فصلنامه مطالعات جنگ
سال دوم، شماره هفتم، زمستان ۱۳۹۹
مقالهٔ پنجم از صفحه ۱۰۶ تا ۱۲۴

جنگ سایبری و ضرورت سربازگیری با رهنمود از اندیشه‌ی مقام معظم رهبری در این عرصه

سید حمیدرضا قریشی*[۱]، هادی آقایی[۲]، هادی هاشم‌پور حمیدی[۳]

دریافت مقاله: ۹۹/۰۷/۲۵ پذیرش مقاله:۹۹/۱۰/۱۴

چکیده

فضای سایبر محیطی بسیار حساس و حساسیت برانگیز است که با ویژگی‌های خاص خود تمایزات بنیادینی با فضای ملموس واقعی دارد، با عنایت به همین پیچیدگی‌ها و تمایزات، جنگ سایبری نیز یکی از خطرناک‌ترین نوع جنگ و درگیری می‌باشد و به علت وجود چنین ویژگی‌های خاصی است که اکثر امور بشری از جمله جنگ، به این فضای نوین راه یافته‌اند؛ کشور ایران نیز تاکنون بارها در تیررس این نوع تهاجم ها قرار گرفته است که نمونه‌ی بارز آن حملات سایبری موسوم به ویروس استاکس نت به تأسیسات هسته‌ای نطنز می‌باشد. با در نظر گرفتن این مسئله، از آن‌جا که اصلی‌ترین هدف سربازگیری در هر جامعه‌ای آموزش برای جنگ و موقعیت‌های جنگی می‌باشد، از سویی دیگر نظر به بیانات حکیمانه‌ی مقام معظم رهبری که جنگ سایبری و جنگ نرم را بسیار حساس و خطیر برمی‌شمارند، به طوری که ایشان در سخنرانی مورخه۹۱/۷/۲۰ که در جمع دست اندر کاران این حوزه، با تأکید می‌فرمایند اگر من امروز رهبر انقلاب نبودم حتماً رئیس فضای مجازی کشور می‌شدم که این نشان از اهمیت این حوزه در نزد رهبر انقلاب دارد، بنابراین باید به آموزش سربازهایی متخصص با روحیه جهادی و انقلابی در این زمینه اقدام گردد. پژوهش حاضر در پی آن است که با مطرح نمودن کم و کیف جنگ سایبری و ویژگی‌های آن، ضرورت سربازگیری در این عرصه را تبیین نماید؛ بنابراین این پژوهش که به روش کتابخانه‌ای نگارش شده است، با یک آینده‌پژوهی حساب شده، در راستای کیفی‌سازی خدمت نظام وظیفه در ایران بوده و پیشنهادهایی را در این زمینه ارائه می‌نماید.

واژگان کلیدی: فضای سایبر، جنگ سایبری، سرباز سایبری، آینده‌پژوهی

۱- عضو هیئت‌علمی دانشگاه جامع امام حسین (ع)، تهران، ایران Sghoreishi43@gmail.com
۲- پژوهشگر مرکز مطالعات و امنیت ملی دانشگاه جامع امام حسین (ع)، تهران، ایران Hadiaghaei63@gmail.com
۳- کارشناس ارشد حقوق، دانشگاه آزاد واحد علوم تحقیقات تبریز، ایران.

مقدمه

جنگ به‌عنوان پدیده‌ای شوم پیوسته زندگی آدمی را در این کره‌ی خاکی تحت تأثیر خود قرار داده و همواره یکی از بدترین خاطرات انسان بوده است. دولت‌ها همواره برای مقابله با تهاجم‌های دشمنان اقدام به فراهم آوردن ارتش و سربازانی نموده‌اند. حال با ظهور اینترنت به‌عنوان یک ابزار جدید، سریع و ارزان ارتباطی مسئله‌ی جنگ نیز در این فضا مطرح شده است که مقتضیات خاص خود را می‌طلبد، در واقع فضای سایبر میدان جنگ را گسترش داده و عرصه‌ی جدیدی به میدان های سنتی‌تر جنگ همچون زمین، هوا، دریا و فضا افزوده است، در این فضا ارتش‌های فضای واقعی برای دفاع از کیان کشور کارایی چندانی نخواهند داشت (هاشم‌پور حمیدی،۱۳۹۳:۳).

ذکر این نکته مهم است که فعالیت و حملات برشمرده طبق برخی قوانین و مقررات ملی و فراملی جرم تلقی می‌شود .در آن نظام‌ها، نگاه به این قبیل فعالیت‌ها کیفری است، رویکرد این نظام‌ها این است در فضای سایبری جایی برای اطلاعات در نظر گرفته شده و آن فضای مجازی نباید محل تجمع کاربرانی باشد که هدفی سیاسی یا ایدئولوژیک را دنبال می‌کنند. به هر حال به نظر می‌رسد تکلیف مقوله حملات فراملی مربوط به آن در همه نظام‌ها مشخص و همگون نیست و ضروری است که در سطوح ملی و بین‌المللی مقررات مشخصی برای آن وضع شود و تدابیری برای همکاری میان کشورها اتخاذ شود. در واقع مقتضی دفاع در این فضای جدید تشکیل ارتش مختص آن می‌باشد و پژوهش حاضر در پی آن است که با مطرح نمودن کم و کیف جنگ سایبری و ویژگی‌های آن ضرورت سربازگیری در این عرصه را با عنایت به رهنمودهای مقام معظم رهبری تبیین نماید.

از این رو خواننده‌ی محترم در این پژوهش که به روش کتابخانه‌ای نگارش شده است، برای پی بردن به ضرورت سربازگیری در جنگ سایبری با توجه به رهنمودهای مقام معظم رهبری در این عرصه لازم است با تاریخچه جنگ و تحولات آن و همچنین طرح مسئله جنگ در فضای سایبری و ویژگی‌های آن و همچنین شیوه‌های نوین حملات سایبری آشنا گردیده تا در ادامه مطلب بتواند

با تعمق بیشتری به سربازگیری سایبری با توجه به رهنمودهای مقام معظم رهبری که در این عرصه بیان گردیده است توجه نماید.

تاریخچه جنگ و تحولات آن

جنگ به‌عنوان پدیده‌ای که می‌توان وجود آن را با عمر بشری در این کره‌ی خاکی قرین دانست در طول قرون و اعصار تفاسیر و تدابیر خاص خود را داشته است تا آنجا که روزگاری جنگ هیچ محدودیتی به خود نمی‌دید و شاید یگانه محدودیتی که در دوران باستان در عرصه‌ی جنگ دیده می‌شد اعلان رسمی جنگ بود که در یونان ملاحظه می‌گردید ولی قابل توجه آنکه تا قرن چهارم قبل از میلاد معاهدات صلح معمولاً برای یک مدت معین منعقد می‌شد و از این امر چنان بر می‌آید که در ادوار باستانی حالت جنگ حالتی عمومی بین ملت‌ها بوده است (نوس بام،۷:۱۳۳۷). با گذشت زمان و توجه بیشتر افکار بشری بر مسئله جنگ رفته ضرورت تغییر نیز در این حوزه به چشم می‌آید و با ظهور دین مسیحیت و مطرح شدن دو نهاد حقوقی به نام‌های «صلح الهی»[1] و «متارکه الهی»[2] که توسط شورای لاتران مطرح گردیده بود[3] کوشش‌هایی در جهت تدوین قواعد جنگ و افراد و اماکن و کودکان و زنان و حقوق آنان در زمان جنگ به چشم می‌خورد (ضیایی بیگدلی،۳۸:۱۳۸٦) و همچنین می‌توان نظریه‌ی اسلام درباره‌ی جنگیدن و محدودیت‌هایی که

1. In the French Pixar de adieu in the English Pixar god or Peace of God
2. In the French Treves de adieu,in the English Truce of God

۳- مهم‌ترین قواعد حقوق ملل مسیحی عبارت بود از تأسیس دو نهاد حقوقی به نامه‌ای «صلح الهی» و «متارکه‌ی الهی». صلح الهی کوششی بود در راه تنظیم مقررات جنگ که توسط شورای لاتران به سال ۱۰۵۹ تعمیم داده شد. برابر مقررات این نهاد، غیر جنگجویان، کلیساییان، کودکان، زنان، افراد بی سلاح، اموال متبرکه، مانند اموال کلیسا و اموالی که از نظر اقتصادی مفیدند، مانند ابزار و محصولات کشاورزی، حیوانات و...باید از تعرض مصون می‌ماندند و حریم آن‌ها حفظ می‌گردید. متارکه‌ی الهی که شورای کلرمن به سال ۱۰۹۵ مقرراتی در باب آن‌ها وضع نمود، نهادی بود که ایام جنگ و ستیز را محدود می‌نمود...حقوق ملل مسیحی، اساساً از دو جهت با حقوق بین‌الملل معاصر اختلاف داشت: اولاً حقوق ملل به اراده‌ی کشورها به وجود نیامده بود بلکه حقوق مشترکی بود که بر اساس مقتضیات عقل طبیعی، برای ملت‌های مختلف و متمایز تأسیس شده بود. ثانیاً تنظیم روابط میان کشورها، تنها هدف حقوق ملل نبود، بلکه در مجموع، کلیه‌ی روابطی را که خارج از چهارچوب یک کشور معین وجود داشت، در بر می‌گرفت. بدین معنی که کلیه‌ی روابطی که از حدود قلمرو حقوق مدنی خارج بود، مشمول احکام «حقوق ملل می‌شد».

درباره‌ی ایام جنگ در ماه‌های حرام وضع کرده و همچنین جنگیدن در مسجدالحرام و... را ذکر نمود. ولی آنچه که پیوسته با اندیشیدن در این دوران به ذهن متبادر می‌گردد این نکته است که تا عصر حاضر قواعد قابل اعتنایی برای پیش‌گیری از جنگ نبوده است شاید بتوان اولین قدم‌های مؤثر را در تأسیس جامعه ملل دید چراکه هرچند در خود میثاق جامعه جنگ ممنوع اعلام نگردیده بود ولی در تاریخ ۲٤ سپتامبر ۱۹۲۷ مجمع جامعه ملل ضمن یک اعلامیه رسمی جنگ تجاوزکارانه را یک جنایت بین‌المللی محسوب نمود و خواستار ممنوع شدن آن گردید (ضیایی بیگدلی،۱۳۸۰:۸). ولی بعد از گذشت این دوران با میثاق بریان – کلوگ که در سال ۱۹۳۹ مورد تصویب و الحاق ٦۳ کشور از جمله ایران قرار گرفت جنگ ممنوع گردید ولی نکته شایان توجه آن بود که در همین سال جنگ جهانی دوم[1] آغاز گردید با این همه باز نیز نمی‌توان از تأثیر مثبت این معاهده غافل گردید چراکه همین عوامل بود که باعث شد در زمان تدوین منشور سازمان ملل متحد در سال ۱۹٤٥ حفظ صلح به‌عنوان اولین و اصلی‌ترین هدف سازمان در ماده‌ی یک منشور مذکور قرار گرفت و جنگ به صورت رسمی ممنوع گردید.

آن‌گونه که ذکر گردید با تحولاتی که به وجود آمده بود به نظر می‌رسید که آینده‌ی بشر به‌سوی صلح پایدار در حرکت باشد ولی بعد از سال ۱۹٤٥ نیز با توجه به دو قطبی شدن جهان به بلوک شرق و غرب، دور جدیدی از رقابت‌ها میان آمریکا و شوروی آغاز شده بود که به جنگ سرد[2] شهرت یافته است. در واقع این نوع جنگ ترکیبی از جنگ سنتی (جنگ سخت) و جنگ نرم بود که طی آن دو ابر قدرت در عین حال از رویارویی با هم پرهیز می‌کردند؛ اما این وضعیت نیز چندان نپایید با فرو پاشی شوروی در سال ۱۹۹۱ میلادی و پایان جنگ سرد بشریت در فکر این افتاد که چه نیک از گرفتاری دیگری رهیده است ولی در این سال‌ها کارشناسان جنگ ایالات‌متحده با استفاده از تجارب دو جنگ جهانی و دوران جنگ سرد دریافتند که می‌توانند با هزینه کمتر و بدون دخالت مستقیم در سایر کشورها به اهداف خود نائل آیند، با فراگیر شدن

1. World war II
2. Cold war

چنین افکاری در ذهن متخصصان آسوده‌ترین راه این نوع جنگ نیز متبادر به ذهن گردید که همانا جنگ در فضای سایبر بوده است. در واقع جنگ به عرصه‌ای برده شد که آن فضا مترادف با دنیا کامپیوترها و شبکه اینترنت بود (قاجار قیونلو،۱۳۹۱:۱۳۲).

فضای سایبر و طرح مسئله جنگ در آن

بشر در طول تاریخ، مراحل مختلفی را پیموده است و از اوان خلقت در این کره‌ی خاکی به دنبال ارتباط با هم نوع خود بوده است. عمر این ماجرا را می‌توان از روزی که بشر با شوق فراوان با ایماء و اشاره با همنوع خود ارتباط برقرار ساخت تا اختراع خط و ... متصور شد. ولی در قرن ۲۰ میلادی بشر با فراگیر شدن ارتباطات در بستری جدید، رویکردی نو در مقابل خویشتن مشاهده کرد و برای اولین بار مسئله‌ای به نام فضای مجازی[1] برایش مطرح گردید (صابرنژاد،۱۳۹۲:۲۷)؛ که شاید تا آن زمان تصوّر کردن چنین چیزی برای آدمی محال بود. مسئله‌ای که در این فضا ذهن بشری را به خود جلب کرد این بود که آیا قواعد سابق اجتماع، در این عرصه نیز می‌تواند مصداق داشته باشد یا نه؟ و در صورت امکان، هنجارهای آن به چه نحوی تبیین خواهد شد؟ ولی پیش از پاسخ‌گویی به این مسائل باید کم و کیف این فضا به وضوح شناخته شود.

اصطلاح فضای سایبر[2] یا فضای هدایت شده که در لغت به معنای سکان‌دار، راهنما یا حاکم آمده است، نخستین بار در سال ۱۹۲۸ میلادی در یک داستان علمی – تخیّلی به کار برده شد. از آن زمان تاکنون فضای سایبر را به معنای مکانی غیر فیزیکی و مجازی می‌شناسیم که واقعیت‌ها را با عنوان واقعیت مجازی در فضای الکترونیکی بازتاب می‌دهد (مسعودی، ۱۳۸۳: ١٦). «سایبرسپیس» توهم و تصور باطل توافقی است که انسان‌ها خلق کرده‌اند، یک ناحیه واقعی است که فعالیت‌هایی در این فضا اتفاق می‌افتد از جمله تبادل و تجمیع اطلاعات. (بای و همکاران،۱۳۸۸:۲۱). در واقع فضای سایبر محیطی است مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد،

1. Virtual space
2. Cyber space

ملت‌ها، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی (به صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل استفاده و در دسترس استفاده کنندگان و کاربران می‌باشد، کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط هستند (باستانی،۱۳۸۳:۵۶).

اما باید دانست که با مطرح شدن فضای سایبر مهم‌ترین تحولی که در سال‌های اخیر در حوزه جنگ رخ داده است، استقرار و به‌کارگیری فناوری اطلاعات و ارتباطات رایانه محور می‌باشد[۱]؛ اما در این بحبوحه‌ی مناظره پرشور در مورد «فناوری اطلاعات و ارتباطات»[۲] ما نباید این واقعیت را نادیده بگیریم که آن‌چه در پس برخی دستگاه‌ها و ابزارهای عملیات اطلاعاتی قرار دارد به مراتب گسترده‌تر از فناوری رایانه محور اطلاعات و ارتباطات است و چه بسا حتی فناوری را در اموری فراتر از اطلاعات پراکنی درگیر سازد. (هالپین، ۱۳۸۹:۲۵۲) در واقع توجه به این نکته ضروری است که با مطرح شدن جنگ در این عرصه‌ی نوین، جنگ به محیطی برده شد که آن فضا مترادف با دنیا کامپیوترها و شبکه اینترنت بود.

همان‌طور که مشخص است جنگ سایبری شکل کاملاً جدیدی از رزم است که بازتاب آن را هنوز به‌طور کامل نتوانسته‌ایم درک کنیم (Clark,2009:32). اما درباره‌ی این موضوع، آن‌چه که به ذهن متبادر می‌گردد این است که به نظر می‌رسد این نوع جنگ با اشکال سابق جنگ تفاوت چندانی ندارد و فضای سایبر را نیز به عرصه‌های سنتی‌تر افزوده است ولی با این تعریف آنچه که از چشم پنهان می‌ماند. پس‌زمینه جاری حمله سایبری به‌عنوان بخشی از برنامه‌ای کل‌نگر و هماهنگ برای دستیابی به اهداف سیاسی، اقتصادی و اجتماعی کشورهاست (Michael,2010:1.) با وجود این باید به این نکته توجه کرد که بر خلاف دیپلماسی نیروی

---

۱. در واقع مراد از ارتباطات رایانه محور همان فضای سایبر در معنای اخص می‌باشد چراکه حقوق سایبر شاخه‌ای از حقوق مرتبط با کامپیوتر و اینترنت است؛ که راجع به موضوعاتی مانند حقوق مالکیت فکری، آزادی عقیده و دسترسی آزاد به اطلاعات بحث می‌کند.

۲. Information & communication technology(ICT)

نظامی و جنگ اقتصادی در این عرصه موضوع اصلی «که همانا مسئله‌ی کشورها و وجود آن‌ها برای تخاصم بین‌المللی است» به چالش کشیده می‌شود. در واقع فضای سایبر این امکان را برای سوژه‌های[1] غیردولتی نظام بین‌المللی، سازمان‌های تجاری و حتی افراد فراهم می‌کند که وسایل و انگیزه برای فعالیت جنگ‌طلبانه را کسب کنند (Cornish & Livingstone,2010:32) و همین مسئله موجب شده است که در سطح بین‌المللی نیز جهان شاهد چندین جنگ سایبری باشد که بعضی از آن‌ها از این قرارند:

۱. دهه‌ی ۸۰ میلادی حمله‌ی آمریکا به کره شمالی

۲. سال ۱۹۹۵ حمله‌ی هکرهای روسی به سیتی بانک آمریکا

۳. سال ۱۹۹۹ حمله‌ی آمریکا به یوگسلاوی

٤. سال ۱۹۹۹ حمله‌ی آمریکا به شبکه‌های کامپیوتری صرب

۵. سال ۲۰۰۰ حمله‌ی هنگ‌کنگ به چین

٦. سال ۲۰۰۱ حمله‌ی آمریکا به چین

۷. سال ۲۰۰۱ آمریکا و روسیه

۸. سال ۲۰۰۷ روسیه و گرجستان هم‌زمان با ماجرای او ستیای جنوبی

۹. سال ۲۰۱۰ حمله‌ی ویروس استاکس نت[2] به تاسیسات نطنز (مرکز پدافند غیرعامل فاوا،۱۳۸۸:۵۵)

1. Subject

۱. استاکس‌نت به انگلیسیStyx net : یک بدافزار رایانه‌ای (طبق نظر شرکت‌های نرم‌افزار امنیت رایانه‌ای: کرم رایانه‌ای یا تروجان) است که اولین‌بار در تاریخ ۱۳ جولای ۲۰۱۰ توسط ضدویروس وی‌بی‌ای ۳۲ 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 WinCE 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 بوده است. در اواخر ماه مه ۲۰۱۲ رسانه‌های آمریکایی اعلام کردند که استاکس‌نت مستقیماً به دستور اوباما رئیس جمهور آمریکا طراحی، ساخته و راه‌اندازی شده است (پورقهرمانی و صابرنژاد،۱۳۹۲:۳۵).

از فحوای آنچه که بیان گردیده است پیداست که جنگ سایبری یکی از خطرناک‌ترین نوع جنگ و درگیری می‌باشد. ویژگی و اهمیت ویژه این جنگ سبب گردیده است که کشورهایی همچون روسیه، ایالات‌متحده آمریکا و چین این نوع جنگ را مهم‌تر از جنگ خطرناکی همچون نبرد هسته‌ای قلمداد کنند که صد البته یکی از علل اصلی آن فراگیری و سهل‌الوصولی این جنگ می‌باشد. «ریچارد کلارک»[1] مشاور عالی ضدتروریسم آمریکا در دو دوره جرج بوش و بیل کلینتون اعلام کرد: آمریکا توانایی لازم برای مقابله با تلاش تروریست‌ها جهت دستیابی به سیستم رایانه‌ای ایالات‌متحده را ندارد و این موضوع ممکن است به فاجعه در ایالات‌متحده منجر شود، چراکه این نوع جنگ می‌تواند در عرض ۱۵ دقیقه برای ایالات‌متحده بسیار مرگبار و مخرب باشد. (پورقهرمانی و همکاران،۱۳۹۲:۳۹) و با بیان همه‌ی این مسائل به وضوح پیداست که تشکیل ارتش سایبری قدرتمند در این عرصه‌ی نوین برای هر کشوری که در پی حفظ کیان و استقلال خویش است، واجب می‌نماید. کشور ایران نیز از این مسئله مستثنی نبوده و همان‌طور که بیان آن گذشت مورد تهاجمات سایبری نیز قرار گرفته است و به خوبی پیداست که تشکیل چنین ارتشی نیز برای آن ضروری می‌باشد که البته با توجه به فراگیر شدن علوم مرتبط با فضای سایبر در میان جوانان و بالندگی دانشگاه‌های کشور در این زمینه، می‌توان سربازان این ارتش نوین را از میان مشمولین سربازی متخصص در این زمینه فراهم نمود.

ویژگی‌های جنگ سایبری

۱- تعدد بازیگران در فضای سایبری

هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب به این معناست که تقریباً هرکسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت- ملت هستند (Chaney, 2009:5-6).

۲- هزینه کم ورود صرف زمان کم و سرعت بالای اقدام

1. Richard Clarke

هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در نتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد .البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord and Sharp, 2011: 20-28).

۳- ناشناس ماندن بازیگران و عدم قابلیت ردیابی

اینترنت به‌عنوان سیستم نامتمرکز طراحی شده و کاربران آن، غالباً شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند از اقصی نقاط دنیا، بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند (Ibid).

٤- تأثیرگذاری شگرف

ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به مراتب بیشتری از حادثه اولیه در پی داشته باشد .وقوع حمله‌های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی از دست دادن جان انسان‌ها شود، زیرا در این‌گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند (Ibid).

٥- کمرنگ شدن نقش جغرافیا

فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند (Ibid: 8).

٦- ساختار فضای اینترنت

اینترنت، دامنه مشترک و یکپارچه است .استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است .توانایی محدود برای جدا کردن بازیگران و

فعالیت‌های آن‌ها، پاسخ مناسب به تهدید را دشوارتر کرده است (Chaney, Op. Cite: 5- 6). از سوی دیگر، ساختار اینترنت، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی این فضا است (Hallerand Others, 2010:4).

۷- پیچیدگی در مجازات اعمال مجرمانه در فضای سایبر

احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. در نتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیرسایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند(Sharp, Op. cite: Lord and 20-28).

شیوه‌های نوین حمله در جنگ سایبری

عدم اجازه دسترسی به خدمات (داس) یا حملات توزیع شده برای عدم اجازه دسترسی به خدمات (دی داس) حمله‌ای است که به‌موجب آن رایانه یا منبع شبکه برای کاربران غیرقابل دسترس می‌شود. انگیزه و هدف این نوع حمله در هر مورد متفاوت است. این اقدام معمولاً به قصد انقطاع و تعلیق موقت و یا دائمی خدمات میزبان متصل به اینترنت صورت می‌گیرد. حمله داس به وفور اتفاق می‌افتد. میزان این حمله از سال ۲۰۱٤، به ۲۸ مورد در ساعت می‌رسد.[1] سایت های مورد حمله، سایت‌های دارای پروفایل مهم مثل بانک‌ها، ورودی‌های پرداخت با کارت اعتباری و ... هستند. داس و دی داس توسط دو نفر یا بیشتر یا دو بات و بیشتر صورت می‌گیرد. یکی از نمونه‌های اخیر داس در دسامبر ۲۰۱٤ صورت گرفت که در آن کاربران بازی‌های جدید ایکس باکس حدود ۲٤ ساعت قادر به ورود به حساب کاربری خود نبودند.

برای جرم انگاری این نوع حملات سه موضوع مدنظر قرار می‌گیرد: ۱- حمله به قصد کلاهبرداری، تقلب، یا تحصیل مال انجام شود، ۲- مرتکب فاقد حق و اختیار است و ۳- هدف از حمله تحصیل منافع اقتصادی برای خود یا دیگری است. اگر حمله‌ای این سه ویژگی را داشته

1.See:http://www.eweek.com/security/slideshows/ddos-attack-volume-escalates-as-new-methods-emerge.html. (last visit 31.12.2014)

باشد، طبق کنوانسیون بوداپست و مقررات ۲۰۱۳ اتحادیه اروپا قابل تعقیب تحت عنوان کلاهبرداری است. یکی دیگر از شیوه‌های حمله آن است که سیستم با تقاضای ارتباط خارجی مورد هدف قرار گیرد، طوری که نتواند به ترافیک مجاز پاسخ دهد، یا اینکه سرعت آن به قدری کم شود که عملاً غیرقابل دسترس گردد. این نوع حملات منتج به ایجاد بار اضافی می‌شوند. به عبارت ساده‌تر حملات داس رایانه‌های مورد هدف را مجبور به ریست، یا استفاده از منابع خود می‌کند تا نتواند سرویس ارائه دهد و یا ارتباط بین کاربران و رایانه مورد هدف بلوکه شود، به نحوی که قادر به ارتباط مؤثر نباشد. داس در این تعبیر ناقض سیاست استفاده مناسب از اینترنت است و سیاست‌های استفاده قابل قبول را نقض می‌کند.

همان‌طور که ذکر شد این اقدامات را با توجه به ماهیت و هدف آن‌ها را می‌توان از مصادیق جنگ در فضای سایبر تلقی نمود. یکی از نمونه‌های اعتراض‌های در قالب داس مربوط به شیوع کرم ونک در سال ۱۹۸۹ در ایالات‌متحده است. کرم ونک[1] در اعتراض به تسلیحات هسته‌ای، به وب‌سایت‌های ناسا، وزارت انرژی و سایر وب‌سایت‌های دولتی ایالات‌متحده حمله کرد. پیامی که روی صفحه این وب‌سایت‌ها نمایش داده می‌شد این بود که «کرم‌های ونک مخالف قاتلان هسته‌ای هستند. سایت شما رسماً هک شده است. شما از صلح میگویید، اما خود را برای جنگ آماده می‌کنید.» (singer,2014:77) نمونه دیگر، حمله گروه ناشناس در نوامبر ۲۰۱۳ به ارتش الکترونیکی سوریه[2] و دو حساب توئیتری و در اعتراض به دولت بشار اسد به دلیل قطع اینترنت بود. گروه ناشناس صفحه وب‌سایت‌های دولتی سوریه را تغییر داد. البته رابطه میان ارتش الکترونیکی سوریه و دولت سوریه مشخص نیست.

رابرت موریس، هکر کرم ونک اولین متهمی بود که در ۱۹۹۰ طبق قانون سی اف ای ای[3] مصوب ۱۹۸٦ ایالات‌متحده محاکمه شد. او به ۱۰۰۰۰ دلار جریمه نقدی و ٤۰۰ ساعت خدمات اجتماعی محکوم شد. این قانون در آن تاریخ فقط ناظر بر رایانه‌های تحت مالک دولت فدرال یا نهادهای

1. WANK worm
2. Syrian Electric Army
3. Computer Fraud and Abuse Act (1986)

مالی بزرگ بود؛ اما در سال ۱۹۹٦ به‌موجب الحاقیه‌ای دامنه آن به دسترسی بدون مجوز به هر یارانه‌ای تسری پیدا کرد.

داس می‌تواند صرفاً به دلایل سیاسی اتفاق بیفتد. این اقدامات را می‌توان تحت مقوله اعتراض سیاسی یا ضد سرمایه‌گذاری بررسی کرد. مثلاً هکتیویستها صفحه وب‌سایت‌های دولتی و سایت هایی مخالف ایدئولوژی خود را تغییر داده و معمولاً پیام خود را روی آن صفحه می‌گذارند. این حمله با دزدی[۱] در مفهوم سنتی آن متفاوت است. این فرم از فعالیت، آزادی بیان با اهداف ناخواسته و پیش‌بینی نشده است. مشکل حملات اعتراضی داس این است که منابع را هدر می‌دهد و منتج به جنگی می‌شود که هیچ کس برنده آن نیست. در سال ۲۰۰٦ بلو سکیوریتی[۲] به قصد حمله به اسپمرها[۳]، حمله داس گسترده ای علیه بلو سکیوریتی انجام داد. با وجود اینکه بلو سکیوریتی توانست بر اسپمرها غلبه کند، اما آی اس پی[٤] قدیمی و دی ان اس پروایدر[٥] قدیمی خود را از اینترنت خارج کرده و خسارات اقتصادی برای آن‌ها به بار آورد و تجارتشان را نابود کرد[٦].

ارتش سایبری ایران و سربازگیری در آن

طرح تشکیل ارتش سایبری ایران از سال ۱۳۸٤ در سپاه پاسداران انقلاب اسلامی مطرح شد و در ادامه نیز با توجه به تأکیدات مقام معظم رهبری در مورد این حوزه در اجرای آن تسریع به عمل آمد و به سرعت ساختار این مجموعه با پنج کارگروه با وظایف و مأموریت‌های مشخص تصویب شد.

در سایت ویکی‌پدیا آمده است که در اردیبهشت ۱۳۸۸ مؤسسه «Defense Tech» که از مؤسسات نظامی و امنیتی ایالات‌متحده آمریکا است، با استناد به آمار دریافتی از سازمان اطلاعات

---

۱. piracy
۲. Blue Security
۳. spammers
۴. ISP
۵. DNS provider
۶. See http://www.securityfocus.com/news/11392. (last visit 31.12.2014)

آمریکا، ایران را جزء پنج کشور دارای قوی‌ترین نیروی سایبری معرفی کرده است. این مؤسسه با تأکید بر اینکه ارتش سایبری ایران زیرمجموعه تیم رصد سایبری سپاه است، بودجه آن را ۷۶ میلیون دلار اعلام کرده بود این موسسه همچنین تعداد نیروهای این ارتش را بیش از ۲۴۰۰ نفر و ۱۲۰۰۰ نفر ذخیره برآورد کرده بود.

همان‌طور که بیان گردید جمهوری اسلامی ایران یکی از قوی‌ترین ارتش‌های سایبری جهان را در اختیار دارد و آنچه که در این مسئله مورد توجه بوده و مورد تأکید می‌باشد آن است که بتوان با به کارگیری راهکاری مناسب از میان مشمولین متخصص در زمینه‌ی جنگ سایبری در این ارتش به‌عنوان سرباز استفاده نمود که این عمل زمینه‌ساز بهینه‌تر شدن دوران سربازی و استفاده از نیروی متخصص ارزان می‌باشد که محاسن خاص خود را دارد.

استفاده نکردن از نیروی جوانی و نیز تخصص سربازان در فضای سایبر، علاوه بر بی حاصل گذراندن این برهه برای جوانان، کشور را نیز از این بهره‌مندی محروم خواهد ساخت. برای بررسی دقیق باید از سوی مسئولین نیروهای نظامی و سازمان نظام وظیفه عمومی ناجا علل عدم تمایل به تخصصی شدن سربازی را جست‌وجو کرد. با به‌کارگیری سربازهای سایبری در نیروهای مسلح موجبات کارآفرینی، جلوگیری از خروج ارز، بومی‌سازی علمی و اقتدار جهانی جمهوری اسلامی ایران را می‌توان فراهم آورد، توجه به این نکته ضروری است که تنها به‌کارگیری نخبگان کار ساز نیست و میزان جذب مشمولین عادی تحصیل کرده نیز در ارتباط با این فضا باید در دستور کار قرار گیرد. شاید در مقام بیان مهم‌ترین دلیلی که از اجرای تخصصی کردن سربازی در این فضا جلوگیری کرده است، عدم امکان تأمین مالی توسط ارگان‌های نظامی جهت تأمین نیروی خود است.

جنگ سایبری از دیدگاه مقام معظم رهبری

مقام معظم رهبری در اهمیت حفظ نظام، محافظت غیرنظامی را هم‌تراز تمامی دستاوردهای نظام و لازمه حفظ آن‌ها قلمداد نموده و فراگیر شدن و همگانی شدن پدافند غیرعامل را مورد تأکید قرار داده‌اند. «همان‌گونه که شعله از جایی شروع می‌شود و به تدریج همه جا را فرامی‌گیرد، پدافند

غیرعامل نیز باید همچون شعله فراگیر شده و همه افراد کشور آن را به‌عنوان ضامن بقای نظام و یک محمل مناسب برای بقاء، استمرار و تداوم حرکت خروشان انقلاب اسلامی در همه ابعاد، اعمال نمایند. تنها راه مقابله با تهدیدها این است که وضعیت داخلی به‌گونه‌ای ساماندهی شود که دشمن از پیروزی خود مطمئن نباشد و زمینه را برای ماجراجویی فراهم نبیند. ندانستن اینکه دشمن چه در سر دارد و چه می‌خواهد بکند، غفلتی است که ممکن است ما را از امکان برخورد و امکان دفاع محروم کند. تهدید را کاملاً جدی بگیرید، یعنی به هیچ وجه در محاسبات خودتان از جدیت تهدید پایین نیایید، منتهی تهدید جدی معنایش حتمی نیست، هیچ حتمیتی وجود ندارد. وظیفه همه ما این است که سعی کنیم کشور را مستحکم، غیرقابل نفوذ، غیرقابل تأثیر از سوی دشمن، حفظ و نگه داریم. یک وقت دفاع لازم است و یک وقت هجوم لازم است، باید خودمان را از همه جهت آماده کنیم. تا این دشمن وجود دارد، تهدید هست و تا تهدید هست، فکر و آمادگی دفاعی باید باشد. باید دید دشمن از کجا دارد حمله می‌کند، برای یک دفاع خوب هم یک معرفت خوب لازم است، اگر چه برای یک هجوم خوب هم یک معرفت خوب لازم است» (بیانات در دیدار مسئولان پدافند غیر عامل ۱۳۹٤/۸/٤). مقام معظم رهبری پدافند غیرعامل و جنگ سایبری را مثل مصونیت سازی بدن انسان می‌داند که از درون ما را مصون می‌کند. معنایش این است که ولو دشمن تهاجمی هم بکند و زحمتی هم بکشد و ضرب و زوری هم بزند، اثری نخواهد کرد .«کاری کنیم که همت ما فقط مصروف به این نباشد که دشمن را منصرف کنیم یا برای مقابله خودمان را آماده بکنیم. نه کاری کنیم که ما مصونیت در خودمان به وجود بیاوریم .این با پدافند غیرعامل تحقق پیدا می‌کند؛ بنابراین این مسئله، مسئله بسیار مهمی است که بایستی راه بیفتد» (بیانات حضرت امام خامنه‌ای در دیدار با مسئولین نظام ۱۳۹۱/۷/۸) .«دفاع جزئی از هویت یک ملت زنده است. هر ملتی که نتواند از خود دفاع کند، زنده نیست. هر ملتی که به فکر دفاع از خود نباشد و خود را آماده نکند، در واقع زنده نیست. هر ملتی هم که اهمیت دفاع را درک نکند، به یک معنا زنده نیست. ما نمی‌توانیم چشم و قدرت تحلیل داشته باشیم توطئه عمیق عنادآمیز استکبار علیه اسلام و نظام اسلامی را ببینیم، در عین حال به فکر دفاع نباشیم»(بیانات مقام معظم

رهبری در جمع فرماندهان عالی رتبه نیروهای مسلح ۱۳۸۲/٦/۹). همان‌طور که از فرمایشات مقام معظم رهبری بر می‌آید مجموعه اقدامات غیرمسلحانه‌ای که به افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسلیح مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن در جنگ سایبری منجر شود، امری ضروری می‌باشد.

باید توجه نمود که تجارب و شواهد ثبت شده در جنگ‌های اعصار گذشته تاریخ بشری و قرون حاضر، نمونه‌های مدلل و انکارناپذیری است که اهمیت جنگ سایبری و پدافند غیرعامل را آشکار و ثابت می‌کند. به نظر می‌رسد موارد مشروحه مصداق بارز این اهمیت در فرمایشات مقام معظم رهبری می‌باشد که به دفعات در سخنرانی‌هایشان بدان اشاره نموده‌اند:

۱. موجب زده ماندن و حفظ بقای نیروی انسانی می‌گردد که با ارزش‌ترین سرمایه و موجودیت ملی کشور می‌باشد.

۲. موجب صرفه‌جویی کلان اقتصادی و ارزی در حفظ تجهیزات و تسلیحات بسیار گران قیمت نظامی می‌گردد.

۳. مراکز حیاتی و حساس اقتصادی، سیاسی، نظامی، ارتباطی و مراکز عمده علمی و فرهنگی و... را در برابر حملات و بمباران‌های هوایی دشمن حفظ و ادامه فعالیت در شرایط بحران و جنگ را ممکن می‌کند.

٤. موجب تحمیل هزینه قابل توجه به دشمن می‌گردد.

۵. سبب به وجود آوردن تأثیرات روحی و روانی مثبت در شهروندان و رزمندگان می‌گردد.

٦. موجب حفظ نیروها برای ضربه زدن در زمان و مکان مناسب و گرفتن آزادی و ابتکار عمل از دشمن می‌گردد.

۷. اجتناب‌ناپذیر بودن بروز جنگ‌های آینده و لزوم آمادگی دفاعی.

۸. نیل به دفاع غیرعامل در مقایسه با دفاع عامل، ساده‌تر و سهل‌الوصول‌تر و با سیاست و خودکفایی و عدم وابستگی و استقلال کشور موافق‌تر است.

نتیجه‌گیری و پیشنهاد

به وضوح مشخص است که جنگ بعد از پیمودن مراحل گوناگون و گذر از مرحله‌ی جنگ سخت وارد فاز جدیدی شده است که از آن به جنگ سایبری تعبیر گشته است در واقع در این نوع جنگ تخاصم در فضایی جدید به وجود می‌آید که چندان خبری از ویژگی‌های جنگ سخت در آن نیست. این جنگ هر چند که دارای برخی از شباهت‌های بنیادین با جنگ‌های سابق است که عبارت‌اند از بحث تخریب و رساندن آسیب، ولی همان‌طور که گفته شد دارای ویژگی‌های منحصر به فردی است که آن را از جنگ‌های سنتی متمایز می‌نماید که با در نظر گرفتن اوصاف خاص آن به نظر می‌رسد که باید کشورها برای مقابله با این نوع جنگ ارتش‌های مختص آن را طراحی نمایند و این مسئله در ایران نیز مورد توجه بوده و ارتش سایبری در سال ۱۳۸٤ توسط سپاه پاسداران انقلاب اسلامی تعبیه شده است. با توجه به بحث‌های به عمل آمده، به خوبی روشن است که ارتباطات رایانه‌ای جهانی (اینترنت) که در فضایی مجازی صورت می‌گیرد، مرزهای جغرافیایی را در هم شکسته و قلمرو جدیدی برای فعالیت‌های بشری به وجود آورده است. بگونه‌ای که امکان بکارگیری حقوق موجود در چارچوب مرزهای ملی را تضعیف نموده است. با توجه به نفوذ اینترنت در عرصه جنگ سایبری، دولت‌ها خود را ناگزیر به ارتش سایبری نموده و به فراخور حال خود، قوانین داخلی و بین‌المللی برای این فضا وضع نموده‌اند. لکن ماهیت فرامرزی و ابعاد بین‌المللی اینترنت باعث شده تنظیم آن توسط حاکمیت‌های مختلف، موجب اصطکاک صلاحیت‌ها شده و به ابهامات حقوقی این فضا افزوده گردد.

با توجه به رشد سریع تکنولوژی در جهان، به ویژه در فضای سایبر، امروزه دیگر جنگ سایبری کارکردی ساده و آسان ندارند و دارای پیچیدگی‌هایی است. افزایش کارایی نیروهای مسلح یک گروه کوچک، حرفه‌ای و آموزش دیده سایبری از تعداد بی‌شمار سربازان وظیفه کم آموزش دیده هستند. به خصوص آنکه امروزه شیوه فزونی نفرات در جنگ سایبری عامل مؤثری در برتری نظامی نیست.

از همین رو مقام معظم رهبری پدافند غیر عامل را یک مصونیت می‌داند و سیاست‌های کلی نظام و سند چشم انداز ۲۰ ساله کشور پدافند غیرعامل را تعریف کرده و بر این اساس مجموعه اقدامات

غیرمسلحانه‌ای که به افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسلیح مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن منجر می‌شود، پدافند غیر عامل می‌داند.

با مدنظر قرار دادن نتیجه‌گیری به عمل آمده پیشنهادی که می‌توان آن را مطرح نمود، این موضوع می‌باشد که با توجه به فراگیر شدن علوم مرتبط با فضای سایبر در میان جوانان و بالندگی دانشگاه-های کشور در این زمینه، می‌توان سربازان این ارتش نوین را از میان مشمولین سربازی متخصص در این زمینه فراهم نمود که البته این مسئله زمینه‌ساز بهینه‌تر شدن دوران سربازی و استفاده از نیروی متخصص ارزان‌تر می‌باشد.

فهرست منابع:

الف– منابع فارسی

- باستانی، برومند (۱۳۸۳)، جرایم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری، بهنامی، تهران
- بای، حسین‌علی و پورقهرمانی، بابک (۱۳۸۸)، بررسی فقهی و حقوقی جرایم رایانه‌ای، پژوهشگاه علوم و فرهنگ اسلامی، قم،۲۱.
- پورقهرمانی، بابک و صابرنژاد، علی (۱۳۹۲)، ضرورت تدوین قواعد بین‌الملل برای مبارزه با جنگ سایبری، چهارمین همایش مجازی بین‌الملل ایران و جهان،۳۹
- صابرنژاد، علی (۱۳۹۲)، حریم خصوصی در فضای سایبر در حقوق بین‌الملل، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد مراغه.
- ضیایی بیگدلی، محمدرضا (۱۳۸۰)، حقوق جنگ، چاپ دوم، انتشارات دانشگاه علامه طباطبایی، تهران.
- ضیایی بیگدلی، محمدرضا (۱۳۸۶)، حقوق بین‌الملل عمومی، چاپ سی‌ام، انتشارات گنج دانش، تهران.
- قاجار قیونلو، سیامک (۱۳۹۱)، مقدمه حقوق سایبر، چاپ اول، نشر میزان، تهران.
- مرکز پدافند غیر عامل فاوا (۱۳۸۸)، جنگ سایبری، مجله پردازشگر، سال هفتم، ش ۶۴. تهران.
- مسعودی، امیر (۱۳۸۳)، امنیت اطلاعات در فضای سایبر، نشریه کتاب ماه، تهران.
- نوس بام آرتور (۱۳۳۷)، تاریخ حقوق بین‌الملل، زیر نظر احمد متین دفتری، انتشارات امیرکبیر، تهران.
- هالپین ادوارد و دیگران (۱۳۸۹)، جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی، ترجمه آرانی روح‌الله، مرکز پژوهش‌های مجلس، تهران.
- هاشم‌پور حمیدی، هادی (۱۳۹۳)، مفهوم توسل به زور در حقوق بین‌الملل در جنگ سایبری، دومین کنفرانس دفاع ملی سایبری، دانشگاه امام حسین (ع)، تهران.

ب – منابع انگلیسی

- Black-law-dictionary, approaches to cyber space, London ash gate publishing.2004
- Chaney Scott, "Rethinking the Cyber Threat A Framework and Path Forward", Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA, 2009
- Clark, Richard, e ، War from Cyberspace ، the National Interest, 2009
- Cornish, Paul ، David Livingstone ، On Cyber Warfare ، a Chatham House Report ، the Royal Institute of International Affairs, 2010
- Haller, John & Merrell, Samuel A. & Bukovina, Matthew J. & Willkie, Bradford J, Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Software Engineering Institute,2010
- Lord Kristin and sharp, Travis, "America's Cyber future Security and Prosperity in the Information Age", Center for a New American Security, Volume I, 2011

- Michael Alex ،Cyber Probing ،the Politicization of Virtual Attack,Research & Assessment Branch (R&AB), Swenson, United Kingdom,2010
- Singer P.W. and Friedman A. 2014, Cyber security and Cyber war, Oxford.
- http//www.eweek.com/security/slideshows/ddos-attack-volume-escalates-as-new-methods-emerge.html (last visit 31.12.2014)
- http//www.securityfocus.com/news/11392 (last visit 31.12.2014)