ششمین همایش ملی تجارت و اقتصاد الکترونیکی

چالشهای فراروی تجارت و اقتصاد الکترونیکی در عصر جنگ سایبری

علیپور، حمید. فوق لیسانس، مدیرکل توسعه و مهندسی سازمان فناوری اطلاعات، alipour@itc.ir ، ۰۹۱۲۱۳۳۵۵۳۴

چکیده: گسترش اینترنت و کاربردهای آن و ارایه خدمات الکترونیکی توسط بنگاههای تجاری، بانکها و موسسات مالی و اعتباری، کاهش هزینه‌ها و سرعت بالاتر و تنوع بیشتر خدمات ارایه شده به مردم را دربر داشته و گرایش روزافزون مردم به استفاده از این خدمات، نقش آن را در زندگی روزمره مردم پررنگ‌تر کرده است. از سوی دیگر گرایش به استراتژیها و تاکتیکهای جنگ سایبری، امنیت این خدمات را با چالش بیشتر روبرو می‌کند. با در نظر گرفتن وضعیت و سطح فناوری کشور ایران و دشمنان آن، تمام استراتژیهای جنگ سایبری، چالشهایی جدی را برای تجارت و اقتصاد الکترونیکی در کشور ایجاد می‌کنند. جنگهای سایبری می‌توانند مخفیانه دربگیرند و هیچگاه کشورهای متخاصم شناخته نشوند، لذا احتمال وقوع آن بسیار بیشتر از جنگهای فیزیکی است. اهداف یک جنگ سایبری محدود به مجتمع‌ها و تاسیسات نظامی نیست و فعالیتهای مالی و اقتصادی دولتی و خصوصی نیز از اهداف مهم آن هستند .در فضای بدون مرز سایبری، دفاع تنها بر دوش نیروهای نظامی نیست و لازم است کلیه ذی‌نفعان و اهداف احتمالی چنین جنگهایی در دفاع مشارکت داشته باشند. عدم توسعه هماهنگ امنیت فناوری اطلاعات و عدم توجه به توسعه ساختارهای دفاع ملی سایبری، تهدیدی فزاینده برای تجارت و اقتصاد کشور ایجاد خواهد کرد.

کلید واژه‌ها: جنگ سایبری، تجارت الکترونیک، فناوری اطلاعات، دفاع سایبری، امنیت.

---

۱. مقدمه

گسترش اینترنت و کاربردهای آن و ارایه خدمات الکترونیک توسط بنگاههای تجاری، بانکها و موسسات مالی و اعتباری، کاهش هزینه‌ها و سرعت بالاتر و تنوع بیشتر خدمات ارایه شده به مردم را دربر داشته و گرایش روزافزون مردم به استفاده از این خدمات، نقش آن را در زندگی روزمره مردم پررنگ‌تر کرده است. از یک‌سو گسترش این کاربردها، منجر به افزایش بیشتر وابستگی به آنها

می‌شود و از سوی دیگر گرایش به استراتژیها و تاکتیکهای جنگ سایبری بعنوان گونه‌ای از جنگ نرم، به علت مزایای مختلف از جمله هزینه‌های کمتر آن، امنیت این خدمات را با چالش بیشتر روبرو می‌کند. در این مقاله با در نظر گرفتن استراتژیهای جنگ سایبری و مقایسه سطح فناوری سایبری در ایران و کشورهای متخاصم تلاش گردیده است چالشهای فراروی اقتصاد و تجارت الکترونیکی برشمرده شود و راهکارهایی برای بهبود وضعیت امنیت سایبری در این زمینه ارایه شود.

۲. جنگ سایبری و تهدیدهای ناشی از آن

از اواسط دهه ۱۹۸۰ استراتژیها و تاکتیکهای جنگ سایبری بیشترین توجه را در بین برنامه‌ریزان دفاعی در کشورهای صنعتی به خود جلب کرده است. [۱] رشد و همه‌گیری اینترنت و گستردگی کاربرد وب و فناوریهای مربوطه، موجب افزایش این توجه شده است. از اواخر دهه ۱۹۸۰ وزارت دفاع آمریکا و بخشهای مشابه در کشورهای عضو ناتو و دیگر متحدان آمریکا تمرینات آفندی و پدافندی برای جنگاوران فناوری اطلاعات خود تدارک دیده و به اجرا درآورده‌اند. در سالهای بعد و با بروز چندین درگیری نظیر حملات سایبری سال ۲۰۰۷ به استونی وحمله سایبری به گرجستان در سال ۲۰۰۸ و حمله اخیر سایبری به ایران با بدافزار استاکس نت که برخی آن را موشک هدایت شونده سایبری نامیدند موارد بیشتری از حملات سایبری مشاهده شد و اکنون عبارت جنگ سایبری الزاما خواننده را به یاد داستانها و فیلمهای علمی تخیلی نمی‌اندازد و در اکثر کشورهای پیشرفته و یا حتی در حال توسعه بیانگر یک نگرانی رو به رشد است. در اوایل سال ۲۰۰۹ خبر ایجاد فرماندهی جنگ سایبری در پنتاگون برای توسعه جنگ‌افزارهای سایبری و انجام اقدامات آفندی و پدافندی منتشر گردید. و در سال ۲۰۰۸ مرکز تخصصی دفاع سایبری کشورهای عضو پیمان ناتو در شهر تالین کشور استونی آغاز بکار کرد.

۲,۱. استراتژیهای جنگ سایبری

آمادگی برای جنگ سایبری ابتدا نیازمند آنست که مشخص شود جنگ سایبری چیست و مشابه با هر جنگ دیگر لازم است انواع مختلفی که جنگ سایبری می‌تواند پیاده‌سازی شود را معرفی و رسته‌بندی کرد. استراتژیهای جنگ سایبری، همانند استراتژیهای جنگ فیزیکی، برای زمین‌گیر یا ناتوان‌سازی نیروهای نظامی، ناتوان‌سازی زیرساختهای صنعتی و توان تولیدی یا ایجاد اختلال در فعالیتهای اقتصادی دولتی و غیر نظامی به منظور قرار دادن کشور مهاجم یا هدف در وضعیت نامساعد است. هدف کسب برتری، می‌تواند بازه‌ای از بهبود جایگاه مهاجم در مذاکرات تا نابودی کامل یک کشور باشد. کارکرد جنگ سایبری در ده رسته کلی قرار می‌گیرد که در ادامه بیان شده‌اند:[۲]

۲,۱,۱ جنگ سایبری آفندی نابودگرانه

تلاش آگاهانه و سازماندهی شده نظامی به منظور نابودی کامل توانمندیهای نظامی فناوری اطلاعاتی، زیر ساختهای صنعت و تولید فناوری اطلاعات، و فعالیتهای اقتصادی دولتی یا غیر نظامی" فناوری اطلاعات-پایه" دربرابر کشور، منطقه یا جمعیت هدف.

۲,۱,۲ جنگ سایبری آفندی محدود کننده

مشابه جنگ سایبری آفندی نابودگرانه است ولی برای وارد آوردن فشار به منظور کسب موقعیت برتر در مذاکرات برای مهاجم بکار می‌رود. وقتی استراتژی جنگ سایبری آفندی نابودگرانه پیاده می‌شود، هدف نابودی، تا هر درجه ممکن در زیرساخت فناوری اطلاعات و فعالیتهای اقتصادی دولتی و شهروندی مبتنی بر رایانه دشمن است. ولی وقتی استراتژی جنگ سایبری آفندی محدود کننده پیاده می‌شود، اهداف نظامی تا حدی برآورده می‌شود. فلسفه و هدف، تمرکز بر ایجاد ازهم‌گسیختگی و ناتوان‌سازی زیرساخت فناوری اطلاعات و فعالیتهای اقتصادی دولتی و شهروندی دشمن دارد.

۲,۱,۳ جنگ سایبری تروریسم پایدار

تلاشهای آگاهانه در حال انجام یک گروه سیاسی سازماندهی شده دربرابر اهداف نظامی، صنعتی، زیرساختها یا فعالیتهای اقتصادی دولتی یا غیر نظامی فناوری اطلاعات در کشور، منطقه، ساختار دولت، جمعیت یا موجودیت یک سازمان

۲,۱,۴ جنگ سایبری تروریسم اتفاقی

مشابه مورد فوق ولی شامل تلاشهای پراکنده و اتفاقی است.

۲,۱,۵ جنگ سایبری پدافند بازدارنده

تلاش آگاهانه و سازماندهی شده نظامی بازدارنده برای حفاظت در برابر تهاجم نظامی نابودگر دربرابر توانمندیهای نظامی فناوری اطلاعاتی، زیر ساختهای صنعت و تولید فناوری اطلاعات، و فعالیتهای اقتصادی دولتی یا غیر نظامی "فناوری اطلاعات-پایه" در کشور، منطقه یا جمعیت هدف.

۲,۱,۶ جنگ سایبری پدافند نابودگرانه

مشابه جنگ سایبری آفندی نابودگرانه است. تفاوت کلیدی این دو در تاکتیک نیست، بلکه در هدف است. جنگ سایبری آفندی نابودگرانه، دربرابر هدفی است که متجاوز نیست و جنگ سایبری پدافند نابودگرانه دربرابر متجاوز بکار رفته است.

۲,۱,۷ جنگ سایبری پدافند واکنشی محدود کننده

مشابه جنگ سایبری آفندی محدود کننده است ولی با اهداف دفاعی و برای وارد آوردن فشار به منظور کسب موقعیت برتر در مذاکرات برای مهاجم دربرابر کشور منطقه یا جمعیت مهاجم یا نیروی نظامی/تروریستی است.

۲,۱,۸ جنگ سایبری شورش پایدار

تلاشهای آگاهانه در حال انجام یک گروه سازماندهی شده غیر سیاسی، بزهکار یا مزدور دربرابر اهداف نظامی، صنعتی، زیرساختها یا فعالیتهای اقتصادی دولتی یا غیر نظامی فناوری اطلاعات در کشور، منطقه، ساختار دولت، جمعیت یا موجودیت یک سازمان.

۲,۱,۹ جنگ سایبری شورش اتفاقی

مشابه مورد فوق ولی شامل تلاشهای پراکنده و اتفاقی است.

۲,۱,۱۰ جنگ سایبری شورش غیرحرفه‌ای

مشابه مورد فوق ولی شامل تلاشهای پراکنده گروههای کوچک یا افراد آموزش ندیده ناهم‌پیمان است.

۲,۲. برتری های فناورانه کشورهای متخاصم در حوزه سایبر

کشورهای پیشرفته متخاصم در حوزه سایبر از جنبه‌های مختلف دارای نقاط قوت و برتریهایی هستند که تهدیدی بلقوه را برای فضای سایبر کشور ایجاد می‌نماید. در ادامه تعدادی از مهمترین و تاثیرگذارترین نقاط قوت و موارد برتری ارایه شده است:

۲,۲,۱. تسلط نرم افزاری

آمریکا در حوزه نرم افزارهای رایانه‌ای تسلط دارد و گاهی از این کشور بعنوان ابر قدرت سایبری نام برده می‌شود. رژیم صهیونیستی نیز تبدیل شدن به ابر قدرت سایبری را جزو اهداف استراتژیک خود قرار داده است و سالهاست در این زمینه تلاش خود را بکاربسته است. کشورهای عضو ناتو سالهاست در خصوص کسب قابلیتهای جنگ سایبری در تلاش هستند و بیشترین مشارکت در توسعه نرم‌افزارها و سیستمهای عامل از جمله نرم‌افزارهای متن باز در کشورهای بلوک غرب صورت می‌گیرد. سیستمهای عامل شامل هسته و پوسته آن، ابزارهای ترجمه برنامه‌ها، ابزارهای مختلف برنامه‌نویسی، زیر برنامه‌های آماده جهت تولید برنامه‌های کاربردی، انواع برنامه‌های کاربردی، برنامه‌های راه انداز سخت افزار، برنامه‌های راه انداز رایانه که جمعا فضای نرم‌افزاری که رایانه‌ها در آن کار می‌کنند را تشکیل داده است عمدتا در کشورهای بلوک غرب تولید شده است. نرم‌افزارهای نوشته شده در کشورهایی نظیر ایران با استفاده از این فضای نرم‌افزاری تهیه شده است و در داخل خود اجزای نرم‌افزاری از این فضا را جا داده است.

در صورت وجود هرگونه درپشتی یا ابزار نرم‌افزاری در نرم‌افزارهای پایه، کلیه نرم‌افزارهای تولید شده که از آنها استفاده می‌کنند نیز شامل آن ابزارها و درهای پشتی خواهند بود. به این ترتیب هر نرم‌افزار ممکن است یا مستقیما به عنوان یک اسلحه سایبری علیه دارنده آن بکار گرفته شود و یا بعنوان تسهیل کننده و هموار کننده راه دشمن در اجرای یک حمله سایبری عمل نماید. باید به این نکته توجه کرد که کشورهایی که در مجموع این تسلط نرم‌افزاری را بوجود آورده‌اند، برخی با کشور ما رفتاری خصمانه دارند و دیگران نیز اگر متحد و هم پیمان کشورهای متخاصم نباشند در ردیف دوستان کشور ما نیز قرار ندارند.

۲,۲,۲. نیروی انسانی

از نظر تعداد (کمیت) و سطح دانش، مهارت و تجربه (کیفیت) نیروی انسانی، سالهاست در کشورهای بلوک غرب برنامه‌ریزی صورت گرفته و پیشرفتهایی حاصل گردیده است. حوزه نرم افزار، حوزه‌ای است که اگر نیروی انسانی تنها عامل کسب برتری و پیشرفت در آن نباشد، قطعا مهمترین عامل آن است. سالها است با برقراری سطح مناسبی از درآمد ورفاه و گسیل امکانات و عوامل مشوق، افزایش کمی و کیفی نیروی انسانی در این کشورها مد نظر قرار گرفته و در این خصوص برنامه‌ریزی شده است. برنامه‌ریزیها از یک سو گرایش افراد مستعد به تحصیل و کسب مهارت دراین حوزه و از سوی دیگر مهاجرت افراد صاحب دانش و مهارت از کشورهای دیگر به این کشورها را هدف قرار داده است. [۳]

۲,۲,۳. خدمات عمومی اینترنتی

خدمات عمومی متعددی در اینترنت و عمدتا بصورت رایگان در حال ارایه است. هزینه‌های نسبتا پایین ارایه خدمات، امکان جذب تعداد بسیار بالای کاربران در یک گستره جهانی و روشهای مختلف کسب درآمد از خدمات رایگان در مجموع موجب موفقیت چشمگیر برخی کسب‌وکارهای برخط شده است. بیشتر خدمات عمومی با گستره جهانی نظیر خدمات پست الکترونیک، شبکه‌های اجتماعی مختلف نظیر تویتر و فیس‌بوک، موتورهای جستجو، حراج اینترنتی، پیام فوری، گفتگوی زنده (متنی، صوتی، تصویری) و مکالمات اینترنتی در کشورهای بلوک غرب و عمدتا آمریکا در حال ارایه است و یکی دیگر از نقاط قوت در نظر گرفته می‌شود. با سو استفاده از این خدمات می‌توان از آنها برای کسب اطلاعات و جاسوسی، تاثیرگذاری و مهندسی افکار عمومی برای جنگ نرم و حتی بعنوان ابزاری برای نفوذ به رایانه خدمات گیرنده بهره‌برداری کرد. به این ترتیب این خدمات و گسترش دامنه کاربران آن به کشورهای هدف یک ابزار قدرت و برتری است.

۲,۳. موانع، نقاط ضعف و آسیب پذیریهای کلیدی

فعالیتهای انجام شده در خصوص توسعه امنیت فضای سایبر در کشور محدود و اندک بوده است و موانع، نقاط ضعف و آسیب پذیریهای جدی در این خصوص وجود دارد که در ادامه به برخی از مهمترین موارد پرداخته شده است:

۲,۳,۱. ضعف در حوزه نیروی انسانی

فعالیتهای محدودی در حوزه توسعه سطح دانش و آگاهی عمومی و اطلاع رسانی به عامه مردم در کشور صورت گرفته است و فعالیتهای انجام شده موردی، محدود و کوتاه مدت بوده است. ضعف دانش و تجربه امنیت سایبری در عامه مردم و کاربران عمومی رایانه و کارشناسان و کاربران تخصصی و همچنین مدیران بخشهای رایانه و شبکه‌های رایانه‌ای، کارشناسان و مدیران امنیت سایبری، مدیران سطوح مختلف در سازمانهای دولتی و خصوصی و همچنین مشاوران عالی، سیاستگذاران و قانونگذاران مشهود است. علاوه بر این تعداد محدودی از برنامه نویسان در خصوص امنیت رایانه و نحوه تولید نرم‌افزارهای ایمن آموزش دیده‌اند. ضعف اطلاع رسانی گاه به حدی بوده است که آگاهی کافی از خطرات و جدی بودن آن وجود نداشته و به این مقوله به چشم داستان

علمی تخیلی نگریسته می‌شود. گذشته از این، از نظر کمی نیز تعداد کارشناسان و مدیران امنیت سایبری در کشور محدود است و فعالیت قابل توجهای در آموزش و تربیت چنین کارشناسانی در سازمانها مشاهده نمی‌شود و علاوه بر آن توان سازمانها بخصوص سازمانهای دولتی در جذب و نگهداری چنین کارشناسانی محدود بوده است. مهاجرت هر فرد صاحب دانش و تجربه از کشور به کشورهای بلوک غرب که سالها ست ادامه دارد کشور را دچار آسیب پذیری مضاعف می‌نماید. این آسیب پذیری مضاعف شامل تقویت تسلط نرم‌افزاری این کشورها و افزایش فقر نرم‌افزاری در کشور است.

۲،۳،۲. ضعف صنعت نرم افزار

صنعت نرم اقزار در کشور رشد محدودی داشته است و از هیچ روی دارای عمق کافی که بتواند ایجاد کننده سطحی از تسلط نرم‌افزاری باشد نیست. از دیدگاه اقتصادی، محدودیت بازار داخلی بعلت رواج نقض حقوق پدیدآورندگان نرم‌افزار و محدودیت در دسترسی به بازارهای صادراتی از یک سو و محدودیت در دستیابی به منابع مالی و بازار سرمایه از سوی دیگر زمینه مناسبی را برای رشد اقتصادی تولید کنندگان نرم افزار ایجاد نکرده است. علاوه بر این ضعف در سطح دانش، تجربه و مهارت در جنبه‌های عمومی مدیریت، ضعف در بازاریابی و ضعف در کمیت و کیفیت برنامه نویسان از یک سو و محدودیت در همکاریها و مشارکت با شرکتهای خارجی توانمند موجبات توسعه نیافتگی علمی و تجربی صنعت نرم افزار را فراهم کرده است.

۲،۳،۳. تحریمها

تحریمهای وضع شده علیه کشور موانعی را در زمینه نرم‌افزار در کشور ایجاد کرده است. بروز مشکل در دریافت نرم‌افزارهای اصلی و دریافت خدمات پس از فروش و ضعف در امکان بروزرسانی نرم افزارها از یک سو و رواج استفاده از نرم‌افزارهای غیر اصلی بصورت فله در بازارهای نرم‌افزاری داخل کشور و دسترسی به نرم‌افزارهای مختلف از طریق محیطهای به اشتراک گذاری فایل از سوی دیگر آسیب پذیریهای خطرناکی را ایجاد نموده است که می‌تواند در صورت بروز یک حمله سایبری توسط دشمن قابل بهره‌برداری باشد. لازم به ذکر است که ارایه نرم‌افزارهای فله بدون هیچگونه نظارت و بازبینی محتویات صورت می‌گیرد و درموارد زیادی آلوده به بدافزارهای خطرناک بوده و این نرم‌افزارها یکی از راههای رواج آلودگی در کشور بوده‌اند. تحریمها در حوزه نرم‌افزار تناقضی را برای کشور بوجود آورده‌اند. از یک سو در صورت قانونی شدن الزام رعایت حقوق پدیدآورندگان نرم‌افزارهای خارجی، با توجه به تحریمها و عدم فروش این نرم‌افزارها به کاربران داخل کشور استفاده از این نرم‌افزارها غیر قانونی و ناممکن می‌شود و از طرف دیگر در صورت خرید غیر مستقیم و با واسطه، امکان استفاده مناسب از محصول خریداری شده به لحاظ عدم امکان برخورداری از خدمات پس از فروش و پشتیبانی فراهم نمی‌گردد . ادامه وضع موجود نیز علاوه بر آسیب پذیریهای ناشی از عدم استفاده از نرم‌افزار اصلی به لحاظ استفاده تقریبا رایگان از این نرم‌افزارها بازار نرم‌افزار داخل را محدود و صنعت نرم‌افزار کشور را دچار ضعف و عقب ماندگی نموده است. در این خصوص پیشنهادی در بخش راهکارها ارایه شده است.

۲,۴. چالشهای و تهدیدهای اقتصاد و تجارت الکترونیکی

با در نظر گرفته استراتژیهای دهگانه جنگ سایبری و با در نظر گرفتن وضعیت و سطح فناوری کشور ایران و دشمنان آن، تمام استراتژیهای جنگ سایبری، چالشهایی جدی را برای تجارت و اقتصاد الکترونیکی در کشور ایجاد می‌کنند هر چند سطح تهدید دربین این استراتژیها متفاوت است.

حملات از ناحیه جنگ سایبری تروریستی، شورشی و غیرحرفه‌ای بیشترین احتمال وقوع را در استراتژیهای جنگ سایبری دارد. این با حملات نفوذ اتفاقی، که توسط افراد یا گروههای غیرحرفه‌ای در گذشته اتفاق افتاده است، تفاوت دارد و نباید اشتباه گرفته شود. تفاوت اولیه در سطح پیشرفته و نابود کننده بودن حملات و انگیزه‌های سیاسی و اقتصادی پشت آن است. احتمال زیادی دارد جنگاوران سایبری بطور کامل متمرکز بر حمله به یک سازمان خاص نشوند، اما ممکن است به دفعات به شرکتهای ارزنده ضربه بزنند. بدترین حالت برای یک سازمان آنست که هدف حمله مستقیم و انحصاری یک گروه تروریستی یا شورشی قرار گیرد. در این صورت، عملکرد فناوری اطلاعات ضربه خواهد دید و کسب وکار مختل خواهد شد. اگر شرکت تحت حمله برای کسب درآمد وابسته به وب باشد، اختلال می‌تواند مرگ آور باشد.[۴]

حملات جنگ سایبری تمام عیار دربرابر کل کشور نظیر جنگ سایبری نابودگرانه آفندی و پدافندی و جنگ سایبری آفندی و واکنشی محدود کننده، سخت و گران است و مخفی نخواهد ماند. این حملات معمولا به همراه یک جنگ فیزیکی یا حداقل با اعلان جنگ یک کشور بر علیه کشور دیگر صورت خواهد گرفت. در صورت اقدام نظامی و آگاهانه و تمام عیار جنگ سایبری، سازمانهای واقع در خط آتش بین مهاجم و کشور هدف (یا دفاع کننده و کشور متجاوز) هدف حملات بازدارنده یا نابودکننده قرار می‌گیرند. اگر سازمانی در کشور مورد تهاجم قرار گرفته باشد، باید انتظار اختلال یا نابودی را داشته باشد. سازمانها ممکن است دچار ضربه مستقیم جنگ سایبری نابودگرانه آفندی یا پدافندی شوند. احتمال ضربه غیر مستقیم ناشی از جنگ سایبری نابودگرانه و محدود کننده هم وجود دارد.

در یک جنگ سایبری حملات و تهدیدهای متنوعی اقتصاد و تجارت الکترونیکی را با چالش مواجه خواهد کرد. قدرتهای برتر سایبری معمولا مدتها قبل از شروع یک جنگ نابودگر یا محدود کننده، سامانه‌های کشورهایی که هدف بلقوه در نظر گرفته می‌شوند را مورد حملات شناسایی و نفوذ قرار می‌دهند. هدف از این حملات، شناسایی محل درگیری و عناصر مهم و کلیدی آن و نقاط آسیب پذیر است و با نفوذ به سیستمها تلاش می‌شود درگاههای ورود ایجاد و یا کنترل سامانه‌ها بطور نامحسوس در دسترس آنان باشد. با تغییر سامانه‌ها و جابجایی و جایگزینی تجهیزات، نصب نرم‌افزارهای جدید و حذف یا تغییر نرم‌افزارهای قدیمی و نصب تجهیزات یا نرم‌افزارها به منظور تقویت امنیت سامانه‌ها، دشمن تلاش می‌کند درگاههای ورود و کنترل نامحسوس سامانه‌ها را برای خود محفوظ نگه دارد تا به هنگام نیاز و با صدور فرمان تهاجم سایبری آنها را مورد بهره‌برداری قراردهد و قبل از آن اقدام مخربی صورت نمی‌گیرد و تنها ممکن است از قابلیت بدست آمده برای کسب اطلاعات و جاسوسی بهره‌برداری بعمل آید.

در جنگهای سایبری تروریستی با بزهکارانه معمولا مهاجم پس از بدست آوردن امکان نفوذ و حمله، اقدامات مخرب خود را آغاز می‌نماید. بزهکاران که قدرت کسب منافع مادی را بدست آورده اند معمولا تلاش می‌کنند نفوذ صورت گرفته را مخفی نگه دارند تا حداکثر سو استفاده مادی را بعمل آورند. ولی تروریستها تلاش می‌کنند نفوذ صورت گرفته را آشکار و به تیتر خبری تبدیل کنند. مهاجمینی که از انگیزه‌های قومی، فرقه‌ای، سیاسی یا مذهبی خاصی برخوردارند معمولا با تغییر چهره درگاه وب قربانی و قراردادن تصاویر با متون خاص، تلاش می‌کنند گروه یا کشور هدف را بی آبرو نمایند یا اهداف خود را تبلیغ یا پیام خود را منتشر نمایند.

روشهای مختلفی برای حمله و نفوذ به سامانه‌ها ممکن است بکار گرفته شود. ممکن است مهاجم با روشهای مختلف با اخذ کلمه عبور وارد سامانه‌های رایانه‌ای شود یا با استفاده از بدافزارها بطور غیر مستقیم اقدامات خود را پیش‌برد. ممکن است نقاط ضعف هسته یا پوسته سیستم عامل، آسیب پذیری برنامه‌های کاربردی یا آسیب پذیریهای ابزارها یا نرم‌افزارهای پایه بکاررفته در تولید برنامه‌های کاربردی مورد استفاده مهاجم قرار گیرد.

مهاجمین تلاش خواهند کرد به رایانه یا شبکه رایانه‌ای در بخش صف یا ستاد بانکها یا شرکتها و موسسات تجارت الکترونیکی نفوذ کنند. در صورت موفقیت هدف بعدی می‌تواند نفوذ به رایانه‌های حساس و مرکزی بانکی یا تجارت الکترونیکی باشد. نفوذ در هر سطحی صورت گیرد مهاجم می‌تواند با شنود اطلاعات در حال گذر، عملیات کسب اطلاع و شناسایی خود را گسترش دهد و به سامانه‌های بیشتری نفوذ کند یا به اطلاعات حساب کاربران دسترسی پیدا کند. در این حالت نفوذ و دستیابی به اطلاعات بانکهای اطلاعات و کسب قدرت تغییر یا تخریب اطلاعات می‌تواند فاجعه بار باشد. مهاجم که با موفقیت امکان نفوذ در یک سامانه رایانه‌ای را یافته است می‌تواند با نصب نرم‌افزار ناشناس یا جایگزینی اجزای پایه سیستم عامل رایانه، درگاه ورودی برای نفوذهای آتی ایجاد نماید و اگر توان بازنویسی و جایگزینی سفت افزارها را داشته باشد تقریبا این درگاه ورود را دایمی نماید. مهاجم می‌تواند با حملات بدافزاری عام، تلاش نماید تا هر رایانه‌ای را آلوده سازد و پس از آلوده شدن یک رایانه حساس یا مهم، تلاش نماید با استفاده از بدافزارهای خاص درگاه ورود خود به این سامانه‌ها را دایمی سازد. بدافزارهای بکار رفته برای آلوده سازی عام اگر قبلا توسط نرم‌افزارهای ضدبدافزار قابل شناسایی نباشد، کپی آن پس از چند حمله بدست یک شرکت تولید کننده نرم‌افزارهای ضدبدافزار رسیده و به بانک اطلاعاتی بدافزارهای قابل شناسایی افزوده می‌گردد. ولی بدافزارهای خاص بکار رفته برای آلوده سازی هدفمند، از دید نرم‌افزارهای ضد بدافزار مخفی می‌ماند و شناسایی و پاکسازی آنها ساده نیست.

حملات با پیچیدگی کمتر که الزام نفوذ به سامانه‌های رایانه‌ای هدف را ندارد عبارتند از حملات منع سرویس و حملات جعل درگاه وب. در حمله اول منع قدرت سازمان در ارایه خدمات مد نظر قرار گرفته است که معمولا با کمک تعداد زیادی از رایانه‌های آلوده در نقاط مختلف کشور یا جهان صورت می‌گیرد. یک نوع هوشمندانه‌تر از این حملات که با استفاده از تعداد اندکی رایانه ولی با بکارگیری تکنیک تزریق SQL توسط روسها و بر علیه گرجستان صورت گرفت اثر مشابهی ایجاد نمود.[۵] در نوع دوم حملات معمولا هدف گمراهی کاربران و تشویق آنها با روشهای مختلف به مراجعه به درگاه جعلی بجای درگاه اصلی وب خدمات دهنده و اخذ اطلاعات حساب یا کلمه عبور کاربران است.

بسته به وسعت و دامنه حملات انجام شده ممکن است این حملات تبعاتی در سطح ملی یا تبعاتی محدود و در سطح سازمانی داشته باشند. تبعات در سطح ملی میتواند مستقیم یا غیر مستقیم باشد. تبعات مستقیم در سطح ملی ممکن است شامل ایجاد ناتوانی یا کندی در جابجایی نقدینگی دراقتصاد، ایجاد کندی و اختلال در پرداختها و گردش مالی، ایجاد مانع یا ناتوانی در فرآیند سرمایه‌گذاری و تجارت یا ازهم‌گسیختگی تجارت محلی و کمک به درماندگی اقتصادی باشد. تبعات غیرمستقیم در سطح ملی ممکن است شامل ایجاد نارضایتی عمومی و بروز ناآرامیهای اجتماعی، ورود ضربه اقتصادی در سطح ملی، کاهش سطح رفاه عمومی و تولید ناخالص ملی، از دست رفتن اعتماد مردم به بانکداری، اقتصاد و تجارت الکترونیکی و رویگردانی آنان از این خدمات یا از دست رفتن گسترده اطلاعات شخصی و نقض حریم خصوصی افراد باشد. تبعات محدود ممکن است شامل ایجاد مانع یا ناتوانی در مجتمع‌های صنعتی و تولید و توزیع، صدمه اقتصادی سازمانهای هدف قرار گرفته کاهش ارزش سهام یا ورشکستگی سازمان، کاهش حقوق یا مزایا یا بیکاری موقت یا دایمی کارکنان سازمانهای هدف قرار گرفته یا از دست رفتن اعتبار سازمانهای هدف قرار گرفته باشد.

۲,۵. راهکارها

جنگ سایبری بعنوان زیرمجموعه جنگ نرم طبقه بندی و بیشترین تاثیر در انجام یا مقابله با آن توسط انسان صورت می‌گیرد و انسان در آن نقش اساسی و محوری دارد. به این ترتیب مهمترین محور برای راهکارهای مقابله با جنگ سایبری، تربیت و تقویت نیروی انسانی است و افزایش سطح آگاهی، دانش و تجربه و مهارت نیروی انسانی باید به عنوان محور اصلی تمامی اقدامات مد نظر باشد. علاوه بر این اگر نگهداری و حفظ نیروی های تربیت شده با مکانیزمها و سازوکارهای تشویقی مناسب صورت نگرفته باشد، اقدامات صورت گرفته در تربیت نیروی انسانی نمی‌تواند کامل و موثر باشد.

در ادامه لیستس ازراهکارها در دو سطح ملی و سازمانی پیشنهاد گردیده است:

۲,۵,۱. راهکارها در سطح ملی

- توسعه آگاهی عمومی و افزایش سطح دانش و آگاهی امنیت سایبری و آشنایی با خطرات حملات سایبری
- تدوین الزامات آموزشهای ضمن خدمت کارکنان دولت در زمینه امنیت سایبر
- توسعه آموزشهای کوتاه و میان مدت ایجاد مراکز مجاز و رتبه بندی شده آموزش امنیت سایبری وضابطه مند و استاندارد کردن آموزشها در این زمینه
- ایجاد دانشگاه امنیت سایبری و توسعه آموزشهای دانشگاهی در این زمینه
- ایجاد انگیزه برای نگهداری متخصصین امنیت سایبر و ممانعت از فرار مغزها
- ایجاد نظام فکری دفاع مستمر در کلیه سازمانها و بخشها همراه با ساختار سازمانی لازم که بتواند با سرعت و کارایی لازم، برای پدافند در برابر حملاتی که با یا بدون هشدار آغاز می‌شوند، پاسخگو باشد.

- ایجاد سامانه های کنترل و پایش بدافزار و شناسایی رایانه های آلوده با گستره ملی و تدوین ضوابط و قوانین لازم برای الزامات قانونی برای نصب سنسورها، گزارش دهی و پاکسازی رایانه‌های آلوده
- تدوین الزامات و فرآیندهای پایش و گزارش دهی در سطح ملی
- تدوین نظام امنیت نرم‌افزاری کشور و بازبینی و نظارت دقیق و مستمر بر نرم‌افزارهایی که در کشور تکثیر و توزیع می‌گردند
- اجرای مانورهای پدافند سایبری
- ایجاد گروهها و مراکز امداد و نجات رایانه‌ای در سطوح استانی و ملی و برقراری ارتباط با گروههای منطقه‌ای و جهانی
- تقویت پلیس فتا و اخذ قدرت عمل در محدوده ملی، منطقه‌ای و بین‌الملل از طریق برقراری ارتباطات لازم با مجامع منطقه‌ای و بین الملل
- ایجاد سازمان و تشکیلات دفاع ملی سایبری و پدافند غیر عامل سایبری
- سیاستگذاری و ایجاد مشوقهای لازم در جهت افزایش کمیت و کیفیت تولیدات بومی سخت‌افزاری و نرم‌افزاری
- وضع قوانین و ضوابط برای الزام به استفاده حداکثری از سخت افزارها و نرم‌افزارهای تولید داخل و با حداقل استفاده از ابزارها و نرم‌افزارهای پایه غیر بومی و غیر متن باز
- وضع الزام قانونی در رعایت حقوق پدیدآورندگان نرم‌افزارهای شرکتهایی خارجی که کشور را مورد تحریم قرار نداده و بی‌واسطه یا از طریق نماینده رسمی، پشتیبانی و خدمات پس از فروش به مشتریان داخل کشور را تعهد می‌کنند.

۲,۵,۲. راهکارها در سطح دستگاهی

- تدوین و اجرای طرحهای آموزش عمومی برای کلیه سطوح کارکنان متناسب با هر سطح
- برآورد نیاز و تدوین برنامه‌های آموزشی و آموزش و تربیت نیروی انسانی متخصص در زمینه امنیت سایبری
- ایجاد ساز و کار و مکانیزم تشویق و جذب و نگهداری متخصصین امنیت سایبر
- تدوین و ابلاغ سایستهای امنیتی در سطح سازمان و زیربخشها و پایش و بروزرسانی آنها
- بازبینی و نظارت دقیق و مستمر بر نرم‌افزارهایی که به سازمان وارد و مورد استفاده قرار می‌گیرد.
- ایجاد سامانه های کنترل و پایش بدافزار و شناسایی رایانه های آلوده در سطح دستگاه و توابع آن
- انجام ارزیابیهای امنیتی سازمان و مدیریت ریسک و ایجاد سازوکارهای بهبود مستمر امنیت سایبری سازمان
- تست نفوذ تجهیزات و سامانه ها
- تدوین الزامات و فرآیندهای پایش و گزارش دهی‌در سطح سازمانی
- ایجاد گروهها و مراکز امداد و نجات رایانه‌ای در سازمان و برقرار ارتباط با گروهای دستگاه مرکزی و ملی
- استفاده حداکثری از سخت‌افزارها و نرم‌افزارهای تولید داخل و با حداقل استفاده از ابزارها و نرم‌افزارهای پایه غیر بومی و غیر متن باز

- انجام پشتیبان گیریهای منظم و تدوین و اجرای طرحهای مدیریت بحران و بازیابی پس از بحران و تداوم کسب و کار
- از رده خارج کردن یا پیکره بندی مجدد تا سطح سفت افزار در خصوص رایانه‌ها وسامانه‌های رایانه‌ای حساس و مهم که مورد نفوذ قرار گرفته‌اند یا آلوده شده‌اند.

۳. نتیجه‌گیری

جنگهای سایبری بر خلاف جنگهای متداول می‌توانند بدون اعلان جنگ و مخفیانه دربگیرند و شاید تا ماهها یا سالها زمان دقیق شروع و کشور یا کشورهای متخاصم، اهداف و میزان خسارات وارده بر آنها بدرستی شناخته نشوند، لذا احتمال وقوع آن بسیار بیشتر از جنگهای فیزیکی است. نکته دیگر آنکه در دهه اخیر معمولا همراه جنگ فیزیکی نوع و سطحی از جنگ سایبری بکارگرفته شده است و سطح بکارگیری استراتژیهای جنگ سایبری و وزن آن در جنگ علیه اهداف در حال افزایش بوده است. با این وصف در آینده وقوع جنگ سایبری بدون وجود جنگ فیزیکی کاملا طبیعی و محتمل است ولی وقوع جنگ فیزیکی بدون بکارگیری استراتژیهای جنگ سایبری غیر محتمل است. باید به این نکته توجه کرد که اهداف یک جنگ سایبری محدود به مجتمع‌ها و تاسیسات نظامی نیست و فعالیتهای مالی و اقتصادی دولتی و خصوصی نیز از اهداف مهم آن درنظر گرفته می‌شود. لذا در فضای بدون مرز سایبری، دفاع مقوله‌ای نیست که تنها توسط نظامیان صورت گیرد و لازم است کلیه آحاد جامعه و سازمانهای دولتی و خصوصی برای انجام دفاع موثر سایبری آماده باشند و در آن مشارکت داشته باشند. توسعه امنیت فناوری اطلاعات و توجه به توسعه ساختارهای دفاع ملی سایبری، همگام با توسعه کاربردهای فناوری اطلاعات، لازمه حفظ امنیت ملی است. توسعه کاربردهای فناوری اطلاعات بدون رشد و تقویت امنیت و سازوکارهای دفاع سایبری موجب افزایش آسیب پذیری کشور در برابر جنگ سایبری بعنوان شیوه غالب جنگهای آتی است. امنیت فناوری اطلاعات بعنوان یک فناوری انسان محور نیازمند توجه به توسعه و حفظ نیروی انسانی متخصص و متعهد است و پیشرفت درآن بدون پیشرفت در توسعه و حفظ نیروی انسانی مقدور نخواهد شد. حراست مرزهای سایبری کشور نیازمند مغزهایی‌هوشمندو متفکر، چشمانی تیزبین و همیشه باز، گوشهایی شنوا و آماده یادگیری، شامه‌ای قوی و پویا، زبانی گویا، آموزنده، تشویق کننده و هشدار و بیم دهنده، دستانی ماهر و باتجربه و پاهایی همیشه رهرو، پرتوان، مصمم و خستگی ناپذیراست. سرانجام آنکه موفقیت در دفاع موثر سایبری نیازمند برخورداری از زیرساخت توانمند نرم‌افزاری است و بدون دستیابی به سلطه نرم‌افزاری کامل نیست.

مراجع

[1] Erbschloe, Michael.2001.”Information Warfare, How to survive Cyber Attacks”. *Osborne/McGraw-Hill, 1.*

[2] Erbschloe, Michael.2001.”Information Warfare, How to survive Cyber Attacks”. *Osborne/McGraw-Hill, 3.*

[3] Mathis, Robert; Jackson, John. 2008.*” Human resource management 9th Edition* “. *Thomson South-Western. 4,5,6,144.*

[4] Erbschloe, Michael.2001.”Information Warfare, How to survive Cyber Attacks”. *Osborne/McGraw-Hill, 30.*

[5] Korns, Stephen; Kastenberg, Joshua.2009.”Georgia’s Cyber Left Hook”. *Parameters*, Winter 2008-09, 60-76.