فصلنامه امنیت ملی
سال نهم، شماره ۳۱، بهار ۱۳۹۸
مقاله هشتم از صفحه ۱۹۹ الی ۲۱۹

همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی[۱]

احمدرضا فرحبخت[۲]

مهدی دهقانی[۳]

تاریخ دریافت: ۱۳۹۷/۱۰/۱۸ تاریخ پذیرش: ۱۳۹۷/۱۲/۰۹

چکیده:

جنگ الکترونیک و جنگ سایبری در حال تبدیل شدن به عناصر کلیدی صحنه نبرد هستند. تسلط بر طیف الکترومغناطیسی و سامانه‌های اطلاعاتی و استفاده مؤثر و هماهنگ از قابلیت‌های این دو حوزه، عامل برتری‌ساز و تعیین‌کننده در نبردهای آینده خواهد بود.شباهت‌ها و وجوه مشترک جنگ سایبری و جنگ الکترونیک، موجب همگرا شدن این دو عرصه شده است.

محققین در این پژوهش که از نوع کاربردی بوده و به روش توصیفی- تحلیلی با رویکرد اکتشافی صورت گرفته است، 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. برخی الزامات اجرایی همگرایی جنگ الکترونیک و جنگ سایبری عبارتند از: وجود ساختار سازمان یکپارچه در تمامی سطوح، ایجاد واحدهای سایبرالکترونیک در یگان‌های رزمی در سطح تاکتیک، طرح‌ریزی و عملیات مشترک تحت فرماندهی واحد و تشکیل تیم‌های تحقیقاتی مشترک برای دستیابی به سامانه‌ها و تسلیحات با قابلیت‌های ترکیبی سایبری و الکترونیکی.

کلیدواژه‌ها: جنگ سایبری، جنگ الکترونیک، همگرایی، سایبر الکترومغناطیس، سایبرالکترونیک

۱- مقاله علمی- پژوهشی می‌باشد.

۲- دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول)- ar.farahbakht@sndu.ac.i

۳- دانش آموخته دوره دکتری کامپیوتر دانشگاه امام حسین (ع)- drdehghani@ihu.ac.ir

قدمه:

جنگ الکترونیک و جنگ سایبری در حال تبدیل شدن به عناصر کلیدی صحنه نبرد هستند، به‌خصوص زمانی که عملیات نظامی وابستگی بیشتری به تفوق اطلاعاتی داشته باشد. تسلط بر طیف الکترومغناطیسی و سامانه‌های اطلاعاتی، فرمانروایی مطلق در میدان جنگ را به ارمغان خواهد آورد و مخاطرات ناشی از وابستگی عناصر صحنه نبرد به شبکه‌های ارتباطی و سامانه‌های اطلاعاتی را کاهش می‌دهد.

وجوه اشتراکات جنگ سایبری و جنگ الکترونیک در اصول و فرآیند اجرا و همچنین تأثیرات و پیامدهای نسبتاً مشابه آن‌ها در سازمان‌های نظامی، سبب همگرایی[1] بین دو عرصه شده است. استفاده مؤثر و هماهنگ از قابلیت‌های این دو حوزه، عامل برتری‌ساز و تعیین‌کننده در نبردهای آینده خواهد بود. کشورهای بهره‌مند از این دو عامل قادر خواهند بود تا نبردها را با حداقل تلفات انسانی و کمترین هزینه به نفع خود به پایان برسانند. در این مقاله، 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. در نهایت، الزامات ایجاد همگرایی در سازمان‌های نظامی بیان می‌گردد.

این مقاله از آن جهت اهمیت دارد که می‌تواند زمینه‌ساز 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. در صورت انجام نشدن این پژوهش، ضرورت و چگونگی همگرایی جنگ الکترونیک و جنگ سایبری در سطح راهبردی و عملیاتی و تاکتیکی مورد غفلت واقع شده و سازمان‌های نظامی را از قابلیت‌ها و فرصت‌های حاصل از آن، بی‌نصیب و یا کم‌بهره می‌سازد؛ بنابراین هدف از این پژوهش بررسی مفهوم و پیامدهای همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی می‌باشد. سؤال تحقیق عبارت است از این‌که مفهوم و پیامدهای همگرایی جنگ الکترونیک و جنگ سایبری چیست و الزامات اجرای آن در سازمان‌های نظامی کدامند؟

1-Convergence

مبانی نظری

پیشینه پژوهش: بر اساس بررسی‌های به عمل آمده توسط محققین، تحقیقات متعددی در خصوص همگرایی جنگ الکترونیک و جنگ سایبری انجام شده است. برخی از پژوهش‌هایی که به‌نوعی با عنوان و قلمرو موضوعی این پژوهش مرتبط بوده و محققین تاکنون به مقالات آن‌ها دست یافته‌اند، به شرح زیر می‌باشد:

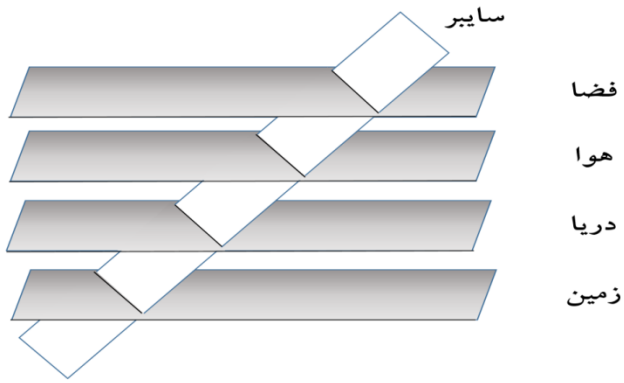
اسکین، ایرماکا و اوسورا[1] در مقاله‌ای تحت عنوان «یکپارچگی جنگ سایبری و جنگ الکترونیک در محیط عملیاتی آینده: جنگ سایبرالکترونیک»، مفاهیم جنگ سایبری و جنگ الکترونیک و ارتباط بین آن‌ها را مورد بررسی قرار داده و به این نتیجه دست یافته‌اند که در سال‌های آینده، موفقیت در میدان جنگ دیجیتال، مستلزم ادغام جنگ سایبری و جنگ الکترونیک می‌باشد (اسکین و همکاران، ۲۰۱۵).

«همگرایی تأثیرات عملیات سایبری و جنگ الکترونیک» عنوان مقاله‌ای است که سنفت[2] به رشته تحریر درآورده است. وی در پژوهش خود همگرا شدن اثرات عملیات سایبری و جنگ الکترونیک را با توجه به تعاملات آن‌ها را بر اساس مدل استاندارد تعامل سیستم باز[3]، 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. وی درک مشترک فرماندهان ارشد نظامی و کارکنان این دو حوزه را اولین گام برای دستیابی به همگرایی واقعی اثرات عملیات سایبری و جنگ الکترونیک می‌داند (سنفت، ۲۰۱۶).

هِیگ[4] در مقاله 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. وی نتیجه می‌گیرد که در این حوزه، عملیات سایبری و جنگ الکترونیک می‌بایست به‌صورت همگام و یکپارچه انجام شود (هِیگ، ۲۰۱۵).

1-Askin, Irmaka and Avsevera
2-Senft
3-Open Systems Interconnection (OSI)
4 -Haig

فضای سایبر: فضای سایبر، یک دامنه جهانی در محیط اطلاعاتی، متشکل از شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای، پردازنده‌ها، کنترل‌کننده‌ها و داده‌های مستقر در آن است *(JP 3-12, 2018, GL-4)*. در کنار چهار عرصه زمین، دریا، هوا و فضاء از حوزه سایبر به عنوان 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 با توجه سرعت رشد فناوری‌ها و توسعه فضای سایبر، در آینده نزدیک، حوزهٔ برتر قدرت، فضای سایبر است. گرچه فضای سایبر، یک قلمروی مستقل در کنار دیگر قلمروها است؛ اما قلمروهای فیزیکی را از طریق طیف الکترومغناطیس و شبکه‌های بی‌سیم و باسیم فراگرفته و با حرکت داده‌ها در طول مسیرهای انتقال از طریق لینک‌ها و گره‌ها در فضای سایبر و طیف الکترومغناطیس، سایر قلمروها را به هم پیوند می‌دهد؛ بنابراین ضمن اینکه فضای سایبر به تنهایی یک عرصه مستقل جنگ پذیرفته شده است؛ موفقیت عملیات‌ها در عرصه‌های فیزیکی نیز مستلزم توانمندی و آمادگی همه‌جانبه در فضای سایبر است. آزادی مانور در فضای سایبر، قابلیت‌های فرماندهان را برای آزادی عمل و اِعمال فرماندهی در حوزه‌های دیگر، افزایش می‌دهد. شکل ۱ رابطه فضای سایبر با سایر قلمروهای قدرت را نشان می‌دهد.



شکل ۱: رابطه فضای سایبر نسبت به سایر قلمروهای قدرت

جنگ سایبری[1]: جنگ سایبری عبارتست از حملات سایبری که به‌وسیله عوامل یک کشور علیه زیرساخت‌های سایبری کشور دیگر، در رابطه با یک سلسله عملیات جنگی انجام می‌شود (تعریف مشترک روسیه و آمریکا، ۲۰۱۴، ۴۳).

جنگ سایبری به سه طریق اتفاق می‌افتد: مقدمه و محرک[2] جنگ؛ بخشی از جنگ ترکیبی[3] و جنگ مستقل سایبری. شکل ۲، انواع حالت‌های جنگ سایبری را نشان می‌دهد.

شکل ۲: انواع حالت‌های جنگ سایبر

عملیات فضای سایبر[4]: عملیات فضای سایبر، به‌کارگیری قابلیت‌های فضای سایبری است که منظور اصلی آن، دستیابی به اهداف در فضای سایبر و یا از طریق آن است (*DOD 2018, 58 ,Dictionary*). ارتش آمریکا، مأموریت‌های فضای سایبر را به‌صورت زیر دسته‌بندی می‌کند: (*FM 3-12, 2017, 1-2*)

عملیات تهاجمی فضای سایبر[5]: عملیاتی که برای اعمال قدرت با استفاده از زور در فضای سایبر یا از طریق آن، انجام می‌شود.

عملیات دفاعی فضای سایبر[1]: عملیاتی که از فضای سایبر وزارت دفاع آمریکا یا فضای سایبر موافق با آمریکا؛ دفاع نموده و از توانایی استفاده از قابلیت‌های دوستانه فضای سایبر محافظت می‌کند.

1-Cyber Warfare
2 -Initiator
3-Hybrid Warfare
4-The Cyberspace Operations (CO)
5 -Offensive Cyberspace Operations (OCO)

عملیات شبکه اطلاعات وزارت دفاع[۲]: عملیاتی که برای طراحی، ایجاد، پیکربندی، امن‌سازی، کاربری، نگهداری و تعمیرات شبکه اطلاعات وزارت دفاع صورت می‌گیرد. شبکه اطلاعاتی وزارت دفاع یک زیرساخت اساسی جنگ برای موفقیت در تمام مراحل عملیات یکپارچه زمینی است که فرماندهی مأموریت، دقت آتش، جاسوسی، لجستیک و درمان از راه دور را فراهم نموده و از تمامی عملیات‌ها، پشتیبانی می‌کند. این رسانه بخشی از فضای سایبری وزارت دفاع و مستقل از آن است و ارتباط میان نیروها در حوزه‌های عملیاتی دیگر فراهم می‌کند. شبکه اطلاعات وزارت دفاع، مجموعه‌ای از قابلیت‌های اطلاعاتی و فرایندهای مربوط به جمع‌آوری، پردازش، ذخیره، انتشار و مدیریت اطلاعات مورد نیاز جنگجویان، سیاست‌گذاران و پشتیبانی از کارکنان است. *(JP 6-0 DODIN)* کارایی، حفاظت و دفاع از این شبکه و داده‌های مرتبط با آن، برای موفقیت فرماندهان در همه سطوح ضروری است.

اقدامات فضای سایبر[۳]: انجام مأموریت‌های فضای سایبر، مستلزم اقدامات مختلف برای ایجاد تأثیرات مشخص در فضای سایبر است. این اقدامات شامل حمله سایبری[۴]، دفاع سایبری[۵]، جاسوسی، نظارت و شناسایی سایبری[۶] و آماده‌سازی عملیاتی محیط[۷] است.

حمله سایبری: یک اقدام سایبری است که تأثیرات مختلف – مانند کاهش، قطع، تخریب یا دستکاری– برای منع استفاده از فضای سایبر ایجاد می‌کند و می‌تواند به صورت پنهان یا آشکار در قلمروهای فیزیکی صورت گیرد *(JP 3-12(R), 2013, II-5)*.

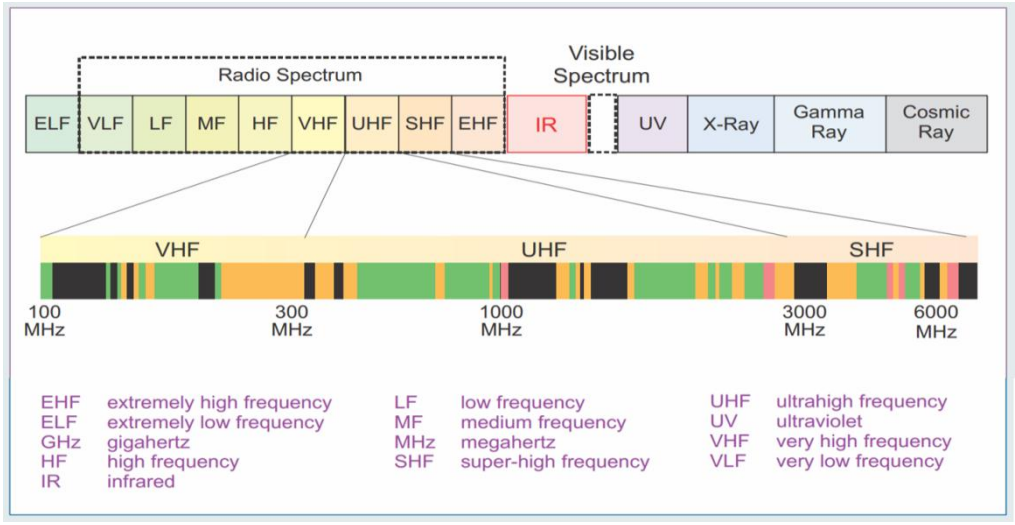
دفاع سایبری: شامل اقداماتی است که معمولاً درون فضای سایبر وزارت دفاع برای امن‌سازی، عملیاتی سازی و دفاع از شبکه اطلاعاتی وزارت دفاع در برابر تهدیدات خاص انجام می‌گیرد. اهداف دفاع سایبری شامل اقداماتی جلوگیری، آشکارسازی، تشخیص، مقابله و کاهش تأثیرات تهدیدات می‌باشد.

آماده‌سازی عملیاتی محیط: شامل فعالیت‌های سایبری غیراطلاعاتی برای برنامه‌ریزی و آماده‌سازی عملیات نظامی پیشرو است. این عملیات در فضای سایبر مطابق با اختیارات نظامی

1-Defensive Cyberspace Operations (DCO)
2-DOD Information Network (DODIN) Operations
3-Cyberspace Actions
4-Cyberspace Attack
5-Cyberspace Defense
6-Intelligence, Surveillance and Reconnaissance (ISR)
7-perational Preparation of the Environment (OPE)

انجام می‌شود؛ لیکن باید با سایر سازمان‌ها و نهادهای دولتی هماهنگ بوده و تعارض نداشته باشد (*FM 3-12, 2017, 1-9*).

عملیات طیف الکترومغناطیس[1]: قابلیت‌های بی‌سیمی فضای سایبر، از طیف الکترومغناطیس برای ایجاد لینک‌های رادیویی به عنوان رسانه مبادله اطلاعات استفاده می‌کند. محدوده فرکانس طیف الکترومغناطیس از صفر تا بی‌نهایت بوده و در ۲۶ باند فرکانسی تقسیم‌بندی شده است. طیف الکترومغناطیس در شکل۳ نشان داده شده است.

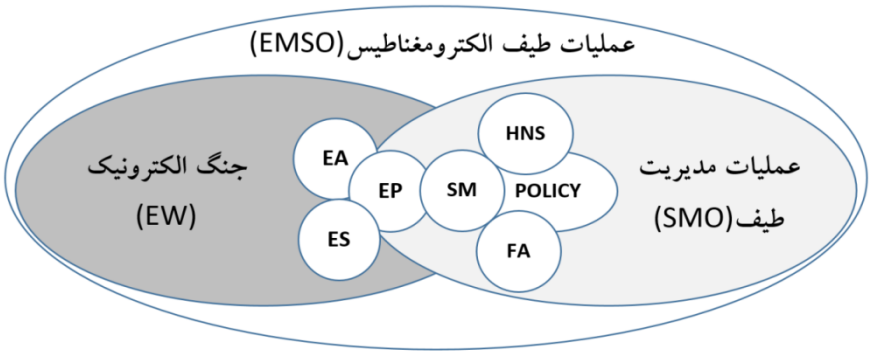


شکل ۳: طیف الکترومغناطیس (*FM 3-13.1, 2012, I- 2*)

عملیات طیف الکترومغناطیس شامل دو بخش عملیات مدیریت طیف[2] و جنگ الکترونیک است. عملیات مدیریت طیف، شامل اقدامات مرتبط با مدیریت طیف[3]، سیاست[4]، تخصیص فرکانس[5] و هماهنگی میزبانی بین‌المللی[6] می‌باشد. این اقدامات، طراحی، مدیریت و اجرای عملیات در محیط الکترومغناطیسی را در تمام مراحل عملیات نظامی ممکن می‌سازد (*FM 6-02,*

1-Electromagnetic Spectrum Operations (EMSO)
2-Spectrum Management Operations (SMO)
3-Spectrum Management (SM)
4-Policy
5-Frequency Assignment (FA)
6-Host Nation Coordination (HNS)

(*2014, 1-9*. عملیات مدیریت طیف، از عملیات جنگ الکترونیک و جنگ سایبری پشتیبانی نموده و اجرای آن‌ها را ممکن می‌نماید. شکل ۴، عملیات طیف الکترومغناطیس را نشان می‌دهد.



شکل ۴: عملیات طیف الکترومغناطیس (*FM 3-12, 2017, 1-25*)

جنگ الکترونیک[1]: طبق تعریف به فعالیت‌هایی شامل استفاده از طیف الکترومغناطیس یا انرژی هدایت‌شده برای کنترل طیف، حمله دشمن یا جلوگیری از حمله دشمن از طریق طیف اطلاق می‌شود***(FM 3-12, 2017, 1-25)***. جنگ الکترونیک می‌تواند از طریق هوا، دریا، زمین و فضاء به‌وسیله سامانه‌های انسانی و غیرانسانی به‌کار گرفته شود.

استفاده گسترده نیروهای نظامی از سامانه‌های الکترونیکی و طیف امواج الکترومغناطیسی در انواع تجهیزات و جنگ‌افزارها و به‌کارگیری آن‌ها در نبردهای امروزی به‌عنوان یک اقدام راهبری و تاکتیکی محسوب شده و بدون اغراق در معادلات نظامی دنیا، جزء پارامترهای تعیین‌کننده است.

بخشی از جنگ الکترونیک، بهره‌برداری از طیف الکترومغناطیس منتشر شده توسط دشمن برای پی بردن به اهداف، توانایی‌ها و در نهایت استفاده از نقاط ضعف برای ضربه زدن به سامانه‌های تسلیحاتی و مخابراتی دشمن و دستیابی به مقاصد خود می‌باشد.

تعیین دقیق موقعیت اهداف نظامی، هدایت هوشمند موشک‌های دوربرد و راهبردی به‌سوی اهداف از پیش تعیین شده، با استفاده از سامانه‌های الکترونیکی و حساسه‌های ویژه جنگ الکترونیک، در شبکه‌های فرماندهی و کنترل نیروهای مسلح، نقش و جایگاهی راهبردی و حیاتی دارد. کمینه کردن کارایی آن دسته از تسلیحات و ادوات نظامی دشمن که در عملکرد آن‌ها

1-Electronic warfare (EW)

تجهیزات الکترونیکی نقش حیاتی دارند از جمله اقدامات جنگ الکترونیک می‌باشد؛ بنابراین توان اطلاعاتی و عملیاتی جنگ الکترونیک (سخت‌افزاری و نرم‌افزاری)، بخشی از توان رزمی نیروهای مسلح هر کشور محسوب می‌شود.

اقدامات جنگ الکترونیک: به‌طور کلی اقدامات جنگ الکترونیک سه دسته زیر را در برمی‌گیرد:

تهاجم الکترونیکی[۱]: استفاده از انرژی الکترومغناطیس؛ انرژی هدایت شده یا تسلیحات ضد تشعشع رادیویی برای حمله به اشخاص، امکانات یا تجهیزات، با اهداف کاهش، خنثی‌سازی یا تخریب قابلیت‌های جنگی دشمن بوده و نوعی آتش[۲] محسوب می‌شود.

حفاظت الکترونیکی[۳]: اقداماتی که برای حفاظت از اشخاص، امکانات یا تجهیزات در مقابل تأثیرات استفاده دوستانه یا دشمن از طیف الکترومغناطیس که قابلیت‌های جنگی خودی را کاهش، خنثی یا تخریب می‌کند.

پشتیبانی جنگ الکترونیک[۴]: فعالیت‌هایی است که توسط یا تحت کنترل مستقیم یک فرمانده عملیاتی با اهداف جستجو، ره‌گیری، شناسایی و تعیین موقعیت منابع انرژی الکترومغناطیسی دشمن، به‌منظور تشخیص فوری تهدید، هدف‌گیری، طراحی و اجرای عملیات‌های بعدی انجام می‌شود.

همگرایی جنگ سایبری و جنگ الکترونیک: جنگ سایبری و جنگ الکترونیک، شباهت‌ها و اشتراکات قابل توجهی با یکدیگر دارند. اقدامات جنگ سایبری و جنگ الکترونیک هر دو بر سه رکن تقریباً مشابه شامل تهاجم، دفاع و پشتیبانی استوار هستند (سنفت، ۲۰۱۶). این ارکان در عملیات فضای سایبر، با عناوین عملیات تهاجم سایبری، عملیات دفاع سایبری و عملیات پشتیبانی سایبری و در جنگ الکترونیک با عناوین اقدامات تهاجم الکترونیکی[۵]، حفاظت الکترونیکی[۶] و پشتیبانی جنگ الکترونیک[۷] نام برده می‌شوند. هریک از این اقدامات در حوزه الکترونیک و سایبر، پیامدهای مشابهی را در پی دارند. به عنوان مثال تهاجم الکترونیکی به دنبال دستیابی به ممانعت[۸]،

1-Electronic Attack (EA)
2-Fires
3-Electronic Protection (EP)
4-Electronic Warfare Support (ES)
5-Electronic Attack (EA)
6-Electronic Protection (EP)
7-Electronic Warfare Support (ES)
8-Deny

اختلال[1]، تخریب[2]، کاهش عملکرد[3] و فریب[4] سامانه‌های رادیویی دشمن است. تهاجم سایبری نیز به دنبال اثرات مشابه است؛ اما هدف‌گیری آن بیشتر بر روی شبکه‌ها و سامانه‌های رایانه‌ای و برنامه‌های کاربردی است. همگرایی این دو حوزه، ادغام فعالیت‌های سایبری و الکترومغناطیسی را در قالب «فعالیت‌های سایبر الکترومغناطیس[5]» شکل می‌دهد. این همگرایی تأثیرات جنگ سایبری و جنگ الکترونیک را در تمامی مراحل عملیات نظامی، ارتقاء می‌بخشد.

در چند سال اخیر، نقش و اهمیت این همگرایی، بیشتر مورد توجه قرار گرفته و در این راستا کنفرانس‌های سالانه بین‌المللی همگرایی جنگ الکترونیک و جنگ سایبر برگزار می‌گردد. با این حال در اغلب کشورها، سازمان‌های نظامی که انجام اقدامات جنگ الکترونیک و جنگ سایبری را بر عهده دارند، از یکدیگر جدا هستند و ساختار سازمانی، تجهیزات و روش‌های عملیاتی آن‌ها متفاوت است؛ اما سازمان‌های نظامی کشورهای دارای قدرتمند در عرصه‌های سایبر و الکترونیک، اثربخشی بیشتر این دو حوزه را در همگرایی و تعامل بین آن‌ها دریافته‌اند. ارتش آمریکا در سال ۲۰۱۴، همگرایی جنگ الکترونیک و جنگ سایبری را به صورت جدی و عملیاتی مورد توجه قرار داده و در این راستا دستورالعمل اجرایی *FM 3-38*[6] با عنوان فعالیت‌های سایبر الکترومغناطیس[7] را صادر نمود. در آوریل سال ۲۰۱۷، دستورالعمل اجرایی *FM 3-12* را با موضوع «عملیات سایبری و جنگ الکترونیک ارتش[8]» به عنوان نسخه کامل‌تر و جایگزین *FM 3-38* توسط ارتش آمریکا منتشر شد. این دستورالعمل تاکتیک‌ها و فرآیندهای هماهنگی و ادغام عملیات فضای سایبر و جنگ الکترونیک ارتش آمریکا برای پشتیبانی از عملیات یکپارچه زمینی و عملیات‌های مشترک را ارائه می‌دهد (*FM 3-12, 2017, v*).

وزارت دفاع انگلستان[9] نیز همگرایی جنگ الکترونیک و جنگ سایبری را مورد توجه قرار داده در فوریه ۲۰۱۸، یادداشت دکترین مشترک ۱۰۱/۱۸ با عنوان فعالیت‌های سایبر و الکترومغناطیس[10][11]

1-Disrupt
2-Destroy
3-Degrade
4-Deceive
5-Cyberspace Electromagnetic Activities (CEMA)
6-United States Army Field Manuals
7-Cyber Electromagnetic Activities (CEMA)
8-Army Cyberspace and Electronic Warfare Operations
9-UK Ministry of Defence
10-Joint Doctrine Note 1/18 (JDN 1/18)
11-Cyber and Electromagnetic Activities

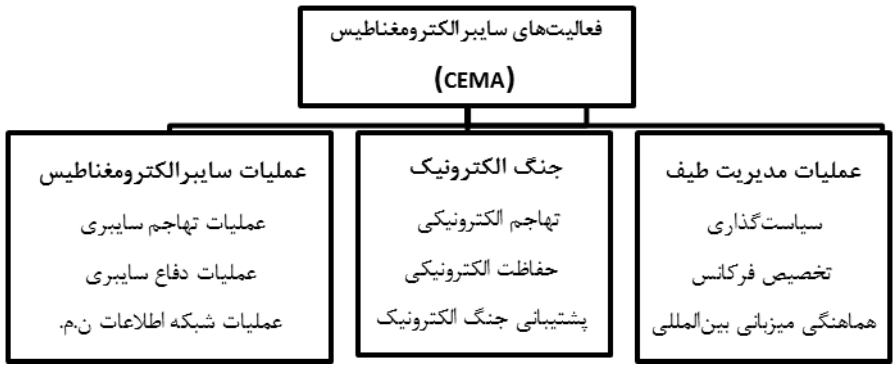
را توسط مرکز توسعه مفاهیم و دکترین[1]، منتشر نمود. در این سند، چشم‌انداز فعالیت‌های سایبر الکترومغناطیس[2] وزارت دفاع انگلستان این‌گونه بیان شده است: همگام‌سازی و هماهنگ‌سازی[3] اقدامات سایبری و الکترومغناطیسی، برتری عملیاتی را فراهم می‌کند که موجب آزادی حرکت و عمل برای خودی و همزمان منع و کاهش استفاده دشمن از محیط الکترومغناطیس و فضای سایبر می‌گردد.*(JDN 1/18, 3)*

در جمهوری اسلامی ایران نیز فرماندهی سایبرالکترونیک، برای انجام عملیات فضای سایبر و جنگ الکترونیک به صورت یکپارچه و در قالب یک سازمان و فرماندهی واحد تشکیل شد.

فعالیت‌های سایبر الکترومغناطیس: ادغام فعالیت‌های سایبری و الکترومغناطیسی در تمام مراحل عملیات، کلید دستیابی و حفظ آزادی عمل در فضای سایبر و طیف الکترومغناطیس برای نیروهای خودی و در عین حال ممانعت از آن برای دشمنان و معارضان است. فعالیت‌های سایبر الکترومغناطیس، قابلیت‌ها را در سراسر حوزه‌ها و عملیات‌های نظامی همگام نموده و اثرات مکمل در فضای سایبری و طیف الکترومغناطیس و از طریق آن‌ها را به حداکثر می‌رساند.

در تعریف وزارت دفاع آمریکا، فعالیت‌های سایبر الکترومغناطیس عبارت است از فرآیند طرح‌ریزی، ادغام و هماهنگ‌سازی عملیات فضای سایبری و جنگ الکترونیک، برای پشتیبانی از عملیات یکپارچه نظامی. این فعالیت‌ها در نمودار ۱ ترسیم شده است *(ADRP 3-0)*.

نمودار ۱: ترسیم فعالیت‌های سایبر الکترومغناطیس طبق تعریف وزارت دفاع آمریکا



1-The Development, Concepts and Doctrine Centre (DCDC)
2-The CEMA Vision
3-The synchronisation and coordination

اما طبق تعریف وزارت دفاع انگلستان، فعالیت‌های سایبر الکترومغناطیس عبارت است از: همگام‌سازی و هماهنگ‌سازی فعالیت‌های تهاجمی، دفاعی، اطلاع‌رسانی[1] و توانمندساز[2] در سراسر محیط الکترومغناطیس و فضای سایبر. شکل ۵ این فعالیت‌ها را نشان می‌دهد *(JDN 1/18, 13)*.

شکل ۵: فعالیت‌های سایبر الکترومغناطیس طبق تعریف وزارت دفاع انگلستان

نمونه‌هایی از همگرایی جنگ الکترونیک و جنگ سایبر: در بین جنگ‌های صورت گرفته تا به امروز، جنگ خلیج‌فارس اولین و مؤثرترین نمونه از جنگ‌های متعارف است که توسط جنگ سایبرالکترونیک پشتیبانی شد. در این جنگ که نقطه عطفی برای مفهوم جنگ سایبرالکترونیک محسوب می‌شود، مؤتلفین با بهره‌گیری از اقدامات همزمان سایبری و جنگ الکترونیک به راحتی موقعیت برتر را به دست آوردند. آن‌ها توانستند ویروس‌های رایانه‌ای را به سامانه یکپارچه دفاع هوایی عراق منتقل نمایند. این ویروس‌ها که به صورت کنترل از راه دور فعال می‌شدند، سامانه

1-Inform activities
2-Enabling activities

حمل و نقل هوایی عراق را پیش از حمله هوایی ارتش آمریکا فرو ریختند. پس از آن سامانه‌های دفاعی منطقه تحت فشار مستمر موشک‌های ضد تشعشع هارم[1] قرار گرفته و تخریب شدند. بدین ترتیب در حالی که هواپیماهای ایالات‌متحده در بغداد پرواز می‌کردند، سامانه دفاع هوایی عراق نتوانست فعال شود. همچنین هماهنگی عملیات فرماندهان عراق با بهره‌گیری از اطلاعات جمع‌آوری‌شده شناسایی و مختل گردید و عملیات متحدان با تلفات انسانی و تجهیزاتی اندک انجام شد.

نمونه دیگر از اقدامات سایبرالکترونیک در ۶ فوریه ۲۰۰۷، توسط رژیم صهیونیستی در عملیات ارچارد[2] علیه سوریه اتفاق افتاد. در این عملیات، نیروی هوایی رژیم صهیونیستی چندین دقیقه وارد حریم هوایی سوریه شد و یک راکتور هسته‌ای را بمباران کرد. تحقیقات بعدی نشان داد که سامانه دفاع هوایی سوریه قبل از عملیات توسط سرویس نظامی رژیم صهیونیستی هک شده و تصویر هوایی فریب به کاربران رادار سوری نمایش داده شده است. رادارها نیز در نزدیکی مرز با ترکیه، از طریق برنامه‌های جنگ الکترونیک مختل شده بودند (اسکین و همکاران، ۲۰۱۵).

واحدهای سایبرالکترونیک در یگان‌های رزمی: همگرایی در حال افزایش از حوزه‌های الکترونیکی و سایبری، تغییرات قابل توجهی را در سازمان‌های رزمی و شیوه‌های نبرد (دَس[3]، ۲۰۱۷) به وجود آورده است. اجرای اقدامات سایبری و الکترونیکی در رزم، مستلزم وجود واحدهای سایبرالکترونیک در ساختار سازمان‌های رزمی است. ارتش آمریکا اعلام کرده است که در سازمان‌دهی مجدد خود، چندین طرح برای ادغام فناوری‌ها، قابلیت‌ها و مفاهیم، در سازمان‌ها و واحدهای عملیاتی را در پیش رو دارد. در همین راستا، به‌منظور فراهم نمودن پشتیبانی مداوم، پاسخگو و به موقع در جنگ الکترونیک و جنگ سایبری تهاجمی، این ارتش به دنبال تشکیل واحدهای سایبرالکترونیک در تمامی واحدهای عملیاتی برای یکپارچه‌سازی فعالیت‌های سایبری و جنگ الکترونیک است (پامرلئو[4]، ۲۰۱۷).

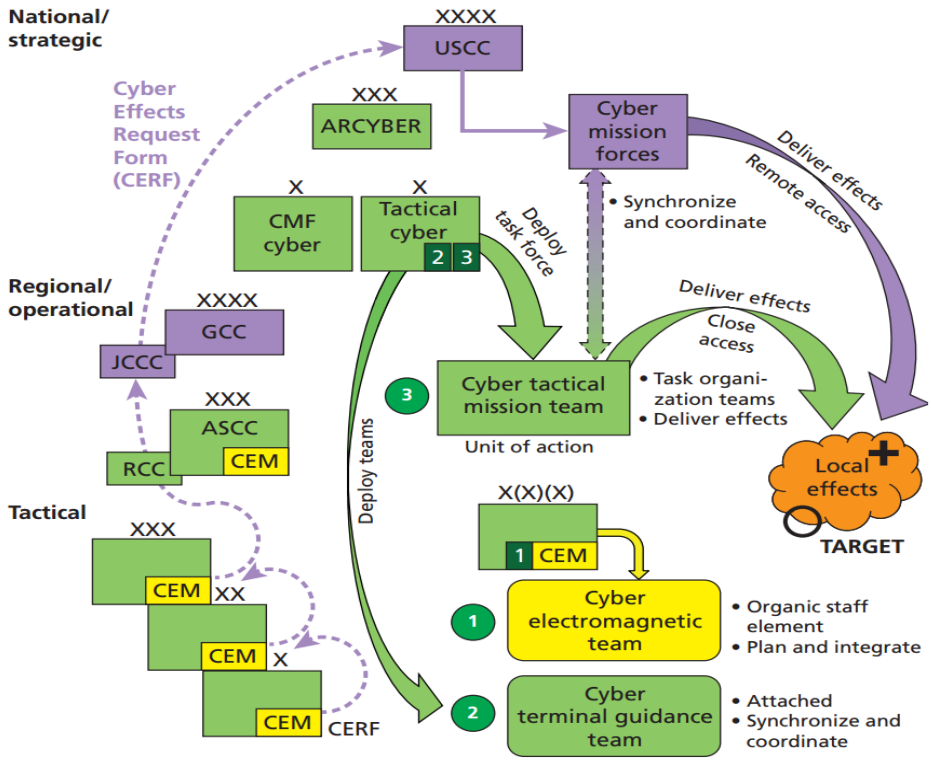
شکل ۶ ساختار سلسله مراتبی سازمان سایبرالکترونیکی ارتش آمریکا را نشان می‌دهد. در این ساختار، تیم سایبر الکترومغناطیس[5] در سطح تیپ[1]، لشکر[2] و سپاه[3] برای اجرای اقدامات جنگ

1-High speed Anti-Radiation Missile (HARM)
2-Orchard Operation
3-Das
4-Pomerleau
5-Cyber Electromagnetic Team (CEM)

سایبری و جنگ الکترونیک در نظر گرفته شده است. درخواست اقدام/تأثیرات سایبری به صورت سلسله مراتبی از سطوح تاکتیکی با کاربرگه درخواست فعالیت سایبری[۴] به مرکز سایبر منطقه‌ای[۵] در سطح منطقه‌ای/عملیاتی[۶] و از آنجا به فرماندهی سایبر ایالات‌متحده[۷] در سطح ملی/راهبردی[۸] منعکس می‌گردد. فرماندهی سایبر ایالات‌متحده به نیروهای مأموریت سایبر[۹] فرمان/مجوز می‌دهد که اقدامات سایبری را به صورت دسترسی راه دور[۱۰] یا توسط تیم‌های مأموریت تاکتیکی سایبر[۱۱] به صورت دسترسی نزدیک[۱۲] بر روی اهداف اجرا نمایند.

از ویژگی‌های این ساختار، می‌توان به مواردی همچون سلسله مراتبی بودن اقدامات و اتصال هر سطح به سطوح بالاتر، تمرکز بر اقدامات محلی، انجام اقدامات سایبری با دسترسی نزدیک و دور، همگامی و هماهنگی بین واحدهای نظامی، مشترک و شرکت‌های پشتیبان و به‌کارگیری افراد سایبری و انجام اقدامات سایبری در سطوح مختلف تاکتیکی (سپاه، لشکر و تیپ) اشاره نمود.

1-Brigade = X
2-Division = XX
3-Corps = XXX
4-Cyber Effects Request Form (CERF)
5-Regional Cyber Center (RCC)
6-Regional/Operational
7-United States Cyber Command (USCC)
8-National/Strategic
9-Cyber Mission Force (CMF)
10-Remote Access
11-Cyber Tactical Mission team
12-Close Access



شکل ۶: ساختار سازمان سایبرالکترونیکی ارتش آمریکا (پورشه[1]، ۲۰۱۷: ۶۵)

روش تحقیق:

پژوهش حاضر از نوع کاربردی بوده و روش آن توصیفی- تحلیلی با رویکرد اکتشافی است و در زمره تحقیقات کیفی دسته‌بندی می‌گردد. داده‌های کیفی این تحقیق از مطالعه منابع و مطالعات پژوهش‌های علمی و با استفاده از روش پژوهش کیفی فراترکیب[2] جمع‌آوری گردید. رویکرد فراترکیب نوعی مطالعه کیفی است که اطلاعات و یافته‌های استخراج شده از مطالعات کیفی دیگر با موضوع مشابه و مرتبط را بررسی می‌کند. در نتیجه نمونه مورد نظر برای فراترکیب از مطالعات کیفی منتخب و بر اساس ارتباط آن‌ها با سؤال پژوهش ساخته می‌شود. فراترکیب با فراهم کردن نگرشی سیستماتیک برای محققان، از طریق ترکیب مطالعات کیفی گوناگون، به کشف موضوعات

1-R. Porche
2-Meta-Synthesis

و استعاره‌های جدید و اساسی می‌پردازد و با این روش، دانش جاری را ارتقاء می‌دهد و دید جامع و گسترده‌ای نسبت به مسائل ایجاد می‌کند (کشتکار، ۱۳۹۵: ۱۶۵).

سه فاز اصلی را برای فراترکیب به شکل زیر ارائه می‌کنند: انتخاب مطالعات بر اساس جستجوی سیستماتیک و گزینش نهایی؛ ترکیب یافته‌ها بر اساس شباهت‌ها و اختلافات و ارائه تلفیقی یافته‌ها در دسته‌بندی گروهی (ساندلوسکی و باروسو[1]،۲۰۰۷)

در این پژوهش، محققین با مطالعه و واکاوی بیش از ۷۰ مقاله علمی و اسناد رسمی قابل دسترس کشورهای منتخب در زمینه‌های جنگ الکترونیک و جنگ سایبر و همگرایی آن‌ها، اطلاعات اصلی مورد نیاز را از بین ۲۰ مقاله علمی پژوهشی یا سند معتبر مرتبط با قلمرو موضوع استخراج نمودند. سپس با روش‌های خبرگی و منطقی به تحلیل و تلفیق یافته‌های حاصل از مطالعات کیفی پرداخته و یافته‌های جدید را ارائه نمودند. نتایج حاصله به تعداد محدودی از خبرگان این حوزه که در دسترس بودند، ارائه شد و نظرات تکمیلی اصلاحی و یا انتقادی آن‌ها دریافت و در ارزیابی نتایج اِعمال گردید.

تجزیه و تحلیل:

جنگ سایبری و جنگ الکترونیک از جنبه‌های مختلف به هم شبیه بوده و یا حداقل اشتراکات و همپوشانی‌هایی با یکدیگر دارند. در این مقایسه، وجوه تشابه و اشتراک اقدامات جنگ الکترونیک و جنگ سایبر قابل مشاهده است.

جدول ۱: مقایسه اقدامات جنگ الکترونیک و جنگ سایبری

جنگ الکترونیک	جنگ سایبری
اقدامات تهاجم الکترونیکی • نفوذ الکترونیکی • فریب الکترونیکی • اختلال الکترونیکی[2] • تسلیحات الکترومغناطیسی • تسلیحات هدایت شونده با حساسه‌های الکترونیکی	**اقدامات تهاجم سایبری** • نفوذ سایبری • فریب سایبری • کاهش سطح کارایی و منع سرویس • تسلیحات سایبری • تخریب سایبری

1-SANDELOWSKI and BARROSO
2-Electronic Jamming

جنگ الکترونیک	جنگ سایبری
اقدامات حفاظت الکترونیکی • سازگاری الکترومغناطیسی[1] • مقاوم‌سازی سخت‌افزاری سامانه‌ها[2] • کنترل انتشار[3] • مدیریت طیف الکترومغناطیس	**اقدامات دفاع سایبری** • اقدامات داخلی دفاعی[4]: عملیات دفاع از شبکه • اقدامات واکنشی عملیات دفاع سایبری[5]
اقدامات پشتیبانی جنگ الکترونیک • امنیت الکترونیکی[6] • جاسوسی/جمع‌آوری اطلاعات سیگنالی[7]، الکترونیکی[8]، مخابراتی[9] و تصویری[10] • هشداردهی تهدیدات[11] • شناسایی الکترونیکی • جهت‌یابی[12] و موقعیت‌یابی[13]	**اقدامات پشتیبانی جنگ سایبری** • امنیت سایبری[14] • جاسوسی/جمع‌آوری اطلاعات سایبری[15] • نظارت/مراقبت[16] • شناسایی[17] • آماده‌سازی عملیاتی محیط[18]

1-Electromagnetic Compatibility
2-Electromagnetic Hardening
3-Emission Control
4-Internal Defensive Measures
5-DCO Response actions
6-Electronics Security
7-Signal Intelligence (SIGINT)
8-Electronic Intelligence (ELINT)
9-Communication Intelligence (COMINT)
10-Image Intelligence (IMINT)
11-Threat Warning
12-Direction Finding
13-Position/Point Finding
14-Cyberspace Security
15-Cyberspace Intelligence
16-Surveillance
17-Reconnaissance
18-Operational Preparation of the Environment (OPE)

حوزه‌های جنگ الکترونیک و جنگ سایبر از جنبه‌های زیر دارای تشابه و همپوشانی هستند:

۱- مبانی، فناوری‌ها، سامانه‌ها و تجهیزات

۲- اقدامات و فرایندها

۳- کارکردها و پیامدها

این وجوه تشابه و اشتراک، موجب همگرایی جنگ الکترونیک و جنگ سایبر در سازمان‌های نظامی پیشرفته برای نیل به اهداف زیر شده است:

هم‌افزایی و بهره‌وری در ساختار سازمانی، فرآیندها، منابع انسانی و تجهیزاتی

ایجاد قابلیت‌های جدید و ارتقاء یافته

افزایش اثربخشی اقدامات در صحنه نبرد

الزامات تحقق همگرایی جنگ الکترونیک و جنگ سایبری در سازمان‌های نظامی عبارتند از:

۱. وجود ساختار سازمان یکپارچه در تمامی سطوح

۲. ایجاد واحدهای سایبرالکترونیک در یگان‌های رزمی در سطح تاکتیک

۳. طرح‌ریزی و عملیات مشترک تحت فرماندهی واحد

۴. تشکیل تیم‌های تحقیقاتی مشترک برای دستیابی به سامانه‌ها و تسلیحات با قابلیت‌های ترکیبی سایبری و الکترونیکی

نتیجه‌گیری:

این مقاله به دنبال شناخت همگرایی حوزه‌های جنگ سایبری و جنگ الکترونیک و الزامات اجرای آن در سازمان‌های نظامی بود. یافته‌های پژوهش نشان داد که وجوه تشابه و اشتراکات این دو حوزه در فناوری و فرآیند اجرا و همچنین تأثیرات و پیامدهای نسبتاً مشابه آن‌ها در سازمان‌های نظامی، سبب همگرایی بین دو عرصه شده است و با پیشرفت فناوری‌های ارتباطات و اطلاعات، طیف الکترومغناطیس و فضای سایبر به هم وابسته‌تر شده و در نتیجه همگرایی جنگ الکترونیک و جنگ سایبری نیز بیشتر می‌گردد.

همچنین همگرایی جنگ الکترونیک و جنگ سایبری 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. این همگرایی مستلزم فراهم شدن الزاماتی از قبیل ساختار سازمان یکپارچه در تمامی سطوح، ایجاد واحدهای سایبرالکترونیک در یگان‌های رزمی در سطح تاکتیک، طرح‌ریزی و عملیات مشترک تحت فرماندهی واحد و همچنین

تشکیل تیم‌های تحقیقاتی مشترک برای دستیابی به سامانه‌ها و تسلیحات با قابلیت‌های ترکیبی سایبری و الکترونیکی است. همگرایی عملیات فضای سایبر و جنگ الکترونیک در تمامی مراحل عملیات‌های نظامی ضروری است.

پیشنهادات: با توجه به نو بودن مبحث همگرایی جنگ الکترونیک و جنگ سایبری و نقش و اهمیت آن در مأموریت‌های دفاعی کشور و همچنین فقر ادبیات در اختیار و منابع علمی پژوهشی داخلی در این خصوص، پیشنهاد می‌شود که این مقاله در دسترس محققین حوزه‌های دفاعی و دانشگاهی کشور قرار گیرد و فعالیت‌های پژوهشی بیشتری نیز در این زمینه انجام شود. در این راستا عناوین زیر برای پژوهش‌های بعدی پیشنهاد می‌گردد.

الگوی راهبردی فعالیت‌های سایبرالکترونیک نیروهای مسلح کشور

ساختار واحدهای سایبرالکترونیک در یگان‌های رزمی نیروهای مسلح با توجه به حوزه‌های مأموریتی آن‌ها

منابع:

- کشتکار هرانکی، مهران، (۱۳۹۵)، ***طراحی الگوی راهبردی نوآوری اجتماعی در جمهوری اسلامی ایران***، رساله دکتری دانشگاه عالی دفاع ملی.

- DOD Dictionary of Military and Associated Terms, 2018, available at www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf
- Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, Drew Herrick, 2017, Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below, available at https://www.rand.org/content/dam/rand/pubs/research_reports/ RR1600/ RR1600/RAND_RR1600.pdf
- James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, 2014, Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2, available at www.ewi.inf0
- Joint Doctrine Note 1/18, Cyber and Electromagnetic Activities, UK Ministry of Defence, 2018, available at: http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/DCDC
- MAJ Michael Senft, Convergence of Cyberspace Operations and Electronic Warfare Effects, 2016, available at http://cyberdefensereview.army.mil/DesktopModules /ArticleCS/Print.aspx?PortalId=6&ModuleId=1233&Article=1136055
- Mark Pomerleau Cyber, Electronic Warfare Integration, Critical for Future Army Ops, 2016, available at https://www.c4isrnet.com/show-reporter/ausa/2016/10/06/cyber-electronic-warfare-integration-critical-for-future-army-ops/
- 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
- Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025, Challenging NATO in the Electromagnetic Spectrum, September 2017, Tallinn, Estonia info@icds.ee, www.icds.ee
- Sandelowski M. Barros J. Handbook for synthesizing qualitative research, Springer publishing company Inc; 2007. Available at: https://epdf.tips/handbook-for-synthesizing-qualitative-research.html
- Subhasis Das, Electronic Warfare: Emerging Trends in Technology, 2017, Available at: http://www.indiandefencereview.com/news/electronic-warfare-emerging-trends-in-technology/
- U. S. Army, 2012, JP 3-13.1: Electronic Warfare Electronic, available at https://info.publicintelligence.net/JCS-EW.pdf
- U. S. Army, 2014, FM 6-02: SIGNAL SUPPORT TO OPERATIONS, available at https://fas.org/irp/doddir/army/fm6-02.pdf
- U. S. Army, 2015, JP 6-0: Joint Communications System, available at https://fas.org/irp/doddir/dod/jp6_0.pdf

- U. S. Army, 2017, FM 3-12: Cyberspace and Electronic Warfare Operations, available at the Army Publishing Directorate site (http://www.apd.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard)
- U. S. Army, 2017, Army Doctrine Reference Publication No. 3-0 (ADRP 3-0), Operations, available at the Army Publishing Directorate site (http://www.apd.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard)
- U. S. Army, 2018, JP 3-12: Cyberspace Operations, available at https://fas.org/irp/doddir/dod/jp3_12.pdf
- Zsolt Haig, Electronic Warfare In Cyberspace, 2015, National University of Public Service, Budapest, Hungary, Available at: https://www.researchgate.net/publication/288871386