فصلنامه مطالعات جنگ
سال سوم، شماره هشتم، بهار ۱۴۰۰
مقالهٔ سوم از صفحه ۵۱ تا ۷۲

نقش فرماندهان نیروهای مسلح در تهدید نو پدید الکترومغناطیس سایبری

حسن عبداللهی[۱]، مصطفی لطفی جلال آبادی [۲] ، افسانه حق نگهدار[۳]

دریافت مقاله: ۱۴۰۰/۰۱/۲۵ پذیرش مقاله:۱۴۰۰/۰۲/۲۷

چکیده

با توجه به تهدیدات موجود علیه منافع جمهوری اسلامی ایران، اقدام انفعالی و عدم برنامه ریزی برای آینده و آینده پژوهی در این حوزه بسیار خطرناک و غیر منطقی می باشد و این شیوه تفکر باعث بروز مشکلاتی جدی برای کشور خواهد شد. لذا بایستی تهدیدات آینده را شناسایی نمود. از این رو هدف این مطالعه تبیین تهدید نوپدید الکترومغناطیس سایبری به عنوان تهدید آینده و بررسی نقش فرماندهان در فضای الکترومغناطیس سایبری است. این تحقیق از نظر هدف از نوع تحقیقات کاربردی و جامعه مورد مطالعه بررسی کتب و اسناد انتشار یافته ایالات متحده آمریکا می باشد یافته های تحقیق حاکی از آن است که جنگ در آینده در فضای عملیاتی جدیدی با نام اقدامات الکترومغناطیس سایبری است که این نبردها در فضای سایبری با بهره‌برداری از طیف الکترومغناطیس است و یک فرمانده برای کنترل صحنه نبرد از جایگاه کلیدی ویژه‌ای برخوردار خواهد شد و بایستی با ایجاد زیرساخت‌های نظامی مناسب و با بهره‌گیری از شبکه‌های ارتباطی غیرنظامی، توانائی مدیریت صحنه میدان در هر دو فاز نبرد و جنگ را داشته باشد.

واژگان کلیدی: فرمانده، الکترومغناطیس سایبری، جنگ‌های آینده، عملیات سایبری و نبرد الکترونیکی

۱ – استادیار برق– الکترونیک، دانشگاه هوایی شهید ستاری، h.abd@ssau.ac.ir ۰۲۱۶۶۶۹۲۹۲۷
[۲] استادیار دانشکده مدیریت دانشگاه هوایی شهید ستاری ۰۹۱۲۵۴۴۱۵۶۰
۳ – کارشناس‌ارشد برق – الکترونیک

مقدمه

در نبردهای آینده، نه‌تنها فرماندهان باید از حداکثر طیف الکترومغناطیس در باندهای نظامی و غیرنظامی بهره‌برداری کنند بلکه باید سه حوزه مدیریت طیف الکترومغناطیس، فضای سایبر و نبرد الکترونیک را با یکدیگر هماهنگ و یکپارچه نمایند. لذا فرماندهان در نیروهای مسلح برای دفاع از شبکه‌های سایبری و طیف الکترومغناطیس خودی و برای ایجاد اختلال در شبکه‌های سایبری و طیف الکترومغناطیس دشمن باید مهارت لازم را داشته باشند تا فرآیند انجام عملیات، مدیریت اطلاعات، فعالیت‌های نفوذی و اجرای اقدامات الکترومغناطیس سایبری را به انجام رسانند. ازاین‌رو در آینده نزدیک، فعالیت‌های الکترومغناطیس سایبری به‌عنوان یکی از عوامل قدرت نبرد، باید توسط فرماندهان در طرح‌ریزی عملیات نظامی به‌عنوان یک سلاح در میدان نبرد مطرح باشد زیرا چارچوب‌های عملیاتی پیچیده‌تر و میدان محدود جنگ فیزیکی به یک میدان جنگ جهانی نامحدود تبدیل‌شده است. این مقاله جزو اولین کارهای تحقیقاتی انجام‌شده بر روی نقش آتی فرمانده در کنترل صحنه نبرد در فضای سایبر و طیف الکترومغناطیس است که می‌تواند مرجعی برای فرماندهان باشد تا با استفاده از آن، توانائی قابلیت روش‌های ابتکاری برای تسخیر، حفظ و بهره‌برداری از برتری نظامی در تمام محیط عملیاتی را داشته باشند.

بیان مساله :

در عصر حاضر، توسعه فن‌آوری اطلاعات و ارتباطات به‌ویژه فن‌آوری‌های مرتبط با فضای سایبری در حوزه غیرنظامی که دروازه آن اینترنت است، به‌عنوان یک سلاح در میدان نبرد مطرح هست و کاربرد آن در آینده نزدیک برای توسعه عملیات 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 به انجام خواهد رسید.

طی جستجو و مطالعات گسترده در خصوص الکترومغناطیس سایبری، سندی مربوط به نیروی زمینی آمریکا به شماره FM 3-38 با عنوان "Cyber Electromagnetic Activities" به دست آمد (Manual Field،۲۰۱۴) این سند در سال ۲۰۱۴ میلادی منتشرشده است که

ارتباط فضای سایبر، جنگ الکترونیک و مدیریت طیف را مطرح می‌کند. این سند بیان می‌کند که جهت پیروزی در نبردهای آینده سه حوزه طیف الکترومغناطیسی، جنگ الکترونیک و مدیریت طیف باید با یکدیگر هماهنگ و یکپارچه شوند، اما چگونگی اجرای آن در عملیات نظامی محرمانه و دارای طبقه‌بندی است. این سوال مطرح می شود که آیاد در جنگ‌های آینده، شیوه فرماندهی تغییر اساسی پیدا خواهد کرد.؟ آیا نبرد الکترومغناطیس در آینده ایجاد خواهد شد؟ فرماندهان در این نبرد چه نقشی را خواهند داشت؟

ضرورت تحقیق

عصر حاضر که عصر اطلاعات است، عموماً نبرد بر سر دانش و سلطه بر روی شبکه و سازمان‌های شبکه شده است (ویژگی اصلی نبردهای جدید). ازاین‌رو، این ویژگی ممکن است مورد تمایل فرماندهانی نباشد که می‌خواهند فرماندهی و اطلاعات (و حتی ارتباطات در بسیاری از ارتش‌ها) را با همان روش‌های سنتی دنبال کنند. در مدل شبکه‌ای، جریان فرمان و اطلاعات لزوماً با یکدیگر متفاوت خواهند بود. اطلاعات حسگرها، فرماندهان و سامانه‌های جنگی با استفاده از یک تور شبکه‌ای به یکدیگر متصل‌اند و داده‌های هشدار از وضعیت به‌طور یقین توسط تمام المان‌ها، در اشتراک خواهند بود. صرف‌نظر از اینکه آن‌ها متعلق به واحدهای مشابهی باشند یا نه، دیگر نیازی نیست که سیر فرمان در سلسله‌مراتب فرماندهی با جریان اطلاعات اشتراک داشته باشند. اطلاعات در شبکه در اختیار همه قرار دارد تا فرمان و کنترل بر اساس آرایش نظامی (ترتیب نیرو یا سازمان نیروها) هدایت شوند. ازاین‌رو، فناوری جدید نه‌تنها چگونگی فرماندهی و کنترل ارتش‌ها را تغییر قابل‌توجهی داده، بلکه سازمان‌دهی و آموزش آن‌ها را نیز عوض کرده است.

از طرف دیگر استفاده از امواج الکترومغناطیس و انرژی تابشی ناشی از تسلیحات ضد تشعشع در حمله (به نیروی انسانی، تسهیلات یا تجهیزات دشمن باهدف فریب، اخلال، کاهش توانمندی یا انهدام قابلیت‌های رزمی)، بخش عمده‌ای از توجه و تلاش نیروهای نظامی را در حوزه آموزش و عملیاتِ جنگال به خود اختصاص داده است. موفقیت در یک حمله الکترونیکی علیه اهداف حیاتی و کلیدی درگرو ترکیب دو عامل (۱) آگاهی از چیدمان سامانه‌های تهدید و (۲) مؤلفه‌های فنی و عملیاتی آن‌ها است.

بنابراین استفاده از سلاح‌های الکترونیکی و انرژی الکترومغناطیسی به‌عنوان یک نیروی مخرب در نبردها سبب شده است که فرماندهان به این طیف و انرژی الکترومغناطیسی و کاربردهای آن با دقت و وسواس بیشتری توجه نمایند. از طرف دیگر استفاده گسترده از بستر اینترنت و فضای سایبر، سبب شده است که علاوه بر جنبه‌های اجتماعی از بعد نظامی نیز به فضای سایبر توجهی خاص شود. چراکه فضای سایبر به این حقیقت تأکید دارد که دیگر یک چارچوب عملیاتی به یک مکان فیزیکی محدود نمی‌شود(**Coonfield**، ۲۰۱۳). بنابراین چارچوب‌های عملیاتی پیچیده‌تر و میدان محدود جنگ فیزیکی به یک میدان جنگ جهانی نامحدود تبدیل‌شده است.
ازاین‌رو واژه جدیدی در حوزه عملیات نظامی با عنوان اقدامات الکترومغناطیس سایبری در سطح دنیا مطرح شد. لذا با توجه به اهمیت هر دو حوزه فضای سایبر و طیف الکترومغناطیس و همچنین مفهوم جدید اقدامات الکتروغناطیس سایبری ضروری است که در خصوص این موضوعات و نحوه ارتباطات آن‌ها با یکدیگر و اهمیت فرماندهی در این حوزه تحقیقاتی انجام گیرد.

اهداف و سؤالات پژوهش

هدف اصلی

۱)تعیین نقش فرماندهان در تهدید نوپدید الکترومغناطیس سایبری

اهداف فرعی

۱) شناسایی نبرد الکترومغناطیس سایبری به عنوان تهدید آینده
۲) شناسایی نقش فرماندهان در نبرد الکترومغناطیس سایبری

سؤال اصلی

۱) فرماندهان نیروهای مسلح در تهدید نوپدید الکترومغناطیس سایبری چه نقشی بایستی داشته باشند؟

سؤالات فرعی

۱) آیا نبرد الکترومغناطیس سایبری به عنوان یک تهدید در آینده شناسایی می شود؟
۲) فرماندهان نیروهای مسلح چه نقشی در نبرد الکترومغناطیس سایبری خواهند داشت؟

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(Pub 3-13، ۲۰۱۴ : ۳۵) 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 ، ۲۰۱۳ : ۲) تهدیدکنندگان فضای سایبر، گروههای متعدد با انگیزه‌های متفاوت مانند سرقت، جاسوسی، خرابکاری، انتقام و سرگرمی می‌باشند که از آن میان می‌توان 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 سیاست‌های 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، ۲۰۱۳ : ۶)

اقدامات الکترومغناطیس سایبری:

شکل شماره ۱ حوزه فضای سایبر

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 طیف۳ 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.

---

[1] Cyber Operations (CO)
[2] Electronic Warfare (EW)
[3] Spectrum Management Operations (SMO)

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[1] به معنای آرایش نیروهای نظامی است و اقداماتشان برای ایجاد نیرویی است که با درگیر شدن عمل کنند. از طرف دیگر، همزمانی[2] به معنای آرایش اقدامات نظامی در زمان، مکان و هدف مشخص جهت ایجاد حداکثر توان رزمی در یک زمان و مکان معین است. اقدامات 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 الکترومغناطیس۳ 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 در کاربرد 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.

---

[1] Integrating
[2] Synchronization
[3] Electromagnetic Spectrum (EMS)

اقدامات الکترومغنطیس 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).

اقدامات الکترومغناطیس سایبری:

اقدامات الکترومغناطیس سایبری فعالیت‌های قدرتمندی جهت تسخیر، حفظ و بهره‌برداری از یک برتری بیشتر در برابر مخاصمان و دشمنان در هر دو حوزه فضای سایبری و طیف الکترومغناطیسی است، درحالی‌که استفاده هم‌زمان و مشابه دشمن و مخالفان از آن را کاهش می‌دهد و از مأموریت سیستم فرماندهی نیز محافظت می‌کند. اقدامات الکترومغناطیس سایبری شامل عملیات فضای سایبری[۱]، نبرد الکترونیک[۲] و عملیات مدیریت طیف است (Coonfield ، ۲۰۱۳).

فرماندهی که توسط متخصصین پشتیبانی می‌شود باید هم‌زمان‌سازی و ادغام نمودن عملیات فضای سایبر، جنگ الکترونیک، عملیات مدیریت طیف و توانایی ارتباط دهی جهت رسیدن به نتیجه مورد دلخواه در پشتیبانی از عملیات را انجام دهد.

همان‌طور که در شکل (۲) نشان داده‌شده است انجام اقدامات الکترومغناطیس سایبری در نیروهای ارتش باید به‌صورت یکپارچه باشد. یکپارچگی[۳] یک از آرایش‌های نیروهای نظامی است و

---

۱ Cyber Operations (CO)
۲ Electronic Warfare (EW)
۳ Integrating

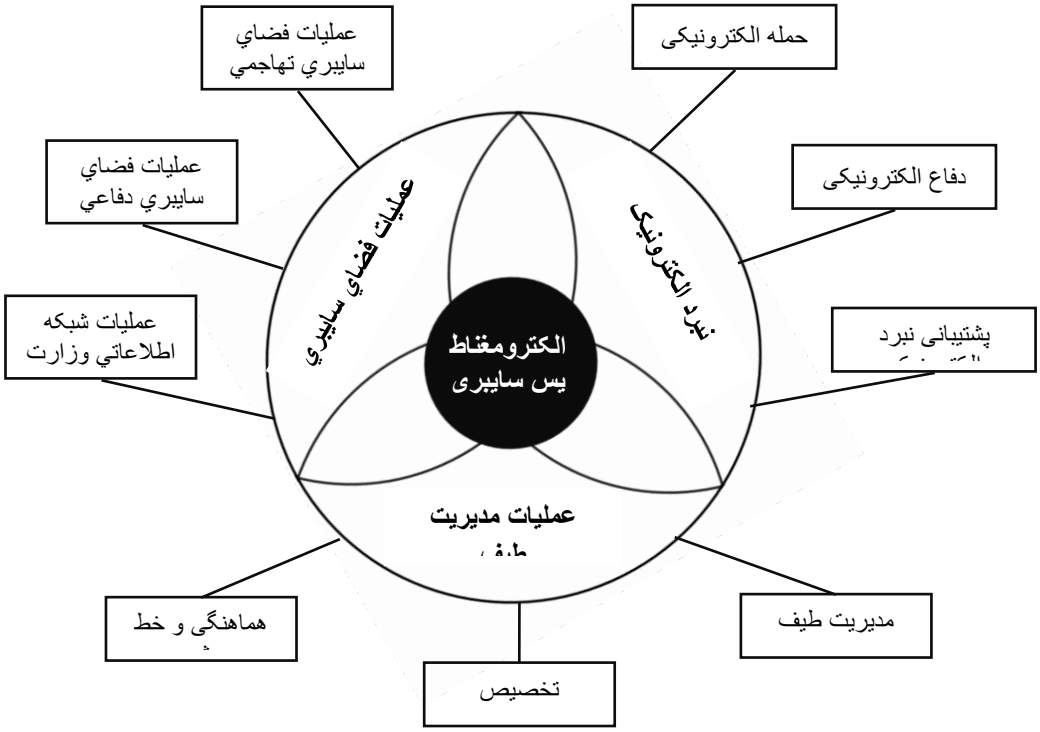
اقداماتشان برای ایجاد نیرویی است که با درگیر شدن عمل می‌کند. هم‌زمانی[۱] آرایشی از اقدامات نظامی در زمان، مکان و هدف مشخصی جهت تولید حداکثر توان رزمی در یک‌زمان و مکان معین است. اقدامات الکترومغناطیس سایبری عملکرد و توانمندی عملیات فضای سایبری، نبرد الکترونیک و عملیات مدیریت طیف را برای تولید اثرات تکمیلی و تقویتی، ادغام و هماهنگ می‌کند. انجام این اقدامات به‌طور مستقل ممکن است از کارآمدی آن بکاهد. اگر ناهماهنگی باشند، این فعالیت‌ها ممکن است منجر به تعارض و تداخل متقابل بین آن‌ها و با دیگر نهادهای استفاده‌کننده از طیف الکترومغناطیسی شود. عملیات فضای سایبری، نبرد الکترونیک و عملیات مدیریت طیف هم‌زمان می‌شوند تا باعث اثر مشخصی در نقاط معین جهت پشتیبانی کل عملیات شوند.

شکل (۲) نشان می‌دهد که عملیات فضای سایبری شامل سه بخش عملیات فضای سایبری تهاجمی، عملیات فضای سایبری دفاعی و عملیات شبکه اطلاعاتی وزارت دفاع است(Bender & Hamilton 2013). نبرد الکترونیک شامل سه زیرمجموعه حمله الکترونیکی، دفاع الکترونیکی و پشتیبانی نبرد الکترونیک است(Field Manual، ۲۰۱۲) و عملیات مدیریت طیف شامل مدیریت طیف، تخصیص فرکانس، هماهنگی کشورها است که برنامه‌ریزی، مدیریت و اجرای عملیات را در داخل محیط عملیاتی الکترومغناطیس در طول مدت تمام مراحل عملیات نظامی قادر می‌سازد(Field Manual، ۲۰۱۰)

عملیات فضای سایبری، نبرد الکترونیک و عملیات مدیریت طیف جهت انجام عملیات یکپارچه ضروری هستند. تا موقعی که این اقدامات در کاربرد و تاکتیکشان تفاوت داشته باشند، عملکردها و توانمندی آن‌ها جهت به حداکثر رساند پشتیبانی باید یکپارچه و هماهنگ باشد. ادغام این اقدامات نیاز به درک درستی از عملکردها و توانمندی‌های بکار برده شده دارد(Lyons، ۲۰۱۳).

---

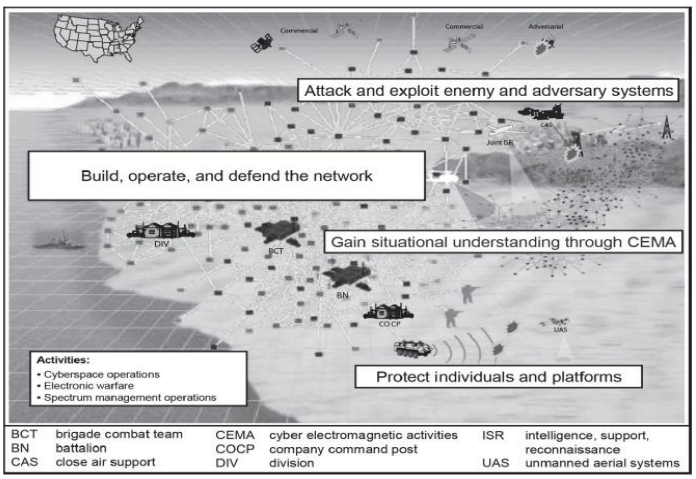
[۱] Synchronization



شکل ۱ حوزه اقدامات الکترومغناطیس سایبری

فعالیت الکترومغناطیس سایبری در عملیات یکپارچه:

شکل ۳ جایگاه عملیات اقدامات الکترومغناطیس سایبری را درصحنه نبرد به تصویر می‌کشد. توانایی برای به دست آوردن و حفظ یک مزیت در فضای مجازی و طیف الکترومغناطیسی مستلزم آن است که ارتش از توانمندی‌های اقدامات الکترومغناطیس سایبری برای انجام موارد زیر استفاده کند(Army Doctrine Publication، ۲۰۱۰)



شکل۲: جایگاه عملیاتی اقدامات الکترومغناطیس سایبری درصحنه نبرد

روش تحقیق

این تحقیق از نظر هدف توسعه ای و از نظر ماهیت و روش توصیفی- تحلیلی با رویکرد اکتشافی است. جامعه آماری تحقیق کتب مرتبط با جنگ سایبری و الکترونیکی و اسناد منتشر شده از ارتش ایالت متحده امریکا است. سعی شده تا با تحلیل‌های کیفی، ضمن دستیابی به شناختی عمیق از موضوع، زمینه افزایش تعمیم‌پذیری و صحت نتایج نیز فراهم آید. با توجه به اهداف و سؤالات پیش رو، محقق، از طرح اکتشافی استفاده نموده است که در آن اطلاعات موردنیاز به روش کتابخانه‌ای می باشد.

یافته های تحقیق

پاسخگویی به سوال اول تحقیق

۱) آیا نبرد الکترومغناطیس سایبری به عنوان یک تهدید در آینده شناسایی می شود؟

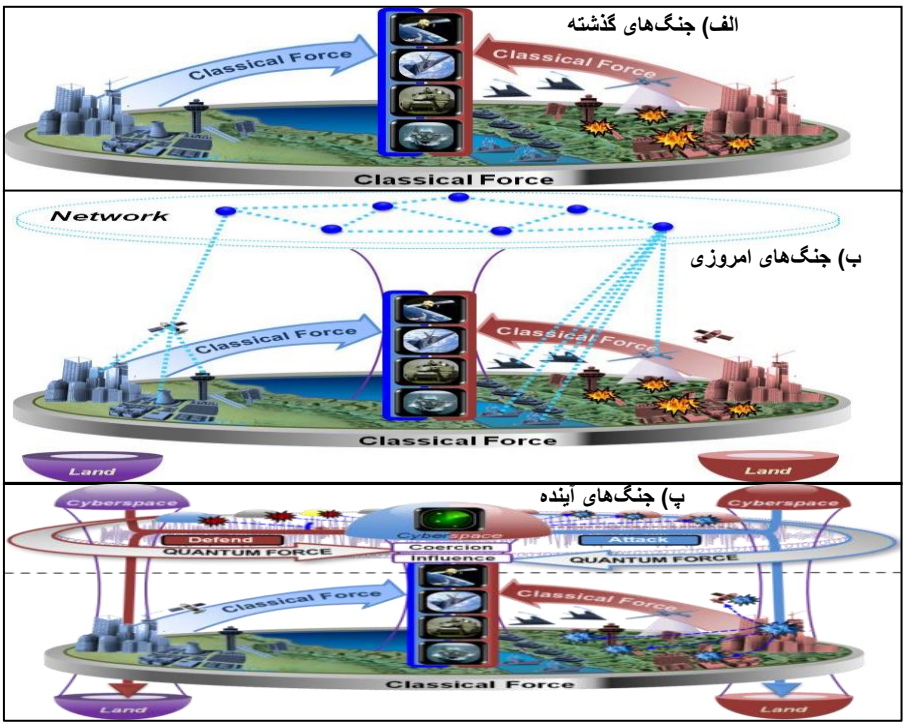
شکل روند تکاملی جنگ‌ها از قرن گذشته تا حال و آینده را نشان می‌دهد. همانطور که در شکل نشان داده شده است این جنگ‌ها به ترتیب از پایین به بالا شامل جنگ‌های سنتی یا کلاسیک، جنگ‌های کلاسیک-شبکه محور و جنگ‌های کلاسیک با اقدامات الکترومغناطیس سایبری است.

قسمت 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 عزیزمان به علت برتری هوائی بیشتر به خصوص در اوایل جنگ از قدرت بیشتری نسبت به دشمن مخاصم برخوردار بود.

قسمت 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 یاد 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 ۴ 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.



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 می‌شود.

نیروهای نظامی باید از وزارت دفاع نیز حمایت کند تا نیازهای مشترکشان را برای اجرای عملیات اطلاعات، جنگ الکترونیک 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.

پاسخگویی به سوال دوم تحقیق

فرماندهان در تهدیدات آینده چه نقشی دارند؟

فرماندهان اهرم اقدامات الکترومغناطیس سایبری هستند و آن‌ها یکی از چهره‌های اصلی و مهم در اقدامات الکترومغناطیس سایبری هستند و دستوراتشان بخشی از یک عملیات مشترک برای رسیدن به اهداف در حوزه طبیعی، فضای سایبری و طیف الکترومغناطیسی است. فرماندهان اقدامات الکترومغناطیس سایبری را برای تصرف، حفظ و بهره‌برداری از یک مزیت (برتری) نسبت به مخالفان و دشمنان در حوزه‌های طبیعی، فضای سایبری و طیف الکترومغناطیسی اجرا می‌کنند تا در حصول نتیجه کلی موفقیت مأموریت تسهیل شود.

فرماندهان بر اساس توصیه‌های ارائه‌شده توسط متخصصین، تصمیم‌گیری را با دریافت اطلاعات از طریق افسران CEMA انجام می‌دهند. فرماندهان با این فرآیند ادغام و هماهنگ‌سازی عملیات فضای مجازی، نبرد الکترونیک و عملیات مدیریت طیف را باتدبیر عملیاتی خودشان هدایت می‌کنند. فرماندهان منابعی را تعیین می‌کنند که جهت حمایت و پشتیبانی از اقدامات الکترومغناطیس سایبری استفاده می‌شوند.

انجام عملیات یکپارچه به فرماندهانی نیاز دارد تا آنچه را که بر محیط عملیاتی تأثیر می‌گذارد را در نظر بگیرند. زمانی که اقدامات الکترومغناطیس سایبری با دیگر قابلیت‌های موجود آن‌ها ادغام و هماهنگ می‌شود، ملاحظات زیر باید توسط فرمانده در نظر گرفته شود:

اجرای اقدامات الکترومغناطیس سایبری می‌تواند با ملاحظات سیاستی و قانونی توأم باشد.

ممکن است زمان اجرای اقدامات الکترومغناطیس سایبری طولانی باشد. زیرا ممکن است به قابلیت استفاده از دارایی‌ها و ملاحظات تصدیق صلاحیت نیاز داشته باشد.

عملیات فضای سایبری برای مأموریت‌هایی که به خارج محیط عملیات گسترش‌یافته است، نیاز به هماهنگی وسیعی دارد (به‌عنوان‌مثال، مقامات سطح ملی).

نبرد الکترونیک می‌تواند در تمام سطوح، فعال و اجرا شود و می‌تواند به حمایت از فرمانده تاکتیکی تأکید کند.

برای دستیابی به اهدافی که قبلاً تنها توسط تخریب فیزیکی به دست می‌آمدند، اقدامات الکترومغناطیس سایبری گزینه‌ای را برای به‌کارگیری اثرات جایگزین، ارائه می‌دهد.

اقدامات الکترومغناطیس سایبری می‌تواند اثرات لحظه‌ای نزدیک و هم‌زمان را در سراسر حوزه‌های مختلف ایجاد کند. این اثرات ممکن است در فضای سایبری و طیف الکترومغناطیسی قسمت‌های خودی، بی‌طرف و دشمن رخ دهد.

احتمال اثرات ناخواسته و آبشاری وجود دارد و ممکن است برای پیش‌بینی دشوار باشد.

درک موقعیت از محیط عملیات، بدون در نظر گرفتن فضای سایبری و طیف الکترومغناطیسی ناقص است.

اقدامات الکترومغناطیس سایبری برای محافظت و اطمینان از دسترسی به سیستم فرمان مأموریت، باید قدرت نفوذ داشته باشد.

نتیجه

در آینده نزدیک حوزه جدیدی بانام اقدامات الکترومغناطیس سایبری به فضای عملیاتی نبردها اضافه خواهد شد که شیوه فرماندهی را دگرگون خواهد کرد. این مقاله، اهمیت و نقش فرمانده در جنگ‌های آینده جهت کنترل میدان نبرد را بیان و واژه و مفهوم و اهمیت اقدامات الکترومغناطیس سایبری را برای نیروهای مسلح معرفی می‌نماید تا چارچوبی برای محیط‌های عملیاتی نظامی معرفی شود. لذا فرمانده با اقدامات الکترومغناطیس سایبری، فعالیت‌های قدرتمندی جهت تسخیر، حفظ و بهره‌برداری از یک برتری بیشتر در برابر مخاصمان و دشمنان در هر دو حوزه فضای سایبری و طیف الکترومغناطیسی را به دست می‌آورد، درحالی‌که استفاده هم‌زمان و مشابه دشمن و مخالفان از آن را کاهش داده و از مأموریت سیستم فرماندهی نیز محافظت می‌شود. فرمانده با اقدامات الکترومغناطیس سایبری عملیات فضای سایبری، نبرد الکترونیک و عملیات مدیریت طیف را با یکدیگر هماهنگ و یکپارچه می‌سازد تا به نتیجه مورد دلخواه در عملیات دست یابد. فرمانده با اقدامات الکترومغناطیس سایبری ساختار اضافی را به هر یک از این حوزه‌ها اضافه نمی‌کند. در اصل هر یک از این حوزه‌ها به‌طور مستقل وظایف خود را انجام می‌دهند و فرمانده وظیفه یکپارچه‌سازی و هماهنگ‌سازی این

سه حوزه را با یکدیگر دارد تا مدیریت صحنه میدان در هر دو فاز نبرد و جنگ را با بهره‌گیری از توانائی اقدامات الکترومغناطیس سایبری به انجام رساند.

بنابراین در نبردهای آینده، فرمانده چهار وظیفه اصلی را در جنگ خواهد داشت که عبارت‌اند از: ۱-انجام فرآیند عملیات (برنامه‌ریزی، آماده‌سازی، اجرا و ارزیابی) ۲-انجام مدیریت دانش، مدیریت اطلاعات و اطلاع‌رسانی ۳-انجام فعالیت‌های نفوذی ۴-انجام CEMA. در مرکز این چهار وظیفه، CEMA برای آرایش نظامی جهت دستیابی به افزایش نفوذ فضای سایبری و طیف الکترومغناطیسی قرار دارد و نقش آن در عملیات یکپارچه باید موردتوجه فرماندهان قرار گیرد. فرمانده CEMA از طریق یکپارچه‌سازی و هماهنگ‌سازی عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف به اجرا درخواهد آورد. باید در نظر داشت که آن‌ها فرآیندی متفاوت و مجزا برای انجام نیازهای عملیاتی خوددارند و این فعالیت‌های مجزا، از طریق دستور فرمانده به یکدیگر گره می‌خورد. این مقاله، اطلاعات لازم را به نیروهای مسلح می‌دهد تا فرماندهان را قادر سازد بر اساس اقدامات الکترومغناطیس سایبری محیط عملیاتی خود را شکل دهند. این پژوهش فرماندهان و افسران را راهنمایی می‌کند تا روش‌های ابتکاری‌شان برای به تصرف درآوردن، حفظ و بهره‌برداری از برتری در تمام یک محیط عملیاتی تقویت شود.

ازآنجاکه روش اجرای اقدامات الکترومغناطیس سایبری در دیگر کشورها و ازجمله ایالات‌متحده آمریکا محرمانه است، در کشور ما نیز لازم است روش اجرای آن متناسب با قوانین کشورمان تدوین و جاری شود تا فرماندهان و کارکنان نظامی با استفاده از آن و تاکتیک‌ها و روش‌های نوین جنگی، بتوانند برنامه‌ریزی، یکپارچه‌سازی و هماهنگ‌سازی اقدامات الکترومغناطیس سایبری را انجام دهند. البته آنان باید مراقب باشند که در هنگام انجام اقدامات الکترومغناطیس سایبری تصمیمات و اقداماتشان بین‌المللی، متناسب با روش جاری کشور و در بعضی مواقع منطبق با قوانین و مقررات کشورهای خارجی باشد.

پیشنهادات

ازآنجاکه نقش الکترومغناطیس سایبری در نبردهای آتی (نه‌چندان دور) پررنگ خواهد شد و در حال حاضر، برنامه واضح و روشنی درزمینه‌ی CEMA در کشور وجود ندارد لذا لازم است اقدامات زیر در سطح نیروهای مسلح کشور عزیزمان مان 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 بر عهده گیرد.

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

۳. فرماندهان و افسران نظامی آموزش‌های لازم را فراگیرند تا CEMA را با استفاده از تاکتیک‌ها و روش‌ها، برنامه‌ریزی، یکپارچه‌سازی و هماهنگ‌سازی انجام دهند و 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 مشترک را داشته باشند. نیروی انسانی متخصص درزمینه‌ی CEMA تربیت شوند تا عملیات آفندی و پدافندی در سطح نیروهای مسلح را به اجرا درآورند.

٤. فرماندهان و افسران ستادی آموزش‌های لازم را فراگیرند تا قابل اجرایی بودن دستورالعمل‌های تدوین‌شده CEMA در عملیات فضای سایبری، جنگ نبرد الکترونیک و عملیات مدیریت طیف را بررسی کنند.

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

٦. 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، زیرساخت‌های فیزیکی، شبکه‌های دیتا و طیف الکترومغناطیسی در سطح نیروهای مسلح ایجاد شود.

۸. از حداکثر ظرفیت طیف الکترومغناطیس در باند نظامی و غیرنظامی جهت بهره‌وری بیشتر از فضای مجازی استفاده شود.

۹. یک شبکه فنی LWN که شامل تمام سامانه‌های مدیریت اطلاعات ارتش و سامانه‌های 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 سامانه‌ها و شبکه‌های دشمن در فضای سایبری و طیف الکترومغناطیسی جهت ایجاد فریب، تنزل، اختلال، انکار، نابودی یا دست‌کاری طرح‌ریزی شود.

۱۱. برنامه برای استفاده از سامانه‌های دشمن و حریف در فضای سایبر برای تسهیل در جمع‌آوری اطلاعات بهره‌برداری طرح‌ریزی شود.

۱۲. از متخصصین و سیستم‌عامل و تجهیزات حفاظت به عمل آید.

منابع

منابع فارسی:

۱. حسن عبداللهی؛افسانه حق نگهدار. "نقش الکترومغناطیس سایبری در کنترل میدان جنگ با ایجاد زیرساخت‌های نظامی سایبری ."علوم و فنون نظامیِ، دوره ۱۱، شماره ۳۱، صفحه ۱۳۵-۱۱۳، بهار ۱۳۹۴.

منابع انگلیسی:

1. Field Manual (FM) 3-38, (2014), Cyber Electromagnetic Activities, Headquarters, Department of the Army Washington.

.

2. Pub, J. (2014). Pub 3-13. Joint Doctrine for Information Operations, U.S. Army.

3. 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.

4. Bender, J. M. & Hamilton, A. (2013). The Cyberspace Operations Planner. Journal Article| Nov, 5(11), 18am.

5. Field Manual (FM) 3-36, (2012), Electronic Warfare, Headquarters Department of the Army Washington, DC, 9 November

6. Field Manual No. 6-02.70, (2010) “Army Electromagnetic Spectrum Operations’, Headquarters Department of the Army Washington, DC, 20 May

7. 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.

8. Army, U. S. "Field Manual No. 3-13, (2013): Inform and Influence Activities." Headquarters Department of the Army Washington, DC, 25 January.

9. Army, U. S. "Army Doctrine Publication (ADP) No. 3-0, 2011 (), Unified Land Operations." Headquarters Department of the Army Washington, DC, 10 October

10. Stamper, Lisa Jayne. "The LandWarNet School, The Army Learning Model, and Appreciative Inquiry: How is a Centralized Training Organization Improved by Introducing Decentralization?" (2015).

11.Miller, Chris. Network Requirements in Support of Army's LandWarNet Transformation. Army War Coll Carlisle Barracks PA, 2011.

12. Eckley, Gordon P. "Voice and data communication system." U.S. Patent 4,740,963, issued April 26, 1988.

13. 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.