذیه: جریان داده های شناور در شبکه، بدون وجود منابع تغذیه، غیرممکن است، لذا چگونگی چینش و نوع منابع تغذیه و قدرت آنها نقش به سزایی دارد. در این مقوله باید به دو نکته توجه داشت: اول طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه است که این طراحی باید به گونه‌ای باشد که

تمامی تجهیزات فعال شبکه، برق مورد نیاز خود را بدون فشار به شبکهٔ تامین نیرو، به دست آورند و دوم وجود منابع تغذیه پشتیبان است، به گونه‌ای که تعداد آنها طوری باشد که نه تنها در مواقع نیاز به منابع تغذیه پشتیبان کفایت کند، بلکه امکان تامین افزونگی مورد نیاز برای تعدادی از تجهیزات بحرانی درون شبکه را هم فراهم کند.

عوامل محیطی: یکی از نکات بسیار مهم در امن سازی فیزیکی تجهیزات و منابع شبکه، امنیت در برابر عوامل محیطی است. نفوذگران در برخی از موارد با تاثیرگذاری بر روی این عوامل، باعث ایجاد اختلال در عملکرد شبکه می‌شوند. از مهمترین عواملی که در هنگام بررسی امنیتی یک شبکه باید در نظر گرفت، می‌توان به دو عامل زیر اشاره کرد: اول احتمال حریق که عموماً غیرطبیعی است و منشاء انسانی دارد و دوم زلزله، طوفان و دیگر بلایای طبیعی.

با وجود آنکه احتمال رخداد برخی از این عوامل، مانند حریق، را می‌توان تا حدود زیادی محدود نمود، ولی تنها راه حل عملی و قطعی برای مقابله با چنین وقایعی، وجود یک سیستم کامل پشتیبان برای کل شبکه است.

۲) امنیت غیرفیزیکی یا تدابیر نرم‌افزاری:

با مروری بر روند اعمال امنیت شبکه در چند دهه ی اخیر دیده می-شود که عوامل غیر فیزیکی بیشترین اثرگذاری را دارند. در این میان دیواره‌های آتش، جزو اولین روش های حفاظت غیرفیزیکی در شبکه بوده است. تله های سیستمی، سیستم‌های تشخیص نفوذ و شبکه‌های خصوصی مجازی نیز پس از آن پا به عرصه وجود گذاشتند. امروزه زیرساخت کلید عمومی و یا اصطلاحاً (PKI) به عنوان یکی از بهترین روش ها برای اعمال امنیت در شبکه شناخته می‌شوند.ذیلاً هریک از این عوامل به طور مختصر توضیح داده می‌شوند .

دیوار آتش: دیوار آتش کامپیوترهایی را که به صورت شبکه به هم وصل شده اند را از حملات نفوذگران که می‌توانند اطلاعات داخل شبکه را کشف کنند، یا از بین ببرند و یا سرویس‌ها را از کار بیاندازند، محافظت می‌کند. دیوار آتش ممکن است یک دستگاه سخت افزاری یا یک نرم افزار باشد که اطلاعاتی که از طریق اینترنت به داخل شبکه وارد می‌گردد را فیلتر کرده و به نفوذگران اجازه ورود به سیستم و دسترسی را نمی‌دهد. دیوار آتش در محل اتصال دو شبکه قرار می‌گیرد.

تله های سیستمی: یک تله سیستمی یک سیستم جمع آوری اطلاعات می‌باشد که با استفاده از ارزش کاذب خود، اطلاعاتی راجع به فعالیت‌های نامجاز جمع آوری می‌کند. تله‌های سیستمی از این جهت که مستقیماً هیچ مشکلی را حل نمی‌کنند، شبیه دیواره‌های آتش و یا سیستم‌های تشخیص دخول سرزده نمی باشند، در عوض ابزار قابل انعطافی هستند که به اشکال مختلف قابل استفاده هستند.

سیستم تشخیص نفوذ: تشخیص نفوذ عبارت است از فرآیند تشخیص تلاش هایی که جهت دسترسی غیرمجاز به یک شبکه یا کاهش کارایی آن انجام می‌شوند. در تشخیص نفوذ باید ابتدا درک صحیحی از چگونگی انجام حملات پیدا کرد، سپس بنابر درک به دست آمده روش دو مرحله‌ای را برای متوقف کردن حملات برگزید. اول اینکه مطمئن شوید که الگوی عمومی فعالیت های خطرناک تشخیص داده شده است. دوم اینکه اطمینان حاصل کنید که با حوادث مشخصی که در طبقه بندی مشترک حملات نمی‌گنجند، به سرعت برخورد می‌شود. به همین دلیل است که بیشتر سیستم های تشخیص نفوذ (IDS) بر مکانیزم هایی جهت به روزرسانی نرم افزارشان متکی هستند که جهت جلوگیری از تهدیدات شبکه به اندازه کافی سریع می‌باشند. البته تشخیص نفوذ به تنهایی کافی نیست و باید مسیر حمله را تا هکر دنبال کرد تا بتوان به شیوه مناسبی با وی نیز برخورد کرد.

شبکه خصوصی مجازی: شبکه خصوصی مجازی یا VPN امکانی است برای انتقال ترافیک خصوصی بر روی شبکه عمومی. معمولاً از VPN برای اتصال دو شبکه خصوصی از طریق یک شبکه عمومی مانند اینترنت استفاده می‌شود. VPN به این دلیل مجازی نامیده می‌شود که از دید دو شبکه خصوصی، ارتباطشان از طریق یک ارتباط خصوصی برقرار است، اما در واقع شبکه عمومی این کار را انجام می‌دهد. در پیاده سازی VPN معمولاً اتصال دو یا چند شبکه خصوصی از طریق یک تونل رمز شده انجام می‌شود و بدینوسیله اطلاعات در حال تبادل بر روی شبکه عمومی از دید سایرین محفوظ می‌ماند.

زیرساخت کلید عمومی (PKI): در این روش برای هر کاربر، یک گواهی صادر می‌شود که از آن طریق می‌توان بسیاری از نیازهای امنیتی را برطرف نمود. تولید گواهی (Certification) و عمل تعیین اعتبار (Validation) دو عامل اصلی مورد نیاز در PKI می‌باشند. هدف در عمل اول ایجاد ارتباط بین کاربر (یا شرکت) و کلید عمومی

آن بوده و در عمل دوم، تعیین اعتبار گواهی می‌باشد. با توجه به مطالب ذکر شده، PKI را می‌توان به صورت مجموعه‌ای از سخت افزار، نرم افزار، کاربران، سیاست ها و رویه‌هایی که برای ایجاد مدیریت، ذخیره، توزیع و انهدام گواهی مبتنی بر رمزنگاری با کلید عمومی مورد نیاز می‌باشند، تعریف نمود.

۳) تدابیر مدیریتی

کنترل‌های مدیریتی غالباً به برقراری کنترل‌ها از طریق دستورالعمل-ها و روش‌ها تاکید دارد، مانند انتخاب صحیح کارکنان، آموزش و پرورش و سرپرستی آنها در حیطه سیستم‌های اطلاعاتی. برخی از این نوع اقدامات عبارتند از:

- رشد تعهد به سازمان
- ممانعت از دسترسی کارکنانی که اخراج یا بازنشسته شده‌اند و یا انتقال یافته اند.
- تغییر دوره‌ای کلمه عبور کارکنان.
- تدوین و تهیه استانداردهای توسعه سیستم‌ها و مستندات آن.
- انجام بازرسی‌های مستمر از سیستم ها (برنامه ای و دارای زمانبندی)

مدیران شبکه (سیستم)، مدیران سازمان و کاربران معمولی جملگی عوامل انسانی در یک سازمان می‌باشند که حرکات اشتباه هر یک میتواند پیامدهای منفی در ارتباط با امنیت اطلاعات بدنبال داشته باشد.

۶- کاربردهای عملیات روانی

بی‌گمان فضای سایبری (و بطور خاص اینترنت) در آینده بیش از پیش به منزله یکی از فضاهای اطلاع‌رسانی و همچنین به منزله ابزاری برای نفوذ و یا فشار بر تصمیم‌گیرندگان به کار می‌رود. بنابراین میدان جنگ کنونی، افکار و اذهان مردم است و معیار برد و باخت به فرهنگ هر جامعه بستگی دارد. سلاح‌های کشتارجمعی، در واقع سلاح‌های انفصال جمعی است و در حال حاضر، مناطق جنگی گزارش‌های خبری در اینترنت‌اند. طبق گزارشی در زمینه علوم دفاعی، مرکز ثقل کاربران رسانه‌ها به سرعت به سوی اینترنت گرایش می‌یابد. اکنون دیگر واژه پخش به معنای چگونگی روش کار یک رسانه نیست و مخابره برنامه‌های رادیویی و تلویزیونی نیز دیگر نقش چندانی در شکل‌دهی نظرات و آرای مردم ندارند. امروزه، برای ارتباط با مردم باید با استفاده از عملیات روانی و محیط اطلاعاتی پیشرفته بین‌المللی به اذهان آنان نفوذ یافت و بدون اعمال تغییرات اساسی در نقش‌های روزمره نیروهای عملیات روانی، نخواهیم توانست با چرخه تولید اطلاعات دشمن مقابله کنیم. اینترنت همان‌گونه که رسانه‌ای با توان تأثیرگذاری بالقوه و روزافزون است، می‌تواند برای عملیات روانی نیز ابزار مناسبی باشد. اگر به اینترنت از جنبه مخاطب و اهداف بنگریم، ظرفیت‌هایش به منزله ابزاری برای اجرای عملیات روانی افزایش می‌یابد. در حال حاضر، عاملان دولتی و غیردولتی برای کسب حمایت و تأیید داخلی و بین‌المللی به صورت فزاینده‌ای به اینترنت روی آورده‌اند و از این طریق، عملیات روانی را در میان سازمان‌های بین‌المللی، قانونی جلوه می‌دهند. برای نمونه، گروه اجرای موافقت‌نامه ۱۹۹۷ دیتون وابسته به سازمان تأمین امنیت و همکاری اروپا برای تکمیل اطلاعات متعارف عمومی و اطلاعاتی در مورد رأی‌دهندگان، از اینترنت استفاده کرد و بدین طریق نه تنها بر مشروعیت خود به منزله سازمانی بین‌المللی تأکید کرد، بلکه توانست حمایت دیگران را نیز به دست آورد. در واقع مردم به تدریج با عملیات اطلاعاتی آشنا می‌شوند و به چارچوب آن پی می‌برند. در گذشته در این نوع عملیات اطلاعات از مردم پنهان نگه داشته می‌شد، اما اکنون اینکار ممکن نیست بلکه مهم‌ترین اصل این است که درک، دریافت و متعاقب آن رفتار مردم را تحت تأثیر قرار داد. برای رسیدن به این هدف، باید اطلاعات موجود در دسترس مردم را دستکاری کرد و تغییر داد تا در موقعیت مورد نظر، رفتار مطلوب، از آنها سر بزند. مخالفان بالقوه نیز به این موضوع پی برده‌اند، همان طور که آرکیولا و رونفلد می‌گویند، دشمنان ما بیشتر علاقه‌مندند که مطالب را بر روی سایت قرار دهند تا اینکه از آن برداشت کنند. بنابراین، آنها می‌توانند از اینترنت برای بسیج نیروها و انتشار نظراتشان استفاده کنند و سعی دارند بر نظرات و عقاید سایر مردم تأثیر گذارند [9].

با توجه به مطالب یاد شده، اینترنت چه برای اهداف تهاجمی و چه برای اهداف دفاعی استفاده شود، ابزار بسیار مهمی برای اجرای عملیات‌های روانی به شمار می‌رود و باعث می‌شود تا نیروهای استفاده‌کننده از این رسانه به توانایی‌ها و برتری‌های اطلاعاتی چشمگیری دست یابند. کاملاً واضح است که دولت یا نهادی که

کنترل، مدیریت و سازماندهی اطلاعات را در دست دارد، همواره قدرتمندترین است [10].

۷- نتیجه

برای معرفی و ارائه سناریوهای مقابله با تهدیدات سایبری ابتدا به شناخت تهدیدات و محدودهٔ عملیاتی آنها در حوزه مورد نظر پرداخته شد. سپس ویژگی‌ها و الگوی یک جنگ سایبری را تعریف نموده و بر اساس این مبانی راه های مقابله با تهدیدات را معرفی و بررسی نمودیم. در این راستا از نیازمندی های یک جنگ سایبری شروع کرده و ابزارها و سلاح های آن را معرفی و نقاط آسیب پذیر را معرفی نمودیم و دیدیم که برای مقابله به تاکتیکها و تکنیک های مناسبی نیازمندیم. تاکتیک ها در سطح کلان و سیاست گذاریهای ارشد مطرح میشوند و تکنیک‌ها طیف وسیعی از روشهای مقابله براساس مصادیق عینی ضعفها، تهدیدات و درگیری‌ها را دربرمی‌گیرد، از مولفه‌های متعدد در امنیت فیزیکی گرفته تا عوامل و ابزارهای غیرفیزیکی و نرم افزاری. در انتها نیز نگاهی گذرا به کاربردهای عملیات روانی در جنگ های سایبری داشتیم.

بدیهی است آنچه که در این مقاله مطرح شد بیشتر به کلیات و مباحث زیربنایی از هر دو منظر فنی و غیر فنی توجه داشت و برای پرداختن به هر مقوله و زیرشاخه های آن، با جزئیات وبا تحقیق عمیق‌تر می‌توان مقالات متعددی ارائه نمود.

مراجع

[1] Tim Bass & Lt. Col. Glenn Watt.(6/1997), A SIMPLE FRAMEWORK FOR FILTERING QUEUED SMTP MAIL (CYBERWAR COUNTERMEASURES). IEEE. 0-7803-4249

[2] Mikael Simovits& Tomas Forsberg, Business Intelligence and Information Warfare on The Internet, Mikael Simovits: ICL SVENSKA AB-Torshamnsgatan 36-164 93 Kista- Suède Tomas Forsberg: ABB INFOSYSTEMS AB- StoraGatan 3-721 80 Västerås – Suède.

[3] O. Sami Saydjari, (December 2002), Defending Cyberspace .

[4] Dr. J. Ken Williams, (4/2003). Zel Technologies, LLC

[5] GadiEvron, (Winter/Spring 2008), Science & Technology-Battling Botnets & Online Mobs, Georgetown Journal of International Affairs.

[6] James Walden, A Real-Time Information Warfare Exercise on A Virtual Network, James Walden: University of Toledo 1005 Abbe Rd N Elyria, OH 44035 jwalden@eecs.utoledo.edu .

[7] Clay Wilson, (March 20, 2007), CRS Report for Congress-Information Operations, Electronic Warfare, and Cyberspace: Capabilities and Related Policy Issues, Congressional Research Service. Clay Wilson : Specialist in Technology and National Security Foreign Affairs, Defense, and Trade Division.

[8] AndrzejBiałas.” It Security Development- Computer-Aided Tool Supporting Design and Evaluation”, AndrzejBiałas: Institute of Control Systems, 41-506 Chorzów, Długa 1-3, Polandabialas@iss.pl .

[9] Mehdi Akhtar Mohagheghi, The sociology of internet.

[10] David S. Alberts, John J. Garstka, Fredrick P, Stein, (August 1999/Second printing February 2000), Network centric warfare : developing and leveraging information superiority, 2nd Edition (Revised).

[11] Dorothy Denning, Information Warfare and Security, Addison-Wesley, 1999 5- DoD dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/jel/doddict/data/i/index.html.

[12] Charles Billo.(November 2004), Cyber Warfare & Analysis of The Means & Motivations of Selected Nation States, INSTITUTE FOR SECURITY TECHNOLOGY STUDIES.Revised December 2004, Charles Billo: Welton Chang 45 Lyme Road Hanover, NH 03755 603-646-0700.

This page is intentionally left blank