فصلنامه علوم و فنون نظامی/ سال هشتم/ شماره ۲۲، پاییز و زمستان ۱۳۹۰
صص ۸۷-۶۷

تاریخ دریافت مقاله: ۱۳۹۱/۰۶/۰۳
تاریخ پذیرش مقاله: ۱۳۹۱/۱۰/۱۰

بررسی نقش جنگ سایبری در عملیات مشترک و مرکب

محمدرضا اسماعیل‌زاده[۱]
مجید رجب‌پور[۲]

چکیده :

امروزه طراحان جنگی به خوبی می‌دانند که اجرای عملیات به صورت تک‌نیرویی و مبتنی بر یکی از عرصه‌های زمین، هوافضا و دریا پیامدی جز شکست و یا تحمل تلفات سنگین به دنبال نخواهد داشت. لذا طرحریزی و اجرای عملیات‌ها غالباً به صورت مشترک و با مشارکت عناصری از هر یک از عرصه‌های پیش‌گفته انجام می‌شود. بکارگیری مشترک عرصه-های سنتی موجب تقویت قدرت سخت در میدان نبرد شده در حالی که بخش قابل توجهی از توان رزمی دشمن را روحیه، احساسات و انگیزه نیروی انسانی تشکیل می‌دهد که بایستی به وسیله قدرت نرم مستهلک گردد. فرماندهان عملیات‌های مشترک با الحاق فضای سایبر به عنوان بعد پنجم میدان نبرد به عرصه‌های سنتی، از قدرت نرم و سخت جنگ سایبری بهره برده و با ترکیب آن به آلیاژی جدید به نام قدرت هوشمند دست یافته‌اند. شاخصه‌های منحصر بفرد عرصه سایبری موجب پراکندگی قدرت شده و میل به جنگ ناهمطراز را به شدت نزد بازیگران دولتی و غیر دولتی افزایش داده و قدرت‌های نظامی بزرگ را با چالش مواجه کرده است. آنها با گسترش پیمان‌های نظامی قبلی خود مثل ناتو و یا ایجاد پیمان‌های جدید بین. المللی ، بناچار عملیات‌های مرکب را برای دستیابی به اشراف نسبی در این عرصه طراحی و اجرا می نمایند.

کلید واژه‌ها:

عملیات مشترک و مرکب، جنگ سایبری، فرماندهی مخصوص، جنگ ناهمطراز، قدرت هوشمند

۱- کارشناسی ارشد مدیریت دفاعی mreb2009@gmail.com
۲- عضو هیئت علمی دافوس آجا

مقدمه

عصر حاضر شاهد شکل‌گیری فضایی است که اغلب فعالیت‌ها و خدمات بخش‌های دولتی و غیر دولتی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات بانکی و مالی، تجارت، ارتباطات، صنایع دفاعی، سلامت و انرژی مبتنی بر زیرساخت‌های الکترونیکی و مجازی است. توسعه روز افزون فن‌آوری ارتباطات و اطلاعات موجب پیدایش شبکه‌های پیچیده‌ای شده که فضای تبادل اطلاعات (فتا) را تشکیل داده و به فضای مجازی[1] یا فضای سایبری[2] تعبیر می شود.

گسترش و نفوذ این فضا اغلب فعالیت‌ها را با تغییرات شگرفی روبرو کرده است. ارتش‌ها نیز از این قاعده مستثنی نبوده و به منظور بهره‌گیری بیشتر از خدمات فضای سایبر به سمت الکترونیکی شدن پیش رفته و امور عملیاتی، اطلاعاتی، اداری و لجستیکی خود را بر روی زیرساخت‌های این بستر بنا کرده‌اند. این تحولات به قدری زیاد بوده که از آن به «انقلاب در تلاش‌های نظامی [3] یاد می‌شود. این تحولات موجب پیدایش فرصت‌ها و چالش‌های جدید پیش روی بازیگران دولتی و غیردولتی شده و زمینه خلق مفاهیمی چون جنگ سایبری[4]، تروریسم سایبری[5]، جرائم سایبری[6]، قدرت سایبری[7]، جاسوسی سایبری[8] و غیره را پدید آورده است.

بررسی جنگ‌های قرن اخیر نشان می‌دهد که طراحان عملیات‌های نظامی از تمام ظرفیت‌های میادین نبرد حقیقی شامل هوا، فضا، زمین و دریا برای برای نیل به پیروزی و تحمیل خسارت سنگین به طرف مقابل استفاده کرده‌اند. آنها به منظور استفاده از سه اصل وحدت فرماندهی، تمرکز و صرفه‌جوئی در قوا کلیه نیروها را تحت هدایت و رهبری یک فرماندهی مشترک قرار می‌دهند. اما آنچه در دهه اخیر توجه فرماندهان نظامی را به خود جلب کرده، استفاده از ظرفیت‌های منحصر بفرد عرصه سایبری است که خلاف عرصه‌های سنتی ماهیتی مجازی دارد. میدان جنگ سایبری قبل، حین و یا بعد از نبرد حقیقی به فعالیت خود ادامه داده و به عنوان بعد پنجم میدان نبرد پس از عرصه‌های سنتی همواره به عنوان مکمل میدان نبرد حقیقی برای فرماندهان بوده است حتی در برخی موارد که ورود به جنگ حقیقی به دلایلی امکان پذیر نیست این نوع جنگ می‌تواند اثرات سخت نیز از خود به جای گذاشته و به تنهایی پتانسیل یک میدان نبرد واقعی را داشته باشد. فرماندهان

1 - Virtual Space
2 - Cyberspace
3 - Revolution in Military Affairs (RMA)
4 - Cyber War
5 - Cyber Terrorism
6 - Cyber Crime
7 - Cyber Power
8 - Cyber Espionage

عملیات مشترک با بکارگیری عنصر سایبری در کنار دیگر عناصر میدان رزم، سبک‌های نوینی در نحوه جنگیدن خلق کرده‌اند.

ارتش‌ها با سلاح نرم‌افزار در حال ساختن برج و باروهای دفاعی خود در حوزه سایبر هستند تا نوعی از "بازدارندگی" را در برابر دشمن به نمایش بگذارند. کنترل و هدایت پتانسیل‌های بالقوه این عرصه و در صورت نیاز به فعلیت در آوردن آن سبب در اختیار گرفتن نیروی فوق‌العاده‌ای می‌گردد که به سادگی موازنه قوا را به نفع یکی از طرفین تغییر می‌دهد. به همین دلیل این نوع جنگ از اقبال خوبی در بین تمامی کشورها برخوردار است. کشورهای توسعه یافته که متولی زیر ساخت های فن‌آوری هستند به راحتی می توانند از چالش ها و فرصت های آن استفاده کرده و دیگر کشورها را با خسارات احتمالی روبرو کنند، از طرف دیگر کشورهای در حال توسعه نیز با آگاهی از آسیب پذیر بودن کشورهای گروه اول به دلیل وابستگی شدید آنها به این فضا ، فرصت خوبی برای جبران موازنه قوا به دست‌آورده‌اند.

تایید این مطلب این‌گونه در سند"استراتژی وزارت دفاع آمریکا در فضای مجازی" آمده-است: "موانع اندک برای ورود فعالیت‌های بدخواهانه به فضای مجازی از جمله دسترسی گسترده به ابزارهای هک کردن، نشان می‌دهد که یک فرد یا گروه کوچکی از بازیگران به طور بالقوه توانایی ایجاد آسیب جدی بر امنیت اقتصادی و ملی آمریکا و وزارت دفاع دارند. این فناوری‌ها با مقیاس کوچک می‌توانند تاثیر نامتقارنی نسبت به اندازه‌شان ایجاد کنند. دشمنان بالقوه مجبور نیستند سامانه‌های تسلیحاتی گران قیمتی داشته باشند تا بتوانند تهدید بزرگی بر علیه امنیت ملی آمریکا اعمال کنند". (مجازی, ۱۳۹۰, ص. ۴)

ارتش‌ها برای آفند و پدافند در این فضا، از کلیه نیروهای دیجیتالی خود که در نیروهای مختلف حضور دارند استفاده کرده و در قالب فرماندهی مشترک، وحدت تلاش و فرماندهی را در این حوزه فراهم کرده‌اند تا در موقع لزوم با اجرای عملیات مشترک قادر به پاسخگویی به موقع و مناسب باشند. همچنین به دلیل گستردگی میدان نبرد در این حوزه، انتظار می-رود که کشورها به دنبال ایجاد پیمان‌های نظامی بین‌المللی بوده تا بتوانند در قالب عملیاتی مرکب پاسخگوی نیازهای خود در فضای سایبر باشند. چنانکه ایالات متحده، استرالیا، کانادا، انگلستان و ناتو، تحت طرح جامع امنیت سایبری ملی همکاری خود را از ماه می ۲۰۱۱ آغاز کرده است. (http://www.defense.gov/news/newsarticle.aspx?id=64, 2011)

مبانی و مفاهیم نظری

فرماندهی مخصوص

فرماندهی مخصوص نوعی از فرماندهی است با ماموریت کلی و مداوم که معمولا از یگان‌های یک نیروی مسلح تشکیل می‌گردد. این فرماندهی ممکن است برای یک منظور و مدت زمان معین شامل یگان‌های ستادی از سایر نیروهای مسلح باشد. این نوع فرماندهی بنا بر پیشنهاد فرمانده کل ارتش و تصویب فرماندهی معظم کل قوا تشکیل می‌گردد. هرگاه یک ماموریت کلی و مداوم که اجرای آن مستلزم شرکت یگان‌های یک نیروی مسلح در یک منطقه بوده و لزوم هدایت راهبردی واحدی را ایجاب نماید وجود داشته باشد این فرماندهی تشکیل می‌گردد. منظور از تشکیل این نوع فرماندهی اطمینان از آزادی عمل بیشتر است.(نیازی، فرج پور، توکلی، ۱۳۹۰:۱۶)

نیروی مشترک

به نیروئی اطلاق می‌گردد که از عناصر قابل ملاحظه دو نیرو یا بیشتر از نیروهای مسلح (زمینی، هوائی، دریائی و قرارگاه پدافند هوائی) یک کشور تشکیل یافته باشد و تحت نظر فرماندهی مشترک واحد که مجاز به اعمال فرماندهی عملیاتی و یا کنترل عملیاتی است عمل خواهد نمود. (همان:۹)

نیروی مرکب[1]

نیروی مرکب نیروئی است که از عناصر عمده نیروهای مسلح دو یا چند کشور تشکیل و تحت اختیار یک فرمانده به منظور ایجاد فرماندهی مرکب قرار داده می‌شود. به عبارتی دلالت بر حضور و ترکیب نیروهای چندین کشور یا ملت از قبیل نیروهای متفق[2]، نیروهای متحد[3]، نیروهای ائتلاف[4] و نیروهای چند ملیتی[5] می‌نماید. .(همان:۷۷)

عملیات مشترک و مرکب: عملیاتی که توسط نیروی مشترک و یا مرکب انجام می‌شود.

سایبر و فضای سایبر[6]: مفهوم سایبر و فضای سایبر برای اولین بار در سال ۱۹۸۴ توسط داستان داستان نویسی به نام ویلیام گیبسون در یک داستان علمی- تخیلی بکار گرفته شد. در واقع به هر آنچه که مرتبط با شبکه‌های رایانه‌ای و فعالیت‌های رایانه‌ای و مجازی باشد سایبر اطلاق می‌شود به علاوه برای معرفی گونه‌ی برخط، مجازی یا رایانه‌ای هر چیزی نیز می‌تواند بکار رود. (شریف، ۱۳۸۴ : ۱۳)

1- Combined Force
2- Allied Forces
3- Unified Forces
4- Coalition Forces
5- Multinational Forces
6- Cyberspace

وزارت دفاع امریکا فضای سایبر را مجموعه ای از شبکه‌های به هم وابسته زیر ساخت-های فن‌آوری اطلاعات شامل اینترنت، شبکه‌های مخابراتی و رایانه‌ای، پردازشگرها و کنترلرهای جاسازی شده در این شبکه می‌داند. در این فضا الکترونیک و طیف الکترومغناطیس به منظور ذخیره‌سازی، اصلاح و تغییر داده‌ها از طریق سامانه‌های شبکه‌ای استفاده می‌شوند. (Andress, 2011, p. 2)

جنگ اطلاعات[1] و جنگ سایبر[2]

جنگ اطلاعات بخشی از عملیات اطلاعاتی است و شامل هر فعالیت نظامی که در زمان جنگ اتفاق بیافتد و در محیط اطلاعاتی انجام شود می‌گردد. نگرانی از حملات کشورهای خارجی و جنگ اطلاعات به قدری زیاد است که حتی کشوری مثل آمریکا را ، که خود در فن‌آوری اطلاعات حرف اول را می زند نیز به چاره اندیشی وادار کرده است(حسن بیگی، ۱۳۸۸ : ۱۰۵) .

تعاریف زیادی در مورد جنگ سایبر و جنگ اطلاعات توسط کارشناسان نظامی و غیرنظامی انجام شده لیکن آنچه بیشتر در این مقاله مورد توجه است تعاریفی است که متخصصین وزارت دفاع آمریکا به طور رسمی در اواخر دهه ۱۹۹۰ منتشر کردند. در این تعاریف جنگ اطلاعات عبارت است از:

"اقدامات اتخاذ شده برای تحقق برتری اطلاعاتی که از طریق تاثیرگذاری بر اطلاعات و سامانه‌های اطلاعاتی دشمن، که از راهبرد ملی نظامی پشتیبانی کرده و در عین حال اطلاعات و سامانه‌های خودی را ارتقاء بخشیده و از آنها دفاع می‌کند".

در تعریف دیگری دانشگاه دفاع ملی ایالات متحده آمریکا، ضمن تاکید بر نقش فن‌آوری پیشرفته اطلاعات، بازیگران این عرصه جنگی را فقط نظامیان دانسته و می‌گوید: "جنگ اطلاعات یعنی کاربرد اطلاعات و سامانه‌های اطلاعاتی به عنوان یک سلاح در درگیری‌هائی که اطلاعات و سامانه‌های اطلاعاتی یک هدف نظامی مهم به شمار می روند."

مارتین لیبیکی[3] ضمن وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل مختلف جنگ اطلاعاتی را به شرح زیر نام می برد:

۱. **جنگ فرماندهی و کنترل**[4]: هدف آن تقابل با رهبری و هدایت جنگ و همچنین ارتباطات است.

1-Information warfare(IW)

2- Cyber warfare

۳ – اقتصاددان و مولف کتاب "اشراف بر فضای سایبر: جنگ اطلاعات و امنیت ملی

4– Command and Control Warfare (C2W)

۲. **جنگ برپایه اطلاعات نظامی**: عملیات‌هائی است بر ضد حساسه‌های جمع‌آوری اطلاعات نظامی.
۳. **جنگ الکترونیک**[1]: در برابر حساسه‌هائی مثل رادار و سامانه‌های ارتباطی صورت می-پذیرد تا ضمن اخلال در آنها در صورت لزوم شنود، فریب، تزریق توان بیش از حد (اُورپاورینگ) ، سمت یابی[2] و موقعیت‌یابی[3] نیز انجام شود.
۴. **عملیات روانی**[4]: هدف آن رهبری، جامعه، نیروهای دشمن و منازعات فرهنگی است. در این جنگ از اطلاعات برای تغییر ذهنیت و طرز فکر دوستان، بی‌طرف‌ها، و دشمنان استفاده می‌شود.
۵. **جنگ هکرها**: به عملیات در شبکه‌های رایانه‌ای شناخته می‌شود.
۶. جنگ اطلاعات اقتصادی: ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.
۷. **جنگ سایبر**: ترکیبی از همه موارد شش گانه بالا. (شریف، ۱۳۸۴: ۲۱)

در حقیقت مارتین لیبیکی جنگ سایبر را مترادف جنگ اطلاعات دانسته است. البته در تعاریف دیگری که از جنگ سایبر شده نیز می‌توان تائید این مطلب را دید. به طور مثال ریموند پارکز و دیوید دوگان از پژوهشگاه ملی ساندیا در نیومکزیکو در تعریف جنگ سایبر می‌نویسند: "جنگ سایبر زیرمجموعه جنگ اطلاعاتی بوده و شامل اقداماتی است که در دنیای سایبر رخ می‌دهند. دنیای سایبر هرگونه واقعیت مجازی است که توسط مجموعه رایانه‌ها و شبکه‌ها ایجاد می‌شود. در بین فضاهای سایبر متعدد و مختلف، اینترنت و شبکه-های مرتبطی که حاوی مطالب چندرسانه‌ای هستند، بیشترین ارتباط را با جنگ سایبر دارند". (شریف، ۱۳۸۴:۲۳)

قدرت سایبری

برای بهره‌گیری از قدرت سایبری ابتدا بایستی مفهوم آن را شناخت تا در ادامه بتوان راه‌کارهای نیل به این قدرت را بررسی و پیاده‌سازی کرد. قدرت سایبری نیز همانند دیگر مفاهیم ناشی شده از این فضا دارای تعریف واحدی نیست و نظریه پردازان بسیاری در این خصوص سخن گفته‌اند. یکی از معروف‌ترین این نظریه پردازان، جوزف‌اس‌نای[5]، استاد برجسته دانشگاه هاروارد است که در مقاله‌ای تحت عنوان "قدرت سایبری" برگرفته از

1- Electronic warfare
2 - Direction finding
3 -Position finding
4 - Psychological operations
5 - Joseph S. Nye

کتاب خود او به نام "آینده قدرت در قرن۲۱"[1]، ضمن تعریف مفهوم فضای سایبر به تشریح ویژگی های این قدرت در جهان امروزی پرداخته و می‌گوید :

قدرت سایبری توانایی کسب نتایج مطلوب با استفاده از منابع اطلاعاتی الکترونیکی در حوزه سایبری است .یا به عبارتی توانایی استفاده از فضای سایبر برای خلق مزیت‌ها و تاثیر بر رویدادهای محیط‌های عملیاتی دیگر و ابزارهای قدرتe است. قدرت سایبری می‌تواند برای حصول به نتایج مطلوب در داخل فضای سایبر استفاده شود، یا می‌تواند از ابزارهای سایبری برای کسب نتیجه مطلوب در حوزه‌های دیگر خارج از آن استفاده کند. (Joseph S. Nye, 2010, p. 8)

در فضای سایبر شواهدی از رفتار قدرت سخت و نرم[2] را می‌توان در تمامی جنبه‌ها یافت. اولین روی قدرت، قابلیت یک بازیگر برای وادار کردن دیگران به انجام چیزهایی بر خلاف سلیقه یا راهبردهای اصلی خودشان است. در زمینه قدرت نرم، یک فرد یا سازمان ممکن است تلاش نماید تا دیگران را متقاعد سازدکه رفتارشان را تغییر دهند. همچنین اطلاعات سایبری می‌توانند به یک منبع قدرت سخت تبدیل شوند، که می‌تواند به اهداف فیزیکی در یک کشور دیگر صدمه وارد کند. برای مثال، بیشتر صنایع مدرن و خدمات دولتی فرایندهایی دارند که توسط رایانه‌های متصل به سامانه‌های کنترل نظارتی و جمع‌آوری داده‌ها[3]، پردازش می‌شوند. نرم‌افزار مخربی که به این سیستم‌ها وارد می‌شود، می‌تواند برای خاموش کردن فرایندی که آثار کاملا فیزیکی دارد برنامه‌ریزی شده باشد. (همان :۱۱)

وی در ادامه ضمن تشریح زمینه‌های بوجود آمدن قدرت به ویژگی‌های دیگر این فضا اشاره کرده و می‌گوید: قدرت در زمینه معنا می‌یابد، و رشد سریع فضای سایبر زمینه‌ای جدید و مهم در سیاست جهان است. گمنامی[4]، هزینه پایین ورود[5]، نامتقارن بودن در آسیب‌پذیری[6] و گسترش و نفوذ این فضا باعث شده که بازیگران کوچکتر در فضای سایبر نسبت به حوزه‌های سنتی‌تر سیاست جهانی ظرفیت بیشتری برای اعمال قدرت سخت و نرم دارند. تغییرات بوجود آمده در اطلاعات همیشه تاثیر مهمی بر قدرت داشته‌اند، اما حوزه سایبر یک محیط مصنوعی جدید و غیرقابل پیش‌بینی است. ویژگی‌های فضای سایبر برخی از اختلافات قدرت بین بازیگران را کاهش داده و بدین ترتیب مثال خوبی از پراکندگی قدرت را که ویژگی سیاست جهانی در قرن حاضر است، به نمایش می‌گذارد. قدرت‌های بزرگ نخواهند توانست به اندازه حوزه‌هایی چون دریا و خشکی بر این حوزه مسلط شوند.

1- The Future of Power in the 21st Century
2- hard and soft power behavior
3 - Supervisory Control and Data Acquisition (SCADA)
4 - Anonymous
5 - Low cost of investment for entry
6 - Asymmetrical vulnerability

انتقال قدرت از یک کشور برتر به کشور دیگر یک رویداد تاریخی آشناست، اما پراکندگی قدرت روندی جدید است. مشکل تمامی کشورها در عصر اطلاعات جهانی امروز این است که چیزهای بیشتری خارج از کنترل قدرتمندترین کشورها حادث می‌شوند. به قول یکی از مدیران سابق برنامه‌ریزی سیاسی وزارت خارجه آمریکا، "گسترش سریع اطلاعات به اندازه گسترش تسلیحات به غیر قطبی شدن جهان کمک می‌کند ". (Joseph S. Nye, 2010, p. 1)

راهبردهای ایالات متحده در فضای سایبر

اشراف اطلاعاتی در آتی حتی برای صاحبان فناوری وجود نخواهد داشت زیرا که هیچ کس درک کاملی از محیط نداشته و نخواهد توانست جریان پیوسته و عظیم اطلاعاتی را که در چنین محیطی در حرکت است کنترل کند. از جمله تاثیرات اجتماعی کلیدی فناوری در آینده بی تاثیر نمودن هر گونه تلاش برای ایجاد کنترل متمرکز بر آنهاست. (حسن پور, ۱۳۸۸ : ۹۲).

عدم کنترل و تمرکز بر جریان اطلاعات در فضای سایبر موجب توزیع و پراکندگی قدرت شده و در نتیجه از اشراف اطلاعاتی قدرت‌های سلطه‌جو کاسته است. ایالات متحده سعی دارد که اشراف اطلاعاتی خود را تا حد امکان افزایش و یا دست کم در سطح گذشته حفظ نماید. در این راستا با تدوین "اولین سند راهبرد برای عملیات در فضای سایبر"[1] و"اولویت-های دفاعی امریکا در قرن۲۱"[2] راهبردهای جدید نظامی خود را برای بهره‌گیری از ظرفیت‌های نهفته در این فضا رونمائی کرده است. شایان ذکر است که در اولین سند منحصراً به فضای سایبر پرداخته شده و در سند دوم که راهبردهای دفاعی کلی در قرن جاری را بررسی می‌کند چندین مرتبه بر عملیات موثر در فضای سایبر تاکید شده است. بررسی بخش‌هایی از این دو سند می‌تواند به عنوان چراغ راهی برای دستیابی به رهیافت راهبردی در این فضا مد نظر باشد.

در اولین سند که بخش‌هائی از آن توسط معاون وزیر دفاع -ویلیام جی لین[3] منتشر شد آمده است که: اولین استراتژی وزارت دفاع برای عملیات در فضای سایبری، دفاع از کشور در برابر حملات شبکه‌ای است که به صورت بالقوه ویرانگر هستند. ما به صورت دقیق نحوه شکل گیری فضای مجازی در اجرای یک مأموریت و یا سناریوهایی که از آن بر می‌خیزد را نمی‌دانیم اما محوریت فناوری اطلاعات و وابستگی عملیات‌های نظامی و جامعه ما عملا این موضوع را تضمین می‌کند که از طرف دشمنان در آینده مورد هدف قرار

1- First Strategy for Operating in Cyberspace , By Cheryl Pellerin , American Forces Press Service(Jul,14,2011)
2 -Priorities For 21th Century Defense(Jun,3,2012)
3 -William J. Lynn III, Deputy Defense Secretary

خواهیم گرفت. تحلیل ما بر این است که حملات سایبری سهم ویژه‌ای از درگیری‌های آینده را خواهند داشت. وجود ابزارهایی که شبکه های حیاتی را مختل، تخریب و منجر به آسیب فیزیکی و یا باعث تغییر در عملکرد سامانه‌های کلیدی شوند، نشانه یک تغییر استراتژیک در تهدیدات مجازی در حال تکامل است. به عنوان نتیجه ای از این تهدید، فشردن کلیدی در یک کشور، می‌تواند در یک چشم به هم زدن نقطه دیگری در آن سوی جهان را تحت تاثیر قرار دهد. در قرن ۲۱، هر بیت و بایت می‌تواند به اندازه گلوله و بمبی خطرناک باشد. یک عنصر مهم در استراتژی این است که یک حمله را دفع و یا به حداقل درجه خطر رساند. اگر بتوان تاثیر حملات را بر عملیات‌های خودی به حداقل رسانده و حتی آن‌ها را به سرعت به نفع خود تغییر داد، در آنصورت می‌توان محاسبات حمله کننده را برریخت. سایر عناصر و ارکان این راهبرد عبارتند از:

۱. فضای مجازی را یک صحنه نبرد همانند هوا، زمین، دریا و فضا تلقی کرده و حفاظت از شبکه‌ها، آموزش و تجهیز نیروهایی برای مأموریت‌های مجازی را راه اندازی کنیم.
۲. معرفی مفاهیم جدید بر روی بخش‌های شبکه‌ای، از جمله حفاظت‌های فعال مجازی، استفاده از سنسورها، نرم افزار و امضاء برای جلوگیری از کدهای مخرب، قبل از اینکه بر روی عملیات تأثیری بگذارند.
۳. همکاری با سازمان امنیت ملی و بخش خصوصی برای محافظت از زیرساخت‌های حیاتی ملی مانند شبکه برق، سیستم حمل و نقل و بخش مالی.
۴. ساخت سیستم‌های دفاعی تجمعی مجازی با کمک متحدان و شرکای بین‌المللی، برای گسترش آگاهی از فعالیت‌های مخرب و کمک به دفاع در برابر حملات.
۵. ایجاد تغییرات اساسی در چشم انداز فناوری امنیت سایبری، مخصوصاً به وسیله افزایش امنیت شبکه. (http://www.defense.gov/news/newsarticle.aspx?id=64686)

این نکته حائز اهمیت است که ایالات متحده علاوه بر تدوین راهبرد، ایجاد ساختاری مناسب، ائتلاف بین‌المللی و سرمایه‌گذاری در تحقیق و توسعه امنیت شبکه را به صورت توام راه‌کار برون رفت از چالش‌های این فضا می‌داند. به همین دلیل در ماه می سال ۲۰۱۰، فرماندهی سایبری ایالات متحده به منظور تمرکز عملیات‌ها و حفاظت از شبکه‌ها ایجاد می‌گردد. همچنین ایالات متحده همکاری خود را با استرالیا، کانادا، انگلستان و ناتو، تحت طرح جامع امنیت سایبری ملی رئیس جمهور باراک اوباما آغاز کرده و در ماه‌های آینده نیز این همکاری با سایر ملل افزایش خواهد یافت. همچنین نیم میلیارد دلار در زمینه تحقیق و توسعه در جهت سرعت بخشیدن به تحقیق بر روی فناوری‌های دفاعی پیشرفته، سرمایه گذاری کرده است. (http://www.defense.gov/news/newsarticle.aspx?id=64686)

وی در ادامه سخنان خود به روشنی نگرانی ایالات متحده اشاره کرده و می‌گوید: در حال حاضر گسترش زیرساخت‌های حیاتی نظامی به شرکت‌های خصوصی که ساخت تجهیزات و فناوری‌های مورد نیاز وزارت دفاع را بر عهده دارند بستگی دارد. این یک نگرانی قابل توجه است که در طول یک دهه گذشته، چندین ترابایت از اطلاعات شبکه‌های همکار با وزارت دفاع توسط مزاحمان خارجی ربوده شده است. فقط در یک حمله صورت گرفته در ماه مارس سال ۲۰۱۰، ۲۴۰۰۰ فایل دزدیده شده است. وی ادامه داد: محدوده داده‌های به سرقت رفته از مشخصات قطعات کوچک یک تانک، هواپیما و یا زیر دریایی تا ارتباطات هوایی هواپیماها، فناوری‌های نظارتی، سامانه‌های ارتباطی ماهواره‌ای و پروتکل‌های امنیتی شبکه است. اقدامات کنونی نیز هنوز نتوانسته‌اند به صورت کامل جلوی خروج این اطلاعات حساس را بگیرند. ما باید بیشتر برای حفاظت از ذخیره‌سازهای دیجیتالی که نوآوری‌های طراحی‌هایمان را در بر دارند تلاش کنیم.
(http://www.defense.gov/news/newsarticle.aspx?id=64686)

در سند "اولویت های دفاعی آمریکا در قرن۲۱" نیز نگاه ویژه‌ای به فضای سایبر و چالش‌های بر آمده از آن شده است. در این سند تاکید شده که افراد دولتی و غیر دولتی توانمندی و قصد هدایت جاسوسی سایبری و حمله سایبری را به صورت بالقوه بر روی ایالات متحده دارند که اثر شدیدی بر روی هر دو بخش عملیات های نظامی و مشتریان خانگی خواهد داشت. بنابراین به منظور جلوگیری از دستیابی دشمنان بالقوه به اهداف خود، ایالات متحده باید توانایی خود را در مناطقی که دسترسی و آزادی عمل او را به چالش کشیده حفظ کند. در این مناطق، دشمنان خبره از قابلیت های نامتقارن الکترونیک و جنگ سایبری، بالستیک و موشک‌های کروز، دفاع هوایی پیشرفته، مین‌های دریایی و روش‌های دیگر که باعث پیچیده‌تر شدن محاسبات عملیاتی می شود استفاده می‌کنند. کشورهایی مانند چین و ایران اهداف نامتقارن خود را در حالی که سلاح‌ها و فن‌آوری پیچیده خود را گسترش می‌دهند همچنان پیگیری خواهند کرد تا با قابلیت‌های طرح ریزی قدرت ما مقابله نمایند. (DOD, 2012, p. 10)

آنها به خوبی دریافته‌اند که دیگر کشورها فضای سایبری را در جهت اعمال قدرت نرم و سخت خود بکار خواهند گرفت و آنها به ناچار بایستی برای مقابله با این تهدیدات جدید تغییراتی در ساختار و ترکیب نیروهای خود به‌وجود آورند. در این سند این تغییرات به روشنی اشاره شده و اذعان شده که جنگ‌های امروزی به تغییر وضعیت در ساختارهای فعلی نیروهای مسلح منجر شده است. به نحوی که این نیروها در مقابل طیف وسیعی از اتفاقات آینده بایستی سریع، قابل انعطاف و آماده باشند. ما بویژه در دستیابی به اطلاعات نظامی، نظارت و شناسایی، مبارزه با تروریسم، مبارزه با سلاح‌های کشتار جمعی و توفق بر فضای سایبر که توانمندی‌های حیاتی را برای دستیابی به پیروزی در آینده در اختیار ما

قرار می‌دهند، سرمایه‌گذاری خود را ادامه خواهیم داد. پیش بینی ما با توجه به برنامه‌ریزی-ها این است که در آینده نیروهایی خواهیم داشت که با هدایت و بکارگیری سلاح‌های ترکیبی در صحنه نبرد زمینی، هوایی، دریایی و فضای سایبر به طور کامل اهداف تهاجمی بر علیه ما را در یک منطقه کاملاً از بین ببرند. (همان ص.۱۰)

ایالات متحده ضمن پذیرش اینکه امروزه سامانه‌های فضایی و زیر ساخت‌های پشتیبانی آنها با تهدیدات زیادی همچون کاهش، از هم گسیختگی و تخریب مواجه هستند بر این نکته نیز تاکید دارد که نیروهای مسلح قادر نیستند عملیات‌های خود را بدون شبکه‌های اطلاعاتی و ارتباطی مدرن و مطمئن به طور موثر در فضای سایبر هدایت نمایند. بر این اساس راه‌کار اتخاذ شده برای وزارت دفاع ادامه همکاری و سرمایه‌گذاری با متحدان بین-المللی و شرکاء داخلی است تا به توانمندی‌های پیشرفته‌تر برای حفظ شبکه‌ها، مقدورات عملیاتی و قابلیت انعطاف در فضای سایبر دست یابد. (DOD, 2012, p. 11)

برای پیاده‌سازی و اجرای موارد عنوان شده در راهبردهای بالا، ایجاد ساختاری که بتواند ضمن آفند، تهدیدات ناشی از این فضا را نیز کاهش دهد ضروری به نظر می‌رسد به همین دلیل اینک آژانس امنیت ملی آمریکا "فرماندهی سایبر[1]" از نوع فرماندهی مشترک را ایجاد و همه واحدهای فعال جنگ‌های دیجیتالی در نیروهای نظامی آمریکا (زمین، دریا، هوا و فضا) تابع آن شده‌اند.فرماندهی سایبری آمریکا ماموریت برنامه‌ریزی، هماهنگ‌سازی، ادغام، همگام‌سازی و انجام فعالیت‌هایی خاص را بر عهده دارد. این فرماندهی ضمن هدایت عملیات‌ها و دفاع از شبکه‌های اطلاعاتی ویژه وزارت دفاع، برنامه‌ریزی و مقدمات لازم را برای عملیات‌های سایبری نظامی همه جانبه به منظور توانمندسازی نیروهای آمریکایی در تمام حوزه‌ها به انجام می‌رساند. این فرماندهی آزادی عمل نیروهای آمریکایی و متحدین این کشور را در فضای سایبری تضمین نموده و متقابلاً دشمن را از این توانایی محروم می-کند. ترکیب نیرویی قرارگاه سایبری از نیروی هوایی بیست‌وچهارم ارتش آمریکا[2]، فرماندهی سایبری نیروی زمینی[3]، قرارگاه سایبری ناوگان دریایی[4] و قرارگاه سایبری نیروی تفنگداران دریایی[5] تشکیل شده است. (Thomas K. Andersen,2011,p.29)

1 - USCYBERCOM
2 24th Air Force (AFCYBER)
3 - Army Forces Cyber Command (ARCYBER)
4 - Fleet Cyber Command (FLTCYBERCOM)
5 - Marine Forces Cyber Command (MARFORCYBER)

مصادیق جنگ سایبری

بررسی حملات سایبری که در چند سال گذشته به وقوع پیوسته می‌تواند برای تبیین بهتر نقش جنگ سایبری در عملیات‌های نظامی مفید باشد به ویژه اینکه اغلب این حملات با عملیات مشترک و مرکب نیز همراه بوده است.

۱. **جنگ کوزوو**: در این جنگ یکی از بارزترین حملات سایبری در عملیاتی مرکب توسط نیروهای ناتو بر علیه صرب‌ها انجام شد. در این جنگ عملیات سرکوب پدافند هوایی[1] نیروهای صرب تقریبا به طور کامل انجام و برتری هوایی[2] توسط ناتوکسب گردید. نیروهای صرب نتوانستند از موشک‌های زمین به هوا[3] که در اختیار داشتند استفاده کنند. کنند. علت این امر در گزارشی که بعدها ژنرال جامپر فرمانده نیروی رزمی نیروی هوایی آمریکا داد مشخص شد که حکایت از هدایت عملیات اطلاعاتی به وسیله تزریق ویروس و ارتباطات فریبنده به سامانه‌های رایانه‌ای و شبکه مایکروویو دشمن داشت. هر چند بعید است که اپراتورهای آمریکائی قادر به وارد کردن کدهای مخرب[4] به رادارهای موشک-های زمین به هوا باشند لیکن وی بعدا تایید کرد که نیروهای متفق از ابتدا قصد استفاده از نبردی تهاجمی بر علیه رایانه‌ها و پدافند هوایی دشمن را ، همانند یک جنگ‌افزار دقیق در طی عملیات‌های اطلاعاتی توسط نیروهای آمریکایی داشته اند.وی گفت ما جنگ اطلاعاتی بیشتری نسبت به نبردهای قبلی انجام دادیم و ما این پتاسیل را اثبات کردیم. ژنرال جامپر اضافه کرد اگرچه اطلاعات بیشتری در این زمینه وجود دارد که به علت طبقه بندی بالا قادر به گفتن آنها به کمتر کسی است لیکن تجربه جنگ کوزوو به ما پیشنهاد می‌کند که "به جای نشستن و صحبت کردن در رابطه با پادهای برهم زننده الکترون‌ها، بایستی درباره دستکاری الکترونی میکروچیپ‌هایی صحبت کنیم که قلب و روح سامانه‌های SA-10, SA-12 هستند تا بگوییم این یک یخچال است نه یک رادار-. چنین تلاش‌های پیشگامانه آفندی با استفاده از جنگ‌های سایبری کاهش بهره‌گیری دشمن از سامانه‌های زمین به هوا و دیگر سامانه‌های پدافندی را به دنبال خواهد داشت و دیگر نیازی به یک اقدام ضربتی با موشکهای ضدرادار پرسرعت[5] برای خنثی کردن پدافند پدافند هوائی نیست. (Lambeth , 2000, p. 112)

۲. **عملیات گلوله سربی**[6]: در سال ۲۰۰۸ بدترین نفوذ در تاریخ آمریکا به رایانه‌های محتوی اطلاعات طبقه‌بندی شده نظامی پنتاگون توسط کرم Agent.btz رخ داد . حمله زمانی

1 - SEAD
2 - Air Superiority
3 - SAM
4 - Malicious Code
5 -High-speed Anti-Radiation Missile
6 - Operation Buckshot Yankee

آغاز شد که یک حافظه فلش حاوی کدهای مخرب که توسط یکی از آژانس‌های اطلاعاتی بیگانه تولید شده بود از طریق درگاه USB به یک لپ‌تاپ در یکی از پایگاه‌های نظامی در خاور میانه متصل و بلافاصله از این طریق خود را بر روی شبکه رایانه‌ای کنترل فرماندهی وزارت دفاع آمریکا بارگذاری کرد. این کرم پس از اسکن پورت ها، درب پنهانی[1] را باز و سپس کنترل سرور مرکزی را از راه دور به عهده می گرفت. این حمله تنها یک نفوذ موفق نبود بلکه بیش از هزاران فایل از شبکه‌های آمریکا و شرکاء صنعتی او شامل نقشه سلاح‌ها، طرح‌های عملیاتی و دیگر داده‌ها به سرقت رفت. عملیات پدافندی در مقابل این حمله سایبری "عملیات گلوله سربی" نام گرفت و پنتاگون حدود ۱۴ ماه وقت صرف پاک کردن این کد از شبکه‌های نظامی خود کرد. این عملیات از این جهت در بین تمامی حملات سایبری بر علیه ایالات متحده اهمیت دارد که نقطه عطفی در تجدید نظر در راهبرد دفاع سایبری ایالات متحده شد و در نهایت منجر به تشکیل فرماندهی سایبری ایالات متحده امریکا[2] گردید.
(http://www.foreignaffairs.com/articles/66552/willi, 2010)

۳. **حملات سایبری علیه جمهوری اسلامی ایران:** بدون شک حملات سایبری علیه جمهوری اسلامی ایران را می‌توان نقطه عطف در کاربرد سلاح سایبری دانست، روزی که حمله سایبری به نام استاکس‌نت ۳ کارشناسان را با مفهوم واقعی جنگ سایبری آشنا کرد. جنگی که در آن زیرساخت‌های داده‌ای و در مفهومی وسیع‌تر زیرساخت‌های سایبری یک کشور مورد هجوم قرار می‌گیرند و در آن همانند جنگ‌های کلاسیک ابتدا جمع‌آوری داده‌های حیاتی مورد نیاز و سپس ضربه زدن به اهداف مورد نظر انجام می‌گیرد. (ویژه نامه افتانا،۱۳۹۱: ۲)

سلسله‌ای از حملات سایبری بر علیه ج.ا.ا طراحی شده بود که هر کدام ابعاد تازه‌ای از جنگ سایبری و توانمندی‌های آن را برای عموم آشکار می‌کردند. حملاتی که اگرچه آلودگی‌های را در دیگر نقاط جهان نیز در پی داشت اما به طور حتم برای حمله علیه ما طراحی شده بود. رالف لانگنر مدیر شرکت امنیتی لانگنر آلمان در پاسخ به این سوال که آیا شما مطمئن هستید که این ویروس برای تاسیسات هسته ای نطنز بوده می‌گوید: بله امروز ما مطمئن هستیم که این ویروس برای تاسیسات هسته ای نطنز بوده زیرا تمامی نشانه‌های پیدا شده با تاسیسات اتمی نطنز مطابقت دارد. اینکه چه کسی در پشت این قضیه قرار دارد هنوز کاملاً مشخص نشده و یک راز است اما کارشناسان معتقدند این ویروس توسط برخی دولت‌ها و با اهدافی خاص همچون جنگ سایبری و به منظور جاسوسی طراحی شده است.

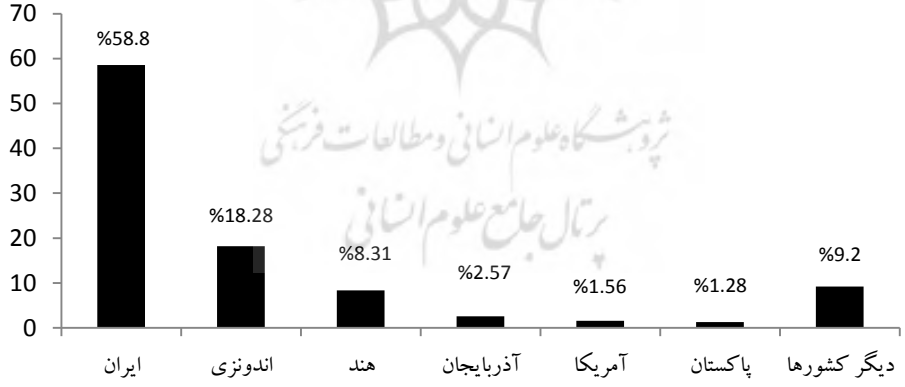
1 - Backdoor
2 - U.S. Army Cyber Command, 2nd Army
3 - Stuxnet

این ویروس قصد داشته با جایگزینی خود در نرم افزار اصلی کنترلی نیروگاه و با ارسال دستورهای غلط باعث اخلال در عملکرد توربین‌ها و در نهایت از کار افتادن سانتریفیوژها گردد. به اعتقاد رالف لانگنر ایالات متحده و رژیم صهیونیستی توسط موساد این کرم مخرب را برای تاسیسات هسته‌ای ایران راه اندازی کرده‌اند. استاکس نت برای کامپیوتر سامانه‌های کنترل صنعتی زیمنس آلمانی ساخته شده که معمولا برای مدیریت منابع آب، سکوهای نفتی، نیروگاه‌ها و دیگر زیرساخت‌های حیاتی مورد استفاده قرار گرفته‌اند. نماینده روسیه در ناتو در ماه ژانویه گفت: استاکس باعث می شود سانتریفیوژهای تولید اورانیوم غنی شده در نیروگاه بوشهر از کنترل خارج شده و باعث فاجعه چرنوبیل(۱۹۸۶- اوکراین) دیگری شود. (http://english.iribnews.ir/NewsBody.aspx?ID=12844,1390)

گزارش شرکت امنیتی سیمانتک[1] که برای اولین بار این ویروس را شناسایی کرده بود نیز اظهارات لانگنر را تائید می‌کند که هدف این کرم بدست گرفتن سیستم های کنترل صنعتی(اسکادا) دانست. باورکردنی نبود که استاکس‌نت از چهار قابلیت آسیب پذیری موسوم به روز صفر[2] (Zero-day) بهره برداری کرده بود که این در نوع خود بی‌سابقه است.

استاکس‌نت اولین قطعه یک بدافزار بود که از آسیب پذیری فایل‌های اجرایی ویندوز بهره می‌برد و قادر بود پس از اتصال یک درایو قابل حذف[3] (همانند حافظه فلش) بلافاصله خود را بروی آن کپی نماید. نمودار شکل (۱) نشان‌دهنده میزان آلودگی کشورهای مختلف به این کرم است که متاسفانه ۶۰٪ آلودگی جهان در ایران گزارش شده است.

نمودار(۱) آلودگی کشورهای مختلف جهان به ویروس استایکس نت



Source: (http://www.symantec.com/security_response/writeup., 2010)

1 -Symantech

۲- تهدید رایانه ای است که سعی در استفاده از نقاط آسیب پذیر نرم افزارهای کاربردی دارد و توسعه دهندگان آن نرم افزار هنوز فرصت نیافته اند که وصله امنیتی خود را برای بر طرف کردن این حفره امنیتی به کاربران ارائه دهند.

3 -Removable drive

این کرم ضمن سرقت کدها و پروژه های طراحی روی اسکادا با استفاده از رابط‌های برنامه نویسی کد خود را نیز بر روی کنترل کننده‌های منطقی قابل برنامه‌ریزی (PLC) بارگذاری می کرد. استاکس‌نت از نوع روتکیت‌های[۱] معمولی نبود که تنها خود را در ویندوز پنهان سازد بلکه قادر به پنهان کردن کد تزریق شده خود درPLC نیز بود.

همزمان اطلاعات جدیدی درباره دوکو[۲]، تروجان تازه کشف شده‌ای که روابط نزدیکی با بدافزار «صنعتی» استاکس نت دارد، منتشر شد. این ویروس فایل‌هایی یا پیشوند DQ ایجاد می‌کند. دوکو از یک حفره (محل آسیب پذیری)در ویندوز (فونت TrueType) مورد استفاده در فایل‌های ورد و یا صفحات وب استفاده کرده و کد خود را اجرا می‌کند. برای مثال، یک سند ورد خاص که روی دستگاه قربانی باز شده باشد، می‌تواند برای باز کردن دسترسی‌ها و سپس اجرای کدهای مورد نظر مورد استفاده قرار گیرد.با توجه به اینکه حفره امنیتی در سیستم عامل ویندوز است و نه در نرم افزار "ورد". بنابراین شرکت میکروسافت از این آسیب آگاه بوده و در حال تهیه وصله امنیتی[۳] است .همزمان مقامات رسمی ایرانی گزارش کردند که یک حمله سایبری توسط بدافزاری به نام استارس صورت گرفته است. طبق برخی گزارش‌ها، استارس[۴] احتمالا نسخه اولیه دوکو است.
(http://ictpress.ir/Default,fa- IR,ICTPress,Content,NewsDetail,Key,10831.aspx, 1389)

در سوم اردیبهشت‌ماه ۹۱ حمله سایبری دیگری به سرورهای وزارت نفت به نام حذف کننده[۵] انجام شد که هدف این ویروس پاک کردن اطلاعات سرورهای این وزارتخانه بود. بروز حمله سایبری به وزارت نفت یک پیامد مهم دیگر داشت و آن آشکار شدن بدافزار شعله آتش[۶] موسوم به فلیم بود. سرمایه‌گذاری دولتی، پیچیدگی فوق‌العاده بالا، هوشمندی در طراحی و روش تکثیر، تنوع عملکرد، ثبت هر گونه فعالیت کاربران، آنالیز ترافیک شبکه، بستر سازی برای فعالیت‌های مخرب آتی، ایجاد سکوی توسعه برای بدافزارهای آتی، قرارگرفتن در حالت نهفته و انجام عکس‌العمل متناسب یا ضدبدافزار نصب شده روی سامانه، هدف قرار دادن یک کشور یا یک صنعت خاص در یک کشور خاص، تخریب نوع یا انواعی از سخت‌افزارهای عمومی و خاص نمونه‌هایی از ویژگی‌های فلیم است. (ویژه نامه افتانا, ۱۳۹۱, ص.۲)

---

۱ - Rootkit : نوعی بدافزار که قادر است موجودیت فرایندها و یا برنامه های خود را مخفی نگاه داشته تا هکر بتواند کنترل رایانه را در دست گیرد

2 - Duku
3 - Patch
4 - Stars
5 - Wiper
6 - Flame

بدافزاری که از آن به عنوان جعبه ابزار بدافزاری یا یک سلاح واقعی سایبری نام برده می-شود. خوشبختانه تجربه استاکس‌نت، سبب شد که مرکز به خوبی وارد عمل شود و با تحلیل اطلاعات موجود و در زمان نسبتا مناسب، نسبت به این رخداد واکنش نشان دهد.اما این رخداد ابعاد نگران کننده دیگری را نیز در بردارد. شروع نامشخص فعالیت این بدافزار که بین دو تا هشت سال قبل تخمین زده می‌شود، ما را مطمئن می‌کند که این بدافزار، اولین و آخرین این سلاح‌ها نبوده و نخواهد بود. پیچیدگی ابعاد طراحی این سلاح سایبری که به بیان ساده صدبرابر بیشتر از یک بدافزار متعارف و ۲۰ برابر بیش از استاکس‌نت بوده است، این پیام را می‌رساند که باید منتظر سلا حهایی با تخریب بسیار بیشتر و تنوع عملکرد و گستردگی وسیع‌تر باشیم. ضمناً با توجه به اینکه فلیم مربوط به تکنیک‌های طراحی چند سال قبل است، پیشرفت تکنیک‌های تولید بدافزارهای حال حاضر و آتی دور از انتظار نخواهد بود. حال با توجه به آنچه گفته شد، آیا تصور گزافی است که کشور در شرایط جنگ سایبری فرض شود؟(همان،ص ۳)

کارشناسان کسپرسکی بر این باورند که این ویروس یک نمونه کمیاب از "بمب سایبری" است و این امر نشان‌دهنده این است که هم‌اکنون جنگ اینترنتی مخفیانه‌ای در جریان است. ساخت این ویروس نمی‌توانسته بدون حمایت مالی یک یا چند دولت صورت گرفته باشد. از میان شش کشور ایران، سودان، سوریه، لبنان، عربستان سعودی و مصر، رایانه‌های ایرانی بیشترین هدف حمله این ویروس بوده‌اند.
.(http://ictpress.ir/Default,fa-IR,ICTPress,Content,NewsDetail,Key,11743.aspx)

کارشناسان می‌گویند به نظر می‌رسد این ویروس پیچیده‌ترین و خرابکارانه‌ترین بدافزار مخرب در طول تاریخ بوده است. این برنامه قادر است حتی از شبکه‌های بسیار امن نیز عبور کرده و عملکردهای کنترل کننده رایانه را روزانه و به طور سری برای طراحان آن ارسال نماید. این کدها می‌تواند دوربین و میکروفون رایانه را فعال کرده ، ضربات صفحه کلید را ثبت[1] کند، از صفحه نمایش عکس بگیرد، منطقه جغرافیایی را از تصاویر استخراج و ارسال و دریافت دستورات و داده‌ها را از طریق فن آوری بی سیم بلوتوث انجام دهد. همه این امور را شعله وقتی انجام می‌داد که یک نرم‌افزار معمولی در حال به روزرسانی خود بود. شعله با استفاده از رمزنگاری پیچیده، شکستن الگوریتم خود را چندین سال به تعویق انداخت.

تام پارکر، متصدی ارشد فناوری در شرکت فوژن‌ایکس[2] گفت: " نوشتن این بدافزار چیزی نیست که محققان امنیتی زیادی دارای مهارت و یا منابع برای انجام آن باشند لذا انتظار می‌رود کسانی همانند نفراتی که در آژانس امنیت ملی هستند و در پیشرفته‌ترین ریاضیات رمزنگاری مهارت دارند بتوانند چنین کاری را انجام دهند

1- Key Logging

۲ - Fusionx : شرکتی امنیتی که متخصص در شبیه سازی پاسخ به حملات سایبری است.

(http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html)

نتیجه‌گیری:

عملیات‌های مشترک در جنگ‌های نوین از تمامی عرصه‌های نبرد در هوا، فضا، دریا، زمین و سایبر بهره می‌برند. در این عملیات‌ها عنصر سایبری در کنار سایر عناصر رزم قرار گرفته و در تصمیم‌سازی و تصمیم‌گیری به فرمانده کمک می‌نماید. عنصر سایبری می‌تواند با طرح‌ریزی حملات سایبری قبل، حین و بعد از جنگ حقیقی کمک شایانی به فرمانده عملیات مشترک نماید. به عنوان یک کاربرد حمله سایبری در قبل از وقوع جنگ می‌توان به فرآیند طرحریزی مشترک اشاره کرد. در این فرآیند ابتدا بایستی اخبار مربوط به بند ۱توانایی‌های دشمن" در برآورد اطلاعاتی و فرماندهی جمع‌آوری شود تا نقطه شروعی برای مدار طرحریزی فراهم گردد. ظهور بدافزارهایی چون استاکس نت، دوکو و فلیم نشان دادند. که می‌توان جمع‌آوری اطلاعات مربوط به این بند را توسط یک عملیات سایبری فراهم کرد.

مطلب دوم اینکه از حملات سایبری می‌توان توام با عملیات نیروهای مشترک نیز بهره برد. در این مرحله همانند جنگ کوزوو با استفاده از پتانسیل‌های جنگ سایبری قادر خواهیم بود

جنگ‌افزارهای هوشمند آفندی و پدافندی دشمن و سامانه کنترل و فرماندهی را که عموما مبتنی بر زیرساخت‌های سایبری هستند هدف قرار داده و از تحمیل تلفات به نیروهای خودی جلوگیری نمائیم. بنابراین علاوه بر جمع‌آوری از تخریب و یا اخلال در اطلاعات نیز می‌توان برای تحقق بخشی از سناریوی نبرد حقیقی استفاده کرد.

سوم اینکه از پتانسیل قدرت نرم جنگ سایبری می‌توان بعد از نبرد حقیقی و به منظور عملیات روانی تحکیمی استفاده کرد. بنابراین اهمیت بعد پنجم (سایبری) از دیگر ابعاد کمتر نبوده بلکه به خاطر ویژگی های خاص خود حتی به تنهایی می‌تواند در مواردی شرط لازم و کافی برای نیل به نتیجه مطلوب باشد. حملات سایبری در جنگ های اخیر شرط لازم برای نبرد حقیقی بوده است و در آینده شاید شرط کافی باشد و مهاجم با دستیابی به اهداف خود جنگ را خاتمه دهد. با توجه به گسترش و نفوذ آن در زیرساخت‌های نظامی دور از ذهن نخواهد بود که در آینده به تنهائی پتانسیل یک نبرد واقعی را نیز داشته باشد.

بنابراین نقش بعد سایبر در جنگ های نوین بر هیچ کس پوشیده نیست و لزوم توجه جدی به آن را می طلبد. نادیده گرفتن این بعد به منزله غفلت از بخشی از صحنه نبرد است که موجب وارد شدن خسارت بیشتر حتی در صورت نیل به پیروزی می گردد. با توجه به ظرفیت قدرت سایبری در هردو حوزه نرم و سخت می توان به عنوان یک قدرت هوشمند آن را در نظر گرفت.

اما همه این قابلیت‌ها تنها در صورتی مهیا خواهد شد که اصول اولیه جنگ در این بعد نیز مد نظر قرار گیرد. اصولی همچون تمرکز، وحدت تلاش و فرماندهی، آفند و صرفه‌جوئی در قوا مستقل از نوع عرصه نبرد بوده و در عرصه سایبری نیز رعایت این اصول اجتناب ناپذیر است. تحقق اصول یاد شده نیاز به نیروی انسانی متخصص، ساختار و تجهیزات و اعتبارات دارد. بایستی همانطور که برای دیگر ابعاد میدان نبرد نیرویی خاص در نظر گرفته شده، ساختاری مستقل نیز به این عرصه جنگ اختصاص یابد. این ساختار می‌تواند در قالب فرماندهی مخصوص و یا مشترک شکل گیرد تا در هنگام یک عملیات مشترک عنصری از این فرماندهی در اختیار یک قرارگاه مشترک عملیاتی و تحت فرماندهی فرمانده عملیات مشترک قرار گیرد. بنابراین برداشتن گام های زیر برای نیل به کلیه اهداف پیش گفته ضروری است:

ایجاد ساختار فرماندهی مخصوص سایبری

به منظور اطمینان از آزادی عمل بیشتر و با توجه به وجود معیار[۱] مورد نیاز تشکیل فرماندهی مخصوص، ایجاد چنین ساختاری می تواند کارایی و اثربخشی مطلوبی بر انجام ماموریت در این حوزه داشته باشد. "فرماندهی سایبری" این عرصه را به عنوان میدانی توصیف می کند که می‌تواند همچون زمین، هوا و فضا و دریا گستره جنگ‌ها و درگیری‌های آتی باشد. این فرماندهی مستقل از منطقه جغرافیایی بوده بنابراین فرماندهی سایبری بر مبنای وظیفه تشکیل شده است نه بر مبنای منطقه[۲] و وظیفه آن صیانت از فضای تبادل اطلاعات در سطح آجا است. این ماموریت شامل موارد آفندی و پدافندی زیر است:

الف) انجام عملیات‌های اطلاعاتی[۳] شامل عملیات روانی، جنگ الکترونیک، عملیات امنیتی، فریب اطلاعاتی و عملیات شبکه‌ای : شناسایی زیرساخت‌ها و نقاط آسیب‌پذیر شبکه‌های ارتباطی (مخابراتی و رایانه‌ای) دشمن در فضای سایبر به منظور اخلال، جمع‌آوری، تخریب و از کار اندازی خدمات

ب) سیاست گذاری و هدایت تمرکزی طراحی و ساخت و پیاده‌سازی سخت افزارها و نرم افزارهای بومی به ویژه در حوزه امنیت شبکه به منظور رفع و یا کاهش نقاط ضعف و آسیب پذیری شبکه های آجا

ج) تدوین و پیاده سازی استانداردها و آیین نامه‌های مورد نیاز در حوزه سایبر

۱- وجود یک ماموریت کلی و مداوم که اجرای آن مستلزم شرکت یگان های یک نیروی مسلح در یک منطقه بوده و لزوم هدایت راهبردی واحدی را ایجاب نماید. (نیازی ، فرج پور ، توکلی, ۱۳۹۰, ص. ۱۶)

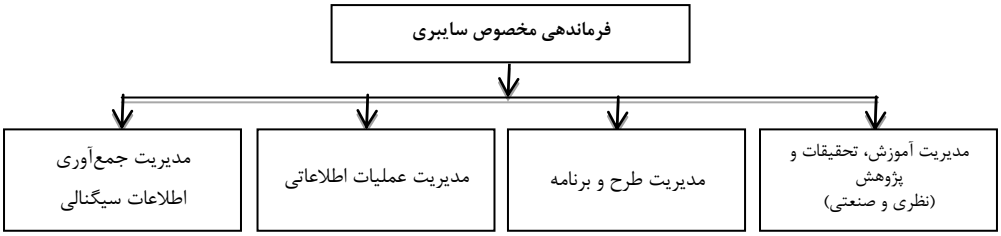
۲- ماهیت مسئولیت ها ،ماموریت ها و وظائف واگذاری به فرماندهان تعیین کننده فرماندهی برپایه وظیفه یا منطقه خواهد بود. (نیازی ، فرج پور ، توکلی, ۱۳۹۰)

3 - Information operations (IO

د) آینده پژوهی تهدیدات و فرصت‌های حوزه سایبر

بنابراین این فرماندهی بایستی حداقل دارای ۴ بخش مدیریتی باشد که در شکل(۲) نمایش داده شده است. بدیهی است ترسیم ساختاری دقیق نیاز به پژوهشی مفصل در این زمینه داردکه خارج از حوصله موضوع مقاله است.

شکل(۲) ساختار سازمانی پیشنهادی فرماندهی مخصوص سایبری



۱. **آموزش:** تدوین و تدریس دروس جنگ سایبری در قالب دوره های طولی در دانشگاه‌ها و مراکز آموزشی آجا به ویژه دافوس و دوره‌های عرضی امنیت شبکه و رایانه به عنوان مهارت هفتم به ویژه برای فرماندهان و مدیران

۲. **رزمایش:** بدیهی است در عرصه جنگ سایبری نیروهای فنی در لجمن[۱] قرار گرفته و رزم سایبری را هدایت می‌کنند. این نیروها همانند دیگر عناصر نیروی رزمی برای رسیدن به آمادگی کامل در برابر حملات سایبری نیاز به انجام رزمایش دارند. بنابراین ایجاد میدان مشق سایبری در قالب رزمایش مستقل و یا مشترک با دیگر نیروها الزامی است.

۳. جنگ ناهمطراز: شاخصه‌هائی چون هزینه پایین ورود و نامتقارن بودن در آسیب‌پذیری شرایط بسیار مناسبی را برای جنگ ناهمطراز فراهم کرده است. بنابراین اگر به دنبال موازنه قوا هستیم عرصه سایبر ظرفیت‌های زیادی را برای تحقق این امر در اختیار ما قرار می‌دهد.

۴. **انعقاد پیمان‌های دفاعی بین‌المللی:** بررسی خصوصیات حملات سایبری علیه ج.ا.ایران نشان از حمایت دولت‌ها در طراحی و انتشار بدافزارهای پیچیده دارد که بیانگر ائتلاف بین‌المللی در عرصه سایبر است. اگرچه شاخصه گمنامی جنگ سایبری سبب شده که هیچگاه به طور قطع و یقین مشخص نشود که حمله از طرف چه کشور یا کشورهایی صورت گرفته لیکن راهبردهای منتشره ایالات متحده و رژیم صهیونیستی نشان از انجام یک عملیات مرکب بر علیه نظام مقدس ج.ا.ایران دارد. با توجه به گسترش سریع و نفوذ زیاد این فضا بدیهی است که ج.ا.ایران نیز به تنهائی قادر به دفاع سایبری نخواهد بود. بنابراین بایستی

[۱] لبه جلوئی منطقه نبرد

پیمان‌های دفاع سایبری با کشورهایی که دارای منافع مشترک هستند؛ منعقد گردد تا عملیات‌هایی مرکب در حوزه سایبر طرحریزی و اجرا گردند.

منابع و مأخذ

۱. شریف, ا. (۱۳۸۴). *جنگ و دفاع سایبر*. وزارت دفاع و پشتیبانی نیروهای مسلح-موسسه آموزشی و تحقیقاتی صنایع دفاعی.

۲. نیازی، علی، فرج‌پور، عبدالحسین، توکلی، ابوالفضل. پاییز(۱۳۹۰). عملیات مشترک و مرکب. تهران، دانشگاه فرماندهی و ستاد آجا.

۳. حسن بیگ، ابراهیم، ۱۳۸۸. حقوق و امنیت در فضای سایبر، تهران، دانشگاه عالی دفاع ملی

۴. حسن‌پور، جعفر، فصلنامه اطلاعاتی حفاظتی جامعه اطلاعاتی، شماره ۶، تهران، پائیز ۱۳۸۸، ۹۲.اشراف اطلاعاتی در افق ۱۴۰۴ یا عصرسایبر.

۵. صالحی، علیرضا ، ویژه نامه افتانا(فلیم) . تهران ، تیر(۱۳۹۲) .ص۲

6. J. Andress, S. Winterfeld. (2011). Cyber Warfare Techniques, Tactics and Tools for Security Practitioners. USA: Elsevier
7. Departmen Of Defense(DOD). (2012) Priorities For 21th Century Defense , Sustaining US global leadership. Washington
8. Joseph S. Nye. (2010). Cyber Power (The future of power in the 21th century). MIT-Harvard Minerva Project ,Harvard Kennedy School
9. Lambeth , B. S. (2001). NATO's Air War for Kosovo: A Strategic and Operational Assessment. New York: Cornell University.
10. Thomas K. Andersen. (2011). AIR FORCE DOCTRINE DOCUMENT. Washington ,USAF Publication
11. http://ictpress.ir/Default,fa-IR,ICTPress,Content,NewsDetail,Key,10831.aspx
12. http://english.iribnews.ir/NewsBody.aspx?ID=12844,
13. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain
14. http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
15. http://www.defense.gov/news/newsarticle.aspx?id=64(2011).