جغرافیا (فصلنامه علمی ـ پژوهشی و بین‌المللی انجمن جغرافیای ایران)
دوره جدید، سال دوازدهم، شماره ۴۳، زمستان ۱۳۹۳

فضای سایبری و تعاریف جدید در جغرافیای سیاسی

حسن کامران دستجردی[۱] و زهرا میرمحمدی[۲]

تاریخ وصول: ۱۳۹۲/۷/۱۸، تاریخ تایید: ۱۳۹۲/۱۰/۱۵

چکیده

سال‌های زیادی از شروع بحث فضای مجازی گذشته و جغرافیای سیاسی جهان را متحول ساخته است ولی به‌دلیل بدیع بودن موضوع و شاید غیرقابل لمس بودن آن، در مورد حتی معنای ابتدایی‌ترین اصطلاحات مانند فضای مجازی، جنگ سایبری، حمله سایبری، و غیره انسجام خاصی وجود ندارد .این مقاله نتیجه گردآوری، مطالعه و تحقیق بر روی مستندات و اقدامات کشورهای پیشرو در این زمینه مانند روسیه و آمریکا بوده و درصدد استخراج تعاریف، اصطلاحات، طبقه‌بندی، ویژگی، انواع و ... جنگ سایبری است.

کلیدواژگان: سایبر، فضای سایبری، جنگ سایبری، حمله سایبری، پدافند سایبری، دفاع سایبری، تروریسم سایبری.

۱. دانشیار دانشگاه تهران، پست الکترونیک: Dastjerdi.ha@yahoo.com
۲. پژوهشگر مرکز تحقیقات ایران، پست الکترونیک: mirmohammadi@itrc.ac.ir

مقدمه

توجه و حساسیت به مقوله امنیت ملی، در هزاره‌ای که تمام نیروی اکثر حاکمان زورگو متوجه و متمرکز بر تجاوز و نفوذ است، امری کاملاً ضروری و اجتناب‌ناپذیر است. بدون شک هر لحظه دشمن می‌تواند در حال طرح ریزی حمله باشد و تنها یک راه یا روزنه نفوذ کافی‌است تا وی به قصد خود نائل گردد. در تعریفی سنتی سربازان از مرزهای جغرافیایی حفاظت می‌کنند و مسئولین فرهنگی به تهاجم فرهنگی می‌اندیشند. این اندیشه که "این‌ها را با ما کاری نیست که اگر زمان آن فرا رسد، تفنگ بر دست گرفته و آتش می‌کنیم" در دنیای امروز ما بسیار خطرناک و دور از ذهن است. در دنیای پیشرفته امروز وبا گسترش خدمات دولت الکترونیک و وابستگی زیر ساخت‌های حیاتی کشورها به فضای مجازی، تهدیدات و مخاطرات متعددی وجود دارند که عموماً به آنها توجه نمی‌شود یا کمتر مورد توجه قرار می‌گیرند. امروز برای تضعیف دشمن لزومی ندارد حتماً خطوط راه‌آهن او را بمباران کنیم، بلکه یک مودم و سیستم رایانه برای حمله کافیست.

با گسترش روزافزون استفاده از رایانه در دنیا، تشکیل و گسترش فضای مجازی و غیرفیزیکی که افراد به ناچار بر حسب عادت در آن غرق می‌شوند می‌توان ادعا نمود که استفاده همه‌جانبه از رایانه‌ها، فضای سایبری را به اندازه کهکشان گسترده کرده است. پس باید در این گستره نیز نیرومند شد و توانایی لازم برای مقابله با دشمن سایبری را کسب نمود.

این مختصر، فقط مقدمه‌ای بر تبیین و توضیح این امر است که حفاظت از مرزهای مجازی که اطلاعات و آمار مهم، ضروری، حساس و حیاتی را درون خود جای داده‌اند و تمام عناصر وابسته به دنیای مجازی را در خود دارند، بیش از حفاظت از مرزهای جغرافیایی برای هر کشوری دارای اهمیت است.

مفاهیم اولیه:[2,1]

کارشناسان روسیه و آمریکا بر روی بیست اصطلاح سایبری به توافق رسیدند. آنها سندی تحت عنوان واژه‌نامه مشترک آمریکا و روسیه را تدوین نموده‌اند که می‌توان آن را مرجعی بین‌المللی و استاندارد برای تعاریف و اصطلاحات مربوط به حوزه سایبر قلمداد کرد. این بیست اصطلاح

در سه حوزه قابل طبقه‌بندی هستند:

حوزه اول: شامل شش اصطلاح فضا، زیرساخت، سرویس سایبری و زیرمجموعه‌های حیاتی‌تر آنها که شامل فضا، زیرساخت و سرویس‌های حیاتی و حساس سایبری هستند، می‌باشد.ارتباط بین فضا، زیرساخت‌ها و سرویس‌های سایبری به راحتی قابل نمایش در یک گرافیک ساده و بدون انتقال اطلاعات غلط، نیست، فضای سایبری با کمک زیرساختها ایجاد می‌شود و به همین ترتیب سرویس‌ها بر روی فضای مجازی و زیرساختها قابل ارائه هستند. برای درک بهتر معنا و مفهوم این موضوع به تعریف این شش اصطلاح اشاره می‌شود:

سایبر: سایبر پیشوندی برای توصیف یک شخص، یک شی، یک ایده و یا یک فضاست که مربوط به دنیای رایانه و اطلاعات بوده که همگی در نتیجه انتشار روز افزون رایانه پدید آمده‌اند. کما اینکه اغلب عناصر درگیر با اینترنت با این پیشوند قابل تشریح هستند.

فضای سایبری: یک محیط الکترونیکی و غیرفیزیکی است که از طریق آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند. ترکیب دو کلمه "فضا و سایبر" حاکی از آن است که این عبارت دارای بعد است. بعضی افراد از فضای سایبری به‌عنوان فضایی جدید در کنار زمین، هوا، دریا و فضا یاد کرده و آن را فضایی مصنوعی ساخته شده توسط انسان می‌دانند. این واژه تشریح سرزمین غیرفیزیکی تشکیل شده توسط نظام‌های رایانه‌ای می‌باشد. در فضای سایبری نمی‌توان از حواس پنج‌گانه طبیعی استفاده نمود ولی این گستره دارای عناصر[1] خاص خود است مانند (فایل‌ها، پیغام‌های الکترونیکی، عکس‌ها، فیلم‌ها و ...). این فضا دارای مدل انتقالی و حمل و نقل نیز می‌باشد. برخلاف فضای حقیقی، سیر و گشت در این سرزمین بدون هیچ‌گونه حرکت فیزیکی و بسیار سریع مقدور است، و تنها با حرکت موشواره یا فشردن کلیدی در صفحه کی‌بورد امکان‌پذیر می‌شود.

زیرساخت‌های سایبری: به اجتماعی از مردم، پردازش‌ها، سیستم‌هایی که فضای سایبری را تشکیل می‌دهند گفته می‌شود. زیرساختهای سایبری هشت جزء مهم، محیط (ساختمان، محل برج‌های سلولی، فضایی که ماهواره‌ها در آن قرار دارند، زمین و دریا که از آنها کابل عبور

1.Object

کرده و ...)، انرژی(برق، باتری، ژنراتور و...)، سخت‌افزار (تراشه‌های سیمی‌کانداکتور، کارت‌های الکترونیکی، مدار بسته، امکانات انتقال فلزی و فیبر نوری و...)، نرم‌افزار (کد منبع، برنامه‌های کامپایلر، نسخه‌های کنترل و مدیریت دیجیتال، پایگاه داده و...)، شبکه (نود، ارتباطات، توپولوژی، پروتکل و...)، انتقال[1](انتقال‌دهنده‌های اطلاعات بر روی زیرساخت‌ها، الگوها و ارقام ترافیکی، رهگیری اطلاعات و...)، انسان (طراحان، پیاده‌سازان، اپراتورها، کارمندان تعمیر و نگهداری و ...) و سیاست (قوانین و قواعد مورد توافق، استانداردها، مقررات و ...) را دربر می‌گیرند.

سرویس‌های سایبری: مبادله طیف وسیعی از داده‌ها به صورت مستقیم و یا غیرمستقیم در فضای مجازی برای بهره‌مندی انسان‌ها می‌باشد. سرویس‌های سایبری با کمک نرم‌افزارهای کاربردی فراهم می‌شوند. کاربردها ممکن است با پردازش و توزیع داده‌ها در فضای سایبری اجرا شوند. این بدین معناست که سرویس‌ها وابسته به موقعیت مکانی و جغرافیایی نیستند. سرویس‌های سایبری هم می‌توانند به صورت آنلاین و یا آفلاین، هم به شکل محلی و یا راه دور، هم به فرم بلادرنگ و یا با تاخیر زمانی انجام شوند. این سرویس‌ها در حال حاضر باید به‌عنوان یک مفهوم پایان‌ناپذیر در نظر گرفته شوند و ارائه سرویس‌های جدید نباید خارج از تصور باشند.

زیرساخت‌ها و سرویس‌های سایبری برای حفظ امنیت عمومی و ملی، ثبات اقتصادی و ثبات بین‌المللی حیاتی هستند. بنابراین لازم است زیرساختها و سرویس‌های بحرانی (حساس) در فضای سایبری شناسایی شوند.

زیرساختهای حساس(بحرانی): زیرساخت‌هایی که سرویس‌های امنیت عمومی و ملی، ثبات اقتصادی، ثبات بین‌المللی به آن‌ها وابسته هستند و به پایداری و ترمیم فضای مجازی کمک می‌کنند، زیرساخت‌های حساس هستند.

اکثر زیرساخت‌های حساس معمولاً منجر به ایجاد ارتباطات، تولید انرژی، بستر نقل و انتقال، خدمات مالی و عملیات دولتی پیوسته (زیرساختهایی که عملیات دولتی بدون قطعی و اختلال

1. Payload

به‌کار خود ادامه دهند) می‌شوند. بنابراین سیستم‌های رایانه‌ای و عملیات شبکه‌ای برای بهره‌برداری اولیه از مهم‌ترین جنبه‌های این بخش بسیار مهم هستند. بسیاری از کشورها به زیرساخت‌های حساس سایبری وابسته‌تر از بعضی کشورهای دیگر هستند. میزان وابستگی تا حدی به دلیل افزایش پیچیدگی خدمات و تا حدی به دلیل کم بودن تکنولوژی[1] و بازگشت به بالا[2] است.

سرویس‌های حساس(بحرانی): سرویس‌هایی که برای حفظ امنیت عمومی و ملی، ثبات اقتصادی، ثبات بین‌المللی ضروری هستند را شامل می‌شوند.

حوزه دوم: در این بخش به ارائه تعاریف برای پنج اصطلاح جرم، تروریسم، برخورد، جنگ و امنیت سایبری می‌پردازیم. تعریف اصلی برای وقوع جرم این گونه است، عموماً وقتی جرم رخ می‌دهد که قانون شکسته می‌شود.

جرائم سایبری: استفاده از فضای سایبری برای اهداف جنایی و نقض قوانین بین‌المللی و داخلی تعریف شده در فضای سایبری می‌باشد.

با توجه به قوانین موجود در فضای سایبری می‌توان جرائم را تعریف و شناسایی نمود. با کمک ساختارهای حقوقی موجود خیلی سریع می‌توان جرائم را ردیابی کرد. این قابل درک است که ملاحظات اداری و قضایی نقش اساسی در استفاده از این واژه دارند. پیچیدگی وقتی بوجود می‌آید که فعالیتی توسط فردی در یک کشور انجام شود در حالیکه منبع آن در کشوری دیگر (کشور دوم) است و تاثیر آن بر افراد، سازمان‌ها و عناصر داخل کشور سوم باشد.

کنوانسیون جرایم سایبری اولین پیمان بین‌المللی به دنبال هماهنگ کردن قوانین جرایم اینترنتی در سراسر کشورهای جهان است که در سال ۲۰۰۱ ایجاد شد و توسط شرکتی متشکل از شورای اروپا و ایالت متحده آمریکا به‌عنوان ناظر شروع به کار نمود. همان‌طور که مشهود است آمریکا در این پیمان بود ولی روسیه نبود.

تروریسم سایبری: استفاده‌کنندگان از فضای سایبری برای اعمال تروریسمی با قوانین سایبری

1. Low - Tech
2. Back -Up

بین‌المللی و یا داخلی در مورد واژه تروریسم می‌باشد.

با توجه به توسعه گسترده اخیر تعریف تروریسم، واژه تروریسم سایبری عمدتاً با تکیه بر فعالیت‌های موجود طراحی شده است.

برخورد سایبری: یک تفاوت کلیدی برای جنگ سایبری و برخورد سایبری وجود دارد. برخورد سایبریمی تواند شامل بازیگران و مهاجمان سیاسی باشد در حالی‌که جنگ سایبری فقط و فقط مهاجمان نظامی را شامل می‌شود. برخورد سایبری خرابکاریهایی کمتر از یک آستانه بحران است و معمولاً کل کشور را درگیر نمی‌کند.

جنگ سایبری: در جنگ سایبری دولتها درگیر می‌شوند و بر روی یک زنجیره‌ای رخ می‌دهد و بر عکس برخورد سایبری فراتر از آستانه بحرانی است و همانطور که در بالا اشاره شد مهاجمان آن حتماً نظامی هستند.

جنگ سایبری میان دولتها یا میان کشورهایی که در آن حملات سایبری میان دولتها به‌عنوان بخشی از یک عملیات نظامی توسط مهاجمان دولتی علیه زیرساختهای سایبری را جنگ سایبری می‌نامند و جنگ سایبری دو گونه شکل می‌گیرد:

۱. در صورت اعلان: که به طور رسمی توسطمقامات یکی از طرفین جنگ اعلام گردد
۲. فقدان اعلان: بدون اعلان رسمی توسط مقامات درگیر سایبری

اگر مهاجمان سیاسی باشند اتفاقات جنگ تلقی نمی‌شوند اما به فعالیتهای نظامی جنگ سایبری اطلاق می‌شود. جنگ سایبری می‌تواند به روش‌های مختلف و توسط گروه‌های مختلف رخ دهد. به‌همین منظور این توافق نامه برای حفاظت از زیرساخت‌های حیاتی کشورها از جنگ و مصون ماندن آنها تهیه شده است.

امنیت سایبری: این اصطلاح یک ویژگی از فضای سایبری است که توانایی مقاومت در برابر تهدیدات عمدی و غیرعمدی و پاسخ و بازیابی به آنها را دارد، امنیت سایبری شامل اطلاعات و سایبر می‌شود. روس‌ها در معنی این واژه اشاره ضمنی به حفاظت می‌کنند در حالی‌که آمریکایی‌ها ارائه حفاظت را مدنظر دارند.

حوزه سوم: این بخش از بحث به تعریف نه واژه، ستیز، حمله، پاتک، اقدام متقابل، پدافند، دفاع، توانایی دفاع، تهاجم، بهره کشی و بازدارندگی (پیشگیری) سایبری می‌پردازد.

ستیز سایبری: به حملات سایبری که توسط مهاجمان دولتی و نظامی علیه زیرساختهای سایبری در رابطه با مبارزه با دولت باشد گفته می‌شود. تفاوت با جنگ سایبری در این است که جنگ اشاره به اقدامات و یا تکنیک‌های انجام شده توسط یک یا بیشتر از طرفین متخاصم دارد.

حملات سایبری: استفاده تهاجمی از سلاح‌های اینترنتی در نظر گرفته شده برای صدمه زدن (آسیب رساندن) به هدف تعیین شده است. لازم به توجه است که، کلمه "آسیب" شامل رفتار اهانت‌آمیز، مهار موقت یا دائم عملیات، خدمات و... می‌باشد. تنها حمله‌ای موثر است که بر روی آسیب‌پذیری ذاتی اعمال شود.

حمله سایبری با توجه به نوع سلاح هدف تعریف می‌شود و نه ماهیت هدف. بنابراین هدف یک حمله سایبری با سلاح‌های سایبر علیه غیرسایبر یا سایبر معنی پیدا می‌کند.

سئوالاتی که برای محققین و صاحب‌نظران در این زمینه مطرح می‌باشد، این است که، آیا مواردی چون "تبلیغات، کنترل وب‌سایت‌ها ومبارزات پست الکترونیکی" حمله را تشکیل می‌دهند؟

آنچه که در آژانس استاندارد ناتو (NSA)و (CNA) تعریف شده است، حملات شبکه‌های کامپیوتری، اختلال، انکار، کاهش و یا از بین بردن اطلاعات ساکن در یک کامپیوتر و یا شبکه کامپیوتری نوعی از حملات سایبری هستند.[2]

پاتک (حمله متقابل) سایبری: استفاده از سلاح‌های اینترنتی در نظر گرفته شده برای صدمه زدن به هدف تعیین شده در پاسخ به حمله است. پاتک سایبری ممکن است نامتقارن باشد. یک پاتک سایبری می‌تواند استفاده از یک سلاح سایبری برای حمله به یک دارایی غیرسایبری و یا در برابر یک دارایی سایبری و نه یک حمله غیرسایبری به یک دارایی غیرسایبری و یا در برابر یک دارایی سایبری باشد. بنابراین این نوع حمله، توسط نوع سلاح و نه ماهیت هدف تعریف می‌شود.

اقدام متقابل(دفاع) سایبری: به‌کارگیری توانایی دفاعی سایبری خاص برای منحرف کردن ویا تغییر مسیر حملات سایبری است. گنجاندن این مطلب در طبقه‌بندی اولیه مربوط به دفاع مهم است، زیرا به توضیح منافع مشروع ملت‌ها و ایالات برای سرمایه‌گذاری در توسعه قابلیت‌هایی که ممکن است برای حفاظت از منافع خود لازم باشد، کمک می‌کند.

به عبارت دیگر، اقدامات متقابل دفاع سایبری، اقداماتی است که توسط یک حزب به صورت"

"فعال" یا "غیرفعال" به عنوان بخشی از یک استراتژی دفاعی در طی یک حمله و یا بعد آنکه بر ضد منافع حزب صورت گرفته است، می‌باشد. در مدل فعال، اقدام متقابل می‌تواند با تلاش برای مختل کردن مهاجم به حمله او واکنش نشان دهد. اما در مدل غیر فعال، می‌تواند توانایی حفاظت از منافع خود رادر برابرحمله بالا ببرد

پدافند سایبری: به قابلیت‌های سازمان یافته برای محافظت در برابر کاهش اثرات و صدمات حملات سایبری و بازیابی سریع خرابی‌ها و یا به اقدامات دفاعی صورت گرفته توسط یک کشور و یا حزب برای حفاظت از منافع خود در پیش‌بینی ازحمله گفته می‌شود.

دفاعی موثراست که به‌طور خودکار در سیستم‌های الکترونیکی به‌طور معمول بر اساس تشخیص، انزوا، گزارش، بهبود و خنثی‌سازی انجام شود که به این ویژگی "پدافند غیرعامل" گفته می‌شود. اما در صورتی‌که توانایی برای جذب ابزار یک حمله که ممکن است یک استراتژی دفاعی موثر باشد را "پدافند عامل" گویند.

توانایی دفاع سایبری: توانایی موثر محافظت و یا دفع در برابر استثمار و یا حمله سایبری، که ممکن است به‌عنوان یک عامل بازدارنده سایبری مورد استفاده قرار گیرد.

بهره‌کشی سایبری: استفاده از فرصت‌ها در فضای مجازی برای رسیدن به یک هدف است. این فرصت می‌تواند با قدرتی که در مهاجم وجود دارد و یا با استفاده از آسیب‌پذیری‌های دشمن پیش آید.

توانایی تهاجم سایبری: توانایی برای شروع یک حمله سایبری که ممکن است به‌عنوان یک عامل بازدارنده سایبری مورد استفاده قرار گیرد.

تعاریف شناخته شده در طول این فرایند مورد مشورت صاحب‌نظران و محققان قرار گرفته است. به عنوان مثال، وزارت دفاع ایالات متحده آمریکا دارای یک تعریف مرتبط برای این واژه "عملیات فضای مجازی جهت به‌کارگیری قابلیت‌های اینترنتی که در آن هدف اصلی دفاع در داخل و یا از طریق فضای مجازی تعریف شده است" دارد. این عملیات شامل عملیات شبکه‌های کامپیوتری و فعالیت‌های مرتبط با کار و دفاع از شبکه اطلاعات جهانی هستند.[1,3]

بازدارنده سایبری: یک ساز و کار اعلام شده است که فرض آن در دلسرد کردن مهاجم جنگ سایبری و یا یک فعالیت تهدیدآمیز در فضای مجازی موثر است. ساز و کارهای بازدارنده

سایبری را می‌توان سیاست، استقرار، سلاح، توانایی و یا اتحاد دانست.

جنگ فیزیکی با جنگ سایبری از برخی جهات کاملاً شبیه به هم هستند. مثلاً هدف اصلی در جنگ، از هر نوع که می‌خواهد باشد، وارد آوردن ضرر و زیان به دشمن است. انگیزه اصلی در جنگ باید قاعدتاً تصاحب منابع دشمن باشد. در حقیقت فلج نمودن دشمن بدون در اختیارگرفتن منابع آن چندان معقول به‌نظر نمی‌رسد. جنگ سایبری[1] به بازیگران این امکان را می‌دهد که بدون توسل به جنگ مسلحانه، به اهداف سیاسی و راهبردی خود دست یابند. در ذیل به ویژگی‌های خاص جنگ سایبری اشاره می‌کنیم.

- فضای مجازی قدرت غیرواقعی به بازیگران کوچک و کم‌اهمیت می‌دهد.
- با استفاده از آدرس اشتباه، سرورهای خارجی و اسامی مستعار، مهاجمان می‌توانند در عین ناشناس بودن و مصونیت نسبی برای مدت کوتاهی در فضای سایبری فعالیت و خرابکاری کنند.
- در فضای مجازی، مرز بین نظامی و غیرنظامی و نیز فیزیکی و مجازی چندان روشن و شفاف نیست، از این رو، قدرت یا از طریق دولت‌ها، یا بازیگران غیردولتی اعمال می‌شود یا از طریق پروکسی‌ها.
- در کنار سایر میدان‌های سنتی نبرد مثل زمین، هوا، دریا و فضا باید فضای مجازی را «پنجمین میدان نبرد» دانست. جنگ سایبری از اجزای جدید این محیط چند بعدی است، اما کاملاً جدا از آن در نظر گرفته نمی‌شود.
- در فضای مجازی، اقدامات شبه‌جنگی به احتمال زیاد همراه با سایر اشکال زور و منازعه رخ می‌دهد، اما روش‌ها و ابزارهای جنگ سایبری قطعاً متفاوت از سایر جنگ‌ها خواهد بود.

بارزترین ویژگی جنگ سایبری (امنیت سایبری به‌طور عام)، تحول سریع تهدیدات است. این

1. Cyber War

تغییرات می‌توانند آنقدر ناگهانی و غیرمنتظره باشند که از همان ابتدا دور تسلسل عمل و عکس‌العمل در راهبرد سنتی را از حرکت بیاندازند.

نیازمندی‌های جنگ سایبری: بدون شک عملیات سایبری دارای ملزومات خاص خود است؛ توان انسانی متخصص و تجهیزات مورد لزوم. البته اولین نیاز این نوع عملیات، حضور و اتصال در این فضا است. اشیائی که در فضای سایبری حضور نداشته باشند عملاً هم از گزند حمله مصون هستند و هم خود هرگز مبادرت به حمله نمی‌نمایند.

مقاصد جنگ سایبری[5,4]

در شرایطی که مبارزه فیزیکی مدنظر باشد، جنگ سایبر موفق نیست و نمی‌تواند منجر به اشغال سرزمین شود و تقریباً غیرقابل تصور است که یک جنگ سایبر هرچند قوی بتواند دولت دشمن را سرنگون کند. جنگ سایبری متناسب با مقصد آن متفاوت عمل می‌کند. مقاصد در جنگ سایبری به سه صورت مقاصد نظامی، غیر نظامی(دولتی) و شخصی تقسیم‌بندی می‌شوند.

وقتی مقصد نظامی باشد، درست مانند جنگ واقعی در اینجا بر خلاف چهار رکن دیگر جنگ که پیش‌تر بیان داشتیم، این جنگ در سایه‌ی فضای مجازی صورت می‌پذیرد. در اینجا به یک مرکز فرماندهی جنگ سایبر نیاز است و نیازمند سلاح‌هایی مجازی و دفاعی هستیم تا جلوی حمله گرفته شود و ما نیز قادر به حمله‌ی متقابل باشیم.

مقصد غیر نظامی، عبارت از اختلال در سرویس‌دهنده‌ی وب، سیستم‌های اطلاعات سازمانی، سیستم‌های سرور، لینک‌های ارتباطی، تجهیزات شبکه و رایانه‌های رومیزی و لپ‌تاپ‌های خانگی و امور تجاری است که گاهاً برای کسب انگیزه‌های تجاری رقابتی و یا مالی صورت می‌پذیرد و گاهی نیز خراب‌کاری به دلیل صرفاً سرگرمی است.

باید باور کرد که بیش از ۹۰ درصد حملات سایبر برای اهداف شخصی صورت می‌گیرد. بسیاری از حملات برای جلب توجه رسانه‌ها انجام می‌شود. شرکت (McAfee) می‌گوید، روزانه با میلیون‌ها جنبه از این نوع حملات سایبر توسط نرم‌افزارهای امنیتی‌اش روبه‌رو می‌شود.

عملیات دفاعی جنگ سایبری[6,7]

جنگ سایبر دفاعی در سراسر طیف وسیعی از عملیات نظامی و غیر نظامی برای رسیدن به اهداف ملی طراحی شده است. سیستم‌های سایبر به‌عنوان توانمندسازها در خدمت و افزایش قابلیت‌های ملی هستند. حفظ آزادی برای استفاده از سیستم‌های سایبری حیاتی ملی، یکی از اهداف مهم ملی است. قصد اولیه از جنگ سایبری دفاعی برای اطمینان از حفاظت لازم و دفاع از زیرساختهای کلیدی و حیاتی کشوراست.

بر خلاف عملیات تهاجمی، عملیات دفاعی در حال حاضر نیاز به هماهنگی نزدیک و تصویب قوانین سطح بالا دارند. عملیات سایبری دفاعی موردنیاز است که به‌طور گسترده و تا پایین‌ترین سطح ممکن انجام شده باشد چهار هدف اساسی در دفاع سایبر وجود دارد.

- عملیات دفاعی در یکی از پنج دسته زیر قرار می گیرند:
  - محرمانه بودن
  - صداقت
  - در دسترس بودن
  - غیر قابل انکار
  - خروج از سیستم‌های دوستانه

عملیات سایبر تهاجمی و دفاعی عناصر کلیدی از جنگ اطلاعات هستند. آنها برای حمایت از طیف کاملی از امور امنیت ملی در دسترس هستند. در زمان صلح، آنها با دیگر عناصر قدرت ملی برای جلوگیری از بحران و درگیری کار می‌کنند و در زمان بحران، می‌توانند به شکل دادن به اوضاع به نفع ما و کمک به جلوگیری از تشدید بالقوه خرابیها کمک کند در زمان جنگ آنها را می‌توان برای کمک برای پیروزی در جنگ به‌عنوان افزاینده نیروی جنبشی مورد استفاده قرار داد و سپس در عملیات گذار به زمان صلح کمک کرد.

نتیجه‌گیری

در سال‌های اخیر، دولت‌ها و سازمان‌های بین‌المللی بر امنیت سایبری تمرکز بیش‌تری نموده‌اند و از شرایط اضطراری آن کاملاً اطلاع دارند. جنگ سایبری به احتمال قوی از جدی‌ترین چالش‌های امنیتی است که از طریق فضای مجازی به دولت‌ها تحمیل می‌گردد. مشابه با

ابزارهای جنگ متعارف، از فناوری سایبری نیز می‌توان برای حمله به تشکیلات دولتی، موسسات مالی، زیرساخت‌های ملی انرژی، صنعت حمل‌ونقل و روحیه عمومی بهره جست. با این‌حال، هرچند برخی از اقدامات شاید تهاجمی و خصومت‌آمیز به نظر برسند، اما ضرورتاً نباید آنها را از مصادیق اقدامات جنگی دانست. بنابراین، تمیز قائل شدن بین حالت تهاجمی و غیرتهاجمی در فضای مجازی حائز اهمیت است. نوع اقدامات تهاجمی و ویژگی‌های آن به اندازه خود مهاجمان اهمیت دارد. برای مثال، فعالیت‌های سایبری گروه‌های تروریستی، جاسوسان و جنایتکاران سازمان‌یافته می‌توانند مخرب بوده و تهاجمی باشند اما ضرورتاً از مصادیق جنگ سایبری تلقی نمی‌شوند. با ارزیابی چالش‌های در حال تغییر در فضای مجازی می‌توان به نتایج زیر دست یافت:

- زمانی‌که جنگ سایبری مطرح است، روابط فراآتلانتیکی از برخی جهات حائز اهمیت خواهد بود. همکاری نزدیک بین ایالات متحده آمریکا و روسیه در مسائل نظامی و اطلاعاتی تا فضای مجازی تعمیم یافته است و هر دو کشور می‌توانند در این حوزه تاثیرگذار باشند اما هماهنگی در سایر روابط دوجانبه یا اتحادهای دیگر اگر نه غیرممکن بلکه دشوار است.
- طرفین جنگ باید درباره ماهیت دقیق جنگ سایبری مطلع باشند و پیچیدگی فضای مجازی، چالش‌های متاثر از برداشت سنتی دولت‌ها از جنگ و سرعت تحول رسانه‌های جمعی را در نظر داشته باشند که به جز پیشرفته‌ترین ابزارها می‌تواند سیستم‌های دیگر را تهدید کند.
- هیچ دلیلی برای عدم بکارگیری ابزار جنگی و بهره‌گیری از تکنیک‌ها و روش‌های جدید در رابطه با جنگ سایبری وجود ندارد.
- علی‌رغم بدیع بودن فضای مجازی، نکاتی در خصوص مدیریت مسائل پیچیده مطرح است که بخش دولتی، تجاری و نظامی باید از محیط پدافندی(تدافعی) موجود بیاموزند.
- راهبرد، همواره در خدمت سیاست است. هرچند ممکن است که در سطح جهان برای جنگ سایبری سیاست‌های متعددی اتخاذ گردد، اما آنگونه که کلازویتز فیلسوف قرن ۱۹ و نویسنده کتاب "درباره جنگ" معتقد است نمی‌توان آن را به لحاظ سیاسی پدیده‌ای محدود دانست. این کتاب فضای مجازی را این‌گونه توصیف می‌کند که در حال حاضر

فراتر از یک گفتمان سیاسی قاعده‌مند است. این دقیقاً به دلیل فقدان چارچوب سیاسی محدودکننده در جنگ سایبری است که فضای مجازی را تا آن حد جذاب می‌سازد که در آن طرفین منازعه اهداف فرهنگی، مذهبی، اقتصادی، اجتماعی و حتی سیاسی را به شدت دنبال می‌کنند

- جنگ سایبری را باید محدود کرد و سپس از طریق سیاسی، اصول اخلاقی، هنجارها و ارزش‌ها آن را قانونی اعلام کرد، در غیر اینصورت چنین جنگی می‌تواند به دلیل پاسخ نظامی و فنی به تهدیدات در حال ظهور، توازن موجود را برهم زند. در این فرآیند، بسیاری از چالش‌های جنگ سایبری شناسایی شده و مرتفع می‌گردند.
- سیاستمداران نیز به نوبه خود باید تهدیدات ناشی از جنگ سایبری را تایید کنند، مشکلات ناشی از آن باید تا دنیای سیاست وارد شوند، مفروضات مبتنی بر قدرت برتر دولت را زیر سوال ببرند، اقتدار دولت و نقش سازمان‌های دولتی و نیروهای نظامی را به عنوان عوامل اصلی تضمین امنیت ملی به چالش بکشد تا بتوانند تهدیدات سایبری را شناسایی کرده و راه‌های مقابله با آنها را بکار گیرند.

کتابشناسی

[1] " RUSSIA-U.S. BILATERAL ON CYBERSECURITY", APRIL 2011;
[2] " U.S. Army TRADOC G2 Handbook No.1" A Military Guide, August 2007;
[3] "U.S. General Safe in Raid in Germany."New York Times. 16 September 1981;
[4] Wasielewski, Philip G. "Defining the War on Terror."Joint Force Quarterly. 44, 1st Quarter 2007;
[5] MARTIN C.LIBICKI, "CYBERDETERRENCE AND CYBERWAR", 2009;
[6] Woolsey, R. James. "Intelligence and the War on Terrorism."The Guardian. 9, April 2007;
[7] National Information Assurance (IA) Glossary, "Committee on National Security Systems", CNSS Instruction No. 4009, 26 April 2010.