



فصلنامه علمی پژوهش‌های سایبرالکترونیک

صاحب امتیاز: دانشکده علوم و مهندسی دفاعی دانشگاه افسری و تربیت پاسداری امام حسین (ع)

سر دبیر: دکتر محمدعلی جوادزاده

مدیر مسئول: دکتر محمد کاظم بصیرتی

اعضای هیئت تحریریه

دکتر محمد کاظم بصیرتی	استادیار دانشگاه
دکتر حمیدرضا لشکریان	استادیار دانشگاه
دکتر مسعود باقری	دانشیار دانشگاه
دکتر محمدعلی جوادزاده	استادیار دانشگاه
دکتر حمید باباخانیان	مدرس دانشگاه
دکتر ضرغام رستمی	استادیار دانشگاه
دکتر حسین صابری	استادیار دانشگاه
دکتر مهدی علی‌نژاد	استادیار دانشگاه
مهندس سید محمود قطبانی	مدرس دانشگاه
مهندس علیرضا صفایی	مدرس و عضو هیئت علمی دانشگاه
مهندس حامد شیروی	مدرس دانشگاه
مهندس مرتضی یزدان‌پناه	مدرس دانشگاه
مهندس یوسف برجعلی	مدرس دانشگاه



همکاران علمی و داوران این شماره

دکتر منصور احدنژاد، دکتر حمید اکبری، دکتر رضا جلالی، دکتر بهروز خادم، دکتر علی کریمی، دکتر مصطفی عباسی،
دکتر مهدی علی‌نژاد، دکتر مهدی نقوی، مهندس علی بهتری، مهندس حامد شیروی، مهندس رامین دلیر،
مهندس سامان کشوری، مهندس پیمان قنوازی، مهندس مجید حاج جواد

مدیر اجرایی: مهندس علیرضا صفایی

ویراستار ادبی: سرکار خانم مهندس طوفانی

ویراستار انگلیسی و مترجم: مهندس فرامرز شمس سوسه‌باب

حروفچین و صفحه‌آرا: مهندس مرتضی یزدان‌پناه

طراح جلد: مهندس علی ذوالفقاریان

شمارگان: ۱۰۰ (نسخه چاپی) ۲۰۰ (نسخه الکترونیکی) قیمت نسخه چاپی:

نشانی: تهران، بزرگراه شهید بابایی، بعد از پل لشکرک، دانشگاه افسری و تربیت پاسداری امام حسین (ع)، دانشکده علوم و مهندسی دفاعی، تلفن: ۷۷۱۰۳۰۵۰ داخلی ۱۰۹

Web Site: www.Jce.ihuo.ac.ir

E-mail: Jce@ihuo.ac.ir

تمام حقوق مادی و معنوی برای دانشکده علوم و مهندسی دفاعی محفوظ است.

فهرست

- ❖ **سخن سردیر**..... (یازده)
- ❖ **تقسیم‌بندی معنایی برای تصاویر پهپاد با استفاده از روش‌های یادگیری عمیق**..... ۱۳
 - **سید محمدعلی ضیائی**
- ❖ **کاربرد سطوح انتخاب‌گر فرکانسی پهن باند در الکترونیک دفاعی**..... ۲۷
 - **علی عزیزی**
- ❖ **بررسی ارتباطات بی‌سیم برای شبکه هوشمند مبتنی بر رویکردها و فناوری‌های نوپدید از دیدگاه EMC**..... ۳۷
 - **ضرغام رستمی، احمد عطائی**
- ❖ **تحلیل و شبیه‌سازی ساختار نیم جمع‌کننده‌های نوری مبتنی بر بلورهای فوتونی و ارائه پیشنهادهایی جهت بهبود عملکرد در مدارهای مجتمع نوری**..... ۴۷
 - **محمد مقصودی**
- ❖ **مزایای استفاده از جنگ سایبر الکترونیک در محیط‌های عملیاتی**..... ۵۷
 - **مهرداد نجفی نوکاشتی، محمدرضا موحدی‌صفت**
- ❖ **ارائه یک دسته‌بندی بر اساس مشخصه‌های سیستم عامل‌های بی‌درنگ**..... ۷۱
 - **مهدی قزلسفلو، مهدی نقوی**

مزایای استفاده از جنگ سایبرالکترونیک در محیط‌های عملیاتی

مهرداد نجفی نوکاشتی^۱، محمدرضا موحدی صفت^۲

چکیده

میدان نبرد آینده یک جنگ شبکه‌ای بیش از حد متصل خواهد بود. در میدان نبرد آینده که زمین، دریا، هوا و فضای بیرونی توسط طیف فرکانس به هم متصل می‌شوند، مناطق جنگ الکترونیک و جنگ سایبری به تدریج با هم همپوشانی خواهند داشت. جنگ الکترونیک سایبری فناوری‌ای است که می‌تواند با یکپارچه‌سازی قابلیت انتقال امواج الکترومغناطیسی با قدرت بالا در مسافت‌های طولانی و قابلیت دستکاری/اختلال اطلاعات جنگ سایبری، اثر هم‌افزایی داشته باشد.

فضای سایبری و طیف الکترومغناطیسی یک محیط عملیاتی مشترک را ایجاد می‌کنند که می‌توان آن را حوزه الکترومغناطیسی سایبری نامید. منظور از حوزه الکترومغناطیسی سایبری معادل‌سازی اصطلاحات فضای سایبری و طیف الکترومغناطیسی نیست، بلکه به این معناست که همپوشانی قابل توجهی بین آنها وجود دارد و توسعه فناوری آینده احتمالاً این همگرایی را افزایش می‌دهد. در این حوزه، فعالیت‌های فنی اطلاعاتی هماهنگ و یکپارچه صورت می‌گیرد. این فعالیت‌ها را می‌توان عملیات الکترومغناطیسی سایبری نامید.

برای توسعه‌ی جنگ الکترونیک سایبری، لازم است ابتدا تهدیدات واقع‌بینانه و سیستم‌های تسلیحاتی که در برابر حملات جنگ الکترونیک سایبری آسیب پذیر هستند شناسایی شوند، فناوری‌های اصلی لازم استخراج شوند و بر توسعه‌ی آنها تمرکز شود. هنگام تجزیه و تحلیل موارد جنگ الکترونیک سایبری، تهدیدات هدفی که می‌توان با آنها مقابله کرد عبارتند از: "تهدیدات مجهز به گیرنده‌ی ناوبری ماهواره‌ای"، "پهپاد کوچک"، "پهپاد متوسط/بزرگ/سامانه ارتباطی ماهواره‌ای" و "شبکه فرماندهی و کنترل دشمن".

۱ دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه عالی دفاع ملی

۲ عضو هیئت علمی دانشگاه عالی دفاع ملی

این مقاله، ضمن بررسی مفاهیم و پیامدهای همگرایی جنگ الکترونیک و سایبری و الزامات اجرای آن در محیط‌های عملیاتی، فناوری جنگ الکترونیک سایبری را با توجه به روند گسترش طیف فرکانس (از دیدگاه جنگ الکترونیک و منطقه‌ی میدان نبرد به سمت فضای سایبری) معرفی کرده و جهت توسعه‌ی جنگ الکترونیک سایبری را تشریح می‌کند.

کلیدواژه‌ها: جنگ سایبری، جنگ الکترونیک؛ جنگ الکترونیک سایبری؛ سایبرالکترونیک، سایبر الکترومغناطیس جنگ، محور شبکه.

۱- مقدمه

در میدان نبرد آینده که حوزه‌های زمین، دریا، هوا و فضا توسط یک طیف فرکانسی به هم متصل می‌شوند، حوزه‌های جنگ الکترونیک و جنگ سایبری به تدریج با یکدیگر همپوشانی خواهند داشت. برای انجام مؤثر عملیات نظامی، یک فناوری جنگ الکترونیک سایبری که باعث ترکیب دو فناوری مذکور می‌شود، مورد نیاز است. وجوه اشتراکات جنگ سایبری و جنگ الکترونیک در اصول و فرآیند اجرا و همچنین تاثیرات و پیامدهای نسبتاً مشابه آن‌ها در سازمان‌های نظامی، سبب همگرایی بین این دو عرصه شده است.

استفاده مؤثر و هماهنگ از قابلیت‌های این دو حوزه، عامل برترساز و تعیین‌کننده در نبردهای آینده خواهد بود. کشورهای بهره‌مند از این دو فناوری قادر خواهند بود تا نبردها را با حداقل تلفات انسانی و کمترین هزینه به نفع خود به پایان برسانند.

امروزه ما در یک دنیای شبکه‌ای زندگی می‌کنیم. گسترش فناوری اطلاعات، نحوه تعامل انسان‌ها با یکدیگر و محیط اطراف خود را تغییر می‌دهد. تحرک نقش فزاینده‌ای در زندگی سریع ما دارد. ارتباطات سیار، اینترنت موبایل، ناوبری و ... با اتصال بی‌سیم در طیف الکترومغناطیسی در حال انجام است.

نیروهای مسلح مدرن در دنیای مبتنی بر شبکه‌های بی‌سیم امروزی، در محدوده‌ی وسیعی جهت ارتباطات، کنترل سلاح، اطلاعات، نظارت، ناوبری و حفاظت نیرو از طیف الکترومغناطیسی استفاده می‌کنند. امروزه وسایل الکترونیکی متعددی با انواع و نام‌های مختلف در میدان جنگ وجود دارد که در این زمینه کار می‌کنند. اطلاعات و محیط الکترومغناطیسی، قابلیت‌های همکاری بین آن‌ها را ضروری می‌سازد. استفاده انبوه از فناوری‌های اطلاعات و ارتباطات در میدان نبرد، مستلزم حضور نیروهای نظامی در فضای سایبری و استفاده از طیف الکترومغناطیسی است.

هدف از این پژوهش بررسی مفاهیم و پیامدهای همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در محیط‌های عملیاتی است. در این پژوهش، مفاهیم و اقدامات جنگ الکترونیک و جنگ سایبری و همچنین وجوه مشترک و ارتباط بین آن‌ها مورد بحث قرار گرفته و مفهوم و علت همگرایی این دو حوزه و پیامدهای آن بررسی خواهد شد. این پژوهش می‌تواند زمینه ساز توجه بیشتر سازمان‌های نظامی به همگرایی جنگ الکترونیک و جنگ سایبری شده و بهره‌وری و اثربخشی فعالیت‌های این دو حوزه در صحنه نبرد را فراهم آورد.

۲- مبانی نظری

پیشینه پژوهش:

تحقیقات متعددی در خصوص همگرایی جنگ الکترونیک و جنگ سایبری انجام شده است. برخی از پژوهش‌هایی که با عنوان و قلمرو موضوعی این پژوهش مرتبط بوده و توسط محققین به صورت مقاله ارائه شده است، به شرح زیر است:

احمد رضا فرحبخت و مهدی دهقانی در مقاله‌ی "همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی" ضمن تبیین مفاهیم و اقدامات جنگ الکترونیک و جنگ سایبری، به مقایسه و احصاء وجوه مشترک بین آن‌ها پرداخته و پیامدهای همگرایی این حوزه‌ها را مورد بررسی قرار داده‌اند و به این نتیجه دست یافته‌اند که ادغام اقدامات جنگ الکترونیک و جنگ سایبری و شکل‌گیری فعالیت‌های سایبرالکترونیک، قابلیت‌های جدید و ارتقاء یافته‌ای را ایجاد نموده و می‌تواند هم‌افزایی و بهره‌وری در ساختار سازمانی، منابع انسانی و تجهیزاتی را به ارمغان آورده و اثربخشی اقدامات را در صحنه نبرد افزایش دهد. [۱]

کیم سویون در مقاله‌ی "فناوری جنگ الکترونیک سایبری و جهت توسعه آن"، ضمن معرفی فن‌آوری جنگ الکترونیک سایبری بیان می‌دارد که حوزه‌های جنگ الکترونیک و جنگ سایبری به تدریج با یکدیگر همپوشانی خواهند داشت و برای انجام مؤثر عملیات نظامی، یک فناوری جنگ الکترونیک سایبری که این دو فناوری را ترکیب می‌کند مورد نیاز است. [۳]

سینف در پژوهش خود تحت عنوان "همگرایی تأثیرات عملیات سایبری و جنگ الکترونیک" همگرا شدن اثرات عملیات سایبری و جنگ الکترونیک را مورد بررسی قرار داده و نتیجه می‌گیرد که تفاوت‌های متمایز بین این دو حوزه و تجربه محدود استفاده از عملیات سایبری نسبت به جنگ الکترونیک در جنگ‌ها، مانع ادغام آن‌ها شده و اثربخشی آن‌ها را کاهش می‌دهد. [۴]

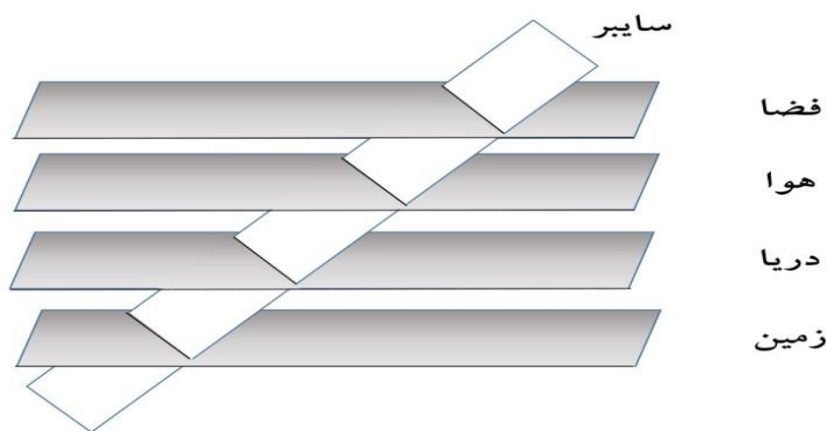
اس‌کین، ایرماکا و اوسورا در مقاله‌ای تحت عنوان "یکپارچگی جنگ سایبری و جنگ الکترونیک در محیط عملیاتی آینده: جنگ سایبرالکترونیک"، مفاهیم جنگ سایبری و جنگ الکترونیک و ارتباط بین آن‌ها را مورد بررسی قرار داده و به این نتیجه دست یافته‌اند که در سال‌های آینده، موفقیت در میدان جنگ دیجیتال، مستلزم ادغام جنگ سایبری و جنگ الکترونیک می‌باشد. [۵]

هیگ در مقاله‌ی خود با عنوان "جنگ الکترونیک در محیط فضای سایبر"، بیان می‌دارد که ترکیب طیف الکترومغناطیس و فضای سایبر، یک محیط عملیاتی نظامی جدید به نام حوزه سایبرالکترونیک را به وجود آورده و موجب همگرایی اقدامات جنگ الکترونیک و جنگ سایبر شده است که در این حوزه، عملیات سایبری و جنگ الکترونیک می‌بایست به صورت همگام و یکپارچه انجام شود. [۶]

۳- تعاریف و مفهوم‌شناسی

۳-۱- فضای سایبر

فضای سایبر، یک محیط الکترونیکی است که اطلاعات از طریق آن، تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود. در کنار چهار عرصه زمین، دریا، هوا و فضا، از حوزه سایبر به‌عنوان پنجمین عرصه قدرت یاد می‌شود. در طول هزاره‌ها و قرن‌های گذشته، تسلط بر حوزه‌های سرزمینی و قلمروهای فیزیکی، قدرت محسوب می‌شد و در حال حاضر نیز چنین است؛ اما طبق مطالعات راهبردی و باتوجه به سرعت رشد فناوری‌ها و توسعه فضای سایبر، در آینده نزدیک، حوزه برتر قدرت، فضای سایبر است. شکل (۱) رابطه فضای سایبر با سایر قلمروهای قدرت را نشان می‌دهد. [۱]



شکل ۱: رابطه فضای سایبر نسبت به سایر قلمروهای قدرت

۳-۲- جنگ سایبری

جنگ سایبری یک حمله سایبری است که توسط بازیگران دولتی علیه زیرساخت‌های سایبری، به‌عنوان بخشی از یک اردوکشی دولتی انجام می‌شود. جنگ سایبری، مؤلفه‌ای از عملیات سایبری است که قدرت سایبری را در خارج از قلمرو پدافند سایبری، برای تشخیص، تحذیر، منع و شکست دادن دشمنان انجام می‌شود. [۲]

۳-۳- جنگ الکترونیک

جنگ الکترونیکی اقدام نظامی است که شامل استفاده از انرژی الکترومغناطیسی و هدایت شده برای کنترل طیف الکترومغناطیسی یا حمله به دشمن است. جنگ الکترونیک نقش بسیار مهمی در هر عملیات نظامی ایفا می‌کند. تمام اجزای سرویس، جنگ الکترونیک را برای پشتیبانی از مأموریت‌ها هدایت و ادغام می‌کنند. جنگ الکترونیک به منظور ایجاد اختلال و افزایش زمان واکنش تصمیم‌گیری دشمن، با آتش‌کشنده ادغام و هماهنگ می‌شود. [۷]

جنگ الکترونیک از سه حوزه اصلی تشکیل شده است:

اقدامات پشتیبانی جنگ الکترونیک، اقدامات متقابل الکترونیکی (یا حمله الکترونیکی) و حفاظت الکترونیکی مهم‌ترین مسئله این است که در ست مانند جنگ الکترونیک، اطلاعات سیگنال نیز در طیف الکترومغناطیسی عمل می‌کند. اقدامات پشتیبانی جنگ الکترونیک و سیگنال‌های مأموریت‌های اطلاعاتی از منابع و روش‌های جمع‌آوری اطلاعات یکسان استفاده می‌کنند.

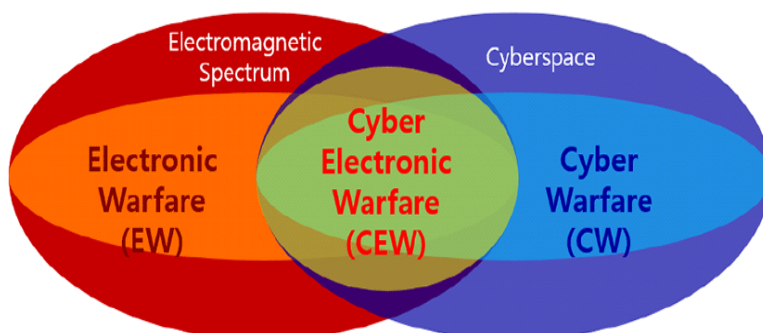
اقدامات متقابل الکترونیکی شامل استفاده از انرژی الکترومغناطیسی، انرژی هدایت‌شده یا سلاح‌های هدایت خانگی برای حمله به سیستم‌ها، تأسیسات یا تجهیزات الکترونیکی با هدف تخریب، خنثی کردن یا از بین بردن توانایی رزمی دشمن است. این شامل اقدامات انجام شده برای جلوگیری یا کاهش استفاده موثر دشمن از طیف الکترومغناطیسی، مانند پارازیت و فریب الکترونیکی، و همچنین استفاده از سلاح‌هایی است که از انرژی الکترومغناطیسی یا هدایت شده برای از بین بردن دارایی‌های الکترونیکی دشمن استفاده می‌کنند. [۷] [۸]

اقدامات متقابل الکترونیکی می‌تواند تهاجمی یا تدافعی باشد. فعالیت‌های تهاجمی عموماً با ابتکار نیروهای دو ست انجام می‌شود. مانند؛ ایجاد اختلال در رادار یا سیستم‌های فرماندهی و کنترل دشمن - استفاده از موشک‌های ضد تشعشع برای سرکوب سیستم دفاع هوایی دشمن - استفاده از تکنیک‌های فریب الکترونیکی برای گیج‌کردن سیستم‌های اطلاعاتی، نظارتی و شناسایی (ISR) دشمن و استفاده از سلاح‌های انرژی هدایت شده برای از کار انداختن تجهیزات یا توانایی دشمن. [۹]

۳-۴- جنگ الکترونیک سایبری

جنگ الکترونیک سایبری به یک اقدام نظامی اطلاق می‌شود که با استفاده از طیف الکترومغناطیسی، فضای سایبری از جمله فضای شبکه‌ی بی‌سیم دشمن را مختل، تخریب و کنترل می‌کند. [۹]

همانطور که در شکل (۲) نشان داده شده است، جنگ الکترونیک سایبری می‌تواند در جایی انجام شود که طیف جنگ الکترونیک و جنگ سایبری با یکدیگر همپوشانی دارند. به عبارت دیگر، جنگ الکترونیک سایبری (CEW) را می‌توان به عنوان مفهومی دانست که به عنوان باند فرکانس تهدید اصلی جنگ الکترونیک از رادار به منطقه ارتباطی گسترش یافته و فناوری اختلال شبکه سیمی جنگ سایبری به تدریج به یک فناوری اختلال شبکه بی‌سیم تبدیل خواهد شد. بنابراین، تخمین زده می‌شود که حوزه جنگ الکترونیک سایبری، جایی که فن‌آوری‌های جنگ الکترونیک و جنگ سایبری می‌توانند همگرا شوند، با پیشرفت این دو فناوری گسترش خواهد یافت. [۱۰] [۱۱]



شکل ۲: مفهوم جنگ الکترونیک سایبری (CEW)

۴- ویژگی‌های جنگ سایبری، جنگ الکترونیک و جنگ الکترونیک سایبری

ویژگی‌های جنگ سایبری، جنگ الکترونیک و جنگ الکترونیک سایبری به شرح زیر مقایسه و تحلیل می‌شوند. همانطور که از جدول (۱) مشاهده می‌شود، فناوری جنگ سایبری نسبت به جنگ الکترونیک در قابلیت‌های اختلال اطلاعات دارای مزیت است. به عبارت دیگر، کدهای مخرب (مثلاً پیام‌های نادرست، ویروس‌ها) می‌توانند به طور مداوم یا طولانی مدت اطلاعات فضای سایبری را دستکاری و مختل کنند. از سوی دیگر، فناوری مبتنی بر جنگ الکترونیک در قابلیت انتقال امواج رادیویی با قدرت بالا نسبت به جنگ سایبری برتری دارد. بنابراین، می‌تواند تهدیدات (مانند سیستم‌های فرماندهی و کنترل واقع در اعماق جهان) را از ده‌ها تا صدها کیلومتر در فضای طیف الکترومغناطیسی فیزیکی مورد حمله قرار دهد. جنگ الکترونیک سایبری می‌تواند یک فناوری کلیدی برای پاسخگویی به تهدیدات سایبری در حال تکامل باشد، زیرا می‌تواند با ترکیب نقاط قوت جنگ سایبری و فن‌آوری‌های جنگ الکترونیک، اثرات هم‌افزایی در فضای فیزیکی و شبکه‌های بی‌سیم (طیفی) و فضای سایبری ایجاد کند. [۱۱] [۱۲]

جدول ۱: ویژگی‌های جنگ سایبری، جنگ الکترونیک و جنگ الکترونیک سایبری

جنگ الکترونیک سایبری	جنگ الکترونیک	جنگ سایبری	
فضای سایبری + فیزیکی	فضای فیزیکی (فضای طیف)	فضای سایبری	هدف حمله
بدافزار + طیف الکترومغناطیسی با قدرت بالا	طیف الکترومغناطیسی با توان بالا	بدافزار	عامل حمله
فضای سایبری و انسداد سیستم (دراز مدت)	انسداد سیستم (کوتاه مدت)	آلودگی فضای سایبری (دراز مدت)	اثر حمله

۵- همگرایی بین فضای سایبر و طیف الکترومغناطیسی

استفاده از انرژی الکترومغناطیسی و عملیات در فضای سایبری برای جنگ مدرن ضروری است. نیروهای نظامی از شبکه‌های کامپیوتری بی‌سیم برای هماهنگ کردن عملیات، استفاده از حسگرهای هوا و زمین برای شناسایی و تعیین موقعیت دشمن، استفاده از رادار برای برقراری ارتباط با یکدیگر و استفاده از پارازیت‌های الکترونیکی برای کور کردن رادارهای دشمن یا مختل کردن ارتباطات آنها استفاده می‌کنند. با استفاده از روترهای بی‌سیم یا رادیوهای تاکتیکی که تقریباً بخشی از هر شبکه رایانه‌ای هستند، فضای سایبری و طیف الکترومغناطیسی اکنون یک محیط پیوسته و منسجم را تشکیل می‌دهند. طیف الکترومغناطیسی و فضای سایبری به عنوان یک محیط اطلاعاتی خاص، برای عملیات نظامی اساسی است، به طوری که ما باید آن را هم‌تراز با حوزه‌های سنتی زمین، دریا، هوا و فضا قرار دهیم. دریا، سالار گریز، رئیس عملیات نیروی دریایی ارتش آمریکا در این باره گفت: در واقع درگیری‌های آینده صرفاً با استفاده از طیف الکترومغناطیسی و فضای سایبری به دست نمی‌آید، بلکه در طیف الکترومغناطیسی و فضای سایبری پیروز می‌شود. [۱۳]

یکی از ویژگی‌های مهم فضای سایبری این است که سیستم‌های اطلاعاتی شبکه‌ای با استفاده از طیف الکترومغناطیسی و/یا اتصال سیمی در آن کار می‌کنند. فرآیندهای مختلف مدیریت اطلاعات الکترونیکی (جمع‌آوری داده‌های الکترونیکی، پردازش داده‌ها، ذخیره سازی داده‌ها و ارتباطات) در این سیستم‌ها در حال انجام است. همه دستگاه‌هایی که در طیف الکترومغناطیسی کار می‌کنند، در فضای نبرد در شبکه نیستند بلکه دستگاه‌های مستقل نیز وجود دارند (به عنوان مثال، حسگرهای بدون مراقبت، دستگاه‌های مختل‌کننده قابل مصرف، دستگاه‌های انفجار دست ساز کنترل شده رادیویی و غیره). بنابراین فضای سایبری با طیف الکترومغناطیسی برابری نمی‌کند بلکه فقط می‌تواند برای سیستم‌های الکترونیکی تحت شبکه اعمال شود. در نتیجه، دو حوزه - یعنی فضای سایبری و طیف الکترومغناطیسی - به یکدیگر نزدیک شده و بین آنها همگرایی وجود دارد.

فضای سایبری در سایر حوزه‌های زمین، دریا، هوا و فضا وجود دارد. استفاده از فناوری‌های الکترونیکی برای ایجاد فضای سایبری و نیز، استفاده از طیف الکترومغناطیسی است که فضای سایبری را از سایر حوزه‌ها متمایز نموده و آن را منحصر به فرد می‌کند. [۱۴]

یکی از ویژگی‌های اصلی فضای سایبری این است که نمی‌تواند بدون بهره‌برداری از طیف الکترومغناطیسی موجود وجود داشته باشد. علاوه بر این، شبکه‌های فناوری اطلاعات و ارتباطات نیز برای اتصال ضروری خود از طریق فرکانس رادیویی به طیف الکترومغناطیسی وابسته هستند. [۱۵]

امروزه در میدان نبرد، شبکه‌هایی از وسایل الکترونیکی (مانند؛ رادار، رادار، دستگاه‌های ناوبری، سیستم‌های شناسایی نبرد در میدان جنگ و رایانه‌ها) ایجاد شده‌اند که جدا کردن اجزای آنها بسیار دشوار است. لذا باید آنها را به هر طریقی به عنوان یک سیستم پیچیده که دارای یک محیط عملیاتی مشترک است تفسیر کنیم. در میدان

جنگ، این سیستم‌های شبکه از انرژی الکترومغناطیسی برای جمع‌آوری، ذخیره و انتقال داده‌ها و اطلاعات استفاده می‌کنند.

فضای سایبری و طیف الکترومغناطیسی بخشی از محیط اطلاعاتی هستند. «محیط اطلاعاتی به عنوان فضای سایبری و فیزیکی تعریف می‌شود که در آن اطلاعات دریافت، پردازش و منتقل می‌شود که شامل خود اطلاعات و سیستم‌های اطلاعاتی است».

محیط اطلاعاتی دارای سه بعد مرتبط با هم شامل بعد فیزیکی، بعد اطلاعاتی و بعد شناختی است. این محیط، عرصه عملیات اطلاعاتی است که در آن فعالیت‌های مبتنی بر اطلاعات در ابعاد فیزیکی، اطلاعاتی و شناختی انجام می‌شود. طیف الکترومغناطیسی و فضای سایبری در ابعاد فیزیکی و اطلاعاتی محیط اطلاعاتی قرار دارند. [۱۶]

۵-۱- عملیات الکترومغناطیسی سایبری

فعالیت‌های الکترومغناطیسی سایبری، فعالیت‌هایی هستند که برای تصاحب، حفظ و بهره‌برداری از مزیت‌ها در مقابل دشمنان در هر دو فضای سایبری و طیف الکترومغناطیسی و در عین حال جلوگیری و ممانعت از استفاده دشمن و هم‌چنین حفاظت از سیستم فرماندهی استفاده می‌شوند. [۱۶]

فعالیت ضروری الکترومغناطیسی سایبری؛ یکپارچه سازی و همگام سازی عملکردها و قابلیت‌های عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف برای تولید اثرات مکمل و تقویت‌کننده است. فعالیت‌های ناهماهنگ ممکن است منجر به درگیری و تداخل متقابل بین آنها و سایر نهادهایی شود که از طیف الکترومغناطیسی استفاده می‌کنند.

فعالیت‌های الکترومغناطیسی سایبری عبارتند از: عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف. لذا عملیات الکترومغناطیسی سایبری علاوه بر جنگ الکترونیک، دو قابلیت دیگر را نیز شامل می‌شود. [۱۶]

عملیات فضای سایبری استفاده از قابلیت‌های فضای سایبری است که هدف اصلی آن دستیابی به اهداف در فضای سایبری یا از طریق آن می‌باشد. عملیات فضای سایبری شامل سه عملکرد است: عملیات فضای سایبری تهاجمی، عملیات فضای سایبری دفاعی و عملیات شبکه اطلاعاتی.

عملیات مدیریت طیف؛ عملکردهای مرتبط با مدیریت طیف، تخصیص فرکانس، هماهنگی کشور میزبان و خط‌مشی است که برنامه‌ریزی، مدیریت و اجرای عملیات را در محیط عملیاتی الکترومغناطیسی در تمام مراحل عملیات نظامی ممکن می‌سازد.

در حالی که عملیات فضای سایبری به طور کامل بخشی از عملیات الکترومغناطیسی سایبری است، جنگ الکترونیک و اطلاعات سیگنال‌ها در محیط ارتباطات اطلاعاتی شبکه‌ای به عنوان حوزه‌های عملیات سایبری الکترومغناطیسی تفسیر می‌شوند.

هدف اساسی عملیات الکترومغناطیسی سایبری، اطمینان در استفاده از سیستم‌های ارتباطات الکترونیکی شبکه خودی و فرآیندهای موجود در آنها و همچنین شناسایی و کاهش قابلیت‌های مشابه دشمن است. این عملیات می‌تواند تهاجمی و تدافعی باشد.

عملیات تهاجمی الکترومغناطیسی سایبری یک کارکرد دوگانه دارد: شناسایی و همچنین تأثیرگذاری و تخریب سیستم‌های اطلاعات شبکه‌ای نیروهای مخالف. مهاجم با استفاده از تکنیک‌های عمدتاً غیرفعال و کنار زدن مقررات امنیت اطلاعات، سیستم‌های ارتباطی را شناسایی کرده، وارد شبکه‌های رایانه‌ای می‌شود و به پایگاه‌های اطلاعاتی دسترسی پیدا می‌کند و نرم‌افزارهای مخرب (بدافزار) را برای اصلاح و یا حذف اطلاعات مهم دشمن بکار می‌گیرد و می‌تواند سیستم را با داده‌های گمراه‌کننده بارگذاری کند.

عملیات دفاعی الکترومغناطیسی سایبری تمایل به اطمینان از دسترسی به اطلاعات و فرآیندهای مبتنی بر اطلاعات در سیستم‌های ارتباط اطلاعات شبکه خودی و اطمینان از استفاده مؤثر از این سیستم‌ها دارد که باعث به حداقل رساندن آسیب‌پذیری سیستم‌ها و کاهش تداخل‌های ناخواسته در بین آنها می‌شود. انطباق هماهنگ دفاع مؤثر این امکان را فراهم می‌کند که از سیستم‌های ارتباطی اطلاعات شبکه خودی در برابر انکار سرویس، دسترسی غیرمجاز، اختلال و غیره محافظت کنیم.

۶- روندها و نمونه‌هایی از جنگ الکترونیک سایبری

از سال ۲۰۱۴، کشورهای پیشرفته نظامی (ایالات متحده آمریکا، استرالیا، ژاپن، انگلستان، کانادا و غیره) تمایل به همگرایی و یکپارچه‌سازی عملیات سایبری و جنگ الکترونیک از نظر دکتین، سازمان، فناوری و غیره داشته و ابزارهای مختلف یکپارچه‌سازی جنگ الکترونیک سایبری را به کار می‌گیرند.

حمله نیروی هوایی اسرائیل به تأسیسات هسته‌ای در سوریه به نام "عملیات باغ (۲۰۰۷)" نمونه‌ای از جنگ الکترونیک سایبری است. حدود ۱۰ هواپیما (شامل جنگنده‌ی اف ۱۵ آی، جنگنده‌ی اف ۱۶ آی، یک جمع‌کننده‌ی اطلاعات الکترونیکی، یک هلیکوپتر و غیره) عملیات حمله به سوریه را انجام دادند که در نتیجه‌ی آن، سایت رادار سوریه با حملات الکترونیکی مانند اختلال و بمب‌های دقیق معمولی نابود شد. جنگنده‌ی اف ۱۵ آی متعلق به نیروی هوایی اسرائیل مجهز به سیستم جنگ الکترونیک اس‌پی‌اس-۲۱۱۰ اسرائیل الیسرا است که به داشتن نرم‌افزار جنگ الکترونیک سایبری به نام «سوتر» معروف است. این حمله هوایی غیرمعمول به تأسیسات نظامی سوریه توسط اسرائیل، که در سپتامبر ۲۰۰۷ انجام شد، علاقه جهانی را به تکنیک اختلال موسوم به sutter، برانگیخت. [۱۷] [۱۸]

نمونه‌ی دیگر از جنگ الکترونیک سایبری، سرنگونی یک هواپیمای بدون سرنشین توسط Krasukha-2,4 است که در جنگ داخلی روسیه انجام شده است (۲۰۱۵). Krasukha یک تجهیزات جنگ الکترونیکی از نوع وسیله نقلیه زمینی است که یک جمر پر قدرت برای مقابله با اهداف هوایی مانند هواپیماها، پهپادها و پهپادها محسوب می‌شود. کراسوخا همچنین به انجام عملیات ضد پهپاد برای حفاظت از پایگاه در اطراف پایگاه‌های نظامی روسیه در ارمنستان معروف است. [۱۹]

هک هواپیمای بدون سرنشین توسط ج.ا. ایران نیز یک مورد معروف در جنگ سایبرالکترونیک است. در سال ۲۰۱۱ یک پهپاد آمریکایی (لاکهد مارتن RQ-170) که در حال شناسایی یک تأسیسات هسته‌ای با استفاده از یک دستگاه جنگ الکترونیک سایبری بود، توسط ج.ا. ایران در نزدیکی شهر کاشمر هدایت و فرود آورده شد. در آوریل ۲۰۱۲، ج.ا. ایران موفق به استخراج داده‌های جمع‌آوری شده توسط این هواپیمای بدون سرنشین شد. [۲۰] [۲۱]

هک هواپیمای بدون سرنشین ایران نیز یک مورد معروف جنگ سایبری الکترونیکی است. در ۴ دسامبر ۲۰۱۱ یک پهپاد آمریکایی لاکهد مارتن RQ-170 توسط ایران در نزدیکی شهر کاشمر در شمال شرق ایران دستگیر شد. ایران اعلام کرد که یک پهپاد آمریکایی را که در حال شناسایی یک تأسیسات هسته‌ای با استفاده از یک دستگاه جنگ الکترونیک سایبری بود، هدایت و فرود آورده است. دولت ایالات متحده در ابتدا ادعاهای ایران را رد کرد، اما رئیس‌جمهور اوباما بعداً گزارشی دریافت کرد و متوجه شد که پهپاد آمریکایی سقوط کرده است و درخواست کرد که این پهپاد بازگردانده شود. در آوریل ۲۰۱۲، ایران مدعی شد که موفق به استخراج داده‌های جمع‌آوری شده توسط هواپیماهای بدون سرنشین شده است. [۲۰] [۲۱]

۷- فناوری و چشم‌انداز توسعه مورد نیاز جنگ الکترونیک سایبری

در میان فناوری‌های مورد نیاز برای جنگ الکترونیک سایبری، به فناوری‌های مهمی که باید در راستای روند رو به رشد تهدیدات، توسعه یابند، پرداخته می‌شود. [۲۲]

۷-۱- فناوری اختلال در پیام با استفاده از امواج الکترومغناطیسی

در حال حاضر، طیف فرکانسی که در آن تهدیدات هدف توسط جنگ الکترونیک و جنگ سایبری همپوشانی دارند، به عنوان یک باند ارتباطی شناسایی می‌شود. لازم است که دو فناوری بتوانند با «تشخیص/ انتقال امواج الکترومغناطیسی پر قدرت» و «دستکاری/ اختلال در اطلاعات» با توسعه‌ی فناوری جنگ الکترونیک سایبری توسط همگرایی قابلیت‌های جنگ سایبری، هم‌افزایی داشته باشند.

فناوری اختلال باند ارتباطی جنگ الکترونیک موجود عمدتاً شامل فناوری انتقال نویز است که باعث تداخل ارتباطی بی‌سیم می‌شود، اما اخیراً به تدریج در حال تبدیل شدن به فناوری جنگ الکترونیک سایبری است که می‌تواند پیام‌ها را با استفاده از فناوری فریب که باعث انتشار پیام‌های نادرست می‌شود، دستکاری کند. فناوری فریب، فناوری‌ای است که پیام اصلی را با تعدیل "قدرت سیگنال، فاز سیگنال، مدت زمان سیگنال" و غیره دستکاری می‌کند. درجه و محتوای دستکاری ممکن است بسته به تهدید هدف و هدف حمله متفاوت باشد.

۷-۲- فناوری تشخیص خودکار نقاط ضعف در شبکه‌های بی‌سیم

هسته فناوری جنگ الکترونیک سایبری می‌تواند شامل شناسایی خودکار و حمله به مخاطبین شبکه بی‌سیم باشد که در برابر امنیت، آسیب‌پذیر هستند. به جای تهدیدات حمله مجهز به تجهیزات رمزنگاری یا پروتکل‌های

خصوصی، یک مفهوم حمله‌ی هوشمند مورد نیاز است که به طور خودکار، نقاط قابل نفوذ آسیب‌پذیر را شناسایی کرده و کدهای مخرب را از طریق آنها اعمال کند. کدهای مخرب بارگیری شده از طریق نقطه‌ی آسیب‌پذیر به طور طبیعی از طریق شبکه دشمن پخش می‌شوند.

۷-۳- انتخاب تهدید واقعی و فناوری حمله سفارشی

سیستم‌های تسلیحاتی مجهز به گیرنده‌های GPS^۱ پهباد (هواپیماهای بدون سرنشین)، موشک‌های هدایت شونده با GPS و غیره (که پروتکل‌های آنها افشا شده یا به عنوان نقاط آسیب‌پذیر شناخته می‌شوند)، سیستم‌های شبکه بی‌سیم باز (تضعیف شده) و سیستم‌های ماهواره‌ای، به عنوان تهدید اصلی در جنگ الکترونیک سایبری، می‌توانند اهداف حمله‌ی واقع‌بینانه باشند. [۲۲] [۲۳]

۷-۳-۱- فناوری پیشرفته اختلال سیگنال ناوبری ماهواره‌ای

فناوری اختلال سیگنال ناوبری ماهواره‌ای برای مقابله با تهدید ناشی از سیگنال‌های ناوبری مورد نیاز است. اگر فناوری جنگ الکترونیک موجود، هواپیماهای بدون سرنشینی که توسط سیگنال‌های ناوبری ماهواره‌ای هدایت می‌شوند را از مدار خارج کند باعث سقوط آنها می‌شود. جنگ الکترونیک سایبری، پیام‌های ماهواره ناوبری را شناسایی و تحلیل می‌کند، پیام‌های نادرست (فریبنده) تولید می‌کند و تهدیدهایی را به مسیرهای خاص مخابره می‌کند.

۷-۴- فناوری اختلال کنترل رادیویی [۲۲] [۲۳]

فناوری اختلال کنترل رادیویی برای پاسخگویی فعال‌تر به تهدید حملات سایبری فیزیکی ناشی از سیگنال کنترل تیرانداز، کاملاً ضروری است. سیگنال‌های کنترل رادیویی بر خلاف سیگنال‌های ناوبری ماهواره‌ای در دسترس عموم، بر اساس سیگنال‌های پروتکل/کد خصوصی هستند. بنابراین، پس از تخمین این موضوع با استفاده از تکنیک‌های پیشرفته‌ی هوش مصنوعی (مانند یادگیری عمیق)، توسعه و به کارگیری فناوری جنگ الکترونیک سایبری که می‌تواند سیگنال‌های کنترل رادیویی را شناسایی (تحلیل) کند و پیام‌های نادرست تولید و ارسال کند، ضروری است.

۸- توسعه جنگ الکترونیک سایبری [۲۴]

میدان نبرد آینده یک جنگ شبکه‌ای خواهد بود که در آن تقریباً تمام سیستم‌های تسلیحاتی با استفاده از یک شبکه بیش از حد متصل به هم ارتباط دارند. در میدان نبرد آینده، جایی که زمین، دریا، هوا و فضای بیرونی توسط طیف فرکانس به هم متصل می‌شوند، جنگ الکترونیک و جنگ سایبری به تدریج با هم همپوشانی خواهند داشت و فناوری جنگ الکترونیک سایبری که این دو فناوری را همگرا می‌کند، برای پاسخ مؤثر به این مورد، نیاز است.

^۱ Global Position System

برای این منظور لازم است به جنگ سایبری-الکترونیکی به شیوه‌ای واقع‌بینانه و تدریجی نگاه شود. هنگام تجزیه و تحلیل موارد جنگ الکترونیک سایبری در خارج از کشور و سطح فناوری داخلی، تهدیدات هدفی که می‌توان با آنها مقابله کرد عبارتند از: "تهدیدات مجهز به گیرنده ناوبری ماهواره‌ای"، "پهپاد کوچک"، "پهپاد متوسط/بزرگ/سامانه ارتباطی ماهواره‌ای" و "شبکه فرماندهی و کنترل دشمن".

۹- نتیجه‌گیری

فضای سایبری و طیف الکترومغناطیسی بخشی از عملیات نظامی مدرن است. نیروهای نظامی از انواع مختلف دستگاه‌های الکترونیکی شبکه‌ای و سیستم‌های ارتباطی اطلاعاتی در میدان جنگ استفاده می‌کنند. استفاده از این سیستم‌های شبکه‌ای برای دستیابی به برتری عملیاتی ضروری است.

جنگ الکترونیک در طیف الکترومغناطیسی با استفاده از تاکتیک‌ها، تکنیک‌ها و رویه‌های تهاجمی و تدافعی به دستیابی برای برتری اطلاعاتی و موفقیت عملیات نظامی کمک می‌کند.

سیستم‌های اطلاعات الکترونیکی شبکه‌ای در فضای سایبری و طیف الکترومغناطیسی کار می‌کنند و یک محیط عملیاتی نظامی مشترک ایجاد می‌کنند. این محیط، حوزه الکترومغناطیسی سایبری است. در این حوزه، عملیات الکترومغناطیسی سایبری هماهنگ و یکپارچه انجام می‌شود. جنگ الکترونیکی که علیه سامانه‌های اطلاعاتی شبکه‌ای دشمن و یا برای حفاظت از سامانه‌های مشابه ما استفاده می‌شود، قابلیت اصلی این عملیات است.

در این پژوهش، فن‌آوری جنگ الکترونیک سایبری معرفی شد که فناوری انتقال امواج الکترومغناطیسی پر قدرت جنگ الکترونیک را با توجه به جامعه بیش از حد متصل و تهدیدات سایبری و گسترش منطقه میدان نبرد و فناوری دستکاری/اختلال پیام سایبری ترکیب می‌کند. جنگ و تحولات عمده‌ای که باید در راستای روند رو به رشد تهدیدات بر روی آنها متمرکز شود.

برای توسعه جنگ الکترونیک سایبری، لازم است ابتدا تهدیدات واقع‌بینانه و سیستم‌های تسلیحاتی که در برابر حملات جنگ الکترونیک سایبری آسیب پذیر هستند شناسایی شوند، فناوری‌های اصلی لازم استخراج و بر توسعه‌ی آنها تمرکز شود.

منابع:

- [۱] احمدرضا فرحبخت، دهقانی، "همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی"، فصلنامه امنیت ملی، سال نهم، شماره ۱۳، بهار ۱۳۹۸.
- [۲] سند دستورالعمل پدافند سایبری زیرساخت‌های صنعتی کشور، قرارگاه پدافند سایبری کشور، آذر ۱۴۰۰.
- [3] Syeon Kim, Cyber Electronic Warfare Technologies and Development Directions, **2021**. J. Korean Inst. Electromagn. Eng. Sci. **2021**; 32(2):119-126
- [4] MAJ Michael Senft, Convergence of Cyberspace Operations and Electronic Warfare Effects, **2016**, available at <http://cyberdefensereview.army.mil/DesktopModules>
- [5] Osman Askin,a, Riza Irmaka, Mustafa Avsevera,**2015**, Cyber Warfare and Electronic Warfare: Integration in the operational environment of the future, available at: <http://proceedings.spiedigitallibrary.org>
- [6] Zsolt Haig, Electronic Warfare In Cyberspace, **2015**, National University of Public Service, Budapest, Hungary, Available at: <https://www.researchgate.net/publication/288871386>
- [7] S. Kim, "CEW(Cyber Electronic Warfare) concept and application plan for military operation," Great Debate for Joint, Seoul, **2018**.
- [8] JP 3-13.1 Electronic warfare. July 9, **2019**. Joint Chief of Staff.
- [9] FM 3-36 Electronic warfare. 06 April **2021**. Headquarters, Department of the Army.
- [10] Electronic Warfare Joint Publications, JP, 3 -13.1 (**2019**). Google Scholar.
- [11] Stauffer, D., "Electronic Warfare: Bloodless Battles," Prospective, 34 (1), 23-26 (**2017**).
- [12] Wilson, JR, "Electronic Warfare: The Cat and Mouse Game Continues," Military & Aerospace Electronics, 24 (9), 10-25 (**2013**). Google Scholar.
- [13] Greenert J.: Wireless cyberwar, the EM spectrum, and the changing Navy. <http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrumchanging-navy/> (online, cit. **2015**)
- [14] The National Military Strategy for Cyberspace Operations. **2018**., Chairman of the Joint Chiefs of Staff. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (online, cit. **2015**-01-10)
- [15] JP 1-02 Department of Defense Dictionary of Military and Associated Terms. 08 November **2016**.
- [16] Kuehl, D.: From Cyberspace to Cyberpower: Defining the Problem. in: Cyberpower and National Security. ed. Kramer, F. D. et al., **2016**., 24-43 pp. ISBN-10: 1597974234
- [17] Golden, A., "Radar Electronic Warfare," American Institute of Aviation and Astronautics, Washington.
- [18] Farquharson, J., "Instruments of Darkness: The History of Electronic Warfare, 1939-1945," War In History, 14 (1), 127-129 (**2007**). <https://doi.org/10.1177/0968344506072134> Google Scholar
- [19] H Hildmann, E Kovacs, "A Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety " . **2019**.
- [20] Major, P., "Listening Behind the Scenes: BBC Broadcasting in East Germany and Reflections on the Cold War," History of the Cold War, 13 (2), 255-275 (**2016**). <https://doi.org/10.1080/14682745.2012.746840> Google Scholar
- [21] McBride, Jay, "Electronic Warfare in Vietnam," Marine Journal, (1), 39 (**2015**). Google Scholar
- [22] Wilson, JR, "Electronic Warfare as a Part of All Military Operations," Military & Aerospace Electronics, 25 (8), 8-17 (**2016**).
- [23] OA Hathaway, SJ Shapiro, The internationalists: How a radical plan to outlaw war remade the world. **2017** - books.
- [24] da Cruz, Cyber Mercenaries: A New Threat to National Security, **2020**

Advantages of using cyber electronic warfare in operational environments

Mehrdad Najafi Nokashti, Mohammad Reza Movhedi Sefat

Abstract

The future battlefield will be a hyper-connected network war. In the future battlefield where land, sea, air and outer space are connected by the frequency spectrum, the areas of electronic warfare and cyber warfare will gradually overlap. It means a cyber electronic warfare technology that converges. Cyber electronic warfare is a technology that can have a synergistic effect by integrating the ability to transmit high-power electromagnetic waves over long distances and the ability to manipulate/disrupt information (message) of cyber warfare.

There is an overlap between cyberspace and the electromagnetic spectrum, and it has multidisciplinary effects. Cyberspace and the electromagnetic spectrum create a common operating environment that can be called the cyber electromagnetic domain. Cyber electromagnetic domain is not meant to equate the terms of cyber space and electromagnetic spectrum, but it means that there is a significant overlap between them and the development of future technology is likely to increase this convergence. In this field, information technical activities are coordinated and integrated. These activities can be called cyber electromagnetic operations.

This article, while examining the concepts and consequences of the convergence of electronic warfare and cyber warfare and the requirements for its implementation in operational environments, introduced cyber electronic warfare technology according to the trend of expanding the frequency spectrum (from the point of view of electronic warfare and the battlefield area towards cyber space). and explains the development direction of cyber electronic warfare .

Keywords: cyber war, electronic war; cyber electronic warfare; Cyberelectronics, cyber electromagnetic warfare, network axis.