تاریخ دریافت مقاله: ۱۳۹۳/۰۱/۱۹
تاریخ پذیرش مقاله: ۱۳۹۳/۱۰/۲۵

تبیین نقش جنگ سایبری در جنگ‌های آینده

ایرج بختیاری[۱]

چکیده:

روند رو به رشد تحول و پیشرفت روز افزون فناوری اطلاعات و کاربرد گسترده آن در عرصه فضای مجازی و استفاده از ابزار و تجهیزات سخت افزاری و نرم افزاری مرتبط، بر روشها و فنون نبردها تاثیر داشته و شکل جدیدی از جنگ را پدید آورده است. الزام نیروهای مسلح کشورها بهره برداری از آخرین دستاوردهای فناوری را امری حیاتی نموده است از این رو شناخت صحیح و ورود به موقع در عرصه های نوین دفاعی همواره یکی از دغدغه های طراحان و بازیگران حوزه راهبرد و دفاع می‌باشد. در این مقاله الگوهای کشورهای صاحب فناوری در فضای مجازی بین تجهیزات ارتباطی ، مخابراتی، شبکه‌های رایانه ای و سیستم مبتنی بر رایانه مورد مطالعه قرار گرفته و فضای سایبر و و فرصتها و تهدیدهای آن در جنگ آینده بررسی شده است نتیجه مقاله حاکی از این است که جنگ سایبری به اندازه کنشهای عینی میادین نبرد جدی است . در این راستا اقدامن لازم برای کاهش نسبی آسیب پذیری نیروهای مسلح جمهوری اسلامی ایران در برابر حملات سایبری پیشنهاد می‌شود

کلید واژه‌ها:

جنگ سایبر، اطلاعات، ارتباطات رایانه‌ای ، شبکه

۱- دانشجوی دکتری مدیریت راهبردی، دانشگاه عالی دفاع ملی

مقدمه

در طول تاریخ؛ دکترین نظامی، سازمان و راهبرد کشورها تحت تاثیر فناوری های نوین، همواره دستخوش تحول و تکامل بوده بطوریکه جنگهای نسل اول تا ششم را رقم زده است. فرآیند صنعتی شدن و رقابت تسلیحاتی در زمینه ساخت و بکارگیری سلاحهای گرم منجر به بروز جنگ فرسایشی اول جهانی و رشد صنایع بزرگ اسلحه و مهمات‌سازی و حضور تانک در مانور مکانیزه جنگ دوم جهانی گردید. در عصر حاضر یا عصر اطلاعات مفاهیم دهکده جهانی[1] و جهانی شدن[2] و یا به تعبیری جهانی‌سازی روندی است که ایجاد بستر ارتباطات لازم و شبکه جهانی اینترنت و امکان دسترسی آسان و آنی[3] به اطلاعات، جهشی شگفت‌انگیز در عرصه رشد و پیشرفت جهانی ایجاد نموده است بطوری‌که عملیات در قلمرو اطلاعات به اندازه عملیات در زمین، دریا، هوا و فضا واجد ارزش و اهمیت گردیده است. تحول و جهش کنونی در حوزه فناوری اطلاعات و ارتباطات سبب ظهور شیوه نوینی از جنگ گردیده که در آن پیروز میدان نبرد کسی است که اطلاعات بیشتری دارد نه آن که تنها به تمرکز قوا و تحرک می‌اندیشد.

حضور سامانه های پیچیده ارتباطی و الکترونیکی نوین، سناریوی نبردهای آینده را طوری تغییر داده که از یک سو این سامانه ها به فرماندهان در تصمیم ازی براساس تصاویر و اطلاعات زمان حقیقی نبرد کمک کرده و از سوی دیگر وابستگی به سامانه‌های الکترونیکی و ریزپردازنده‌ها، آنان را در برابر جنگ سایبری بسیار آسیب پذیر نموده است.

واژه جنگ سایبری[4] برای تشریح نوع جدیدی از جنگ که بر سامانه های ارتباطی و الکترونیکی دشمن متمرکز می‌گردد، ابداع شده است. در این جنگ نیازی به اعزام لشکرها یا ناوهای جنگی نبوده و به جای آن از ویروس‌های رایانه‌ای و بمب‌های پالس الکترومغناطیسی استفاده می‌شود که قادراست خرابی‌های وسیعی در مدارات الکترونیکی سامانه‌های C4I، رادارها، رایانه‌ها، سلاح های هوشمند و سامانه‌های مراقبتی به وجود آورد. این نوع از جنگ، مقدم بر جنگ واقعی بوده و حتی ممکن است از وقوع آن قبل از شروع جلوگیری کند.

1. global village
2. globalization
3. online
4. Cyber Warfare

کشورهای در حال توسعه به دلیل نداشتن تولیدات الکترونیکی پیچیده و سامانه‌های مرتبط و وابستگی عمیق به فناوری‌های خارجی آسیب‌پذیری بیشتری در این زمینه داشته و آسیب‌پذیری جدی آنان در برابر هرگونه تهدید سایبری در برابر دشمنان و عناصر نفوذگر داخلی و خارجی در پی داشته است. بنابراین نیاز به آموزش مفاهیم و ابعاد این جنگ در نیروهای مسلح شدیدا احساس می شود و تدوین راهبردهای مناسب در زمینه شناخت و مقابله با تهدیدات جنگ سایبری نیز از ضروریات عصر حاضر می‌باشد.

مفاهیم نظری

فضای سایبر[1]

این فضا در دنیای اینترنت، رسانه و ارتباطات بسیار مطرح می‌شود. واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده و نخستین بار اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر[2] در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (کامپیوتر ها) است. با توسعه اینترنت، واژه های ترکیبی بسیاری از کلمه سایبر مانند؛ فضای سایبر، شهروند سایبر ، پول سایبر ، فرهنگ سایبر ، راهنمای سایبر ، تجارت سایبر ، کانال سایبر و .... بوجود آمده-اند

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون[3] نویسنده داستان علمی تخیلی:" برنینگ کروم" در کتاب نورومنسر[4] درسال۱۹۸۴ به کار برده است. فضای سایبری به فضایی اطلاق می‌شود که با استفاده از فناوری اطلاعات و ارتباطات و شبکه‌ها اجزا و ساختارهای آن یا برپایه تخیل‌ها فاقد مبنای واقعی و یا بر پایه واقعیت‌های شبیه‌سازی شده طراحی و ابداع می‌گردد.(حافظ نیا، ۱۳۹۰ :۱۱). یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرار کنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد. در واقع می توان گفت که فضای سایبر گستره‌ای

1. Cyberspace
2. Norbert Wiener
3. WilliamGibson
4. Neuromancer

از ذهن است که می تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد. با این رویکرد ارتباط سایبری به مجموعه ای از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیا گفته می شود. یک سیستم آنلاین نمونه ای از فضای سایبراست که کاربران آن می توانند از طریق ایمیل و... با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها ویا حرکات ماوس صورت می گیرد (حسن بیگی، ۱۳۸۴ :۲۳).

فضای سایبر سیستم عصبی این زیرساختها و به عبارت دیگر سیستم کنترلی مملکت محسوب می‌شود. فضای سایبر، مرکب از صدها هزار رایانه، مسیریاب، سوئیچ و فیبر نوری می‌باشد که فعالیت زیرساختهای حیاتی، به این تجهیزات وابسته است. بنابراین سلامت عملیات فضای سایبر اهمیت اساسی در امنیت ملی و اقتصاد دارد.(حسن بیگی، ۱۳۸۸: ۲۶۹)

در نوامبر ۲۰۰۵، فرمانده نیروی هوایی، مایکل دبلیو وین[1] و ژنرال مایکل موزلی[2] در نامه‌ای مشترک به کارکنان نیروی هوایی مفهوم جدیدی به نام فضای سایبر را تعریف کردند. بر این اساس فضای سایبر شامل امنیت شبکه، انتقال داده و تسهیم اطلاعات بود. (انتشارات مرکز آینده پژوهی علوم و فناوری دفاعی، ۱۳۸۸: ۱)

فضای سایبر فضایی است که در آن فعالیت های گوناگون در ابعاد داده ورزی و اطلاع رسانی، ارتباطات و ارائه خدمات ، مدیریت و کنترل از طریق سازو کارهای الکترونیکی و مجازی انجام می پذیرد. (صدری و دیگران،۱۳۸۴: ۵۸)

فضای سایبر از نگاه دیوید بل[3] (۲۰۰۱) یکی از صاحبنظران حوزه ارتباطات فضای سایبر یک شبکه گسترده جهانی است که شبکه های مختلف رایانه ای در اندازه های متعددو حتی رایانه‌های شخصی را با استفاده از سخت افزارهای گوناگون و با قرادادهای ارتباطی به یکدیگر وصل می‌کند. فناوری‌های ارتباط از را ه دور اساس فضای سایبر را تشکیل می‌دهد. هر چند برخی از این فناوری‌ها مانند تلگراف و تلفن در اوایل قرن نوزده اختراع شده بودند اما همه گیر و ارزان شدن این فناوری ها و بالا رفتن توان فنی آن ها که شرط اصلی ظهورفضای سایبر است در چند سال اخیر اتفاق افتاده است (شریفی هولاسو ، ۱۳۸۷: ۵۲)

---

1. Micheal w.wynne
2. Micheal moseley
3. David Bell

در دیدگاه جامعه شناسانه فضای سایبر یک دنیای جدید، یک دنیای موازی است که با خطوط ارتباطی و کامپیوترهای جهان خلق و نگهداری می‌شود دنیایی که در آن تردد جهانی دانش، رموز، سنجش‌ها، شاخص‌ها، سرگرمی‌ها و عاملیت دیگر انسانی شکل می‌گیرد .(بل ،۱۳۸۹: ۲۳-۲۲). در این رویکرد فضای سایبر شامل؛ فضایی خیالی که در آن افکار مجذوب توهمی رویا گونه می‌شود، دنیای مفهومی تعاملات شبکه‌شده بین افراد و آفریده-های معنوی‌شان و هر چیز همراه با شبکه‌ها و تعاملات آن، حالتی از اندیشه که توسط افراد در ارتباط و به‌وسیله بازنمایی دیجیتالی زبان و تجربه حسی به اشتراک گذارده می‌شود، افرادی که از نظر زمان و مکان از یکدیگر جدا ولی به وسیله شبکه‌ای از ابزارهای فیزیکی دسترسی به یکدیگر متصل‌اند (دوران ،۱۳۸۱: ۲۳).

در یک جمع‌بندی می‌توان گفت؛ فضای سایبر فضای تولید و تبادل اطلاعات و هر چیزی که قابلیت اتصال به شبکه را دارد، می‌باشد. در این فضا تولید اطلاعات همان‌جایی است که استفاده از اطلاعات و نگهداری اطلاعات همزمان انجام می‌پذیرد. فضای سایبر مبتنی بر بستر شبکه است و در شبکه تولید از انتقال جدا نیست و همزمان اتفاق می‌افتد. فضای سایبر با فضای سنتی در تحلیل، توجیه و شناخت تفاوت دارد.

جنگ و عصراطلاعات

ظهور عصر اطلاعات مفاهیم و مبانی زندگی دوران صنعتی را دستخوش تحول نمود و به-تبع آن در عرصه جنگ، انقلاب اطلاعات به‌گونه‌ای مفهوم نبرد را تغییر داد که دیگر شاهد نبرد فرسایشی خونین نیروهای نظامی نخواهیم بود. در عوض، نیروهای کوچک و چالاکی که به اطلاعات بلادرنگ ماهواره‌ها و حسگرهای صحنه نبرد مسلح شده‌اند، با سرعت اعجاب‌آوری به محل‌های غیرمنتظره حمله می‌برند و کسی که در جنگ اطلاعات بیشتری دارد، ابهام فضای جنگ را از بین برده و از مزایای قطعی آن بهره‌مند خواهد شد.

در عصر کنونی اطلاعات دیجیتال با اطلاعات آنالوگ از جهاتی متفاوت است. بر خلاف آنالوگ، شنود و نمونه‌برداری از این اطلاعات تاثیری بر شبکه نمی‌گذارد و اطلاعات تماما قابل تجمیع است. در این فضا اگر مشکلی در ارسال اطلاعات پیش آید خود اطلاعات تخریب می‌گردد.

در شبکه هر بعد آن طرف مقابل را نمی‌شناسد اما کسی که شبکه را مدیریت می‌کند اشراف بالایی داشته و همه چیز را می‌تواند ثبط و ضبط نماید.(پورابراهیمی، ۱۳۹۳)تحولات

شگرف در جمع‌آوری، ذخیره‌سازی، پردازش، انتقال و ارائه اطلاعات باعث شده اطلاعات در حال تبدیل‌شدن به یک منبع راهبردی به عنوان یک عنصر بانفوذ و ارزشمند در عصر فراصنعتی- همانند نقشی که سرمایه و کار در عصر صنعتی داشتند- شود. انقلاب اطلاعات در حال به چالش کشیدن طراحی سازمان‌هاست بگونه‌ای که سلسله مراتب سازمان‌هایی که بصورت متعارف طراحی شده‌اند را از هم می‌پاشد و به مرور زمان از بین می‌برد. انقلاب اطلاعات اغلب قدرت را به نفع بازیگران کوچکتر و ضعیفتر اشاعه و توزیع مجدد می‌کند. این انقلاب از مرزهای فعلی مسئولیت‌ها عبور و مرزهای جدیدی برای این مسئولیت‌ها ترسیم کرده و عموماً سیستم‌های بسته را مجبور به بازشدن نموده و باعث تغییرجهت در چگونگی کشمکش بین جوامع و برپایی جنگ توسط نیروها شود.

جنگ آینده

تا به حال در کتب و مقالات و اسناد منتشر شده حجم گسترده‌ای از ادبیات مربوط به جنگ آینده منتشر شده و براساس آنچه که در کتاب جنگ و ضد جنگ تافلرها[1] و فرجام تاریخ و واپسین انسان، در سال ۱۹۹۵ آمده؛ عمده این ادبیات دو رویکرد کلی به موضوع داشته‌اند نخست بر سناریوپردازی در مورد جهان و جنگ آینده و دوم بر توصیف روندهای کنونی و پیش بینی جهان آینده بر اساس آن استوار است. جنگهای آینده ماهیتاً با جنگهای ماقبل و تجربه شده حداقل سه تفاوت اساسی دارند؛ ۱) فناوری تسلیحاتی به مراتب پیشرفته تر از گذشته ۲) استراتژیهای جدید نظامی ۳) توجه به شیوه های جنگ نامتقارن در آنها .(باقری، ۲۷:۱۳۸۵)در دهه‌های اخیر، نظریه پردازان و صاحب نظران نظامی و حتی سیاسی عبارتهای جنگهای نوین، جنگهای مدرن[2]، جنگهای تمیز و جنگهای آینده در ادبیات مرتبط با امور نظامی اعم از گفتاری و یا نوشتاری در مقاطع مختلف زمانی به‌منظور بیان تغییر و تحولات بوجود آمده در ماهیت جنگ‌ها و منازعات انسانی مطرح نموده و مراد هر یک از آنها در استفاده از این مفهوم گرچه دارای مشترکاتی بوده اما متناسب با مقطع و شرایط زمانی خاص خود و با دیدگاه‌های متفاوتی بیان شده است. ماهیت جنگ‌ها هم پابه‌پای تحولات بنیادی در ماهیت سایر پدیده‌های اجتماعی و فرهنگی، علمی و فناوری، اقتصادی و سیاسی در حال دگرگونی بوده است، این دگرگونی گاه در قالب بیانی تازه و در حوزه بازاندیشی نمودار شده و گاه حاصل هم افزایی علوم مختلف و نو اندیشی های صورت گرفته در چارچوب نظریات جدید

---

1. Alvin and Hidi Tafler
2. Modern Warfare

رخ نموده است. در چند دهه اخیر شکل جنگ به مرور تغییر یافته و به نظر می رسد که جنگهای کلاسیک بین کشورها - که سناریوی جنگ سرد از آن متأثر بود- به تاریخ پیوسته است. نمایش صحنه‌های جنگ الکترونیکی یا به اصطلاح، جنگ تمیز در حمله ایالات متحده به عراق با استفاده از رایانه‌های عملیاتی مختل کننده اعمال دشمن و بمب‌های هوشمند نابود کننده عملیات ترابری و عبور و مرور تانک‌ها، کامیون‌ها و توپ‌های جنگی موجب فلج شدن آتش‌های پشتیبانی و عملیات‌های آماد و پشتیبانی عراق شد.

باری بوزان بر پنج حوزه قابل شناسایی در فناوریهای تسلیحاتی جنگهای آینده در زمینه های قدرت آتش، تحرک، ارتباطات، محافظت و اطلاعات تأکید دارد.

تافلر نیز در کتاب«جنگ و پاد جنگ» بر ویژگیهایی همچون تنوع و دگرگونی، غیر انبوه سازی، برخورداری از پایه‌ها و زیرساخت‌های غیر نظامی، سرعت عمل و تحرک، قدرت تخریب، انسجام و پیوستگی، فناوری‌های حفاظتی و حجم و دقت بالای آتش به عنوان مشخصه‌های اصلی فناوری‌های نظامی در جنگ‌های پست مدرن تأکید دارد.

ویژگیهای جنگ آینده

مطالعات نشان می دهد جنگ آینده احتمالی موضوعی است که تقریبا همه کشورها در طرح ها، برنامه و ملاحضات دفاعی و امنیتی خود به آن پرداخته و بسته به نوع تهدیدی که در حریم امنیتی خود داشته اند آن را مطرح ساخته اند. اگرچه دیدگاه‌های مختلفی مطرح شده اما نهایتا همه کشورها در مواردی اشتراک نظر دارند، اینکه در جنگهای آینده:

الف) فناوری‌های تسلیحاتی بسیار متفاوت از جنگ‌هایی که تا کنون رخ داده خواهد بود.

ب) جنگ‌ها در آینده کوتاه مدت، مستمر، سریع و شدید خواهند بود و قسمت عمده لوازم و زمینه های پیروزی یا شکست قبل از جنگ ایجاد می‌شوند.

ج) محیط جنگ آینده و جغرافیای جنگ متفاوت از گذشته خواهد بود.

د) زمان نقش کلیدی دارد.

ه) مردم دارای نقش محوری هستند و هزینه‌های جنگ‌ها بسیار بالا خواهد بود.

و) به‌دلیل شکاف استراتژیک قدرت بین بازیگران بین الملل نقش نبردهای نا متعارف و نامنظم در جنگ‌ها بسیار پررنگ خواهد بود و قدرت‌های برتر در مقابله با شیوه‌های جنگ نامنظم و نامتقارن آسیب‌پذیرخواهند بود.

ز) مقاومت، شکیبایی، میل به از خود گذشتگی و شجاعت راه‌های موثری است برای مقابله با دشمنی

که به فن‌آوری پیشرفته مجهز و تمایل زیادی به درگیری دارد. بنابراین وجود اراده جنگی، میل به دفاع و تمایل به جنگجویی کماکان مهمترین رکن قدرت دفاعی یک کشور را تشکیل می دهد.

ح) یکی از راههای مقابله با سلاحهای هوشمند در جنگهای آینده، تقسیم یگانهای بزرگ به یگانهای کوچک و متحرک است که خود به‌خود وسعت صحنه نبرد را افزایش خواهد داد.

ط) آتش و مانور خصوصا از طریق هوا در این جنگ‌ها همچنان حیاتی خواهد بود.

ی) تصرف و کنترل زمین همچنان به عنوان معیاری برای پیروزی مطرح است و نیروی زمینی محور ارتش را تشکیل خواهد داد.

ک) غیر قابل پیش بینی بودن حوادث و وضعیت‌ها به‌دلیل رویکرد نامنظم در جنگهای آینده.

فناوری‌های تسلیحاتی جنگ‌های آینده

یکی از عوامل اساسی که تأکید بر آن ماهیت جنگ‌های آینده را نسبت به جنگ‌های پیشین متمایز می‌سازد، ویژگی منحصر به‌فرد فناوری‌های نوین به‌کارگرفته شده در این جنگ می‌باشد. باری بوزان[1] بر پنج حوزه قابل شناسایی در فناوری‌های تسلیحاتی آینده در زمینه قدرت آتش، تحرک، ارتباطات، حفاظت و اطلاعات تأکید دارد و جی. ای. سینگ[2] در این زمینه به فناوری‌های نظامی قابل بکارگیری در ضربات ایستگاهی دقیق، فرماندهی، کنترل و اطلاعات پیشرفته، جنگ اطلاعاتی و جنگ غیرکشنده اشاره دارد.

تافلر[3] در کتاب «جنگ و پادجنگ» بر ویژگی‌هایی همچون تنوع و دگرگونی و غیرانبوه سازی، برخورداری از پایه‌ها و زیرساخت‌های غیرنظامی، سرعت عمل و تحرک، قدرت تخریب، انسجام و پیوستگی فناوریهای حفاظتی و حجم بالای آتش به عنوان مشخصه های اصلی تکتولوژیهای نظامی در جنگهای آینده (پست مدرن) تأکید دارد. بطور کلی فناوری-های تسلیحاتی جنگ‌های آینده در چهار دسته قابل شناسایی هستند:

- **فناوریهای اطلاعاتی**: بر اساس این نوع فناوری‌ها که منتج به دریافت، پردازش انتقال و توزیع اطلاعات در کمترین زمان ممکن است(جنگ‌های اطلاعاتی چون جنگ فرماندهی و کنترل[4]، جنگ هوشمند، جنگ الکترونیک و جنگ رایانه‌ای)

---

1. Bary Bozan
2. J.A.Sing
3. Tafler
4. Command and Control Warfare

- **فناوریهای نرم افزاری:** نرم افزارها گرچه محصول تفکر انسآنها هستند اما این قابلیت را دارند که پس از طراحی فارغ از محدودیت‌های انسانی به ایفای نقش در صحنه جنگ‌ها بپردازند.

- **فناوریهای سلاحهای کشتار جمعی:** بر خلاف سلاح هسته‌ای که فناوری آن در اختیار تعداد محدودی ازکشورهای دنیا می‌باشد، دسترسی به فناوری سایر سلاحهای کشتارجمعی نظیر سلاحهای شیمیایی و بیولوژیکی برای اکثر کشورها چندان مشکل نیست فناوری این سلاح-ها حربه‌ای در دست برخی از کشورها برای جبران عقب ماندگی‌های خویش در سایر زمینه-های فناوری‌های تسلیحاتی محسوب می‌شود و به‌همین خاطر قدرت‌های بزرگ و صاحبان فناوری‌های پیشرفته از احتمال آسیب دیدن در این عرصه ها به شدت نگرانند.

- **فناوریهای سلاحهای متعارف:** هر چند جنگ‌های آینده بیشتر بر سه دسته از فناوری‌های ذکر شده مبتنی است اما این به هیچ وجه به معنای سکون و ایستایی سلاحهای متعارف نیست. همگام با سایر فناوری‌های تسلیحاتی،روزبه‌روز بر کارآیی و اثربخشی فناوری‌های مربوط به سلاحهای متعارف افزوده می‌شود و بعضاً سطح فناوری این سلاح‌ها در جنگ‌های آینده بطور کلی با گذشته متفاوت خواهد بود.

همانطور که بیان شد یکی از ابعاد مهم جنگ آینده جنگ اطلاعات است که مبتنی بر اطلاعات و شبکه و فضای مجازی است که همین امر جنگ سایبری را به جنگ‌های آینده پیوند می‌دهد.

تعاریف و مفاهیم جنگ سایبری

رایاجنگ، نبرد مجازی، یا جنگ سایبری، به نوعی از نبرد اطلاق می‌گردد که طرفین جنگ در آن از رایانه و شبکه‌های رایانه‌ای (به خصوص شبکه اینترنت) به عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند و از مقاصد آن انجام کارهای خشونت بار جهت ارعاب و یا تغییر عقیده یک گروه یا کشور است. جنگ سایبر به قصد کارهای سیاسی و یا آرمانی انجام و مکان‌ها و زیرساخت‌های حیاتی مانند انرژی، حمل‌ونقل، ارتباطات و سرویس‌های ضروری (مانند پلیس و خدمات پزشکی) را هدف قرار می‌دهد و از شبکه به عنوان بستر انجام این اعمال خرابکارانه استفاده می‌کند.

مارتین لیبیکی، از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی آمریکا، در کتاب «جنگ اطلاعاتی چیست؟» می‌نویسد «تلاش برای درک مفهوم جنگ

اطلاعاتی مانند این است که چند نفر نابینا بخواهند با لمس کردن بخش‌های مختلف یک فیل بگویند که این موجود چیست. جنگ اطلاعاتی نیز شامل بخش‌های مختلف و متعددی می شود.»

مگان برنز در سال ۱۹۹۹ با نگرشی کلی می‌گوید؛ جنگ اطلاعاتی طبقه یا مجموعه ای از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست یافته و آن را حفظ می‌کند.

مارتین لیبیکی ضمن وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفت شکل مختلف جنگ اطلاعاتی را به شرح زیر نام می‌برد:

- جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.
- جنگ برپایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم هائی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
- جنگ الکترونیک با استفاده ازتکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری.
- جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرزفکر دوستان، بی طرف‌ها، و دشمنان استفاده می‌شود.
- جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
- جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.
- جنگ سایبر ترکیبی از همه موارد شش گانه بالا.

به هدایت عملیات نظامی بر اساس قوانین حاکم بر اطلاعات، جنگ سایبر گویند. هدف از این نوع جنگ، تخریب سیستم‌های اطلاعاتی و ارتباطاتی می‌باشد؛ تلاش این جنگ در جهت شناسایی مسائلی است که دشمن به شدت از آن محافظت می‌کند؛ این جنگ حرکتی در جهت تغییر "توازن اطلاعات و دانش" به نفع یک طرف است، به‌خصوص اگر توازن نیروها برقرار نباشد. (ضیایی‌پرور،۱۳۸۶ :۱۲۴)

جنگ اطلاعاتی[۱]

به اقداماتی اطلاق می گردد که به منظور کسب برتری اطلاعاتی میدان نبرد از طریق مخدوش کردن اطلاعات و اختلال در سامانه اطلاعاتی دشمن و محافظت از اطلاعات و سامانه اطلاعاتی خودی اجرا می‌شوند. برابر تعریف وزارت دفاع ایالات متحده تعریف نظامی آن عبارتست از اقداماتی که برای دستیابی به برتری اطلاعاتی در پشتیبانی از راهبرد ملی نظامی از طریق تحت تاثیر قرار دادن اطلاعات و سامانه اطلاعاتی دشمن و نفوذ دادن و دفاع کردن از اطلاعات و سامانه اطلاعاتی خودی به مورد اجرا گذارده می شوند.

جنگ سایبری

عبارت است از اقدامات آفندی غیر متحرکی که به منظور کسب برتری اطلاعاتی از طریق تحت تاثیر قراردادن سامانه اطلاعاتی و شبکه‌های رایانه‌ای دشمن اتخاذ می‌گردند.(کلمنس ، ۱۹۹۹) بر اساس این تعریف به نظر می‌رسد که جنگ سایبری زیر شاخه ای از جنگ اطلاعاتی بوده و شامل اقداماتی است که در فضای سایبری در تقابل با فضا یا دنیای واقعی صورت می پذیرد. بستر جنگ سایبری عبارت است از هر سامانه واقعیت مجازی که دربرگیرنده مجموعه ای از رایانه ها و شبکه ها باشد. یکی از شاخص ترین محیط های جنگ سایبری، اینترنت و شبکه های (نظامی یا غیر نظامی) مرتبط می باشد که به نحوی اطلاعات را به اشتراک می گذارند. جنگ سایبری ارتباطی تنگاتنگ با مفهوم سایبرنتیک[۲] دارد که به معنای " دانش کنترل و ارتباط در انسان، حیوان وماشین" می باشد. امروزه اغلب سامانه های کنترل و ارتباط با استفاده از تراشه های حافظه و واحدهای ریزپردازنده خودکار شده و به هدفی ایده آل برای رزمنده سایبری تبدیل گشته اند که حیطه مطلق سایبرنتیک محسوب می شود. یک مزاحم الکترونیکی یا تروریسم سایبری از هر کجای دنیا قادر است به رایانه های موجود در یک شبکه متصل وارد شود. به دست آوردن جواز

---

[1]. Information Warfare

ورود به رایانه ها از طریق ارتباطات شبکه نسبتا آسان، ارزان و نوعا فاقد خطرپذیری کشف و دستگیری است.

انواع جنگ سایبری

جنگ سایبری به شیوه‌های مختلفی شکل می‌گیرد. که کارکرد و اساس اجرایی آنها از فرآیند پیچیده ای تبعیت می‌نماید. بنابراین مروری بر میزان امکانات و دایره اثرگذاری جنگهای سایبری درک عمومی را از جنگهای سایبری بیشتر می‌نماید جدول ۱ این فرایند را به وضوح بیان می‌کند

مولفه های کارکردی / نوع جنگ	امکانات	عملکرد	اثر گذاری
نفوذ سایبری	یک سامانه با کنترل نرم افزاری	تهاجم و دستکاری به شیوه نفوذ و یورش سایبری	اختلال در شبکه و سرریز شدن اطلاعات سیستم.
دستکاری سایبری	یک سامانه با کنترل نرم افزاری	به دست گرفتن کنترل سامانه‌ها از طریق نرم افزارهای مرتبط	ایجاد خرابی و خسارت در سامانه خاموش کردن سیستم ها و مختل کردن شبکه‌ها
تاخت سایبری	نرم افزار و پست های الکترونیکی	ارسال ویروسهایی برای حمله به سامانه و از بین بردن کارآیی آن	تخریب نرم افزارها و داده‌ها در یک سامانه
دستبرد سایبری	نرم افزارهای جاسوسی و پستهای الکترونیکی	سرقت پست الکترونیک به دست آوردن فهرست گذر واژه‌ها	انتقال، تخریب و یا تغییر و در اختیار گرفتن اطلاعات
عاملان سایبری غیر عمدی	اپراتورهای سایبری، نیروهای سایبری، رزمندگان سایبری	عمد و قصد و نیت جنگ سایبری	اثرگذاری بر برخی مواقع جدی می شود اما غیر عمدی است
عاملان سایبری عمدی	مخاطرات	اقدام غیر عمدی	تهدیدامنیت ملی
ویروس افکنی	افراد	وارد نمودن دستی یا الکترونیکی یک ویروس یا کد ویروس به سامانه ها	از بین بردن کارایی رقبا و سرقت اطلاعات آنها

نفوذگران و هکرها نیز در فرایند کارکرد تکاملی جنگ سایبری ابزار زیربنایی محسوب می-شوند تبیین روابط و میزان اثرگذاری هر کدام از این نفوذ گران در محیط تعاملی سایبری اهمیت دارد در این رابطه مطالعه مختصر نفوذ گذان مورد توجه قرار می گیرد.

انواع نفوذگران درجنگ سایبری

نفوذگران در فضای سایبر به طرق مختلف دسته‌بندی شده‌اند که معروف‌ترین آنها بشرح ذیل می‌باشد:

- گروه نفوذگران کلاه سفید[1]:کسی که بتواند ازسد موانع امنیتی یک شبکه بگذرد اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند. این افراد متخصصین شبکه‌ای هستند که چاله‌های امنیتی شبکه را پیدا و به مسوولان گزارش می‌دهند.
- گروه نفوذگران کلاه سیاه[2]: اشخاصی هستند که وارد کامپیوتر قربانی خود شده و به دستبرد اطلاعات، جاسوسی و یا پخش ویروس و غیره می‌پردازند.
- گروه نفوذگران کلاه خاکستری[3]: اشخاصی هستند که حد وسط دو تعریف بالا می‌باشند.
- گروه نفوذگران کلاه صورتی[4]: این افراد آدم‌های کم‌سوادی هستند که با چند نرم‌افزار خرابکارانه به آزار و اذیت دیگران اقدام می‌کنند.
- گروه نفوذ گران کلاه قرمز[5]: عده‌ای متخصص که اطلاعاتی نادرست را به شبکه های اینترنت وارد می‌کنند.

حملات نفوذگران عمدتا با قصد و منظورهایی صورت می‌گیرد شامل: شنود که در این روش نفوذ گر می‌تواند به شکل مخفیانه از اطلاعات نسخه برداری کند، تغییر اطلاعات که در این روش نفوذگر به دستکاری و تغییر اطلاعات می‌پردازد، افزودن اطلاعات که در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند و وقفه که در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

فنون جنگ سایبری

فنون متعددی در جنگ سایبری وجود دارد که در دو بخش نرم افزار و سخت افزار قابل اجرا هستند. هر کدام از بخشها بیانگر نوع نگاه خاصی به فضاو جنگ سایبری می باشد. در این رویکرد دایره اثرگذاری و کارکرد نرم افزار و سخت افزار جنگهای سایبری متفاوت است نگاهی به جدول ۲ این تفاوت را نشان می دهد

1 . White hat hackers
2 . Black hat hackers
3 . Gray hat hackers
4 . Pink hat hackers
5. Red hat hackers

نرم افزار	ویروس‌ها	نرم افزارهایی که پس از ورود به رایانه هدف نظیر ویروس های واقعی تکثیر و سبب سردرگمی نرم افزاری و با انتقال به محیط شبکه کل سامانه را مختل می¬نمایند
	اسب تروا	در دنیای دیجیتال یک بدافزار ضد امنیتی است که در ظاهری خوشایند مخفی و هنگام دریافت و باز نمودن یک فایل تصاویر و یا موسیقی دلخواه یک برنامه خطرناک در سیستم رها شده که می تواند کل دیسک را پاک و یا شماره کارت اعتباری و گذرواژه آن را به یک مقصد ناشناس ارسال نماید
	کرم	برنامه‌هایی که خود را مکررا تکثیر کرده و فضای حافظه را اشباع نموده و قادرند با تاخیر فعال شده و خود را در سراسر فضای شبکه تکثیر و سبب کند شدن سیستم گردند
	شنود	برنامه ای که کلیه مکالمات و تبادلات مالی را شنود و از این راه نام ها، شناسه ها و گذرواژه ها را به دست می آورد
	برنامه‌های رمزشکن	با استفاده از روش آزمون و خطای خودکار به کد و رمزسیستم ها دست پیدا کرده و نوع پیچیده توان بالقوه از کار انداختن سامانه حفاظتی سیستم های مورد حمله را دارد
	برنامه های برچسب	یک برچسب شناسایی را در یک رایانه (درایو راه انداز آن) نصب و آنرا برای نفوذ سایبری در آینده نشانگذاری می‌کنند
	بمب منطقی	قطعه کدهای مخرب جاسازی شده‌ای که با ایجاد صدا در زمان معین و یا هنگام انجام عمل خاصی منفجر شده و پس از رهایی در محیط سیستم اثرات نامطلوب نظیر تخریب BIOS[1] از خود به جای می‌گذارند
سخت افزار	میکروب	باکتری‌های زنده‌ای که بر روی مواد خاصی از قطعات سخت‌افزاری سیستم‌ها نظیر سیلیکون و پلاستیک رشد کرده و تکامل می‌یابند و اگر وارد تجهیزات الکترونیکی شوند مدارهای الکترونیکی و مواد عایق را خورده و سیستم را غیر قابل استفاده می‌نمایند
	نانو ماشین یا مورچه آتشین	روبات‌های بسیار ریزی که با انرژی خورشیدی کار می‌کنند و دارای حواس بینایی، بویایی، شنوایی و توان حرکت و انفجار بنا به دستور را دارا و قادرند از منافذ دستگاه های الکترونیکی وارد شده و مدارات الکترونیکی آنرا تخریب نمایند
	اخلال تراشه‌ای	تراشه‌های پیشرفته محتوی میلیون‌ها مدار الکترونیکی مجتمع که شرکت های سازنده قادرند به راحتی آنها را برای بروز نقص و یا حتی انفجار در زمان معین یا پس از دریافت یک سیگنال با فرکانس خاص برنامه ریزی نمایند
	درِ نفوذ یا درپشتی	مکانیسمی که در یک سیستم توسط سازنده آن تعبیه شده و راه عبوری به سیستم مورد نظر و عبور از گره‌های امنیتی عادی برای وی محسوب می شود
	بمب پالس الکترومغناطیسی	نیروهای ویژه پس از نفوذ به مناطق عقب دشمن می توانند در نزدیکی تجهیزات آسیب پذیر اقدام به تولید انفجار پالس الکترومغناطیسی نمایند که سیستم های رایانه ای و ارتباطی را در شعاع عمل خود مختل نماید
	پارازیت دهنده‌ها	ابزارهایی که در مراکز C4I، سامانه‌های پدافند هوایی، رادارها و سایر سلاح هایی که توسط رایانه کنترل می شوند
	فرکانس رادیویی پر انرژی	توسط فرستنده های رادیویی بر روی اهداف الکترونیکی ارسال و موجب اختلال در عملکرد آن می‌شوند
	دستگاه‌های الکترومغناطیسی ناپایدار	پالس‌هایی تولید می‌کنند که دارای طول موج بسیار کوچکی بوده و می‌توانند بر روی طیف وسیعی از ابزارهای الکترونیکی تاثیری شبیه صاعقه را ایجاد نمایند

تحلیل سناریویی جنگهای سایبری

سناریو ۱): اختلال در شبکه حمل و نقل و ترافیک شهری

چنانچه مهاجمی به سیستم مدیریتی شبکه‌های ارتباطی و حمل و نقل مترو که توسط سیستم های مکانیزه کنترل می‌شود، نفوذ و کنترل آن را بدست آورد، می‌تواند با دادن

[1]. Basic Input Output System.

برنامه‌ای اشتباه به سیستم‌های هدایت کننده باعث برخورد قطارها شود، چنین حادثه‌ای باعث کشته و مجروح شدن عده زیادی از مردم خواهد شد. بطور مشابه فرض کنید هدایت شبکه کنترل ترافیک در سطح شهر توسط مهاجمی هک شده و اطلاعات غلط در رابطه با ترافیک بخش‌های مختلف مخابره شود. مثلا در جایی از شهر که ترافیک عادی است اعلام کند که تصادفی رخ داده و راه بسته شده و رانندگان را به بخش دیگری از شهر هدایت کند که در آن نقطه از شهر، تصادفی واقعی صورت گرفته، در نتیجه تعداد زیادی از خودروها به یک منطقه پرترافیک وارد می شوند که باعث تصادفات و راه بندان شدید و هرج و مرج در شهر خواهد شد.

سناریو ۲): اختلال در شبکه برق کشور: زندگی روزمره امروزی وابستگی زیادی به سیستم برق-رسانی وجود دارد. فرضاً سیستم برق منطقه یا یک شهر که به کمک شبکه‌های رایانه‌ای کنترل می‌شود مورد تهاجم و یا حمله نفوذگران قرار گیرد و بطور کلی قطع و یا کنترل آن بدست مهاجمان افتد، در این صورت تمام سیستم‌های خدماتی، اضطراری و سیستم‌های خانگی و ... که وابسته به فعال بودن شبکه برق می باشند مختل خواهند شد. به‌عنوان مثال این اتفاق باعث از کار افتادن تمام سیستمهای بانکی، حمل و نقل و ارتباطات، کنترل ترافیک، برق منازل، آب‌رسانی و خدمات درمانی و... می‌شود که این عوامل جدا از احتمال خسارات جانی و مالی سبب نارضایتی و ترس و وحشت در مردم خواهد شد.

سناریو ۳) اختلال در شبکه‌های مالی و بانکی کشور: با توجه به این که کنترل و دسترسی به سیستم‌های خودپرداز و یا سامانه‌های پُز توسط سیستم مرکزی رایانه‌ای کنترل و هدایت می شود اگر هکری به این سیستم نفوذ کرده و کنترل آن را به‌دست گیرد، می‌تواند موجودی حساب‌های مختلف را جابجا کند یا کلمه عبور کاربران را تغییر دهد، این عمل برداشت از حساب بانکی را مختل و منجر به ترس مردم و بی‌اعتمادی و هجوم آنها به بانک-ها و اختلال در سیستم اقتصادی می شود.عدم کنترل سریع چنین وضعی و ادامه یافتن آن می‌تواند منجر به از بین رفتن اعتبار پولی و ارزی یک کشور در سطح جهانی شود.

سناریو ۴) اختلال در شبکه اطلاع رسانی کشور: در زندگی کنونی، صدا و سیما به عنوان یک رسانه قابل اعتماد و در دسترس همگان، با پخش خبرهایی از قبیل مسایل مهم روز سراسر دنیا، اخبار هواشناسی، وقوع حوادث و اتفاقات داخلی و خارجی، اطلاعیه های عمومی و بسیاری مسایل دیگر به یکی از مهمترین عناصر یک کشور تبدیل گشته است. حال در نظر

بگیرید، این رسانه ملی مورد تهاجم و یا حمله نفوذگران قرار گیرد و کنترل آن بدست مهاجمان بیافتد، برای مثال مهاجمان با اشاعه یک خبر دورغین مانند وقوع یک زلزله و یا درگرفتن یک حمله نظامی در مرزهای کشور و یا شیوع یک بیماری و ... از طریق یکی از منابع اطلاع‌رسانی گروهی مانند رادیو در سطح جامعه سبب ایجاد رعب و وحشت گردد. این امر سبب ایجاد واکنش های منفی فراوانی از قبیل هجوم به بانک ها،تعطیل شدن بازارها و مراکز خدمات رسانی، خروج افراد از شهرها و ... می شود که این اقدامات نتیجه‌ای جز اغتشاش و بی نظمی در سطح جامعه نخواهد داشت و بازگشت به وضعیت عادی و جلب اعتماد دوباره مردم امری دشوار خواهد بود

اثرات کلی فنون جنگ سایبری بر تجهیزات

نفوذ در ارتباطات فیبر نوری کمی پیچیده است اما نوارهای مغناطیسی در مقابل جنگ سایبر کاملا آسیب پذیر بوده و دیسک‌های سخت نیز مستعد پذیرش آسیب‌های جدی هستند. تکنیک‌های جنگ سایبری در ارتباطات ماهواره‌ای بسیار موثراند زیرا این سیستم‌ها عموما به کشورهای صاحب فناوری ماهواره وابسته‌اند و فناوری ارسال و دریافت آن علیرغم استفاده از سیستم رمز آسیب‌پذیر است. سیستم های ارتباطی ماکروویو در ماهیت ایستا بوده و لذا با استفاده از تجهیزات سد کننده به سادگی قابل سد شدن هستند. بمب‌های پالس الکترومغناطیسی تاثیرات مخربی بر این تجهیزات دارند.

مفهوم جنگ سایبری به دنبال ظهورفناوری های عصر اطلاعات نظیر ماهواره، پست الکترونیک، اینترنت، رایانه و سایر ریزتراشه ها و تبدیل جهان به یک دهکده مطرح گردیده است. جنگ سایبری هر سه ضلع مثلث دولت، ملت و نیروهای مسلح را شامل می شود و یکی از بارزترین تهدیدات ناهمطراز می‌باشد. حملات سایبری در راستای عملیات روانی، تروریسم و خرابکاری قلمداد می‌شود و به دلیل ارزانی ابراز فناوری اطلاعات در مقایسه با سایر فناوری‌های حوزه دفاع، احتمال بهره‌برداری از جنگ سایبری در جنگ‌ها بسیار افزایش یافته است. چنین حملاتی را تروریست‌ها برای گسترش وحشت، خلافکاران برای کسب درآمدهای نامشروع و یا دولت- ملت[1] خاص برای رویارویی با دشمن به‌کار می‌گیرند. این جنگ نه تنها وب‌سایت‌های بخش‌های دولتی و خصوصی دشمن را مورد حمله قرار می‌دهد،

[1]. Nation- state

بلکه هدف‌های با ارزش‌تر نظیر شبکه‌های کنترل تاسیسات و تجهیزات نظامی را نیز مد نظر دارد. برخی از مصادیق جنگ سایبری عبارتند از:

۱- انفجار و یا نقص در سیستم تسلیحات نظامی به دلیل خرابی رایانه‌ها.

۲- قطع کامل سیستم های تلفن و منابع تغذیه الکتریکی.

۳- استفاده از اینترنت (سایت‌های خبری عمده) برای انتشار اخبار دروغین یا از کار انداختن منابع خبری اینترنتی.

۴- ایجاد محرومیت از امکانات مخابراتی و ارتباطی.

۵- مختل نمودن سیستم کنترل ترافیک و حمل و نقل هوایی و ریلی.

سامانه‌های نظامی که به نوعی به رایانه‌ها متکی هستند در برابر جنگ سایبر آسیب‌پذیرند که نمونه‌هایی از آن عبارتند از: سامانه‌های فرماندهی و کنترل مکانیزه (C4ISR)- سامانه-های مخابراتی و ارتباطی- سامانه‌های مراقبت و هشدار دهنده-سامانه‌های جنگ الکترونیک دستگاه‌های رمزکننده/ رمزگشا- شبکه‌های رایانه‌ای نظامی- سیستم‌های سلاح(سامانه‌های سلاح مدرن در توپخانه، زرهی، پدافند هوایی، پیاده و هوانیروز که برای تعیین موقعیت دشمن و اهداف، تعیین برد یا فاصله، رهگیری، آتش و سایر اعمال به رایانه متکی باشند اهداف خوبی را برای جنگ سایبری تشکیل می‌دهند). تعدادی از این موارد عبارتند از: کشف راداری، کنترل و هدایت موشک‌ها، کنترل آتش، شناسایی دوست از دشمن[1] و اطلاعات حاصله از سیستم موقعیت یاب جهانی(GPS).

تهدیدات جنگ سایبری می‌تواند دامن‌گیر بخش‌های مختلف خصوصی و دولتی در هر کشور شود. سرقت اطلاعات راهبردی، اقتصادی، نظامی و یا تخریب، از کاراندازی سرویس‌ها و خدمات عمومی یا خصوصی می‌تواند نمونه‌ای از نتایج جنگ سایبری باشد.

در حوزه فناوری اطلاعات زیرساخت شبکه‌های الکترونیکی، سوئیچ‌های مخابراتی و مراکز داده به عنوان یکی از اهداف اصلی در لحظات اولیه تهاجم در جنگ های اخیر مورد توجه ویژه قرار داشته است، لذا بایستی طراحی، مهندسی، پیاده سازی و بکارگیری آنها را در تمامی سطوح مدیریتی بصورت هوشمندانه عمل نمائیم. امروزه با گره خوردن فناوری اطلاعات در ماموریت تمامی دستگاه‌های اجرایی کشور حتی کوچکترین عملکردهای اجرایی، قابلیت‌های ممتازی را در مأموریت آنها اضافه نموده است به نوعی که شاهدیم

---

[1].IFF

توسعه این زیرساخت همواره به عنوان افتخارات مدیران در ارائه گزارش های پیشرفت عملکرد آن‌ها ارائه می گردد. این در حالیست که اگر این توسعه با مشاوره امنیتی مناسب و رویکرد صحیح از شناخت تهدیدات تخصصی آن حوزه نباشد در زمان بحران و شرایط اضطرار، انتظار می‌رود فناوری به کمک مدیر آمده و بالابردن توان مدیریت را در این شرایط تسهیل نماید. اما بدلیل عدم عملکرد صحیح و خارج شدن از مدار و همچنین جایگزینی سیستم‌های سنتی از چرخه عملکرد، شرایط پیچیده‌ای از بحران را رقم خواهد زد که اساتید حوزه مدیریت بحران از آن تحت عنوان هم افزایی بحران‌ها و تبدیل یک بحران کوچک به بحران منطقه‌ای یا ملی یاد می‌کنند. بنابراین به کلیه مدیران ارشد دستگاه‌های اجرایی کشور توصیه می‌شود دانش و آگاهی خود را در حوزه ماهیت تهدیدات نوین بر علیه زیرساخت‌های مراکز ثقل توسعه داده و بر اساس آن طرح های توسعه‌ای خود را تدوین نمایند. به این ترتیب فضای سایبر در برگیرنده بخش اعظم محیط کارکردی دنیای مدرن خواهد بود و هرگونه درگیری در آن به شدت پر اهمیت تلقی می گردد.

وقوع جنگ سایبری

متخصصان امنیت ملی ایالات متحده، جمهوری اسلامی ایران را در فهرست کشورهایی که در آسیا دارای عناصر آموزش دیده در زمینه جنگ سایبری می باشد بعد از چین و هند قرار داده اند. رهبران در تهران که سالیان دراز از بی بهره‌گی ایرانیان از دانش مکفی در زمینه فناوری جنگ اطلاعاتی رنج برده اند بر سازمان دهی گروه های دولتی در این زمینه همت گماشته و اگرچه مسئولان این کشور تاکنون در بیان موضوعات جانب احتیاط را نگه داشته‌اند اما هرگز دست از تلاش اقتصادی و سیاسی برای گسترش فناوری نوین در بخش دفاع فروگذار ننموده اند. (Billo, 2004) آنان حداقل در دو زمینه فعالیت نموده اند:

۱- نیروهای مسلح و دانشگاه های صنعتی تلاش مشترکی را برای ایجاد مراکز تحقیق و توسعه مستقل در زمینه فناوری اطلاعات و آموزش مهارتهای مرتبط به عمل آورده اند.

۲-ایران برای خرید فناوری اطلاعات و ملزومات فناورانه و آموزشی آن از روسیه و هند تلاش نموده است. روی‌هم‌رفته به‌نظر می‌رسد ایران منابع خود را در زمینه سلاح‌های نامتعارف و بخش فناوری اطلاعات به‌منظور کسب قدرت و اعمال نفوذ بیشتر در آسیای مرکزی مصروف داشته است.

بررسی نظریه فوق در خصوص توانمندی ایران و چند کشور منطقه در زمینه جنگ اطلاعاتی و سایبری و مرور وقایع معاصر در این زمینه نشانگر آن‌است که احتمال استفاده از

تسلیحات نامتعارف همواره با موانع محدودکننده بین‌المللی کاهش یافته و جنگ‌های تمام عیار نیز جای خود را به جنگ‌های محدود سپرده و توجه ارتش‌های جهان به‌سوی کاربرد مبانی جنگ‌های ناهمطراز معطوف گردیده و بسیاری از دولت - ملت‌ها ترجیح می‌دهند به جای درگیری واقعی قدرت نمایی نموده و بازدارندگی را تقویت نمایند.جنگ سایبری اولین بار در سال ۱۹۹۱ در جنگ اول خلیج فارس توسط ارتش امریکا مورد استفاده قرار گرفت. در آن جنگ به‌صورت بسیار ابتدایی از روش جنگ سایبری برای شنود پست الکترونیکی فرماندهان عراقی استفاده به‌عمل آمد. هم‌چنین در نبرد هوایی ۷۸ روزه امریکا و متحدانش بر علیه یوگسلاوی، پنتاگون به سیستم پیشرفته رایانه‌ای پدافند هوایی بلگراد نفوذ و پیام‌ها و اطلاعات جعلی ارسال نمود[1]. در حالیکه بسیاری از کشورهای منطقه در حال توسعه زیرساخت‌ها و توانمندی‌های فناوری اطلاعات خود هستند ارتش‌ها نیز به فراخور جایگاه اجتماعی‌شان در کشورهای مختلف در حال توسعه فناورانه خود می‌باشند.(Ibid)

ایده کلی درباره گسترش جنگ سایبری بر این موضوع استوار است که هر طرف که از آخرین دستاوردهای فناوری برخوردار بوده و فشار بیشتری بر دشمن وارد آورد و موفق به ایجاد اختلال در سامانه‌های مخابراتی رقیب در محیط سایبر گردد نیمی از جنگ را از پیش برده است. اکنون که کشورهای منطقه در حال توسعه سامانه‌های مرتبط با فضای سایبر می‌باشند، در این میان اسرائیل و متحدین وی در منطقه از قویترین تهدیدات سایبری برای سایر کشورهای منطقه می‌باشند.

مصداق‌های عینی جنگ سایبری

الف)جنگ بین روسیه و گرجستان: در ساعات آغازین آتش این جنگ در فضای سایبر روشن شد. بسیاری از سرورهای شبکه انفورماتیک گرجستان، کمی قبل از آغاز عملیات نظامی روسیه به مناطق استقلال طلب اوستیای جنوبی، مورد حملات کنترل از راه دور قرار گرفت. در شرایطی که سایت وزارت امور خارجه و وزارت دفاع زیر حملات هکرها قرار داشتند، سایت رسمی میخائیل ساکاشویلی رئیس جمهور گرجستان و شبکه‌های اصلی تلویزیونی این کشور هدف مستمر حملات عدم پذیرش سرویس بودند. در حملات عدم پذیرش

[1]. Jon Dougherty, "U.S. developing cyber-warfare capabilities, Threats range from teen hackers to sophisticated nation-states", www.WorldNetDaily.com

سرویس[1] به علت ارتباط بیش از حد با پایگاه اینترنتی مورد نظر، سرویس جوابگو نبوده و کاملا مسدود می‌گردد. سایت‌های گرجستان که تحت این حملات قرار داشتند به‌روزسازی-ها و اخبار جدید را دریافت نمی‌کردند. حکومت گرجستان این تهاجمات انفورماتیکی را مربوط به پاسخ مسلحانه به روسیه و درگیری‌های اوستیای جنوبی دانست. در این راستا، موسسه تحقیقاتی آمریکایی یو.اس.سورت که برای وزارت امنیت امریکا کار می‌کند پس از کنترل و بازبینی یک حمله (DOS) را در سرور سایت رئیس جمهور گرجستان شناسایی کرد.

ب) جنگ ۳۳ روزه اسرائیل و حزب ا...لبنان: در حالی‌که آمریکا، اسرائیل، متحدان اروپایی آنها و برخی از سران سازش‌کار عرب، در آغاز جنگ ۳۳ روزه با قاطعیت و اطمینان از نابودی حداکثر سه روزه حزب الله سخن می‌گفتند، به دلیل عدم توجه اسرائیل به تکنیک های دفاع غیرعامل و برتری حزب‌الله در نبردهای اطلاعاتی با بکارگیری تکنیک‌های پدافند غیرعامل در حوزه IT و استفاده از ابزارآلات و تجهیزات بومی موجب ناکامی اسرائیل در دستیابی به اهداف خود شدند. تهدید سایت‌های اینترنتی طرفین، حملات متناوب DOS، شنود و جاسوسی از جمله اقدامات در حوزه فضای سایبری جنگ ۳۳ روزه می‌باشد.

ج) جنگ بین روسیه و استونی: در آوریل سال ۲۰۰۷ هکرهایی که از طرف دولت روسیه حمایت می‌شدند، حملات سایبری را شروع که طی آن وب سایت های احزاب سیاسی، بانک ها، روزنامه‌ها و وزارتخانه‌های استونی به مدت حدود ۳ هفته مورد حمله قرار گرفت. این حملات از زمانی آغاز شد که در استونی تصمیم گرفته شده بود مجسمه برنزی شکست اتحاد جماهیر شوروی سابق در جنگ جهانی دوم در تالین ویران شود .

تحلیلگران، شبکه هکرهای روس را مسئول این حملات دانسته اند به طوری که یارت آرمین کارشناس انفورماتیکی توضیح داده است سرورهایی که از آنها این حملات انجام می شود تحت کنترل شبکه کسب و کار روسیه (شبکه هکرهای جنایتکار روسیه) است. این شبکه به شدت از سوی دولت روسیه حمایت می شود.

چ) جنگ بین آمریکا و چین : نزدیک به یکصد حمله سایبری بین آمریکا و چین درگرفته است که مشهورترین آنها در مارس و آوریل سال ۲۰۰۱ بوده است و دامنه های آن تا حدودی به اروپا نیز کشیده شد. این جنگ بر سر موضوع برخورد هواپیمای جاسوسی

[1] . Denial of Service

آمریکا با جت چینی بوده است. با حمله های DOS به سایت دولتی چین آغاز گردید (www.travelsichuan.gov.cn) و در نهایت این حملات منجر به تخریب اطلاعات، دزدیدن و صدمه به منافع و سرورهای دو کشور شد.گفته شده درصد تخریب حاصل از این جنگ در چین، ۱۰ برابر آمریکا بوده است.

ابزارحملات سایبری(بدافزارها[1])

الف)استاکس‌نت (Stuxnet): استاکس‌نت یک بدافزار رایانه‌ای (وُرم یا تروجان) است که اولین‌بار در تاریخ ۱۳ ژوئیه ۲۰۱۰ توسط ضدویروس وی‌بی‌ای۳۲ شناسایی شد. این بدافزار با استفاده از نقص امنیتی موجود در میانبرهای ویندوز، با آلوده کردن رایانه‌های کاربران صنعتی، فایل‌های با قالب اسکادا که مربوط به نرم‌افزارهای wincc و pcs7 شرکت زیمنس می‌باشد را جمع‌آوری کرده و به یک سرور خاص ارسال می‌کند. براساس نظر کارشناسان شرکت سیمانتک، این بدافزار به دنبال خرابکاری در تأسیسات غنی‌سازی اورانیوم نطنز بوده‌است. در اواخر ماه مه ۲۰۱۲ رسانه های آمریکایی اعلام کردند که استاکس‌نت مستقیماً به دستور اوباما رئیس جمهور آمریکا طراحی، ساخته و راه‌اندازی شده.گرچه در همان زمان احتمال این می‌رفت که آمریکا تنها عامل سازنده نباشد. در ژوئیه سال۲۰۱۳ میلادی، ادوارد اسنودن اعلام کرد این بدافزار با همکاری مشترک آمریکا و اسرائیل ساخته شده است. در جدول زیر کشورهای مورد هجوم و میزان تاثیر این بدافزار بر سیستمهای مورد استفاده آورده شده است:

کشور	کامپیوترهای آلوده شده
ایران	۵۸,۸۵٪
اندونزی	۱۸,۲۲٪
هند	۸,۳۱٪
آذربایجان	۲,۵۷٪
ایالات متحده	۱,۵۶٪
پاکستان	۱,۲۸٪
دیگر کشورها	۹,۲٪

ب) استارس[2]: ویروس استارس یک ویروس رایانه‌ای است که در آوریل ۲۰۱۱ در ایران شناسایی شد. این ویروس که از خانواده استاکس‌نت دانسته می‌شود، خود را در میان

[1]. malwares
[2] . Stars

پرونده‌های پی‌دی‌اف مخفی می‌کند. به گفته رئیس سازمان پدافند غیر عامل ایران، استارس ممکن است با فایلهای اجرایی سازمان‌های دولتی ایران اشتباه گرفته شود.

ج) بدافزار شعله[1]: که به عنوان Flamer و یا Sky wiper نیز شناخته می‌شود قطعه پیچیده‌ای از یک بدافزار کامپیوتر است که رایانه‌های با سیستم‌عامل ویندوز را مورد حمله قرار می‌دهد. این بدافزار از سال ۲۰۰۶ شروع به فعالیت کرده‌است و برای جاسوسی اینترنتی و تخریب اطلاعات مهم در کشورهای خاورمیانه و اروپای شرقی استفاده می‌شود. این بدافزار در ۲۸ می۲۰۱۲ بوسیله تیم واکنش سریع به مشکلات رایانه‌ای ایران، آزمایشگاه کسپراسکای، و آزمایشگاه CrySys دانشگاه تکنولوژی و اقتصاد بوداپست کشف شد. بررسی‌های اولیه نشان می‌داد که بیشترین آلودگی به ترتیب رایانه‌ای کشورهای ایران ۱۸۹ رایانه، اسرائیل ۹۸ رایانه، سودان ۳۲ رایانه را تحت تاثیر قرار داده است. با توجه به برآوردهای کسپراسکای، فلیم حدود ۱۰۰۰ ماشین را آلوده کرده‌است.

چ) اِشِلون[2]: اشلون نام یک شبکه اطلاعاتی برای جمع‌آوری و تحلیل داده است که از جانب پنج کشور امضاکننده پیمان اوکاسا (استرالیا، کانادا، نیوزیلند، بریتانیا و ایالات متحده آمریکا) اجرا می‌شده و بر طبق اسنادپارلمان اروپا، برای نظارت بر ارتباطات نظامی و دیپلماتیک اتحاد جماهیر شوروی و هم‌پیمانانش در بلوک شرق در زمان جنگ سرد و اوایل ۱۹۶۰ میلادی پایه‌گذاری شده است. پارلمان اروپا در گزارش خود در مورد پروژه اشلون که در سال ۲۰۰۱ میلادی منتشر شد نتیجه‌گیری می‌کند که بر پایه اطلاعات موجود اشلون این توانایی را داشته است که تماس‌های تلفنی، دورنگارها، ایمیل‌ها و دیگر تحرک جهانی داده‌ها که از طریق انتقال ماهواره‌ای، شبکه‌های تلفن عمومی و مایکروویو جابجا می‌شده‌اند را رهگیری و محتوایشان را بررسی نماید.

نقاط ضعف دفاع سایبر

در بند ۱۱ سیاست‌های کلی نظام در خصوص پدافند غیرعامل (ابلاغی از سوی مقام معظم رهبری) چنین آمده است: اصول و ضوابط مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ایسرقت اطلاعات استراتژیک اقتصادی، نظامی‌و یا تخریب و از کاراندازی سرویس‌ها و خدمات عمومی یا خصوصی می‌تواند نمونه‌ای از نتایج جنگ سایبری باشد. در حوزه فناوری

---

[1] . Flame
[2] . Echelon

اطلاعات زیرساخت شبکه های الکترونیکی، سوئیچ های مخابراتی و مراکز داده به عنوان یکی از اهداف اصلی در لحظات اولیه تهاجم در جنگ‌های اخیر مورد توجه ویژه قرار داشته است، لذا بایستی در طراحی، مهندسی، پیاده‌سازی و بکارگیری آنها در تمامی سطوح مدیریتی، بصورت هوشمندانه اقدام نمائیم. به دلیل ویژگی‌های حملات سایبر و فضای سایبر مواردی‌که در دفاع بسیار حایز اهمیت بوده و مقوله دفاع را دچار چالش جدی می‌نماید شامل؛ بررسی هویت و مکان مهاجم، شناسائی نیت مهاجم، تشخیص حمله‌های از قبل طراحی شده، و بررسی و ارزیابی تلفات بعد از جنگ می‌باشند. با این رویکرد دفاع سایبری شامل بهره‌گیری از کلیه امکانات سایبری و غیرسایبری کشور به منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به‌موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری توسط متخاصمین سایبری اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم، گروه‌های تحت حمایت پنهان دولتهای متخاصم، جاسوسان سایبری، تروریستهای سایبری، مجرمین سازمان یافته، هکرهای دارای انگیزه سیاسی و امنیتی و سایر منشاءهای تهدید مطرح شده و رسیدگی فوری و موثر به منشاء و کلیه پیامدهای ناشی از تهاجم سایبری، می‌گردد. (پور ابراهیمی، ۱۳۹۲: ۱۲۲) بخشی از فعالیت-های نیروهای مسلح، حفاظت و حمایت از زیرساخت های سایبری کشور است که شامل زیرساختهای اقتصادی نیز می‌شود. براساس ابلاغ فرماندهی کل قوا سازمان دفاع غیرعامل کشور،اقدام به تشکیل قرارگاه دفاع سایبری و رصد تهدیدات سایبری علیه زیرساخت‌های امنیت ملی کشور از جمله زیرساخت‌های سایبری در عرصه اقتصادی نموده است. در این چارچوب، وظایف قرارگاه دفاع سایبری کشور، اعلام هشدارهای ملی در برابر تهدیدات امنیتی کشور، ایمن‌سازی زیرساخت های کشور نسبت به تهدیدات سایبری و ایجاد توان بازدارندگی در این حوزه و کمک به تولید نرم‌افزارهای بومی می‌باشد. در این رابطه، ساختار مشترکی بین وزارت دفاع، سازمان پدافند غیرعامل کشور، وزارت ارتباطات و فناوری اطلاعات ایجاد شده است تا مرکز دفاع سایبری بتواند پروژه‌ها و نرم افزارهایی را که عمدتاً کارکردهای زیرساختی دارند، با استفاده از ظرفیت دانشگاه‌ها، شرکت‌های خصوصی و محققین تولید کند. بر این اساس، رسالت قرارگاه دفاع سایبری اجرایی کردن سیاست‌های کلی نظام در رابطه با امنیت فضای تبادل اطلاعات است. در حال حاضر، تلاش می‌شود هماهنگی‌های لازم بین دستگاه-های متولی اصلی امنیت و دفاع کشور شامل وزارت اطلاعات، وزارت ارتباطات و فناوری

اطلاعات، وزارت دفاع، سازمان پدافند غیرعامل و سایر بخش ها مانند وزارت صنایع که می توانند در این زمینه مؤثر باشند، ایجاد شود. (شکوه،۱۳۹۱: ۱۱۴-۱۱۸)

رویکرد و اقدامات دیگر کشورها

امروزه دولت آمریکا بیش از پیش در باره موضوعات جنگ سایبر فعالیتهای سازمان یافته انجام می‌دهد و در این کشور دو دیدگاه در این راستا وجود دارد. یکی تهدیدات سایبر را یک مسئله امنیت ملی تلقی و معتقد است منافع ملی و زیرساختهای حیاتی را در معرض تهدید قرار می‌دهد. درنتیجه نیروهای نظامی باید مسئولیت مقابله با این تهدیدات را بر عهده گیرند. و دیگری با حضور نظامیان در این حوزه موافق نبوده و مسئولیت آنرا مربوط به نهادهای مدنی و نیروهای انتظامی مانند اف.بی.آی می‌دانند.(آذر و مسلمی، ۱۳۹۳ :۱۰۸) بسیاری از کشورها دارای نیروی سایبری معروف به ارتش سایبری هستند که در زمینه نبرد و دفاع سایبری فعالند اما رویکرد اصلی آنها در جنگ سایبری حمله سایبری است تا دفاع، چرا که در این حوزه حمله بهترین دفاع است.

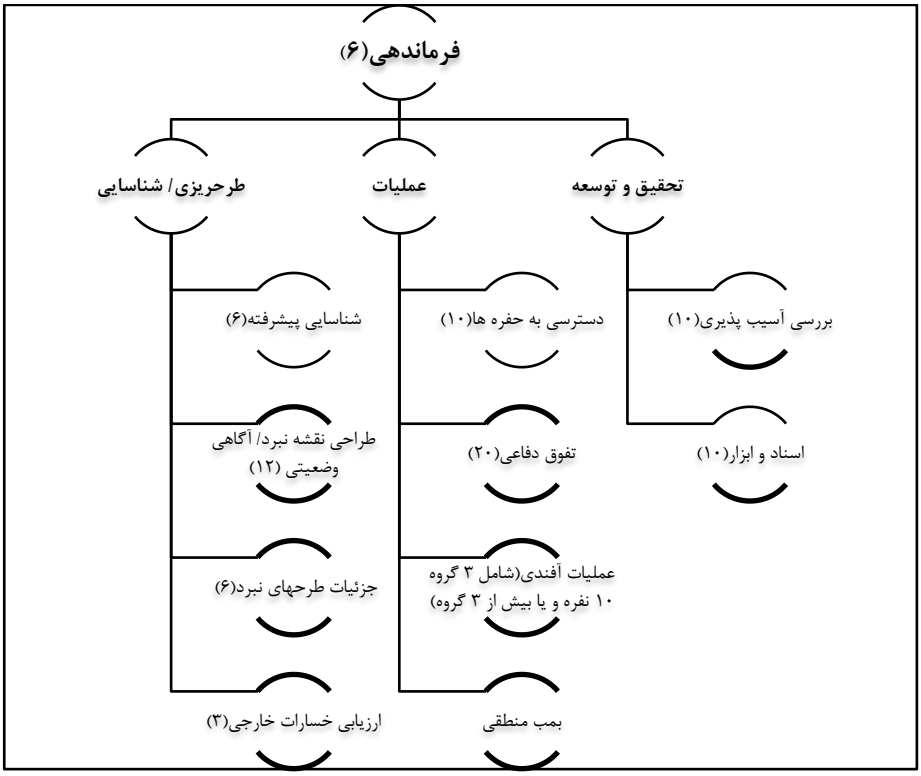
مؤسسه تکنولوژی دفاعی[1] از مؤسسات نظامی و امنیتی ایالات متحده آمریکا اقدام به انتشار مقاله ای با عنوان" ارزیابی ارتش سایبر ایران[2] " نموده است .در این مقاله ایران جزء پنج کشور دارای قوی‌ترین نیروی سایبری معرفی شده و تعداد نیروهای سایبری ایران ۲۴۰۰ نفر و ۱۲۰۰۰ نفر نیروی ذخیره برآورد شده است که دارای بودجه ۷۶ میلیون دلاری می باشد. سازمان سیا با اذعان به توانایی و ابتکار ایاران و همچنین برشمردن مشخصاتی از ارتش سایبر ایران اذعان می کند: با این آمارها می‌توان تا حدی توانایی علمی ایران در نبرد سایبر را تخمین زد. از دیگر گزارش‌های مشابه می‌توان به مقاله اخیر مجله "فارین پالیسی" (چاپ آمریکا) اشاره داشت که اقدامات نیروهای سایبری ایران علیه سایتهای مستهجن در را اقدامی بشردوستانه و به نفع حقوق بشر معرفی کرده است

در دنیای امروز با تسلط دنیای غرب بر عناصر اصلی سایبری مانند بسترهای ارتباطی (فیبرهای نوری، ماهواره ها) و اتصال دهنده‌ها در روترهای اصلی در اینترنت، متاسفانه احتمال تسلط دنیای اسلامی در ۱۰ سال آینده بسیار دور از ذهن است. شاید زمان آن باشد تا دنیای اسلام، علاوه بر تقابل آشکار فیزیکی دست به جنگ سایبری علیه صهیونیسم بزند و در این راستا مسلمانان باید دارای علم و آگاهی بیشتری نسبت به مقوله جنگ در فضای

---

[1]. Defense Tech
[2]. Iranian cyber warfare assessment

سایبری بوده و سربازان خود را آموزش دهند. الگوی ۱ نمونه ای از شمای سازمانی یک گردان سایبری را بیان می نماید:



مدل ۱) شمای سازمانی یک گردان سایبری

نتیجه گیری

روند روبه‌رشد و سرعت بالای تاثیر انقلاب اطلاعاتی و درپی آن رسوخ کاربرد ابزار و تجهیزات سخت و نرم‌افزاری دنیای دیجیتال در تمامی عرصه‌های زندگی بشر، امر گریزناپذیری شده و کاربران فضای سایبر همواره روزافزون می‌شوند. جنگ سایبری یکی از قلمروهای مطرح در عرصه برخوردهای بین‌المللی در سالهای آغازین هزاره سوم بوده و فرصت ها و تهدیدهای قابل توجهی را در عرصه امنیت ملی و دفاع مطرح نموده است. بدون شک عدم توجه کافی به این زمینه، تهدیدها را بالفعل نموده و باعث از دست رفتن فرصت ها خواهد شد. در فضای سایبر که تقریبا تمام بستر و ابزار آن توسط دشمن طراحی و ساخته شده، وابستگی فناورانه به کشورهای بیگانه بالاترین تهدید و تلاش در زمینه به حداقل رساندن وابستگی سایبری بالاترین اولویت در راهبرد جنگ سایبری است. بنابراین

تشکیل هسته های سیاست گذاری در سطح ملی و ساختارهای واکنش سریع در حوزه دفاع از اهم امور است. آن چه که امروز بسیار اهمیت دارد استفاده از زمان و تسریع در طرحریزی جنگ سایبری در سطح ملی و با تاکید بر نیروهای مسلح می باشد.

برخی اقداماتی که می‌تواند تا حدودی آسیب‌پذیری (نیروهای مسلح) جمهوری اسلامی ایران را در جنگ آینده در برابر حملات سایبری کاهش دهد به شرح زیر پیشنهاد می‌گردد:

- **آگاه‌سازی سایبری:** همگام با پیشرفت فناوری اطلاعات، آسیب‌پذیری ها نیز افزایش یافته و نیاز به ارتقای آموزش و دانش سایبری کارکنان نیروهای مسلح بیش از پیش گردیده است. برای این مهم لازم است سرفصل‌های آموزشی مرتبط با موضوع در مراکز آموزشی و دانشگاه های نیروهای مسلح در همه مقاطع گنجانیده شود. همچنین اهمیت موضوع در بخش‌های تحقیق و توسعه سازمان‌ها و یگان‌های نیروهای مسلح تبیین و تحقیقات مرتبط با مقولات جنگ های نوین دارای اولویت گردند.
- **ایجاد امنیت در شبکه:** اقدامات تامینی لازم برای محافظت از سیستم های ارتباط و مخابرات نیروهای مسلح به عمل آمده و روشهای اثربخش برای جلوگیری از ورود عوامل غیر مجاز، کشف حملات سایبری، ریشه کن کردن ویروس ها، کرمها و سایر عوامل مزاحم به سیستم‌ها به مورد اجرا گذارده شود. طرح تامین لازم برای مقابله با حملات سایبری که در برگیرنده خط مشی‌های لازم برای مقابله با شرایط قابل پیش‌بینی و غیر قابل پیش-بینی موجود و مبتنی بر طرح های امنیت ملی تدوین گردد. تجهیزات الکترونیکی و مخابراتی توسط متخصصین خبره و متعهد داخلی به دقت بازبینی گردد تا از عاری بودن آنها از آلودگی های پیش گفته اطمینان حاصل گردد.
- **خودکفایی تجهیزاتی:** برای دستیابی به امنیت واقعی چاره‌ای جز اجتناب از واردات تجهیزات خارجی و اتکا به تولیدات بومی رایانه، وسایل مخابراتی و سیستم های تسلیحاتی و نظایر آن وجود ندارد. علاوه برآن نیاز به سرمایه‌گذاری در بخش نرم افزارهای بومی نیز بسیار ضروری به نظر می رسد.
- **رویکرد آفندی جنگ سایبری:** نقاط ضعف سیستم های مخابراتی و الکترونیکی دشمن را باید شناسایی نموده و در حوزه جنگ سایبری رویکرد فعال را اتخاذ و تجربه و تبحر کافی را در زمینه به‌کار گیری ابزار و روشهای جنگ سایبری را کسب نمود.

- **آموزش خبرگان نفوذگر:** در زمینه آموزش و تربیت خبرگان نفوذگر در سیستم‌های الکترونیکی و مخابراتی، لازم است اقدامات جدی در مراکز آموزش فرهنگی نیروهای مسلح به عمل آید.
- **هماهنگی اقدامات جنگ سایبری در بالاترین رده:** اهمیت جنگ سایبری ایجاب می‌نماید که هماهنگی‌های لازم برای اتخاذ تدابیر لازم در سطح ملی و با مشاورت خبرگان نظامی صورت پذیرد. در این رابطه تشکیل یک هسته سیاست‌گذاری در سطح ملی با عنوان شورای عالی فضای مجازی کشور شکل گرفته و لازم است نقش و جایگاه آجا نیز در این شورا تعیین گردد . در هر صورت آنچه که از اهمیت بالایی برخوردار است دستیابی به یک راهبرد ملی در زمینه جنگ سایبری است که تابعی از راهبرد دفاعی کشور باشد.
- **شناسایی و به کارگیری کلیه امکانات بالقوه سایبری در کشور:** شرکت‌های پیشرو در تولید نرم-افزار، دانشگاه‌ها و مراکز صنعتی ، مراکز تحقیقاتی صنعتی و غیرصنعتی، جشنواره‌های علمی معتبر، همایش‌ها و نمایشگاه‌های تخصصی و نظایر آن بستر و زمینه‌های علمی و فنی مورد نیاز کشور را اداره و ارائه می نمایند که لازم است در راستای نیازمندی‌های نیروهای مسلح شناسایی و از آنان بهره برداری به‌عمل آید. ترکیبی از خبرگان و متخصصین فناوری اطلاعات در نیروهای مسلح و بخش های یاد شده می تواند زمینه لازم برای تشکیل یک نیروی واکنش سریع سایبری را فراهم آورده و در موقع لزوم در اسرع وقت نسبت به انجام عملیات آفندی و یا پدافندی اقدام نمایند.
- **ایجاد ساختار مناسب در سطح نیروهای مسلح:** به منظور ورود در عرصه جنگ سایبری و هماهنگی عملیاتی، ایجاد ساختارهای هماهنگ کننده ستادی و یگانهای عملیاتی در همه سطوح نیروهای مسلح ضروری است.

منابع:

- آذر داود، مسلمی حسین؛ شناخت تهدیدات فضای سایبری و پدافند از آن، تهران، انتشارات دانشگاه فرماندهی و ستاد، ۱۳۹۳
- باقری، محمد حسن، جنگ آینده از منظر آماد و پشتیانی، فصلنامه علوم و فنون نظامی ، شماره ۱۱، ۱۳۸۴
- بل، دیوید، درآمدی بر فرهنگ های سایبر،ترجمه مسعود کوثری وحسین حسنی، تهران انتشارات جامعه شناسان، ۱۳۸۹

- پور ابراهیمی محمدرضا، پدافند ملی سایبر، دانشگاه عالی دفاع ملی، ۱۳۹۲
- "جنگ سایبری: روش ها، نیروها و سلاح های کشتار جمعی"، بیارد کلمنس ، میلیتاری ریویو، شماره ۷۹، سپتامبر ۱۹۹۹
- حفظ‌نیا محمدرضا، جغرافیای سیاسی فضای مجازی، انتشارات سمت، تهران، ۱۳۹۰.
- حسن بیگی ابراهیم، حقوق و امنیت در فضای سایبر، انتشارات دانشگاه عالی دفاع ملی، تهران، ۱۳۸۸
- دوران ، بهزاد، تاثیر فضای سایبر بر هویت اجتماعی ،پایان نامه دکتری ، دانشگاه تربیت مدرس ، دانشکده علوم انساتی،۱۳۸۱
- شکوه حسن، اقتصاد ودفاع ملی(چارچوبی برای مطالعه)، فصلنامه مطالعات راهبردی شماره۳، تهران، ۱۳۹۱
- شریفی هولاسو ، اسماعیل، پایان نامه کارشناسی ارشد جامعه شناسی ، تهران دانشگاه تربیت مدرس، ۱۳۸۷
- گلمنس بیارد، "جنگ سایبری: روش ها، نیروها و سلاح های کشتار جمعی" ، میلیتاری ریویو، سپتامبر ۱۹۹۹، شماره ۷۹.
- صدری ، محمدرضا ، کروبی، محمد تقی، ابعاد حقوقی محیط سایبر در پرتو توسعه ملی ، تهران، انتشارات بقعه،۱۳۸۴
- فصلنامه علوم و فنون نظامی، شماره‌های ۱۰و ۱۱، انتشارات دافوس، تهران، ۱۳۸۴
- نیروی هوایی و ماموریت فضای سایبر، موسسه آموزشی و تحقیقاتی صنایع دفاعی، مرکز آینده پژوهی علوم و فناوری دفاعی ، ۱۳۸۸
- Joint Vision 2020, Washington, DC: The Joint Chiefs of Staff Office
- http://www.gsc.army
- http://www.Trojan Horse Attacks.htm
- http://www.nanite , what is definition, nanomachines.htm
- Charles Billo & Welton Chang, "Cyber Warfare an analysis of the means and motivations of selected nation states", Institute for security technology studies at Dartmouth College., November ; 2004
- Jon Dougherty, "U.S. developing cyber-warfare capabilities, Threats range from teen hackers to sophisticated nation-states".
- http://www.WorldNetDaily.com/ WorldNet Daily US developing cyber-warfare capabilities.htm