فصلنامه مطالعات جنگ
سال دوم، شماره ششم، پائیز ۱۳۹۹
مقاله پنجم از صفحه ۱۰۰ تا ۱۲۶

واکاوی تهدیدات نوین سایبری در نیروهای مسلح

علی‌اصغر بوژمهرانی*[۱]، محمدرضا مهدوی حاجی[۲]

دریافت مقاله: ۹۹/۰۵/۰۷ پذیرش مقاله: ۹۹/۰۸/۱۷

چکیده

تهدیدهای سایبری پدیده‌ای جدید است که با تحول فناوری‌های نوین در جهان گسترش یافته است، اگرچه جنگ سایبری به معنای واقعی تابه‌حال صورت نگرفته است ولی حملات روزانه سایبری حکایت از چشم‌انداز مخوف جنگ سایبری در آینده دارد. با پیشرفت روزافزون این حوزه و وابستگی نیروهای مسلح کشورها به این تکنولوژی می‌توان به این حقیقت رسید که جنگ‌های دهه‌های آینده جنگ سایبری خواهد بود و این مقاله در پی پاسخ به این پرسش است که تهدیدات نوین سایبری علیه نیروهای‌مسلح چیست و راهکارهای مقابله با آن کدام‌اند؟ در پاسخ به این پرسش در راستای آموزش، ارتقای امنیت، ایمنی و پایداری زیرساخت‌های حیاتی نیروهای‌مسلح در مقابل تهدیدات احتمالی‌سایبری دشمن اقدامات مثمر ثمری در سطح سازمان‌های نیروهای مسلح صورت پذیرفته است. لذا می‌توان گفت فضای اطلاعاتی و سایبری به همین نسبت که می‌تواند فرصت‌های بسیار زیادی را برای نیروهای مسلح کشورمان به وجود آورد به همان اندازه نیز می‌تواند تهدیدهای بزرگی را برای این بخش ایجاد نماید. بر این اساس امروزه افزایش توانمندی نیروهای مسلح، ارتقاء مهارت سایبری، تربیت نیروهای زبده، شناخت تهدیدات نوین‌سایبری و چالش‌های آن در جنگ‌های اطلاعاتی آینده سایبری، برای مقابله با تهدیدهای امنیتی، مهم‌ترین راهکار برای حفظ منافع ملی و زیرساخت‌های حیاتی در فضای سایبری بوده که برای موفقیت استراتژی دفاع بایستی اهداف، تجهیزات و قابلیت تهاجمی سایبری به‌عنوان یک اسلحه برای فرماندهان نظامی و کارشناسان دفاعی و نظامی کشور شناخته شود.

واژگان کلیدی: تهدیدهای سایبری، جنگ سایبری، جنگ اطلاعات، چالش‌های امنیتی، فضای سایبر.

۱- کارشناس مهندسی تکنولوژی نرم‌افزار رایانه amboj110@gmail.com
۲- کارشناس ارشد مدیریت دانش و فناوری اطلاعات mahdavihaji20@gmail.com

مقدمه

همواره یکی از موضوعات حیاتی و انکارناپذیر در زندگی بشر، جنگ و نبرد بوده است. کشورها خواسته یا ناخواسته، به‌طور دائم با این پدیده روبه‌رو خواهند بود. با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و در عین حال نامتوازن ساختار فناوری اطلاعات، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و پرداخت سریع و در عین حال نظام‌مند، معقول و هدفمند به‌منظور مصون‌سازی این بستر از تهدیدات موجود در جهات حفظ امنیت ملی و مخاصمات امروز بین‌المللی را می‌طلبد، ازاین‌رو تحول عظیم در فن‌آوری‌ها، به ویژه فن‌آوری اطلاعات که از آن به‌عنوان انقلاب در امور نظامی نام برده می‌شود، موجب ظهور تغییرات اساسی در سازمان‌های نظامی شده است (یادگاری و همکاران، ۱۳۹۶:۳).

در این شرایط نوین، ادبیات سازمان‌های نظامی به‌واسطه پیدایش فن‌آوری اطلاعات، به‌طور اساسی متحول شده است. بسیاری از مفاهیم و فنون فرماندهی، سازمان‌دهی و چگونگی دفاع، تغییر یافته و فضای تهدید و چگونگی عملیات رزم تحت تأثیر این حوزه قرار گرفته است. کیفیت و مفاهیم نظامی شامل دکترین، سازمان، آموزش، تجهیزات و تسلیحات، رهبری و مدیریت، مهارت‌ها و نیروهای نظامی نیز به شدت تحت تأثیر این روند قرار گرفته‌اند.

حضور سامانه‌های پیچیده ارتباطی و الکترونیکی نوین، سناریوی نبردهای آینده را طوری تغییر داده که از یک‌سو این سامانه‌ها به فرماندهان در تصمیم‌سازی بر اساس 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 آسیب‌پذیر نموده است (بختیاری،۱۳۹۳:۲).

در چارچوب اهمیت سطح مناسبات امنیت سایبری در منازعات آینده، کشورها با هدف ارتقاء سطح امنیت ملی خود، به این سمت خواهند رفت که از تاکتیک‌های جنگی غیرمعمول به‌عنوان راهکار جنگی در مواجهه با نیروهای نظامی پیشرفته استفاده نمایند. تکنولوژی‌هایی همچون ماهواره، اینترنت، تلفن همراه و سایر سیستم‌های اطلاعاتی با قابلیت‌های بالا که قادرند حجم

قابل‌توجهی از اطلاعات را ذخیره و انتقال دهند، به شکل گسترده‌ای می‌توانند عملیات‌های جنگی مخربی را در فضای سایبر بر علیه کشور هدف سازمان‌دهی نمایند. بر اساس شکل‌گیری چنین روندهایی است که مؤسسات فعال در حوزه مطالعات آینده پیش‌بینی می‌کنند که تا سال ۲۰۲۵ برخی از کشورها احتمالاً از سلاح‌هایی استفاده می‌کنند که جهت تخریب و نابودی سیستم‌ها و شبکه‌های اطلاعاتی، حس‌گرها، سیستم‌های ارتباطی و الکترومغناطیسی طراحی شده‌اند (فرزاد رستمی، ۱۳۹۵:۴).

از طرفی فرماندهان عملیات‌های مشترک با الحاق فضای سایبر به‌عنوان بعد پنجم میدان نبرد به عرصه‌های سنتی، از قدرت نرم و سخت جنگ سایبری بهره برده و با ترکیب آن به آلیاژی جدیدی به نام قدرت هوشمند دست یافته‌اند. شاخصه‌های منحصربه‌فرد عرصه سایبری موجب پراکندگی قدرت شده و میل به جنگ ناهمطراز را به شدت نزد بازیگران افزایش داده و قدرت‌های نظامی بزرگ را با چالش مواجه کرده است (اسماعیل‌زاده، ۱۳۹۱: ۱). آنچه مطالعه حاضر به دنبال آن است، بررسی این موضوع است که اساساً با توجه به پیچیدگی‌های روز افزون تحولات نظام بین‌الملل و تعاملات تنگاتنگ و نزدیک، فعل و انفعالات سیاسی و فرآیندهای نظامی به دلیل گستردگی میدان نبرد در این حوزه که محیط جنگ‌های پیشرفته را به شدت گسترش داده است؛ تهدیدات نوین سایبری علیه نیروهای مسلح جمهوری اسلامی ایران کدام‌اند و راهکارهای مقابله با تهدیدها و چالش‌های فرارو چگونه است؟

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 با 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

---

1. Cyberspace
2. Norbert Wiener

ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (کامپیوترها) است. با توسعه اینترنت، واژه‌های ترکیبی بسیاری از کلمه سایبر مانند؛ فضای سایبر، شهروند سایبر، پول سایبر، فرهنگ سایبر، راهنمای سایبر، تجارت سایبر، کانال سایبر و... به وجود آمده‌اند.

واژه "فضای سایبر" را نخستین بار ویلیام گیبسون[1] نویسنده داستان علمی تخیلی "پرنینگ گروم" در کتاب نورومسر[2] در سال ۱۹۸۴ به کار برده است. فضای سایبری به فضایی اطلاق می‌شود که با استفاده از فناوری اطلاعات و ارتباطات و شبکه‌ها اجزا و ساختارهای آن بر پایه تخیل‌های فاقد مبنای واقعی و یا بر پایه واقعیت‌های شبیه‌سازی شده طراحی و ابداع می‌گردد. (بختیاری،۱۳۹۳: ۳).

یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها با حرکات ماوس صورت می‌گیرد. در واقع می‌توان گفت که فضای سایبر گستره‌ای از ذهن است که می‌تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد. با این رویکرد ارتباط سایبری به مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق کامپیوتر و وسایل مخابراتی بدون در نظر گرفتن جغرافیا گفته می‌شود. یک سیستم آنلاین نمونه‌ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها و یا حرکات ماوس صورت می‌گیرد (بختیاری،۱۳۹۳: ۳-۵).

فضای سایبر سیستم عصبی و به عبارت دیگر سیستم کنترلی مملکت محسوب می‌شود. فضای سایبری 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

---

1. WilliamGibson
2. Neuromancer

اساسی در امنیت ملی و اقتصاد دارد. (حسن بیگی، ۱۳۸۸: ۲۶۹). در نوامبر ۲۰۰۵، فرمانده نیروی هوایی، مایکل دبلیو وین و ژنرال مایکل موزلی 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 آینده‌پژوهی علوم و فناوری دفاعی، ۱۳۸۸: ۱). فضای سایبر فضایی است که در آن فعالیت‌های گوناگون در ابعاد داده‌ورزی و اطلاع‌رسانی، ارتباطات و ارائه خدمات، مدیریت و کنترل از طریق ساز و کارهای الکترونیکی و مجازی انجام می‌پذیرد. (صدر و دیگران، ۱۳۸۸: ۱) فضای سایبر از نگاه دیوید بل یکی از صاحب‌نظران حوزه ارتباطات فضای سایبر یک شبکه گسترده جهانی است که شبکه‌های مختلف رایانه‌ای در اندازه‌های متعدد و حتی رایانه‌های شخصی را با استفاده از سخت‌افزارهای گوناگون و با قراردادهای ارتباطی به یکدیگر متصل می‌کند. فناوری‌های ارتباط از راه دور اساس فضای سایبر را تشکیل می‌دهد. هرچند برخی از این فناوری‌ها مانند تلگراف و تلفن در اوایل قرن نوزده اختراع شده بودند اما همه‌گیر و ارزان شدن این فناوری‌ها و بالا رفتن توان فنی آن‌ها که شرط اصلی ظهور فضای سایبر است در چند سال اخیر اتفاق افتاده است. در دیدگاه جامعه‌شناسانه 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. در این رویکرد فضای سایبر شامل؛ فضایی خیالی که در آن افکار مجذوب توهمی رویاگونه می‌شود، دنیای مفهومی تعاملات شبکه شده بین افراد و آفریده‌های معنوی‌شان و هر چیز همراه با شبکه‌ها و تعاملات آن، حالتی از اندیشه که توسط افراد در ارتباط و به وسیله 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 (بختیاری،۱۳۹۳: ۳–۵).

در فرهنگ اصطلاحات نظامی، فضای سایبری به‌عنوان یک حوزه جهانی در داخل محیط اطلاعات تعریف می‌شود که متشکل از شبکه‌های به هم وابسته از زیرساخت‌های فناوری اطلاعات است: از

قبیل اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های کامپیوتری، پردازنده‌ها و کنترل‌کننده‌ها، درواقع محیط الکترونیکی که شامل دستگاه‌ها، شبکه‌ها و سخت‌افزارهای ارتباط دهنده آن‌ها است که در فضای مجازی قرار گرفته است. این یک محیط ملموس نیست که کسی بتواند ببیند یا احساس کند، اما عاملی است که سریع‌تر از اندیشه و فکر است و داده در یک چشم به هم زدن در سراسر جهان انتقال می‌یابد در ۲۰ سال گذشته، استفاده از قابلیت‌های سایبر در مراکز مهم فرماندهی و کنترل و بخش پدافندی برای حفاظت بوده است و به توانایی آفندی سایبر توجه کمتری شده است. اخیراً رویکرد استفاده از سایبر به‌عنوان وسیله‌ای برای دستیابی به اهداف ملی تغییر کرده است. لذا فضای سایبر نه تنها بایستی مورد توجه فرماندهان نظامی قرار گیرد بلکه از قابلیت تهاجمی سایبری به‌عنوان یک اسلحه نیز باید استفاده شود (عبدالهی، ۱۳۹۴: ۳)

فضای سایبر به مجموعه‌ای از ارتباطات انسان‌ها از طریق رایانه‌ها و وسایل مخابراتی در یک محیط غیر فیزیکی و الکترونیکی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود که در آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود و کاربران آن می‌توانند از طریق رایانه‌ها با یکدیگر ارتباط برقرار کنند. برخلاف فضای واقعی که در آن از حواس پنج‌گانه طبیعی استفاده می‌شود در فضای سایبر از عناصری مثل فایل‌ها، پیغام‌های الکترونیکی، عکس‌های فیلم‌ها و ... استفاده می‌شود و نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال از طریق فشردن کلیدها با حرکات ماوس صورت می‌گیرد. در حال حاضر ارتش ایالات‌متحده به‌طور چشمگیری در جهان مبتنی بر شبکه و فضای سایبر کار می‌کند. به این چیزی که واژه فضای سایبر نامیده شد در حال حاضر بیش از ۱/۱ میلیارد دستگاه ارسال و دریافت داده متصل شده است. این دستگاه‌ها، بهره‌وری و توانایی بشر را برای ارتباطات اجتماعی افزایش می‌دهند، اما ریسک‌پذیری امنیت تبادل اطلاعات بشر را زیاد می‌کند، زیرا سایبر می‌تواند وسیله‌ای برای سرقت اسرار محرمانه از شرکت‌ها و اسرار دولتی از حکومت‌ها باشد و وسیله‌ای برای رسیدن به اهداف سیاسی و نظامی نیز باشد، درحالی‌که

هویت‌سازمانی استفاده‌کنندگان آن‌ها در درون وب ازدیگراشخاص ناشناس پنهان مانده است (کونفیلد[1]، ۲۰۱۳، ۲).

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 (بختیاری،۱۳۹۳: ۵).

امنیت سایبری، تهدیدهای سایبری و پدافند سایبری

فضای سایبری در حال ساخت محیط جدیدی در فضای فرهنگی و هویتی است. تا قبل از عصر سایبر هویت انسان به نژاد، قبیله و عرصه جغرافیایی استوار بود و زیست جهان مشهود و نامشهود در مکان و زمان خاص جغرافیایی فرهنگ را تشکیل می‌داد. با شکل‌گیری فضای سایبر و رشد سریع آن مفاهیم عرصه زندگی نیز به سمت تغییرگام برداشت. همه‌چیز از هویت روابط و تعاملات خصوصی و گروهی در حال تغییر است و انسان در حال تبدیل به انسان سایبری شده با، حکمرانی، فرهنگ تعاملات و مدل زندگی خاص خود است. امنیت در پارادایم فضای سایبری تابع دو عنصر کلیدی انسان و فضای سایبر است. مسئله اول انسان ویژگی‌ها و قابلیت‌هایش است و مسئله دوم ابعاد، قابلیت‌ها و مبانی شکل‌گیری فضای سایبری است. کنش‌وتعامل کنشگران این دو عامل، موجب شکل‌گیری فضای تهدیدزایی شده که ابعاد گسترده و متنوعی را در حوزه امنیت شکل می‌دهد.

امنیت سایبری، ریشه اصلی فنّاوری‌ها، فرآیندها و شیوه‌های طراحی شده برای محافظت از شبکه‌ها، کامپیوترها، برنامه‌ها و داده‌ها در مقابل حملات، خسارات و دسترسی‌های غیرمجاز است. در یک زمینه محاسباتی، امنیت شامل دو بخش امنیت سایبری و امنیت فیزیکی می‌شود و اطمینان

[1]. Coonfield

یابی از امنیت سایبری نیاز به تلاش‌های هماهنگ در سرتاسر سیستم اطلاعات دارد (جزیره امنیت اطلاعات و ارتباطات، ۱۳۹۶).

تهدیدهای سایبری از ماهیتی متنوع، گسترده و منحصربه‌فرد برخوردارند. متنوع ازآن‌رو که این تهدیدها تمام حوزه‌های زندگی بشر را تحت تأثیر قرار داده‌اند و در نتیجه عدم امنیت در فضای سایبری بسیار بالاست. گستردگی نیز از آن رو که نه‌تنها بازیگران دولتی، بلکه شرکت‌های خصوصی، گروه‌ها و افراد را نیز درگیر خود کرده است و منحصر به فرد بودن نیز بدین علت است که ماهیت این تهدیدها متمایز از فایده‌های سنتی و رایج گذشته است. امروزه امنیت سایبری در ارتباط مستقیم با امنیت ملی کشور بوده و نمی‌توان امنیت ملی را منحصراً در ارتباط با مرزهای خارجی و حفاظت از جان شهروندان به‌وسیله نیروهای نظامی تعریف کرد. به‌طورکلی می‌توان امنیت سایبری را به‌عنوان حفاظت از زیرساخت‌های اطلاعاتی مهم و فرایندها و محتوای آن تعریف کرد.

پدافند سایبری؛ پدافند در فضای سایبرعلیه تهدیدات عاملانه واحدهای نظامی سایبری کشورها برعلیه کشور، امروزه کشورهای زیادی ارتش درست کرده که برعلیه اهداف استراتژیک سایبری کشورهای دیگر حمله کنند. منظور از پدافند سایبری هر نوع هک و نفوذ نیست به تهدیدی گفته می‌شود که بتواند با دشمن سازمان یافته در حوزه‌های سایبری مقابله نماید (جلالی، ۱۳۹۰: ۲۳-۵۱).

ماهیت تهدیدات سایبری

تهدیدهای سایبری پدیده‌ای جدید است که در دهه‌های اخیر، هم‌زمان با تحول فن‌آوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به‌گونه‌ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت جدید تهدیدهای نوین سایبری و ویژگی‌ها و نمودهای منحصر به فردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید (خلیل‌پوررکن‌آبادی و نورعلی‌وند، ۱۳۹۱:

۲). در این بخش، پس از تعریف تهدیدهای سایبری، ویژگی‌ها و نمودهای آن را به‌طور مختصر مورد بررسی قرار می‌دهیم.

الف) تعاریف

در همایشی که در ۲ مارس ۲۰۱۰ از سوی موسسه بین‌المللی CMCI و مؤسسه مطالعاتی نیروی دریایی ایالات‌متحده با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، تهدیدهای سایبری به صورت «وقایعی که به صورت طبیعی و یا توسط انسان (به صورت عمدی یا غیر عمدی) بر فضای مجازی تأثیرگذار باشد با حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد» تعریف شد (CACI and USNI,2010). فضای سایبری نیز از سوی برخی کارشناسان به‌عنوان «تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی و یا کاربران آن شکل می‌گیرد» تعریف شده است (لورد و شارپ[1]، ۲۰۱۱: ۲۰).

ب) ویژگی‌های تهدیدهای سایبری

تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند. از یک‌سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه‌کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌های زیر خلاصه می‌شود:

- **تعداد 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 سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت– ملت هستند (چمی، ۲۰۰۹: ۵–۶).
- **هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام:** هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در

[1] . Lord & Sharp

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.

- **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.
- **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 پی‌داشته 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 این گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند (لورد و شارپ، ۲۰۱۱: ۲۰-۲۸).
- **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 (استار[1]، ۲۰۰۹: ۱۸).
- **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 بسیار دشوار کرده است (چرمسی[2]، ۲۰۰۹: ۶-۵). از سوی دیگر، ساختار اینترنت، دولت‌ها و شرکت‌های

---

1 . Starr
2 . Charmcy

خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی‌ها و فن‌آوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است (هالر و همکاران[1]، ۲۰۱۰).

- **پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری:** احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. درنتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیرسایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند (لورد و شارپ، ۲۰۱۱: ۲۰–۲۸).

پ) انواع تهدیدهای سایبری

بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. این اهداف در فضای مجازی از شیوه‌های متفاوتی حاصل می‌شوند که مهم‌ترین آن‌ها عبارت‌اند از: جنگ سایبری، تروریسم سایبری، جرائم سایبری، جاسوسی سایبری و آشفتگی سایبری (خلیلی‌پوررکن آبادی، ۱۳۹۱: ۵).

جنگ و عصر اطلاعات

ظهور عصر اطلاعات مفاهیم و مبانی زندگی دوران صنعتی را دستخوش تحول نمود و به تبع آن در عرصه جنگ، انقلاب اطلاعات به گونه‌ای 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 غیر منتظره 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. برخلاف آنالوگ، شنود و نمونه‌برداری از این اطلاعات تأثیری بر شبکه نمی‌گذارد و اطلاعات تماماً قابل تجمیع است. در این فضا اگر مشکلی در ارسال اطلاعات

[1] . Haller and Et al

پیش آید خود اطلاعات تخریب می‌گردد. در شبکه هر بُعد آن طرف مقابل را نمی‌شناسد اما کسی که شبکه را مدیریت می‌کند اشراف بالایی داشته و همه چیز را می‌تواند ثبت و ضبط نماید. (پورابراهیمی، ۱۳۹۳) تحولات شگرف در جمع‌آوری، ذخیره‌سازی، پردازش، انتقال و ارائه اطلاعات باعث شده اطلاعات در حال تبدیل شدن به یک منبع راهبردی به‌عنوان یک عنصر بانفوذ و ارزشمند در عصر فرا صنعتی همانند نقشی که سرمایه و کار در عصر صنعتی داشتند، شود. انقلاب اطلاعات در حال به چالش کشیدن طراحی سازمان‌هاست به‌گونه‌ای که سلسله مراتب سازمان‌هایی که به‌صورت 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 تغییر جهت در چگونگی کشمکش بین جوامع و برپایی جنگ توسط نیروها می‌شود (بختیاری، ۱۳۹۳: ۵-۶).

جنگ آینده

تا به حال در کتب و مقالات و اسناد منتشر شده حجم گسترده‌ای از ادبیات مربوط به جنگ آینده منتشر شده و بر اساس آنچه که در کتاب جنگ و ضد جنگ تافلرها و فرجام تاریخ و واپسین انسان، در سال ۱۹۹۵ آمده؛ عمده این ادبیات دو رویکرد کلی به موضوع داشته‌اند نخست بر سناریو پردازی در مورد جهان و جنگ آینده و دوم بر توصیف روندهای کنونی و پیش‌بینی جهان آینده بر اساس آن استوار است. جنگ‌های آینده ماهیتاً با جنگ‌های ماقبل و تجربه‌شده حداقل سه تفاوت اساسی دارند؛ ۱) فناوری تسلیحاتی به مراتب پیشرفته‌تر از گذشته ۲) استراتژی‌های جدید نظامی ۳) توجه به شیوه‌های جنگ نامتقارن در آن‌ها (باقری، ۱۳۸۵: ۲۷). در دهه‌های اخیر، نظریه‌پردازان و صاحب‌نظران نظامی و حتی سیاسی عبارت‌های جنگ‌های نوین، جنگ‌های مدرن، 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 به وجود 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 پا به پای 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 هم‌افزایی علوم مختلف و نو اندیشی‌های صورت گرفته در چارچوب نظریات جدید رخ نموده است. در چند دهه اخیر شکل جنگ به مرور تغییر یافته و به نظر می‌رسد 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 ایالات‌متحده 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[1] بر پنج حوزه قابل‌شناسایی در فناوری‌های تسلیحاتی جنگ‌های آینده در زمینه‌های قدرت آتش، تحرک، ارتباطات، محافظت و اطلاعات تأکید دارد و جی. ای. سینگ[2] در این زمینه به فناوری‌های نظامی قابل به‌کارگیری در ضربات ایستگاهی دقیق، فرماندهی، کنترل و اطلاعات پیشرفته، جنگ اطلاعاتی، و جنگ غیر کشنده اشاره دارد.

تافلر[3] نیز در کتاب «جنگ و پاد جنگ» بر ویژگی‌هایی همچون تنوع و دگرگونی، غیر انبوه‌سازی، برخورداری از پایه‌ها و زیرساخت‌های غیرنظامی، سرعت عمل و تحرک، قدرت تخریب، انسجام و پیوستگی، فناوری‌های حفاظتی و حجم و دقت بالای آتش به‌عنوان مشخصه‌های اصلی فناوری‌های نظامی در جنگ‌های پست مدرن تأکید دارد (بختیاری،۱۳۹۳: ۵-۶).

ویژگی‌های جنگ‌های آینده

مطالعات نشان می‌دهد جنگ آینده احتمالاً موضوعی است که تقریباً همه کشورها در طرح‌ها برنامه و ملاحظات دفاعی و امنیتی خود به آن پرداخته و بسته به نوع تهدیدی که در حریم امنیتی خود

---

1. Bary Bozan
2. J.A.Sing
3. Tafler

داشته‌اند آن را مطرح ساخته‌اند. اگرچه دیدگاه‌های مختلفی مطرح شده اما نهایتاً همه کشورها در مواردی اشتراک نظر دارند، اینکه در جنگ‌های آینده:

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

ب) جنگ‌ها در آینده کوتاه مدت، مستمر، سریع و شدید خواهند بود و قسمت عمده لوازم و زمینه‌های 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) به دلیل شکاف استراتژیک قدرت بین بازیگران بین‌الملل نقش نبردهای نامتعارف و نامنظم در جنگ‌ها بسیار پررنگ خواهد بود و قدرت‌های برتر در مقابله با شیوه‌های جنگ نامنظم و نامتقارن آسیب‌پذیر خواهد بود.

ز) مقاومت، شکیبایی، میل به از خود گذشتگی و شجاعت راه‌های مؤثری 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 می‌دهد.

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

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

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

ک) غیرقابل پیش‌بینی بودن حوادث و وضعیت‌ها به دلیل رویکرد نامنظم در جنگ‌های آینده (بختیاری،۱۳۹۳: ۸).

جنگ سایبری

۱.جنگ سایبر به هرگونه عمل خصمانه علیه سیستم‌های رایانه‌ای، شبکه‌های رایانه‌ای با پایگاه‌های داده رایانه‌ای دشمن اطلاق می‌شود که با هدف کاهش کارایی یا ناتوان‌سازی صورت پذیرد. حملات سایبری، سیستم‌های هدف خود را غیرقابل استفاده نموده کارایی آن‌ها را کم کرده با تزریق اطلاعات غلط تصمیم‌گیری کاربران را کاهش می‌دهند و حتی منجر به سرقت اطلاعات می‌شوند. به بیانی دیگر جنگ سایبر عبارت است از به‌کارگیری برنامه‌ریزی شده عملیات آفندی و پدافندی که در آن توسط یک ابزار رایانه‌ای علیه ابزار رایانه‌های دیگر حملاتی صورت می‌گیرد ضمن اینکه به کارگیری تعمدی ابزارها و شبکه‌های رایانه‌ای به‌منظور اثرگذاری بر تصمیم‌گیری مخاطبان را نیز باید در زمره جنگ سایبر به حساب آورد (محمدی، ۱۳۸۹: ۱۱)

۲.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) به‌عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند و از مقاصد آن انجام کارهای خشونت‌بار 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 به‌عنوان بستر انجام این اعمال خرابکارانه استفاده می‌کند. مارتین لیبیکی، از محققان برجسته موسسه مطالعات استراتژیک در دانشگاه دفاع ملی آمریکا، در کتاب «جنگ اطلاعاتی[1] 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 می‌شود.»

مگان برتر در سال ۱۹۹۹ با نگرشی کلی می‌گوید؛ جنگ اطلاعاتی طبقه یا مجموعه‌ای از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات

[1]. Information Warfare

است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست یافتـه و آن را حفظ می‌کند.

مارتین لیبیگی ضمن وفادار ماندن به تعریف کاملاً نظامی از جنگ اطلاعاتی هفـت شـکل مختلـف جنگ اطلاعاتی را به شرح زیر نام می‌برد.

- جنگ فرماندهی و کنترل[1] که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.
- جنگ بر پایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم‌هایی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
- جنگ الکترونیک با استفاده از تکنیک‌های رادیویی، الکترونیک، یا رمزنگاری.
- جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرز فکر دوستان، بی‌طرف‌ها و دشمنان استفاده می‌شود.
- جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
- جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات با تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی
- جنگ سایبر ترکیبی از همه موارد شش‌گانه 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؛ تـلاش ایـن جنـگ در جهـت شناسـایی مسائلی است که دشمن به شدت از آن محافظت می‌کند. این جنگ حرکتی در جهت "تغییر تـوازن اطلاعات و دانش" به نفع یک طرف است، به خصوص اگر توازن نیروها برقرار نباشد. (بختیـاری، ۱۳۹۳: ۱۰)

۳.عبارت است از اقدامات آفندی غیر متحرکی که به‌منظور کسب برتری اطلاعاتی از طریق تحت تأثیر قرار دادن سامانه اطلاعاتی و شبکه‌های رایانه‌ای دشمن اتخاذ می‌گردند (کلمنس، ۱۹۹۹). بر اساس این تعریف به نظر می‌رسد که جنگ سایبری زیرشاخه‌ای از جنگ اطلاعاتی بوده و

[1]. Command and Control Warfare

شامل اقداماتی است که در فضای سایبری در تقابل با فضا با دنیای واقعی صورت می‌پذیرد، بستر جنگ سایبری عبارت است از هر سامانه واقعیت مجازی که در برگیرنده مجموعه‌ای از رایانه‌ها و شبکه‌ها باشد. یکی از شاخص‌ترین محیط‌های جنگ سایبری، اینترنت و شبکه‌های نظامی یا غیرنظامی مرتبط می‌باشد که به نحوی اطلاعات را به اشتراک می‌گذارند. جنگ سایبری ارتباطی تنگاتنگ با مفهوم سایبرنتیک دارد که به معنای "دانش کنترل و ارتباط در انسان، حیوان و ماشین" می‌باشد. امروزه اغلب سامانه‌های کنترل و ارتباط با استفاده از تراشه‌های حافظه و واحدهای ریزپردازنده خودکار شده و به هدفی ایده‌آل برای رزمنده سایبری تبدیل گشته‌اند که حیطه مطلق سایبرنتیک محسوب می‌شود. یک مزاحم الکترونیکی با تروریسم سایبری از هر کجای دنیا قادر است به رایانه‌های موجود در یک شبکه متصل، وارد شود. به دست آوردن جواز ورود به رایانه‌ها از طریق ارتباطات شبکه نسبتاً آسان، ارزان و نوعاً فاقد خطرپذیری کشف و دستگیری است (بختیاری، ۱۳۹۳: ۱۱).

انواع جنگ سایبری

جنگ سایبری به شیوه‌های مختلفی شکل می‌گیرد؛ که کارکرد و اساس اجرایی آن‌ها از فرآیند پیچیده‌ای 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 به‌وضوح بیان می‌کند.

جدول شماره ۱: انواع جنگ سایبری (بختیاری، ۱۳۹۳)

مؤلفه‌های کارکردی / نوع جنگ	امکانات	عملکرد	اثرگذاری
نفوذ سایبری	یک سامانه با کنترل نرم‌افزاری	تهاجم و دست‌کاری به شیوه نفوذ و یورش سایبری	اختلال در شبکه و سرریز شدن اطلاعات سیستم
دست‌کاری سایبری	یک سامانه با کنترل نرم‌افزاری	به دست گرفتن کنترل سامانه‌ها از طریق نرم‌افزارهای مرتبط	ایجاد خرابی و خسارت در سامانه، خاموش کردن سیستم‌ها و مختل

			کردن شبکه‌ها
تاخت سایبری	نرم‌افزار و پست‌های الکترونیکی	ارسال ویروس‌های برای حمله به سامانه و از بین بردن کارایی آن	تخریب نرم‌افزارها و داده‌ها در یک سامانه
دستبرد سایبری	نرم‌افزارهای جاسوسی و پست-های الکترونیکی	سرقت پست الکترونیک به‌دست‌آوردن فهرست گذرواژه‌ها	انتقال، تخریب و یا تغییر و در اختیارگرفتن اطلاعات
عاملان سایبری غیرعمدی	اپراتورهای سایبری، نیروهای سایبری، رزمندگان سایبری	عمد و قصد نیت جنگ سایبری	اثرگذاری بر برخی مواقع جدی می‌شود اما غیرعمدی است.
عاملان سایبری عمدی	مخاطرات	اقدام غیرعمدی	تهدید امنیت ملی
ویروس افکنی	افراد	وارد نمودن دستی یا الکترونیکی یک ویروس یا کد ویروس به سامانه‌ها	ازبین‌بردن کارایی رقبا و سرقت اطلاعات آن‌ها

نفوذگران و هکرها نیز در فرایند کارکرد تکاملی جنگ سایبری ابزار زیربنایی محسوب می‌شوند تبیین روابط و میزان اثرگذاری هرکدام از این نفوذگران در محیط تعاملی سایبری اهمیت دارد (بختیاری، ۱۳۹۳: ۱۲).

اثرات کلی فنون جنگ سایبری بر تجهیزات

نفوذ در ارتباطات فیبرنوری کمی پیچیده است اما نوارهای مغناطیسی در مقابل جنگ سایبر کاملاً آسیب‌پذیر بوده و دیسک‌های سخت نیز مستعد پذیرش آسیب‌های جدی هستند. تکنیک‌های جنگ سایبری در ارتباطات ماهواره‌ای بسیار مؤثرانـد زیرا این سیستم‌ها عموماً به کشورهای صاحب فناوری ماهواره وابسته‌اند و فناوری ارسال و دریافت آن علیرغم استفاده از سیستم رمز آسیب‌پذیر است. سیستم‌های ارتباطی ماکروویو در ماهیت ایستا بوده و لذا با استفاده از تجهیزات سد کننده به‌سادگی قابل سد شدن هستند. بمب‌های پالس الکترومغناطیسی تأثیرات مخربی بر این تجهیزات دارند.

مفهوم جنگ سایبری به دنبال ظهور فناوری‌های عصر اطلاعات نظیر ماهواره، پست الکترونیک، اینترنت، رایانه و سایر ریز تراشه‌ها و تبدیل جهان به یک دهکده مطرح گردیده است. جنگ سایبری هر سه ضلع مثلث دولت، ملت و نیروهای مسلح را شامل می‌شود 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 به کار می‌گیرند. این جنگ نه تنها وب سایت‌های بخش‌های دولتی و خصوصی دشمن را مورد حمله قرار می‌دهد، بلکه هدف‌های با ارزش‌تر نظیر شبکه‌های کنترل تأسیسات و تجهیزات نظامی را نیز مدنظر دارد. برخی از مصادیق جنگ سایبری عبارت‌اند از:

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

۲.قطع کامل سیستم‌های 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 حمل‌ونقل هوایی و ریلی سامانه‌های نظامی که به نوعی به رایانه‌ها متکی هستند در برابر جنگ سایبر آسیب‌پذیرند که نمونه‌هایی از آن عبارت‌اند از: سامانه‌های فرماندهی و کنترل مکانیزه (C4ISR) سامانه‌های 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، شناورها، پیاده و هوانیروز که برای تعیین موقعیت دشمن و اهداف، تعیین برد یا فاصله،

[1]. Nation- state

رهگیری، آتش و سایر اعمال به رایانه متکی باشند اهداف خوبی را برای جنگ سایبری تشکیل می‌دهند. تعدادی از این موارد عبارت‌اند از: کشف راداری، کنترل و هدایت موشک‌ها، کنترل آتش، شناسایی دوست از دشمن و اطلاعات حاصله از سیستم موقعیت‌یاب 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 کار اندازی 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 به‌عنوان یکی از اهداف اصلی در لحظات اولیه تهاجم در جنگ‌های اخیر مورد توجه ویژه قرار داشته است، لذا بایستی طراحی، مهندسی، پیاده‌سازی و به‌کارگیری آن‌ها را در تمامی سطوح مدیریتی به‌صورت هوشمندانه عمل نماییم. امروزه با گره خوردن فناوری اطلاعات در مأموریت تمامی دستگاه‌های اجرایی کشور حتی کوچک‌ترین عملکردهای اجرایی، قابلیت‌های ممتازی را در مأموریت آن‌ها اضافه نموده است به نوعی که شاهدیم توسعه این زیرساخت همواره به‌عنوان افتخارات مدیران در ارائه گزارش‌های پیشرفت عملکرد آن‌ها ارائه می‌گردد. 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 بالا بردن توان مدیریت را در این شرایط تسهیل نماید؛ اما به دلیل 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 هم‌افزایی 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 برعلیه زیرساخت‌های مراکز ثقل توسعه داده و بر اساس آن طرح‌های 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 می‌گردد (بختیاری، ۱۳۹۳: ۱۸-۱۶).

تهدیدها و چالش‌های امنیتی در جنگ‌های سایبر

حکومت، بخش خصوصی و شهروندان، همگی از جانب بازیگران دولتی یا غیردولتی، مجرمان سازمان‌یافته و گروه‌های تروریستی هستند. علی‌رغم رشد آگاهی و شناخت جهانی از فضای سایبر، ماهیت، نوع، ابزار، تکنیک‌ها و تاکتیک‌های حملات در جهان مجازی همچنان ناشناخته باقی مانده است (شاختیمان[1]، ۲۰۱۱). ماهیت تهدیدها در جنگ‌های سایبر برخلاف جنگ‌های سخت‌افزاری مبهم و نامشخص هستند. در این فضا شناسایی ماهیت و انگیزه بازیگرانی که تنها با هدف مجرمانه حملاتی را طراحی می‌کنند از اهداف گروه‌هایی که دارای انگیزه سیاسی هستند، کار بسیار پیچیده‌ای است (لین[2]، ۲۰۱۱).

با وجود این، شناسایی ماهیت و انگیزه‌های واقعی دشمنان در فضای مجازی برای تدوین سیاست‌های کارآمد امنیتی بسیار مهم تلقی می‌شود؛ از طرفی می‌توان گفت ماهیت تهدیدها در جنگ‌های سایبری به تناسب بازیگران آن متفاوت است؛ بنابراین ماهیت تهدیدها در فضای مجازی متناسب بااینکه این حملات از جانب دولت‌ها، گروه‌های افراط‌گرای ایدئولوژیکی یا سیاسی، مجرمان سازمان‌یافته یا گروه‌های کوچک طراحی شده باشد، متفاوت خواهد بود. با وجود این وجه مشترک همه تهدیدهای سایبر، عدم تقارن آن‌ها است. بر همین اساس از جنگ سایبر معمولاً با عنوان جنگ نامتقارن نیز نام برده می‌شود (ماه پیشانیان، ۱۳۹۰: ۶).

تهدیدهای مستقیم نظامی در فضای سایبر

تکنولوژی‌های سایبر با دارا بودن عملکردهای بسیار مشخص نظامی می‌توانند به‌طور مستقیم بر میدان نبرد تأثیرگذار باشند. بخش نظامی هر کشوری برای آموزش و تجهیز نیروها، سیستم‌های جنگ‌افزاری، ماهواره‌ها و شبکه‌های ارتباطی با داده‌پردازی اطلاعات به تکنولوژی‌های سایبری وابسته است. در واقع می‌توان گفت فضای اطلاعاتی و سایبری به همان نسبت که می‌تواند فرصت‌های بسیار زیادی را برای نیروهای نظامی هر کشور به وجود آورد، به همان میزان نیز

---

1 . Shachtiman
2 . Lynn

می‌تواند تهدیدهای بزرگی را برای این بخش ایجاد کند. بنابراین امروزه سرنوشت جنگ را دیگر تخریب‌ها، انفجارها و عملیات فرسایشی تعیین نمی‌کنند بلکه از هم گسیختگی ظرفیت‌های فرماندهی و کنترل در فضای مجازی می‌تواند بسیار برای نتیجه برخوردها تعیین کننده باشد. علاوه بر این، امروزه بعد اطلاعاتی به‌عنوان یکی از ابعاد محوری جنگ در همه عملیات‌ها، رزم‌ها و نبردهای آینده دخیل خواهد بود. همچنین در جنگ‌های‌آینده، کسب برتری سریع درحوزه اطلاعاتی یکی از عوامل مهم موفقیت خواهد بود (ماه پیشانیان،۱۳۹۰: ۶).

نتیجه‌گیری و پیشنهادها

فضای سایبری و فناوری‌های وابسته به آن، یکی از مهم‌ترین منابع قدرت در هزاره سوم هستند، با عنایت به اهمیت شبکه جهانی اطلاع‌رسانی به‌عنوان یک پدیده غیرقابل انکار عصر فرا مدرن که واجد فرصت‌های بسیار و حامل تهدیدهای جدی است، طراحی استراتژی جمهوری اسلامی ایران در ارتباط با فناوری اطلاعات و بهره‌مندی از فرصت‌ها و تهدیدها به موازات تقویت نقاط قوت و قدرت سایبری در پنجمین عرصه نبرد و تدبیر در ترمیم نقاط ضعف در این حوزه از اهمیتی ویژه برای امنیت ملی و نیروهای مسلح جمهوری اسلامی ایران برخوردار است. ارتش‌ها با سلاح نرم‌افزار در حال ساختن برج و باروهای دفاعی خود در حوزه سایبر و جنگ سایبری هستند تا نوعی از بازدارندگی را در برابر دشمن به نمایش بگذارند. کنترل و هدایت پتانسیل‌های بالقوه این عرصه و در صورت نیاز به فعلیت درآوردن آن سبب در اختیار گرفتن نیروی فوق‌العاده‌ای می‌گردد که به سادگی موازنه قوا را به نفع یکی از طرفین تغییر می‌دهد. به همین دلیل این نوع جنگ از اقبال خوبی در بین تمامی کشورها برخوردار است. کشورهای توسعه یافته که متولی زیرساخت‌های فن‌آوری هستند به راحتی می‌توانند از چالش‌ها و فرصت‌های آن استفاده کرده و دیگر کشورها را با خسارات احتمالی روبرو کنند، نیروهای مسلح به دلیل گستردگی میدان نبرد در این حوزه و برای ارتقای امنیت، ایمنی و پایداری زیرساخت‌های حیاتی خود در مقابل تهدیدات احتمالی سایبری و پاسخگویی به موقع و مناسب و برای ایجاد اختلال در اطلاعات نظامی دیگران از طریق ابزارهای رایانه‌ای و اینترنت، ایجاد آشفتگی و سردرگمی در فرآیند تصمیم‌گیری

گروه‌های هدف، تلاش برای شکل دادن به افکار عمومی جامعه هدف، ایجاد اختلال در تجهیزات راداری، موشکی و پردازش و تحلیل اطلاعات که از جمله مصادیق پیشرفت‌های انقلاب اطلاعاتی بوده و تحت عنوان فرآیندهای جنگ آینده اطلاعات مورد استفاده قرار می‌گیرد، بایستی ضمن کسب مهارت‌های لازم و تربیت نیروهای دیجیتالی زبده و استفاده حداکثری از ظرفیت فناوری اطلاعات، فرصت‌های جدیدی را برای بهبود و ارتقاء شیوه‌های استفاده از این فضا و همچنین شاخص‌های آن جهت حفظ و پایداری سامانه‌ها و دفع دسیسه‌ها و نیات پلید دشمن در برابر تهدیدات نوین سایبری فراهم نمایند.

هدف از توجه به چنین روندهایی ترسیم چشم‌انداز امنیتی آینده فرماندهان نظامی نیروهای مسلح برای دفع تاکتیک‌های دشمن در بهره‌گیری از فنون جنگ‌های سایبری علیه سیستم‌های فناوری اطلاعات و برنامه‌ریزی‌های استراتژیک برای مقابله با چالش‌های احتمالی و تقویت نقاط مثبت نیروهای مسلح جمهوری اسلامی ایران است تا در صورت اجرای تهدیدها، پایداری را ارتقاء، آسیب‌پذیری‌ها را کاهش و به تداوم خدمات ضروری بر بستر فناوری اطلاعات از سوی سازمان‌های نیروهای مسلح در زمان بحران کمک و بتوانند از قابلیت تهاجمی سایبری به‌عنوان یک اسلحه استفاده نمایند. بدون شک کشورهایی که چنین چشم‌اندازهای را برای آینده خود ترسیم می‌کنند توانایی بیشتری برای مقابله با تهدیدها و چالش‌های فرارو داشته و می‌توانند به گونه‌های بهتری از فرصت‌های ایجاد شده بهره‌برداری نمایند.

راهکارها و پیشنهادها

۱. مقابله با تهدیدات فضای سایبری از طریق آموزش و تجمیع اطلاعات.

۲. توسعه امن زیرساخت‌ها و رعایت اصول پدافند غیرعامل در مراکز فاوا نیروهای مسلح متناسب با پیشرفت‌های تکنولوژی.

۳. ارتقای ضریب امنیت، ایمنی و پایداری، ایجاد و حفظ امنیت زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات نیروهای مسلح در مواجهه با تهدیدات و امکان ادامه مأموریت در شرایط بحران.

۴. ایمن‌سازی زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات نیروهای مسلح در قبال حملات فیزیکی.

۵. تولید دانش فنی و بومی و بهره‌گیری آگاهانه از فناوری مناسب و روزآمد کشور و عرصه بین‌الملل به‌وسیله توسعه جهاد علمی.

۶. کاهش آسیب‌پذیری زیرساخت‌های کلیدی و مراکز ویژه، حیاتی، حساس و مهم نیروهای مسلح در حوزه فناوری اطلاعات و ارتباطات در برابر تهدیدات.

۷. اهمیت ویژه برای برگزاری رزمایش‌های مختلف سایبری و مشترک برای حفظ و ارتقای آمادگی فاواهای نیروهای مسلح در مقابل بحران‌ها.

۸. آموزش و تربیت نیروهای زبده دیجیتالی و به‌کارگیری آنان در سازمان‌های نیروهای مسلح.

۹. ایجاد کمیته‌های مشترک تخصصی سایبری در سطح نیروهای مسلح به‌منظور سیاست‌گذاری و نظارت راهبردی.

۱۰. متناسب‌سازی آموزش‌های تخصصی با نیازهای سازمان‌های نیروهای مسلح.

۱۱. تهیه و تأمین سخت‌افزارهای نیروهای مسلح از داخل کشور و صرفاً از طریق مراکز مصوب و واگذاری آن سازمان‌ها.

۱۲. ارتقاء مکانیزم‌های امن‌سازی متناسب با تکنولوژی‌های نوین و پیاده‌سازی فرهنگ برنامه‌نویسی امن با اجرای استراتژی دفاع چندلایه از عمق و همچنین اتخاذ یک استاندارد کد نویسی امن در نیروهای مسلح.

۱۳. تحلیل و پایش به موقع ترافیک شبکه (NAT[1]) در سازمان‌های نیروهای مسلح با استفاده از آخرین استانداردهای امنیتی.

۱۴. استفاده از هکران حرفه‌ای برای شبیه‌سازی نفوذ در سیستم‌ها و سنجش وضعیت امنیت فناوری اطلاعات و ارتباطات در نیروهای مسلح.

---

[1]. network traffic analysis

۱۵.استفاده از فناوری‌های گمراه کننده[1] (طعمه‌گذاری یا فریب) جهت شناسایی فرایندهای شناختی مهاجمان در شبکه‌های نیروهای مسلح.

۱۶.مطالعه و حرکت به سمت استفاده از رایانش کوانتومی در حوزه امنیت، با توجه به قابلیت‌های بسیار ممتاز این فناوری جهت رمزنگاری داده‌ها و اطلاعات، بهره‌برداری از این تکنولوژی در حس‌گرهای بسیاری دقیق در حوزه الکترونیک، مغناطیس، میدان‌های گرانشی، دما و اندازه‌شناسی کوانتومی به دقیق‌ترین شکل ممکن در پروژه‌های تحقیقاتی نیروهای مسلح نظیر سامانه‌های جنگال، موشکی، پهپادی، شناوری سطحی و زیرسطحی.

۱۷.استفاده راهبردی از عملیاتی‌های اطلاعاتی در نیروهای مسلح.

۱۸.ایجاد، تجهیز و نگهداری شبکه دیتا و طیف الکترومغناطیس در سطح نیروهای مسلح به‌منظور بهره‌وری بیشتر از فضای مجازی.

۱۹.استفاده از ترفندهای فریب معکوس.

۲۰.کسب آمادگی لازم برای مقابله با حملات ترکیبی یا سه‌شاخه.

۲۱.تسلط و توجه به تهدیدات جدید سایبری.

۲۲.هوشمندی مقابله با تهدیدات در جهت تقویت وضعیت امنیت نیروهای مسلح.

۲۳.اتخاذ تمهیدات لازم در خصوص مقابله با باج افزارها و بدافزارها به‌منظور جلوگیری از آسیب‌پذیری نیروهای مسلح.

---

[1]. deception technology

فهرست منابع:

الف– منابع فارسی

- بختیاری، ایرج (۱۳۹۳)، تبیین نقش جنگ سایبری در جنگ‌های آینده، فصلنامه علوم و فنون نظامی، سال ۱۰، شماره ۲۸، ص ۴۷-۷۴.
- جلالی، غلامرضا (۱۳۹۰)، پدافند غیرعامل و تهدیدات نوین: انتشارات بوستان حمید، ص ۲۳-۵۱.
- یادگاری، وحید و سیلیانی، ناصر و متین‌فر، احمدرضا (۱۳۹۶)، نقش امنیت فاوا در جنگ سایبری علیه سازمان‌های امنیتی با رویکرد پدافند غیرعامل، فصلنامه پژوهش‌های حفاظتی- امنیتی دانشگاه جامع امام حسین (علیه‌السلام)، سال ۶، شماره ۲۱، ص ۱-۲۴.
- رستمی، فرزاد (۱۳۹۵)، تحول در ماهیت جنگ‌های آینده جمهوری اسلامی ایران؛ سناریوها، فرصت‌ها و چالش‌ها، مجله سیاست دفاعی، سال ۲۴، شماره ۹۷، ص ۱۲-۴۶.
- اسماعیل‌زاده، محمدرضا و رجب‌پور، مجید (۱۳۹۱)، بررسی نقش جنگ سایبری در عملیات مشترک و مرکب، فصلنامه علوم و فنون نظامی، سال ۸، شماره ۲۲، ص ۱-۲۰.
- سامی، اشکان (۱۳۹۳)، تهدیدات سایبری و راهکارهای دفاعی: انتشارات دانشگاه شیراز، ص ۲-۱۳.
- خلیلی‌پوررکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی. فصلنامه مطالعات راهبردی، سال ۱۵، شماره ۵۶ ص ۲-۲۶.
- جالینوسی، احمد و ابراهیمی، شهروز و قنواتی، طیبه (۱۳۹۱)، جایگاه فضای سایبر و تهدیدهای سایبری در استراتژی امنیت ملی ایالات‌متحده آمریکا، فصلنامه دانش سیاسی و بین‌الملل، سال ۲، شماره ۵ ص ۱-۱۵.
- اسمعیل‌زاده ملاباشی، پرستو و عبداللهی، محسن و زمانی، سیدقاسم (۱۳۹۶)، حملات سایبری و اصول حقوق بین‌الملل بشردوستانه، فصلنامهٔ مطالعات حقوق عمومی، دوره ۴۷، شماره ۲، ص ۲-۱۵.
- حسن‌بیگی، ابراهیم (۱۳۹۲)، توسعه شبکه ملی دیتا، چالش‌های فراروی و تهدیدهای متوجه امنیت ملی، فصلنامه مطالعات مدیریت، شماره ۴۸، ص ۲-۱۹.
- حسن‌بیگی، ابراهیم (۱۳۸۸)، حقوق و امنیت در فضای سایبر، انتشارات دانشگاه عالی دفاع ملی، تهران، ص ۴-۲۷۰.
- محمدی، محمود (۱۳۸۶)، نقش فن‌آوری اطلاعات در جنگ‌های آینده، فصلنامه مطالعات بسیج، سال ۱۰، شماره ۳۴، ص ۱-۹.
- عبدالهی، حسن و حق‌نگهدار، افسانه (۱۳۹۴)، نقش الکترومغناطیس سایبری در کنترل میدان جنگ با ایجاد زیرساخت‌های نظامی سایبری، فصلنامه علوم و فنون نظامی، سال ۱۱، شماره ۳۱، ص ۱-۲۳.

- ماه‌پیشانیان، مهسا (۱۳۹۰)، فضای سایبر و شیوه‌های نوین درگیری ایالات‌متحده آمریکا با جمهوری اسلامی ایران، فصلنامه پژوهش فرهنگی، سال ۱۲، شماره ۱۳، ص ۱-۲۸.
- صدری، محمدرضا و کروبی، محمدتقی (۱۳۸۸)، ابعاد حقوقی محیط سایبر در پرتو توسعه ملی، تهران، انتشارات بقعه، ص ۱.

ب– منابع انگلیسی

- Small Business Innovation Research Program (SBIR). Institute of Education Sciences. Retrieved 2018-02-15.
- Coonfield III, J. D. (2013). Cyber Electromagnetic Activities within the Mission Command Warfighting Function: Why is it Important and What is the Capability? (No. ATZL-SWV-GDP). ARMY COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH KS.
- CACI International Inc. and U.S Naval Institute (July 2010); "Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain.
- Lord, Kristin M. & Sharp, Travis (2011); "America's Cyber future Security and Prosperity in the Information Age", Center for a New American Security, Volume I.
- Starr, Stuart H. (2009); "Towards an Evolving Theory of Cyber power", National Defense University, Center for Technology and National Security Policy.
- Charney, Scott (2009); "Rethinking the Cyber Threat A Framework and Path Forward", Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA.
- Haller, John & Merrell, Samuel A. & Butkovic, Matthew J. & Willke, Bradford J. (2010); Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Software Engineering Institute.
- Shachtman, N. (2011, July 15). "Pentagon makes love, not cyber war".Retrieved from CNN.
- Lynn, W. J. (2011, February 15). "Remarks on Cyber at the RSA,Conference". Retrieved from U.S. Department of Defense.