فصلنامه علوم و فنون نظامی
زمستان ۱۳۸۵

مفهوم جنگ سایبری و کاربرد آن در جنگ آینده

اکبر توکل[۱]

چکیده

پیشرفت روز افزون فناوری اطلاعاتی و گستردگی ابزار و تجهیزات سخت افزاری و نرم افزاری، اشکال جدیدی از جنگ را پدید آورده است. مسلما به دلیل اجبار کشورها/ارتش ها در بهره برداری از آخرین دستاوردهای فناوری، شناسایی و ورود به موقع و صحیح در عرصه های نوین به یکی از دغدغه های طراحان و بازیگران حوزه راهبرد و دفاع تبدیل گردیده است. جنگ سایبری یکی از این مقوله هاست که در فضای مجازی بین تجهیزات ارتباطی، مخابراتی، شبکه های رایانه ای و سیستم های مبتنی بر رایانه با شدت تمام توسط کشورهای صاحب فناوری بر علیه سایرین در جریان است. شناسایی اجمالی این فضا و بررسی فرصت ها و تهدید های موجود هدف از نگارش این مقاله می باشد.

واژه های کلیدی: سایبر، الکترونیک، اطلاعات، رایانه، مخابرات، ارتباط، شبکه

۲- معاون پژوهش دافوس آجا

مقدمه:

"عملیات در قلمرو اطلاعات به اندازه عملیات در زمین، دریا، هوا و فضا واجد ارزش و اهمیت گردیده است."[1]

در طول تاریخ دکترین نظامی، سازمان و راهبرد کشورها تحت تاثیر فناوری های نوین همواره دستخوش تغییرو تحول بوده است. صنعتی شدن منجر به بروز جنگ فرسایشی اول جهانی گردید. حضور تانکها منجر به مانور مکانیزه در جنگ دوم جهانی گردید.

خیزش حاضر در فناوری اطلاعات سبب ظهور نوعی از جنگ گردیده است که در آن پیروز میدان نبرد کسی است که اطلاعات بیشتری دارد نه آن که تنها به تمرکز قوا و تحرک می اندیشد.

سامانه های ارتباطی و الکترونیکی پیچیده نوین، سناریوی نبرد آینده را تغییر داده اند. از یک سو این سامانه ها به فرماندهان در تصمیم سازی بر اساس تصاویر و اطلاعات زمان حقیقی نبرد کمک کرده و از سوی دیگر وابستگی به سامانه های الکترونیکی، ریز پردازنده ها و تراشه های حافظه آنان را در برابر جنگ سایبری بسیار آسیب پذیر نموده است.

واژه جنگ سایبری برای تشریح نوع جدیدی از جنگ که بر روی سامانه های ارتباطی و الکترونیکی دشمن متمرکز می گردد، ابداع شده است. در این جنگ نیازی به اعزام لشکرها یا ناوهای جنگی نبوده و به جای آن از ویروس های رایانه ای، بمب های منطقی و بمب های پالس الکترومغناطیسی استفاده می شود که قادراست خرابی های وسیعی در مدارات الکترونیکی سامانه های C4I، رادارها، رایانه ها، سلاح های هوشمند

[1] - Joint Vision 2020, Washington, DC: The Joint Chiefs of Staff Office, June 2000.

و سامانه های مراقبتی به وجود آورد. این نوع از جنگ مقدم بر جنگ واقعی بوده و حتی ممکن است قبل از شروع از وقوع آن جلوگیری کند.

کشورهای در حال توسعه به دلیل نداشتن تولیدات الکترونیکی پیچیده و سامانه های مرتبط و وابستگی عمیق به فناوری های خارجی آسیب پذیری بیشتری در این زمینه دارند. این امر سبب آسیب پذیری جدی آنان در برابر هر گونه تهدید سایبری نه تنها در برابر دشمنان بلکه در برابر عناصر نفوذگر داخلی و خارجی خواهد شد. بنابراین نیاز به آموزش مقوله این جنگ در ارتش شدیدا احساس می شود. تدوین یک راهبرد در زمینه شناخت و مقابله با تهدیدات جنگ سایبری نیز یکی از ضروریات می باشد.

تعاریف و مفاهیم جنگ سایبری:

۱- **جنگ اطلاعاتی**[1]: به اقداماتی اطلاق می گرددکه 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 می شوند. 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. "

۲- **جنگ سایبری**: عبارت است از "اقدامات آفندی غیر متحرکی که به منظور کسب برتری اطلاعاتی از طریق تحت تاثیر قراردادن سامانه اطلاعاتی و شبکه های رایانه ای دشمن اتخاذ می گردند."[2] بر اساس این تعریف به نظر می رسد که جنگ سایبری زیر

---

[1] -Information Warfare

۲–بیارد کلمنس فرمانده نیروی دریایی امریکا در سال ۱۹۹۹ ، "جنگ سایبری: روش ها، نیروها و سلاح های کشتار جمعی" ، میلیتاری ریویو، سپتامبر ۱۹۹۹، شماره ۷۹، صفحه ۳۵ که در آدرس اینترنتی زیر موجود می باشد.
http://www-cgsc.army.military/ milrev/English/sepoct99/clemen.htm, June 2002.

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. با درنظر گرفتن جنبه نظامی جنگ سایبری می توان آنرا جنگی در حوزه اینترنت قلمداد نمود.

۳- **فضای سایبری**[1]: فضای سایبری عبارت است از فضای غیر ملموس بین رایانه ها جاییکه داده ها یا اطلاعات بصورت لحظه ای در مسیر عبور از یک رایانه به رایانه دیگر درشبکه های محلی یا جهانی در آن یافت می شوند. این رایانه ها ممکن است برای مقاصدی نظیر ارتباط، هدایت سلاح ها، شناسایی و مراقبت یا اموری نظیر حسابداری و بانکداری مورد استفاده قرار گرفته باشند. این فضا همچنین شامل امواج حاصله از ابزارهای مخابراتی، ماکروویو و ارتباطات ماهواره های می شود. از آنجا که همه یگانهای نظامی در همه ارتش ها به نوعی به شبکه جهانی ارتباطات متصل هستند لذا همگی ساکنین فضای سایبری محسوب می گردند.

۴- **سایبرنتیک**[2]**:** جنگ سایبری ارتباطی تنگاتنگ با مفهوم سایبرنتیک 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.

---

[1] - Cyber Space

۲–در علوم رایانه ای معنای لغوی این کلمه "فرمانشناسی" است. و در اصل به معنای علم فرمانش، (فیزیولوژی) مطالعه ومقایسه بین دستگاه عصبی خودکارکه مرکب از مغز واعصاب باشدبادستگاه الکتریکی ومکانیکی است.

۵- **تروریسم سایبری[1]:** یک مزاحم الکترونیکی از هر کجای دنیا قادر است به رایانه های موجود در یک شبکه متصل وارد شود. به دست آوردن جواز ورود به رایانه ها از طریق ارتباطات شبکه نسبتا آسان، ارزان و نوعا فاقد خطرپذیری کشف و دستگیری است.

انواع جنگ سایبری

۱- **نفوذ سایبری[2]:** عبارت است از ایجاد رخنه در یک سامانه با کنترل نرم افزاری بنحوی که بتوان آن سامانه را مورد یورش، تهاجم و دستکاری قرار داد. یک روش نفوذ و یورش سایبری وارد کردن مقادیر بزرگی از اطلاعات به درون یک سامانه می باشد که سبب سرریز شدن اطلاعات سیستم و سقوط شبکه مربوطه می گردد.

۲- **دستکاری سایبری[3]:** به دنبال نفوذ سایبری به دست گرفتن کنترل سامانه ها از طریق نرم افزارهای مرتبط و به کاربردن آنها برای ایجاد خرابی و خسارت در سامانه را دستکاری سایبری می نامند. برای مثال استفاده از ابزارهای نرم افزاری برای خاموش کردن سیستم ها و مختل کردن شبکه ها مصداقی از دستکاری سایبری است.

۳- **تاخت سایبری[4]:** پس از انجام موفقیت آمیز یک نفوذ سایبری، تخریب نرم افزارها و داده ها در یک سامانه یا حمله به سامانه به نحوی که کارآیی آن از بین برود را تاخت سایبری می نامند. این تاخت هم چنین ارسال ویروسهایی را شامل می شود که از طریق پست الکترونیک اضافه بار زیادی را بر سامانه تحمیل می نمایند.

۴- **دستبرد سایبری[5]:** به دنبال یک نفوذ سایبری موفق ، هرگونه دستکاری یا در اختیار گرفتن اطلاعات یک سامانه که منجر به انتقال، تخریب و یا تغییر اطلاعات آن

---

[1] - Cyber Terrorism
[2] - Cyber Infiltration
[3] - Cyber manipulation
[4] - Cyber Assault
[5] - Cyber Raid

گردد را دستبرد سایبری گویند. برای مثال سرقت پست الکترونیک و یا به دست آوردن فهرست گذر واژه ها[1] از یک سرویس دهنده پست الکترونیک.[2]

۵- **عاملان سایبری عمدی:** افرادی هستند که به طور عمدی و با قصد و نیت جنگ سایبری را به مورد اجرا می گذارند. به این افراد هم چنین اپراتورهای سایبری، نیروهای سایبری، رزمندگان سایبری یا عده های سایبری نیز اطلاق می گردد.

۶- **عاملان سایبری غیر عمدی:** افرادی که به طور غیر عمدی در سامانه ها نفوذ می نمایند اما امنیت ملی را به مخاطره انداخته و عموما از مخاطرات ایجاد شده توسط اعمال خود آگاه نمی باشند.

۷- **ویروس افکنی:** عمل وارد نمودن دستی یا الکترونیکی یک ویروس یا کد ویروس به سامانه ها می باشد.

ویژگی های جنگ سایبری:

برجسته ترین ویژگی های جنگ در فضای اطلاعاتی به شرح زیر می باشند:

۱- **سرقت پنهان اطلاعات**: اطلاعات دارایی بی نظیری است که اگر به طور حرفه ای به سرقت رود تنها سارق است که می داند که این اطلاعات در دو نقطه وجود دارند. مالباخته چنین سرقتی در بی اطلاعی کامل به سر برده و سرنخی از ماجرا در دست نخواهد داشت. رزمنده سایبری بر روی سرقت اطلاعات تمرکز کرده و مخفیانه به سامانه هدف نفوذ می نماید. این عمل از طریق جاسوسی یا دزدی و هم چنین شکستن کدها و رمزهای ارتباطی و نظامی سامانه های هدف امکان پذیر می گردد.

[1] - Password list
[2] - Mail server

۲- **تغییر اطلاعات**: یک ویژگی دیگر در جنگ سایبری این است که رزمنده سایبری به جای سرقت اطلاعات ممکن است ترجیح دهد تا اطلاعات را در راستای دستیابی به اهداف خود تغییر دهد. کاربر ممکن است تا مدت ها به این موضوع پی نبرد.

۳- **تخریب اطلاعات:** اگر رزمنده سایبری توانایی تغییر و دستکاری اطلاعات را داشته باشد، مسلما توانایی تخریب آن ها را نیز خواهد داشت. بیشمار اتفاق افتاده است که اطلاعات موجود در یک رایانه به دلیل نواقص سامانه ای به طور تصادفی از بین رفته و با تخریب گردیده اند. این اتفاق ممکن است در اثر ورود یک ویروس رایانه ای جدید و یا به واسطه تاثیر پالس های الکترومغناطیسی حاصله از دستگا ههای الکترونیکی و الکتریکی در مجاورت سامانه به وجود آمده باشد.

۴- **تخریب تسهیلات اطلاعاتی:** سامانه های فرمان و کنترل نیروهای مسلح و سامانه های سطوح ملی عمیقا به اطلاعات و پایگاه داده های سازمان ها وابسته هستند. رزمنده سایبری بر اساس موقعیت، بهترین گزینه را در خصوص تخریب تسهیلات اطلاعاتی ارتش یا کشور هدف و یا از بین بردن کامل توانایی های دشمن در پردازش اطلاعات و ارتباط به نحوی که قبل از شلیک اولین گلوله از پا در آمده باشد را انتخاب می نماید.

۵- **دشواری ارزیابی و اخطار تک:** این ویژگی از جنگ سایبری جنبه دیگری از مشکلات اساسی موجود در فضای سایبری را بیان می نماید. مشکل اصلی این است که به سختی می توان بین یک حمله سایبری و سایر رویدادها نظیر اتفاقات، نقص سامانه، اشباع سامانه و یا حتی نفوذ تصادفی افراد معمولی تفاوتی قائل شد. استنتاج اصلی این ویژگی آنست که یک ملت یا سازمان ممکن است حتی نداند که مورد حمله واقع گردیده و یا اینکه حمله کننده کیست و یا روش حمله چه بوده است.

۶- **ورود ارزان:** متفاوت از فناوری سلاح های سنتی، نفوذ به سامانه های اطلاعاتی نیازی به سرمایه گذاری کلان اقتصادی و نظارت دولتی ندارد. تنها پیش نیاز رزمنده

سایبری، داشتن تبحر و خبرگی در سامانه ها و دسترسی به شبکه داده ها و اطلاعات مهم هدف است.

۷- **نامرئی بودن و عدم شفافیت مرزهای سنتی:** با وجود تعداد وسیعی از عوامل موثر در فضای جنگ سایبری ازجمله وجود طرفهای بسیار، سامانه های سلاح، وابستگی به فناوری و تجهیزات خارجی و احتیاج به خبرگان نرم افزاری؛ تشخیص بین تهدیدات داخلی و خارجی بطور روزافزون دشوارتر می شود. قربانی حمله سایبری ممکن است از حمله مطلع نشده و یا حمله ور را نشناسد و مزیت نامرئی و ناشناس بودن در محیط جنگ سایبر و عدم شفافیت قوانین حاکم بر آن سبب می شود که فنون جنگی بالقوه خطرناک به کار گرفته شده و بر خلاف محیط جنگ های سنتی حتی نتوان متجاوز را تنبیه نمود. نامرئی بودن الکترونیکی رزمنده سایبری امکان درگیری با اهداف بی شماری را به طور همزمان برای او فراهم می آورد. قدرت او بستگی به توان مودمی دارد که او را به شبکه های موجود در کشورهای هدف متصل می نماید.

۸- **رویداد انفجاری**: یکی از مهمترین ویژگیهای حمله سایبری اثرات انبوه یک رویداد بر روی یک سازمان یا کشور است. وقتی تنها یک نسخه از یک بمب منطقی در داده ها یا رایانه های یک سازمان رسوخ نماید می تواند سراسر شبکه ارتباطات راه دور یک کشور را مختل می نماید. دامنه تخریب یک بمب منطقی ممکن است حتی از این هم فراتر رفته و سایر سامانه های آن سازمان یا کشور را تحت تاثیر قرار دهد.

فنون جنگ سایبری:

فنون متعددی در جنگ سایبری وجود دارد که در دو بخش نرم افزار و سخت افزار قابل اجرا هستند.

الف: نرم افزار: این فنون همه کدها و برنامه های نرم افزاری مرتبط را شامل می شود که برخی از آنها به شرح زیر می باشد.

۱- **ویروس**: ویروس های رایانه ای برنامه های نرم افزاری هستند که پس از ورود به رایانه هدف نظیر ویروس های واقعی تکثیر کرده و زیاد می شوند. این امر سبب سردرگمی نرم افزار رایانه ای و نقص در سامانه می گردد. اگر رایانه در محیط شبکه باشد ویروس ها از آن طریق از یک رایانه به رایانه دیگر منتقل شده و کل سامانه را مختل خواهند نمود. ویروس ها می توانند از طریق ابزارهای آلوده نظیر دیسکت ها از یک رایانه به رایانه دیگر منتقل شوند. ویروس ها برای منظورهای متعدد وبا دامنه راهبردی حملات مشخص از اختلال موقت در اطلاعات خاص تا غیر فعال شدن دائمی روند ذخیره داده ها و حافظه اطلاعات در سامانه ها طراحی می گردند. یک ویروس محتوی دستوراتی برای وقوع تعدادی از رویدادها می باشد که بر عملکرد سیستم آلوده تاثیر نامطلوب دارد. این تاثیرات می توانند از کاملا بی ضرر تا کاملا مخرب ارزیابی شوند.برخی از این تاثیرات بدین شرح است:

- برنامه زمان زیادتری برای اجرا صرف می کند.
- عملیات مورد نیاز روی دیسک ها بیش از اندازه معمولی است.
- رجوع منابع سیستم به دیسک ها بدون دلیل و متناوبا تکرار می شود.
- شماره سریال دیسک تعویض می شود.
- فایل های پنهان و سکتورهای خراب روی دیسک زیاد می شود.
- اندازه فایل های اجرایی تغییر می نماید.
- تغییرات غیر منتظره در تاریخ و ساعت سیستم پدید می آید.
- حافظه آزاد سیستم کاهش محسوس پیدا می نماید.
- خطاهای غیر منتظره و متفاوت در سیستم مشاهده میشود[۱].

[۱]- مجله دنیای رایانه شماره ۱۴ صفحه 13

۲- **اسب تروا**[1]: در افسانه ها آمده است که سربازان یونانی با مخفی شدن در یک اسب چوبی عظیم الجثه و پیشکش آن به شهر تروا وارد شهر شده و آنان را شکست دادند. در دنیای دیجیتال یک اسب تروا عبارت از یک برنامه بدخواهانه ضد امنیتی است که در ظاهری خوشایند مخفی گردیده است. برای مثال هنگامی که یک فایل حاوی تصاویر و یا موسیقی دلخواه را دریافت و باز می نمایید یک برنامه خطرناک را در محیط سیستم رها کرده اید که می تواند کل دیسک شما را پاک کرده و یا شماره کارت اعتباری شما و گذرواژه آن را به یک مقصد ناشناس ارسال نماید.[2]

۳- **کرم**[3]: کرم ها برنامه هایی هستند که خود را مکررا تکثیر کرده و فضای حافظه و دیسک ها را اشباع می نمایند. گاهی کرم ها برای تکثیر از طریق شبکه طراحی شده و و قادرند با تاخیر فعال شده و خود را در سراسر فضای شبکه تکثیر نمایند. یک کرم یک برنامه مستقل است که قادر است خود را به صورت تصاعدی افزایش داده و از یک رایانه به رایانه دیگر در شبکه رسوخ نماید. کرم ها معمولا در صدد تغییر برنامه های دیگر نیستند و همچنین داده ها را تخریب نمی نمایند بلکه تنها در صدد آنند که منابع سیستم و شبکه را مصرف کرده و سبب افت سیستم گردند.

۴- **شنود**: برنامه ای است که کلیه مکالمات و تبادلات مالی را شنود و از این راه نام ها، شناسه ها و گذرواژه ها را به دست می آورد. برنامه های شنود و دیدبان، گذرواژه ها و اطلاعات با ارزش سیستم ها را گل چین و شکار می نمایند.

۵- **برنامه های رمزشکن**: این برنامه ها اولین برنامه های به کارگرفته شده در نفوذ سایبری بودند. ساده ترین شکل این برنامه هاباستفاده از روش آزمون و خطای

---

[1] - Trojan Horse
[2] - http://www.Trojan Horse Attacks.htm
[3] -Worms

خودکاربه کدورمزسیستم ها دست پیدا می نماید . برنامه های رمز شکن پیچیده توان بالقوه از کار انداختن سامانه حفاظتی سیستم های مورد حمله را دارند.

۶- **برنامه های برچسب**: این برنامه ها یک برچسب شناسایی را در یک رایانه نصب و آنرا برای نفوذ سایبری در آینده نشانگذاری می کنند. برخی از این برنامه ها قادرند تا برچسب را در درایو راه انداز سیستم نصب نمایند.

۷- **بمب منطقی**: یک بمب منطقی قطعه کدهای مخرب جاسازی شده ایست که با ایجاد صدا در زمان تعیین شده و یا هنگام انجام عمل خاصی در سیستم منفجر شده و پس از رهایی در محیط سیستم اثرات نامطلوب نظیر تخریب BIOS[1] از خود به جای می گذارند.

ب- سخت افزار:

۱- **میکروب:** میکروبها باکتری های زنده ای هستند که بر روی مواد خاصی از قطعات سخت افزاری سیستم ها نظیر سیلیکون و پلاستیک رشد کرده و تکامل می یابند. این باکتری ها اگر وارد تجهیزات الکترونیکی شوند مدارهای الکترونیکی و مواد عایق را خورده و سیستم را غیر قابل استفاده می نمایند.

۲- **نانو ماشین (مورچه آتشین):** این ماشین ها روبوت های بسیار ریزی هستند که با انرژی خورشیدی کار می کنند و دارای حواس بینایی، بویایی، شنوایی و توان حرکت و انفجار بنابه دستور را دارا می باشند. این روبوت ها قادرند از سوراخ های دستگاه های الکترونیکی وارد شده و مدارات الکترونیکی آنرا تخریب نمایند.[2]

۳- **اخلال تراشه ای:** تراشه های پیشرفته محتوی میلیونها مدار الکترونیکی مجتمع[3] هستند که شرکت های سازنده قادرند به راحتی آنها را برای بروز نقص و یا حتی انفجار

---

[1] - Basic Input Output System.
[2] -http://www.nanite- a what is definition, nanomachines.htm
[3] - Integrated Circuits. (IC)

در زمان معین یا پس از دریافت یک سیگنال با فرکانس خاص برنامه ریزی نمایند. حتی با ارسال فرکانس های خاص میتوان موقعیت دقیق استقرار این تراشه ها را در سازمان یا کشور هدف تعیین کرد. تنها مشکل باقیمانده حصول اطمینان از استقرار این تراشه ها در نزدیکی هدف مورد نظر رزمنده سایبری می باشد. ساده ترین راه کار تعبیه این ویژگی ها در کلیه تراشه های صادراتی به کشور هدف است.

۴- **درهای نفوذ:** یک در نفوذ یا درپشتی، مکانیسمی است که در یک سیستم توسط سازنده آن تعبیه شده است و راه عبوری به سیستم مورد نظر و عبور از گره های امنیتی عادی برای وی محسوب می شود. کلیه سیستم های سخت افزاری تولید ایالات متحده مجهز به سیستم درهای نفوذ می باشند به نحوی که به سادگی در جنگ اطلاعاتی بر علیه کاربران مورد استفاده قرار بگیرند.

۵- **بمب پالس الکترومغناطیسی**[1]**:** منبع پالس میتواند یک انفجار هسته ای یا غیر هسته ای باشد. 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 می نماید.

۶- **پارازیت دهنده ها:** ابزارهایی هستند که در مراکز C4I، سامانه های پدافند هوایی، رادارها و سایر سلاح هایی که توسط رایانه کنترل می شوند پخش شده و پارازیت یا صداهای باند کوتاه قوی را برای خراب کردن سیستم های حساس الکترونیکی تولید می نمایند.

۷- **فرکانس رادیویی پر انرژی**[2]**:** این فرکانس ها توسط فرستنده های رادیویی بر روی اهداف الکترونیکی ارسال و موجب اختلال در عملکرد آن می شود.

---

[1] - Electromagnetic Pulse (EMP) Bomb.
[2] - High Energy Radio Frequency (HREF)

۸- **دستگاه های الکترومغناطیسی ناپایدار**[1]: این دستگاه ها پالس های تیرک مانندی را تولید می کنند که دارای طول موج بسیار کوچکی بوده و می توانند بر روی طیف وسیعی از ابزارهای الکترونیکی تاثیری شبیه صاعقه را ایجاد نمایند.

اثرات کلی فنون جنگ سایبری بر تجهیزات:

نفوذ در ارتباطات فیبر نوری قدری پیچیده می باشد. نوارهای مغناطیسی در مقابل جنگ سایبر کاملا آسیب پذیر بوده و دیسک های سخت نیز مستعد پذیرش آسیب جدی هستند.

روش های جنگ سایبری در ارتباطات ماهواره ای بسیار موثر بوده زیرا این سیستم ها عموما به کشورهای صاحب فناوری ماهواره وابسته می باشد و فناوری ارسال و دریافت آن علیرغم استفاده از سیستم رمز آسیب پذیر است.

سیستم های ارتباطی ماکرویو در ماهیت ایستا بوده و لذا با استفاده از تجهیزات سد کننده به سادگی قابل سد شدن هستند. بمب های پالس الکترومغناطیسی تاثیرات مخربی بر تجهیزات دارند.

کاربرد سایبر در جنگ:

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 و به تعبیر نوتر چادر[2] مطرح گردیده است. جنگ سایبری هر سه ضلع مثلث دولت، ملت و ارتش را شامل می شود و یکی از بارزترین تهدیدات ناهمطراز می باشد. حملات سایبری در راستای عملیات روانی، تروریسم و خرابکاری قلمداد می شود. به دلیل ارزانی ابراز فناوری اطلاعات د ر مقایسه با سایر فناوری های حوزه دفاع، احتمال بهره برداری از جنگ سایبری در جنگ ها بسیار افزایش یافته است. چنین حملاتی را تروریست ها برای

[1] - The Transient Electromagnetic Devices (TEDs)
[2] - Global Village or Global Tent

گسترش وحشت، جنایتگران برای کسب درآمد های نامشروع و یا دولت- ملت خاص برای رویارویی با دشمن به کار می گیرند. این جنگ نه تنها وب سایت های موسسات و سازمانهای دولتی و بخش خصوصی دشمن را مورد حمله قرار می دهد بلکه هدف های با ارزش تر نظیر شبکه های کنترل تاسیسات و تجهیزات نظامی را نیز مورد نظر دارد. برخی از مصادیق جنگ سایبری عبارتند از:

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

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

۳- استفاده از اینترنت (همه سایت های خبری عمده) برای انتشار اخبار دروغین یا ازکارانداختن همه منابع خبری اینترنتی.

۴- ایجاد محرومیت از امکانات مخابراتی و ارتباطی.

۵- مختل کردن سیستم کنترل عبورو مرور هوایی و راه آهن.

۶- اهداف نظامی مهم: همه سیستم های نظامی که به نوعی به رایانه ها متکی هستند در برابر جنگ سایبر آسیب پذیر هستند که نمونه هایی از آن عبارتند از:

- سیستم های فرمان و کنترل مکانیزه (C4I)
- سیستم های مخابراتی و ارتباطی
- سیستم های مراقبت و هشدار دهنده
- سیستم های جنگ الکترونیک
- دستگاه های رمزکننده/رمزگشا
- شبکه های رایانه ای نظامی
- سیستم سلاح ها: سیستم سلاح های مدرن در توپخانه، زرهی، پدافند هوایی، پیاده و هوانیروز که برای تعیین موقعیت دشمن/هدف، تعیین برد/ فاصله، رهگیری، آتش و سایر اعمال به رایانه متکی باشند اهداف خوبی را برای جنگ سایبری تشکیل می دهند.

تعدادی از این موارد عبارتند از: جستجوی راداری، کنترل و هدایت موشک ها، کنترل آتش، شناسایی دوست از دشمن و اطلاعات حاصله از سیستم موقعیت یاب جهانی(GPS)

وقوع جنگ سایبری

پاراگراف زیر از مقاله ای تحت عنوان "جنگ سایبری: تحلیلی بر ابزارها و انگیزه های چند کشور" چاپ "موسسه مطالعات امنیتی فناوری در کالج دارتموث ایالات متحده" نقل گردیده است.[1]

" 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 بهره گی 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 داشته اند اما هرگز دست از تلاش اقتصادی و سیاسی برای گسترش فناوری نوین در بخش دفاع فروگذار ننموده اند. 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- تهران برای خرید فناوری اطلاعات و ملزومات فناورانه و آموزشی آن از روسیه و هند تلاش نموده است.

---

[1] -"Cyber Warfare an analysis of the means and motivations of selected nation states", Charles Billo, November 2004

روی هم رفته به نظر می رسد ایران منابع خود را در زمینه سلاحهای نامتعارف و بخش فناوری اطلاعات به منظور کسب قدرت و اعمال نفوذ بیشتر درآسیای مرکزی مصروف داشته است."

بررسی نظریه فوق در خصوص توانمندی ایران و چند کشور منطقه در زمینه جنگ اطلاعاتی و سایبری و مروروقایع معاصر در این زمینه نشانگر آن است که احتمال استفاده از تسلیحات نامتعارف همواره با موانع محدود کننده بین المللی کاهش یافته و جنگ های تمام عیار نیز جای خود را به جنگ های محدود سپرده و توجه ارتش های جهان به سوی کاربرد مبانی جنگ های ناهمطراز معطوف گردیده و بسیاری از ملت – دولت ها ترجیح می دهند به جای درگیری واقعی قدرت نمایی نموده و بازدارندگی را تقویت نمایند. جنگ سایبری بی وقفه بین کشورهای غیر دوست و گاهی دوست در جریان است. رشد فزاینده مصادیق این جنگ را می توان بین کشورهای چین و تایوان، چین و ژاپن، هند و پاکستان و بسیاری از دیگر کشورها در منطقه مشاهده کرد. جنگ سایبری اولین بار در سال ۱۹۹۱ در جنگ اول خلیج فارس توسط ارتش امریکا مورد استفاده قرار گرفت. در آن جنگ به صورت بسیار ابتدایی از روش جنگ سایبری برای شنود پست الکترونیکی فرماندهان عراقی استفاده به عمل آمد. هم چنین در نبرد هوایی ۷۸ روزه امریکا و متحدانش بر علیه یوگسلاوی، پنتاگون به سیستم پیشرفته رایانه ای پدافند هوایی بلگراد نفوذ و پیام ها و اطلاعات جعلی ارسال نمود[1]. در حالیکه بسیاری از کشورهای منطقه در حال توسعه زیرساخت ها و توانمندی های فناوری اطلاعات خود هستند ارتش ها نیز به فراخور جایگاه اجتماعی اشان در کشورهای مختلف در حال توسعه فناورانه خود می باشند. اما مشخصه بارز توسعه در همه این کشورها فقدان فناوری بومی وبهره برداری از سیستم های خارجی پیچیده و متنوع و غیر مطمئن و بالطبع

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

وابستگی عمیق و شدید آنها به کشورهای پیشرفته می باشد. به همین دلیل تهدیدات جنگ سایبری بیش از همه در بین کشورهای در حال توسعه بر علیه یکدیگر مطرح گردیده است.

ایده کلی در باره 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 سامانه های مخابراتی دشمن در محیط سایبر گردد نیمی از جنگ را از پیش برده است.

فناوری اطلاعاتی تافته در تاروپود ماشین جنگی ابرمتجاوزان قرن اکنون که کشورهای منطقه در حال توسعه سامانه های مرتبط با فضای سایبر می باشند به تهدیدی روزافزون برای امنیت ملی آنان تبدیل گشته است.

در این میان اسراییل و کشورهای خائن متحد وی در منطقه از قویترین تهدیدات سایبری برای سایر کشورها در منطقه می باشند. سایت حزب اله لبنان که در لبنان و فلسطین اشغالی و سایر نقاط جهان منجمله امریکا از استقبال بالایی در میان مراجعین برخورداراست همواره مورد تهاجم سایبری رژیم صهیونیستی اسراییل قرار دارد و مزاحمت های زیادی در مراجعه خوانندگان به این سایت وجود دارد.

در جنگ ۳۳ روزه لبنان اندکی بعد از به اسارت درآمدن سربازان اسراییلی توسط حزب الله و قبل از آغاز نبرد واقعی سایت مذکور به طور کامل توسط روش های جنگ سایبری اسراییل مختل گردید.[1]

لذا پاره ای از اقدامات که می تواند تا حدودی آسیب پذیری نیروهای مسلح و ارتش جمهوری اسلامی ایران را در جنگ آینده در برابر حملات سایبری کشورهای متخاصم کاهش دهد به شرح زیر پیشنهاد می گردد:

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

۱- **آگاه سازی سایبری**: همگام با پیشرفت فناوری اطلاعاتی آسیب پذیری ها نیز افزایش یافته و اهمیت ارتقای آموزش و دانش سایبری همه کارکنان آجا بیش از پیش گردیده است. برای این مهم لازم است تا سرفصل آموزش های مرتبط با موضوع در مدارس و دانشگاه های آجا در همه مقاطع گنجانیده شود. هم چنین در بخش های تحقیق و توسعه همه سازمانها و یگانهای آجا اهمیت موضوع تبیین و تحقیقات مرتبط با مقولات جنگ های نوین دارای اولویت گردند.

۲- **ایجاد امنیت در شبکه**: اقدامات تامینی لازم برای محافظت از سیستم های ارتباط و مخابرات آجا 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 سیستم ها به مورد اجرا گذارده شود. طرح تامین لازم برای مقابله با حملات سایبری که در برگیرنده خط مشی های لازم برای مقابله با شرایط قابل پیش بینی و غیر قابل پیش بینی را داشته باشد، باید مبتنی بر طرح های امنیت ملی تدوین گردد. تجهیزات موجود الکترونیکی و مخابراتی باید توسط متخصصین خبره و متعهد داخلی به دقت بازرسی گردیده تا از عاری بودن آنها از آلودگی های پیش گفته اطمینان حاصل گردد.

۳- **خودکفایی تجهیزاتی:** برای دستیابی به امنیت واقعی چاره ای جز اجتناب از واردات تجهیزات خارجی و اتکا به تولیدات خانگی رایانه، وسایل مخابراتی و سیستم های تسلیحاتی و نظایر آن وجود ندارد. علاوه برآن نیاز به سرمایه گذاری بومی در بخش نرم افزار نیز بسیار ضروری به نظر می رسد.

۴- **اتخاذ مشی فعال جنگ اطلاعاتی سایبری:** نقاط ضعف سیستم های مخابراتی و الکترونیکی دشمن را باید شناسایی نموده و در حوزه جنگ سایبری مشی فعال را اتخاذ و تجربه و تبحر کافی را در زمینه به کار گیری ویروس، میکروب، کدهای رمزشکن، نفوذگری، ارسال پارازیت و غیره کسب نمود.

۵- **آموزش خبرگان نفوذگر:** در زمینه آموزش و تربیت خبرگان نفوذگر درسیستم های الکترونیکی و مخابراتی باید اقدامات جدی در مراکز آموزش فرهنگی آجا به عمل آید.

۶- **هماهنگی اقدامات جنگ سایبری در بالاترین رده:** اهمیت جنگ سایبری ایجاب می نماید که هماهنگی های لازم برای اتخاذ مشی لازم در سطح ملی و با مشاورت خبرگان نظامی صورت پذیرد. در حال حاضر فقدان چنین هماهنگی سبب از هم گسیختگی و عدم ورود صحیح ارکان کشور در این عرصه گردیده است به نحوی که امکان ارزیابی واقعی جایگاه کشور و آجا در این عرصه و وضعیت دشمنان بالقوه آن وجود ندارد. در این رابطه تشکیل یک هسته سیاستگذاری در سطح ملی با حضور کلیه عناصر ذیربط در وزارت علوم، تحقیقات و فناوری و یا وزارت دفاع ضروری می باشد. 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 می باشد..

۷- **شناسایی و به کارگیری کلیه امکانات بالقوه سایبری در کشور:** شرکت های پیشرو در تولید نرم افزار، دانشگاه های صنعتی معتبر، کارخانجات الکترونیکی پیشرفته، مراکز تحقیقاتی صنعتی و غیر صنعتی، جشنواره های علمی معتبر، همایش ها و نمایشگاه های تخصصی و نظایر آن بستر وزمینه های علمی و فنی مورد نیاز کشور را اداره و ارائه می نمایند که لازم است در راستای نیازمندی های آجا شناسایی و از آنان بهره برداری به عمل آید. ترکیبی از خبرگان و متخصصین فناوری اطلاعات در آجا و بخش های یاد شده می توانند زمینه لازم برای تشکیل یک نیروی واکنش سریع سایبری را فراهم آورده ودر موقع لزوم در اسرع وقت نسبت به انجام عملیات آفندی و یا پدافندی اقدام نمایند.

۸- **ایجاد ساختار سازمانی مناسب در آجا:** به منظور ورود در عرصه جنگ سایبری و هماهنگی عملیاتی، ایجاد ساختارهای هماهنگ کننده ستادی و یگانهای عملیاتی در همه سطوح آجا ضروری است.

نتیجه:

هیچ نشانه ای از کاهش سرعت رشد انقلاب اطلاعاتی مشهود نیست. جنگ سایبری یکی از قلمروهای مطرح در عرصه برخوردهای بین المللی در سالهای آغازین هزاره سوم بوده و فرصت ها و تهدیدهای قابل توجهی را در عرصه امنیت ملی و دفاع مطرح نموده است. بی شک عدم توجه کافی به این زمینه، تهدیدها را بالفعل نموده و فرصت ها را خواهد سوخت. وابستگی فناورانه به کشورهای بیگانه بالاترین تهدید و تلاش در زمین خودکفایی 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 آجا می باشد.

منابع:

۱- "جنگ سایبری: روش ها، نیروها و سلاح های کشتار جمعی"، بیارد کلمنس فرمانده نیروی دریایی امریکا در سال ۱۹۹۹، میلیتاری ریویو، سپتامبر ۱۹۹۹، شماره ۷۹، صفحه ۳۵

۲- مجله دنیای رایانه شماره ۱۴ صفحه 13

3- Joint Vision 2020, Washington, DC: The Joint Chiefs of Staff Office, June 2000.

4- http://www-cgsc.army.military/milrev/English/sepoct99/clemen.htm,June2002

5- http://www.Trojan Horse Attacks.htm

6- http://www.nanite- a what is definition, nanomachines.htm

7- 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

8- Jon Dougherty, "U.S. developing cyber-warfare capabilities, Threats range from teen hackers to sophisticated nation-states", http://www.WorldNetDaily.com/ WorldNetDaily U_S_ developing cyber-warfare capabilities.htm,