جنگ نرم و امنیت در فضای سایبرنتیک

نویسندگان: مجید نجات‌پور[۱]، مصطفی محمدی[۲]
امید اصغری[۳]، حیدر شهریاری[۴]

تاریخ دریافت: ۹۰/۷/۲۳ تاریخ پذیرش نهایی: ۹۰/۱۰/۱۹

فصلنامه مطالعات راهبردی بسیج، سال پانزدهم، شماره ۵۴، بهار ۱۳۹۱

چکیده

یکی از تحوّلات دوران معاصر در عرصهٔ نظام بین‌الملل، انقلاب اطلاعات و فنّاوری ارتباطات است. تحت تأثیر این فنّاوری‌ها، جنگ، تغییر و تحوّلات گسترده‌ای به خود دیده که از آن جمله می‌توان به جنگ نرم و تحوّل مفاهیمی چون امنیت در فضای سایبرنتیک اشاره کرد. به واقع؛ امروزه فنّاوری‌های اطلاعاتی و ارتباطاتی موجب تغییر ماهیت جنگها و ایجاد فضاهای جدیدی برای فعالیت انسانی شده‌اند. همچنین تحت تأثیر انقلاب ارتباطاتی، اشکال جدیدی از جنگ مانند جنگ مجازی(سایبری) به وجود آمده و شکل سنّتی جنگ مانند جنگ روانی، متأثّر از این انقلاب تغییر کرده است.

مقالهٔ حاضر علاوه بر بررسی ابعاد مفهومی فضای سایبرنتیک، به تأثیرات این انقلاب در حوزه‌های مختلف نظامی و ظهور اشکال جدیدی از جنگ پرداخته است. نتیجه اینکه، ماهیت جنگ در دوران معاصر با استفاده از فنّاوری‌های اطلاعاتی و ارتباطاتی تحوّل یافته است و شاهد وقوع جنگهای متفاوت در عرصهٔ نظام بین‌الملل هستیم که از آنها تحت عنوان جنگهای ناهمگون، اطلاعاتی، نرم، مجازی و غیره نام برده می‌شود. تبیین اشکال جنگهای متأثّر از پیشرفتهای ارتباطی از جمله جنگ مجازی، از جمله اهدافی است که این پژوهش درصدد پاسخ دادن به آنهاست. در این راستا، فرضیهٔ مقاله این است که: فنّاوری اطلاعات و ارتباطات به شکل‌گیری جنگهای نوینی تحت عنوان جنگ مجازی منجر شده است.

واژگان کلیدی:

ارتباطات، فنّاوری ارتباطات، سایبرنتیک، خشونت، جنگ نرم، جنگ مجازی.

---

۱. دانشجو دکتری دانشگاه علامه طباطبایی(ره).
۲. کارشناس ارشد علوم سیاسی دانشگاه اصفهان.
۳. دانشجو دکتری علوم سیاسی دانشگاه تربیت مدرس.
۴. دانشجو دکتری علوم سیاسی دانشگاه علامه طباطبایی(ره).

مقدمه

در عصر حاضر که به اعتقاد بسیاری از اندیشمندان و محققان، عصر انقلاب اطلاعات و فنّاوری ارتباطات است، فنّاوری اطلاعات و ارتباطات در همهٔ زوایای زندگی انسان نفوذ کرده و زندگی او را تغییر داده است. ماهیت جنگ، همپای تحوّلات بنیادی در ماهیت سایر پدیده‌های اجتماعی و فرهنگی، علمی و فنّاورانه، اقتصادی و سیاسی، توأمان در حال دگرگونی است. این پدیده، جوامع بشری را با مفاهیم و مؤلّفه‌های جدیدی مانند جنگ‌افزارهای اطلاعاتی و الکترونیکی، راهزنان رایانه‌ای، فضای سایبرنتیکی و غیره آشنا کرده است. به گفتهٔ بسیاری از صاحب‌نظران، عصر ارتباطات و فنّاوری‌های مربوط به آن، موجب ظهور آسیبها و تهدیدهای جدید در حفاظت از اخبار و اطلاعات حساس امنیتی(سیاسی، اقتصادی، نظامی) شده است. هرفرید مونکلر، یکی از محققان حوزهٔ جنگهای نوین، استدلال می‌کند که جنگ در این عصر، با دوران گذشته فرق کرده و بازیگران غیر دولتی از جمله: تروریستها، جنگ‌سالاران، کودکان و ...، با استفاده از امکاناتی که انقلاب اطلاعات و فنّاوری ارتباطات در اختیار آنها قرار داده است، وارد عرصهٔ جنگ شده‌اند.

در عصر انقلاب اطلاعات و ارتباطات و در جنگهای آینده، بر خلاف عصر صنعتی، حصول پیروزی علاوه بر جنبهٔ نظامی و صنعتی، شامل پیروزی سیاسی نیز خواهد بود؛ یعنی ممکن است دشمن از نظر نظامی شکست بخورد، اما از نظر سیاسی با بهره‌برداری از تسهیلات عصر اطلاعات و ارتباطات، به حیات و مبارزه ادامه دهد. در این جنگها، ابتکار عمل، اطلاعات، ارتباطات راه دور و آموزش، اهمیت بسیار دارد.

در عصر اطلاعات و ارتباطات، جنگ به طور بی‌سابقه‌ای از طریق رسانه‌های جمعی(رایانه، اینترنت، ماهواره و ...) انجام می‌گیرد و از سویی؛ فضای جنگ، وسعت، ارتفاع و ابعاد آن گسترش یافته است. جنگهای پیشین در چهار بُعد زمین، دریا، هوا و فضا انجام می‌گرفت، اما اکنون بُعد پنجم؛ یعنی الکترونیکی نیز به آن افزوده شده است. زمان جنگ، کوتاه‌تر و توسّل به آن، ناگهانی و غیر قابل پیش‌بینی شده و شمار جنگ‌افزارها افزایش یافته است.(ناجی‌راد، ۱۳۸۴، ص ۲۰۹-۲۰۸)

جنگهایی که تحت تأثیر انقلاب اطلاعات و فنّاوری ارتباطات رخ می‌دهند، با جنگهای سنّتی و کلاسیک که بین دولتها رخ می‌داد، تفاوت دارند. در جنگهای نوین، خبری از خصوصیات جنگهای سنّتی مانند نبرد سرنوشت‌ساز و رویارویی نظامی و غیره نیست؛ بلکه در آنها، پراکنده کردن قوا، ناهمگون‌سازی و دولت‌زدایی از جنگ مطرح است. بنابر این، جنگهای نوین به وسیلهٔ ابزارهای نوین ارتباطاتی مانند رسانه‌های جمعی، اینترنت، ماهواره و غیره در فضای مجازی رخ می‌دهند. با توجه به تغییر و تحوّل گسترده‌ای که امروزه در عرصهٔ فنّاوری رخ می‌دهد، عرصه و فضای جنگها نیز دگرگون شده است؛ به گونه‌ای که امروزه از آن با عنوان «فضای مجازی» یاد می‌کنند.

واژهٔ «سایبر» از لغت یونانی «گیبرنیتس» به معنی سکاندار یا راهنما مشتق شده است. گروهی معتقدند مفهوم فضای مجازی با اختراع تلفن توسط الکساندر گراهام‌بل در سال ۱۸۷۶ ایجاد شده است؛ چرا که پیش از آن، فعالیتهای بشری محدود به روابط و تماسهای فیزیکی بود و هیچ‌گاه بشر تصوّر نمی‌کرد روزی بتواند فراتر از دنیای فیزیکی محدود خود، با دیگر افراد ارتباط برقرار کند.(جلالی، ۱۳۸۳، ص ۲۰)

نخستین بار، اصطلاح «سایبرنتیک» را ریاضیدانی به نام نوربرت وینر در کتابی با عنوان سایبرنتیک و کنترل ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برد. سایبرنتیک، علم

مطالعه و کنترل سازوکارها در سیستم‌های انسانی، ماشینی و رایانه‌ای است(وینر، ۱۳۷۲، ص ۲-۱). سالها بعد ویلیام گیبسون، نویسندهٔ داستانهای علمی- تخیّلی، عبارت «فضای مجازی» را در کتاب «نورومانسر» در سال ۱۹۸۴ به کار برد.(صارمی‌راد، ۱۳۷۹، ص ۴۴)

فضای مجازی، فضایی است که تحت تأثیر انقلاب اطلاعات و فنّاوری ارتباطات که وجه مشخصهٔ آن فرامکانی و فرازمانی است، به وجود آمده و جنگی که در این فضا اتفاق می‌افتد، جنگی است متأثّر از انقلاب اطلاعات و فنّاوری ارتباطات، که به «جنگ مجازی» معروف است. این جنگ یکی از اشکال جنگهای نوین و دارای ویژگی‌های خاص خود است که در این مقاله به بررسی آن خواهیم پرداخت. برای تفهیم جنگ مجازی، ابتدا باید فضای مجازی و عناصر آن را درک کنیم. بنابراین، ابتدا فضای مجازی، ویژگی‌ها و تهدیدهای آن بررسی و در ادامه، به بررسی جنگ مجازی و ویژگی‌های آن می‌پردازیم.

اهمیت و ضرورت پژوهش

تا قبل از تشکیل نیروی هوایی، راهبرد زمینی در جنگ غلبه داشت. وقتی نیروی هوایی وارد عرصهٔ جنگ شد، بحث شناسایی، حمایت از نیروی زرهی و تهدید مناطق اقتصادی در دستور کار راهبردشناسان نظامی قرار گرفت. اما در دوران معاصر با توجه به انقلاب الکترونیکی، شاهد انجام عملیاتی هستیم که در آنها چشم و گوشهای غیر زمینی وارد صحنهٔ جنگ می‌شوند؛ یعنی نظامیان در اتاق جنگ و بیرون از میدان جنگ در آمریکا می‌نشینند و از طریق ماهواره‌ها، به صورت مستقیم، حتی نبرد نفر به نفر را در بحران کوزوو از نزدیک می‌بینند و جنگ را هدایت می‌کنند.

اگر بپذیریم که اطلاعات نظامی در طرّاحی راهبردهای نظامی و به طور کلی در روند جنگ، نقش مهمی دارد؛ بنابر این، ما در عصری زندگی می‌کنیم که به دلیل سرعت ارتباطات، که یکی از مشخصه‌های عصر جهانی شدن (انفجار اطلاعات و سرعت ارتباطات) است، سرنوشت و نوع جنگها و حتی سلاحها دچار دگرگونی‌های اساسی شده است. به طور مثال، شاهد نوعی جنگ، به عنوان جنگ الکترونیکی هستیم که بدون استفاده از رادارهای پیشرفته، سیستم‌های هدایت کنندهٔ موشکی بسیار دقیق، سلاحهای پیشرفتهٔ لیزری و بدون داشتن اطلاعات دقیق، پیروزی در آن امکان‌پذیر نیست.

به همین دلیل، امروزه همهٔ ارتشهای دنیا سرمایه‌گذاری‌های عظیمی را در حوزهٔ ارتباطات انجام می‌دهند؛ چرا که بدون آگاهی از تأثیر و نقش فنّاوری ارتباطاتی در جنگ، امکان موفقیت برای هیچ کشوری وجود ندارد و راه پیروزی، آشنایی با انواع جنگها (جنگ مجازی، الکترونیکی و ...) است.

بنابر این، مطالعه و بررسی فنّاوری ارتباطات و تأثیر آن بر جنگ و امور نظامی و نیز شناخت از ابزارها و فنّاوری‌های نوین جنگی و مجهّز شدن به آنها، برای هر کشوری که خواهان حفظ قدرت و بقا در نظام بین‌الملل است، ضروری به نظر می‌رسد.

روش تحقیق

روش تحقیق در این پژوهش، توصیفی- تحلیلی است. در روش توصیفی، تلاش شده تا آثار و پیامدهای انقلاب اطلاعات و فنّاوری ارتباطات بر جنگ و همچنین اشکال جدید جنگهای متأثّر از این انقلاب؛ یعنی جنگ نرم، مطالعه و با گردآوری اطلاعات و داده‌ها، نقش محوری

ارتباطات را در جنگهای نوین، در پی تحوّلات جدید بین‌المللی تحلیل شود. پژوهش حاضر با هدف توصیف، تحلیل و تبیین مراحل مختلف جنگ نرم و امنیت در فضای سایبرنتیک دنبال می‌شود. جمع‌آوری داده‌ها از طریق مطالعات کتابخانه‌ای و اسنادی است که تحلیل این فرایند به صورت نظری انجام خواهد شد. همچنین واحد تحلیل در این تحقیق، جنگ نرم در عرصهٔ نظامی و عملیات جنگی است.

چارچوب نظری پژوهش

برای بررسی و توضیح تفاوت جنگهای گذشته با جنگهای متأثّر از انقلاب اطلاعات، از نظریهٔ جنگهای نوین دانشمند آلمانی، هرفرید مونکلر بهره می‌بریم. بر اساس این نظریه، جنگهایی که امروزه در جهان رخ می‌دهد، از لحاظ مکانی و زمانی متفاوت است. در گذشته، جنگ در زمان و مکانی خاص صورت می‌گرفت، اما امروزه جنگ در همهٔ زمانها و مکانها با استفاده از فنّاوری ارتباطاتی رخ می‌دهد(مونکلر، ۱۳۸۴، ص ۲۰-۱۰). در مقایسهٔ جنگهای گذشته با جنگهای متأثّر از انقلاب ارتباطات، شاید بتوان خصوصیات جنگهای گذشته یا برخی از جنگهایی را که امروزه به سبک سنّتی انجام می‌شوند، چنین بیان کرد:

- جنگ محدود به زمان و مکان معیّنی است؛ یعنی می‌توان به طور مشخصهٔ گسترهٔ جغرافیایی معیّنی را برای درگیری‌ها بیان کرد. در ضمن، جنگ در زمانی خاص آغاز می‌شود و پایان می‌یابد.
- گر چه وقوع جنگ برای کسب قدرت بیشتر یا حفظ قدرت موجود است، اما در گذشته قدرت را در گسترهٔ سرزمینی، نیروی انسانی و تجهیزات می‌دانستند که همه کمّی، قابل مشاهده و در محدودهٔ زمانی و مکانی جنگ، قابل دسترسی بود.
- در گذشته طرفهای درگیر جنگ در مقابل هم صف‌آرایی می‌کردند و هدف به طور عمده حذف فیزیکی نفرات و ادوات طرف مقابل بود.

اما در عصر ارتباطات که حصارهای زمان و مکان برداشته شده، پدیدهٔ جنگ هم به امری فرا زمانی و فرا مکانی تبدیل شده است. امروزه دیگر نمی‌توان جنگ را منحصراً در گسترهٔ جغرافیایی ویژه و زمان معیّنی تعریف کرد. اگر در گذشته این محدودیتها، طرفهای جنگ را برای به دست آوردن منافع مورد نظر دچار تردیدها و مشکلاتی می‌کرد، امروز دیگر می‌توان از جنگی مستمر، گسترده و در تمام لحظات و ساعتها سخن گفت.

در آزمون فرضیهٔ مقاله باید گفت که تأثیرات کامل انقلاب فنّاوری ارتباطات و اطلاعات بر ثبات جهانی و جنگ هنوز به طور کامل شناخته نشده، ولی آشکار است که عصر ارتباطات و اطلاعات تهدیدها، آسیب‌پذیری‌ها و جنگ را تغییر داده است(عبدالله‌خانی، ۱۳۸۶، ص ۲۶). انقلاب در فنّاوری ارتباطات و اطلاعات، موجب شده است که دیگر جنگها به فضای واقعی محدود نشوند و فضای دیگری به نام فضای مجازی (سایبر)به وجود آید که جنگ تحت تأثیر آن قرار گیرد و شاهد اشکال جدیدی از جنگ، مانند جنگ مجازی باشیم. جنگ در فضای مجازی بر خلاف جنگ در فضای واقعی است؛ زمان و مکان در آن وجود ندارد و هر زمان و مکانی می‌تواند عرصهٔ جنگ باشد. بنابر این، ماهیت جنگها دچار تغییر و تحوّل شده است و جنگهای متأثّر از انقلاب ارتباطات و اطلاعات بر خلاف جنگهای گذشته، از قاعده و قانون خاصی پیروی نمی‌کنند و تفاوت بین جبهه و پشت از بین رفته است.

از این رو، در بررسی نحوهٔ جنگهای آینده، آماده‌سازی و ایجاد تحوّل لازم در امور مختلف

نظامی به منظور بهره‌برداری از پتانسیل‌های بالقوّهٔ آن، در دستور کار بسیاری از کشورهای جهان قرار گرفته است.

۱. فضای مجازی و ویژگی‌های آن

فضای مجازی، محیط الکترونیک واقعی است که در آن، ارتباطات انسانی به شیوه‌ای سریع و فراتر از مرزهای جغرافیایی و با ابزار خاص، زنده و مستقیم روی می‌دهد(سلیمانی فارسانی، ۱۳۸۸، ص۴۱). بر خلاف فضای واقعی، در فضای مجازی نیاز به جابه‌جایی‌های فیزیکی نیست و همهٔ اعمال فقط از طریق فشردن کلیدها یا حرکات موشواره صورت می‌گیرد. فضای مجازی، به مجموعه‌ای از ارتباطات درونی انسانها از طریق رایانه و مسائل مخابراتی، بدون در نظر گرفتن جغرافیایی فیزیکی، گفته می‌شود. ماهیت فضای مجازی، ماهیتی فرافیزیکی و غیر ملموس است و به طور کلی، متفاوت با ماهیت فضای سنّتی است. با توسعهٔ فضای مجازی، مفاهیم و اصطلاحاتی در ادبیات الکترونیکی جهان رایج شد که اساس خود را از فعالیتها و توسعهٔ بشری در فضای فیزیکی به امانت گرفتند؛ از جمله: دولت الکترونیکی، تجارت الکترونیکی، جنگ مجازی و ... .(دی‌آنجلیز، ۱۳۸۳، ص ۶۰).

منظور از فضای مجازی، ترکیبی از دهها هزار رایانهٔ به هم پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سوییچ‌ها و کابلهای فیبر نوری است که امکان ایجاد ارتباطات را در یک سیستم جامع فراهم می‌آورند(افتخاری، ۱۳۸۲، ص۵؛ موحدی‌صفت، ۱۳۸۶، ص۲۴۶). فضای مجازی، شبکه‌های رایانه‌ای و مخابراتی متّصل به هم است که اطلاعات را در کمترین زمان و بیشترین مکان مبادله می‌کند. در نتیجه، بارزترین ویژگی فضای مجازی، امکان دسترسی سریع به تمامی اطلاعات «برخط» با کمترین هزینه است(جلالی فراهانی، ۱۳۸۵، ص ۸۶). از دیگر ویژگی‌های آن می‌توان به جهانی و فرامرزی بودن، دستیابی آسان به آخرین اطلاعات، جذّابیت و تنوّع و آزادی اطلاعات و ارتباطات اشاره کرد(سلیمانی فارسانی، ۱۳۸۸، ص ۴۱). بنابر این، امروزه ما فضای مجازی را به معنای مکانی غیر فیزیکی می‌شناسیم که واقعیتها را با عنوان واقعیت مجازی در فضای الکترونیکی بازتاب می‌دهد(مسعودی، ۱۳۸۳، ص ۱۶). اکنون کشورهای پیشرفتهٔ دنیا تقریباً همهٔ امور خود را از طریق این شبکه‌ها که بسان ستون فقرات و نخاع عصبی تجارت، علم، فرهنگ، سیاست و امنیت آنها درآمده، انجام می‌دهند.

با توجه به آسیب‌پذیری و قابل نفوذ و هک شدن شبکه‌های رایانه‌ای و نیز اتّکای کامل کشورهای پیشرفته به این شبکه‌ها، اختلال یا اخلال در سامانهٔ آنها، می‌تواند ضربات جبران ناپذیری به آنها وارد کند و حتی سقوط دولتها را در پی داشته باشد. فضای مجازی دارای ویژگی‌های خاص خود است؛ از جمله ویژگی‌های اساسی فضای مجازی که باعث ایجاد محیطی مناسب برای سربازان جنگهای مجازی (رایاسرباز) می‌شود، می‌توان به موارد ذیل اشاره کرد:

الف) جهانی و فرامرزی بودن: از ویژگی‌های منحصر به فردی که فضای مجازی را ممتاز می‌کند، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن، به آسانی، به جدیدترین اطلاعات دست یابد. مرزهای جغرافیایی تا کنون نتوانسته‌اند از گسترش روزافزون فضای مجازی جلوگیری کنند. از این رو، هر نوع ایجاد محدودیت و مرزبندی در برابر آن بسیار دشوار است.

ب) دستیابی آسان به آخرین اطلاعات: چنانچه بخواهید به آخرین مقاله، کتاب یا

خبری که در زمینه‌ای تخصصی در گوشه‌ای از دنیا منتشر شده، دست یابید، ساده‌ترین و سریع‌ترین راه، استفاده از فضای مجازی است(طارمی، ۱۳۸۷).

ج) جذّابیت و تنوّع: رسانه‌ها از فیلم، عکس، متن یا هر هنر دیگری برای جذّاب کردن خویش استفاده می‌کنند و این ابزارها در فضای مجازی قابل دستیابی است؛ به ویژه آنگاه که هیچ نظارت و فیلتری توان محدود کردن آن را نداشته باشد. از ویژگی‌های منحصر به فردی که در تنوّع و جذّابیتهای فضای مجازی تأثیر بسزایی دارد، مشتری‌محوری محض است. در متون نوشتاری ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به راحتی می‌تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظرسنجی و ارزیابی در این فضا بسیار آسان‌تر و روزآمدتر است و این توانایی را به داده‌پردازان، فروشندگان و عرضه‌کنندگان محصولات اینترنتی می‌دهد که از آخرین خواسته‌های مشتریان و مخاطبان خود مطلع شوند.

د) آزادی اطلاعات و ارتباطات: معنای واقعی آزادی اطلاعات، در فضای مجازی محقق شده است. از این رو، شما هر نوع اطلاعاتی که بخواهید ـ اعم از فرهنگی، سیاسی و اقتصادی ـ بدون محدودیتهای حاکم بر دیگر رسانه‌ها، در فضای مجازی قابل دسترسی است. آزادی ارتباطی نیز از ویژگی‌های فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نیست.(فضای سایبر چیست؟ ۱۳۸۸)

ه) گمنامی: شناسایی و ردیابی یک رایاسرباز در فضای مجازی و پیدا کردن مکان فیزیکی وی با توجه به فنون خاص پنهان‌سازی در این فضا، بسیار مشکل است.

و) تجهیزات ارزان و در دسترس: سهولت دسترسی به ابزارهای حمله و جاسوسی و هزینهٔ آنها نسب به جنگ‌افزارهای حملات دیگر، سازمانهای تروریستی را قادر ساخته تا با استفاده از تجهیزات پیچیده، پیشرفته، بروز و از طریق ارتباطات پنهان، به زیرساختهای هدف، حمله و به مقاصد خود دست یابند.

ز) در دسترس بودن هدف: اهداف اینترنتی و ارتباطاتی به طور روز افزون در حال گسترش است؛ به طوری که یک رایاسرباز قادر است ۲۴ ساعته در حال ارتباط با هدف باشد.

از دیگر مؤلّفه‌های این فضا می‌توان به توجه رسانه‌ای، تأثیرگذاری بر میزان نیرو، تأثیرات فیزیکی، هوشمندی و سادگی استفاده نیز اشاره کرد.(شرکت ایزایران، ۱۳۸۸)

۲. تهدیدهای فضای مجازی

نشت اطلاعات، سرقت داده‌های حیاتی کشور و آسیب‌پذیری شبکه‌های جامع اطلاع‌رسانی، از مهم‌ترین اشکالات امنیتی در فضای مجازی‌اند که اگر از طرف حکومتها توجه ویژه‌ای به آنها نشود، به عنوان تهدیدی جدّی برای منافع پایه‌ای کشورها تلقّی می‌شوند. وجود شبکهٔ جهانی اینترنت که امکان دسترسی‌های مختلف را برای همهٔ افراد در سرتاسر جهان میسّر کرده، واقعیتی انکارناپذیر است که به عنوان مهم‌ترین بستر فضای مجازی و مهم‌ترین عامل در امنیت ملی و زیرساختهای کشورهای توسعه‌یافته، تهدیدهای مجازی درون آن شکل گرفته و فعال می‌شوند.

به طور کلی تهدیدهای فضای مجازی که می‌توانند باعث صدمه در زیرساختارهای کشور شوند، در چهار حوزهٔ ذیل قرار دارند:

الف) کاربران خانگی: در زمان اتصال به شبکه می‌توانند با ورود به سامانه‌های موجود،

تهدیدهایی را ایجاد کنند. معمولاً با توجه به آنکه اثر خاصی از آنها در شبکه ثبت نمی‌شود، شناسایی آنها دشوار است.

ب) مؤسسات بزرگ: مانند شرکتها و دانشگاهها که به بخشهایی از زیرساختها دسترسی دارند. لذا از طریق آنها توانایی کافی در کارکنان و دانشجویان برای نفوذ به شبکه‌ها فراهم است.

ج) بخشهای مهم دولتی و مؤسسات ملی: بنا به اقتضا باید برخی از اطلاعات را به صورت اشتراکی در اختیار کاربران قرار دهند و لذا خطر نفوذ از این ناحیه وجود دارد.

د) کاربران شبکهٔ اینترنت: کاربران شبکهٔ اینترنت با نفوذ در سرویس‌دهندگان موجود در زیرساختارها می‌توانند تهدیدی برای آنها به شمار آیند.(موحدی‌صفت، ۱۳۸۶، ص ۲۵۳ـ۲۵۱)

۳. فضای مجازی و جنگ

ظهور عصر مجازی، مفاهیم و مبانی متعددی از زندگی دوران صنعتی را دستخوش تغییر و تحوّل قرار داده است که از جمله آنها می‌توان به بحث جنگ اشاره کرد. انقلاب اطلاعات به گونه‌ای مفهوم نبرد را تغییر داده که بیش از این دیگر شاهد نبرد فرسایشی خونین نیروهای نظامی نخواهیم بود(علیزاده، ۱۳۸۸، ص ۴۵). در عوض، نیروهای کوچک و چالاکی که به اطلاعات لحظه‌ای ماهواره‌ها و حسگرهای صحنهٔ نبرد مسلّح شده‌اند، با سرعت اعجاب‌آوری به محلهای غیرمنتظره حمله می‌برند. فاتح و پیروز این جنگ، کسی است که می‌تواند از اطلاعات برای از بین بردن «ابهام فضای جنگ» (که دشمن را فراگرفته است) استفاده کند (نوری آزاد، ۱۳۸۸).

در طول تاریخ؛ رهنامه، سازمان و راهبرد نظامی در اثر پیشرفتهای پیوستهٔ فنّاوری، دستخوش تغییرات بنیادین شده‌اند. صنعتی شدن به جنگ فرسایشی بین ارتشهای انبوه در جنگ جهانی اول منتهی شد. انقلاب اطلاعات باعث ظهور نوعی از جنگ می‌شود که نه تعداد زیاد نیرو و نه تحرّکشان، به نتایج مورد نظر منجر نخواهد شد؛ در عوض، کسی که اطلاعات بیشتری دارد، ابهام فضای جنگ را (که دشمن را در بر گرفته است) از بین برده، از مزایای قطعی آن بهره‌مند خواهد شد.

تحوّلات شگرفی در جمع‌آوری، ذخیره‌سازی، پردازش، انتقال و ارائهٔ اطلاعات و همین طور سازمانهایی که از افزایش اطلاعات منتفع می‌شوند، در حال وقوع است. اطلاعات در حال تبدیل شدن به یک منبع راهبردی‌اند و می‌توانند خود را به عنوان عنصری بانفوذ و ارزشمند در عصر فراصنعتی، همانند نقش سرمایه و کار در عصر صنعتی، مطرح کنند. انقلاب اطلاعات در حال به چالش کشیدن طرّاحی بسیاری از سازمانهاست. این انقلاب، سلسله‌مراتب سازمانهایی را که به صورت متعارف طرّاحی شده‌اند، 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 می‌کند. انقلاب اطلاعات می‌تواند باعث تغییر جهت در چگونگی کشمکش بین جوامع و نیز چگونگی برپایی جنگ به وسیلهٔ نیروها شود.(پاک‌نظر، ۱۳۸۰، ص ۶۹-۶۸).

۴. جنگ مجازی و تعاریف آن

جنگ مجازی مقولهٔ گسترده‌ای است که تروریسم اطلاعاتی، حمله‌های معنایی و جنگ شبیه‌سازی شده را در بر می‌گیرد. جنگ مجازی به مقدار بسیار کم قابل کنترل است و از آنجا

که خیلی تخیّلی به نظر می‌رسد، فقط به مقدار اندک با جنگ اطلاعاتی به عنوان یک کل، متفاوت است(آلبرتس و پاپ، ۱۳۸۵، ص ۱۱۹). آنچه ما به عنوان جنگ مجازی می‌شناسیم، در واقع هدایت عملیات نظامی بر اساس قوانین حاکم بر اطلاعات است. هدف از این نوع جنگ، تخریب سیستم‌های اطلاعاتی و ارتباطاتی است. تلاش این جنگ در جهت شناسایی اموری است که دشمن به شدّت از آن محافظت می‌کند. این جنگ حرکتی در جهت تغییردهی «توازن اطلاعات و دانش» به نفع یک طرف است؛ به خصوص اگر توازن نیروها برقرار نباشد. در واقع؛ به کمک دانش، سرمایه و نیروی کار کمتری هزینه خواهد شد. این جنگ از فنّاوری‌های گوناگون بهره می‌برد؛ از موارد برجستهٔ این نوع فنّاوری‌ها می‌توان به فرماندهی و کنترل برای رسیدن به هوشمندی، توزیع و پردازش برای رسیدن به ارتباطات روشی، تثبیت موقعیت و شناخت هویت دوست و دشمن در زمینهٔ مبادلات سیستم‌های جنگی هوشمند اشاره کرد.(قاسمی، ۱۳۸۸، ص ۳۲)

جنگ مجازی و همچنین سایبرنتیک به صورت استفاده از رایانه و اینترنت برای جنگیدن در فضای مجازی تعریف می‌شود(عبدالله‌خانی، ۱۳۸۶، ص ۱۳۶). به عبارت دیگر؛ جنگ مجازی را می‌توان هر گونه عمل جنگی دانست که در آن از سیستم‌های اطلاعاتی یا فنّاوری دیجیتالی، چه به عنوان ابزار حمله و چه به عنوان آماج حمله استفاده می‌شود. این حملات باید منجر به اعمال خشونت بر ضد اشخاص یا دارایی‌ها، به میزانی که ایجاد رعب و وحشت کند، انجام شود.(قربان‌نیا، ۱۳۸۳، ص ۲۰)

استارک، جنگ مجازی را چنین تعریف می‌کند: جنگ مجازی عبارت است از استفادهٔ هدفمند یا تهدید به استفاده از جنگ رایانه‌ای یا توسّل به خشونت بر ضد اهداف رایانه‌ای با انگیزه‌های سیاسی، اجتماعی، اقتصادی یا مذهبی از سوی گروههای غیر دولتی یا گروههای تحت هدایت و حمایت دولت به منظور ایجاد ترس و نگرانی و وحشت در جمعیت مورد نظر و آسیب رساندن به دارایی‌ها و اموال نظامی و غیر نظامی(Stark, 1999, P.9). این جنگ با هدف از هم گسیختن سیستم‌های اطلاعاتی و مخابراتی، سیستم‌های کنترل و فرماندهی، ارتباطات، خبرگیری و جاسوسی نیروهای نظامی دشمن و غیر عملیاتی کردن آنها در صحنهٔ نبرد یا در حالت عادی صورت می‌گیرد. این به معنای تلاش برای داشتن آگاهی بیشتر در مورد دشمن و در عین حال تخریب آگاهی او نسبت به خود است. اگر موازنهٔ نیروها بین طرفهای درگیر برقرار نباشد، تلاش می‌شود تا موازنهٔ «اطلاعات و دانش» را به نفع خود تغییر دهند. این شکل از جنگ، در بر گیرندهٔ فنّاوری‌های گوناگون به ویژه برای هوشمند ساختن سیستم‌های تسلیحاتی، کور کردن مدارهای الکترونیکی، قفل کردن سیستم‌ها را دچار اضافه‌بار اطلاعاتی کردن و در نهایت نفوذ به داخل مدارها و خطوط اطلاعاتی و ارتباطاتی است(ناجی‌راد، ۱۳۸۴، ص ۲۲۳). هدف اصلی از انجام جنگ مجازی، ایجاد اختلال در ارتباطات بین خطوط دشمن است.

۵. تاریخچهٔ جنگ مجازی

در گذشته‌های دور و به طور عملی در تمام فرهنگهای کهن، پدیدهٔ جنگ را نه تنها یک مسئلهٔ راهبردی سیاسی و نظامی، بلکه مسئله‌ای معنوی و اخلاقی تلقّی می‌کردند. اما با پیدایش تغییرات در نظام جهانی، نظریه‌های جنگ طی سه قرن گذشته از مراحل چندی گذر کرده است. به طور طبیعی، جنگ‌افزارهای نظامی و اطلاعاتی نیز پابه‌پای نظریه‌های جنگ دگرگون شده‌اند که در ادامه، به تحوّل تاریخی آن می‌پردازیم.

فنّاوری‌های اطلاعاتی و ارتباطاتی، حتی در اشکال اولیه‌شان، تأثیر بسزایی در امنیت ملی و امور دفاعی داشته است. نمونه‌های فراوانی در تاریخ وجود دارد که این نظر را ثابت می‌کنند. اگر چه نخستین نمونه‌های تاریخی، چیزی جز علایم آتش نبودند که نیروهای فاتح یونانی از آنها استفاده می‌کردند؛ چنان که هزار سال پیش از میلاد، آشیل گزارش کرد پیامها، فاصلهٔ ۵۰۰ کیلومتری را یک شب طی می‌کردند. کما بیش در همان زمان، سلیمان پادشاه به وسیلهٔ کبوترهای پیام‌رسان، بدون اینکه ملکهٔ سبا با خبر شود، با نیروهای نظامی‌اش ارتباط بر قرار می‌کرد.

۵۰۰ سال بعد، همزمان با «نبرد ماراتون»، هرودوت، چاپارهای نیروهای نظامی ایران را ستود؛ زیرا آنها به طور مرتب بین داریوش و ارتش او که در حال جنگ با یونان بود، رفت و آمد می‌کردند و اخبار جنگ را به اطلاع کوروش می‌رساندند؛ هیچ چیز نمی‌توانست این پیکها را از انجام وظیفه‌شان در کوتاه‌ترین زمان ممکن بازدارد؛ برف، باران، گرما و تاریکی هیچ کدام نمی‌توانستند مانع فعالیت آنها شوند. بنابر این، اهمیت اطلاعات و ارتباطات برای امور نظامی در زمان یونانی‌ها و ایرانی‌ها امری بدیهی بود.

طی دو هزار سال بعد، فنّاوری‌های اطلاعاتی و ارتباطی به آهستگی پیشرفت کرد و زمان، فاصله و مکان همچنان به عنوان موانعی قابل توجه برای افزایش توانمندی نظامی باقی ماندند. با وجود این، اهمیت فنّاوری‌های اطلاعاتی و ارتباطاتی در جنگ، دفاع و امنیت ملی، به عنوان یک امر بدیهی به قوّت خود باقی ماند. به عنوان مثال، در سال ۱۵۸۸ فنّاوری اطلاعاتی و ارتباطاتی در پیروزی نیروی دریایی انگلستان بر ناوگان اسپانیا تأثیری حیاتی داشت؛ به گونه‌ای که ۱۳۰ کشتی نیروی دریایی اسپانیا در آبهای دریایی مانش شکست خوردند. آنها با علائم آتش و ستونهایی از دود، سواحل انگلستان را مشخص کرده و این به معنی پیشروی ناوگان اسپانیا از پلیموت به لندن بود؛ فاصله‌ای ۳۲۰ کیلومتری که طی کردن آن ۲۰ دقیقه طول می‌کشید. کشتی‌های انگلستان که در دریا به حال آماده‌باش بودند، طی دستوری کوتاه، ناوگان اسپانیا را از پا درآورده و سلطهٔ دریایی و رهبری اروپا را در نبود نیروی دریایی اسپانیا به دست آوردند. فیلیپ تیلور تاریخدان می‌نویسد: «تبلیغات در زمان یونانیان باستان به بلوغ رسید اما بار دیگر پس از آنکه انقلاب صنعتی، رسانه‌های گروهی را گسترش بخشید، به اوج رسید».(تافلر و تافلر، ۱۳۷۴، ص ۲۲۴)

در سالهای آخر قرن ۱۶ و اوایل قرن ۱۹، فنّاوری‌های اطلاعاتی و ارتباطاتی به پیشرفت آرام خویش ادامه دادند و دیگر فنّاوری‌ها نیز پیشرفت چشمگیری کردند؛ به گونه‌ای که گاهی اهمیت توسعهٔ فنّاوری اطلاعاتی و ارتباطاتی بیش از پیش مطرح می‌شد. فنّاوری‌های ارتباطات، مدتها قبل‌تر از فنّاوری‌های ذخیره و پردازش اطلاعات وجود داشته‌اند.(دارنلی و فدر، ۱۳۸۴، ص ۳۳)

نیروی دریایی سلطنتی انگلستان دوباره نمونهٔ درخشان دیگری از پیشرفت در فنّاوری‌های اطلاعاتی و ارتباطاتی را به نمایش گذاشت و نشان داد که چگونه پیشرفت در یک نوع فنّاوری، در بیشتر موارد آثار دیگر فنّاوری‌ها را افزایش می‌دهد و چگونه این فنّاوری‌ها هماهنگ با هم، بر امور امنیت ملی در سطوح راهبردی، روشی و عملیاتی اثر می‌گذارند.

در اواسط قرن نوزدهم، فنّاوری‌های مهمی در نخستین انقلاب اطلاعاتی اختراع شد؛ از جمله: اختراع تلگراف، تلفن و رادیو که بر توانمندی‌های نظامی و محیط راهبردی تأثیر گذاشت. برای مثال در جریان جنگ داخلی آمریکا، ارتش از تلگراف برای هدایت سربازان، تأمین پشتیبانی، افزایش کارامدی و سازماندهی نظامی و تقویت اطلاعات مربوط به تحرّکات و عملکرد دشمن استفاده کرد. در جریان جنگ جهانی دوم و پس از آن، فنّاوری‌های

دومین انقلاب اطلاعاتی جدید؛ تلویزیون، رایانه‌های نسل اول و ماهواره‌ها، دست‌کم به اندازه فنّاوری‌های نخستین انقلاب اطلاعاتی و فنّاوری ارتباطاتی در جنگ، دفاع و امنیت ملی تأثیری مهم گذاشت.

برخی از تحلیلگران استدلال می‌کنند که در اواخر دهۀ ۱۹۸۰ و اوایل دهۀ ۱۹۹۰ فنّاوری‌های جدید و نوظهور اطلاعاتی و ارتباطاتی عصر اطلاعات، در فروپاشی اتحاد جماهیر شوروی، پایان یافتن جنگ سرد و نابودی نظام بین‌المللی دو قطبی تأثیر مهمی داشته‌اند. کاربرد گستردۀ سلاحهای هدایت‌شونده و دقیق، «سیستم‌های موقعیت‌یاب جهانی»، یکی شدن سیستم‌های حسگر داده‌ها و ارتباطات، تجسّس سریع و ارتباطات عملیات پیشرفتۀ مشترک در جنگ خلیج فارس در سال ۱۹۹۱ بیشتر به عنوان وجه تمایز بین جنگهای قدیمی و جنگهای عصر اطلاعات به حساب می‌آید.(آلبرتس و پاپ، ۱۳۸۵، ص ۳۲-۲۵)

به نظر می‌رسد پایان جنگ سرد که با شکوفایی انقلاب ارتباطات و گسترش فنّاوری ارتباطات مصادف شد، تصوّرات، تفکّرات و نظریات نظامی پیشین را به چالش طلبید. در نتیجه، محققان و مراکز مطالعات راهبردی، به ویژه سازمانهای دفاعی – نظامی، به نظریه‌پردازی در زمینۀ چالشهای آینده رو آوردند(کرگ، ۱۳۷۸، ص ۲۰). از جمله چالشهای اساسی که امروزه گریبانگیر کشورها و نظامهای سیاسی شده، جنگ مجازی است که عملاً فضای امنیتی آنها را مورد تهدید قرار می‌دهد. جنگ در فضای مجازی، نتیجۀ تحوّل در تاریخ جنگهاست.

نخستین جنگ با استفاده از فضای مجازی، اواسط دهۀ ۷۰ میلادی، در دوران جنگ سرد، بین دو ابرقدرت آن زمان (ایالات متحدۀ آمریکا و شوروی سابق) اتفاق افتاده؛ اما در اغلب مستندات، مورد «کوزوو» به عنوان اولین جنگ مجازی بیان شده است. توجه به نکات ذیل در بررسی تاریخچۀ جنگهای مجازی حائز اهمیت است: اول اینکه، ریز مستندات این جنگها (نحوۀ عمل، نتایج، آثار و...) با توجه به ارتباط مستقیم با امنیت ملی کشورها، به عنوان اسناد با سطح محرمانگی بالا تلقّی شده، دولتها مانع از فاش شدن آنها می‌شوند. دوم اینکه، ماهیت جنگهای مجازی، از جرایم مجازی مانند هک یا انتشار ویروسها کاملاً متفاوت است؛ یک جنگ مجازی توسط دولت یا گروهی متخاصم به منظور ایجاد اختلال یا صدمه زدن به زیرساختهای هدف، طرح‌ریزی و اجرا می‌شود. آنچه تحت عنوان جرم مجازی شناخته می‌شود، در واقع می‌تواند به عنوان ابزارهای یک جنگ مجازی مورد استفاده قرار گیرد.(سیدمفیدی، ۱۳۸۴، ص ۱۰)

۶. محدودۀ جنگ مجازی

عملاً محدوده‌ای را نمی‌توان برای جنگ مجازی تجسّم کرد؛ زیرا جنگ مجازی، محدودیت مکانی و عملیاتی خاصی ندارد.

الف) محدودۀ عملیاتی جنگ مجازی: محدودۀ عملیاتی جنگ مجازی بسیار گسترده است؛ از تولید پارازیت مخابراتی گرفته تا عملیات روانی، از تغییر صفحات یک تارنما گرفته تا بمباران رایانامه‌ای. اما در نهایت، اصل تهدیدهای منابع اطلاعاتی است؛ به نحوی که امنیت ملی دشمن مورد مخاطره قرار گیرد. بنابر این، بستر عملیات مجازی، همانا زیرساختهای اطلاعاتی است.(همان، ص ۱۴)

ب) محدودۀ جغرافیایی: برای فضای مجازی نمی‌توان محدودۀ جغرافیایی تصوّر کرد؛ بنابر این، جنگ مجازی نیز دارای مرز نیست. ولی باید در نظر داشت که این تجسم به علت مقایسۀ مستقیم فضای مجازی با دنیای واقعی و بر اساس دانسته‌ها و قراردادهای فیزیکی

است. اما در عمل، فضای مجازی نیز دارای مرز است. تصوّر کنید که سیستم رایانه‌ای شما از طریق خطوط شهری به اینترنت متصل است؛ اکنون شما در فضای مجازی هستید، ولی مالکیت اشیای درگیر، بعضاً کاملاً مشخص است. لذا می‌توان مرزها را تعیین کرد. تنها تفاوتی که بین مرز مجازی با مرز حقیقی وجود دارد، همانا عدم محدودیت در ترسیم مرز و مدار بسته بودن آن است.(همان)

۷. اشکال مختلف جنگ مجازی

جنگ مجازی مقوله‌ای گسترده است که تروریسم اطلاعاتی، حمله‌های معنایی، جنگ شبیه‌سازی شده و جنگ گیبسون را در بر می‌گیرد.

الف) تروریسم اطلاعاتی: یکی از پردامنه‌ترین جنگهای کنونی، جنگی است که گروهها و سازمانهای تروریستی با استفاده از جنگ‌افزارهای شبکه‌ای و اطلاعاتی مدرن انجام می‌دهند. بهره‌برداری از شبکه‌های اطلاعاتی آشکار که امروزه به بهترین وسایل ارتباطی مبدّل شده‌اند، هم نیازهای تروریستها را در ایجاد ارتباط برطرف کرده و هم زمینه‌های جمع‌آوری اطلاعاتی را برای آنها فراهم می‌کند. بنا به تعریف، «تروریسم اطلاعاتی، جنگی است که در آن تروریستها توانایی‌های سیستم‌های اطلاعاتی شبکه‌ای را در تحقق اهداف تروریستی به کار می‌گیرند».

تروریسم اطلاعاتی با هدف انجام فعالیتهای تروریستی در حوزهٔ اطلاعات صورت می‌گیرد و دو عامل جنگ‌افزار و محیط جنگ اطلاعاتی، مهم‌ترین معیارهای موفقیت یا عدم موفقیت در آن محسوب می‌شوند. عامل نخست جنگ افزارهای تروریسم اطلاعاتی که در شبکه‌ها امروزه به نرم‌افزارهای خاص این جنگ و شیوه‌های به کارگیری تعامل سیستمی در آن مربوط، می‌شود. نرم‌افزارهای خاص در این حوزه، نقش جنگ‌افزارهایی را بر عهده دارند که سرعت و دقت عمل آنها دقیقاً با شاخصهای یک جنگ‌افزار واقعی در میدان نبرد، برای ایجاد موفقیت در این جنگ اهمیت دارند. عامل دوم، توانایی‌های سیستم‌های اطلاعاتی است که به هر اندازه وسیع‌تر و گسترده‌تر باشند، می‌توانند نیازهای مختلف یک سیستم را برطرف کنند.(ترکاشوند، ۱۳۸۸)

ب) حملهٔ معنایی: تفاوت حملهٔ معنایی با جنگ نفوذگری در این است که جنگ نفوذگر به صورت تصادفی یا نظام‌مند، خرابی‌هایی را در سیستم به وجود می‌آورد که باعث می‌شود سیستم از عملکرد خویش بازماند. سیستمی که مورد حملهٔ معنایی قرار می‌گیرد، از فعالیت خود بازنمی‌ماند و یک سیستم عمل‌کنندهٔ درست به شمار می‌آید، اما پاسخهای متفاوت با واقعیت می‌دهد. پس می‌توان گفت که حملهٔ معنایی یک خرابی در سیستم است. حملهٔ معنایی از خصوصیات معیّن سیستم‌های اطلاعاتی سوء استفاده می‌کند. به طور مثال، سیستم‌ها شاید به درون‌داده‌های حسگری متّکی باشند که تصمیم‌هایی دربارهٔ دنیای واقعی گرفته‌اند(به عنوان مثال، سیستم نیروی هسته‌ای که فعالیتهای لرزه‌ای را نشان می‌دهد). اگر حسگرها فریب بخورند، سیستم‌ها نیز ممکن است فریب داده شوند(مثل خاموشی سیستم‌ها با وجود فقدان زمین‌لرزه). ممکن است حفاظ‌ها فریب بخورند.(آلبرتس و پاپ، ۱۳۸۵، ص ۱۲۰)

ج)جنگ شبیه‌سازی شده: جنگ واقعی، کثیف، ابلهانه و خطرناک است. جنگ شبیه‌سازی شده فاقد این صفات است. اگر دقت شبیه‌سازی به اندازهٔ کافی خوب باشد و هر سال این دقت افزایش یابد، نتایج آن شباهتی منطقی با تضاد خواهد داشت(همان، ص ۱۲۱). در جنگ واقعی همان جریانات و اتفاقاتی رخ می‌دهد که به صورت واقعی وجود دارد؛ اما با زمان

مجازی و فنّاوری تصویری و رایانه‌ای، منظره‌ای بدون خون‌ریزی، انسانی، بهداشتی و پاکیزه و فهرست واقعی تلفات انسانی آن را نمی‌دانند. ایالات متحده پس از جنگ ویتنام شاهد پیشرفتهای فنّاوری بوده است؛ از این رو عموم آمریکایی‌ها به این باور رسیده‌اند که دیگر هیچ دشمنی به نیرومندی آنها نیست؛ آنها همواره پیروز هستند و با کمترین کشته و مجروح در جنگها پیروز می‌شوند. در شبیه‌سازی جنگ به صورت مجازی، مرگ در صحنهٔ نبرد تخفیف داده شده، از معرض دید دور و جنگ واقعی از ذهن بیرون می‌شود. در شبیه‌سازی‌های تدارک دیده شده در اجرای مجازی جنگ، این خطر وجود دارد که افراد بیاموزند که چگونه بکشند و هیچ مسئولیتی در قبال آن به عهده نگیرند؛ مرگ را تجربه کنند اما نتایج غمبار آن را متحمّل نشوند. در این جنگ، تنها با تشابه و اختلافِ جنگ و بازی مواجه نیستیم، بلکه با این امر مواجهیم که آنها در یک فضای مشابه در کنارِ یکدیگر پیش می‌روند.(Derian, 2000, P.3-1)

د) جنگ گیبسون: قهرمانان و ضد قهرمانان در رمانهایی مانند «نورمانسر»، «تضعیف» ویلیام گیبسون و «ریزش برف» نوشتهٔ نیل استفنسون، شخصیتهایی مجازی هستند که در داخل سیستم‌های کلان قرار دارند و در آنجا به صورت مجازی با یکدیگر مبارزه می‌کنند که این مبارزه، شرافتمندانه نیست. این مسئله که این قهرمانان و ضد قهرمانان در آن سیستم‌ها چه کاری انجام داده یا دلیل اینکه چرا هر کسی دوست دارد شبکه‌ای به وجود آورد تا به مبارزه با دنیای اول برخیزد، به صورت واقعی هرگز نشان داده نشده است.(آلبرتس و پاپ، ۱۳۸۵، ص ۱۲۱)

۸. ابزارهای جنگ مجازی

جنگ مجازی دارای ابزارهای خاص خود است که تحت تأثیر انقلاب اطلاعات و فنّاوری ارتباطات به وجود آمده‌اند. ابزارهای جنگ مجازی را تلفیقی از دانش و تجهیزات تشکیل می‌دهند. دانش تخصصی اثر بالاتری دارد، ولی بدون شک ابزار نیز نقش کلیدی دارد. از ابزارهای جنگ مجازی می‌توان به موارد ذیل اشاره کرد:

الف) ابزارهای شناسایی: عموم ابزارهای شناسایی در خود فضای مجازی یا اینترنت وجود دارند که از جملهٔ آنها می‌توان به موتورهای جستجوی دامنه‌ها، ثبات دامنهٔ اینترنتی، ثبات آدرس اینترنتی، روشهای ردیابی، ابزارهای شناسایی DNS ، ابزارهای شناسایی شبکه و همبندی آن و ابزارهای متفرقه اشاره کرد.(جنگ سایبر، ۱۳۸۸، ص ۶۵)

ب) ابزارهای وارسی: با ابزارهای وارسی می‌توان سامانه‌های زنده، فعال و قابل دسترسی از طریق اینترنت را مشخص کرد. انواع جاروب کننده‌ها، انواع وارسی کننده‌های پورتهای TCP و UDP ، به عنوان نمونه‌های کلی ابزارهایِ وارسی در جنگ مجازی‌اند.(همان)

ج) ابزارهای کنکاش: ابزارهای کنکاش عموماً درون سیستم‌های عامل حضور دارند. این ابزارها مبادرت به بیرون کشیدن اطلاعات خاص سیستم‌های عامل و شبکه‌ها، نظیر عناصر کاربردی و تولیدات نرم‌افزاری می‌کنند.(همان)

د) ابزارهای نفوذ: ابزارهای نفوذ به طور کلی به دو دسته تقسیم می‌شوند: اول اینکه، صرفاً مجازی هستند و دوم اینکه، ابزارهای فیزیکی/مجازی، مانند امواج کوتاه و بلندِ دستکاری شده، موسوم به بمب الکترونیکی را شامل می‌شوند.

ه) ابزارهای ارتقای مزایا: از ابزارهای ارتقای مزایا می‌توان روشها و ابزارهای تزریق، روشهای فریبکارانه و استراق سمع را نام برد.(جنگ سایبر، ۱۳۸۸، ص ۶۵)

و) ابزارهای پنهان: از ابزارهای پنهان می‌توان موارد ذیل را نام برد:

-انواع اسبهای تروا: برنامه‌هایی هستند که در فضای مجازی برنامه‌ها پنهان می‌شوند و برنامهٔ خود را به اجرا در می‌آورند. اسب تروا می‌تواند خود را استتار کند و حتی در برنامهٔ ایمنی شبکهٔ SATAN قرار گیرد.(Colarik, 2008, P.12)

- انواع ویروسهای رایانه‌ای و کرمها: ویروسها برنامه‌هایی‌اند که قادر به تکثیر خود به برنامه‌های بزرگ‌تر هستند. برنامه‌های ویروسی زمانی فعال می‌شوند که برنامهٔ میزبان شروع به فعالیت کند و به دنبال آن، ویروس خود را تکثیر می‌کند(Haeni, 1997, P.12). کرمها برنامه‌ای مستقل هستند که خودشان را تکثیر می‌کنند و از یک رایانه به رایانهٔ دیگر و اغلب بر روی شبکه‌ها می‌روند و بر خلاف ویروسها، برنامه‌های دیگر را تغییر نمی‌دهند.(حسینی، ۱۳۷۹، ص ۱۰)

- نقاط پنهان در سیستم عامل: این ابزار شامل سازوکارهایی است که طرّاح نرم‌افزار آن را در زمان ساخت نرم‌افزار تعبیه می‌کند تا زمانی که سیستم‌های حفاظت رایانه به طور طبیعی فعالیت می‌کنند، به طرّاح امکان دهد به طور مخفیانه وارد سیستم شود.(صدوقی، ۱۳۸۲، ص ۱۳۱)

- جنگ‌افزارهای حملات*DOS*: در استفاده از این نوع روشها جنبهٔ در دسترس بودن هدف، مورد تهدید قرار می‌گیرد. این حملات به عنوان ابزاری برای دیگر سناریوهای جنگی نیز مورد استفاده قرار می‌گیرند.(جنگ سایبر، ۱۳۸۸، ص ۶۵)

۹ .انواع نفوذگران در جنگ مجازی

در جنگ مجازی انواع نفوذگران، حمله‌ها و اهداف آنها عبارتند از:

- **گروه نفوذگران کلاه سفید**: هر کسی با دانش خود بتواند از سد موانع امنیتی یک شبکه بگذرد و به داخل شبکه راه پیدا کند اما اقدام خرابکارانه‌ای انجام ندهد را یک هکر کلاه سفید می‌خوانند. هکرهای کلاه سفید متخصصین شبکه‌ای هستند که سوراخ‌های امنیتی شبکه را پیدا می‌کنند و به مسئولان گزارش می‌دهند.

- **گروه نفوذگران کلاه سیاه**: به این گروه کراکر هم می‌گویند. این افراد آدمهایی هستند که با دانش خود، وارد رایانهٔ قربانی خود شده، به دستکاری اطلاعات، جاسوسی، پخش کردن ویروس و غیره می‌پردازند.(جنگ سایبر، ۱۳۸۸)

- **گروه نفوذگران کلاه خاکستری**: شاید سخت‌ترین کار، توصیف حوزهٔ این گروه از نفوذگرهاست. گاهی به این نفوذگرها، Whacker هم می‌گویند(البته زیاد مصطلح نیست). این گروه از نفوذگرها بنا به تعریفی، حد وسط دو تعریف گذشته‌اند.(پور روستایی، ۱۳۸۹)

- **گروه نفوذگران کلاه صورتی**: این افراد آدمهای کم‌سوادی هستند که فقط با چند نرم‌افزار به خرابکاری و آزار و اذیت بقیه اقدام می‌کنند.(جنگ و دفاع سایبر، ۱۳۸۴، ص ۴۰)

۱۰. حملات جنگ مجازی

حملات جنگ مجازی، نوعی حمله است که در آن یک مؤلّفهٔ رایانه‌ای وجود دارد که سیستم‌های هدف را غیر قابل استفاده و کارایی آنها را کم کرده، با تزریق اطلاعات غلط، دقت تصمیم‌گیری کاربران را کاهش می‌دهد و حتی منجر به سرقت اطلاعات می‌شود(مرادی، ۱۳۸۷، ص ۵۷). در این جنگ، از فنّاوری رایانه‌ای می‌توان برای تهدید یا حمله کردن به منابع رایانه‌ای قربانی بهره گرفت. این عمل می‌تواند به شکل تهدید یا حمله بر ضد زیرساختهای ملی که به شدّت به شبکه‌های رایانه‌ای وابسته شده‌اند و ارتباط متقابل با این شبکه‌ها دارند، تجلّی یابد. تهدید تأسیسات آب و برق و سیستم حمل و نقل عمومی، تهدید نهادهای تجاری و شرکتهای

فراملی و تهدید نیروهای امنیتی، مشخص‌ترین و بارزترین گونهٔ این تهدیدها به شمار می‌روند. حملات جنگ مجازی چند تفاوت عمده با شکلهای معمول حمله دارند، که عبارتند از:

– حملات جنگ مجازی به وسیلهٔ عوامل نامعلوم صورت می‌گیرد و ردیابی و یافتن محل اختفای آنان بسیار دشوار است. این‌گونه حملات، فاصله و مکان را که در حملات سنّتی در آن استقرار می‌یافتند، محو کرده و از بین می‌برند.

– حملات جنگ مجازی بسیار ارزان‌تر از حملات معمولی است و در عین حال، فاقد آسیب‌پذیری‌ها و هزینه‌هایی‌اند که اغلب متوجه شخص مهاجم می‌شود.

– ساختارهای شبکه‌ای گروههای مهاجم، آنها را در مقابل هر گونه اقدام تلافی‌جویانه ایمن ساخته، باعث افزایش توان خودترمیمی آنها می‌شود.(کاکاوند، ۱۳۸۲، ص ۱۵)

۱۱. انواع حمله در جنگ مجازی

چندین نوع حمله در این شیوه از جنگ وجود دارد که در طیفی از کم‌شدّت تا شدید دسته‌بندی شده‌اند:

– **خرابکاری اینترنتی**: حملاتی برای تغییر محتوا و شکل صفحات وب یا اختلال در سرویس‌دهی که آسیب چندانی وارد نمی‌کند.(جنگ و دفاع سایبر، ۱۳۸۴، ص ۴۱)

– **گردآوری داده‌ها**: دسترسی به اطلاعات طبقه‌بندی شده که امکان جاسوسی از نقاط مختلف جهان را فراهم می‌کند.

– **حملات گستردهٔ اخلال در سرویس‌دهی**: در این نوع حمله، شمار زیادی از رایانه‌ها در یک کشور مبادرت به ایجاد اخلال در سرویس‌دهی به سیستم‌های کشور دیگر می‌کنند.

– **اخلال در تجهیزات**: فعالیتهای نظامی که در آنها از رایانه و ماهواره برای هماهنگی استفاده می‌شود، در خطر این نوع حمله قرار دارند؛ زیرا مهاجمان می‌توانند فرمانها و ارتباطات را رهگیری کرده یا تغییر دهند.

– **حمله به زیرساختارهای حیاتی**: نیروگاههای برق، تأسیسات آبرسانی و سوخت‌رسانی، ارتباطات و حمل و نقل در برابر این نوع حمله، با آسیب‌پذیری زیاد مواجه هستند.(عبداله‌خانی، ۱۳۸۶، ص ۱۳۶)

– **شنود**: نفوذگران می‌توانند به شکل مخفیانه از اطلاعات نسخه‌برداری کنند.

– **دستکاری و تغییر اطلاعات**: نفوذگر علاوه بر دسترسی و توانایی خواندن اطلاعات، به دستکاری و تغییر اطلاعات نیز می‌پردازد.

– **جعل و افزودن اطلاعات**: نفوذگر اطلاعات را به سرقت نمی‌برد و دستکاری هم نمی‌کند، بلکه اطلاعات دیگری را به اطلاعات موجود اضافه می‌کند.

– **حمله از نوع وقفه**: نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.(پور روستایی، ۱۳۸۹)

۱۲. نقاط افتراق جنگ مجازی با جنگهای گذشته

جنگ فیزیکی و مجازی از برخی جهات کاملاً شبیه به هم هستند؛ به عنوان مثال، هدف اصلی در جنگ ـ از هر نوع ـ وارد آوردن ضرر و زیان به دشمن است و روش اصلی در جنگ، قاعدتاً تصاحب منابع دشمن خواهد بود. نقاط افتراق جنگ مجازی نسبت به مجازی جنگها را می‌توان به صورت ذیل دسته‌بندی کرد:

– **حمله از راه دور**: اولین تفاوت جنگ مجازی با دیگر جنگها و بالاخص جنگ فیزیکی و حقیقی، قابلیت طرّاحی، اجرا و نتیجه‌گیری از راه دور است.

– **دشواری در شناسایی و ردیابی**: به سبب خصایص پروتکل‌های ارتباطی در فضای مجازی، عملاً شناسایی و ردیابی منبع اصلی حمله و مهاجم اصلی، بسیار دشوار و گاهی غیرممکن است.

– **تهدید سه‌جانبهٔ امنیت**: در جنگ مجازی، هر سه جنبهٔ امنیت (امنیت، ایمنی و پایداری) می‌تواند مورد تهدید قرار گیرد.(حملات سایبر، ۸۸۳۱)

– **اندازهٔ هدف**: در جنگهای فیزیکی عموماً به دنبال تخریب مناطق جغرافیایی بزرگ‌تر هستند، ولی در جنگ مجازی باید اهداف مهم و اساسی «از نظر مجازی و نقش آنها» را هدف قرار داد. این اهداف ممکن است از نظر فیزیکی بسیار ناچیز باشند، ولی نقش بزرگی ایفا کنند.

– **انتشار حمله**: حملهٔ مجازی می‌تواند به سادگی از چندین منبع ـ کانال صورت پذیرد؛ در حالی که هدایت و راهبری حمله‌های فیزیکی که از چندین محل آغاز می‌شوند، بسیار دشوار است.

– **هزینه**: بدون شک هزینه جنگ فیزیکی از جنگ مجازی بیشتر است و این خصوصیت بارز فضای مجازی است که عوامل و عناصر آن سهل‌الوصل‌تر و ارزان‌تر هستند.

– **مسئولیت‌پذیری**: از آنجایی که قوانین مدوّن و مشخص بین‌المللی برای مبارزه و ایجاد دعاوی مجازی وجود ندارد، کشورها به سادگی از زیر بار مسئولیت حملات مجازی خود شانه خالی می‌کنند.

– **ابزارها و سلاحهای جنگ مجازی**: سلاح جنگ مجازی را تلفیقی از دانش و تجهیزات تشکیل می‌دهد. دانش تخصصی، بالاترین اثر را دارد؛ ولی بدون شک، ابزار نیز نقش کلیدی خواهد داشت.(سیدمفیدی، ۱۳۸۴، ص ۱۷)

۱۳. تحوّلات آتی جنگ مجازی

در آینده شاهد تحوّل ماهیت جنگ خواهیم بود. البته برخی افراد به اشتباه معتقدند که این تحوّلات به معنی اتّکای صِرف به جنگ خودکار، ماشینی و دور ایستا است؛ در حالی که انقلاب اطلاعات بر تعامل انسان و ماشین در یک فضای جدید و ارتقای توانمندی انسانها دلالت دارد و نه جدایی و خودمختاری ماشینها؛ به گونه‌ای که سلاحهای هوشمند ما به جای ما، با یکدیگر بجنگند. در واقع؛ شاید در بعضی موارد، جنگ با سرعت بالا و از راه دور رخ دهد؛ اما در موارد دیگر، جنگ با سرعت پایین و بسیار نزدیک به دشمن انجام خواهد شد. بنابر این، روش متعارف جنگ نوین، ترکیب جدیدی از سرعت بالا و پایین و درگیری دور و نزدیک خواهد بود و نه یکی از این دو حالت.

میادین جنگ پست‌مدرن به خاطر انقلاب اطلاعات و فنّاوری ارتباطات در سطوح راهبردی و روشی، دگرگون می‌شوند. افزایش روزافزون دامنه و عمق منطقهٔ عملیات از یک سو و افزایش فوق‌العادهٔ دقت تخریب حتی توسط سلاحهای متعارف از سوی دیگر، نشانگر اهمیت چشمگیر فنّاوری‌های مرتبط بوده و بیانگر آن است که اگر چه طرّاحی و اجرای «تمام‌عیار» یک جنگ مجازی، مستلزم دسترسی به فنّاوری پیشرفته است، اما جنگ مجازی به خودی خود به فنّاوری پیشرفته وابستگی قطعی ندارد. در واقع؛ برای جنگ مجازی فقط حضور فنّاوری پیشرفته الزامی نیست، بلکه ابعاد روانی و سازمانی آن نیز به اندازهٔ ابعاد فنی آن اهمیت دارند.

اهمیت نسبی جنگ علیه نظام فرماندهی و کنترل و ارتباطات دشمن، همگام با ظهور

جنگ مکانیزه مطرح شد. در جنگ جهانی دوم، رهنامهٔ حملهٔ برق‌آسا، که به نوعی ویژگی‌های جنگ مجازی را در بر داشت، در دو سطح روشی و راهبردی، هدف اصلی خود را به صورت ایجاد اختلال در توانمندی ارتباطات و کنترل دشمن تعریف کرد. برای مثال، ارتش سرخ شوروی از لحاظ تعداد تانک بر ارتش آلمان نازی برتری داشت؛ اما در ارتش شوروی، فقط تانکهای فرماندهی، مجهز به سیستم‌های ارتباطی بودند؛ در حالی که آلمانی‌ها همهٔ تانکهای خود را به سیستم‌های ارتباطی مجهز کرده و به همین خاطر به مزیت نسبی دست یافته بودند.

هنوز یک چارچوب نظری جامع برای ابعاد اطلاعاتی و ارتباطی جنگهای نوین ارائه نشده است؛ با وجود این، نقش چشمگیر و تعیین‌کنندهٔ «دانش» در محیط‌های بحرانی، از جمله محیط‌های جنگی انکارناپذیر است. از این رو، جنگ مجازی را نباید فقط مجموعه‌ای از روشهای عملیاتی جدید به شمار آورد، بلکه باید آن را سبک نوینی از جنگ دانست که تسلّط بر آن، مستلزم ارائهٔ رهیافتها، راهکارها و راهبردهای نو در زمینه طرّاحی و سازماندهی نفرات، رهنامه و سازمان نظامی است. آنچه امروز روشن است اینکه، جنگ مجازی را می‌توان در همهٔ زمینه‌ها تعریف کرد. برای مثال، جنگ مجازی در وضعیت آفندی یا پدافندی در سطوح راهبردی یا روشی؛ علاوه بر این، جنگ مجازی طیف کاملی از عملیات زرهی سنگین تا مأموریتهای کوچک مقابله با شبه‌نظامیان را در بر می‌گیرد.

در جنگ مجازی نه تنها نگرش جدیدی نسبت به مفهوم«تهاجم» مطرح می‌شود، بلکه «شکست و تسلیم شدن دشمن» نیز تغییر می‌کند. در سراسر عصر مدرن، منازعه و جنگ بین دولت ـ ملتها از سبک جنگ فرسایشی تبعیت کرده است؛ به این صورت که برای شکست نهایی دشمن، لازم بود ابتدا نیروهای مسلح او به هلاکت برسند. این طرز جنگ، تا قرنهای متمادی دست‌نخورده باقی ماند تا اینکه در خلال جنگ جهانی اول، آمار زیاد کشته‌شدگان، سیاستمداران و فرماندهان نظامی را بر آن داشت که در جستجوی راه حلی برای خون‌ریزی کمتر برآیند. حملهٔ برق‌آسای آلمان نازی به ارتش فرانسه، نمونهٔ بارزی بود از طرز نوین جنگ که از جنگ فرسایشی با تلفات انسانی بالا پرهیز می‌کرد. هر چند در طرح حملهٔ برق‌آسا که بر قابلیت مانور سریع تکیه داشت، هنوز انهدام نیروهای دشمن، از اجزای دستیابی به اهداف نظامی محسوب می‌شد.

آدمیرال چبروسکی، الگوی جدیدی را برای جنگهای نوین پیشنهاد داده است؛ این الگو بیشتر بر «شبکه‌ای شدن» امور نظامی تمرکز دارد تا بر اطلاعات و سیستم‌های اطلاعاتی. در این الگو که با عنوان «الگوی شبکه‌محور» شناخته می‌شود، جنگ، محصول تعامل همزمان سه حوزه دانسته شده است که عبارتند از: حوزهٔ فیزیکی، حوزهٔ اطلاعاتی و حوزهٔ شناختی.

حوزهٔ فیزیکی جایی است که حمله، حفاظت و مانور در محیط‌های زمینی، دریایی، هوایی و فضایی انجام می‌شود. در این حوزه، امکانات فیزیکی و شبکه‌های ارتباطی که آنها را به یکدیگر پیوند می‌دهند، وجود دارد. سنجش عناصر و مؤلفه‌های این حوزه، آسان بوده و تاکنون به طور سنّتی، قدرت نظامی با توجه به این حوزه تعیین می‌شده است.

حوزهٔ اطلاعاتی جایی است که اطلاعات تولید شده، مدیریت و به اشتراک گذاشته می‌شود. این حوزه، اطلاع‌رسانی به رزمندگان را تسهیل و دستورات نظامی را از طریق نظام فرماندهی، کنترل و منتقل می‌کند.

حوزهٔ شناختی نیز درون ذهن افراد قرار دارد. اینجا جایی است که درک، برداشت، باورها

و ارزشهای نظامیان حضور دارد و پایهٔ تصمیم‌گیری آنها را تشکیل می‌دهد. حوزهٔ شناختی را باید جایگاه امور نامحسوس و ناملموس مانند توان رهبری، روحیهٔ جنگجویی، انسجام یگانها، سطح آموزش و تجربه و آگاهی دانست. تعیین و سنجش ویژگی‌های این حوزه، اگر نگوییم غیر ممکن، بسیار دشوار و شامل زیر مجموعه‌ای تحت عنوان ذهن افراد است که برای هر یک از افراد، منحصر به فرد است.(مرادی، ۱۳۸۷، ص ۱۷)

۱۴. راهکارهای مقابله با جنگ نرم

در این قسمت، با توجه به ظرفیتهای راهبردی کشورها، راهکارهایی در راستای افزایش توانایی‌های اطلاعاتی و نیز راهکارهای برای مقابله با جنگ نرم پیشنهاد شده است:

الف) ارائهٔ شناخت درست از تهدید

ارائهٔ شناخت درست و کامل در رابطه با جنگ نرم و تعیین مرزها، از اصول اساسی و مهم و به عبارتی؛ وضعیت‌سنجی علمی است. به این معنا که ما در کجای این مقابله قرار داریم و میزان آسیب‌پذیری، تهدیدها و فشارها چگونه است. این امر، تلاش نخبگان را می‌طلبد و طرّاحی یک فرم برآورد اطلاعات راهبردی در این زمینه ضروری است.

ب) توسعه‌بخشی عملیات رسانه‌ای

دامنهٔ اطلاع‌یابی از دشمن را باید گسترش دهیم. باید جهانی شدن را به مثابهٔ یک فرایند طبیعی در نظر بگیریم و مهم اینکه، کشورها باید جایگاه خود را در این فرایند، تعریف یا از فضای مجازی به نحو مطلوب استفاده کنند. شاید در کوتاه‌مدت بتوان فضای مجازی را محدود کرد، اما در درازمدت باید تلاش در استفادهٔ حداکثری از این فضا باشد تا مقابله به درستی انجام شود. به عبارت دیگر؛ هر کس بتواند در آینده، ارزشهای خود را در فضای مجازی محدود کند، حرف اول را خواهد زد.

تهدیدهای نرم از ماهیت پیچیده‌ای برخوردارند که ثمرهٔ بازخوانی آرا و اندیشه‌های نخبگان است. بر خلاف تهدیدهای سخت که هنگام اندازه‌گیری به سهولت قابل رؤیتند، تهدیدهای نرم به دلیل غیر محسوس بودن، ماهیت نامشخصی برای اندازه‌گیری دارند. در این میان، نقش رسانه‌ها و وسایل ارتباط جمعی در پشتیبانی و حمایت از روند اجرایی این تهدیدها بسیار حایز اهمیت است. اصلی‌ترین ابزار کشورها در راه‌اندازی عملیات روانی علیه کشور دیگر، استفاده از دستاویزی به نام رسانه است. کشورها بدون تمسّک به رسانه نمی‌توانند دست به عملیات روانی بزنند. رسانه می‌تواند به عنوان اولین عامل رشد فزایندهٔ شایعه، به طرّاحان عملیات روانی در یک کشور کمک کند.

نتیجه‌گیری و پیشنهادها

جنگ مجازی عبارت است از انجام یا آماده شدن برای انجام عملیاتهای نظامی، مطابق با اصول مربوط به اطلاعات. جنگ مجازی؛ یعنی ایجاد اختلال، اگر نگوییم نابودی کامل، در سیستم‌های اطلاعاتی و ارتباطی که دشمن برای «دانستن» خود به آنها تکیه می‌کند. هدف اصلی در جنگ مجازی، بر هم زدن «موازنهٔ اطلاعات و دانش» به نفع نیروهای خودی است؛ به ویژه اگر «موازنهٔ توان رزمی» وجود نداشته باشد. بنابر این، در جنگ مجازی

می‌توان با بهره‌گیری از دانش برتر، ضعف سرمایه و نفرات کمتر را جبران کرد و به پیروزی قاطع دست یافت. جنگ مجازی در فضای مجازی رخ می‌دهد که ظهور فضای مجازی یکی از پیامدهای انقلاب اطلاعات و فنّاوری ارتباطات است. در این جنگ با استفاده از فنّاوری‌های پیشرفتهٔ اطلاعاتی و ارتباطاتی، به زیرساختهای اطلاعاتی حمله می‌شود. به واقع اگر بخواهیم جنگ را بر پایهٔ نظریهٔ جنگهای نوین یا جنگهای نسل چهارم ارزیابی کنیم، باید به این نکته توجه داشته باشیم که این نظریه درصدد بیان چه شکلی از جنگ است و چرا مطرح شده است. این نظریه بیشتر تمرکز خود را بر روی جنگهای نامتقارن قرار داده که طرفهای درگیر در آن یا حداقل یک طرف، شرایط دولت بودن را ندارد و بیشتر جنگها جنبهٔ خصوصی پیدا کرده است. صرف نظر از معدود جنگهای دوران کنونی و جنگهایی که به سبک سنّتی انجام شده‌اند، بقیهٔ جنگها از این نظریه پیروی می‌کنند که علت این تغییر و تحوّل در جنگ، انقلاب در اطلاعات و فنّاوری ارتباطات است.

در طی تاریخ، رهنامه، سازمان و راهبردهای نظامی به خاطر خط شکنی‌های انقلابی در فنّاوری، دستخوش تغییرات عمیق شده‌اند. فنّاوری‌های نوین به صورت یک سلاح جدید، یک منبع انرژی جدید، یا یک وسیلهٔ ارتباطی جدید، همگی موجب شده‌اند که با اصلاح رهنامه، سازمان و راهبرد نظامی، طرف نوآور از جنگ فرسایشی پرهیز کرده، در عوض به طرز نوین جنگ قاطع و سریع دسترسی داشته باشد. البته همان‌طور که اکثر تاریخدانان تأکید می‌کنند، نفوذ فنّاوری‌های نو لزوماً جنگ را متحوّل نمی‌کند، بلکه آنچه اهمیت فوق‌العاده دارد، نگرشها و منطق سازماندهی جنگ است. در واقع؛ اگر بگوییم فنّاوری جدید حتی جهان‌بینی‌ها و الگوهای ذهنی را متحوّل می‌کند، سخنی به گزاف نگفته‌ایم. بر این اساس، رشد خیره‌کنندهٔ فنّاوری اطلاعات و ارتباطات، که گاهی با عنوان «انقلاب اطلاعات و فنّاوری ارتباطات» شناخته می‌شود، موج پرقدرتی است که ماهیت و ویژگی‌های جنگ و منازعه را از بیخ و بن تغییر خواهد داد.

از آغاز دههٔ ۱۹۹۰ طلیعهٔ یک انقلاب نوین در امور نظامی آغاز شده و گفته می‌شود اثرات آن نسبت به سایر انقلابهای نظامی گذشته، بسیار عمیق‌تر است. بررسی‌ها نشان می‌دهند که منشأ این انقلاب، پیشرفتهای حاصل در فنّاوری‌های نوین، به ویژه فنّاوری‌های اطلاعات و ارتباطات و شرایط و الزامات محیطی (اقتصادی، سیاسی و اجتماعی) بوده است. انقلابهای نظامی به طور عمده شرایطی جدید و متفاوت با گذشته خلق می‌کنند و به همراه خود، فرصتها و تهدیدهای نوینی برای کشورها به ارمغان می‌آورند. پیشرفتهای سریع فنّاوری‌های نظامی، توانایی دولتهای ملی را در اتّکا به خویش کاهش داده است. اساساً جنگ در حال حاضر، به فنّاوری الکترونیکی و ارتباطات وابسته است و این چیزی است که در جنگ خلیج فارس ۱۹۹۱ ثابت شد. تخریب و نابودسازی انبوه که از فاصلهٔ دور می‌توان ایجاد و از طریق موشکها و ناوهای هواپیمابر آن را عملی کرد، در چند ساعت ارتش بزرگی را در هم می‌کوبد؛ به خصوص اگر قدرت دفاعی آن ارتش با دستگاههای الکترونیکی کور شده باشد و اهداف حمله نیز به وسیلهٔ ماهواره‌ها شناسایی شده باشند و رایانه‌هایی که هزاران کیلومتر دورتر از صحنهٔ جنگند، هدایت‌کنندهٔ آتش در این جنگ نامریی باشند. البته همیشه جنگ به فنّاوری وابسته بوده است. تفاوت دوران فعلی، سرعت تحوّلات فنّاورانه است که باعث می‌شود تسلیحات در مدت کوتاهی، کهنه و عقب‌افتاده شوند. این امر همه را وادار به ارتقای مستمر دستگاههای تسلیحاتی می‌کند.

در حوزهٔ نظامی و عملیات جنگی، فنّاوری اطلاعات و ارتباطات تقریباً همه چیز را متحوّل می‌کند؛ از آموزش نیروهای انسانی تا پشتیبانی و حتی روابط عمومی، ساخت و تولید حسگرها و سیستم‌های اطلاعاتی پیشرفته را در بر می‌گیرد. بنابر این، در جنگهای نوین دیگر نمی‌توان ادّعا کرد که پیروزی به این بستگی دارد که کدام یک از طرفین بیشترین مقدار سرمایه، نفرات و فنّاوری را به میدان نبرد می‌برد، بلکه مهم این است که کدام یک از طرفین، بهترین اطلاعات مرتبط با میدان نبرد را در اختیار دارد.

در گذشته، رکن اساسی پیروزی در جنگ، حذف فیزیکی دشمن بود؛ اما اکنون پابه‌پای پیشرفت در ساخت فنّاوری‌های جنگی، از بین بردن روحیه، به تنش کشاندن و ایجاد اضطراب روانی دشمن از یک سو و تأثیر بر ذهن دشمن، تحریف حقیقت و تخریب فرهنگی از سوی دیگر، نقش اصلی و اساسی را در جنگها ایفا می‌کند.

انقلاب در اطلاعات و فنّاوری ارتباطات، منجر به ظهور اشکال جدیدی از جنگ یا تغییر در اشکال قدیمی جنگ شده است و ما امروزه اصطلاحاتی مانند جنگ نرم، جنگ اطلاعاتی، جنگ روانی، جنگ مجازی، جنگ رایانه‌ای و غیره را به طور مکرر از رسانه‌ها و وسایل ارتباط جمعی می‌شنویم که با استفاده از فنّاوری ارتباطات رخ می‌دهند. در این مقاله، تمرکز بر روی جنگ مجازی بود. جنگ مجازی یکی اشکال جدید جنگ در عصر حاضر است که با استفاده از اشکال جدید فنّاوری ارتباطاتی مانند رایانه و اینترنت در فضای مجازی واقع می‌شود. این جنگ نه دارای زمان خاصی است و نه می‌توان مکانی را به طور مشخص عرصهٔ آن دانست، بلکه در هر لحظه و هر مکانی با استفاده از فنّاوری‌های اطلاعاتی و ارتباطاتی رخ می‌دهد. امروزه ارتشها با به کارگیری روشهای جنگ مجازی، از یک برتری اطلاعاتی برخوردار شده‌اند.

از این رو، بررسی نحوهٔ جنگهای آینده، آماده‌سازی و ایجاد تحوّل لازم در امور مختلف نظامی به منظور بهره‌برداری از پتانسیل‌های بالقوهٔ آن، در دستور کار بسیاری از کشورهای جهان قرار گرفته است.

منابع

۱. آلبرتس، دیوید اس. و دانیل اس. پاپ(۱۳۸۵)؛ **گزیده‌ای از عصر اطلاعات: الزامات امنیت ملی در عصر اطلاعات**، ترجمه علی علی‌آبادی و رضا نخجوانی، تهران، پژوهشکده مطالعات راهبردی.

۲. افتخاری، اصغر(۱۳۸۲)؛ **استراتژی ملی برای تأمین امنیت در فضای مجازی**، تهران، پژوهشکده مطالعات راهبردی.

۳. پاک‌نظر، ثریا(۱۳۸۰)؛ **«مروری بر اشکال جدید جنگ در هزارهٔ سوم: جنگهای مجازی و اینترنتی»**، نشریه وب، ش ۱۸(آذرماه).

۴. پور روستایی، محمدعلی(۱۳۸۹)؛ **«جنگ با سلاح فنّاوری اطلاعات»**، خبرنامه الکترونیکی فنّاوری اطلاعات، ش ۱.

۵. تافلر، آلوین و هیدی تافلر(۱۳۷۴)؛ **جنگ و پادجنگ**، ترجمه مهدی بشارت، تهران، اطلاعات.

۶. ترکاشوند، جلال(۱۳۸۸)؛ **«تأثیر فنّاوری اطلاعات بر گسترش تروریسم»**:
http//:bashgah.net/pages.26103-html

۷. جلالی، امیرحسین(۱۳۸۳)؛ **«جرایم سایبر»**، نشریه رسالت، چهاردهم اردیبهشت.

۸. جلالی فراهانی، امیرحسین(۱۳۸۵)؛ **«تروریسم سایبری»**، فقه و حقوق، ش ۱۰.

۹. **«جنگ سایبر»**(۱۳۸۸)؛ سایت دانشگاه آزاد اسلامی قزوین:
http//:www.qiau.ir/thread.2523-html

۱۰. **«جنگ سایبر»**(۱۳۸۸)؛ نشریهٔ علمی، خبری، تحلیلی و آموزشی پردازشگر، ش ۵۵.

۱۱. **جنگ و دفاع سایبر؛ گزارش گام دوم معرفی امور نظامی و دفاعی سایبر**(۱۳۸۴)؛ تهران، اندیشگاه شریف و اندیشکدهٔ کاوشگران آینده، وزارت دفاع و پشتیبانی نیروهای مسلح، موسسه آموزشی و تحقیقاتی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فنّاوری دفاعی.

۱۲. حسینی، سیدجمال(۱۳۷۹)؛ **«جنگ‌افزارهای اطلاعاتی»**، ماهنامه نگاه، سال اول، ش ۳ (خرداد).

۱۳. دارنلی، جیمز و جان فدر(۱۳۸۴)؛ **جهان شبکه‌ای درآمدی بر نظریه و عمل در باب جامعهٔ اطلاعاتی**، ترجمه نسرین امین‌دهقان و مهدی محامی، تهران، چاپار.

۱۴. دی آنجلیز، جینا(۱۳۸۳)؛ **جرایم سایبر**، ترجمه سعید حافظی و عبدالصمد خرم‌آبادی، تهران، شورای عالی توسعهٔ قضایی.

۱۵. سلیمانی فارسانی، امین(۱۳۸۸)؛ **«انقلاب اسلامی و جنگ نرم»**، پیام انقلاب، ش ۳۱.

۱۶. سیدمفیدی، کاوه(۱۳۸۴)؛ **«جنگ سایبری»**، قابل دسترسی در:
http//:www118.ba118.com/EbookB1.htm

۱۷. شرکت ایزایران، مرکز پدافند غیر عامل(۱۳۸۸)؛ **«حملات سایبر»**:
http//:www.ccw.ir/content/100/default.aspx

۱۸. صارمی‌راد، تورج(۱۳۷۹)؛ **«سایبرهای کامپیوتری»**، نشریه ریزپردازنده، ش ۸۲ .

۱۹. صدوقی، مرادعلی(۱۳۸۲)؛ **تکنولوژی اطلاعات و حاکمیت ملی**، تهران، وزارت امور خارجه.

۲۰. طارمی، محمدحسین(۱۳۸۷)؛ **«فضای سایبر: آسیبها و مخاطرات»**:
http//:www.rasekhoon.net/Article/Show.41605-aspx

۲۱. عبدالله‌خانی، علی(۱۳۸۶)؛ **جنگ نرم ۳: نبرد در عصر اطلاعات**، تهران، ابرار معاصر تهران.
۲۲. علیزاده، حمیدرضا(۱۳۸۸)؛ «**نبرد سایبر**»، امید انقلاب، ش ۴۰۰-۳۹۹ (اردیبهشت و خرداد).
۲۳. فضای سایبر چیست؟(۱۳۸۸)؛ قابل دسترسی در:
http//:basiji.co.cc/forum/index.php?topic;954.0=wap2
۲۴. قاسمی، فائزه(۱۳۸۸)؛ **بررسی نظریه‌های فمینیستی جنگ**، اصفهان، دانشکده علوم اداری و اقتصاد، دانشگاه اصفهان.
۲۵. قربان‌نیا، ناصر(۱۳۸۳)؛ «**مواجهه با تروریسم: رویکرد نظامی، سیاسی و حقوقی**»، فصلنامه نامه مفید، ش ۴۳.
۲۶. کاکاوند، عباس(۱۳۸۲)؛ «**حملات سایبری چالش جدید آمریکا**»، نشریه رسالت، چهارم شهریور.
۲۷. کرگ، میلز(۱۳۷۸)؛ «**چالشهای امنیتی در آغاز قرن ۲۱**»، ترجمه حیدرعلی بلوچی، فصلنامه امنیت ملی، ش ۱.
۲۸. مرادی، مختار(۱۳۸۷)؛ «**مدیریت میدان نبرد: مقدمه‌ای بر محیط‌شناسی نظامی و جنگهای اطلاعاتی**»، نشریه علوم اجتماعی، ش ۱۰ (دی‌ماه).
۲۹. موحدی صفت، محمدرضا(۱۳۸۶)؛ «**امنیت ملی در فضای سایبر: فرصتها و تهدیدها با تأکید بر استقرار دولت الکترونیک**»، فصلنامه مطالعات دفاعی استراتژیک، سال هشتم، ش ۳۰ (تابستان و پاییز).
۳۰. ناجی‌راد، محمدعلی(۱۳۸۴)؛ **جهانی شدن تروریسم**، تهران، دفتر مطالعات سیاسی و بین‌المللی.
۳۱. نوری آزاد، سعید(۱۳۸۸)؛ «**جنگ جهانی سایبر: فضای مجازی عرصهٔ نبرد جدید**»:
http//:www.magiran.com/npview.asp?ID1902597=
۳۲. وینر، نوربرت(۱۳۷۲)؛ **استفادهٔ انسانی از انسانها: سایبرنتیک و جامعه**، ترجمهٔ مهرداد ارجمند، تهران، انتشارات آموزش و پرورش انقلاب اسلامی.
33. Colarik ,M ,Andrew .(2008) **Introduction to Cyber Warfare and Cyber Terrorism ,USA ,**Lech Janczewski ,University of Auckland.
34. Derian ,Der**"** .(2000) **Virtuos War ;Virtual Theory ,"***International Organizations* ,Summer.
35. Haeni ,E .Reto .(1997) **Information Warfare an Introduction**, Washington DC ,George Washington University ,Cyberspace Policy Institute.
36. Stark ,Rods .(1999) **Cyber Terrorism ,Rethinking New Technology**, Department of Defense and Strategic Studies.