بُعد هفتم: فضای سایبر

حبیب صدرزاده

کارشناس نرم‌افزار رایانه ، گردان فاوا ، پایگاه هوایی شهید بابایی

اصفهان، ایران

Habibsadrzadeh@gmail.com

چکیده

با رشد علم و دانش بشری و انقلاب فناوری اطلاعات و ارتباطات در عصر اطلاعات، سبک، تاکتیک، راهبرد، سازمان و دکترین جنگها دستخوش تغییراتی عظیم و براساس این دگرگونی گردید. هر آفندی به دفاع و پدافندی متناسب با آن نیازمند است تا در تهاجم رقیب بتوان از زیرساختهای حیاتی سازمان و کشور نگهداری کرد. در این متن، سعی شده است با تعریف و بیان ویژگیهای جنگ سایبری، فضای سایبری و مؤلفه های این فضا بررسی شود و در هر حوزه، نقاط آسیب پذیر عنوان و پدافند سایبری تشریح گردد.

کلمات کلیدی

جنگ سایبری ، فضای مجازی ، فضای سایبری ، جنگ اطلاعاتی ، پدافند سایبری ، تعاریف ، ویژگیها .

۱- مقدمه

جنگ از اوایل پیدایش بشر با او متولد شد. انسان بر پایه ذات و سرشت خود همواره با جنگ و یا آمادگی برای شروع جنگ، زندگی کرده است. بسیاری از پیشرفتهای بشری در پاسخگویی به نیاز انسان در پیشبرد جنگ حاصل شده است. انسان به علتهای مختلف آغازگر جنگها بوده است چه برای به دست آوردن غذا ،آب و سرزمین در گذشته و چه برای کسب قدرت سیاسی و اقتصادی در دنیای امروز. کلاوزویتس در تعریفی امروزی، جنگ را ادامه سیاست با ابزاری دیگر و مشخصاً ابزار پیشبرد منافع سیاسی می‌داند که اصولاً جنگ مساله ای سیاسی است. در یک تعریف جامع، جنگ به عنوان خشونت سازمان یافته تمام عیار بین گروههای سیاسی مثلاً دولتها توصیف می‌گردد.

نظر متخصصان درباره رابطه جنگ و پیشرفت البته متفاوت است؛ گروه اول جنگها را تا حدودی مسبب ترقی و پیشرفت و گروه دوم پیشرفتهای بشری را باعث تغییر در نوع و سبک جنگ می‌دانند.

اختراع تیر و کمان که شاید بتوان آنرا درجهت شکار و کسب غذا دانست، بانی تحولی بزرگ در جنگ بود. مکانیسم اصلی این سلاح تبدیل انرژی پتانسیل به انرژی جنبشی بود. تیر و کمان باعث بروز تاکتیکهای مناسب با این فناوری بود که منجر به رشد پیاده نظام و تحرک بیشتر آن گردید. دستیابی انسان در حدود سال۱۵۰۰ قبل از میلاد به علم ذوب فلزات، اولین جهش در فناوری نظامی محسوب می‌گردد.

توجه به ترابری در جنگ و استفاده از اسب، فیل و شتر، نقطه شروعی برای استراتژیستهای میدان نبرد بود تا هنر خود را در نمایش تاکتیکهای جنگی نشان دهند.

یکی از عواملی که انقلابی در امور نظامی پدید آورد، اختراع باروت بود. از این زمان به بعد انسان درصدد اختراع و دستیابی به دستگاهی بود که بتواند با کنترل انرژی حاصل از انفجار باروت و در اثر واکنشهای شیمیایی آن، جسمی مانند پیکان را در مسیر دلخواه پرتاب کند. آغاز عصر باروت منجر به ظهور طیف بسیار گسترده ای از جنگ افزارها همچون تفنگهای ساچمه ای، تفنگهای خان دار، تفنگهای خودکار، مسلسلهای سنگین، سلاح کمری، توپ، تانک، مین، راکت و انواع و اقسام موشکها شد.

با پرواز نخستین وسیله هوایی در اوایل قرن بیستم در سال ۱۹۰۳ توسط برادران رایت پدیده نویی در جهان به نام هواپیما متولد شد. با قاطعیت می‌توان گفت که این وسیله ابتدا برای خدمت در جنگ ساخته نشد بلکه پاسخی به رویاهای بشر در سیر آسمانها و علاقه اش به پرواز بود. نخستین سفارش هواپیما برای ارتش آمریکا در سال ۱۹۰۸داده شد و در سال ۱۹۰۹ به بخش هوایی ارتش آمریکا تحویل گردید و بدین ترتیب نیروی هوایی در میدان نبرد ظاهر شد.

در جنگ جهانی اول، نیروی دریایی آلمان با بهره گیری از بمباران هوایی در شب توانست عملاً بنادر نیروی دریایی انگلستان را فلج کند و این نخستین تاریخ بهره گیری و کاربرد راهبردی بمباران هوایی بود .در طی جنگ جهانی اول کشورهای مختلف درگیر اعم از انگلیس، آلمان و فرانسه ترکیب مسلسل با هواپیماهای جنگنده را با جدیت پیگیری می‌کردند. دکترین حمله رعدآسا یا بلیتزکرگ در سال ۱۹۴۰ میلادی از آثار این دوره است.

سال ۱۹۴۵ میلادی، در پایان جنگ جهانی دوم، با انفجار دو بمب اتمی در شهرهای هیروشیما و ناکازاکی ژاپن توسط بمب افکنهای آمریکایی، جنگهای خونین و ویرانگر در مقیاس جهانی به اوج خود رسید و فروکش کرد اگرچه از آن زمان تا کنون، همچنان در گوشه و کنار دنیا صدای شلیک گلوله و انفجارهای مهیب به گوش می‌رسد.

با اختراع ریزپردازنده‌ها و انقلاب رایانه‌های شخصی در نیمه دوم قرن بیستم، بشر پا به عصر اطلاعات گذاشت. با انقلاب فناوری اطلاعات و ارتباطات، ظهور آرپانت در سال ۱۹۶۹ و فراگیر شدن اینترنت در ۱۹۹۵ میلادی، جهان شاهد انقلاب دیگری در امور نظامی (RMA[1]) بود. پیشرفتهای بزرگ در قدرت محاسبه رایانه ها، کاهش ابعاد فیزیکی اجزای رایانه و هزینه های پایین آنها، موجب جهش چشمگیری در امور نظامی گردیده است.

جنگ افزارهای هدایت پذیر دقیق، روباتها، فناوری غیر کشنده، تسلیحات هدایت مستقیم انرژی، نظام یکپارچه فرماندهی و کنترل، عملیات روانی مبتنی بر رسانه ها، انتشار ویروسهای رایانه ای، جنگ فضایی و جنگ سایبری از نتایج این نسل از جنگها می‌باشند. [۲]

۲- ابعاد جنگ

نکته قابل توجه در طبقه بندی جنگها مکان و فضای وقوع نبرد یا بُعد جنگ است. اولین و قدیمی ترین بُعد جنگ، سطح زمین بوده است. بُعد تاریخی دوم، سطح آب بوده است که با توانایی شناوری

[1] Revolution In Military Affairs

تجهیزات جنگی بر سطح آب آغاز و به جنگ دریایی شناخته می‌شود.

در قرن بیستم، ابعاد جدیدی به جنگ اضافه گردید:

بُعد سوم : سطح زیردریاها و اقیانوسها (جنگ زیردریایی)

بُعد چهارم : هوای روی سطح زمین(جنگ هوایی)

بُعد پنجم : سرزمین متخاصمان(جنگ راهبردی و جنگ بین قاره ای) بعد از جنگ جهانی دوم، فضا نیز به عنوان بُعد ششم از جنگ مطرح گردید که البته هنوز جنگ واقعی در آن اتفاق نیفتاده است(جنگ فضایی) اما با ظهور انقلاب اطلاعات، بحثهای گسترده ای درباره فضای مجازی (فضای سایبر) به عنوان بُعد جدیدی از جنگ در حال انجام است(جنگ اطلاعاتی).

بُعد هفتم : فضای سایبر (جنگ سایبری). [۲]

۳- تعاریف

جنگ سایبری را می‌توان شاخه ای از جنگ اطلاعاتی دانست و این دو را زیرمجموعه جنگ نرم (Soft Warfare) قرار داد. جنگ نرم در مقابل جنگ سخت (Hard Warfare) ، جنگی بدون درگیری فیزیکی و فاقد تجهیزات و ادوات معمول نظامی است. در جنگ نرم خبری از صدای غرش بمب افکنها و یورش تانکها، شلیک گلوله و انفجارهای عظیم در مفهوم متداول آن نیست. جوزف نای، پژوهشگر برجسته آمریکایی، قدرت نرم را ابزاری برای موفقیت در سیاست جهانی می‌داند. [۵]

وزارت دفاع آمریکا در اواخر دهه1990 جنگ اطلاعاتی را در یک تعریف رسمی به صورت زیر منتشر کرد : "جنگ اطلاعاتی عبارت است از اقدامات اتخاذ شده برای تحقق برتری اطلاعاتی که از طریق تاثیرگذاری بر اطلاعات و سیستمهای اطلاعاتی دشمن از راهبرد نظامی ملی پشتیبانی کرده و در عین حال اطلاعات و سیستمهای خودی را ارتقاء بخشیده و از آنها دفاع می‌کند".

جنگ سایبری هدایت عملیات نظامی بر اساس قوانین حاکم بر اطلاعات و از طریق دنیای اطلاعات و ارتباطات است. هدف اصلی در جنگ سایبر بر هم زدن موازنه اطلاعات و دانش به نفع نیروهای خودی است به ویژه اگر موازنه توان رزمی و نظامی وجود نداشته باشد. جنگ سایبر یک جنگ دانش بنیان و مبنای آن فناوریهای پیشرفته اطلاعاتی است که می‌توان با بهره گیری از دانش برتر، ضعف سرمایه و کمبود نیروی انسانی را جبران کرده و به پیروزی قاطع دست یافت. با این توضیح می‌توان جنگ سایبری را نمونه ای از جنگهای ناهمتراز (نامتقارن) برشمرد.

ریموند پارکز و دیوید دوگان از پژوهشگاه ملی ساندیا در نیومکزیکو در تعریف جنگ سایبر می‌نویسند : "جنگ سایبر زیرمجموعه ای است از جنگ اطلاعاتی که شامل اقداماتی می‌شود که در دنیای سایبر رخ می‌دهند. دنیای سایبر هرگونه واقعیت مجازی است که توسط مجموعه رایانه‌ها و شبکه‌ها ایجاد می‌شود. در بین دنیای سایبر متعدد و مختلف، اینترنت و شبکه های مرتبطی که حاوی مطالب چند رسانه ای هستند، بیشترین ارتباط را با جنگ سایبر دارند". [۷]

۴- ویژگیهای جنگ سایبری

- ملموس و عینی نیست. در جنگ سایبری دودی حاصل از انفجار مشاهده نمی شود.
- تمایز میان جنگ و صلح در زمان بسیار دشوار است. ظاهراً همیشه جنگ سایبری برقرار است.
- تفاوتی میان غیرنظامی و نظامی وجود ندارد. همه افراد درگیر جنگ یا دفاع سایبری هستند.
- همانند دوران صنعتی جنگها، جنگ سایبری فرسایشی و طولانی مدت نیست.
- دانش بنیان است. جنگ سایبری، جنگ مغزها و اندیشه هاست.
- بمبها، موشکها، هواپیماهای جنگنده، تانکها و ناوهای جنگی آن رایانه ها، سیستمهای فرماندهی و کنترل متمرکز، شبکه‌های اجتماعی و پایگاههای داده در فضای شبکه، اینترنت و وب هستند.
- از لحاظ سازمانی شبکه محور است و همانند جنگهای کلاسیک، سلسله مراتب مشخصی ندارد.
- آمار نیروی انسانی و تجهیزات طرفین درگیری، تأثیری در نتیجه جنگ سایبری نخواهد داشت. (جنگ نامتقارن یا ناهمتراز است)
- حملات سایبری معمولاً از راه دور صورت می‌گیرد.
- شناسایی و ردیابی مهاجمان بسیار دشوار و گاهی غیرممکن است. (مشکل اسناد حملات سایبری)
- جنگی غیرکشنده است و تلفات انسانی ندارد.
- هزینه جنگ سایبری بسیار کمتر از نبرد فیزیکی و کلاسیک است. [۸]

۵- تولد یک سلاح جدید

بمب الکترومغناطیسی در واقع چیزی نیست جز یک شار مغناطیسی فوق العاده نیرومند که با گسیل امواج پر قدرت (SHF) سوپر فرکانسهای با طول موج بالاتر از ده گیگا هرتز موسوم به امواج میکرو ویو پر قدرت (High Power Microwave) می‌تواند هر گونه دستگاههای الکتریکی یا الکترونیکی واقع در محدوده عمل خود را در یک باند فوق گسترده (UWb) که مخفف عبارت Ultra Wide band می‌باشد، فلج نماید. روزی را تصور کنید که در یک شهر معمولی و در یک زمان، تمام دستگاههای الکتریکی روشن و در حال کار ناگهانی سوخته و از کار بیفتد و تمام دستگاههای خاموش نیز در آن واحد روشن شده و پس از چند لحظه آنها نیز بسوزند. در چنین شهری پس از انفجار بمب الکترومغناطیسی بر فراز شهر، در کسری از ثانیه یک تا دو میلیارد وات انرژی الکتریکی، کلیه سیستمهای مخابراتی ، رادیویی و تلویزیونی را از کار بیندازد.

برق شهر قطع می‌گردد؛ مدار الکتریکی همه رایانه‌ها می‌سوزد؛ تمام باتریها و خازنها منفجر می‌شوند؛ لامپ تصویر همه تلویزیونها و مانیتورهای خاموش یا روشن نورانی شده و می‌سوزد؛ همه موتورهای الکتریکی با آخرین دور ، همه و همه از کار می‌افتند و ناگهان شهر در قهقرا فرو می‌رود؛ سیستمهای گرمازایی و سرمازایی ، پمپهای آب و حتی ساعتهای مچی نیز از کار می‌افتند.

شهر بدون الکتریسیته ، موتور ، باتری ، مخابرات و ارتباطات کاملا فلج می‌شود. همه این اتفاقات با سرعت نور یعنی کسری از ثانیه پس از انفجار یک بمب الکترومغناطیسی در حوزه میدان مغناطیسی آن اتفاق می‌افتد. با این حال سلاح مغناطیسی را می‌توان یک اسلحه انسانی نیز به حساب آورد چرا که به ساختمانها و انسانها کمترین آسیب را می‌رساند. تولد این سلاح جدید که تنها به مدارات الکترونیکی آسیب می‌رساند، نتیجه تغییر رویکرد جنگهای عصر اطلاعات و جنگهای سایبری است. [۱۱]

۶- اهمیت فضای مجازی

"بهترین شکل هنر جنگ، پیروزی بدون جنگیدن در یک نبرد مسلحانه ساده است."

سن تزو فرمانده نظامی و سیاستمدار کهنه کار چینی در ۲۴ قرن پیش، کتاب هنر جنگ

تاریخ نگاران امور نظامی و استراتژیستهای جنگی، نبرد سایبری را طبق نظریه نسلهای جنگ (یک نظریه درسطح تاکتیکی از ویلیام اس لیند و چهار تن از افسران نیروی زمینی و تفنگداران دریایی آمریکا در۱۹۸۹)، "جنگ نسل چهارم (4GW)[۱] و با محوریت فناوری جدید" می‌نامند و براساس نظریه عصرهای جنگ (یک نظریه که تمدن غرب را به چهار عصر انرژی مبنا تقسیم می‌کند توسط دکتر تی لیندسی مور در۱۹۸۷)، "جنگ عصر چهارم و دوره پست مدرن" می‌دانند و مطابق نظریه موجهای جنگ (نظریه آلوین و هایدی تافلر در ۱۹۹۱)، "جنگ موج سوم و دوره دانش" طبقه بندی می‌کنند و یا حتی در مقایسه با نظریه دوره‌های جنگ "دوره ششم: و برتری اطلاعاتی" می‌شناسند؛ به هرترتیب و با هر نامی جنگهای امروز و آینده از این نوع هستند و دست کم ترکیبی از جنگ سایبری و جنگهای فیزیکی که با گذشت زمان به نظر می‌رسد سایبر غالب فضای نبردها را فرا خواهد گرفت. [۲]

در سال ۱۹۷۰ میلادی ویلیام وست مورلند، ژنرال ارتش آمریکا در کنگره گفت:" در آینده در جبهه‌های نبرد، با استفاده از ارتباطات اطلاعاتی، ارزیابی و تجسس هوشمندانه توسط رایانه و کنترل شلیک خودکار، می‌توانیم نیروهای دشمن را شناسایی، ردگیری و مورد هدف قرار دهیم. من مطمئنم که مردم آمریکا انتظار دارند که کشور از تمام مزایای این فناوری استفاده کند تا به استقبال پیشرفت نهایی برود که امکان جایگزینی ماشین را به جای انسان فراهم می‌کند ." [۹]

کلینتون رییس جمهور آمریکا در ۱۹۹۸، طرح سیاست حافظت از زیرساختهای حساس در مقابل نقاط آسیب پذیر شبکه مجازی دولت را ارائه داد. این طرح زمینه ساختاربندی و سازمان دهی کسب آمادگی برای یک بحران سایبر را فراهم می‌ساخت.

بوش رییس جمهور آمریکا در ۲۰۰۳ ، سیاست فضای مجازی امن را در راهبرد ملی فضای مجازی امن (راهبرد ملی امنیت فضای سایبر) مطرح کرد. طرح بوش شامل سه هدف راهبردی بود. الف- جلوگیری از حمله های سایبر علیه تأسیسات حیاتی آمریکا، ب- کاهش آسیب پذیریهای ملی در برابر حملات سایبری و ج- به حداقل رساندن صدمات و زمان برگشت و بازیابی پس از وقوع حمله های سایبری. [۶]

نیروی هوایی ایالات متحده، نخستین نیروی نظامی ای بود که فضای سایبری در بیانیه مأموریت آن گنجانده شد. فرمانده نیروی هوایی ،

[۱] Fourth Generation Warfare

مایکل دبلیو وین در سال ۲۰۰۵، مأموریت نیروی هوایی را اینگونه بیان می‌کند: "در اختیار داشتن گزینه های مستقل به منظور دفاع از ایالات متحده آمریکا و منافع جهانی آن در هوا، فضا و فضای سایبر". نیروی هوایی فضای مجازی را به عنوان یک حوزه درگیری جنگی محدود شده توسط طیف الکترومغناطیس یا فضای مانوری طیف الکترومغناطیسی تعریف کرد.

فرمانده نیروی هوایی در سال ۲۰۰۶ اعلام کرد که هشتمین واحد نیروی هوایی مسئول فضای مجازی است که یک گام عمده به سمت انجام این مأموریت جدید بود. این واحد نقشه راه آینده نیروی هوایی را در حوزه فضای مجازی توسعه داده و به سازمان دهی، آموزش و تجهیز این نیرو جهت کسب آمادگی برای انجام عملیات در فضای مجازی می‌پردازد. بخش عمده این مأموریت، ایمن سازی فضای سایبر از طریق ممانعت از دسترسی دشمن به همان فضا است.

مرکز امنیت اطلاعات و آموزش و پژوهش (CISER) در داخل اداره اطلاعات نیروی هوایی نیز مأموریت دارد که به توسعه توان کارشناسی فرماندهان در حوزه سایبر با استفاده از دکترین، تکنیکها و فناوریهای کسب برتری و اشراف در فضای سایبر بپردازد.[۹]

اوباما از بدو ورود به دفتر ریاست جمهوری در سال ۲۰۰۹ میلادی، فضای سایبری را به عنوان یکی از داشته‌های راهبردی ملی معرفی کرد و خواهان تنظیم یک سند سیاست‌گذاری فضای سایبری (CYBERSPACE POLICY REVIEW)شد و از نهادهای مختلف امنیتی این کشور خواست تا راهبردی کلان برای تأمین امنیت این فضا طراحی کنند. در می سال ۲۰۱۱، کاخ سفید نیز سند راهبرد بین‌المللی برای فضای سایبری (INTERNATIONAL STRATEGY FOR CYBERSPACE) را منتشر کرد. در واقع این سند نشانه‌ای بود هم برای متحدان و هم برای دشمنان که آمریکا چه انتظاراتی از این نسل جدید رسانه‌های نوظهور دارد و چه برنامه‌هایی برای آن تدارک دیده است.

آمریکا مرکز فرماندهی سایبری (سایبرکام) را در می سال ۲۰۱۰ تأسیس کرد. سایبرکام سه مأموریت بر عهده دارد: الف- حفاظت روزانه از تمام شبکه‌های دفاعی، ب- ایجاد زنجیره‌ای از فرماندهان که به رئیس جمهور ختم می‌شود و ج- همکاری با شرکای مختلف برای داد و ستد اطلاعات مربوط به تهدیدات سایبری و واکنش هماهنگ به این تهدیدات.

آمریکا مسئولیت‌های مربوط به امنیت سایبری را میان دو نهاد وزارت دفاع و وزارت امنیت داخلی، تقسیم کرده است. برای سال مالی ۲۰۱۲، این دو آژانس روی هم رفته درخواست ۳.۴ میلیارد دلار بودجه برای رفع و رجوع امور مربوط به فضای سایبری کرده‌اند.

مؤسسه نورتون در گزارشی در سال ۲۰۱۰ اعلام کرد که نزدیک به دو سوم مردم سراسر دنیا قربانی جرائم سایبری شده‌اند. مطالعه‌ای هم که از سوی مؤسسه مک‌آفی در سال ۲۰۰۹ صورت گرفت، نشان می‌دهد که جرائم سایبری، از جمله دزدی اطلاعات و عبور از دیوارهای امنیتی، یک تریلیون دلار در سراسر دنیا به تجارت جهانی خسارت وارد کرده است.

وقوع مجموعه‌ای از رویدادهای مهم و برجسته در سال‌های ۲۰۱۰ و ۲۰۱۱ میلادی، اهمیت و پیچیدگی تهدید حملات سایبری را پررنگ کرده است. از جمله این حوادث می‌توان به هک شدن سایت گوگل و شرکت‌های انرژی غربی، انتشار ویروس رایانه ای استاکس‌نت و حمله به شبکه‌های دولتی کره جنوبی اشاره کرد. [۶]

طرح ارتش آمریکا برای عملیاتهای سایبری بین سالهای ۲۰۱۶ تا ۲۰۲۸ میلادی در یک سند ۷۲ صفحه‌ای در اوایل سال ۲۰۱۰ منتشر شده است. این طرح عملیاتهای سایبری و امکانات مورد نیاز آمریکا برای سالهای ۲۰۱۶ تا ۲۰۲۸ را ارائه می‌دهد. این سند نشان می‌دهد که واژگان کنونی ارتش آمریکا در این زمینه، از جمله عملیاتهای شبکه‌های رایانه‌ای، جنگ الکترونیک، و عملیاتهای اطلاعاتی، به مرور زمان به شدت ناکارآمد خواهند شد. ابعاد اول و دوم این طرح نشان می‌دهد که چگونه فرماندهان و کارکنان از قدرت اطلاعات استفاده می‌کنند تا بتوانند مأموریتهای خود را با موفقیت انجام دهند. بعد سوم بر کسب و حفظ مزیتی در وسایل همگرای فضای سایبری و طیف الکترومغناطیس متمرکز است. این سند مدعی است که ساختار ارتش آمریکا برای پیشی گرفتن از دشمنان و ناکام گذاشتن آنها در این عرصه به خوبی در این سه بُعد تعبیه شده است و می‌تواند در رسیدن به نتایجی کمک کند که باید با اقداماتی یکپارچه در سطوح تاکتیکی، عملیاتی و استراتژیک به آنها نائل شد.[۱]

درجنگ سایبر موضوعات گسترده ای اعم از سازمان و دکترین نظامی، راهبرد، تاکتیک و طراحی مطرح می‌شوند. این جنگ باعث خلق دکترینهای جدید در زمینه انواع نیروهای موردنیاز و اینکه چگونه و کجا باید آنان را مستقر کرد، گردیده است. این که چه نوع

کامپیوترها، حسگرها، شبکه‌ها و پایگاه داده‌ها را انتخاب و در چه موقعیتی آنها را قرار داد، اهمیتی هم‌سطح با نحوه استقرار بمب‌افکنها، تانکها و پیاده نظام و عملیات پشتیبانی و لجستیکی از آنها در گذشته دارد؛ ابزارهای آفند سایبری و پدافند سایبری مطرح می‌شوند که خاص این حوزه هستند. وقتی همه چیز اطلاعات است، توانایی کنترل اطلاعات خود و مختل کردن ارتباطات، فرماندهی و کنترل دشمن، اولین عامل اصلی موفقیت نیروی نظامی خواهد بود.

۷- چند سناریوی یک حمله سایبری

الف- ساده ترین سناریو نفوذ به شبکه و دسترسی به اطلاعات با ارزش می‌باشد. پس از دسترسی رفتار طرف مهاجم سه گونه خواهد بود. رفتار اول کُپی یا سرقت اطلاعات قربانی است. قربانی می‌تواند شخص، سازمان یا یک دولت باشد. با در دست داشتن اطلاعات باارزش و شاید طبقه بندی شده، سیاستهای آتی قربانی و داده‌های محرمانه وی نمایان می‌شود.

رفتار دوم مخدوش کردن یا تغییر اطلاعات قربانی است. قربانی با دراختیار داشتن داده‌های غلط، از رسیدن به هدف صحیح خود بازخواهد ماند. رفتار سوم حذف اطلاعات است. بدون داده‌های مهم، قربانی برای تصمیم گیری و هرنوع عملیات آتی درمانده خواهد شد. مصداق این سناریو، نفوذ به شبکه نیروهای نظامی یک کشور و استفاده از اطلاعات سری در جهت مقابله نظامی در میدان نبرد با کشور قربانی است. مفاهیمی چون جاسوسی سایبری (CyberEspionage) و تروریسم سایبری (CyberTrurism) اینجا مفهوم می‌یابند.

جدیدترین داده های گروه آمادگی مواقع اضطراری رایانه ای ایالات متحده آمریکا[1] نشان می‌دهد که ۸۴ درصد حملات رایانه ای جهت کسب اطلاعات هستند. فعالیت مجرمانه ای که در آن تلاشهای پنهانی برای به دست آوردن کلمات عبور یا مواردی نظیر جزئیات کارت اعتباری انجام می‌شود.این گروه درسال ۲۰۰۳میلادی برای محافظت از زیرساخت اینترنتی کشور آمریکا وهماهنگی دفاع وپاسخ به حملات سایبری تأسیس شد.

رخنه به شبکه‌های حیاتی می‌تواند با استخدام نفوذگران متخصص (Hackers) صورت بگیرد و یا با ارائه نرم‌افزارهای کاربردی و عمومی همانند دیکشنریها که در تهاجم سایبری نقش جاسوس را ایفا کنند (SpyWares).

در آوریل سال ۲۰۰۹، جاسوس‌های کامپیوتری توانستند به پروژه ۳۰۰ میلیارد دلاری جنگنده‌های استرایک فایتر در پنتاگون نفوذ کنند، گران‌ترین برنامه تسلیحاتی وزارت دفاع در طول تاریخ. در کمتر از یک چشم به هم زدن راهزنان سایبری توانستند با چندین ترابایت اطلاعات در مورد طراحی و سیستم‌های الکترونیکی این جنگنده، بگریزند. مقامات رسمی اعلام کردند که به نظر می‌رسد هکرهای چینی عاملان این سرقت بوده‌اند، اما مشکلات ناشی از "مسئله اسناد" ، تأیید چنین ادعایی را بسیار دشوار می‌سازد. [۶]

ب- حمله سایبری به خدمات رسانیهای عمومی با هدف ایجاد نارضایتی در طرف درگیر و دامن زدن به اعتراضهای ناشی از این نارضایتیها در فضای سیاسی، نمونه سناریوی دیگری است. مثال این نوع حمله، ارسال داده‌های ناخواسته و حجیم با تعداد گسترده به سرورهای بانکی است که موجب بروز اختلال در سامانه‌های پولی و مالی و در نتیجه ایجاد گره در نقل و انتقال تجاری و درنهایت بهره برداری سیاسی از فضای نارضایتی عمومی مردم خواهد شد. تهاجم به سامانه‌های مخابراتی و قطع خطوط تلفن و اینترنت مثال دیگری از این سناریو است. اختلال در مکانهای مختلف از فضای سایبر می‌تواند با انتشار ویروسهای رایانه ای یا ارسال ایمیلهای ناخواسته (Spams) درحجم بالا انجام شود.

ج- سناریوی دیگر ایجاد، توسعه و هدایت شبکه‌های اجتماعی (Social Networks) در فضای سایبر است. طرف مهاجم با هدایت این شبکه‌ها به واقع جریان فکری طرف قربانی خود را در اختیار گرفته و با تعریف نیازهای جدید، سوژه‌های اعتراض و نارضایتی و سیاه نمایی از جامعه هدف، سعی در رسیدن به مقاصد خود را خواهد داشت. اگرچه در ایجاد دو سایت فیس بوک و توئیتر، بزرگترین شبکه‌های اجتماعی جهان با میلیونها عضو، نمی توان بطور قطع وجود این نوع سناریو را عنوان کرد ولی در عمل، کارکردی این گونه پیدا کرده اند.

د- انتشار گسترده میکرو رباتهای حسگر(SM)[2] در مکانهای حساس فیزیکی رقیب، یک سناریو از جنگ سایبری است. این جاسوسان سایبری، سامانه های الکترومکانیکی بسیار ریز چند میلیمتری بوده که

[1] United States Computer Emergency Readiness Team

[2] Sensor Micro robots

می‌توان از آنها به صورت انبوه برای گردآوری داده در زمین و هوا و سپس ادغام داده‌ها و ارسال آن برای پردازش و توزیع استفاده نمود.
برای گسترش این میکرو رباتها در منطقه مورد نظر از روش هایی نظیر پرواز دادن بر فراز منطقه و خزش آنها در روی زمین استفاده می‌گردد. گردآوری داده توسط سنسورهای ریزی که روی آنها کار گذاشته شده، صورت می‌گیرد. ارتباطات از طریق ایستگاههای تقویت فیزیکی میکروروباتها انجام می‌شود. برخی کاربردهای این نوع میکروروبات عبارت است از : ایجاد شبکه امنیتی برای حفاظت از تجهیزات با ارزش، مراقبت و شناسایی و جمع آوری اطلاعات جاسوسی از توانمندیهای دشمن. [۳]

۸- محیط فضای سایبر و حوزه‌های آسیب پذیری

مطابق شکل (۱)، محیط فضای سایبر شامل ۶ حوزه می‌باشد. شناخت ابعاد و ویژگیهای این محیط، تحلیلگران و استراتژیستهای دفاع سایبری را در شناخت نقاط قوت و ضعف جبهه خودی و دشمن و حوزه‌های آسیب پذیر آن یاری خواهد نمود.

- کاربران و نیروی انسانی
- داده‌ها و اطلاعات
- روشها و رویه‌های اجرایی
- نرم‌افزارهای رایانه ای
- سخت افزارهای رایانه ای
- شبکه‌های رایانه‌ای

سه حوزه اول،کاربران، رویه‌ها و داده‌ها در دفاع سایبری تا حدود زیادی قابل کنترل هستند. می‌توان کاربرانی دارای صلاحیت و تأییدشده را وارد این حوزه کرد. آموزش مداوم و بروز رسانی شناخت نیروی انسانی از تهدیدات فضای سایبر، می‌تواند از آسیب پذیریها از این طریق بکاهد اگرچه نظارت همیشه لازم است. داده‌ها را می‌توان کنترل و مهار نمود تا کدام اطلاعات وارد رایانه‌ها شده و در شبکه‌ها به اشتراک گذارده شوند. قوانین و دستورالعملها، رویه هایی تعیین شده از جانب سازمان هستند که نقشه راه رسیدن به فضای امن سایبر را نشان می‌دهند.

شکل ۱

سه بخش باقیمانده دیگر، نرم‌افزار، سخت افزار و شبکه هستند که نه تنها امروز بلکه مهم تر از آن در آینده نیز نقاط مهم آسیب پذیر محیط فضای مجازی باقی خواهند ماند. [۹]

۹- پدافند سایبری

"هرکه قبل از وقوع دسیسه‌ها چاره نجوید، پشیمانی در هنگامه هجوم آنها، سودش نخواهد بخشید."

حضرت علی(ع)- کتاب الحیاۀ ج۱ ص ۳۹۳ [۴]

شناخت محیط فضای سایبر و حوزه‌های آسیب پذیر کشور، اولین نکته از پدافند سایبری است. پس از شناخت، پژوهش، طراحی و برنامه ریزی برای هر حوزه خاص، قدم بعدی است. فضای سایبر به شدت مبتنی بر علم و فناوری و دانش بنیان است. فرماندهان و مدیران این عرصه همچنین طراحان دکترین و سازمان دهی پدافند آن نیز به همان شدت باید متخصص و مسلح به دانش این فن باشند. دانش این فضا ترکیبی از علوم مختلف مانند رایانه، الکترونیک، ارتباطات، روانشناسی، جامعه شناسی، حقوق و ... است.

۹-۱- کاربران و نیروی انسانی

پدافند این حوزه را باید به دو بخش تقسیم نمود. بخش نخست کاربرانی هستند که در فضای سایبر با اطلاعات سر و کار دارند. تعریف سطح دسترسی افراد به اطلاعات و آموزش تخصصی نیروی انسانی دو قدم بلند این حوزه است. در تعریف سطح دسترسی یک قانون کارآمد می‌گوید: "هرکس تنها اطلاعاتی در اختیار داشته باشد

که برای پیشبرد کار تعریف شده سازمانی خود، بدان احتیاج دارد و نه بیشتر."

نفوذ دشمن از حفره خلأ علمی کاربران می‌تواند با آموزش مستمر و بروز رسانی این آموزشها مسدود گردد. تأیید صلاحیت و شاخت سابقه به همراه نظارت پیگیر می‌تواند به میزان چشمگیری آسیب پذیری این حوزه را کاهش دهد.

بخش دوم که بخش روانی این حوزه است، در واقع شامل افرادی است که مخاطب فضای مجازی هستند و همیشه تحت تأثیر سناریوهای متخصصین روانشناسی و جامعه شناسی دشمن در بستر فضای سایبر قرار دارند؛ افرادی که به عضویت شبکه‌های اجتماعی همانند فیس بوک و توئیتر در می‌آیند و یا اینکه مخاطب رسانه‌های مختلف این فضا هستند.

دانشمندان علوم ارتباطات سه موج اصلی را در انقلاب ارتباطات و رسانه از هم تمییز می‌دهند: موج اول رسانه‌های چاپی[1] مانند کتاب، مطبوعات و نشریات، موج دوم رسانه‌های صوتی و تصویری[2] مانند تلویزیون و ماهواره و موج سوم رسانه‌های دیجیتال[3] مانند چند رسانه ایها و اینترنت. [۱۲]

در عصر اطلاعات و موج سوم رسانه ها، حذف یا فیلتر راه حل مناسبی به نظر نمی رسد. حضور فعال در این عرصه و بهره برداری هوشمندانه، این حوزه تهدید را به فرصت تبدیل خواهد نمود. استفاده مثبت انقلابیون عرب در بیداری اسلامی خاورمیانه و شمال آفریقا در سال ۲۰۱۱ میلادی از شبکه‌های اجتماعی برای پیشبرد روند انقلاب، از نمونه‌های این مدعا است.

اقبال عمومی و میلیونی گسترده به این شبکه‌ها ظاهراً نیاز جدید بشر امروزی است. برای مثال حضور فراگیر و هوشمندانه در فیس بوک و تشکیل گروههای بحث و تبادل نظر سازنده و روشنگرانه می‌تواند هدایت نیروی انسانی را باعث و نه تنها نفوذ دشمن را سرکوب کند بلکه به سلاحی برای آفند سایبری بدل شود. طراحی مناسب، جذاب و بومی از این نوع شبکه‌ها قدم بعدی است.

گام بلند مدت بعدی، آموزش و بالا بردن فرهنگ و دانش رسانه ای نیروی انسانی است؛ با ترتیبی که حملات روانی و سایبری از این حوزه، آثار مخرب کمتری به فضای مجازی خودی وارد نماید.

[1] printed media
[2] Visual media
[3] Digital media

۹-۲- داده‌ها و اطلاعات

طبقه بندی ارزش اطلاعاتی راه گشا و حتی کاهش دهنده هزینه پدافند در این حوزه است. برای صیانت از داده‌های اطلاعاتی باید به میزان حساسیت و منافعی که آن اطلاعات فراهم می‌کنند، هزینه نگهداری پرداخت نمود و تلاش امنیتی انجام داد. اینکه چه نوع اطلاعاتی و بر روی چه مکانی از فضای سایبر قرار گیرد و یا کدام پایگاه دانش روی کدام سرور فعالیت نماید، همانند سازماندهی توپخانه، ناوهای جنگی و جنگنده‌های هوایی در نبردهای اعصار گذشته است.

۹-۳- روشها و رویه‌های اجرایی

دستورالعملهای درج و استخراج اطلاعات، نگهداری داده ها، تهیه نسخه‌های پشتیبان که درصورت بروز حملات سایبری، سامانه در کوتاهترین زمان به حالت پایدار قبلی بازگردد، همه و همه باید توسط یک نگاه کارشناسی و متخصص به دقت تهیه و تنظیم شده و جهت اجرای صحیح به نیروی انسانی و کاربران فضای مجازی ابلاغ گردد.

۹-۴- نرم‌افزارهای رایانه ای

این حوزه یکی از نقاط آسیب پذیر فضای سایبر است که قبلاً به آن اشاره شد. یک نرم‌افزار کاربردی می‌تواند بطور کاملاً نامحسوس یک جاسوس سایبری باشد که در لایه‌های پنهان سیستم عامل فعالیتهای مخربی همچون سرقت اطلاعات و یا تخریب آنها را انجام می‌دهد. این جاسوس مجازی تنها زمان کمی پس از اتصال به شبکه، داده‌های به سرقت برده را به مقصد ارسال می‌کند. خود سیستم عامل که بستر فعالیت نرم‌افزار است، می‌تواند کلیه فعالیتهای کاربر را رصد کرده و جاسوس اصلی این سناریو باشد.

پدافند مؤثر این حوزه بومی سازی خط طراحی و تولید نرم‌افزار است. امّا آیا می‌توان کلیه نرم‌افزارها را کنار گذاشت و تنها و تنها از نرم‌افزارهای بومی قابل اعتماد استفاده کرد؟ این کار غیرمنطقی است و در دهکده جهانی امروز نمی توان در یک فضای سایبر بسته زندگی کرد. راه حل آن بومی سازی نرم‌افزارهای پدافندی فضای مجازی است؛ نرم‌افزارهایی همچون دیواره‌های آتش (فایروال[4])، آنتی

[4] Firewall

ویروسها و ضدجاسوسها[1]. دیواره آتش یک نرم‌افزار کنترل کننده است که کلیه پورتهای ورودی و خروجی سامانه را بررسی و از هرگونه فعالیت مشکوک جلوگیری می‌کند به علاوه قابلیت‌های حفاظتی و نظارتی دیگر.

ویندوز شرکت میکروسافت رایجترین و پرکاربردترین سیستم عامل دنیا است. این مسأله باعث هجوم گسترده نفوذگران سایبری به این سیستم عامل و محصولات نرم‌افزاری این شرکت شده است. پنج هدف از اهداف بالای فهرست سیستمهای عامل آسیب پذیر در سال ۲۰۰۶ تماماً متعلق به شرکت مایکروسافت وشامل برنامه های کاربردی اینترنت اکسپلورر (IE) ومایکروسافت آفیس (MS Office) است .

تولید یک سیستم عامل مطمئن بومی با اتکا به دانش داخلی، بستر امنی برای فعالیت‌های نرم‌افزاری خواهد بود. در این راه توجه ویژه به برنامه‌های کد باز (Open Source) و سیستم عامل مهمی چون لینوکس کارساز هستند. اینگونه برنامه‌ها به متخصصین امکان می‌دهند که تا ریزترین لایه‌ها فرو رفته و از کارکرد همه بخشها اطمینان حاصل نمایند به علاوه اینکه آن برنامه یا سیستم عامل را به دلخواه برای خود سفارشی نموده و مطابق نیازهای سازمانی کدنویسی کنند.

۹-۵- سخت افزارهای رایانه‌ای

سناریوی این حوزه می‌تواند جاگذاری یک قطعه سخت افزاری خاص درون رایانه یا تجهیزات شبکه همچون روترها و سوئیچها باشد. مأموریت این قطعه جمع آوری اطلاعات و ارسال به مقصد تعیین شده خواهد بود. بومی نمودن سخت افزاری برای کشورهای درحال توسعه به علت تکنولوژی بالای فناوری در این عرصه، بسیار مشکل است ولی غیرممکن نخواهد بود و می‌تواند به عنوان یک ایده بلندمدت هدف گذاری گردد.

تولید سخت افزارهای کنترلی همچون دیواره‌های آتش سخت افزاری و تجهیزات شبکه که در خط مقدم فضای سایبری خودی قرار می‌گیرند، از اولویتهای این بومی سازی هستند. اگر درگاه (Gateway) ورود به شبکه سازمان یا فضای مجازی کشور خوب محافظت شود، درصد امنیت بطور چشمگیری افزایش می‌یابد.

۹-۶- شبکه‌های رایانه‌ای

شبکه‌ها شامل سخت افزار شبکه، نرم‌افزار و رسانه‌های انتقال و ارتباط بطور توأم هستند. در بخش سخت افزاری تعداد زیادی از شرکتها و حتی افراد در منازل خود برای راه اندازی شبکه های بزرگ و کوچک رایانه ای از تجهیزات شبکه ای مختلف اعم از روتر و کارت شبکه استفاده می کنند. بخش اعظم این بازار در حال حاضر در کنترل شرکت سیسکو (CISCO) است. طبیعی است این انحصار در بازار سخت افزار شبکه ها، نقطه آسیب پذیری برای برپایی یک فضای سایبری امن خواهد بود.

به نوشته روزنامه فرانسوی تریبون، کاربران اینترنت در ایران از ۱ میلیون نفر در اوایل قرن بیست و یکم به ۲۳ میلیون نفر در هشت سال بعد رسید. امروزه کاربران اینترنت در ایران، کمی بیشتر از ۲۸ میلیون نفر هستند. جهان درحال اتصال مجازی و تبدیل شدن به یک دهکده کوچک دیجیتالی برپایه فناوریهای نوین اطلاعاتی و ارتباطی است. [۱۰]

در اینترنت امروزه هر کاربر برای دست‌یابی به اطلاعات در خصوص یک موضوع باید از موتورهای جستجو (Search Engine) استفاده کند. اگر موتور جستجو نباشد اساساً نمی‌توان به محتوای اینترنت دسترسی پیدا کرد. نقش موتور جستجو، هدایت در وب است؛ یعنی هر آنچه که بخواهد به کاربر نشان می‌دهد. نقش مدیریت موتورهای جستجو اینجا آشکار می‌شود.

همانند چندین حوزه قبل که بررسی شد، امنیت و پایداری این حوزه نیز به روند تولید مطمئن و نظارت در برپایی و بکارگیری شبکه بستگی تام دارد و باز همانند بخشهای گذشته با سلاح بومی سازی شبکه‌ها و رمزنگاری در انتقال داده‌ها و ارتباطات شبکه، فضای سایبر خودی را با پدافند سایبری ایمن حفاظت نمود.

[1] Anti spyware

۱۰- نتیجه

سهم عمده جنگهای آینده با نبردهای سایبری و اطلاعاتی خواهد بود. همانگونه که اشاره شد به گفته "سن تزو" فرمانده نظامی و سیاستمدار کهنه کار چینی در۲۴ قرن پیش درکتاب "هنر جنگ"، بهترین شکل هنر جنگ، پیروزی بدون جنگیدن در یک نبرد مسلحانه ساده است. برتریهای این نوع نبرد در مقایسه با لشگرکشیهای نظامی، سیاستمردان و دولتمردان را بسوی آن می‌کشاند تا ضمن حفظ یا بدست آوردن قدرت سیاسی، اقتصادی و بازدارندگی نظامی، به دلیل گمنامی و بی هویت بودن تعاملات دیجیتال، ژستهای حقوق بشری خود را حفظ کرده و پشتیبانی افکار عمومی را که با جنگهای فیزیکی و ویرانیهای آن مخالفت می‌کنند، بدست آورند.

کشور ما به دلیل اتخاذ سیاستهایی مبتنی براصول خود درجهان و پایداری بر مواضع خود، همواره مورد انواع تهدیدات قرار داشته است. اکنون که نوع تهدیدات به تهدیدات سایبری، جنگ نرم و نبردهای روانی معطوف شده است، باید با یک نگاه آینده پژوهانه و با برنامه ریزیهای کوتاه مدت، میانمدت و بلندمدت در این عرصه، پدافند سایبری کشور را جهت مقابله تقویت نمود.

درحال حاضر که کشور گامهای اولیه را بسوی فضای مجازی بر می‌دارد و زیرساختها درحال طراحی و آماده سازی هستند، تأسیس تشکیلاتی مناسب جهت هماهنگی کلیه نهادهای دولتی و خصوصی و اتخاذ وحدت رویه در مقابله با تهدیدات سایبری ضروری است؛ تیمی متخصص که با نگاه به آینده و شناخت نقاط آسیب پذیر، سیاستها و نقشه راه فضای سایبر را تهیه نماید. در این راه، استفاده از تجربه کشورهای دیگر و اتکا به پتانسیل جوانان مستعد و بخش خصوصی و صدالبته بومی سازی حوزه‌های مختلف این فضا، می‌تواند تهدیدات سایبری را ناکام نماید.

مراجع

[۱] تدابیر عملیات‌های سایبری آمریکا برای ۲۰۱۶ ـ ۲۰۲۸ ، سایت باشگاه افسران جوان جنگ نرم (club.revayat.ir)، شهریور ۱۳۹۰

[۲] اندیشگاه شریف ، مطالعات تطبیقی انقلاب در امور نظامی ، ویرایش مسعود منزوی ، مرکز آینده پژوهی علوم و فناوری دفاعی مؤسسه آموزشی و تحقیقاتی صنایع دفاعی ، مرداد ماه ۱۳۸۸

[۳] اندیشگاه شریف ، پارادایم های حاکم بر جنگ های آینده ، ویرایش مسعود منزوی ، مرکز آینده پژوهی علوم و فناوری دفاعی مؤسسه آموزشی و تحقیقاتی صنایع دفاعی ، مرداد ماه ۱۳۸۸

[۴] طاهره مسلمی زاده ، پایگاه دانش آیات و روایات آینده ه اندیشی ، ویراسته عقیل ملکی فر ، مرکز آینده پژوهی علوم و فناوری دفاعی مؤسسه آموزشی و تحقیقاتی صنایع دفاعی ، اسفند ماه ۱۳۸۴

[۵] ذبیح‌الله تجری غریب‌آبادی ، جنگ نرم چیست و راه‌های مقابله با آن کدام است؟ ، سایت ابنا (ABNA.ir) ، ۱۳۸۹

[۶] جنگ‌سایبری مؤثرتر از اقدامات‌نظامی یا سیاسی‌سنتی خواهد بود، سایت باشگاه افسران جوان جنگ نرم (club.revayat.ir) ، ۱۳۹۰

[۷] جنگ و دفاع سایبر، اندیشگاه شریف و اندیشکده کاوشگران آینده ، دی ماه ۱۳۸۴

[۸] کاوه سیدمفیدی ، جنگ سایبری ، سکیور تارگت ، مارس و آوریل ۲۰۰۴

[۹] شین پی .کوریل ، نیروی هوایی و مأموریت فضای مجازی(سایبر) :دفاع از شبکه رایانه ای نیروی هوایی در آینده ، ترجمه مسعود منزوی ، مرکز آینده پژوهی علوم و فناوری دفاعی مؤسسه آموزشی و تحقیقاتی صنایع دفاعی ، مهر ماه ۱۳۸۸

[۱۰] اینترنت و تاریخچه آن ، مقالات وب ،(komakweb.com)

[۱۱] بمب الکترومغناطیس ، دانشنامه رشد ، (daneshnameh.roshd.ir)

[۱۲] جنگ نرم در فضای سایبر ، سایت تبیان ، (tebyan.net)

[13] Shane P. Courville , AIR FORCE AND THE CYBERSPACE MISSION DEFENDING THE AIR FORCE'S COMPUTER NETWORK IN THE FUTURE , US Air University , December 2007