تاریخ دریافت:۱۳۹۴/۰۴/۱۰
تاریخ پذیرش: ۱۳۹۴/۰۹/۱۳

فصلنامه علوم و فنون نظامی/
سال یازدهم/ شماره ۳۱، بهار ۱۳۹۴
صص ۱۳۵-۱۱۳

نقش الکترومغناطیس سایبری در کنترل میدان جنگ با ایجاد زیرساخت‌های نظامی سایبری

حسن عبدالهی[۱]
افسانه حق نگهدار[۲]

چکیده:

در عصر حاضر، توسعه فن‌آوری اطلاعات و ارتباطات به ویژه فن‌آوری‌های مرتبط با فضای سایبری، در حوزه غیرنظامی که دروازه آن اینترنت است، به عنوان یک سلاح در میدان نبرد مطرح می‌باشد و کاربرد آن در آینده نزدیک برای توفیق عملیات‌های نظامی امری انکارناپذیر خواهد بود. بنابراین روش‌های نوین جنگی با کنترل میدان نبرد توسط یکپارچه‌سازی و هماهنگ‌سازی فضای سایبر، نبرد الکترونیک و مدیریت طیف الکترومغناطیس با عنوان الکترومغناطیس سایبری انجام خواهد شد. سیر این تحول توسط ایجاد زیرساخت‌های نظامی مناسب و با بهره‌گیری از شبکه‌های ارتباطی غیرنظامی و همچنین استفاده از حداکثر ظرفیت طیف الکترومغناطیسی انجام خواهد شد. حائز اهمیت است که تهدیدات امنیتی آن نیز تغییر اساسی پیدا خواهد کرد. این مقاله، اقدامات الکترومغناطیسی سایبری را به نیروهای نظامی معرفی می‌کند، اطلاعات کاربردی مفیدی را به آنها می‌دهد و نحوه انجام عملیات نظامی با اتخاذ رویکرد آفندی و پدافندی در این حوزه را بیان می‌کند. از طرف دیگر بسترهای راهبردی به منظور بهره‌گیری از قابلیت‌های الکترومغناطیس سایبری در جهت انجام عملیات نظامی علیه دشمن را معرفی می‌نماید؛ تا آنها بتوانند برای دفاع از آرمان‌ها و اهداف نظامی و غیرنظامی کشور و برای جلوگیری از پیاده‌سازی و اجرای اهداف دشمنان با روش‌های نوین نبرد آشنا شوند. این مقاله اهمیت موضوع الکترومغناطیس سایبری را به فرماندهان و نیروهای نظامی جهت طرح‌ریزی محیط عملیات نوین و نحوه انجام عملیات یکپارچه با استفاده از مبانی اقدامات الکترومغناطیسی سایبری را نشان می‌دهد. همچنین این مقاله می-تواند مرجعی برای فرماندهان و نیروهای نظامی باشد تا توانائی قابلیت روش‌های ابتکاری برای تسخیر، حفظ و بهره‌برداری از برتری نظامی در تمام محیط عملیاتی تقویت شود.

کلیدواژه

الکترومغناطیس سایبری، جنگهای آینده، عملیات نظامی سایبری، نبرد الکترونیکی، فضای سایبری

---

۱ - استادیار برق- الکترونیک، دانشگاه هوایی شهید ستاری
* نویسنده مسئول h.abd@ssau.ac.ir
۲ - کارشناس‌ارشد برق - الکترونیک

مقدمه:

پیشرفت فن‌آوری اطلاعات و ارتباطات در عصر حاضر، سبک تعامل انسان‌ها با یکدیگر و با محیط اطرافشان را تغییر داده است و همچنین نحوه کار، شیوه زندگی روزمره و نگرش بشر را نیز تحت تأثیر خود قرار داده است که می‌توان به تأثیرات آن در طول مدت عملیات نظامی اشاره نمود.

در جهانی که در آن هر کسی می‌تواند دشمن باشد، یا یک دشمن می‌تواند در هر جایی باشد، عملکرد باید چگونه باشد و چطور باید فکر کرد. در چنین شرایطی، شبکه‌های اطلاعات دیجیتال در محیط عملیاتی باید دوباره تعریف شوند. از طرف دیگر، آیا تلاش ما یا دشمنان ما برای کنترل میدان نبرد به خطوط عملیاتی، مناطق عملیاتی یا حتی به مناطقی که در خط دید مستقیم است محدود می‌شوند؟ (Coonfield, 2013:1)

رایانه‌ها جنگ‌افزارهای جدید هستند که اهداف آنها حمله به شبکه‌های کنترل‌کننده سیستم‌های ارتباطی و زیرساخت‌های حیاتی است. حملات توسط هر کشور یا هر گروه می-تواند با انگیزه‌های سیاسی، اجتماعی و اقتصادی انجام شود. این بعد جدید، چیزی است که فضای سایبر نامیده می‌شود. فضای سایبر به عنوان مجموعه تعاملهای انسانها اطلاق می‌شود که از طریق رایانه و فن‌آوری‌های نوین ارتباطات، بدون در نظر گرفتن "مکان" و "زمان" انجام می‌شود. (خانیکی و بابائی، ۱۳۹۰: ۷۶)

این فضا یک آزادی عمل جدید برای عملیات‌های دشمن است و یک نگرانی جدید برای نحوه دفاع از نیروهای خودی است. برای بعضی‌ها، سایبر چیزی بیشتر از دسترسی به شبکه نیست، چیزی است که وجود دارد و زمانی که کار نمی‌کند اسباب ناراحتی است. برای بعضی‌ها، سایبر مهم‌ترین چیز برای عملیات‌شان است، زیرا دسترسی همزمان به تمام نقاط میدان نبرد و هدایت روند تغییرات محیط عملیاتی را امکان‌پذیر می‌سازد. سؤال این است که آیا سایبر از جنبه‌های مهم عملیات نظامی است؟ آیا بستگی به آن چیزی دارد که از سایبر برای عملیات استفاده می‌شود و همچنین بستگی به کسی دارد که از سایبر استفاده می‌کند؟

در فرهنگ اصطلاحات نظامی، فضای سایبری به عنوان یک حوزه جهانی در داخل محیط اطلاعات تعریف می‌شود که متشکل از شبکه به هم وابسته از زیرساخت‌های فناوری اطلاعات است: از قبیل اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های کامپیوتری و پردازنده‌های و کنترل‌کننده‌ها. در واقع محیط الکترونیکی که شامل دستگاه‌ها، شبکه‌ها و

سخت‌افزارهای ارتباط دهنده آن‌ها است 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.

در۲۰ سال گذشته، استفاده از قابلیتهای سایبر در مراکز مهم فرماندهی و کنترل و بخش پدافندی برای حفاظت بوده است و به توانائی آفندی سایبر توجه کمتری شده است. اخیرا رویکرد استفاده از سایبر به عنوان 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 به عنوان یک اسلحه نیز باید استفاده شود.

این مقاله، جزو اولین کارهای انجام شده در حوزه پژوهش بر روی اهمیت فضای سایبر و طیف الکترومغناطیس در نبردهای آینده است. این پژوهش که با عنوان اقدامات الکترومغناطیسی سایبری مطرح است، در حال حاضردر نشریات آموزش‌های ارتش، عملیات زمینی یکپارچه و مأموریت فرماندهی ارتش آمریکا مدون شده است (FM 3-38, 2014:1-96). لذا نیروهای مسلح نیز برای دفاع از شبکه‌های سایبری و طیف الکترومغناطیس خود و برای ایجاد اختلال در شبکه‌های سایبری و طیف الکترومغناطیس دشمن باید مهارت لازم را داشته باشند. از اینرو در آینده نزدیک الکترومغناطیس سایبر به عنوان یکی از عناصر قدرت نبرد باید در طرح ریزی عملیات‌های نظامی مطرح باشد.

این مقاله شامل پنج بخش است. بعد بِیان مقدمات در بخش اول، دربخش دوم، مبانی نظری CEMA تعریف و عملیات‌های فضای سایبری، نبرد سایبری و عملیات‌های مدیریت طیف توضیح داده می‌شود. بخش سوم، CEMA در یک محیط عملیاتی، دامنه فضای سایبری و خصوصیات دامنه فضای سایبر را بیان می‌کند. دربخش چهارم محیط اطلاعات، فعالیت‌های الکترومغناطیس سایبری به عنوان یک توانایی وابسته به اطلاعات بیان می‌شود. بخش پنجم، به فعالیت الکترومغناطیس سایبری در عملیات زمینی یکپارچه، ساخت، بهره-برداری و دفاع از شبکه، حمله و بهره‌برداری از سیستم‌های دشمن و مخاصمان و به حفاظت از افراد و سیستم عامل می‌پردازد. در پایان نیز نتیجه این تحقیق ذکر می‌گردد.

مبانی نظری:

فضای سایبر

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 (Pub3-13, 2014:35) که در آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود و کاربران آن می‌توانند از طریق رایانه‌ها با یکدیگر ارتباط بر قرار کنند. بر خلاف فضای واقعی که در آن از حواس پنج گانه طبیعی استفاده می‌شود در فضای سایبر از عناصری مثل فایل‌ها، پیغام‌های الکترونیکی، عکس‌ها، فیلم‌ها و ... استفاده می شود و نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیرد. در حال حاضر ارتش ایالات متحده به طور 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 هویت سازمانی استفاده‌کنندگان آن‌ها در درون وب از دیگر اشخاص ناشناس پنهان مانده است. (Coonfield, 2013:2) تهدیدکنندگان فضای سایبر، گروههای متعدد با انگیزه‌های متفاوت مانند سرقت، جاسوسی، خرابکاری، انتقام و سرگرمی می‌باشند که از آن میان می-توان به موارد زیر اشاره کرد: جاسوسها و دشمنان خارجی، تروریستها و گروههای افراطی، جنایتکاران و گروههای جنایی، هکرها و گروههای با انگیزه‌های تفننی، مخالفین داخلی و... (ملزومات امنیت در فضای سایبر ملی: ۲). بنابراین توانایی هدف قرار دادن هر چیز متصل به شبکه توسط یک گروه تقریباً ناشناس که دارای زیرساخت‌ها و توانایی‌های حلقه‌ای هستند، ترسناک است.

پس چرا سایبر برای برای نیروهای نظامی مهم است؟ امروزه محیط عملیاتی بسیار پیچیده و سناریوی آن بر اساس دو تهدید رودررو و فناوری موجود دشمنان است. سایبر، داده‌ها را به عنوان یک سلاح در میدان نبرد معرفی می‌کند، پالس‌های الکترونیکی از یک ماشین به

ماشین دیگر از طریق حوزه سایبر ارسال می‌شود. هنگامی که این داده‌ها در نقطه انتها بازیافت می‌شود، اطلاعات استخراج می‌گردد.

ارزش قابل اطمینان‌ترین داده‌ها، با توانایی جمع‌آوری قابل اعتمادترین اطلاعات مساوی است. بر این اساس استفاده از فضای مجازی در سازمان‌های نظامی، توانایی یگان‌ها برای رسیدن به بهترین درک از حوادث اتفاق افتاده در میدان نبرد را افزایش می‌دهد. در عوض، توانایی دست‌کاری همان اطلاعات می‌تواند منجر به تصمیم‌گیری غلط یا سبب دگرگونی عملیات نظامی شود. این مفهوم ارائه اطلاعات قابل‌اعتماد به فرماندهان نظامی، سنگ‌بنای عملیات شبکه‌های اخیر بوده است و منجر به پیشرفت‌های بسیاری در فناوری و سیاست-های کاربری شده است. با این حال، اخیراً حمله به شبکه‌ها افزایش یافته است. تنوع حملات سایبری، نه تنها زیرساخت‌های نظامی و غیرنظامی را هدف قرار داده، بلکه توانایی سایبری به عنوان یک سلاح با کاربرد نظامی پر رنگ شده است.

پس چه باید کرد؟ جنگ‌های سنتی(کلاسیک) در چهار حوزه مرسوم هوایی، زمینی، دریایی و فضایی در محیط طیف الکترومغناطیسی انجام می‌شود. پنجمین حوزه که ساخت دست بشر است، فضای سایبری است. گستردگی و سرعت تغییرات محیط‌های عملیاتی، ایجاب می‌نماید که ارتش‌های امروزی نیز در فضای سایبری کار کنند. طیف الکترومغناطیسی ابزار آن‌ها است که روزبه‌روز درخواست برای اشغال آن در حال افزایش است.

در ۶۰ سال گذشته وابستگی ارتش‌ها به سیستمهای دیجیتال برای افزایش بهره‌وری و پیشرفت توان رزمی زیاد شده است. مباحث ارزشمندی در عملیات دفاع سایبری وجود دارد، اما به جنبه ترکیب حمله سایبری با عملیات نظامی چندان توجه نشده است. اقدامات الکترومغناطیسی سایبری برای بخش نظامی سایبر تعریف شده است. پس سؤال این است که هدف آن در عملیات نظامی چیست؟ در واقع اقدامات الکترومغناطیس سایبری یک راهنما و دستورالعمل برای اجرای آن است. (Coonfield,2013:6)

الکترومغناطیس سایبری:

اقدامات الکترومغناطیس سایبری، فعالیت‌های موثری جهت تسخیر، حفظ و بهره‌برداری از یک برتری بیشتر در برابر مخاصمان و دشمنان در هر دو حوزه فضای سایبری و طیف الکترومغناطیسی هستند، بطوریکه استفاده مشابه و همزمان دشمن و مخالفان را کاهش می‌دهد و از مأموریت سیستم فرماندهی نیز محافظت می‌کند. این اقدامات شامل

عملیات‌های فضای سایبری[1]، نبرد الکترونیکی[2] و عملیات مدیریت طیف[3] است. (Coonfield ، ۲۰۱۳ : ۲۸) همانطورکه از شکل ۱ ملاحظه می‌شود CEMA در مرکز آنها است تا آرایش نیروهای نظامی برای دستیابی به افزایش نفوذ در فضای سایبری و استفاده از طیف الکترومغناطیسی و کنترل عملیات زمینی یکپارچه شکل گیرد. شکل ۱ حوزه فضای سایبر اقدامات الکترومغناطیس سایبری از طریق یکپارچه‌سازی و هماهنگ‌سازی عملیات فضای سایبری، نبرد الکترونیک و عملیات مدیریت طیف اجرا می‌شود. فرماندهی که با مشاوره متخصصین عملیات انجام می‌دهد باید توانائی هماهنگی و تلفیق عملیات فضای سایبر، نبرد الکترونیک، عملیات مدیریت طیف و ارتباط دهی آنها را داشته باشد تا به نتیجه مورد دلخواه در پشتیبانی از عملیات زمینی یکپارچه دست یابد.

انجام CEMA در نیروهای مسلح باید بصورت یکپارچه باشد. در ارتش یکپارچگی[4] به معنای آرایش نیروهای نظامی است و اقداماتشان برای ایجاد نیرویی است که با درگیر شدن عمل کنند. از طرف دیگر، همزمانی[5] به معنای آرایش اقدامات نظامی در زمان، مکان و هدف مشخص جهت ایجاد حداکثر توان رزمی در یک زمان و مکان معین است. اقدامات

---

1 Cyber Operations (CO)
2 Electronic Warfare (EW)
3 Spectrum Management Operations (SMO)
4- Integrating
5- Synchronization

الکترومغناطیس سایبری عملکرد و توانمندی CO، EW و SMO را برای انجام اقدامات تکمیلی و تقویتی، تلفیق و هماهنگ می‌کند. انجام این اقدامات به طور مستقل ممکن است از کارآمدی آنها بکاهد. اگر این فعالیتها ناهماهنگ باشند، ممکن است منجر به تعارض و تداخل متقابل بین آنها و یا با دیگر نهادهای استفاده کننده از طیف الکترومغناطیسی شود. CO، EW و SMO جهت پشتیبانی از کل عملیات همزمان می‌شوند تا باعث ایجاد اثر مشخصی در نقاط معین شوند.

واحد CEMA مسئول برنامه‌ریزی، تلفیق و هماهنگ‌کننده CO، EW و SMO جهت پشتیبانی از مأموریت فرمانده و وضعیت مورد نظر در داخل فضای سایبر و طیف الکترومغناطیس[1] است. در حین زمان اجرا، واحد CEMA مسئول همزمان‌سازی CEMA به بهترین نحو جهت اجرای مأموریت است.

عملیات‌های فضای سایبری، EW و SMO برای انجام عملیات‌های زمینی یکپارچه ضروری هستند. وقتی‌که این اقدامات درکاربرد و تاکتیکشان متفاوت شدند، عملکردها و توانمندیهای آنها باید هماهنگ و یکپارچه شوند تا پشتیبانی خود از عملیات زمینی یکپارچه را به حداکثر رسانند. تلفیق این اقدامات نیاز به درک درستی از عملکردها و توانمندی‌های بکار برده شده در آنها دارد.

عملیات‌های فضای سایبری:

عملیات‌های فضای سایبری، استفاده از امکانات فضای سایبری است که هدف اصلی آن دستیابی به اهدافی است که در راستای فضای سایبری است. عملیات‌های فضای سایبری شامل سه بخش است: عملیات‌های فضای سایبری تهاجمی[2]، عملیات‌های فضای سایبری دفاعی[3] و عملیات شبکه اطلاعات وزارت دفاع[4](Bender، ۲۰۱۳ : ۴)

عملیات‌های فضای سایبری تهاجمی : حمله سایبری به مجموعه اعمالی گویند که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه‌های موجود در فضای سایبری انجام می‌شود. استفاده تهاجمی از سلاح‌های اینترنتی برای آسیب رساندن به اهداف تعیین شده است. حملات شبکه‌های کامپیوتری، اختلال، انکار، کاهش و یا از بین

1 - Electromagnetic Spectrum (EMS)
2 - Offensive CyberspaceOperations (OCO)
3 - Defensive CyberspaceOperations (DCO)
4- Department of Defense Information Network Operations (DODIN)

بردن اطلاعات مقیم در یک کامپیوتر و یا شبکه کامپیوتری نوعی از حملات سایبری هستند.(حسینی، ۱۳۹۲ : ۴۷)

عملیات‌های فضای سایبری دفاعی: به‌کارگیری توانائی دفاعی سایبری خاص برای منحرف کردن و یا تغییر مسیر حملات سایبری را دفاع سایبری گویند. به عبارت دیگر، اقداماتی که توسط یک کشور به صورت "فعال" یا "غیرفعال" به عنوان بخشی از یک استراتژی دفاعی در طی یک حمله و یا بعد از آنکه بر ضد منافع کشوری صورت گرفته باشد، گویند. در مدل فعال، اقدام متقابل می تواند با تلاش برای مختل کردن مهاجم به حمله او واکنش نشان دهد. اما در مدل غیر فعال، می تواند توانائی حفاظت از منافع خود را در برابر حمله بالا ببرد. (دستجردی، ۱۳۹۳ : ۱۵۰)

عملیات‌های شبکه اطلاعات وزارت دفاع: این عملیات‌ها برای طراحی، ساخت، پیکربندی، امنیت، نگه‌داری و حفظ شبکه‌های وزارت دفاع برای ایجاد و حفظ صحت اطلاعات در شبکه‌های اطلاعاتی وزارت دفاع هستند. شبکه‌های اطلاعاتی وزارت دفاع در سطح جهانی به هم پیوسته و دارای مجموعه‌ای از قابلیت‌های تبادل اطلاعات در پایانه‌ها هستند و همچنین دارای فرآیندهای منسجمی برای جمع آوری، پردازش، ذخیره سازی، انتشار و مدیریت اطلاعات بر اساس تقاضای نظامیان، سیاست گذاران و پرسنل پشتیبانی کننده هستند. (FM 3-38 ، ۲۰۱۴ : ۳۵)

نبرد الکترونیک[1]:

هرگونه اقدام نظامی مربوط به الکترومغناطیس و یا انرژی هدایت شده برای کنترل طیف الکترومغناطیسی یا حمله به دشمن را نبرد الکترونیک گویند. نبرد الکترونیک شامل سه زیر مجموعه است: حمله الکترونیکی، دفاع الکترونیکی و پشتیبانی نبرد الکترونیک (FM 3-36، ۲۰۱۲ : ۴).

عملیات‌های مدیریت طیف:

عملیات‌های مدیریت طیف فعالیتهای به هم وابسته‌ای از مدیریت طیف، تعیین فرکانس و هماهنگی در داخل و خارج کشور است و همچنین خط مشی است که برنامه‌ریزی، مدیریت و اجرای عملیات‌ها را در داخل محیط عملیاتی الکترومغناطیسی در طول مدت انجام تمام مراحل عملیات‌های نظامی امکان‌پذیر می‌سازد (FM 6-02.70، ۲۰۱۰ : ۷).

[1] Electronic Warfare(EW)

اقدامات الکترومغناطیس سایبری در یک محیط عملیاتی

یک محیط عملیاتی ترکیبی از شرایط، موقعیت و توانایی‌هایی است که بر نحوه استفاده از امکانات اثر می‌گذارد و به تصمیمات فرمانده مرتبط است. آنالیز از یک محیط عملیاتی باید شامل پنج حوزه و EMS باشد. به طور طبیعی چهار حوزه مرسوم (هوایی، زمینی، دریایی و فضایی) و طیف الکترومغناطیس وجود دارد. پنجمین حوزه که ساخت دست بشر است، فضای سایبری است.

فضای سایبری و طیف الکترومغناطیس توانایی تقسیم اطلاعات، برقراری ارتباط، یکپارچگی و همزمانی عملیات‌ها را در کل رده‌ها و مأموریت‌های جنگی برای فرمانده ایجاد می‌کند. اما فضای سایبری و طیف الکترومغناطیس یک قابلیت مفید، ارزان و ناشناس برای مخالفان و دشمنان نیز است بطوریکه شرایط را برای به خدمت گرفتن فعالیت‌های اطلاعاتی، آموزشی، فرماندهی و کنترل آماده می‌کنند. CEMA فرمانده‌هانی را تربیت می‌کند که توانائی بدست آوردن و حفظ یک مزیت و برتری در فضای سایبر و طیف الکترومغناطیس را داشته باشند (Lyons ، ۲۰۱۳ : ۱۰).

دامنه فضای سایبری

حوزه فضای سایبری جهانی است و در داخل یک محیط اطلاعات قرار دارد که شامل شبکه به هم وابسته‌ای از زیرساخت‌های فن‌آوری اطلاعات و داده‌های مقیم است، از قبیل اینترنت، شبکه‌های ارتباطات راه دور، سیستم‌های کامپیوتری، پردازنده‌های تعبیه شده و کنترل‌کننده‌ها. عملیات در فضای سایبری کمکی برای رسیدن به یک برتری مهم عملیاتی جهت پیشبرد اهداف نظامی است.

بصورت طبیعی فضای سایبری در داخل تمام تجهیزات و سیستم‌ها در چهار حوزه وجود دارد. به عنوان مثال، سرورهای شبکه ممکن است در یک مجموعه داده-زمینی یا در داخل کشتی‌های جنگی در دریا مسقر شوند. عملیات در فضای سایبری وابسته به لینک‌ها و گره-هایی است که در حوزه‌های طبیعی وجود دارد. بنابراین عملیات‌ها در فضای سایبری، آزادی عمل برای انجام عملیات در چهار حوزه طبیعی و طیف الکترومغناطیس را ممکن می‌سازد.با تأثیر طیف الکترومغناطیس ، دیتا یا زیرساخت فیزیکی، عملیات‌ها در حوزه‌های دیگر از طریق فضای سایبری ایجاد می‌شود.

امروزه، عموماً فضای سایبری و حوزه‌های فضایی وابستگی زیادی به هم دارند زیرا آنها در ارتباطات راه دور و شبکه‌ها نقش دارند. عملیات در حوزه فضا به فضای سایبر و طیف الکترومغناطیس جهت پشتیبانی از عملیات فضا وابسته است. یک فضای سایبری با دسترسی جهانی توسط قابلیت‌های فضایی ایجاد می‌شود. توجه به این روابط متقابل در هنگام برنامه‌ریزی برای CEMA مهم است.

خصوصیات دامنه فضای سایبر

فضای سایبری دارای ویژگی‌هایی است که با حوزه‌های زمینی، هوایی، دریایی و فضایی تفاوت‌های زیادی دارد. فضای سایبری سیستمی از سیستم‌ها است که در آن تعداد زیادی از سیستم‌های کوچک و متنوع وجود دارد که ساختاری مشابه سیستم اصلی را تشکیل می-دهند. این سیستم‌ها در هر یک از چهار حوزه طبیعی وجود دارند. روند تغییرات در فضای سایبری اغلب بوسیله توسعه و پژوهش صنعت خصوصی جلو برده می‌شود. پویایی و پیوستگی فضای سایبر سبب می‌شود که قابلیت‌های فن‌آوری اطلاعات همیشه در حال گسترش و تکامل باشد. از آنجا که فضای سایبری به دست بشر ساخته شده است، تنها از طریق نگهداری و تعمیر دائمی سیستمها است که بقای فضای سایبری ادامه می‌یابد.

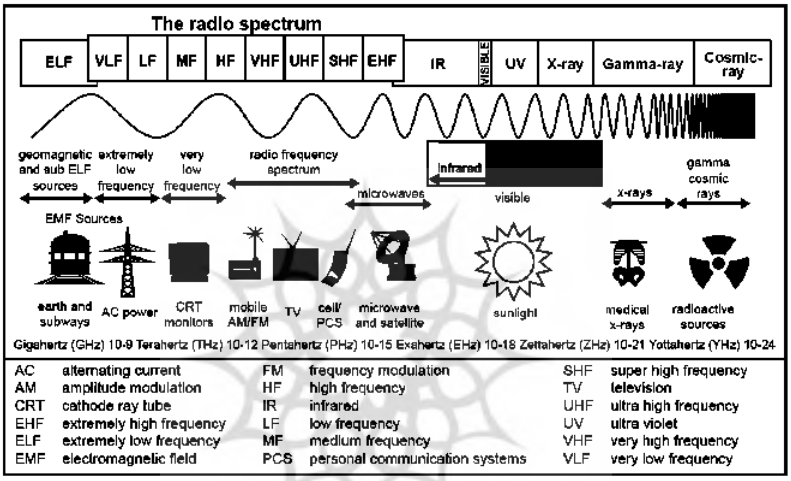
فضای سایبری به این حقیقت تأکید دارد که محدوده عملیاتی به یک مکان فیزیکی محدود نمی‌شود. میدان‌های نبرد سنتی به فضای فیزیکی محدود می‌شود و واکنش به آنچه در میدان جنگ سنتی(کلاسیک) اتفاق می‌افتد، می‌تواند منشأ اثرات اجتماعی و سیاسی در سراسر جهان شود، بنابراین برخورد فیزیکی واقعی، محدود به میدان جنگ فیزیکی است. اما گنجایش و ظرفیت فضای سایبری و طیف الکترومغناطیس تا حد زیادی گسترده است و محدوده عملیات آن نیز پیچیده است، بنابراین محدود عملیات میدان جنگ فیزیکی به یک میدان جنگ جهانی تبدیل می‌شود. به عنوان مثال، یک ویروس اجرا شده در فضای سایبری قادر است علاوه بر ضربه زدن به هدف تعیین شده‌اش، بطور غیر مشخص به سیستم‌های موجود در دیگر کشورها از جمله خود کشور حمله کننده نیز ضربه بزند. خسارت‌های ناخواسته از این نوع حملات معمولاً قابل پیش‌بینی نیست.

فضای سایبری یک محیط ایجاد شده و محافظت شده است تا استفاده و بهره‌برداری از اطلاعات، تعاملات بشر و ارتباطات آنها آسان شود. ارتباط این حوزه با طیف الکترومغناطیس بواسطه سیستم‌های ارتباطات راه دور است. این سیستم‌ها از طیف الکترومغناطیس استفاده می‌کنند و با شبکه‌های سراسری برای ایجاد فضای سایبری همگرا می‌شوند. بطور کلی

اقدامات مؤثر فضای سایبری به زیرساخت‌های فیزیکی، شبکه‌های دیتا و طیف الکترومغناطیس وابسته است.

طیف الکترومغناطیسی

طیف الکترومغناطیسی، طیف وسیعی از فرکانس‌های تشعشعات الکترومغناطیسی از صفر تا بی‌نهایت است که به ۱۶ باند بر اساس حروف الفبای معین شده تقسیم شده است که در شکل ۲ این طیف نشان داده شده است(FM 3-38 ، ۲۰۱۴ : ۱۴).



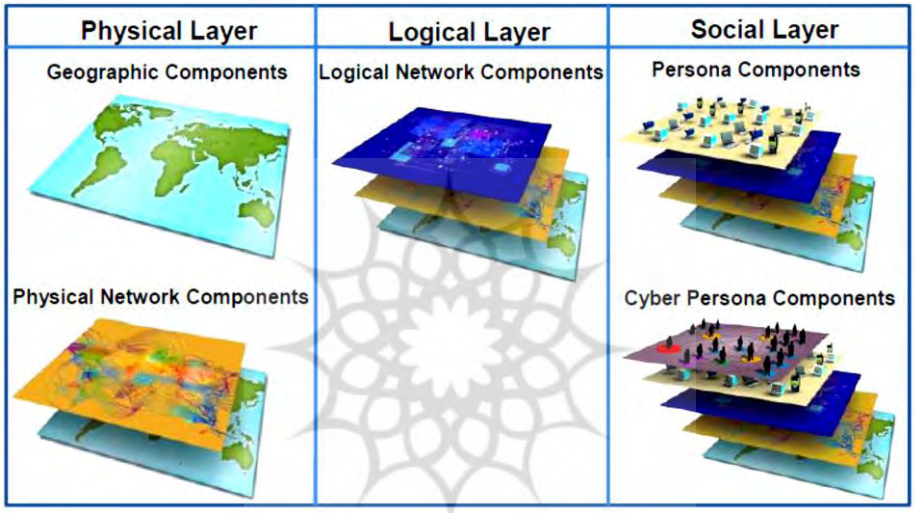
شکل ۲ طیف الکترومغناطیس

همان‌طور که این شکل نشان می‌دهد، دستگاهها و سیستم‌ها در بازه‌های مختلف فرکانسی کار می‌کند. لذا پویایی فضای سایبر به تعداد سیستمهای است که در طیف الکترومغناطیس کار می‌کند. بنابراین افزایش استفاده از سیستم‌های بی‌سیم باعث شده است که طیف الکترومغناطیس موجود، یک منبع با تقاضای بالا شود. بنابراین در محیط الکترومغناطیسی که ازدیاد فعالیت همراه با فشردگی و رقابت زیاد است، دسترسی راحت به طیف الکترومغناطیس مشکل است.

یافته‌های تحقیق بر روی اقدامات الکترومغناطیس سایبری

فضای سایبری و طیف الکترومغناطیس بخشی از محیط اطلاعات هستند. محیط اطلاعات شامل مجموعی از اشخاص، سازمان‌ها و سیستم‌هایی است که به جمع‌آوری، پردازش، ارسال یا انجام کاری بر روی اطلاعات می‌پردازد. ابعاد سه گانه محیط اطلاعات (فیزیکی،

اطلاعاتی و شناختی) برای اجرای CEMA استفاده می‌شود. اقدامات الکترومغناطیس سایبری در بعدهای فیزیکی و اطلاعاتی اجرا می‌شود و اهداف را در بعد شناختی پشتیبانی می‌کند. طیف الکترومغناطیس در بعد فیزیکی محیط اطلاعات قرار دارد. سه لایه از فضای سایبری (فیزیکی، منطقی و ماهیت مجازی) در ابعاد فیزیکی و اطلاعاتی محیط اطلاعات قرار دارند که در شکل ۳ این لایه ها نشان داده شده است (TRADOC PAM 525-7-8، ۲۰۱۰: ۸).



شکل ۳ لایه‌های فضای سایبر

بعد فیزیکی، ترکیبی از عناصر قابل لمس مانند شبکه‌های ارتباطات راه دور، زیرساخت‌ها و سیستم‌های اطلاعاتی، ماهواره‌ها، سیستمهای فرستنده، محل‌های ملاقات، نشریات چاپ شده، تابلوهای تبلیغاتی، آگهی‌ها، مجسمه‌ها، اشیاء نمادین، سازمان‌ها، گروه‌ها و اشخاص تشکیل شده است. در واقع، ابزار و روش‌های مورد استفاده برای فعال نمودن جریان اطلاعات در میان تولید کنندگان، کاربران، مخاطبان و سیستم‌ها عناصر ملموس است. بعد فیزیکی شامل عناصری مانند مسیرهای انتقال از طریق طیف الکترومغناطیس نیز است. اجزا یا لایه فیزیکی فضای سایبری مستقر در زمین، هوا، دریا یا فضا در بعد فیزیکی است و ساده‌ترین راه برای اندازه‌گیری هستند.

بعد اطلاعاتی شامل خود اطلاعات است، خواه آن در حال استراحت یا خواه در حال حرکت باشد. بعد اطلاعاتی اشاره به محتوی و جریان اطلاعات دارد از قبیل متن و یا تصاویر، یا

داده‌ای که کارکنان می‌توانند جمع‌آوری، پردازش، ذخیره، ارسال و نمایش دهند. بعد اطلاعاتی، توسط جابجائی داده‌های کامپیوتر از طریق فضای سایبر و ارسال الکترومغناطیسی از طریق طیف الکترومغناطیس برای اجرای CEMA بیان می‌شود. در این بعد لایه‌های هویتی و منطقی فضای سایبری قرار دارد. بعد اطلاعاتی، پیوند لازم بین بعد فیزیکی و بعد شناختی را ایجاد می‌کند.

بعد شناختی از ترکیب دانش، ارزش‌ها، باورها، مفاهیم، اهداف و ادراک اشخاص و گروه‌های ارسال و دریافت کننده اطلاعات تشکیل شده است. این بعد تمرکز بر زمینه‌های اجتماعی، فرهنگی، مذهبی و تاریخی دارد و درک آنهایی که اطلاعات را تولید می‌کنند و مخاطبانی که دریافت کننده اطلاعات هستند را تحت تأثیر قرار می‌دهد. دولت‌ها، جوامع، نیروهای نظامی، نیروهای دشمن و دیگر نقش‌آفرینان، همگی در این بعد، فکر، مشاهده، تجسم، درک و تصمیم‌گیری می‌کنند. این نقش‌آفرینان، سازندگان و کاربران اطلاعاتی هستند که از طریق بعد فیزیکی جابجا می‌شوند.

اقدامات الکترومغناطیس سایبری به عنوان یک توانایی وابسته به اطلاعات

توانایی‌های وابسته به اطلاعات شامل توانایی‌ها، تکنیک‌ها یا قابلیتهای بکارگیری از اطلاعات است که برروی هر سه بعد محیط اطلاعات تأثیر می‌گذارد تا منجر به یک نتیجه شود. این توانمندی‌ها شامل عملیات‌های امور عمومی، عملیات‌های پشتیبانی اطلاعات نظامی، دوربین‌های رزمی، تعامل فرمانده و سرباز، عملیات‌های امور مدنی، ملاحظات فرهنگی و مدنی، امنیت عملیات‌ها، فریب نظامی و CEMA می‌شود اما تنها محدود به این موارد نمی‌شود.

CEMAاز طریق فعالیت‌های نفوذی و اطلاع‌رسانی[1] با اثرگذاری بر محیط اطلاعات قدرتمند می‌شود. CEMA یک توانمندی وابسته به اطلاعات محسوب می‌شود که باید با دیگر توانمندی‌های وابسته به اطلاعات یکپارچه و هماهنگ شود. فعالیت‌های نفوذی و اطلاع رسانی تلفیقی از طراحی اقدامات وابسته به اطلاعات است؛ بطوریکه مطالب، پیام‌ها و اقدامات را با عملیات همزمان می‌کند و به کشورها، مخاطبان جهانی و شنوندگان خارجی که تاثیرگذار بر تصمیمات دشمنان و حریفان هستند، اطلاع رسانی می‌نماید. این فعالیت‌ها

[1] Inform and influence activities (IIA)

از طریق محیط اطلاعات انجام می‌شود. محیط اطلاعات می‌تواند تأثیر غیر مستقیم بر محیط عملیاتی داشته باشد و می‌تواند روی عملیات‌های نظامی و نتیجه آن تأثیر گذار باشد. اطلاع رسانی و CEMA هر دو به هم مربوطند، اما تمرکز IIA برروی محیط اطلاعات بطور همه جانبه است. هر دو IIA و CEMA یکپارچه هستند و از توابعی که مؤثر بر ادراک و تصمیمات هستند حمایت می‌کنند. به عنوان مثال، CEMA می‌تواند تلاش‌های پیام رسان را برای توزیع پیام با تأمین امکانات اضافی تقویت کند. علاوه بر این، قابلیت‌های تهاجمی و تدافعی مرتبط با CEMA وجود دارد که می‌تواند به تقویت دیگر اهداف وابسته به اطلاعات مانند حفاظت از اطلاعات خودی کمک کند.

هر دو CEMA و IIA نیاز به مهارت مختلف و منحصر به فرد مجموعه دارند تا فرآیندهای برنامه‌ریزی مورد نیاز را بطور مؤثر اجرا کنند. در حقیقت هر دو اقدامات یکپارچه شده‌اند. برنامه‌ریزی مؤثر، نیاز به یک درک کلی از توانایی‌های به خدمت گرفته شده و مشاوره با کارشناس مربوط به موضوع دارد. برنامه‌ریزی CEMA می‌تواند مستقل از IIA باشد. با این حال، در صورت امکان، CEMA و IIA برای دستیابی به اثرات همزمان و مکمل باید برنامه ریزی شود. (FM3-13: 2013 ،p24-30 **Error! Reference source not found.**)

فعالیت الکترومغناطیس سایبری در عملیات زمین یکپارچه

توانایی بدست آوردن و حفظ یک مزیت در فضای مجازی و طیف الکترومغناطیس مستلزم آن است که نیروهای نظامی از توانمندی‌های CEMA برای انجام موارد زیر استفاده کنند. (ADP3-0, 2011:8)

- ساخت، راه‌اندازی و دفاع از شبکه
- حمله و بهره‌برداری از سیستم‌های دشمن و حریف
- بدست آوردن شناخت موقعیتی از طریق CEMA
- حفاظت از افراد و سیستم‌عامل

ساخت، راه‌اندازی و دفاع از شبکه

عملیات زمین یکپارچه بطور چشم‌گیری به توانایی شبکه[1] جهت جمع‌آوری، پردازش، ذخیره‌سازی و انتشار اطلاعات وابسته است. توانمندی شبکه بوسیله شبکه جنگ زمینی[2]

1. Net-enabled
2. LandWarNet (LWN)

پشتیبانی می‌شود. در آمریکا، LWN بخش ارتشی سازمان شبکه‌های اطلاعات دفاعی[1] است. شبکه جنگ زمینی یک شبکه فنی است که شامل تمام سیستم‌های مدیریت اطلاعات ارتش و سیستم‌های اطلاعاتی است که جمع‌آوری، پردازش، ذخیره، نمایش، انتشار و محافظت از اطلاعات در سراسر جهان را انجام می‌دهد. در ارتش آمریکا، LWN شامل تمام زیرساختهای شبکه‌های خود ارتش و شبکه‌های اجاره‌ای ارتش است که طبق شکل ۴ از پایین به بالا به ترتیب از ۵ لایه سنسورها و نحوه قرار گیری آنها، کاربردها، سرویس‌ها، زیرساختهای انتقال داده و استاندارد تشکیل شده است. بنابراین LWN یک شبکه ساده نیست (C/EM CBA,2010:26) این شبکه، اطلاعات مورد نیاز فرماندهان در هر محیط و در هر زمان را جهت تسهیل در اقدامات اساسی تأمین می‌کند. زیرساخت شبکه توسط CEMA ایجاد می‌شود. پس از تأسیس آن، شبکه باید به گونه‌ای راه‌اندازی شود که اجازه - دهد تا آن شکل بگیرد و پویایی رسالت مأموریت حفظ شود. این امکان از طریق مدیریت تنظیمات شبکه، اجرا، تخصیص منابع، عیوب و امنیت همسو شده با نیت و اولویت‌ها فرمانده در کل بازه عملیات نظامی بدست می‌آید.

با توجه به افزایش وابستگی به توانمندی‌های شبکه، عملیات زمین یکپارچه به فضای سایبری و تهدیدات EW بسیار حساس هستند. زیرا می‌تواند محرمانگی و یکپارچگی مأموریت سیستم فرماندهی و اطلاعات را به خطر اندازد، عملیات تهاجمی دشمن در فضای سایبری و طیف الکترومغناطیس می‌تواند بر تمام عملیات‌های خودی تأثیر گذارد. توانایی دشمن برای دستیابی به فضای سایبری نظامی می‌تواند منجر به دستکاری اطلاعات در سیستم‌های نظامی شود. این تغییر می‌تواند اقدامات بعدی مورد نظر را تحت تأثیر قرار دهد (به عنوان مثال، به تأخیر انداختن یک حمله) و منجر به کاهش اعتماد در سیستم‌های خودی شود. کاهش اعتماد، منجر به کاهش درک موقعیت از محیط اطلاعات نظامی می- شود.

عملیات ذاتی شبکه، اقداماتی برای دفاع از آن بوسیله نظارت، آشکارسازی، تجزیه و تحلیل و واکنش به فعالیت‌های غیرعادی شبکه هستند. دفاع از شبکه بوسیله درک بهتر از محیط عملیاتی، از طریق کشف و اصلاح تهدیدات و آسیب‌پذیری‌های مربوط به سایبر فراهم می- شود. دریافت نشانه‌ها و هشدارها می‌تواند منجر به تشخیص حمله شود. بخشی از نیازهای

1. Department of Defense Information Networks (DODIN)

فرماندهان فضای سایبری توسط یکپارچگی ساختار شبکه، راه‌اندازی و عملیات‌های دفاعی (بعنوان عملیات شبکه جنگ زمینی شناخته می‌شود) فراهم می‌شود تا از دسترس بودن سیستم و شبکه، تحویل اطلاعات و حفاظت اطلاعات مطمئن شوند(Chris, 2011)

حمله و بهره‌برداری از سیستم‌های دشمن و مخاصمان

حمله به دشمن و سیستم‌ها و شبکه‌های حریف می‌تواند آزادی عمل آنها را در فضای سایبری و طیف الکترومغناطیس را مختل و کاهش دهد. CEMA به فرماندهی توانائی می-دهد تا بتواند در سراسر زنجیره ایجاد فریب، تنزل، اختلال، انکار، نابودی یا دستکاری کند و CEMA می‌تواند از سیستم‌های دشمن و حریف برای تسهیل در جمع‌آوری اطلاعات بهره-برداری کند. این توانمندی‌ها ممکن است برای هدف قرار دادن دشمن و فضای سایبری دشمن مورد استفاده قرار گیرد. ایجاد اثرات اولیه در فضای سایبری توسط EW و ایجاد اثرات پی در پی در حوزه‌های طبیعی توسط طیف الکترومغناطیس انجام می‌شود تا سیستم‌های سلاح، فرآیندهای فرماندهی و کنترل و زیرساخت‌های حیاتی و منابع کلیدی را تحت تأثیر قرار دهند.

CEMA مرگ ناشی از سلاح‌های کلاسیک را افزایش می‌دهد. مثال‌ها عبارتند از: استفاده از لینک‌های داده و شبکه‌های مبتنی بر سیستم‌های هدف‌دار، هدف قرار دادن و هدایت نهایی از طریق سیستمهای لیزری، سیستم‌های تعیین موقعیت جهانی و سلاح‌های جستجوگر

درک فرمانده از وضعیت محیط عملیات توسط CEM

فرماندهان و کارکنان نظامی داده‌ها را برای افزایش درک‌شان پردازش می‌کنند. در پایین-ترین سطح، فرآیند تبدیل داده‌ها به اطلاعات است. سپس تجزیه و تحلیل اطلاعات به دانش تبدیل می‌شود. پس از آن فرماندهان و کارکنان نظرشان را برای تبدیل دانش به درک از وضعیت محیط عملیات اعمال می‌کنند. اقدامات الکترومغناطیس سایبری قابلیت‌هایی را ایجاد می‌کند که درک وضعیت از یک محیط عملیات تا حد زیادی افزایش یابد. این قابلیت‌ها باعث می‌شوند که شبکه‌ها، سیستم‌های اطلاعاتی و تجهیزات مجهز شوند همچنین CEMA وسیله‌ای برای برقراری ارتباط است تا درک فرمانده از وضعیت یک محیط آسان شود. فضای سایبر و طیف الکترومغناطیس باید بوسیله نیروهای نظامی تقویت شود تا ارتباط از طریق صدا (Liang,2001:pp1-10)، داده‌ها، چت، ویدئو، تله کنفرانس، پست الکترونیکی و ... برقرار شود. به عنوان مثال در ایالات متحده از فضای سایبری و طیف الکترومغناطیس برای فراهم نمودن اطلاعات بلادرنگ از طریق سنسورهای نوری،

الکترونوری، حرارتی، موج میلی متری، یا چند طیفی برای فرماندهان و سربازان استفاده می‌شود. موقعیت‌یاب جهانی سیار نمونه‌ای از سیستم‌هایی است که از فضای سایبری و طیف الکترومغناطیس استفاده می‌کند تا بتواند سیستم‌هایی را فعال نماید که فرماندهان از مکان سربازان در میدان جنگ آگاه شوند. بنابراین CEMA باعث افزایش بقاء نیروهای نظامی می‌شود. نمونه‌هایی از علل افزایش بقا در جنگ الکترونیک شامل هزینه‌های است که برای فلرها، اقدامات ضد الکترونیکی در مقابل دستگاه‌های انفجار کنترل شونده رادیویی و جمینگ برای غیرفعال کردن تجهیزات یا قابلیت‌های دشمن انجام می‌شود. افزایش بقا SMO از طریق کاهش تداخل الکترومغناطیسی در سیستم‌های خودی است که در جنگ الکترونیک استفاده می‌شود. CO از طریق انتقال امن و بدون وقفه داده‌ها و اطلاعات نیز سبب افزایش بقا می‌شود زیرا قدرت مبارزه نیرویهای نظامی افزایش می‌یابد.

نقش اقدامات الکترومغناطیسی سایبری در جنگهای آینده

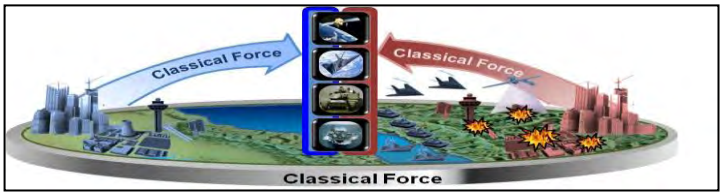
شکل ۴ روند تکاملی جنگها از گذشته تا حال و آینده را نشان می‌دهد. همانطور که در شکل نشان داده شده است این جنگها به ترتیب از پایین به بالا شامل جنگهای سنتی یا کلاسیک، جنگهای کلاسیک-شبکه محور و جنگهای کلاسیک با اقدامات الکترومغناطیس سایبری است.

الف) این شکل، نحوه جنگهای گذشته در ۳ حوزه زمینی، هوائی و دریایی با پشتیبانی وزارت دفاع را نشان می‌دهد. در این جنگها، برتری با نیروی است که از قدرت هوائی بیشتری برخوردار است. بنابراین کشورها جهت حفظ برتری خود تلاش می‌کردند تا فضای بیشتری از آسمان را اشغال کنند تا تعیین کننده برنده نهائی جنگ شوند. به عنوان مثال می‌توان به جنگ ایران و عراق اشاره نمود که کشور عزیرمان به علت برتری هوائی بیشتر به خصوص در اوایل جنگ از قدرت بیشتری نسبت به دشمن مخاصم برخوردار بود.

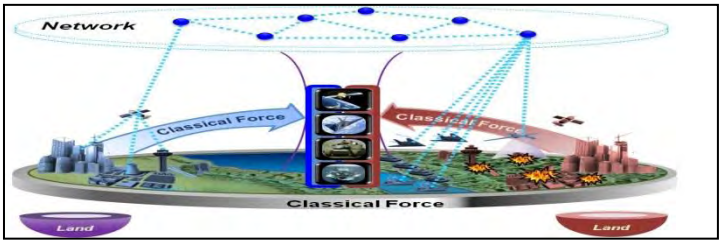
ب) شیوه جنگهای امروزی را نشان می‌دهد که پیشرفت فناوری‌های جدید به خصوص شبکه‌های ماهواره‌ای و ارتباط اطلاعات فضایی به جنگهای کلاسیک اضافه شده است. از اینرو جنگ‌های امروزی در ۳ حوزه یاده شده در جنگ‌های سنتی و با پشتیبانی توسط وزارت دفاع در قالب یک شبکه یکپارچه صورت می‌پذیرد. در این نوع از جنگها برتری با نیروی است که فضای بیشتری را اشغال کرده است. لذا تمام کشورها تلاش می‌نمایند تا با

ارسال ماهواره به فضا، از فضای بیشتری برخوردار شود تا قدرت ارتباط فضایی آن بیشتر شود. به عناون مثال می‌توان به جنگ عراق و آمریکا اشاره نمود، که هدایت صحنه نبرد این جنگ با تبادل اطلاعات در یک شبکه یکپارچه نظامی بین نیروهای زمینی، هوائی، دریایی با پشتیبانی وزارت دفاع از طریق مرکز فرماندهی و کنترل مرکزی انجام می‌شد.

در قسمت پ شکل ۵ نحوه نبردهای آینده را نشان می‌دهد. در جنگهای آینده که به زودی با آن مواجه خواهیم بود، نبردها با اقدامات الکترومغناطیس سایبری است. در جنگ‌های آینده، علاوه بر جنگ‌های کلاسیک شبکه محور از حوزه پنجم استفاده خواهد شد که استفاده از امکانات شبکه‌های ارتباطی غیر نظامی یا همان فضای سایبر است که بدست افراد غیر نظامی در حال گسترش و توسعه است و دروازه ورود به آن اینترنت است. در جنگها آتی بین نیروهای سایبر و نیروهای رزمی باید همگرائی وجود داشته باشد. بنابراین یک عملیات نظامی موفق به یکپارچگی و موفقیت فضای سایبری نیاز خواهد داشت. در جنگهای سنتی و امروزی، درگیری نیروها مستقیم و به‌صورت رودرو است. در فاز اول جنگ‌های آینده، درگیری‌ها به صورت مستقیم و رودرو نخواهد بود بلکه نبردها در حوزه پنجم و در فضای سایبر اتفاق خواهد افتاد؛ پس از آن شاهد جنگ‌های رودرو خواهیم بود. لذا درگیری در دو فاز نبرد و جنگ اتفاق خواهد افتاد. در درگیریهای آتی، برتری با نیروی است که توانائی مدیریت صحنه نبرد در هر دو فاز را دارد. در این حوزه با بهره‌گیری از فضای مجازی غیر نظامی امکان دسترسی به تمام نقاط صحنه نبرد و غیر نبرد امکان پذیر خواهد بود. لذا در این شیوه برتری با نیرویی است که قدرت نبرد در فضای سایبر را نیز داشته باشد. یک فرمانده علاوه بر آشنائی با جنگهای کلاسیک باید از نبردهای سایبری نیز شناخت کامل داشته باشد.



الف) جنگهای گذشته



ب) جنگهای امروزی

پ) جنگهای آینده

شکل ۴ شکل تغییر شکل محیطهای عملیاتی جنگها از گذشته تا آینده الف) شیوه جنگها در گذشته (کلاسیک-جنگهای هواپایه ب) شیوه جنگهای امروزی (کلاسیک-شبکه محور) پ) شیوه جنگها در آینده (سرزمین سایبر)

از آنجا که در دنیای کنونی، اینترنت دروازه فضای سایبر است و نحوه استفاده از آن نیز در سال‌های اخیر به عنوان ابزاری برای دستیابی به اهداف ملی تغییر کرده است، لذا نه تنها فضای مجازی توسط فرماندهان نظامی باید دیده شود، بلکه پتانسیل تهاجمی سایبری به عنوان یک سلاح نظامی نیز باید در نظر گرفته شود. بنابراین برای حفاظت و دفاع سایبری، الحاق توانمندی‌های سایبری به شرح وظایف فرماندهی و کنترل در حوزه نظامی ضروری است. اقدامات الکترومغناطیسی سایبری باید از افکار و اهداف فرمانده حمایت کند تا قابلیت نیروهای نظامی برای رسیدن به نتایج مطلوب افزایش دهد.

در حال حاضر مأموریت اصلی کارکنان در جنگ شامل چهار وظیفه اصلی است: انجام فرآیند عملیات (برنامه‌ریزی، آماده‌سازی، اجرا و ارزیابی)، انجام مدیریت دانش و مدیریت اطلاعات و اطلاع رسانی، انجام فعالیت‌های نفوذی، انجام CEMA . در مرکز آن، CEMA برای آرایش نظامی جهت دستیابی به افزایش نفوذ فضای سایبری و طیف الکترومغناطیسی و نقش آن در عملیات زمین یکپارچه، طراحی می‌شود. CEMA از طریق یکپارچه‌سازی و

هماهنگ‌سازی عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف اجرا می-شود.

نیروهای نظامی باید از وزارت دفاع نیز حمایت کند تا نیازهای مشترکشان را برای اجرای عملیات اطلاعات، جنگ الکنرونیک و عملیات سایبری از طریق اجرای CEMA، IIA و تلفیق فعالیت‌های مربوط به اطلاعات دیگر انجام دهد. این فعالیت‌های مجزا، از طریق دستور فرمانده به یکدیگر گره می‌خورد؛ هرچند که آنها فرآیندی متفاوت و مجزا برای انجام نیازهای عملیاتی خود دارند.

نتیجه‌گیری:

این مقاله به بحث در مورد اصول اقدامات الکترومغناطیس سایبری، معرفی دامنه فضای سایبری و توصیف طیف الکترومغناطیسی در درون محیط عملیاتی و محیط اطلاعاتی پرداخته است و سپس با بحثی از مفاهیم CEMA در پشتیبانی از عملیات زمینی یکپارچه به پایان رسیده است.

در این تحقیق، اهمیت فضای سایبری و طیف الکترومغناطیسی بیان شد تا فرماندهان و کارکنان نظامی بتوانند با استفاده از تاکتیک‌ها و روش‌های نوین، برنامه‌ریزی، یکپارچه‌سازی و هماهنگ‌سازی CEMA را انجام دهند. تمام اعضای شاغل در نیروهای مسلح مخاطبان اصلی این تحقیق هستند. فرماندهان و کارکنان ستادی به عنوان یک نیروی مشترک عملیاتی، قابل اجرایی بودن دستورالعمل‌های تدوین شده CEMA را در عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف باید بررسی کنند. مربیان و نیروهای تحت آموزش در کل نیروهای مسلح نیز از این مقاله می‌توانند استفاده کنند. بر اساس این تحقیق، فرماندهان، کارکنان و زیردستان باید مراقب باشند که تصمیمات و اقداماتشان بین-المللی، متناسب با روش جاری کشور و در بعضی مواقع منطبق با قوانین و مقررات کشورهای خارجی در هنگام انجام CEMA باشد. فرماندهان در تمام سطوح باید مراقب باشند که سربازانشان مطابق با قانون جنگ و قوانین درگیری عمل کنند.

در حال حاضر، برنامه واضح و روشنی در زمینه CEMA در کشور وجود ندارد از آنجاکه نقش الکترومغناطیس سایبری در نبردهای آتی(نه چندان دور) پررنگ خواهد شد، لذا لازم است اقدامات زیر در سطح نیروهای مسلح کشورمان به انجام رسد.

۱. واحد CEMA در مرکز عملیات فضای سایبری، نبرد الکترونیک و عملیات مدیریت طیف در نیروهای مسلح تشکیل شود تا مسئولیت برنامه‌ریزی، یکپارچه‌سازی و

هماهنگ‌سازی این سه عملیات را در نیروهای نظامی برای دستیابی به افزایش نفوذ در فضای سایبری و استفاده از حداکثر ظرفیت طیف الکترومغناطیسی و همچنین پشتیبانی از مأموریت فرمانده را برعهده گیرد.

۲. نقشه راه اقدامات الکترومغناطیس سایبری در نیروهای مسلح توسط متخصیص تدوین شود.

۳. فرماندهان و کارکنان نظامی آموزش‌های لازم را فرا گیرند تا با استفاده از تاکتیک‌ها و روش‌ها، برنامه‌ریزی، یکپارچه‌سازی و هماهنگ‌سازی CEMA را انجام دهند. تا توانائی هماهنگی و تلفیق عملیات فضای سایبر، نبرد الکترونیک، عملیات مدیریت طیف و ارتباط دهی آنها را جهت رسیدن به نتیجه مورد دلخواه در پشتیبانی از عملیات زمینی یکپارچه داشته باشند.نیروی انسانی متخصص در زمینه CEMA تربیت شوند تا عملیات‌های آفندی و پدافندی در سطح نیروهای مسلح را به اجرا در آورند.

۴. فرماندهان و کارکنان ستادی آموزشهای لازم را فرا گیرند تا قابل اجرایی بودن دستورالعمل‌های تدوین شده CEMA در عملیات فضای سایبری، جنگ نبرد الکترونیک و عملیات مدیریت طیفرا بررسی کنند.

۵. مفهوم CEMA در نشریات آموزشی واحدهای آموزشی نیروهای مسلح، عملیات زمینی یکپارچه و مأموریت فرماندهی مدون شود.

۶. نیروهای مسلح برای دفاع از شبکه‌های سایبری خودی و برای ایجاد اختلال در شبکه‌های دشمن در جنگهای آینده باید از آمادگی و مهارت‌های لازم برخوردار باشند.

۷. برای حفظ برتری در فضای سایبری و طیف الکترومغناطیسی از زیرساخت‌های فیزیکی، شبکه‌های دیتا و طیف الکترومغناطیسی در سطح نیروهای مسلح ایجاد، تجهیز و نگهداری شود.

۸. از حداکثر ظرفیت طیف الکترومغناطیس جهت بهره‌وری بیشتر از فضای مجازی استفاده شود.

۹. یک شبکه فنی LWN که شامل تمام سیستم‌های مدیریت اطلاعات ارتش و سیستم-های اطلاعاتی است تشکیل شود تا اطلاعات را جمع‌آوری، پردازش، ذخیره، نمایش، انتشار و محافظت از آن را انجام دهد.

۱۰. برنامه‌ریزی عملیاتی جهت حمله به دشمن و سیستم‌ها و شبکه‌های حریف در فضای سایبری و طیف الکترومغناطیسی جهت ایجاد فریب، تنزل، اختلال، انکار، نابودی یا دستکاری طرح ریزی شود.

۱۱. برنامه برای استفاده از سیستم‌های دشمن و حریف در فضای سایبر برای تسهیل در جمع‌آوری اطلاعات بهره‌برداری طرح ریزی شود.

۱۲. از متخصصین و سیستم عامل و تجهیزات حفاظت بعمل آید.

بررسی دیدگاه‌های چندگانه در مورد سایبر، چگونه باید از آن در نیروهای مسلح مورد استفاده قرار گیرد و قابلیت آن در کجا باید قرار داده شود، مباحثی هستند که باقی می‌ماند و در مورد آن باید تحقیقات لازم انجام شود.

منابع

- هادی خانیکی, & محمود بابائی. (۲۰۱۳). فضای سایبر و شبکه های اجتماعی مفهوم و کارکردها. جامعه اطلاعاتی, دوره اول شماره ۱: ۷۱-۹۶.
- _____، (سال انتشار)، ملزومات امنیت در فضای سایبر ملی" کمیته مطالعات فناوری اطلاعات ۱-۷
- حسینی، ظریف منش. (۱۳۹۲). مطالعه تطبیقی ساختار دفاع سایبری کشورها. فصلنامه پژوهش های حفاظتی و امنیتی, ۲(۵) : ۴۱-۶۸.
- دستجردی حسن کامران, & میرمحمدی زهرا، (۱۳۹۳) فضای سایبری و تعاریف جدید در جغرافیای سیاسی.، جغرافیا، سال دوازدهم، شماره ۴۳: ۱۴۳-۱۵۶
- 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.
- Bender, J. M., & Hamilton, A. (2013). The Cyberspace Operations Planner. Journal Article| Nov, 5(11), 18am.
- Lyons, Sean P. Social Media Analytics: A New Approach for Cyberspace Enabled Understanding of Operational Environments. No. ATZL-SWV. ARMY COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES, 2013.
- Army, U. S. "Army Doctrine Publication (ADP) No. 3-0, 2011 (), Unified Land Operations." Headquarters Department of the Army Washington, DC, 10 October

- Center, D. C. C. A. (2009). Capability Development Integration Directorate,“. In Army Cyber/Electromagnetic Contest Capabilities-Based Assessment (C/EM CBA) Functional Solutions Analysis (FSA) Workshop (Vol. 1).
- Liang, Yi J., Eckehard G. Steinbach, and Bernd Girod. (2001) "Real-time voice communication over the internet using packet path diversity." In Proceedings of the ninth ACM international conference on Multimedia, pp. 431-440. ACM,.
- Conti, Gregory, John Nelson, and David Raymond. "Towards a cyber common operating picture." In Cyber Conflict (CyCon), 2013 5th International Conference on, pp. 1-17. IEEE, 2013.
- Stamper, Lisa Jayne. "The LandWarNet School, The Army Learning Model, and Appreciative Inquiry: How is a Centralized Training Organization Improved by Introducing Decentralization?" (2015).
- Eckley, Gordon P. "Voice and data communication system." U.S. Patent 4,740,963, issued April 26, 1988.
- Miller, Chris. Network Requirements in Support of Army's LandWarNet Transformation. ARMY WAR COLL CARLISLE BARRACKS PA, 2011.
- TRADOC PAM 525-7-8, Army, U. S. (2010), "Cyberspace Operations Concept Capability Plan 2016-2028." US Army Capabilities Integration Center 22.
- Field Manual (FM) 3-36, (2012), Electronic Warfare, Headquarters Department of the Army Washington, DC, 9 November
- Field Manual (FM) 3-38, (2014), Cyber Electromagnetic Activities, Headquarters, Department of the Army Washington.
- Field Manual No. 6-02.70, (2010) “ARMY ELECTROMAGNETIC SPECTRUM OPERATIONS’, Headquarters Department of the Army Washington, DC, 20 May
- Pub, J. (2014). Pub 3-13. Joint Doctrine for Information Operations, U.S. Army.
- Army, U. S. "Field Manual No. 3-13, (2013): Inform and Influence Activities." Headquarters Department of the Army Washington, DC, 25 January.