دوفصلنامه بازی جنگ، سال چهارم، شماره ۹، پاییز و زمستان ۱۴۰۰

تاریخ دریافت: ۱۴۰۰/۰۴/۲۸ تاریخ پذیرش: ۱۴۰۰/۰۶/۱۲

از صفحه ۶۷ تا صفحه ۸۳

الگوی شبکه فرماندهی و کنترل قدرت نرم در نیروهای مسلح

احد نقوی *[۱]

ناصر مختارزاده [۲]

نوع مقاله: مروری

چکیده

گستردگی حوزه دفاعی کشور که تمامی فضای کشور و فراتر از آن شامل: امنیت هوایی، دفاع از فضا در تمامی ابعاد، کشف اهداف، شناسایی، ردگیری دشمن تا تعیین تکلیف آن، رهگیری با تمامی ابزار به ویژه سامانه هواپایه و درگیری و انهدام موجب می‌گردد تا مجموعه تجهیزات کشف، جمع‌آوری، مقابله اعم از عامل و غیرعامل و عملیات سایبری و جنگ الکترونیک و... زمین پایه، دریا پایه و هواپایه در یک ساختار اساسی تجمیع گردند و با این ساختار کلیه تلاش‌ها، هدفمند به‌سوی اهداف هدایت گردند که اصولاً اهداف از جنس و تنوع متفاوتی بوده و علاوه بر سرعت و شتاب و داشتن آزادی عمل در فضا، زمین و دریا ترفندها و فریب‌کاری خاص خود را در فضای مجازی، شبکه‌های اجتماعی و عملیات روانی نیز دارا می‌باشند.

جامع، کامل، متحد و واحد بودن شبکه در ساختاری منسجم از جمله خصوصیات این شبکه است به گونه‌ای که تمام اجزاء این شبکه قادر باشند زبان یکدیگر را درک نموده و مجموعه تدابیر در مقابله با تهدید را به خوبی اجرا نمایند. مشخصه بارز آن تجمیع اطلاعات و اخبار، پردازش و هماهنگی آن، تطبیق و تلفیق اطلاعات و همچنین انتشار این اخبار و اطلاعات به تمامی مراکز فرماندهی و کنترل قدرت نرم مورد نیاز برحسب میزان دسترسی مجاز عناصر به اطلاعات مذکور می‌باشد.

واژه‌های کلیدی:

قدرت نرم، فرماندهی کنترل، تلفیق و تطبیق اطلاعات، عملیات روانی.

---

[۱] پژوهشگر ارشد، معاونت فاوا ارتش جمهوری اسلامی ایران، تهران، ایران.

[۲] پژوهشگر ارشد، معاونت فاوا ارتش جمهوری اسلامی ایران، تهران، ایران.

* نویسنده مسئول: Email: ahdmod92@gmail.com

مقدمه

گستردگی حوزه دفاعی کشور که تمامی فضای کشور و فراتر از آن شامل: امنیت هوایی، دفاع از فضا در تمامی ابعاد، کشف اهداف، شناسایی، ردگیری دشمن تا تعیین تکلیف آن، رهگیری با تمامی ابزار بویژه سامانه هواپایه و درگیری و انهدام موجب می‌گردد تا مجموعه تجهیزات کشف، جمع‌آوری، مقابله اعم از عامل و غیرعامل و عملیات سایبری و جنگ الکترونیک و... زمین پایه، دریا پایه و هواپایه در یک ساختار اساسی تجمیع گردند و با این ساختار کلیه تلاشها، هدفمند به‌سوی اهداف هدایت گردند که اصولاً اهداف از جنس و تنوع متفاوتی بوده و علاوه بر سرعت و شتاب و داشتن آزادی عمل در فضا، زمین و دریا ترفندها و فریبکاری خاص خود را در فضای مجازی، شبکه‌های اجتماعی و عملیات روانی نیز دارا می‌باشند [۱].

بیان مسئله

یکی از مهمترین عرصه‌های نوظهور در امور نظامی که با ورود بشر به عصر اطلاعات، متولد گردیده است، جنگ سایبر و جنگ اطلاعاتی است که اساساً رویکردها، ابزارها، استراتژی‌ها، تاکتیک‌ها و نتایج خاص خود را دارد. جنگ اطلاعاتی یک اصطلاح نسبتا جدید است که طی سال‌های گذشته به واژه‌نامه اصطلاحات نظامی وارد شده است. البته مفهوم استفاده از اطلاعات در جنگ قدمت طولانی دارد. ظهور اصطلاح جنگ اطلاعاتی و اهمیت روزافزون آن احتمالاً با انقلاب اطلاعات ارتباط مستقیم دارد. فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها درسیستم‌های انسانی، ماشینی (و کامپیوتر ها) است. سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر بوجود آمده است که به تعدادی از آنها اشاره می کنیم: فضای سایبر، شهروند سایبر، پول سایبر، فرهنگ سایبر، راهنمایی فضای سایبر، تجارت سایبر، کانال سایبر و .... واژه "فضای سایبر" را نخستین بار ویلیام گیبسون نویسنده داستان علمی تخیلی در کتاب نورومنسر در سال۱۹۸۴ به کار برده است. فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون درنظر گرفتن جغرافیای فیزیکی گفته می شود. یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرارکنند. بر خلاف فضای واقعی، در فضای

سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد[۲,۳].

در حال حاضر کلیه ساختار فرماندهی و کنترل قدرت نرم نیروهای مسلح با رویکردهای جزیره‌ای با موضوعات اشاره شده و نحوه مدیریت فضای مجازی، عملیات روانی و مدیریت شبکه‌های اجتماعی را با بهره گیری از توان تخصصی کارکنان و با جمع‌آوری و یکپارچه‌سازی سنتی و بعضا استفاده از سیستم‌های جزیره‌ای انجام می‌گیرد [۷,۹].

فرماندهی و کنترل قدرت نرم با استفاده از ظرفیت و پتانسیل کلیه سازمان‌های تخصصی در نیروهای مسلح و همچنین بر قراری تعاملات و تبادلات لازم با سایر سازمان‌های لشکری و کشوری میتواند اقدام به جمع‌آوری تحلیل و ارائه اطلاعات و گزارشات مورد نیاز نموده و فرمانده را جهت اتخاذ تصمیم مناسب در مواجهه با مسائل سایبری، فضای مجازی و عملیات روانی مصمم نماید[۹].

فقدان مراکز فرماندهی و کنترل هوشمند در این مهم منجر به بروز برخی کاستی‌ها شده که در ادامه به تعدادی از این کاستی‌ها اشاره می‌گردد:

کاستی‌ها: روش و تجهیزات موجود در برابر مأموریت جدید نیروهای مسلح در حوزه قدرت نرم ، ازقبیل تنوع تهدیدات فضای سایبری، تنوع اقدامات مرتبط با عملیات روانی، تنوع علوم شناختی، تنوع رسانه‌ها بعلت عدم کفایت سیاست‌گذاری جریان اطلاعات و افزایش سطح نظارتی در حوزه فضای مجازی، شبکه‌های اجتماعی، عملیات روانی و علوم شناختی و همچنین فقدان سامانه فرماندهی و کنترل هوشمند و مکانیزه مرتبط با قدرت نرم با آسیب‌های جدی روبرو میباشد[۷].

ضرورت انجام تحقیق

با توجه به تدابیر ابلاغی مبنی بر اهمیت بالای ساعات اول تهدیدات نرم احتمالی و نیاز به تدبیر در خصوص کاهش خسارات ساعات اولیه تهدید نرم، موضوع تشخیص تهدیدات اولیه و شروع جنگ از اهمیت ویژه‌ای برخوردار است. لذا توجه به ویژگی هوشیار بودن شبکه فرماندهی و کنترل با اجتناب از استهلاک شبکه و تجهیزات، در طراحی و معماری شبکه فرماندهی و کنترل، حائز اهمیت ویژه است. ضرورت داشتن ساختار و الگوی مدرن فرماندهی و کنترل بگونه‌ای که بتوان سناریوهای دفاعی مختلف را در شرایط دفاعی متفاوت اجرا نمود و امکان بهره‌مندی از مزایای ساختار در راستای نیل به نیا زها و ضرورت‌های ذیل تدوین نمود:

- معماری، طراحی، تولید و تجهیز و تکمیل کلیه یگان‌های نیروهای مسلح به سامانه‌ها و زیر سامانه های فرماندهی و کنترل قدرت نرم.

- دستیابی به شبکه ارتباطی امن و پایدار مابین مراکز فرماندهی و کنترل قدرت نرم (ثابت و سیار)، سامانه‌ها و زیرسامانه‌ها، حساسه‌ها و تجهیزا ت مرتبط با جنگ نرم.
- بهره‌گیری از کلیه اطلاعات، اخبار، رویدادها، موضو عات عملیات روانی در شبکه‌های اجتماعی، فضای مجازی و همچنین کلیه اطلاعات مؤثر در نیروهای مسلح به صورت بلادرنگ مانند اطلاعات سامانه‌ها، مراکز مدیریت عملیات روانی نیروها، اطلاعات شبکه‌های اجتماعی مرتبط با سایر سازما نها (فتا ناجا، سایبری سپاه و...) از تمامی منابع اطلاعاتی متعلق به کلیه یگانهای درگیر در رزم.
- امکان ارائه تدابیر و دستورات و در نهایت هدایت مراکز فرماندهی و کنترل قدرت نرم نیرویی/منطقه‌ای از طریق بررسی گزارشات تحلیلی بصورت آنلاین در مناطق تحت شبکه فرماندهی و کنترل با تاکید بر استقلال عملکرد نیروها.
- امکان هدایت و کنترل تجهیزات جنگال و پدافند غیرعامل کشوری و لشکری. [۲,۳]

اهداف تحقیق

هدف اصلی

هدف کلی این طرح " معماری، طراحی، پیاده‌سازی و توسعه شبکه یکپارچه فرماندهی و کنترل قدرت نرم نیروهای مسلح " می‌باشد.

اهداف فرعی

- جمع‌آوری و به کارگیری کلیه اطلاعات مؤثر در افزایش قدرت نرم (حوزه‌های فضای مجازی، مولفه‌ها و شاخص‌های اجتماعی و عملیات روانی) نیروهای مسلح از کلیه منابع اطلاعاتی داخل و خارج از نیروهای مسلح
- توزیع و انتشار مؤثر اطلاعات در شبکه.
- دسترسی براساس نیاز کلیه اقدامگرها به اطلاعات و تدابیر تزریق شده در شبکه.
- تحت پوشش قرار دادن تعداد و تنوع زیاد تجهیزات، شبکه‌ها و رسانه‌ها.
- تولید اطلاعات تصمیم ساز.
- دریافت و تأثیردهی بلادرنگ تحلیل اطلاعاتی از طریق داشبور دهای نرم افزاری و تدبیر عملیاتی کاربران باتجربه در شبکه. و ارائه گزارشات تحلیلی در حوزه‌های فضای مجازی، اجتماعی و عملیات روانی.
- ایجاد شرایط امکان کنترل و هدایت کلیه مراکز فرماندهی و کنترل قدرت نرم نیروهای مسلح اعم از مراکز فرماندهی و کنترل قدرت نرم نیرویی.

سوالات تحقیق

سوال اصلی

الگوی مناسب نیازمندیهای فرماندهی و کنترل قدرت نرم نیروهای مسلح چگونه است. ؟

سوالات فرعی

۱. رویکردهای منطقی و سیستمی الگوی فرماندهی و کنترل قدرت نرم چگونه است؟

۲. روابط و تعاملات فی مابین چگونه باید باشد. ؟

۳. تهدیدات حوزه سایبر شبکه فرماندهی و کنترل قرارگاه چیست؟

۴. آسیب‌پذیری شبکه‌های فرماندهی و کنترل قرارگاه در مقابل تهدیدات سایبری چگونه است؟

۵. ساختار مناسب جهت مقابله و کاهش اثر تهدیدات سایبری شبکه فرماندهی و کنترل قرارگاه چگونه باید باشد؟

بخش دوم: ادبیات پژوهش

جنگ سایبری و جنگ اطلاعات، اصول جنگی جدیدی را جایگزین اصول قدیمی نموده‌اند. نوع نیروهایی که در این گونه جنگ‌ها شرکت می‌کنند، نحوه استفاده از آنها و حتی یورش به سوی دشمن، (استراتژی جنگی) نیز با گذشته تفاوت‌های بسیار عمیقی پیدا کرده است. امروزه تصمیم گیری در مورد تعداد، نوع و مکان استفاده از حسگرها، کامپیوترها، شبکه‌ها و بانک‌های اطلاعاتی که در جنگ مورد استفاده قرار میگیرند همان اهمیتی را پیدا کرده که در جنگ جهانی دوم در مورد زمان و نحوه استفاده از بمب افکن‌ها در پشت خط مقدم دشمن مطرح می‌شد

به عنوان یک نوآوری در استراتژی جنگی، جنگ رایانه‌ای قرن ۲۱ را می‌توان با "بلیتز گریک" قرن ۲۰ مقایسه کرد. جنگ رایانه‌ای بلیتز گریک عصر اطلاعات است. بلیتز گریک یا " جنگ رعدآسا نوعی از استراتژی جنگی است که در ابتدا توسط آلمانی‌ها در اسپانیا در سال ۱۹۳۸ و سپس علیه لهستان در سال ۱۹۳۹ بکار گرفته شد. در این نوع جنگ با حمله بسیار سریع و همه جانبه و با حمایت توپخانه و تانک تلاش می‌شود تا دشمن غافلگیر شده و پیش از آنکه بتواند عکس العمل نشان دهد از پای درآید.

تاریخچه جنگ سایبری و شبکه ای

در جنگ رایانه‌ای برتری در کسب، کنترل، پردازش و انتقال اطلاعات و تلاش برای جای گیری صحیح، کشف نقشه‌های دشمن و حمله به ضعیف‌ترین و حساس‌ترین نقطه‌های خطوط دفاعی در مناسب‌ترین لحظات قبل از اینکه دشمن حتی متوجه نقاط ضعف خود شود، از اهمیت شایان توجهی برخوردار است. میدان نبرد پست مدرن با استفاده از فناوری اطلاعات در زمینه‌های استراتژیکی و تاکتیکی نسبت به گذشته خود تغییر خواهد کرد[۹].

در طول تاریخ ودر اکثر دیدگاه‌های سنتی نسبت به ارتش، ارتشیان دارای سلسله مراتب کاملا دقیقی بوده و نیروها به اجرای دقیق و بی‌چون وچرای دستورات مافوق خود افتخار می‌کردند. دراین ارتش‌ها تمامی دستورات دقیقا از بالا دیکته میشد و سربازان پایین‌تر بدون چون وچرا آنها را اجرا می‌کردند. اما امروزه انقلاب اطلاعاتی باعث ایجاد تغییراتی در این وضعیت شده و سلسله مراتب ارتشی در معنای قدیمی خود منسوخ شده وبرای فرمانبرداری نظامی مرزهای جدیدی در حال تعریف است. برای مثال مغول‌ها در قرن ۱۳ بر اساس جنگ اطلاعاتی امروزی، خود را سازمان داده بودند و بیشتر شبیه به یک شبکه بودند تا سلسله مراتبی منظم. به عنوان نمونه‌ای امروزی‌تر می‌توان از ویت کنگ‌هایی که در جنگ آمریکا و ویتنام می‌جنگیدند نام برد. نیروهای نظامی نسبتا کوچکی که در برابر یکی از بزرگترین نیروهای نظامی قرن حاضر بخوبی ایستادگی کرد. ویت کنگ‌ها نیز بیشتر به نظامی شبکه‌ای شبیه بودند تا سیستمی مبتنی بر سلسله مراتبی رسمی. پیشرفت فناوری اطلاعاتی و شبکه‌های رایانه‌ای باعث شد تا صنایع نظامی نیز از این مسئله تاثیر پذیرفته و به سمت رایانه‌ای‌تر شدن پیش روند. امروزه حتی صحبت از چیزی به نام جنگ راه دور به میان می‌آید. جنگی که در آن فرماندهان و افسران از نقطه‌ای بسیار دور مستقیما عملیات نظامی در یک منطقه جنگی را به دست گرفته و آن را هدایت می‌کنند. بر اساس گزارشی که رادیو آمریکا مخابره کرده وزارت دفاع آمریکا قصد دارد سیستم‌های تسلیحاتی و نظامیان را در شبکه‌ای ادغام کند که اصطلاحا NCF یا جنگ مبتنی بر شبکه نامیده میشود.

از نوامبر سال ۲۰۰۲، خلبانان نیروی هوایی آمریکا به آخرین نسخه از یک بازی ویدئویی دست یافته‌اند که می‌توانند از طریق هر کامپیوتر معمولی PC که دارای یک کاوشگر اینترنتی و یک نرم افزار ویژه نظامی باشد به شبکه کامپیوتری نیروی هوایی آمریکا متصل شوند. هنگامی که به شبکه وصل شدند میتوانند هواپیماهای شناسایی (بدون سرنشین) را به طرف هدف، راهنمایی کرده و یا تقاضای حمله هوایی کنند. آنها حتی از طریق یک لپ تاپ متصل به اینترنت می‌توانند مسیر پرواز را طراحی کنند. استفاده نظامی از شبکه اینترنت مسئله عجیبی قلمداد نمی‌شود. نباید از یاد برد که ابداع و اختراع اینترنت توسط نظامیان و بخصوص وزارت دفاع آمریکا صورت گرفته است. در اواسط دهه نود میلادی راه حل وزارت دفاع آمریکا برای متصل کردن سیستمهای نظامی مختلف به زیر یک چتر به گونه‌ای که حتی اگر یک‌بخش دچار صدمه و اخلال شود، بخشهای دیگر به کار خود ادامه دهند، پروژه‌ای به نام آرپانت بود که پدر اینترنت فعلی به شمار می‌رود.

تاریخچه عملکردهای سایبری

• استراتژی رخنه رایانه ای

دولت آمریکا ماهها پیش از شروع جنگ علیه عراق در راستای جنگ اطلاعاتی و عملیات روانی خود علیه این کشور، استراتژی معینی را تحت عنوان استراتژی رخنه و ایجاد اختلال در سیستم‌های رایانه‌ای دشمن تصویب کرده بود. بر اساس این استراتژی ماهها و هفته‌ها پیش از شروع جنگ باید سیستمهای ارتباطی و رایانه‌ای عراق شناسایی می‌شد و عملیات لازم برای نفوذ و ایجاد اختلال در عملکرد آنها صورت می‌گرفت. روزنامه واشنگتن پست در گزارشی که دوهفته پیش از شروع جنگ در عراق منتشر کرد فاش نمود که: آمریکا سرگرم بررسی و طرح‌ریزی برای دست زدن به حملات اینترنتی علیه کشورهایی مانند عراق است. این حملات قرار بود پیش از شروع عملیات نظامی یا همزمان با آن صورت گیرد. سایت اینترنتی BBC دو روز پس از انتشار گزارش چنین نوشت: "در هرگونه نبرد اینترنتی علیه عراق باید نقشی را که رایانه‌ها در اداره امور این کشور ایفا می‌کنند مد نظر قرار داد".

• تروریسم رایانه‌ای

اخلال گران رایانه‌ای دارای اهداف گوناگونی هستند. برخی با هدف کسب پول و سود به شبکه‌ها نفوذ می‌کنند و مثلا با هک کردن کارتهای اعتباری پول سرشاری به جیب می‌زنند. بعضی دیگر هدفشان سرگرمی، تفریح و به رخ کشیدن توان فنی و رایانه‌ای‌شان است. اما بسیاری از هکرها هم دارای گرایشات سیاسی یا اجتماعی هستند. به این گروه از هکرها Actives گفته می‌شود. هدف عمده این گروه از نفوذ کننده‌ها اخلال در سیستمهای رایانه‌ای سازمان‌ها، وزارتخانه‌ها یا شبکه‌های مرتبط با دولت خاصی است. شبکه رایانه‌ای ارتش، وزرات دفاع، وزرات خارجه، پلیس، کاخ ریاست جمهوری، شبکه رادیو و تلویزیون، بانک مرکزی، احزاب سیاسی، پارلمان و کنگره و سایر دستگاههای سیاسی از عمده‌ترین اهداف این گروه به شمار میروند.

وینستون چرچیل در جنگ جهانی دوم از پیدایش جنگ الکترونیک به عنوان نبرد جادویی نام برد واینک پس از ۵۵ سال از آن گفتار نبرد جادویی در عرصه اینترنت تحقق یافته است. به موازات آنکه دولت‌ها و شرکت‌ها سعی می‌کنند تا هرچه بیشتر شبکه‌های رایانه‌ای را تحت نفوذ و کنترل خود درآورند شبکه اینترنت هم به محیطی مناسب برای تروریست‌های رایانه‌ای، فعالان سیاسی و نفوذ گران اینترنتی و حتی خود دولتها تبدیل شده است. در سال ۱۹۹۸ وزارت دادگستری و پلیس فدرال آمریکا به طور مشترک واحد جدیدی به نام مرکز پشتیبانی زیر ساخت ملی تشکیل دادند که وظیفه آن تقویت توان دفاعی ایالات متحده در مقابل تروریسم رایانه‌ای و سایر تهدیدات الکترونیک است.

دو سرهنگ ارتش چین با انتشار کتابی به نام "جنگ نامحدود" این موضوع را مطرح کردند که چین به منظور کسب توانایی جنگیدن با کشور قدرتمندی چون آمریکا نیازمند یافتن شیوه‌هایی جدید و غیر متعارف رویارویی همچنین تروریسم رایانه‌ای است. در سال ۲۰۰۲ نیز چندین پایگاه بین المللی اینترنتی متعلق به گروه مذهبی dafa flaun چین توسط نامه‌های الکترونیک و سایر سلاحهای دیجیتال مورد حمله قرار گرفتند. بسیاری از صاحب نظران مسائل رایانه‌ای و اینترنتی اعتقاد داشتند که این اقدامات از جانب دولت چین که در آن زمان حملاتی را علیه گروه مذکور آغاز کرده بود رهبری شده است. در مه اوت سال ۲۰۰۲ چندین پایگاه دولتی رایانه‌ای تایوان انباشته از پیامهایی شدند که همگی مخالفت خود را با دولت و استقلال این کشور اعلام می‌کردند. به دنبال آن نفوذ گران رایانه‌ای تایوانی وارد پایگاههای چینی شدند و سرود ملی تایوان و نیز پیامهایی را به طرفداری از این کشور انتشار دادند.

ایالات متحده تا به حال با یک تهدید مجبور کننده از ناحیه تروریست‌ها که با استفاده از تکنیک‌های جنگ اطلاعاتی برای از کار انداختن زیر ساخت‌های حساس انجام شده باشد روبرو نبوده است. در این زمان تروریست‌ها برای انجام یک حمله سایبر، انگیزه، توانمندی یا مهارت ندارند. حملات سایبر می‌تواند به عنوان وسیله کمکی جهت حمایت از عملیاتی دیگر مورد استفاده قرار گیرد. مثلا به عنوان پشتیبان عملیات نظامی متعارفی (و نه به عنوان جانشین آنها) انجام گیرد. برای روشن شدن موضوع به مورد زیر اشاره می‌کنیم. در اوایل سال ۱۹۹۸ یک عیب طراحی در سیستم برچسب امنیتی که بطور گسترده‌ای مورد استفاده فرودگاهها، زندانهای ایالتی، موسسات مالی، پیمانکاران ارتش، ادارات دولتی (از جمله سیا) و شرکت‌های برخوردار از فناوری بالا قرار داشت گزارش شد. این آسیب‌پذیری به متجاوزان امکان می‌داد از یک ارتباط شبکه‌ای یا تلفنی برای ایجاد برچسب دائمی یا موقت که موجب دسترسی به مناطق مورد نظر امنیتی، مناطق حساس محافظت از درهای بدون قفل استفاده نماید و برچسب‌هایی طراحی کند که از ورود و خروج شخص به منطقه مورد نظر امنیتی، هیچ نشانه‌ای باقی نگذارد.

یک نمونه جنگ شبکه‌ای را می‌توان در مبارزه ارتش آزادیبخش ملی زاپاتیستا و دولت مکزیک یافت. در اولین روز سال ۱۹۹۴، ارتش آزادیبخش ملی زاپاتیستا، شش شهر را در چیاپاس اشغال کردند و علیه دولت مکزیک اعلان جنگ نموده، خواهان تغییراتی شدند و سرانجام به یک پیکار رسانه‌ای جهانی دست زدند. آنها خواهان اصلاحات سیاسی، اقتصادی و اجتماعی از جمله حقوقی برای بومیان، انتخابات مشروع و منصفانه و لغو مقرارت حاکم بر اجاره زمین شدند. ارتش مکزیک سرزمین‌های اشغالی را پس گرفت، اما زاپاتیست‌ها سعی کردند از دارا بودن زاپاتیست‌ها و حامیان آنها از اینترنت برای سخن گفتن درباره وضعیت خود و هماهنگ

کردن فعالیت‌ها استفاده کنند. یک گروه از حامیان نیویورکی به نام "تاتر مزاحمت الکترونیکی"، حمله به سایت زدیلو رئیس جمهور مکزیک را سازمان دادند. در ۱۰ آوریل ۱۹۹۸ شرکت کنندگان در حمله بروزرهای شبکه وب خود را به سایتی با نرم افزار فلادنت که سایت هدف را با ترافیک بمباران میکرد، وصل کردند. گروه تاتر مزاحمت الکترونیکی برنامه‌ریزی کرد که در ۱۰ مه، حمله را تکرار کند، اما وقتی گروه حقوق بشر مستقر در مکزیک اعتراض نمود برنامه خود را تغییر داد. در نه سپتامبر این گروه دوباره به سایت پرزیدنت زدیلو و نیز سایت‌های پنتاگون و بورس فرانکفورت حمله کرد.

اینکه سیستم‌های حساس بطور بالقوه در معرض حملات سایبر قرا ردارند، با تمرین ژوئن ۱۹۹۷ با اسم رمز" دریافت کننده خوانا" که توسط اداره امنیت ملی آمریکا برگزار شد مورد توجه قرا رگرفت. تعیین آسیب‌پذیری های رایانه‌های ارتش آمریکا و پاره‌ای از زیر ساخت‌های غیر نظامی در برابر یک حمله سایبر هدف این تمرین بود. بنا بر گزارش‌ها، تیمی مرکب از دو عضو، بخشهای معینی از زیر ساخت‌های نظامی از جمله فرماندهی ایالات متحده در اقیانوس آرام را هدف قرار دادند. یک نفر نقش مهاجم را بازی کرد و نفر دیگر کار را زیر نظر داشت تا مطمئن شود که طبق برنامه انجام می‌گیرد. این وارد شوندگان با استفاده از ابزارهای فراوان و رایج ورود غیر مجاز که به آسانی از اینترنت قابل تحصیل است به تعدادی از سیستم‌ها دسترسی ممتاز یافتند. آنها نتیجه گرفتند که زیر ساخت‌های نظامی را می‌توان مختل کرد وآرایش احتمالی نیروها را با مانع روبرو ساخت. این تمرین همچنین شامل سناریوهای مدونی علیه شبکه برق و سیستم اورژانس ۹۱۱ که موجب اخلال در این خدمات می‌گردید نیز بود.

• گذار آمریکا به جنگ سایبری و اطلاعاتی

سابقه ایده جنگ اطلاعات در آمریکا به سال ۱۹۷۰ بر می‌گردد یعنی هنگامی که دکتر "تام رونا" اولین بار این واژه را بکار برد. کارهای انجام شده در این زمینه تا سال ۱۹۹۰ که وزارت دفاع آمریکا ایده جنگ فرماندهی و کنترل را به عنوان بخشی از جنگ اطلاعات در حوزه وسیع تری مطرح نمود انتشار پیدا نکرد. بعد از انتشار کتاب جنگ و ضد جنگ نویسنده‌های متعددی مقالاتی در خصوص راهبرد جنگ خلیج فارس بر مبنای اطلاعات منتشر نمودند

کلنل آلن کمپن در کتاب "اولین جنگ اطلاعات" بحث بکارگیری سامانه C4I در جنگ خلیج فارس و مزایای اختلاف اطلاعاتی بوجود آمده و ایجاد نتایج فریب، مانور و سرعت را مطرح نمود. نیل مانرو در کتاب "سرعت و مرگ" درگیری الکترونیکی و جنگ مدرن اصول جنگ الکترونیک و اثرات آن در فرماندهی و کنترل را به صورت مبسوط ارائه نموده است. در همین ایام ویت شوارتا در کتاب مدرن جنگ اطلاعات: هرج و مرج در ابر آزادراه اطلاعات، تهدیدهای وسیع در شبکه جهانی اطلاعات را بررسی کرده است. کنفرانس‌های متعددی که از سال ۱۹۹۳

در زمینه جنگ اطلاعات و سایبری توسط صنایع دفاعی و حفاظت اطلاعات ارائه شده به ایجاد یک فضای باز نقد وبررسی جنگ اطلاعات و سایبری کمک نموده است. در همین زمان هئیت علوم دفاعی وزارت دفاع ۲ پروژه اصلی در این زمینه را به اجرا گذاشت و لزوم سرمایه گذاری گسترده در زمینه‌های ساماندهی وسئولیتها در IW، ایجاد امنیت برای DII و تحقیق توسعه دربخش IW را توصیه نمود. اهمیت سامانه‌های اطلاعلاتی ملی و پتانسیل آسیب‌پذیری آن دو محور مورد توجه و تاکید آمریکا در مواجهه با تهدیدات و درگیری اطلاعاتی قرا گرفت. ایالات متحده آمریکا در سال ۱۹۹۶ تاکید خود را با ارائه برنامه ویژه حمایت از زیر ساخت اطلاعات در قالب دستور اجرایی ۱۳۰۱۰ به اجرا درآورد. در چشم انداز مشترک ۲۰۱۰ که توسط ستاد مشترک آمریکا در سال ۱۹۹۶ منتشر شد برتری اطلاعات به عنوان محوری‌ترین عنصر موثر در یکپارچگی و تقویت چهار عامل اساسی عملیاتی جنگ‌های قرن۲۱ به شرح زیر معرفی گردید:

۱- برتری مانور؛ برای افزایش سرعت، دقت و تحرک در حمله به هدف از طریق واحد انجام می‌شود.

۲- درگیری دقیق؛ توسط شناسایی و الویت‌بندی دقیق اهداف و استفاده از نیروهای فرماندهی و کنترل مشترک انجام میگیرد.

۳- هدایت لجستیک در جهت حمایت موثر از نیروها با یکپارچه‌سازی اطلاعات از نیازها، امکانات حمل و نقل و منابع صورت می‌گیرد.

۴- حمایت همه جانبه از نیروها، فرایند و سامانه‌ها از طریق هشدار و ارزیابی تهدیدها در تمامی ابعاد (فیزیکی – اطلاعاتی و ادراکی) صورت می‌گیرد.

اعلام هشدار سیا

در سال ۲۰۰۰ جان سرابیان، مدیربخش عملیات اطلاعاتی سیا، طی گزارشی به کمیسیون مشترک اقتصادی کنگره آمریکا نسبت به خطر توسعه توانمندی‌های آفندی اطلاعاتی کشورهای مختلف دنیا، بویژه چین و روسیه، هشدار داد. وی خاطر نشان کرد که سیا به طور مکرر شاهد ظهور دکترین‌ها و برنامه‌های مهم جنگ سایبر در کشورهای مختلف دنیاست.

سرابیان می‌افزاید که " ما بر اساس منابع اطلاعاتی مختلف توانسته‌ایم چندین کشور را شناسائی کنیم که با جدیت و عزم لازم مشغول پیگیری برنامه‌ها و پروژه‌های دولتی در زمینه آفند سایبر هستند. " در این گزارش تاکید شده است که جنگ اطلاعاتی به یک گزینه استراتژیک برای کشورهائی تبدیل می‌شود که به خوبی دریافته‌اند هر گونه مقابله نظامی متعارف با آمریکا محکوم به شکست است. همچنین اظهارات مستند مقامات رسمی روسیه و چین حاکی از آن است که به نظر آنها یک تهاجم سایبر علیه اهداف ملی دشمنان مانند مراکز حمل و نقل و سیستم توزیع و انتقال برق به دلیل عواقب فاجعه‌آمیز آن کاملاً قابل مقایسه با

کاربرد سلاح‌های کشتار جمعی است. یکی از فرماندهان ارشد چینی بر این باور است که می‌توان از طریق جنگ سایبر و "تغییر مستقیم محتوای پایگاه‌های داده دشمن"، مراکز فرماندهی و کنترل دشمن را از کار انداخته و قضاوت و تصمیم‌گیری‌های آنها را توام با اشتباه‌های فاحش کرد. این فرمانده چینی صریحا به امکان تسلط بر نظام بانکی کشور دشمن و حتی بی‌ثبات کردن نظم عمومی اشاره می‌کند.

" فناوری‌ها و ابزارهائی که چند هفته پیش توسط گروهی از خرابکاران نفوذگر مورد استفاده قرار گرفته و موجب شد که امکان دسترسی به چند وب سایت بزرگ موقتا از بین برود، در مقیاس گسترده‌تر دولت – ملت نهایتاً موجب صدمات و خسارت‌های عمده به اقتصاد و زیر ساخت ملی خواهد شد. " {دانیل کوئل} کوئل علاوه بر اشاره به تلاش آشکار مقامات روسیه و چین برای توسعه تکنیک‌های لازم جنگ سایبر خاطر نشان می‌کند که آنها علاقه‌مند هستند که برای ممنوع‌شدن چنین حملاتی اقدامات بین‌المللی از طریق سازمان ملل متحد انجام گیرد. با ارائه مثال‌ها و موارد متعدد می‌توان پیچیدگی جنگ سایبر و نگرانی‌های مربوط به آن را تا حدودی نشان داد. بی‌تردید نقاط ضعف عمده برای دفاع سایبر عبارتند از:

شناسائی هویت و مکان مهاجم

شناسائی مقاصد و اهداف مهاجم

تشخیص به موقع یک تهاجم هماهنگ و گسترده در شرف وقوع

ارزیابی و برآورد میزان صدمات و خسارات بعد از تهاجم

مواردی که به طور خلاصه در زیر معرفی شده‌اند نشان می‌دهند که در قرن بیست و یکم شکل اساسا نوینی از جنگ ظهور می‌کند که کشورهای مختلف دنیا بویژه آمریکا شاید برای مواجهه و درگیر شدن در آن آماده باشند و شاید هم نباشند.

بخش سوم: بررسی الگو

هنگام بررسی الگوی جنگ‌های آینده باید فضای مفهومی چنین جنگ‌هایی را به خوبی تشریح کرد. البته ضروری است پیش از ترسیم این نقشه مفهومی، افق آینده پژوهی صریحا تعیین شود. زیرا با توجه به تحولات شتابانی که در حوزه‌های مختلف تمدن مدرن رخ می‌دهند هر گونه پیش‌بینی یا برآورد درباره وضعیت جهان در دهه‌های آینده احتمالاً با خطای بالا همراه خواهد بود. به عنوان مثال، علی رغم گسترش و نفوذ حیرت انگیز فناوری اطلاعات و ارتباطات و ملموس بودن پیامدها و تاثیرات این فناوری بر چیستی و چگونگی اصول جنگ، امروزه هیچ کارشناسی قادر نیست که پیامدها و تاثیرات پیشرفت‌های انقلابی در زمینه فناوری نانو و فناوری زیستی را، که عصر طلائی آن‌ها شاید از سال ۲۰۲۰ به بعد آغاز شود، بر جنگ‌های دهه‌های آینده به درستی پیش‌بینی کند. در نتیجه افق آینده پژوهی دراین گزارش حداکثر تا

سال ۲۰۱۵ ادامه یافته و ترجیحاً درباره افق‌های دورتر سکوت می‌کند. مفاهیم عملیاتی نوین که در آینده نزدیک شاهد ظهور آن‌ها خواهیم بود به روابط و نحوه تعامل عناصر کلیدی جنگ‌های آینده بستگی خواهند داشت.

در فصل‌های گذشته سه نظریه کلیدی درباره نحوه تکامل امور نظامی در جهان معرفی شدند. اگرچه فرضیات و روش‌های استنتاج این نظریه‌ها تا حدودی با یکدیگر متفاوت هستند اما با مرور و تطبیق این سه نظریه می‌توان وجوه مشترکی بین همه آن‌ها یافت.

مثلاً در نظریه جنگ نسل چهارم که مبتنی بر ایده‌ها یا فناوری‌های نو می‌باشد تسلحیات هدایت مستقیم انرژی، روباتیک و عملیات‌های رسانه ای، و نهایتاً تروریسم معرفی شده‌اند که اینها به مفاهیم جنگ کلاسیک پیشرفته، جنگ روباتی، جنگ روانی، و جنگ ناهمتراز منتج می‌شوند.

همچنین در نظریه جنگ موج سوم که بیشتر در جامعه اطلاعات محور مطرح شده و جنگ‌افزارهای هدایت‌پذیر دقیق، روبات‌ها و فناوری غیرکشنده، تسلیحات هدایت مستقیم انرژی و ویروس‌های رایانه‌ای کانون تمرکز آن می‌باشد، مفاهیم جنگ سایبر ، جنگ کلاسیک پیشرفته و جنگ روباتی مورد تاکید قرار می‌گیرند.

نهایتاً از نظریه جنگ عصر چهارم که به دو صورت سبک غربی مبتنی بر فناوری‌های پیشرفته، تسلیحات هدایت‌پذیر دقیق، جنگ اطلاعاتی، جنگ‌افزارهای غیرکشنده، یگان‌های جنگی روباتیک، تسلیحات هدایت‌کننده انرژی و نیز سبک غیرغربی مبتنی بر تروریسم معرفی می‌شود می‌توان مفاهیم جنگ کلاسیک پیشرفته، جنگ سایبر، جنگ روباتی و جنگ ناهمتراز را استخراج کرد.

در واقع هر سه نظریه مذکور به طور مستقیم یا غیر مستقیم بر اهمیت پنج مفهوم جنگی زیر تاکید می‌کنند:

جنگ کلاسیک پیشرفته (اعم از متعارف و غیرمتعارف)

جنگ روباتی

جنگ روانی

جنگ سایبر

جنگ ناهمتراز

شایان ذکر است که جنگ ناهمتراز به خودی خود یک نوع جنگ متمایز محسوب نمی‌شود بلکه باید آن را یک رویکرد یا نگاه متفاوت به عملیات جنگی تلقی کرد. در واقع در یک جنگ ناهمتراز، تفاوت قابل توجهی بین قوای دو طرف وجود دارد، به همین دلیل می‌توان با توجه به توانمندی‌ها و نقاط ضعف مهاجم و مدافع از هر چهار نوع جنگ کلاسیک پیشرفته، روباتی،

روانی، و سایبر بهره جست. به بیان دیگر جنگ‌های ناهمتراز اساساً دربرگیرنده روش‌هایی‌اند که در سطوح مختلف از مفاهیم و اصول جنگ کلاسیک پیشرفته (با یا بدون کاربرد سلاح‌های کشتار جمعی)، جنگ روانی، جنگ سایبر، و جنگ روباتی تبعیت می‌کنند. همچنین باید خاطر نشان کرد که در تعاریف رایج ارائه شده برای جنگ ناهمتراز بیشتر عدم توازن قدرت بین طرفین درگیر پر رنگ شده و اساساً انجام عملیات ناهمتراز به طرف ضعیف‌تر نسبت داده می‌شود [۶].

در حالی که اگر تعریف جنگ ناهمتراز را با توجه به ویژگی مهم " تاثیر نامتناسب" (یعنی تحقق اهداف استراتژیک از طریق اقدامات غیر استراتژیک) گسترش دهیم، می‌بینیم که انتخاب این رویکرد متفاوت به جنگ لزوما در پرتو موازنه قدرت نظامی انجام نمی‌شود. بنابراین اگر یک طرف قوی تشخیص دهد که می‌تواند با استفاده از روش‌های ناهمتراز به هدف استراتژیک خود یعنی تسلیم شدن دشمن و از بین بردن اراده و روحیه جنگی او دست یابد، قطعا به رویکردهای ناهمتراز متوسل خواهد شد.

در جنگ‌های آینده نیز مانند جنگ‌های گذشته اصولاً تحقق دو هدف بنیادی در دستور کار قرار می‌گیرند که عبارتند از:

تسلیم شدن دشمن

نابود شدن دشمن

نمودار زیر جنبه‌های مختلف تهدیدات سایبر را نشان می‌دهد.

شکل(۱) جنبه‌های مختلف تهدیدات سایبر[۸]

به عنوان مثال، هرگونه ضعف یا قوت در زیر ساخت‌ها و نرم افزارهای حیاتی فناوری اطلاعات و ارتباطات به ضعف یا قوت در مفاهیم مختلف جنگی می‌انجامد. در نتیجه نظام فناوری اطلاعات و ارتباطات بر همه انواع جنگ تاثیرگذار می‌باشد. اما عکس این رابطه لزوماً همیشه صادق نیست. مثلاً جنگ روانی هیچ تاثیر معینی بر نظام فناوری اطلاعات و ارتباطات ندارد.

بخش چهارم: یافته¬های پژوهش و تجزیه و تحلیل داده¬ها

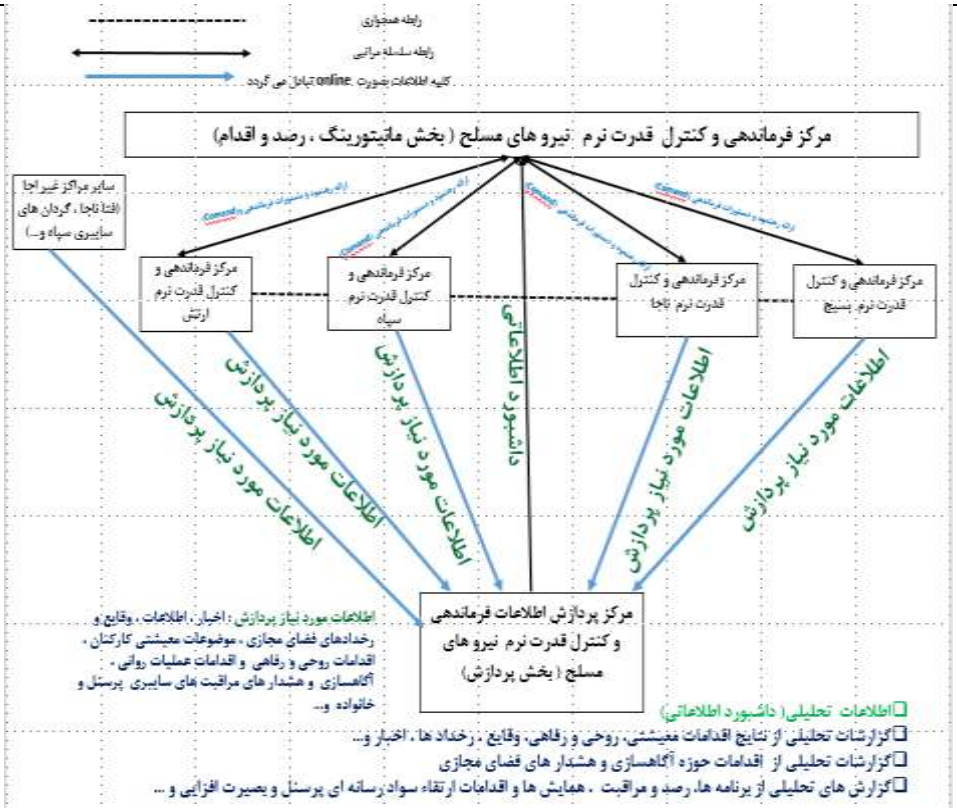
اکثریت مصاحبه شوندگان جنگ اطلاعاتی، رایانه ای و شبکه محور را یکی از ابعاد جنگ های نوین و آینده دانسته و نیاز به مجهز شدن به ابزار آفندی و پدافندی مناسب را یک ضرورت اجتناب ناپذیر می دانند. در این راستا ایجاد ساختار

یگانی مناسب همراه با نیروهای کیفی (دارای توان فنی وعلمی بالا در علوم سایبری)جهت اجرای عملیات در این فضا، دستیابی به ابزارهای ویژه این نوع جنگ و همچنین ایجاد بسترهای خاص را از ملزومات شمرده و اعتقاد دارند که:

با ایجاد مرکز فرماندهی و کنترل قدرت نرم مرکب از کارشناسان مجرب وخبره در زمینه فناوری اطلاعات (محوریت اجرا) و عملیاتی(مشاوره) جهت شناسایی و ارزیابی نقاط آسیب پذیر شبکه فرماندهی و کنترل و مشخص نمودن درگاههای ورودی و خروجی اطلاعات نظارت و بررسی مداوم اطلاعات جابجا شده(پایش)، ایجاد ساختار و بکارگیری نرم افزارهای تخصصی در این زمیه و استفاده از سامانه مدیریت امنیت آموزش و بهره گیری از کارکنان مجاز و رعایت مسائل و نکات امنیتی دفاع سایبری قابل اجرا می‌باشد [۷].

راهکارهای کاربردی

شاخص‌های اصلی در تبین نیازهای فرماندهی و کنترل قدرت نرم شامل مراکز نیرویی، سطوح فرماندهی و کنترل و سامانه‌ها و نرم افزارهای تخصصی در این زمینه می‌باشد که در این تحقیق نهایتا به ساختار ذیل می‌رسیم:



شکل (۲) شاخص‌های اصلی در تبین نیازهای فرماندهی و کنترل قدرت نرم نیروهای مسلح [۷]

نتیجه گیری

چنان که قبلا نیز اشاره شد کشورهائی که مراحل ابتدائی بهره‌برداری از فناوری اطلاعات را پشت سر می‌گذرانند به تدریج از موقعیت عدم آسیب‌پذیری نسبی به موقعیت شامل درجه‌ای از آسیب‌پذیری حرکت می‌کنند.

چنین احتمال می‌رود که در آینده نزدیک بررسی‌های بین‌المللی درباره الگوها، مزایا، محدودیت‌ها، و شرایط جنگ اطلاعاتی و سایبری نهایتاً اکثر کشورهای دنیا را به سمت طرح‌ریزی پدافندی اطلاعاتی سوق داده و آنها را ملزم به ارتقای توان دفاع اطلاعاتی و شبکه‌ای رایانه‌ای در برابر آفندهای آن بویژه از سوی ایالات متحده آمریکا کند. از این رو بعید نیست که یک بازاربین‌المللی برای طراحی و توسعه ابزارهای قوی پدافند سایبری ظهور کند که در طی زمان و حتی در طی یک شبانه‌روز اکثر ابزارها و تکنیک‌های آفندی را خنثی کنند.

پدافند شبکه‌ای فرماندهی و کنترل قدرت نرم شامل اقداماتی می‌شود که به منظور حفاظت، پایش ، تحلیل، آشکارسازی و واکنش به فعالیت‌های غیر مجاز در سیستم‌ها و شبکه‌های فضای

مجازی، شبکه‌های اجتماعی و مجموعه عملیات روانی انجام می‌شود. قدرت نرم آفندی و پدافندی شامل اقداماتی می‌شود که به منظور پرهیز، آشکارسازی و منحرف‌سازی اقدامات مستقیم یا غیر مستقیم دشمن علیه سیستم‌های اطلاعاتی خودی انجام می‌گیرند. در پدافند شبکه فرماندهی و کنترل بر آشکارسازی و تطبیق، یکسان‌سازی و شناسایی اهداف و انجام تدبیرهای لازم اشاره دارد.

قدردانی

از کلیه کسانی که در امر تحقیق حاضر مرا یاری دادند تشکر می‌کنم، همچنین از داوران محترم به دلیل مطالعه دقیق و پیشنهادهای ارزشمندشان که باعث بهبود و ارتقا مقاله حاضر شد کمال تشکر را داریم.

منابع

[۱] اسکیلز، رابرت، جنگ آینده، ترجمه عبدالمجید حیدری، تهران: سپاه پاسداران انقلاب اسلامی، دانشکده فرماندهی و ستاد، دوره عالی جنگ، .۱۳۹۴

[۲] *فصنامه پژوهشی عملیات ر.وانی*

[۳] *جزوه پدافند غیرعامل، قرار گاه پدافند هوائی خاتم الانبیاء*، معاونت پدافند غیر عامل، تهران: تجدید چاپ معاونت آموزش ناجا، ۱۳۹۴.

[۴] *طرح فراسازمانی فرماندهی و کنترل، چشم‌انداز مشترک ارتش آمریکا در افق ۲۰۲۰*، تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی، ۱۳۹۶.

[۵]عقلمند، احمد، *مروری بر تاریخ تحولات فناوری سلاح‌های نظامی*، تهران: امیرکبیر، ۱۳۹۵.

[۶]مکنزی، کنت، *جنگ ناهمتراز*، ترجمه عبدالمجید حیدری و محمد تمنائی، تهران: سپاه پاسداران انقلاب اسلامی، دانشکده فرماندهی و ستاد، دوره عالی جنگ، ۱۳۹۶.

[۷] مونکلر، هرفرید، *جنگ‌های نوین*، ترجمه حسین درگاهی، تهران: سپاه پاسداران انقلاب اسلامی، دانشکده فرماندهی و ستاد، دوره عالی جنگ، ۱۳۹۴.

[۸] دیوسالار، عبدالرسول؛ *راهبردها و معماری کلان فرماندهی و کنترل – جنگ اطلاعات (جلد ۲)*، تهران: موسسه آموزشی و تحقیقاتی صنایع دفاعی، زمستان ۱۳۹۵.

[۹] *جنگ نرم۱(ویژه جنگ رایانه‌ای)*، ضیایی پور، حمید؛ انتشارات مرکز مطالعات و تحقیقات بین المللی ابرار معاصر.

[۱۰]Alvin and Heidi Toffler, *The New intangibles*, In Athena's Camp: Preparing for Conflict in the information age. , RAND, 1999.

[۱۱] Francois L. J. Heisbourg, *Europe's Military Revolution*, , JFQ, Spring 2014.

[۱۲] Harlan Ullman, *Introduction to rapid dominance*, Shock & Ave (book), National Defense University, 2016.

[۱۳] James R. Blaker, *Understanding the revolution in Military Affairs: A Guide to America's 21st Centuary Defense*, Progressive Policy [14] Institute, January 2017.

[۱۴] Raymond C. Parks, David P. Duggan, *Principles of Cyber-Warfare, Proceeding of the 2018 IEEE*, Workshop on Information Assurance and Security.