فصلنامه علمی امنیت ملی
سال چهاردهم، شماره پنجاه و یکم، بهار ۱۴۰۳
مقاله هفتم از صفحات ۲۴۲-۱۹۹

مقاله پژوهشی: واکاوی چالش‌ها و تهدیدات حوزه سایبرالکترونیک

حمیدرضا لشگریان[۱]، محمدرضا حسینی[۲]، قاسم فولادی[۳]، اسماعیل قجری[۴]

تاریخ دریافت: ۱۴۰۱/۱۲/۱۵ تاریخ پذیرش: ۱۴۰۲/۰۸/۲۱

چکیده

گسترش فضای سایبر در بستر طیف الکترومغناطیس و ظهور سلاح‌های هدایت پذیر، خودمختار، دورایستا، فوجی و هوشمند از قبیل پهپاد (پرنده‌های هدایت پذیر)، شهپاد (شناورهای هدایت پذیر)، زهپاد(زیردریایی‌های هدایت پذیر)، ریزپرنده‌ها و ربات‌ها به همراه فناوری‌های فرماندهی و کنترل، پشتیبان تصمیم، رایانش ابری، اینترنت اشیاء میدان نبرد؛ کلان داده‌ها، شبکه‌های سلولار (3G، 4G ، 5G)، فناوری‌های اسکادا و استارلینک محیط صحنه نبرد را به شدت دگرگون و در حوزه‌های غیرنظامی گسترش یافته است. در هم‌تنیدگی فضای سایبر و محیط الکترومغناطیس باعث خلق فضای جدید «سایبرالکترونیک (و یا سایبرالکترومغناطیس)» شده که قادر است در مدت زمان کوتاهی کلیه سرمایه‌های دیگرقلمروها (فیزیکی و سایبری) را تحت تأثیر قرار دهد. در چنین شرایطی، اگر تا به دیروز امکان غافلگیری دور از ذهن نبود، با ترور بزدلانه فرمانده نیروی قدس سپاه و پس‌ازآن ترور شهید فخری‌زاده با سلاح‌های کنترل از راه دور مصداق عینی به خود گرفته است. اولین گام برای مقابله با حملات سایبرالکترونیک، شناخت چالش‌ها و تهدیدات این حوزه است، که سطح غافلگیری را کاهش و تا حدودی از بین می‌برد. لذا سوال این پژوهش این است که چالش‌ها و تهدیدات حوزه سایبرالکترونیک کدامند؟ در این پژوهش با مطالعه اسناد کشورهای صاحب‌نام در حوزه سایبرالکترونیک و مقالات مرتبط و با استفاده از ابزار مکس‌کیودا[۶]با رویکرد فراترکیب تعداد چهار مقوله چالشی و تهدیدزا به ترتیب «فناوری»، «بنیادی»، «یکپارچه‌سازی» و «نیروی عملیاتی» استخراج گردیده است.

کلیدواژه‌ها: سایبرالکترونیک، سایبرالکترومغناطیس، چالش‌ها و تهدیدات سایبرالکترونیک

۱. استادیار دانشگاه امام حسین(ع)
۲. دانشیار دانشگاه عالی دفاع ملی
۳. دانش آموخته مقطع دکتری دانشگاه عالی دفاع ملی
۴. دانشجوی مقطع دکتری دانشگاه دفاع ملی.(نویسنده مسئول)، رایانامه: a.asadabadi98@sndu.ac.ir

[5] Internet Of Battlefield Things (IOBT)
[6] MAXQDA

مقدمه و بیان مسئله

پیشرفت‌های سریع و تحولات پرشتاب فناوری در عصر حاضر، فضای نامطمئن و سرشار از فرصت و تهدید را پیش‌روی جوامع و به‌طور خاص نیروهای نظامی قرار داده است. تغییر فناوری‌های نوظهور و برهم زن[۱] همچون رایانش ابری،[۲] اینترنت اشیاء،[۳] کلان داده،[۴] رایانش کوانتومی،[۵] رباتیک[۶] و خودکارسازی[۷] به همراه هوش مصنوعی باعث خلق ویژگی‌هایی در عملیات نظامی شده است که می‌توان به عدم قطعیت،[۸] غیرخطی بودن،[۹] ناهمگونی و[۱۰] ائتلافی بودن، برق‌آسایی (سرعت عملیات)، منطبق بر سطوح تاکتیکی، عملیاتی و راهبردی،[۱۱] سرعت‌بالا در چرخش اطلاعات،[۱۲] دقت و هوشمندی خیره‌کننده و قدرت تخریب بالای تسلیحات، پیچیدگی، دور ایستایی[۱۳] و مکانیزه شدن[۱۴] تسلیحات اشاره نمود.

---

[1] -Disruptive technology
[2] -Cloud computing
[3] -Internet of Things (IoT)
[4] -Big Data
[5] -Quantum computer
[6] - Robotics

[۷] – (Automation) معمولاً به فرایند قادر ساختن ماشین‌ها به انجام عملیات ترتیبی از پیش تعیین‌شده بدون دخالت انسان یا دخالت کم و هم‌چنین استفاده از تجهیزات خاص که عملیات صنعتی را اجرا و کنترل می‌کنند، گفته می‌شود

[8] -Uncertainty

[۹] – در دو مفهوم غیر پیش‌بینی بودن و اجتناب از خطوط مشخص(حیدری و عبدی،۱۳۹۱)

[۱۰]– عدم تقارن: به‌کارگیری رویکردهای غیرمنتظره برای از سر راه برداشتن و تضعیف قوای دشمن و درعین‌حال بهره‌برداری کردن از نقاط ضعف آن از طریق فناوری‌های غیرمنتظره و نوین یا روش‌های مبتکرانه(حسنلو،۱۳۹٦)

۱۱–رجوع شود به مقاله جنگ‌های آینده(آذرپی،۱۳۸۵ : ۱۱٦)

۱۲–همان(آذرپی،۱۳۸۵ : ۱۱۷)

۱۳– تفوق فناوری نظامی این امکان را به قدرت‌های برتر داده است تا دور از منطقه نبرد، اقدام به هدایت عملیاتی میدان نبرد نمایند.(همان:۱۱۹)

۱٤– بهره‌گیری از تجهیزات بدون سرنشین

جنگ الکترونیک[1] به‌طور تاریخی با طیف الکترومغناطیس سروکار داشته و با وظایفی همچون پشتیبانی الکترونیکی[2]، حفاظت الکترونیکی[3] و حمله الکترونیکی[4] به‌دنبال افزایش میزان بهره‌برداری نیروهای خودی و کاهش میزان بهره‌برداری نیروهای دشمن از طیف الکترومغناطیس درصحنه نبرد است و در عصر حاضر به‌عنوان کلید جادویی توانسته، در کلیه زمینه‌های نظامی که مرهون توسعه و پیشرفت الکترونیک است، اقتدار خود را به نمایش گذارد.

سامانه‌های اطلاعاتی و ارتباط الکترونیکی مبتنی بر شبکه، در فضای سایبر و طیف الکترومغناطیس کار می‌کنند و یک محیط عملیاتی مشترک نظامی را باهم ایجاد می‌نمایند. در این حوزه، عملیات سایبر الکترومغناطیس به‌صورت هماهنگ و یکپارچه انجام می‌شود. جنگ الکترونیک که علیه سامانه‌های اطلاعاتی و ارتباطی شبکه‌ای دشمن استفاده می‌شود و یا از سیستم‌های مشابه ما محافظت می‌کند، قابلیت اصلی این عملیات است (Haig, 2015:33-34).

اولین و مؤثرترین نمونه از بروز حملات سایبرالکترونیک در جنگ دوم خلیج‌فارس بود که با پشتیبانی از عملیات هوایی نیروهای ائتلاف، سیستم پدافند یکپارچه عراق را قبل از حمله هوایی فروریخت. از دیگر نمونه‌های می‌توان به عملیات رژیم اشغالگر قدس علیه سامانه پدافند هوایی سوریه در حمله به نیروگاه هسته‌ای آن کشور در سال ۲۰۰۷ اشاره نمود(Askin, Irmak & Avsever,2015: 06).

---

[1] - Electronic Warfare

[2] - Electronic Warfare Support (ES)

[3] - Electronic Warfare Protection (EP)

[4] - Electronic Warfare Attack (EA)

بیان مسئله:

فضای سایبر محیط الکترونیکی است که از طریق آن، اطلاعات تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌گردد[۱] این فضای ساخته دست بشر با استفاده از طیف الکترومغناطیس و شبکه‌های کابلی توانسته در دیگر قلمروها گسترش یابد و به‌عنوان یک فرا قلمرو ظاهر گردد. عملیات جنگ الکترونیک که بر بستر طیف الکترومغناطیس شکل می‌گیرد با همگرایی جنگ سایبری در حال تبدیل‌شدن به عناصر کلیدی صحنه نبرد می‌باشند. تسلط بر طیف الکترومغناطیس و سامانه‌های اطلاعاتی و استفاده مؤثر و هماهنگ از قابلیت‌های این دو حوزه، عامل برترساز و تعیین‌کننده در نبردهای آینده خواهد بود. شباهت‌ها و وجوه مشترک جنگ سایبری و جنگ الکترونیک، موجب همگرا شدن این دو عرصه تحت عنوان «سایبرالکترونیک» شده است. 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 (فرح‌بخت، دهقانی، ۱۳۹۸ : ۲۰۰).

گسترش عملیات سایبری در بستر الکترومغناطیس- عملیات سایبرالکترونیک- باعث چالش‌های راهبردی در حوزه‌های نظامی و غیرنظامی گردیده است. امروزه در بستر سایبرالکترونیک تسلیحاتی همچون پرنده‌های بدون سرنشین، تسلیحات هوشمند و خودکار از فاصله چند هزار کیلومتری هدایت و کنترل عملیاتی می‌گردند و این تهدیدات هوشمند در حوزه‌های مختلف سایبرالکترونیک و در ابعاد سخت، نیمه سخت و نرم به‌صورت هم‌زمان، آشکارا و نهان پیرامون جمهوری اسلامی به‌صورت بالقوه و بالفعل بر ما می‌تازند. در این شرایط، اگرچه تا دیروز امکان غافلگیری راهبردی دور از ذهن نبود، امروزه با ترور بزدلانه فرمانده نیروی قدس سپاه و فرماندهان محور مقاومت در فرودگاه بین‌المللی عراق و پس‌ازآن ترور دانشمند هسته‌ای-شهید محسن فخری‌زاده- در عمق خاک کشور با سلاح‌های کنترل از راه دور مصداق عینی به خود گرفته است.

---

[۱] - تعریف مشترک آمریکا و روسیه

ظهور شهرهای هوشمند مبتنی بر اینترنت اشیا، کلان‌داده‌ها و رایانش ابری، عدم آگاهی از تهدیدات فناوری‌های مبتنی بر طیف الکترومغناطیس و فضای سایبر، حوزه مدیریت شهری را در برابر حملات سایبرالکترونیک با چالش‌های غافلگیرکننده روبرو خواهد نمود.

افزایش اتکای روزافزون سازمان‌های نظامی به عملیات شبکه محور- شبکه‌های عملیاتی، اطلاعاتی و فرماندهی و کنترل- سامانه‌های الکترونیکی و ابزارهای متنوع خودمختار از قبیل پهپادها، ربات‌ها، تسلیحات، شناورهای سطحی و زیرسطحی هوشمند، باعث خلق چالش‌ها و تهدیداتی در این حوزه گردیده است که می‌توان به نفوذ و ربایش الگوریتم‌ها و در اختیار گرفتن این ابزارها در حین عملیات توسط سلاح‌های سایبرالکترونیک دشمن و به‌تبع آن شکل‌گیری مسائل راهبردی دیگر اشاره نمود.

لذا باتوجه به ظرفیت و قابلیت فضای سایبر و طیف الکترومغناطیس و بهره‌گیری از تجهیزات و بسترهای غیربومی امکان گسترش صحنه نبرد سایبرالکترونیک با حرکت پرشتاب به حوزه‌های غیرنظامی متصور است. امروزه سلاح‌های سایبرالکترونیک قادرند با بهره‌گیری از تکنیک‌های جنگ الکترونیک با ارسال کدهای مخرب، سامانه‌های مخابراتی، ناوبری و کنترلی هواپیماهای مسافربری و تجاری، کشتی‌های تجاری و نفت‌کش‌ها، سامانه‌های کنترل صنعتی شبکه‌های برق، آب، گاز و بنگاه‌ها و صنایع و اقتصاد را با چالش بسیار جدی مواجه نمایند و کشورها را به سمت فلج سازی راهبردی[1]در حوزه‌های اقتصادی، صنعتی و اجتماعی سوق دهند که می‌توان در سطح راهبردی به طراح‌ریزی حمله سایبری تحت عنوان «نیترو زئوس» توسط آمریکا علیه زیرساخت‌های جمهوری اسلامی ایران و در سطح عملیاتی به اقداماتی همچون خرابکاری گسترده در شبکه برق اوکراین در سال ۲۰۱۵ و شبکه برق ونزوئلا در سال ۲۰۱۶، اشاره نمود.

[1] – فلج سازی راهبردی، وضعیتی است که در آن دولت در بخش‌های مختلف(سیاسی، اجتماعی و اقتصادی) امکان اقدام برای جبران خسارت و تغییر طرح‌های اجرایی را نداشته و با ناتوانی برای ضد حمله، در زمانی فشرده حوادث مختلفی در بخش‌های گوناگون علیه کشور رخ دهد (امیرصوفی، ۱۳۹۲).

در شرایط متغیر و پیچیده کنونی که به شدت متأثر از فناوری‌ها نوظهور است، فقدان شناخت چالش‌ها و تهدیدات حوزه سایبرالکترونیک علاوه بر غافلگیری در سطوح مختلف باعث خلق مسائلی همچون عدم یکپارچگی و همگام‌سازی در حوزه‌های سایبری و جنگ الکترونیک، نبود توازن و یکپارچگی در تصمیم‌گیری در برابر تهدیدات این حوزه خواهد شد. نظر به مسائل فوق؛ الزام در شناخت حوزه سایبرالکترونیک لازم است واکاوی چالش‌ها و تهدیدات حوزه سایبرالکترونیک صورت گیرد تا بتوان به‌سرعت نسبت راهکارهای بومی مقابله با چالش‌ها و تهدیدات این حوزه در سطوح مختلف به عمل آورد.

اهمیت پژوهش

نبردهای آینده که بر پایه سایبرالکترونیک شکل خواهند گرفت با چالش‌ها و تهدیدات جدی مواجه است، عوامل ایجابی که باعث اهمیت این تحقیق‌شده عبارت‌اند از:

- ایجاد ادبیات در حوزه سایبرالکترونیک در سطح مدیریت کلان حوزه‌های سایبری و جنگ‌الکترونیک
- ارتقاء سطح فهم و درک مخاطبان و ذی‌نفعان با چالش‌های و تهدیدات حوزه سایبرالکترونیک
- ارتقاء سطح فهم و درک مخاطبان و ذی‌نفعان با روش‌های غافلگیری راهبردی در حوزه حملات سایبرالکترونیک.
- ارتقاء سطح فهم و درک مخاطبان و ذی‌نفعان با بسترهای لازم جهت اقدامات مقابله‌ای و ارتقاء قدرت تصمیم‌سازی در حوزه سایبرالکترونیک

ضرورت پژوهش

عوامل سلبی که در فقدان چنین پژوهشی باعث ضرورت اجرای این تحقیق‌شده عبارت‌اند از:

- غافلگیری راهبردی در حوزه مقابله با حملات سایبرالکترونیک
- تأثیر منفی بر توان دفاعی کشور
- تحمیل هزینه‌های مادی و معنوی بر کشور

- کاهش قدرت بازدارندگی و تاب‌آوری در حوزه سایبری و جنگ‌الکترونیک

نوآوری این پژوهش؛ شناخت چالش‌ها و تهدیدات حوزه سایبرالکترونیک می‌باشد

هدف پژوهش احصاء چالش‌ها و تهدیدات حوزه سایبرالکترونیک است.

سوال پژوهش؛ چالش‌ها و تهدیدات حوزه سایبرالکترونیک کدامند؟

۱. مبانی نظری

۱-۱. پیشینه تحقیق

جنگ خلیج‌فارس اولین و مؤثرترین نمونه از جنگ سنتی است که توسط عملیات سایبرالکترونیک پشتیبانی شد. وزارت دفاع ایالات‌متحده با بکارگیری اقدامات سایبرالکترومغناطیس در جنگ دوم خلیج‌فارس و مشاهده اثرات هم‌افزایی این دو حوزه، اهمیت فضای سایبری و طیف الکترومغناطیسی را برای نیروهای مسلح درک نمود و برای اولین‌بار در سال ۲۰۱۴، کتابچه راهنمای «فعالیت‌های سایبرالکترومغناطیس[1] را منتشر کرد. این کتابچه اهمیت فضای سایبر و طیف الکترومغناطیس(طیف الکترومغناطیس) را برای نیروهای ارتش توصیف و تاکتیک‌ها و رویه‌هایی که فرماندهان و کارکنان از آن‌ها در برنامه‌ریزی، یکپارچه‌سازی[2] و همگام‌سازی[3] سایبرالکترومغناطیس استفاده می‌کنند، ارائه می‌دهد و راهنمایی‌های کافی برای فرماندهان و کارکنان فراهم می‌کند تا رویکردهای جدیدی را، در به‌دست آوردن، حفظ و بهره‌برداری از مزایای موجود در یک محیط عملیاتی ایجاد کنند. سایبرالکترومغناطیس نیروهای نظامی را قادر می‌سازد تا پشتیبانی

[1] Cyber Electromagnetic Activities (FM3-38)

[2] integrating

[3] synchronizing

مطلوبی از اهداف و نیت فرمانده‌هان خود داشته باشند (U.S. Department of the Army Headquarters, 2014: IV).

باتوجه به اهمیت همگرایی فضای سایبر و جنگ الکترونیک، وزارت دفاع آمریکا سند دیگری تحت نام «عملیات فضای سایبر و جنگ الکترونیک» را در سال ۲۰۱۷ منتشر و در سال ۲۰۲۱ آن را بروزرسانی نمود در پیشگفتار این سند، ارتش به دغدغه خود از ناحیه رشد فناوری‌ها و قابلیت‌های عملیاتی همتایان منطقه‌ای خود در حوزه سایبرالکترونیک اشاره کرده و آن‌ها را تهدیدی برای سلطه خود بر فضای سایبر و طیف الکترومغناطیس می‌داند (U.S. Department of the Army Headquarters, 2021).

وزارت دفاع انگلیس در سال ۲۰۱۶ به‌صورت مفهومی فعالیت‌های سایبرالکترومغناطیس را معرفی و دکترین خود را برای سال‌های ۲۰۲۰-۲۰۱۷ تدوین نموده است. در جولای ۲۰۱۶ مرکز توسعه، مفاهیم و دکترین وزارت دفاع بریتانیا ویرایش دوم انتشار مبانی سایبری خود را منتشر کرد. نسخه‌های دکترین سایبری انگلستان اولین سند دکترین انگلستان است که اصطلاح فعالیت‌های سایبرالکترومغناطیس را معرفی می‌کند. در میان هشت باری که این سند ۱۰۰ صفحه‌ای از اصطلاح فعالیت‌های سایبرالکترومغناطیس استفاده کرده است، اشاره نموده است که در گام اول رابطه بین سایبر و فعالیت‌های الکترومغناطیس باید به‌عنوان رابطه انعطاف‌پذیر و با ماهیت مکمل به‌جای رقابت در نظر گرفته شود. و در گام دوم فعالیت‌های سایبرالکترومغناطیس باید به‌طور فزاینده‌ای هماهنگ در داخل دفاع ارائه شود (Soesanto, 2021: 16).

در سپتامبر ۲۰۱۷، این مرکز سند مشترک ۱/۱۷ را تحت عنوان «مفهوم نیروی آینده» منتشر کرد. این سند نشان‌دهنده یک تغییر گام‌به‌گام در رویکرد این کشور از محیطی مجزا به یک مفهوم به‌طور فزاینده مشترک و یکپارچه است (U UK Ministry of Defence,

III :2017). این سند، اولین سند در دسترس عموم بود که به‌طور مفصل وارد جنبه‌های مختلف فعالیت‌های سایبرالکترومغناطیس شده است که می‌توان به معرفی رویکرد فعالیت‌های سایبر و الکترومغناطیس، آگاهی وضعیت فعالیت‌های سایبرالکترومغناطیس، یکپارچه‌سازی و کنترل فعالیت‌های سایبرالکترومغناطیس، متخصصان فعالیت‌های سایبرالکترومغناطیس، آموزش نظری، آموزش عملی و آزمون فعالیت‌های سایبرالکترومغناطیس و انعطاف‌پذیری فعالیت‌های سایبرالکترومغناطیس اشاره نمود (Soesanto, 2021:14).

در فوریه ۲۰۱۸، مرکز توسعه، مفاهیم و دکترین وزارت دفاع انگلیس با انتشار سند دکترین مشترک ۱/۱۸ تحت نام «فعالیت‌های سایبرالکترومغناطیس»[1] تلاش کرد تا وسیع‌ترین مفاهیم از فعالیت‌های سایبرالکترومغناطیس را استخراج و عناصر دکترین خود را ترسیم کند. این دکترین خطوط اصلی فعالیت‌های سایبر و الکترومغناطیس در دفاع انگلیس، ستاد فرماندهی ارتباطات دولتی[2] و سایر شرکای دولت را تعیین و شرح وظایفی از محیط فعالیت سایبرالکترومغناطیس ارائه می‌دهد (UK Ministry of Defence, 2018: III).

بریتانیا در حال حاضر تنها عضو ناتو است که سایبرالکترومغناطیس را به‌عنوان یک حوزه جنگی به رسمیت شناخته است. در سال ۲۰۱۱ فرانسه، مفهوم جنگ سایبرالکترونیک را به‌طور خلاصه در اجلاس موردبحث قرار داد. دو نفر از برجسته‌ترین طرفداران پذیرش فعالیت‌های سایبرالکترومغناطیس در فرانسه، در سال ۲۰۱۴ کتابی باعنوان «نسخه نبرد با سایبرالکترونیک»[3] منتشر نمودند و در سال ۲۰۱۹ برای اندیشکده روابط بین‌الملل فرانسوی

[1] Joint Doctrine Note 1/18 Cyber and Electromagnetic Activities(CEMA)

[2] Government Communications Headquarters

[3] Vers le combat cyber-electronique

در دو الی سه فصل در حوزه سایبرالکترونیک از تاریخچه و پذیرش فعالیت‌های سایبرالکترومغناطیس توسط ارتش ایالات‌متحده صحبت کرده‌اند، اما به هیچ جنبه‌ای از اقدامات ارتش فرانسه برای پذیرش فعالیت‌های سایبرالکترومغناطیس اشاره نکرده‌اند (Soesanto, 2021: 19).

وزارت دفاع استرالیا اولین طرح تلاش برای توسعه استراتژی یکپارچه‌سازی حوزه‌های سایبر و جنگ الکترونیک خود را براساس برنامه‌ریزی راهبردی سال ۲۰۱۱ و چشم‌انداز ۲۰۲۰ منتشر کرده است. این طرح علاوه بر یکپارچه‌سازی در سراسر بخش سایبری و جنگ الکترونیک، راهنمایی‌های مفیدی را در حوزه روندها، اولویت‌ها و سمت‌وسوی سرمایه‌گذاری به‌منظور اطلاع‌رسانی به ذینفعان داخلی و خارجی ارائه می‌دهد.

در این سند چشم‌انداز مرکز جنگ الکترونیک و سایبری استرالیا به عنوان، مرکزی در کلاس جهانی، تحقیقات و توسعه چندمنظوره در حوزه سایبری، سیگنال‌های هوشمند، ارتباطات و جنگ الکترونیک خواهد بود و در یکپارچه‌سازی این حوزه‌ها در ارائه راه‌حل‌های نوآورانه برای مشکلات چالش‌برانگیز در پیوستگی[1] جنگ الکترونیک و سایبری پیشرو خواهد بود (AU Department of Defence: 08).

سرهنگ آناتولی سیگانوک، یکی از اعضای مرکز مطالعات سیاسی و نظامی روسیه، اظهار داشت که «شروع جنگ بدون کنترل طیف الکترومغناطیس نتیجه‌ای جز شکست ندارد» (McCrory, 2020:35). روسیه همچنین از اصطلاح «اطلاعات» در زمینه جنگ سایبری استفاده می‌کند. با انجام این کار، حملات سایبری را به‌اصطلاح گسترده‌تری از جنگ اطلاعاتی مرتبط می‌کند، که شامل جنگ الکترونیک، عملیات شبکه رایانه‌ای و عملیات روانی می‌شود (גיל ברעם ואופיר בראל، ۲۰۲۰: ۱۰۷).

[1] continuum

درحالی‌که چین دکترین رسمی مبنی بر ایجاد ارتباط بین جنگ سایبر و جنگ الکترونیک ندارد، ولی رویکرد چینی‌ها نسبت به جنگ سایبر و جنگ الکترونیک با عملیات سایبرالکترونیک سازگار است تا آنجاکه گره‌های اساسی میدان نبرد را در طیف الکترومغناطیسی می‌دانند. شناخت همگرایی و یکپارچه‌سازی این دو حوزه برای تسلط بر عملیات اطلاعاتی در زمان جنگ ضروری است. دای چینگمین آن را جنگ الکترونیک و شبکه یکپارچه[1]متشکل از «ترکیب جنگ الکترونیک و جنگ شبکه رایانه‌ای» نامیده است. ازنظر دای و دیگر خبرگان این حوزه در موسسه راهبرد نظامی چین، نگاه به ترکیب جنگ الکترونیک و جنگ سایبری ماهیت عملیات جنگ یکپارچه برای مبارزه با سیستم اطلاعاتی دشمن باهدف به‌دست آوردن برتری میدان نبرد است (Bommakanti, 2019: 12). ارتش آزادیبخش خلق چین معتقد است که با ظهور عصر اطلاعات، جنگ آینده رقابت‌هایی برای توانایی بهره‌برداری از اطلاعات خواهد بود (Mallick, 2021: 01).

اصطلاح سایبرالکترونیک/سایبر الکترومغناطیس:

جزوه آموزش و دکترین ارتش ایالات‌متحده[2]از عبارت «نبرد سایبر الکترومغناطیس» برای برجسته‌سازی همپوشانی بین فضای سایبر و طیف الکترومغناطیس استفاده می‌کند. در این پژوهش (موسسه رند[3])، عملیات در فضای سایبر و طیف الکترومغناطیس به عنوان عملیات سایبر الکترومغناطیس (یا عملیات سایبرالکترونیک) تلقی می‌گردد. و در ادامه ذکر می گردد؛ تا آنجاکه ممکن است، ما از اصطلاحات سایبرالکترونیک(یا سایبر الکترومغناطیس) و عملیات سایبرالکترونیک(یا عملیات سایبر الکترومغناطیس) در مقابل

[1] Integrated Network and Electronic Warfare (INEW)
[2] U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-7-8

[3] Rand

اصطلاح ساده سایبر یا عملیات سایبر استفاده می‌کنیم. و همان‌طورکه الدر[1](۲۰۱۰) متذکر می‌شود، این‌یک روش مفیدتر برای توصیف سیستم بزرگ‌تر فن‌آوری‌های مرتبط و متصل است (RAND Corporation, 2013: 16).

در این سند پیشنهاد شده که ارتش در نهایت باید یک عرصه مدیریت شغلی جدید «سایبرالکترونیک» یا «سایبرالکترومغناطیس» ایجاد کند یا وضعیت موجود را برای پشتیبانی از تمام قلمروهای فنی جنگ اطلاعات اصلاح کند. این می‌تواند به‌عنوان اولین گام به‌سوی شاخه جدیدی برای کادر رزمی سایبرالکترونیک باشد که می‌تواند برای پوشش مناطق فرماندهی کنترل جنگ الکترونیک[2]توصیف شود. این گروه شامل جنگ الکترونیک و مدیریت طیف است که در حوزه فنی جنگ اطلاعات قرار می‌گیرد (همان: ٦٩).

فضای سایبر:

اصطلاح فضای سایبر برای اولین بار توسط ویلیام گیبسون در کتاب نورومنسر[3] ذکرشده است. گیبسون در این رمان علمی تخیلی، فضای سایبر را، شبکه رایانه‌ای توصیف کرده است که اغلب برای دنیای مجازی یا واقعی نیز مورد استفاده قرار می‌گیرد. در خصوص فضای سایبر تفاسیر متعددی ذکرشده است. براساس دائره‌المعارف بریتانیکا، فضای سایبر دنیای بی‌نظیر، ظاهراً مجازی است که از طریق پیوند بین رایانه‌ها، دستگاه‌های متصل به اینترنت، سرورها، روترها و سایر مؤلفه‌های زیرساخت اینترنت ایجادشده است (Haig,2015: 27).

در این تعریف فضای سایبر فضای مجازی و در محدوده شبکه اینترنت ذکرشده است. گوردن ریچارد[4]معاون پیشین وزیر دفاع آمریکا، در یادداشتی به وزارت دفاع آمریکا، فضای سایبر را دامنه جهانی در محیط اطلاعاتی متشکل از شبکه وابسته، زیرساخت‌های

---

[1] Elder

[2] command, control, communication, intelligence, and electronic warfare(C3IEW)

[3] Neuromancer

[4] معاون وزیر دفاع (۲۰۰۹-۲۰۰۵)

فناوری اطلاعات، ازجمله اینترنت، شبکه‌های ارتباط از راه دور، سیستم‌های رایانه‌ای و پردازنده‌ها و کنترل‌کننده‌ها تعبیه‌شده نام‌برده است. وزیر دفاع انگلیس، فضای سایبر را فضایی می‌داند، که به حوزه دیگری از جنگ تبدیل‌شده است، ولی از حیث سنتی متفاوت است ازاین‌جهت که هم مؤلفه فیزیکی دارد و هم مؤلفه اطلاعاتی. اشکال سنتی جنگ – حمله، دفاع و بهره‌برداری– هنوز هم وجود دارد، اما اطلاعات بیشتر از افراد یا تجهیزات مورد هدف است (RAND Corporation, 2013: 06).

تفسیر نظامی از فضای سایبر با رویکرد غیرنظامی آن متفاوت است. فضای سایبر با اشاره به سند «استراتژی نظامی ملی برای عملیات فضای سایبر»، دامنه‌ای است که با استفاده از الکترونیک و طیف الکترومغناطیس برای ذخیره، اصلاح و تبادل داده از طریق سیستم‌های شبکه‌ای و زیرساخت‌های فیزیکی مرتبط مشخص می‌شود (Haig, 2015: 26).

دانیل کوئل فضای سایبر را یک دامنه عملیاتی می‌داند که شخصیت متمایز و منحصربه‌فرد آن با استفاده از الکترونیک و طیف الکترومغناطیس برای ایجاد، ذخیره، اصلاح، تبادل و بهره‌برداری از اطلاعات از طریق سیستم‌های مبتنی بر فناوری اطلاعات و ارتباطات متصل به یکدیگر و زیرساخت‌های مرتبط با آن‌ها، ایجاد می‌شود (همان:۲۷).

به‌نظر می‌رسد، کامل‌ترین و شفاف‌ترین تعریف از فضای سایبر مربوطبه دکترین مشترک ناتو در سال ۲۰۲۰ است که علاوه بر همپوشانی تعاریف ذکرشده، شامل شبکه‌ها و سیستم‌های الکترونیکی جدا و مستقل که داده‌ها را پردازش، ذخیره و یا انتقال می‌دهد، نیز هست: «دامنه جهانی متشکل از کلیه ارتباطات به‌هم‌پیوسته، فناوری اطلاعات و سایر سیستم‌های الکترونیکی، شبکه‌ها و داده‌های آن‌ها، ازجمله آن‌هایی [سیستم‌های الکترونیکی یا شبکه‌های] جدا[1] یا مستقل[2] که داده‌ها را پردازش، ذخیره یا انتقال می‌دهند» (NATOSTANDARD, AJP-3.20, 2020: 04).

[1] Separated

[2] Independent

جنگ الکترونیک

ارتش‌های مدرن در یک جهان که به‌طور فزاینده‌ای متکی به شبکه‌های بی‌سیم است فعالیت می‌کنند. نیروهای مسلح از طیف الکترومغناطیس در ابعاد گسترده‌ای برای برقراری ارتباط، کنترل تسلیحات، اطلاعات، نظارت، ناوبری و محافظت از نیرو استفاده می‌کنند. امروزه دستگاه‌های الکترونیک بی‌شماری با تنوع زیاد در میدان‌ها نبرد وجود دارند. این دستگاه‌ها در محیط الکترومغناطیس کار می‌کنند و باعث می‌شود تا قابلیت‌های همکاری بین آن‌ها تشدید شود (Haig, 2015: 23).

برتری طیف الکترومغناطیس درجه‌ای از کنترل در طیف الکترومغناطیس است که امکان انجام عملیات در زمان و مکان معین را بدون تداخل بازدارنده فراهم می‌کند، درحالی‌که بر توانایی دشمن برای انجام همان‌کار تأثیر می‌گذارد. جنگ الکترونیک جلوه‌هایی را در طیف الکترومغناطیس ایجاد و فرماندهان را قادر می‌سازد در حین انجام عملیات، برتری طیف الکترومغناطیس را به‌دست آورند. قابلیت‌های جنگ الکترونیک شامل سامانه‌ها و سلاح‌های مورد استفاده در انجام مأموریت‌های جنگ الکترونیک برای ایجاد اثرات کشنده و غیر کشنده در و از طریق طیف الکترومغناطیس است. امروزه نیروهای مسلح برای انجام عملیات نظامی به تجهیزات ارتباطی با بهره‌گیری از بخش وسیعی از طیف الکترومغناطیس متکی است که به نیروها اجازه می‌دهند صحبت کنند، داده‌ها را ارسال کنند، اطلاعات ناوبری و زمان‌بندی ارائه کنند و نظام فرماندهی و کنترل را در سراسر جهان پیاده‌سازی نمایند. آن‌ها همچنین برای سنجش و آگاهی از محیط عملیاتی به طیف الکترومغناطیس متکی هستند (U.S. Department of the Army Headquarters, 2021: 1-8).

هدف از جنگ الکترونیک جمع‌آوری اطلاعات از طریق بهره‌برداری از تجهیزات الکترونیک یا از کار انداختن تجهیزات الکترونیک مورد استفاده دشمن است. این هدف همچنین با استفاده مؤثر از تجهیزات الکترونیکی خودی و دور نگه‌داشتن این تجهیزات از دسترسی یا تأثیر اختلال دشمن محقق می‌گردد (Askin, Irmak & Avsever,2015:02).

سایبرالکترونیک

از سال ۲۰۱٤، کشورهای پیشرفته در حوزه نظامی (ایالات‌متحده، استرالیا، ژاپن، انگلستان، کانادا و غیره) تمایل به همگرایی و یکپارچه‌سازی عملیات سایبر و جنگ الکترونیک ازنقطه‌نظر دکترین، سازمان، فناوری و غیره دارند و از ابزارهای مختلف یکپارچه‌سازی سایبرالکترونیک استفاده می‌کنند (Kim et al., 2021: 121-122).

با رشد و گسترش فناوری‌ها در ابعاد مختلف زندگی، فضای سایبر، جنگ الکترونیک و عملیات مدیریت طیف به‌طور جدایی‌ناپذیری به هم وابسته شده‌اند و عملیات را به‌صورت تحسین‌آمیز پشتیبانی می‌کنند. عملیات فضای سایبر و جنگ الکترونیک برای اجرای عملیات تسلیحات ترکیبی ضروری است. درحالی‌که این فعالیت‌ها در به‌کارگیری و تاکتیک‌هایشان متفاوت هستند، عملکردها و قابلیت‌های آن‌ها باید برای به حداکثر رساندن پشتیبانی‌شان یکپارچه و همگام شوند (U.S. Department of the Army Headquarters, 2018: 05).

به لطف گسترش فناوری‌ها در ابعاد نظامی و ظهور تجهیزات خودمختار و هوشمند در صحنه‌های نبرد، فرماندهان از قابلیت‌های عملیاتی فضای سایبری و جنگ الکترونیک برای فریب[1]، تنزل رتبه[2]، مختل کردن[3]، انکار[4]، تخریب[5] یا دست‌کاری[6] در چندین دامنه استفاده می‌کنند. این قابلیت‌ها از سامانه‌های دشمن برای تسهیل جمع‌آوری اطلاعات، هدف قرار دادن عملکردهای فضای سایبری و طیف الکترومغناطیس دشمن و ایجاد اثرات مرتبه اول استفاده می‌کنند و همچنین عملیات فضای سایبر و جنگ الکترونیک قادر است اثرات

---

[1] deceive

[2] degrade

[3] disrupt

[4] deny

[5] destroy

[6] manipulate

آبشاری را در چندین حوزه ایجاد نماید تا با استفاده از سلاح‌های ترکیبی برای پیشی گرفتن بر سامانه‌های تسلیحاتی، فرآیندهای فرماندهی و کنترل، زیرساخت‌های حیاتی و منابع کلیدی دشمنان ازنظر فیزیکی و شناختی در همه حوزه‌ها، تأثیر بگذارد (U.S. Department of the Army Headquarters, 2018: 14).

بدون درک همبستگی بین فضای سایبر و جنگ الکترونیک امکان رسیدن به درک لازم وجود نخواهد داشت. جنگ الکترونیک نگران بهره‌برداری از طیف الکترومغناطیس توسط دشمن است، درحالی‌که عملیات سایبری با شبکه‌ها سروکار دارد. این واقعیت که سامانه‌های رادیویی ارتباط مستقیم مابین طیف الکترومغناطیس به‌عنوان قلمرو جنگ الکترونیک و رایانه‌ها به‌عنوان حوزه سایبری ارائه می‌دهد، فرصت‌های منحصربه‌فردی برای توسعه همکاری سایبری و جنگ الکترونیک می‌باشند (Du Plessis, 2014: 03).

در حال حاضر، این دو فناوری در طیف فرکانسی که حوزه تهدیدهای مشترک جنگ الکترونیک و جنگ سایبری است، با یکدیگر همپوشانی دارند، و به‌عنوان یک محدوده ارتباطی شناخته‌شده است. توسعه فناوری جنگ سایبرالکترونیک ضروری است که در آن دو فناوری بتوانند با همگرایی قابلیت‌های جنگ سایبری، اثر هم‌افزایی را اعمال کنند. هسته اصلی فناوری جنگ سایبرالکترونیک می‌تواند شناسایی و حمله خودکار به مخاطبین شبکه‌بی‌سیم باشد که در برابر امنیت آسیب‌پذیر هستند (Kim et al., 2021: 123).

دیجیتالی سازی منجربه همگرایی فعالیت‌های سایبری و اطلاعاتی به حدی شده است که مهم است ما مفاهیم و دکترین خود را با محیط تغییر دهیم. طیف الکترومغناطیس بسیار بیشتر از یک منبع متراکم است. امروزه هر عملیات نظامی، غیرنظامی، اطلاعاتی و امنیت داخلی به توانایی دسترسی و بهره‌برداری از طیف الکترومغناطیس متکی است. ازآنجاکه حوزه‌های فیزیکی (هوا/ زمین/ دریا/ فضا) و سایبری به‌طور فزاینده‌ای به دسترسی و کنترل طیف الکترومغناطیس بستگی دارند، فعالیت الکترومغناطیسی فضای سایبری برای موفقیت عملیات ضروری است. مفهوم فعالیت الکترومغناطیسی فضای سایبری عناصر جنگ سایبر

تهاجمی و دفاعی، جنگ الکترونیک و اطلاعات را یکپارچه می‌کند (Henselmann, Lehto, 2019: 211).

با پیشرفت سریع فناوری اطلاعات و ارتباطات، اهمیت جنگ سایبر و جنگ الکترونیک در فضای سایبر روزبه‌روز در حال افزایش است. توسعه فناوری اطلاعات و ارتباطات محیطی را برای دستیابی به پیشرفت‌های پیش‌رونده در صنعت فراهم می‌کند. فضای سایبر دیگر فضایی برای تبادل اطلاعات بین افراد نیست، بلکه به یک جامعه‌ای تبدیل‌شده که در آن تبادل اطلاعات بین اشیاء امکان‌پذیر است (Choi, Cho, Kwon,2021: 201). لذا فضای سایبر و طیف الکترومغناطیس یک محیط عملیاتی مشترک ایجاد می‌کنند که می‌توان از آن به‌عنوان حوزه سایبرالکترونیک نام برد. حوزه سایبرالکترونیک به معنای مساوی کردن اصطلاحات فضای سایبر و طیف الکترومغناطیس نیست، بلکه بیشتر به این نکته اشاره می‌کند که بین آن‌ها همپوشانی قابل‌توجهی وجود دارد و توسعه فناوری آینده احتمالاً باعث افزایش این همگرایی خواهد شد (Haig, 2015: 29).

چالش‌ها و تهدیدات حوزه سایبرالکترونیک:

محیط عملیاتی آینده نسبت به امروز، غیرقابل پیش‌بینی، پیچیده‌تر و بالقوه خطرناک‌تر خواهد بود در آینده، ساختار فیزیکی فضای سایبر در برابر حمله بسیار آسیب‌پذیر خواهد بود و با استفاده از انواع سلاح‌های بشدت مخرب، از جمله مهمات پرقدرت مایکروویو و سیستم‌های لیزری که به‌طور فزاینده‌ای در برابر مدارهای دیجیتال و یکپارچه موثر هستند. از آنجاکه این چالش‌ها و تغییرات می‌توانند به سرعت رخ دهند، نیروهای نظامی باید توانایی‌های پیشرفته عملیات فضای سایبری را با سرعت بیشتر از نرخ زمانی توسعه توانایی فعلی، داشته باشند (U.S. Department of the Army Headquarters, 2018 :08-09).

جنگ سایبری شامل تمام اقدامات تهاجمی و تدافعی انجام شده در قلمروی سایبری است. یک روش عملیاتی مرسوم در حمله سایبری شامل مراحل اسکن، نفوذ، گسترش جانبی، کنترل دستگاه قربانی، بهره برداری و استخراج است. کد نرم‌افزاری که برای نفوذ از

طریق یک آسیب‌پذیری طراحی شده است به‌عنوان «اکسپلویت»[1] و مسیر حمله به‌عنوان «بردار حمله»[2] نامیده می‌شود. حمله روز صفر حمله‌ای است که بسته پیشگیرانه برای آن اجرا نشده است. هدف جنگ سایبری قرار دادن یک بدافزار در سیستم کامپیوتری است که در صورت فعال شدن می‌تواند طیف وسیعی از عملکردهای مخربانه از جمله موارد ذیل را داشته باشد(PVSM, AVSM, VSM, 2017:03):

- حمله به سیستم کنترل نظارت و جمع‌آوری داده اسکادا یک نیروگاه هسته‌ای، شبکه‌های برق و ارتباطات برای از مدار خارج کردن و یا ایجاد آسیب‌های فیزیکی.
- حمله ویروسی به سیستم‌های ناوبری کشتی‌ها برای ایجاد اختلال در دقت آتش موشک‌ها.
- حملات بدافزاری به سیستم‌های اویونیک هواپیما و سیستم‌های هدایت پهپاد که منجربه تخریب سکوها می‌شود.

جنگ سایبر، همیشه با حملات نرم همراه بوده است، اما اکنون می‌توان از آن برای تخریب فیزیکی نیز استفاده کرد. با همگرایی جنگ سایبر و جنگ الکترونیک یک شکل مرگبار جدید از جنگ ایجاد شده است. این شکل از جنگ می‌تواند فعال یا غیر فعال باشد. جنگ سایبرالکترونیک پسیو[3]به این معنی است که یک بدافزار در شبکه هدف قرار می‌گیرد تا باعث حملات نرم شود درحالی‌که جنگ سایبرالکترونیک اکتیو[4]یک شکل شدیدتر است که شامل انجام اختلال[5]برای انکار بهره‌برداری موثر از طیف الکترومغناطیس (و در نتیجه

[1] Exploit

[2] Attack Vector

[3] Passive CEW

[4] Active CEW

[5] Jamming

شبکه) برای دشمن یا استفاده از سلاح‌های الکترومغناطیس[1] برای از بین بردن ابزارهای الکترونیکی سکوی خصمانه انتخاب شده است. برای انجام حملات سایبری از طریق شبکه‌های بی‌سیم، انجام اقدامات جنگ الکترونیک برای تعیین مشخصات ارتباطات شبکه ضروری است. به‌عنوان نمونه، هواپیمای جنگنده F-35 به لطف توانایی پردازنده اصلی خود در یکپارچه‌سازی عملکردهای مختلف، می‌تواند عملیات شناسایی، اختلال تهاجمی/ دفاعی و حملات سایبری را از یک سکو جنگی انجام دهد (PVSM, AVSM, VSM, 2017: 11).

وزارت دفاع آمریکا در سند عملیات جنگ الکترونیک و فضای سایبر به چندین چالش و تهدید در یکپارچه‌سازی فعالیت‌های فضای سایبر و طیف الکترومغناطیش اشاره نموده است. اولین چالش و تهدید که در این سند به آن اشاره شده است گسترش فن‌آوری‌های تلفن همراه، به‌ویژه در کشورهای در حال توسعه است. گسترش این فناوری می‌تواند به طور چشمگیری تعداد افرادی که قادر به دسترسی و به اشتراک‌گذاری سریع اطلاعات هستند را افزایش دهند. از دیگر فناوری‌های چالشی که در این سند به آن اشاره شده است، رشد بیش از حد بکارگیری ابزارهای خودمختار در میدان نبرد است، این ابزارهای خودمختار همچون سامانه‌های هوایی بدون سرنشین، امنیت را به چالش می‌کشد. توسعه پیشرفته فناوری‌های مستقل در آینده را تصویر کنید که ماشین‌ها با استفاده از الگوریتم‌های پیشرفته و هوش مصنوعی، در میدان نبرد تصمیم می‌گیرند. در نتیجه، این الگوریتم تصمیم‌گیری ممکن است ربوده شوند و هوش مصنوعی دچار نقص شود.

بسیاری از نوآوری‌های طیف الکترومغناطیس سیستم‌های دوگانه (کاربردهای غیر نظامی و نظامی) هستند که قادرند مستقیم آنچه را که قبلاً یک حصار نظامی منحصر به فرد بود، به چالش بکشند، و به طور بالقوه اجازه می‌دهند تا مخالفان بتوانند با قابلیت‌های نظامی کشورهای پیشرفته از جمله ایالات متحده به برابری برسند. لذا نیروهای نظامی با محیطی پیچیده و چالش برانگیز روبرو شده‌اند که توزیع گسترده فضای سایبر و فناوری‌های طیف

[1] EMP

الکترومغناطیس همچنان به محدود کردن مزیت قدرت رزمی که ارتش نسبت به دشمنان بالقوه داشته است، ادامه خواهد داد. گسترش سلاح‌های فضای سایبری و قابلیت‌های طیف الکترومغناطیس تهدید فزاینده‌ای علیه نیروی نظامی وابسته به فضای سایبری است که به فناوری‌های دیجیتالی متکی است. این چالش‌های آینده به طیف کاملی از فضای سایبر و قابلیت‌های جنگ‌الکترونیک نیاز دارد. تا بتواند فرماندهان را برای انطباق با مأموریت‌هایی که به سرعت در حال تغییر هستند از قبیل انجام عملیات غیرمتمرکز در مناطق وسیع، حفظ آزادی عملیاتی مانور، اجرای فرمان مأموریت، و به‌دست آوردن و حفظ ابتکار عمل در فضای سایبر و طیف الکترومغناطیس در طول عملیات تسلیحاتی مشترک، سوق دهد(U.S. Department of the Army Headquarters, 2018 : 20-21).

در مقاله‌ای تحت عنوان « نقاط اصطکاک، اهداف عملیاتی و فرصت‌های تحقیقاتی همگرایی جنگ الکترونیک و سایبری» که ماحصل مباحث کارشناسان و متخصصان نظامی، دولتی، تجاری و دانشگاهیان در کارگاه همگرایی سایبری و جنگ الکترونیک در حاشیه کنفرانس «اقدامات سایبرالکترومغناطیس» در سال ۲۰۱۸ در ایالات متحده برگزار گردیده است، خبرگان حوزه سایبری و جنگ الکترونیک ایالات متحده بر این عقیده‌اند که همچون هر یکپارچه‌سازی، یکپارچه‌سازی حوزه سایبر و جنگ الکترونیک هم نقاط اصطکاک شامل فرهنگ[1]، سیاست[2]، دکترین[3]، عملیات[4] و فناوری[5] که می‌تواند موانعی را برای دستیابی به یک سازمان منسجم ایجاد کند. برای مقابله با این چالش‌ها، ارتش ایالات متحده باید کمبودهای ادغام در دکترین، سازمان[6]، آموزش عملی[1]، مواد[2]، رهبری[3] و

[1] culture

[2] policy

[3] doctrine

[4] operations

[5] echnology

[6] organization

آموزش نظری[4]، پرسنل[5]، امکانات[6] و سیاست (DOTMLPF-P) را شناسایی و برطرف کند. یکپارچه سازی اغلب با برخورد شخصیت‌ها[7]، فرهنگ‌ها، اولویت‌ها[8] و فرماندهی که منجر به ایجاد اصطکاک یا مقاومت در برابر یکپارچه شدن می‌شود، دست و پنجه نرم می‌کنند. یکی دیگر از مباحث مطرح شده در این کارگاه، ظهور فناوری‌های پیشرفته در قابلیت‌های جنگ‌الکترونیک و فضای سایبر است که به کارکنان چیره‌دست(باتجربه) فناورانه نیاز است. و افرادی که ملزم به انجام این مأموریت‌ها هستند ذاتاً در محیط کار عمومی به‌دنبال آن هستند و ارزش و فرصت‌های شغلی آن‌ها تنها با دریافت آموزش‌های پیشرفته افزایش می‌یابد. این حقایق چالش‌هایی را برای جذب و حفظ این نیروها ایجاد می‌کند. با توجه به اینکه عملیات نظامی سنتی از طریق یک رویکرد مرحله‌ای بررسی و اجرا می‌شوند، مراحل برنامه‌ریزی و اجرای عملیات جنگ الکترونیک/سایبر دشوار است. دشواری در شناسایی مراحل جنگ در فضای سایبری زمانی تشدید می‌شود که ما سعی می‌کنیم دکترین عملیات سنتی را در شرایط خاص (اجرای عملیات اطلاعاتی) به‌کار ببریم(Cox et al.,2019 : 95).

در سند دکترین مشترک انگلستان تحت عنوان «فعالیت های سایبری و الکترومغناطیس» ذکر شده است که هزینه‌های پایین نفوذ و بدست آوردن سریع فناوری‌های پیشرفته برای دشمنان و مخالفان انگلستان و متفقین، بدان معنی است که ممکن است آن‌ها به همان اندازه یا بهتر از ما باشند که در استفاده از اطلاعات به عنوان چند برابر کننده توان نیرویی قرار

---

[1] Training(آموزش (فرایند) ایجاد مهارت های خاص در فرد)

[۲] materiel

[3] Leadership

[4] Education(آموزش نظری در کلاس درس یا هر موسسه ای)

[5] personnel

[6] facilities

[7] personalities

[8] priorities

بگیرند. با این حال، چالش ما عملیاتی کردن در محدودیت‌های انگلستان و متفقین، سیاست، دکترین و قانون است، در حالی که مخالفان ما نیازی به این ندارند و در واقع نتیجه‌ای در این امر ندارند. و یکی دیگر از چالش‌های یکپارچه سازی حوزه سایبرالکترونیک در عملیات‌های مشترک و ائتلافی، دستیابی به قابلیت همکاری و حفظ تعادل دانشی در حین انجام عملیات است. در این سند، رشد سریع اقدامات غیر فیزیکی، تصور سنتی از رفتار خصمانه و پاسخگویی به قوانین بین المللی را به چالش می‌کشد. عملیات سایبر همزمان با جنگ الکترونیک در زمینه رویکرد تمام طیف ممکن است نیروهای سنتی را که برای درگیری در محیط الکترومغناطیس و فضای سایبری به طور همزمان آماده نیستند، مغلوب کند. این وضعیت اکنون وجود دارد که با استفاده از فعالیت های الکترومغناطیس و سایبر، مزیت فناوری توسط جنگ غیر متعارف از بین برود(UK Ministry of Defence, 2018 : 06).

در گزارش دانشکده نیروی هوایی ایالات متحده آمریکا تحت عنوان «جنگ در طیف الکترومغناطیس و فضای سایبری»، از تاثیر نامتقارن توسعه سریع فناوری‌های بر توانایی‌های نظامی سنتی ایالات متحده به عنوان بزرگترین چالش در سطه خود بر جهان یاد کرده است. بزرگترین چالش این سلطه که امروزه دیده می‌شود، تأثیر نامتقارن توسعه سریع فناوری بر توانایی‌های نظامی سنتی ایالات متحده است. بسیاری از نیروهای اصلی ارتش ایالات متحده برای اولین بار به‌دلیل این پیشرفت‌های فنی در معرض خطر قرار دارند، که اغلب این تجهیزات با کسری از هزینه سیستم تسلیحاتی تهدید شده تولید می‌شوند. این مقاله استدلال می‌کند که نیروی هوایی ایالات متحده برای حفظ سلاح و تراکم سنسور در یک سناریوی ضد دسترسی، باید در مورد عملیات خود در فضای سایبری و از طریق فضای سایبری و طیف الکترومغناطیسی متفاوت فکر کند و عمل کند. در این گزارش ذکر شده است که به‌طور خاص، ساختار نیروهای عملیاتی فضای سایبر و جنگ الکترونیک نیروی هوایی ایالات متحده برای پاسخگویی به الزامات فرمانده جنگ بهینه نشده است، بنابراین باید تحت ساختار فرماندهی عملیات سایبرالکترومغناطیس دوباره آرایش داده شوند تا از

دسترسی و استفاده از فضای سایبری و طیف الکترومغناطیس در سال ۲۰۴۰ اطمینان حاصل شود (Cole, 2014: 01-02).

در سند منشر شده از وزارت دفاع استرالیا تحت نام « مرکز جنگ الکترونیک و سایبری »، از سهولت دسترسی به فناوری های تجاری با هزینه کم به‌عنوان یک چالش فناورانه برای نیروهای نظامی یاد کرده است. همچنین فضای سایبر و جنگ الکترونیک با چالش‌های ناشی از افزایش سهولت استفاده از فناوری تجاری برای ایجاد تهدیدهای ناشناخته قبلی با هزینه نسبتا کم مواجه هستند. از دیگر چالش‌های ذکر شده در این سند، پیچیدگی و پویایی فضای سایبر که همچنان در حال رشد است، این امر با افزایش تقاضا برای تحرک، انفجار در تعداد و تنوع دستگاه‌های شبکه، رمزگذاری در همه‌جا، افزایش حجم داده‌ها و استفاده گسترده از سیستم‌های تعریف شده توسط نرم‌افزار ایجاد می‌شود. این روندهای فناوری به طور جمعی چالش‌های تحقیقاتی مهمی را برای‌حفظ و گسترش قابلیت‌های سگینت و سایبری برای دسترسی، تجزیه و تحلیل، بهره‌برداری و دفاع ارائه می‌دهد. شبکه‌های ارتباطی و قابلیت‌های بی‌سیم در سایبری، مرکزی برای این مشکل هستند (AU Department of Defence, 2016: 03).

در دستورالعمل تحت عنوان « دستورالعمل امنیت سیستم‌های کنترل صنعتی» تغییرات در ساختار سیستم‌های کنترل صنعتی(اتصال به اینترنت)، آن‌ها را در معرض انواع جدیدی از تهدیدها قرار داده و احتمال این‌که سیستم‌های کنترل صنعتی به خطر بی‌افتد را به میزان قابل توجهی افزایش داده است. این سند در بخشی دیگر ذکر کرده است که بسیاری از فرآیندهای سیستم‌های کنترل صنعتی، عملکرد پیوسته‌ای دارند. لذا خاموشی غیرمنتظره سیستم‌هایی که فرآیندهای صنعتی را کنترل می‌کنند قابل قبول نیست. خاموشی‌ها اغلب باید برنامه‌ریزی شده باشد. در نتیجه عملکرد سیستم عامل سامانه‌های کنترل صنعتی و برنامه‌های کاربردی ممکن است شیوه‌های معمول امنیت فناوری اطلاعات (که اختلال در عملکرد آنها در کوتاه مدت حیاتی نیست) را تحمل نکنند. از دیگر چالش‌هایی که در این سند ذکر شده است، نرم‌افزارهای وصله نشده است. این نرم‌افزارها یکی از بزرگترین

آسیب‌پذیری‌های یک سامانه کنترل صنعتی است. به‌روزرسانی نرم‌افزار در سیستم‌های فناوری عملیاتی، از جمله وصله‌های امنیتی، معمولاً به موقع و براساس خط مشی و رویه های امنیتی مناسب اعمال می‌شود. علاوه بر این، این روش‌ها اغلب با استفاده از ابزارهای مبتنی بر سرور، خودکار می‌شوند. بروزرسانی‌های نرم‌افزاری روی سیستم‌های کنترل صنعتی همیشه نمی‌تواند به موقع اجرا شود زیرا این بروزرسانی‌ها باید قبل از اجرا توسط فروشنده برنامه کنترل صنعتی و کاربر نهایی برنامه مورد آزمایش کامل قرار گیرد و خاموشی سیستم‌های کنترل صنعتی اغلب باید روزها یا هفته‌ها قبل برنامه‌ریزی شود. مسئله دیگر این است که بسیاری از سیستم‌های کنترل صنعتی از نسخه‌های قدیمی سیستم‌عامل‌هایی استفاده می‌کنند که دیگر توسط فروشنده پشتیبانی نمی‌شوند. در نتیجه، وصله‌های موجود ممکن است قابل استفاده نباشند (Stouffer, Scarfone, 2013: 30).

در مقاله تحت عنوان «همگرایی فناوری‌های اطلاعات و فناوری‌های عملیات در زیرساخت‌های حیاتی» از تاخیر در ارسال اطلاعات در سامانه های فناوری عملیات به عنوان چالش اساسی ذکر شده است. تأخیر در اطلاعات که از واحد ترمینال از راه دور[1] به ترمینال اصلی سامانه‌های کنترل صنعتی[2] ارسال می‌شود، می‌تواند منجربه یک رویداد فاجعه‌بار شوند زیرا اطلاعات دستخوش تغییر می‌تواند سرعت توربین، سنسور سطح، سنسور زنگ یا محرک‌ها دیگر باشد. در ادامه این مقاله ذکر شده است، اکثریت قریب به اتفاق سیستم‌های فناوری عملیات به‌صورت ایزوله از سیستم‌ها و زیرساخت‌های فناوری اطلاعات عمل می‌کنند، که معمولاً از آن به عنوان «شکاف هوایی» یاد می‌شود و به سادگی نمی‌توان حملات سایبری را از منظر تشخیص یا دفاع طراحی کرد. شرکت‌های فناوری عملیاتی از نظریه شکاف هوایی به عنوان یک مانع استفاده می‌کنند، زیرا معتقدند سایت‌های مربوطه در برابر حملات سایبری آسیب‌پذیر نیستند. این طرز فکر خود آسیب‌پذیری قابل

[1] RTU

[2] ICS/DCS/SCADA

توجهی را در بازه‌های زمانی تعمیر و نگهداری نشان می‌دهد (Murray, Johnstone and Valli, 2017: 150).

در مقاله تحت عنوان «امنیت سامانه‌های اسکادا در مقابله با حملات فیزیکی-سایبری»، با در نظر گرفتن این ویژگی متمایز سیستم‌های کنترل صنعتی از جمله سامانه‌های اسکادا، ممکن است به دشمنان این فرصت را بدهد که زیرساخت‌های حیاتی را با استفاده از شبکه کامپیوتری به‌جای یک حمله فیزیکی دقیق (و پرهزینه) هدف قرار دهند (V. V. L. Do, Fillatre, Nikiforov and Willett, 2017: 31).

یاشار در مقاله خود تحت عنوان «مزایای عملیاتی استفاده از جنگ سایبرالکترونیک در میدان نبرد» آورده است، گرچه بسیاری از شبکه‌های فرماندهی و کنترل ارتش و سیستم‌های دفاع هوایی شبکه‌های ایزوله یا بسته‌ای هستند که مستقیماً در دسترس نیستند. باتوجه به این، ما باید تهدیدهای سایبری را برای ارتش یا در میدان جنگ نه تنها با شبکه بلکه با انرژی الکترومغناطیسی مورد حمله قرار دهیم. در ادامه یاشار ذکر کرده است، حتی شبکه هایی که مستقیماً به اینترنت متصل نیستند، ممکن است با استفاده از انرژی الکترومغناطیس برای وارسی یا ایجاد اختلال در اجزای الکترونیکی شبکه، به‌طور بالقوه دسترسی ایجاد گردد و یا مورد حمله قرار گیرد. نکته دیگر این‌که، حمله الکترونیکی قابل تشخیص است و دشمنان می‌توانند اقدامات مختلفی را انجام دهند در حالی که تشخیص حمله سایبرالکترونیک تقریباً غیرممکن است. حتی اگر حمله سایبرالکترونیک شناسایی شود، می‌توان گفت که اقدامات احتیاطی در برابر آن خیلی دیر است (YASAR, YASAR and TOPCU, 2012:09).

در مقاله «مکانیزم راه اندازی حملات سایبری در سنسورها و سامانه‌های دریایی»، نویسنده به این نکته توجه کرده است که یکپارچه‌سازی سیستم‌های دریایی سنتی با فناوری‌های نوین دیجیتالی ممکن است فضا را برای توسعه استراتژی‌های حمله جدید باز کند. در ادامه این مقاله آمده است که در طراحی شناورهای امروزی، سیستم‌های شناسایی خودکار اغلب به سیستم‌های ناوبری یکپارچه و سایر فناوری‌های شبکه مانند نمایش

نمودار و سیستم اطلاعات الکترونیکی (سیستم اطلاعات و نمایش نقشه الکترونیکی) متصل است. که باعث ایجاد یک فرآیند سایبری مخرب در شناور می‌شوند. نویسنده در ادامه بیان نموده است که تهدیدات سایبری مربوطبه ضعف‌های سیستم عامل سامانه ناوبری یکپارچه است و مهاجم با سوءاستفاده از آسیب‌پذیری‌های ارتباطی قابل جابجایی یا حتی حملات زنجیره تامین، بدافزار را در سیستم موردنظر از جمله رایانه رادار یا رایانه سیستم اطلاعات و نمایش نقشه الکترونیکی متصل به گیرنده AIS تزریق می‌کند (Leite Junior et al., 2021: 07).

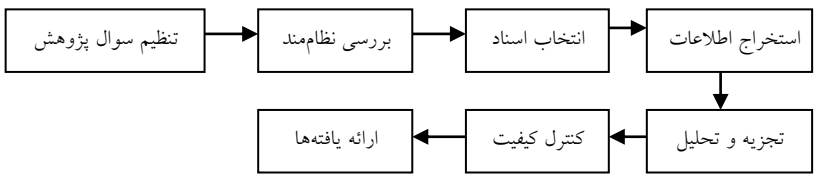
آقای استفان در گزارش وزارت دفاع سوئیس تحت عنوان« هم افزایی در میدان نبرد و توسعه فعالیت‌های سایبر الکترومغناطیسی » از این که در جنگ‌های مدرن، ارتش‌ها در یک محیط بسیار متراکم، رقابتی و پیچیده طیف الکترومغناطیس، چگونه پایدار می‌مانند، عمل می‌کنند و پیروز می‌شوند به‌عنوان چالش عمده‌ای نام برده است (Soesanto, 2021: 07).

در سند وزارت دفاع انگلیس تحت عنوان «مفهوم نیروی آینده» ذکر شده است، در یک محیط سخت و مناقشه‌آمیز ممکن است لازم باشد وابستگی به محیط الکترومغناطیس را کاهش دهیم. ما باید حالت‌های برگشتی را طراحی کنیم که در برابر محیط الکترومغناطیس انکار شده یا تنزل داده شده اعمال گردد و سپس به‌طور منظم تمرین و آزمایش کنیم. اتکای بیش از حد به فناوری برای تقویت فرماندهی و کنترل، یک ضعف بالقوه مهم است. اگر ما نسبت به حریف خود در برابر این تهدید مقاوم‌تر باشیم، می‌توانیم مزیت ایجاد کنیم و محیط الکترومغناطیس را تا حدی تنزل دهیم که بتوانیم عمل کنیم، درحالی‌که آن‌ها نمی‌توانند (UK Ministry of Defence, 2017:24).

۲. روش‌شناسی تحقیق

پژوهش حاضر از نظر داده‌ها و روش تحلیل، کیفی و از لحاظ روش گردآوری داده‌ها، اسنادی است. در این پژوهش از رویکرد فراترکیب استفاده شده است. در رویکرد فراترکیب با فراهم کردن نگرشی نظام‌مند برای محقق از طریق ترکیب پژوهش‌های کیفی

مختلف به کشف موضوعات و استعاره‌های جدید و اساسی می‌پردازد. در نتیجه ضمن ارتقاء دانش جاری، دید جامع و گسترده‌ای را به مسائل به‌وجود می‌آورد. (شهبازی سلطانی و صواتیان، ۱۳۹۶ : ۲۰۷). در این پژوهش از هفت مرحله‌ای فراترکیب سندلوسکی و بارسو(۲۰۰۷) استفاده شده است.



شکل(۱): مراحل هفتگانه فراترکیب

تنظیم سوال پژوهش

نخستین گام در رویکرد فراترکیب، تنظیم سوال پژوهش است که غالباً با تمرکز بر سوالات «چه چیزی»[1]، «چه کسی»[2]، «چه وقت»[3] و «چگونه»[4] بدست می‌آید. در پاسخ به سوال «چه چیزی؟» حوزه سایبر الکترونیک که از در هم‌تنیدگی فضای سایبر و طیف الکترومغناطیس شکل گرفته است دارای چالش‌ها و تهدیداتی است که در نبردهای حاضر و آینده نه چندان دور نقش کلیدی در پیروزی و شکست بازیگران صحنه نبرد سایبرالکترونیک خواهد داشت، لذا هدف از این پژوهش احصاء چالش‌ها و تهدیدات حوزه سایبرالکترونیک است.

در پاسخ به سوال «چه کسی؟» جامعه مورد مطالعه مشخص می‌گردد. جامعه مورد مطالعه در این پژوهش اسناد کشورهای صاحب‌نام در حوزه سایبرالکترونیک و مقالات

[1] What

[2] Who

[3] When

[4] How

مرتبط با این حوزه در دهه اخیر که باتوجه به کلیدواژهای ذکر شده در کاوشگرهای عمومی و اختصاصی خارجی و داخلی، جستجوگردیده است.

در پاسخ به سوال «چه وقت؟» باتوجه به این که حوزه سایبرالکترونیک از حوزه‌های نوپدید است. لذا کلیه اسناد و مقالات در دسترس، مورد بهره‌برداری قرار گرفته‌اند و چارچوب زمانی برای این پژوهش درنظر گرفته نشده است.

در پاسخ به سوال «چگونه؟» که اشاره به روش تجزیه و تحلیل داده‌های و یافته‌های از اسناد مطالعه شده دارد. در رویکرد فراترکیب، کلیه اسناد و مقالات در دسترس مورد مطالعه دقیق قرار گرفته و با استفاده از تحلیل محتوا و نرم‌افزار مکس کیودا۲۰۲۰[1]، متون به شیوه‌ای قاعده‌مند و گام‌به‌گام به واحدهای تحلیلی تقسیم و با دنبال کردن سؤال اصلی یا همان مسئله پژوهش، کدگذاری اولیه صورت گرفت. سپس با استفاده از محتوا و مضمون واحدهای کدگذاری شده است، و سپس کد محور برای هر یک از این واحدها استخراج و براساس کد محور، کدهای اولیه دسته بندی گردیدند. در نهایت با استفاده از تحلیل کدهای محور، مقوله‌های چالشی و تهدیدزای حوزه سایبرالکترونیک احصا گردیده است.

بررسی نظام‌مند متون

در پژوهش حاضر در گام اول، براساس کلید واژه‌های سایبرالکترونیک[2]، سایبرالکترومغناطیس[3]، جنگ سایبر و جنگ الکترونیک در وبگاه‌های گوگل اسکالر[4]، پروکوئست[5]، ساینس دایرکت[6] و سای-هاب[7] جستجو گردید. و سپس در گام دوم، در

---

1 MAXQDA 2020

2 Cyber Electronic

3 Cyber Electromagnetic

4 Scholar. Google. Com

5 ProQuest. Com

6 ScienceDirect. Com

7 SCI-HUB.Se

حین بررسی مقالات و اسناد، با رجوع به منابع مقالات، نسبت به استخراج اسناد و مقالات مرتبط با عنوان پژوهش اقدام گردید.

انتخاب اسناد و مقالات مناسب

در این مرحله، در گام اول پژوهشگر براساس چکیده مقالات نسبت به رد مقالات غیر مرتبط باعنوان تحقیق اقدام و در گام دوم با بررسی روش شناسی و نتیجه‌گیری مقالات، مقالات برتر پالایش و در گام سوم نسبت به مطالعه محتوای مقالات برگزیده اقدام گردید.

استخراج اطلاعات

به‌طور پیوسته و در چندین مرتبه منابع منتخب و برگزیده، بررسی و مورد کنکاش دقیق قرار گرفت و در نهایت عبارات و جملات مرتبط با عنوان پژوهش که به‌صورت مستقیم و یا غیر مستقیم به مقوله چالش‌ها و تهدیدات حوزه سایبرالکترونیک اشاره داشته، با استفاده از نرم‌افزار مکس کیودا دسته‌بندی و کدگذاری گردید.

۳. تجزیه و تحلیل یافته‌ها

هدف در رویکرد فراترکیب ایجاد بستر تفسیر یکپارچه و یکنواخت از یافته‌ها است. واحد تحلیل در این پژوهش، جملات و عباراتی است که اشاره مستقیم و یا غیر مستقیم به چالش‌ها و تهدیدات حوزه سایبرالکترونیک نموده است. مطابق جدول(۱)، محتوای اسنادی که مرتبط با چالش‌های و تهدیدات حوزه سایبرالکترنیک بوده است استخراج، سپس واحدهای تحلیل که بیان کننده نوع چالش است به عنوان کد ثبت گردیده است. تجزیه و تحلیل یافته‌های حاصل از مطالعه و تحلیل اسناد، با استفاده از تحلیل محتوا، کدگذاری گردید، سپس با بررسی کدهای اولیه و با توجه به محتوا و مضامین عبارات کدگذاری شده دسته‌بندی و به هر دسته یک کدمحور اختصاص داده شد. در نهایت با آنالیز دقیق کدهای محور، مقوله‌های اصلی که بیان کننده چالش‌ها و تهدات حوزه سایبرالکترونیک است، انجام گردیده است.

جدول(۱): استخراج کدها از محتوای اسناد

محتوای سند	کد
تغییرات (اتصال سامانه‌های اسکادا به اینترنت) در سیستم‌های کنترل صنعتی آن‌ها را در معرض انواع جدیدی از تهدیدها قرار می‌دهد.	شبکه محورشدن سامانه‌های کنترل صنعتی
در طراحی شناورهای امروزی، سیستم‌های شناسایی خودکار اغلب به سیستم‌های ناوبری یکپارچه و سایر فناوری‌های شبکه متصل است.	شبکه محور شدن سامانه‌ها و سنسورها
حمله ویروسی به سیستم‌های ناوبری کشتی‌ها برای ایجاد اختلال در دقت آتش موشک‌ها	حمله به سیستم‌های ناوبری
حملات بدافزار به سیستم‌های اویونیک هواپیما و سیستم‌های هدایت پهپاد که منجربه تخریب سکوها می‌شود.	حمله به سیستم اویونیک و هدایت هواپیما و پهپاد
اکنون با همگرایی جنگ سایبر و جنگ الکترونیک یک شکل مرگبار جدید از جنگ ایجاد شده است.	حملات فیزیکی
اقدامات سایبرالکترومغناطیس شامل فعالیت‌های سایبر و فعالیت‌های الکترومغناطیس است، اما هیچ تعاریفی تأیید شده برای فعالیت‌های سایبر یا اقدامات الکترومغناطیس وجود ندارد.	مفاهیم نظری
بزرگترین چالشی که نیروی هوایی با آن روبرو است تعریف جدیدی از روابط بین فضای سایبری و عملیات طیف الکترومغناطیس است.	تعریف روابط
معمولاً نگرانی‌های آن‌ها حول دو ایده است: یا جنگ الکترونیک جذب عملیات فضای سایبر می‌شود، یا این‌که عملیات فضای سایبری بخشی از عملیات جنگ الکترونیک یا طیف الکترومغناطیس می‌شود.	جذب فضای سایبر در جنگ الکترونیک، جذب جنگ الکترونیک در فضای سایبر
استفاده از روش‌های پرش فرکانسی و طیف گسترده، حتی شناسایی بازیگران در محیط الکترومغناطیس چالش برانگیز است.	بسیار تکنیکی
چالش عمده‌ای که جنگ مدرن – هم اکنون و هم در آینده – با آن مواجه است، این است که چگونه ارتش‌ها در محیط‌های بسیار متراکم، رقابتی و پیچیده طیف الکترومغناطیس زنده می‌مانند، عمل می‌کنند و پیروز می‌شوند.	محیط‌های بسیار متراکم محیط‌های بسیار رقابتی محیط‌های بسیار پیچیده
ارتش با محیطی پیچیده و چالش برانگیز روبرو شده است که توزیع گسترده فضای سایبر و فناوری‌های طیف الکترومغناطیس همچنان به محدود کردن مزیت قدرت رزمی که ارتش نسبت به دشمنان بالقوه داشته است، ادامه خواهد داد. گسترش سلاح‌های فضای سایبری و قابلیت‌های طیف الکترومغناطیس تهدید فزاینده‌ای علیه نیروی ارتش	گسترش فضای سایبر و گسترش فناوری‌های طیف الکترومغناطیس گسترش سلاح‌های فضای سایبری و گسترش قابلیت‌های طیف الکترومغناطیس

وابسته به فضای سایبری است که به فناوری‌های دیجیتالی متکی است.	
تشخیص حمله سایبرالکترونیک تقریباً غیرممکن است. حتی اگر حمله سایبرالکترونیک شناسایی شود، می‌توان برای اقدامات احتیاطی در برابر آن خیلی دیر است.	غیرقابل تشخیص بودن حملات سایبرالکترونیک
این روندهای فناوری به‌طور جمعی چالش‌های تحقیقاتی مهمی را برای حفظ و گسترش قابلیت‌های سگینت و سایبر برای دسترسی، تجزیه و تحلیل، بهره‌برداری و دفاع ارائه می‌دهد.	روندهای فناوری
در یک محیط سخت و مناقشه‌آمیز ممکن است لازم باشد وابستگی به محیط الکترومغناطیس را کاهش دهیم. ما باید حالت های برگشتی را طراحی کنیم که در برابر محیط الکترومغناطیس انکار شده یا تنزل داده شده اعمال گردد و سپس به طور منظم تمرین و آزمایش کنیم. اتکای بیش از حد به فناوری برای تقویت فرماندهی و کنترل، یک ضعف بالقوه مهم است.	وابستگی به محیط الکترومغناطیس اتکای بیش از حد به فناوری
استفاده بیشتر از وسایل خودمختار در میدان نبرد، از جمله سیستم‌های هوایی بدون سرنشین، امنیت را به چالش می‌کشد.	ابزارهای خودمختار
توسعه پیشرفته فن‌آوری‌های مستقل آینده را به تصویر کنید که ماشین‌ها با استفاده از الگوریتم‌های پیشرفته و هوش مصنوعی، در میدان نبرد تصمیم می‌گیرند. در نتیجه، این الگوریتم تصمیم‌گیری ممکن است ربوده شوند و هوش مصنوعی دچار نقص شود و خطری برای نیروهای ارتش و فناوری‌ها ایجاد کند.	ربایش الگوریتم‌های تصمیم گیر ابزارهای خودمختار نقض در هوش مصنوی ابزارهای خودمختار
تأخیر در اطلاعات که از واحد ترمینال از راه دور به ترمینال سامانه‌های کنترل صنعتی ارسال می‌شود. این‌ها در نهایت می‌توانند منجربه یک رویداد فاجعه بار شوند.	نفوذ به سامانه‌های کنترل از راه دور
نیروی هوایی ایالات متحده برای حفظ سلاح و تراکم سنسور در یک سناریوی ضد دسترسی، باید در مورد عملیات خود در فضای سایبری و از طریق فضای سایبری و طیف الکترومغناطیسی متفاوت فکر کند و عمل کند.	نفوذ به سلاح‌ها و سنسورها
اکثریت قریب به اتفاق سیستم‌های فناوری عملیاتی به‌صورت ایزوله از سیستم‌ها و زیرساخت‌های فناوری اطلاعات عمل می‌کنند، که معمولاً از آن به‌عنوان «شکاف هوایی» یاد می‌شود و به سادگی	نفوذ به شبکه‌های ایزوله

نمی‌توان حملات سایبری را از منظر تشخیص یا دفاع طراحی کرد.	
گسترش فناوری‌های تلفن همراه، به‌ویژه در کشورهای در حال توسعه، به‌طور چشمگیری تعداد افرادی که قادر به دسترسی و به اشتراک‌گذاری سریع اطلاعات دارند، را افزایش می‌دهد.	گسترش فناوری‌های شبکه محور
بسیاری از نوآوری‌های طیف الکترومغناطیس سیستم‌های دوگانه (کاربردهای غیر نظامی و نظامی) هستند که قادرند مستقیم آن‌چه را که قبلاً یک حصار نظامی منحصر به فرد بود، به چالش بکشند.	فناوری‌های دوگانه
یکپارچه‌سازی سیستم‌های دریایی سنتی با فناوری‌های نوین دیجیتالی ممکن است فضا را برای توسعه استراتژی‌های حمله جدید باز کند.	سامانه‌های سنتی متصل به فناوری‌های نوین
ساختار نیروهای عملیاتی فضای سایبر و جنگ الکترونیک نیروی هوایی ایالات متحده برای پاسخگویی به الزامات فرمانده جنگ بهینه نشده است، بنابراین باید تحت ساختار فرماندهی عملیات سایبر/ الکترومغناطیس دوباره آرایش داده شوند تا از دسترسی و استفاده از فضای سایبری و طیف الکترومغناطیس در سال ۲۰۴۰ اطمینان حاصل شود.	ساختار نیروهای عملیاتی
مسئله دیگر این است که بسیاری از سیستم‌های کنترل صنعتی از نسخه‌های قدیمی سیستم عامل‌هایی استفاده می‌کنند که دیگر توسط فروشنده پشتیبانی نمی‌شوند.	نسخه‌های قدیمی سیستم عامل‌های کنترل صنعتی
نرم‌افزارهای وصله نشده یکی از بزرگترین آسیب‌پذیری‌های یک سیستم را نشان می‌دهد.	نرم‌افزارهای وصله نشده
حمله به سیستم کنترل نظارت و جمع‌آوری داده (SCADA) یک نیروگاه هسته‌ای، شبکه‌های برق و ارتباطات برای از مدار خارج کردن و ایجاد آسیب‌های فیزیکی	حمله به فناوری‌های شبکه محور(OT)
مهاجم با سوءاستفاده از آسیب‌پذیری‌های واسطه‌های قابل جابجایی یا حتی حملات زنجیره تامین، بدافزار را در سیستم موردنظر (یعنی رایانه رادار یا رایانه سیستم اطلاعات و نمایش نقشه الکترونیکی متصل به گیرنده AIS) تزریق می‌کند.	واسطه‌های سخت‌افزاری و زنجیره تامین
تهدیدات سایبری مربوط‌به ضعف‌های سیستم عامل سیستم ناوبری یکپارچه است. اقدامات متقابل پیشنهادی دو مورد است: نگهداشت پیشگیرانه (اجرای دستورالعمل‌های بازرسی دوره‌ای) و رعایت مقررات.	سیستم عامل‌های شبکه محور (نرم‌افزار)

زرگترین چالش سلطه که امروزه دیده می‌شود، تأثیر نامتقارن توسعه سریع فناوری بر توانایی‌های نظامی سنتی ایالات متحده است.	تاثیر نامتقارن فناوری بر توانایی‌های سنتی
پیچیدگی و پویایی فضای سایبر همچنان در حال رشد است. این امر با افزایش تقاضا برای متحرک‌سازی، افزایش در تعداد و تنوع دستگاه‌های شبکه، رمزگذاری در همه جا، افزایش حجم داده‌ها و استفاده گسترده از سیستم‌های تعریف شده توسط نرم‌افزار ایجاد می‌شود.	پیچیدگی و پویایی در تعداد و تنوع سنسورها شبکه محور، افزایش حجم داده‌ها
چالش‌هایی در دستیابی به قابلیت همکاری و حفظ تعادل دانشی در حین انجام عملیات مشترک و ائتلاف وجود دارد.	قابلیت همکاری در عملیات‌های مشترک و ائتلاف، دستیابی به تعادل دانشی در عملیات‌های مشترک و ائتلاف
هزینه‌های پایین ورود و اتخاذ سریع فناوری پیشرفته بدان معنی است که ممکن است آن‌ها به همان اندازه یا بهتر از ما باشند که در استفاده از اطلاعات به‌عنوان چند برابر کننده توان نیرویی قرار بگیرند.	هزینه پایین دسترسی به فناوری‌های پیشرفته
همچنین هر دو (فضای سایبر و جنگ الکترونیک) آن‌ها با چالش‌های ناشی از افزایش سهولت استفاده از فناوری تجاری برای ایجاد تهدیدهای ناشناخته قبلی با هزینه نسبتا کم مواجه هستند.	افزایش سهولت در دسترسی به فناوری‌های دوگانه
بسیاری از نیروهای اصلی ارتش ایالات متحده برای اولین بار به دلیل این پیشرفت‌های فنی در معرض خطر قرار دارند، که اغلب این تجهیزات با کسری از هزینه سیستم تسلیحاتی تهدید شده تولید می‌شوند.	هزینه پایین تجهیزات و فناوری‌های تهدید کننده
با درنظر گرفتن این ویژگی متمایز سیستم‌های اسکادا، تروریست‌ها ممکن است زیرساخت‌های ایمنی حیاتی را با استفاده از یک شبکه کامپیوتری به‌جای یک حمله فیزیکی دقیق (و پرهزینه) هدف قرار دهند.	حمله به زیرساخت‌ها با هزینه پایین
حتی شبکه‌هایی که مستقیماً به اینترنت متصل نیستند، ممکن است با استفاده از انرژی الکترومغناطیس برای وارسی یا ایجاد اختلال در اجزای الکترونیکی شبکه، به‌طور بالقوه دسترسی ایجاد کنند و یا مورد حمله قرار گیرد.	شبکه‌های ایزوله
در حقیقت، بسیاری از شبکه‌های فرماندهی و کنترل ارتش و سیستم‌های دفاع هوایی شبکه‌های ایزوله یا بسته ای هستند که	شبکه‌های فرماندهی و کنترل و سامانه‌های دفاع هوایی

مستقیماً در دسترس نیستند. باتوجه به این، ما باید تهدیدهای سایبری را برای ارتش یا در میدان جنگ نه تنها با شبکه بلکه با انرژی الکترومغناطیسی مورد حمله قرار دهیم.	
آزادی مانور نیروها، آزادی عمل، مزیت اطلاعات، برتری تصمیم و ارائه مزیت عملیاتی، این‌ها به نوبه خود به منابع کافی، از جمله نیروی انسانی توانمند برای تصمیم‌گیری و اجرای تغییر در عناصر لازم دفاع نیاز دارند.	نیروی انسانی توانمند
باتوجه به این‌که عملیات نظامی سنتی از طریق یک رویکرد مرحله‌ای بررسی و اجرا می‌شوند، مراحل برنامه‌ریزی و اجرای عملیات جنگ الکترونیک/سایبردشوار است. دشواری در شناسایی مراحل جنگ در فضای سایبری زمانی تشدید می‌شود که ما سعی می‌کنیم دکترین عملیاتی سنتی را در این شرایط بکار ببریم.	طرح‌ریزی و اجرا
یک چالش این است که نوع افرادی که ملزم به انجام این مأموریت‌ها هستند ذاتاً در محیط کار عمومی به‌دنبال آن هستند و ارزش و فرصت‌های شغلی آن‌ها تنها با دریافت آموزش‌های پیشرفته در خدمات افزایش می‌یابد. این حقایق چالش‌هایی را برای جذب و حفظ این سربازان ایجاد می‌کند.	جذب و حفظ نیروی انسانی
ظهور فناوری‌های پیشرفته در قابلیت‌های جنگ‌الکترونیک و فضای سایبر به کارکنان چیره‌دست (باتجربه) فناورانه نیاز دارد.	نیروی انسانی چیره دست
با این حال، مانند هر ادغامی، این اداغام هم نقاط اصطکاک شامل فرهنگ، سیاست، دکترین، عملیات و فناوری می‌تواند موانعی را برای دستیابی به یک سازمان منسجم ایجاد کند. برای مقابله با این چالش‌ها، ارتش ایالات متحده باید کمبودهای ادغام در دکترین، سازمان، آموزش عملی، مواد، رهبری و آموزش نظری، پرسنل، امکانات و سیاست (DOTMLPF-P) را شناسایی و برطرف کند.	دکترین، سازمان، آموزش عملی، آموزش نظری، مواد رهبری، کارکنان، امکانات، سیاست، فرهنگ، عملیات، فناوری
چالش ما عملیاتی کردن در محدودیت‌های انگلستان و متفقین، سیاست، دکترین و قانون است، در حالی که مخالفان ما نیازی به این ندارند و در واقع نتیجه‌ای در این امر ندارند.	سیاست، دکترین، قانون
ادغام‌ها اغلب با برخورد شخصیت ها، فرهنگ‌ها، اولویت‌ها و فرماندهی که منجر به ایجاد اصطکاک یا مقاومت در برابر یکپارچه شدن می‌شود، دست و پنجه نرم می‌کنند.	شخصیت‌ها، فرهنگ‌ها، اولویت‌ها، فرماندهی

آن‌چه نیروی هوایی تا بـه امـروز بـه خـوبی انجـام نـداده، همسـویی تلاش‌های خود در عملیات فضای سایبری بـا مأموریـت‌هـای جنـگ الکترونیک و عملیات طیف الکترومغناطیس می‌باشـد، بـه‌گونـه‌ای کـه به‌طـور مـوثر و جـامع از طیـف الکترومغنـاطیس و فضـای سـایبر در بیشترین توان خود استفاده کند.	عملیاتی سازی
رشد سریع اقدامات غیر فیزیکی، تصـور سـنتی از رفتـار خصـمانه و پاسخگویی به قوانین بین‌المللی را به چالش می‌کشد.	اقدامات نرم
اگرچـه هـدف در اقـدامات سـایبرالکترومغناطیس همگـام سـازی فعالیت‌های تهاجمی، دفاعی و اطلاع رسانی است، اما ممکن است در مقابل کل فعالیت‌های نیروهای مشترک عملی نباشد.	همگام سازی اقدامات سایبری و چنگ الکترونیک
روابط بین فعالیت‌های سایبر و فعالیت‌های الکترومغناطیسی هنـوز در حال بلـوغ اسـت و یـک رویکـرد واحـد بـرای اقـدامات سـایبری و الکترومغناطیس، چالشی است.	نوپدیـد بـودن روابـط حـوزه سایبرالکترونیک

مطابق جدول(۲)، ۷۲ کد از محتوای اسناد مطالعـه شـده اسـتخراج گردیـده اسـت و بـا استفاده از نرم‌افزار مکس کیودا این ۷۲ کدها براساس نوع و ماهیت چالش، به ۲۵ کـدمحور تجمیع گردید. و در نهایت از ۲۵ کدمحور، ٤ مقوله احصا گردیده است.

جدول(۲): استخراج کدها محور و مقوله ها براساس کد استخراج شده از اسناد

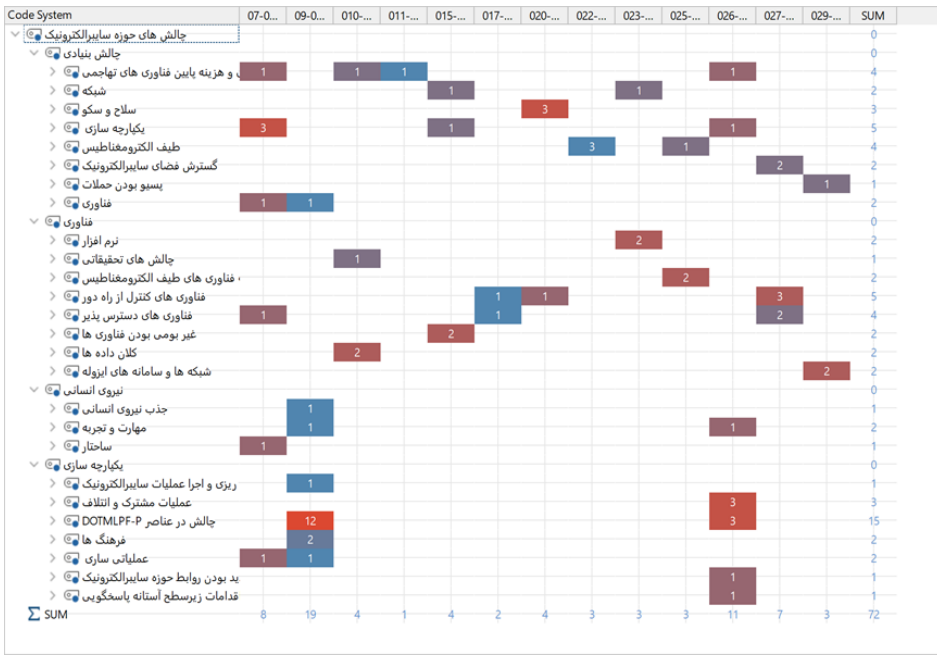
ردیف	کد	کد محور	مقوله
۱	شبکه محور شدن سامانه‌های کنترل صنعتی	شبکه	چالش بنیادین
۲	شبکه محور شدن سامانه‌ها و سنسورها	شبکه	چالش بنیادین
۳	حمله به سیستم های ناوبری کشتی‌ها	سلاح و سکو	چالش بنیادین
٤	حمله به سیستم اویونیک و هدایت هواپیما و پهپاد	سلاح و سکو	چالش بنیادین
٥	حملات فیزیکی	سلاح و سکو	چالش بنیادین
٦	مفاهیم نظری	یکپارچه سازی	چالش بنیادین
۷	روابط	یکپارچه سازی	چالش بنیادین
۸	جذب فضای سایبر در جنگ الکترونیک	یکپارچه سازی	چالش بنیادین
۹	جذب جنگ الکترونیک در فضای سایبر	یکپارچه سازی	چالش بنیادین
۱۰	بسیا تکنیکی	طیف الکترومغناطیس	چالش بنیادین
۱۱	محیط‌های بسیار متراکم	طیف الکترومغناطیس	چالش بنیادین
۱۲	محیط‌های بسیار رقابتی	طیف الکترومغناطیس	چالش بنیادین

۱۳	محیط‌های بسیار پیچیده	طیف الکترومغناطیس	چالش بنیادین
۱٤	گسترش فضای سایبر و گسترش فناوری‌های طیف الکترومغناطیس	گسترش فضای سایبرالکترونیک	چالش بنیادین
۱۵	گسترش سلاح‌های سایبری و گسترش قابلیت های طیف الکترومغناطیس	گسترش فضای سایبرالکترونیک	چالش بنیادین
۱٦	غیرقابل تشخیص بودن حملات سایبرالکترونیک	پسیو بودن حملات	چالش بنیادین
۱۷	روندهای فناوری	چالش‌های تحقیقاتی	فناوری
۱۸	وابستگی به محیط الکترومغناطیس	وابستگی به فناوری‌های طیف	فناوری
۱۹	اتکای بیش از حد به فناوری	وابستگی به فناوری‌های طیف	فناوری
۲۰	ابزارهای خودمختار	فناوری‌های کنترل از راه‌دور	فناوری
۲۱	ربایش الگوریتم‌های تصمیم‌گیر ابزارهای خودمختار	فناوری‌های کنترل از راه‌دور	فناوری
۲۲	نقض در هوش مصنوی ابزارهای خودمختار	فناوری‌های کنترل از راه دور	فناوری
۲۳	نفوذ به سامانه‌های کنترل از راه دور	فناوری‌های کنترل از راه دور	فناوری
۲٤	نفوذ به سلاح‌ها و سنسورها	فناوری‌های دسترس پذیر	فناوری
۲۵	نفوذ به شبکه‌های ایزوله	فناوری‌های دسترس پذیر	فناوری
۲٦	گسترش فناوری‌های شبکه محور	فناوری‌های دسترس پذیر	فناوری
۲۷	فناوری‌های دوگانه	فناوری‌های دسترس پذیر	فناوری
۲۸	سامانه‌های سنتی متصل به فناوری‌های نوین	یکپارچه سازی	چالش بنیادی
۲۹	ساختار نیروهای عملیاتی	ساختار	نیروی عملیاتی
۳۰	نسخه‌های قدیمی سیستم عامل‌های کنترل صنعتی	نرم‌افزار	فناوری
۳۱	نرم‌افزارهای وصله نشده	نرم‌افزار	فناوری
۳۲	حمله به فناوری‌های شبکه محور(OT)	فناوری‌های کنترل از راه‌دور	فناوری
۳۳	واسطه‌های سخت‌افزاری و زنجیره تامین	غیر بومی بودن فناوری‌ها	فناوری
۳٤	سیستم عامل‌های شبکه محور (نرم‌افزار)	غیر بومی بودن فناوری‌ها	فناوری
۳۵	تاثیر نامتقارن فناوری بر توانایی‌های سنتی	فناوری	چالش بنیادین
۳٦	پیچیدگی و پویایی در تعداد و تنوع سنسورها شبکه محور(چالش در تجزیه و تحلیل کلان داده‌ها)	کلان داده‌ها	فناوری
۳۷	افزایش حجم داده‌ها (کلان داده‌ها)	کلان داده‌ها	فناوری
۳۸	قابلیت همکاری در عملیات‌های مشترک و ائتلاف	عملیات‌های مشترک و ائتلافی	یکپارچه سازی
۳۹	دستیابی به تعادل دانشی در عملیات‌های مشرک و ائتلاف	عملیات‌های مشترک و ائتلافی	یکپارچه سازی
٤۰	هزینه پایین دسترسی به فناوری‌های پیشرفته	سهولت دسترسی و هزینه پایین فناوری های تهاجمی	چالش بنیادی
٤۱	افزایش سهولت در دسترسی به فناوری‌های دوگانه	سهولت دسترسی و هزینه پایین فناوری‌های تهاجمی	چالش بنیادی
٤۲	هزینه پایین تجهیزات و فناوری‌های تهدید کننده	سهولت دسترسی و هزینه پایین فناوری‌های تهاجمی	چالش بنیادی
٤۳	حمله به زیرساخت‌ها با هزینه پایین	سهولت دسترسی و هزینه پایین فناوری‌های تهاجمی	چالش بنیادی
٤٤	شبکه‌های ایزوله	شبکه‌های و سامانه‌های ایزوله	فناوری

٤٥	شبکه‌های فرماندهی و کنترل و سامانه‌های دفاع هوایی	شبکه‌های و سامانه‌های ایزوله	فناوری
٤٦	نیروی انسانی توانمند	مهارت و تجربه	نیروی عملیاتی
٤٧	طرح‌ریزی و اجرا	طرح ریزی و اجرا عملیات سایبرالکترونیک	یکپارچه سازی
٤٨	جذب و حفظ نیروی انسانی	جذب نیروی انسانی	نیروی عملیاتی
٤٩	نیروی انسانی چیره دست	مهارت و تجربه	نیروی عملیاتی
٥٠	دکترین	عناصر DOTMLPF-P	یکپارچه سازی
٥١	سازمان	عناصر DOTMLPF-P	یکپارچه سازی
٥٢	آموزش عملی	عناصر DOTMLPF-P	یکپارچه سازی
٥٣	آموزش نظری	عناصر DOTMLPF-P	یکپارچه سازی
٥٤	مواد	عناصر DOTMLPF-P	یکپارچه سازی
٥٥	رهبری	عناصر DOTMLPF-P	یکپارچه سازی
٥٦	کارکنان	عناصر DOTMLPF-P	یکپارچه سازی
٥٧	سیاست	عناصر DOTMLPF-P	یکپارچه سازی
٥٨	امکانات	عناصر DOTMLPF-P	یکپارچه سازی
٥٩	فرهنگ	فرهنگ	یکپارچه سازی
٦٠	فناوری	فناوری	چالش بنیادین
٦١	عملیات	عملیاتی سازی	یکپارچه سازی
٦٢	سیاست	عناصر DOTMLPF-P	یکپارچه سازی
٦٣	دکترین	عناصر DOTMLPF-P	یکپارچه سازی
٦٤	قانون	عناصر DOTMLPF-P	یکپارچه سازی
٦٥	شخصیت‌ها	عناصر DOTMLPF-P	یکپارچه سازی
٦٦	فرهنگ‌ها	فرهنگ	یکپارچه سازی
٦٧	اولویت‌ها	عناصر DOTMLPF-P	یکپارچه سازی
٦٨	فرماندهی	عناصر DOTMLPF-P	یکپارچه سازی
٦٩	عملیاتی سازی	عملیاتی سازی	یکپارچه سازی
٧٠	اقدامات نرم	اقدامات زیرسطح آستانه پاسخگویی	یکپارچه سازی
٧١	همگام سازی اقدامات سایبری و جنگ الکترونیک	عملیات‌های مشترک و ائتلافی	یکپارچه سازی
٧٢	نوپدید بودن روابط حوزه سایبرالکترونیک	نوپدید بودن روابط حوزه سایبرالکترونیک	یکپارچه سازی

کنترل کیفیت

جهت کنترل کیفیت، در گام اول با استفاده از نرم‌افزار مکس کیودا میزان ارتباط کدها با اسناد مطالعه شده استخراج گردیده است. در شکل(۲)، ستون افقی شماره اسناد (مطابق شماره مرجع) و ستون عمودی کدهای محور است. شماره‌های نشان داده شده، نشان دهنده تعداد کدهای است که از هر سند استخراج شده است. در گام دوم یافته‌های استخراج شده به همراه مراحل تجزیه و تحلیل به روش خبرگی – توسط سه تن از اساتید مرتبط با این حوزه – مورد تایید قرار گرفته است.

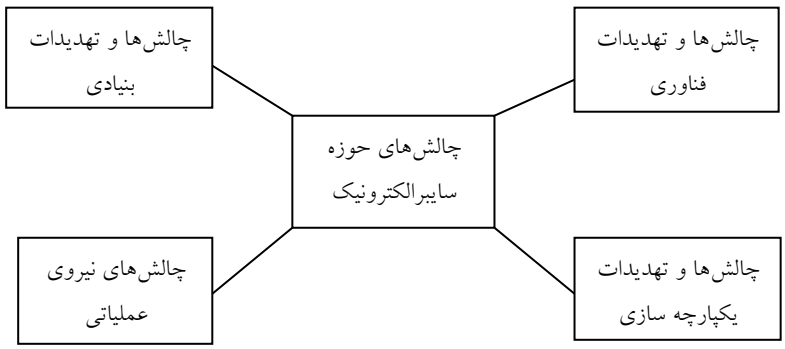


شکل(۲): ارتباط مستندات با کدهای احصا شده

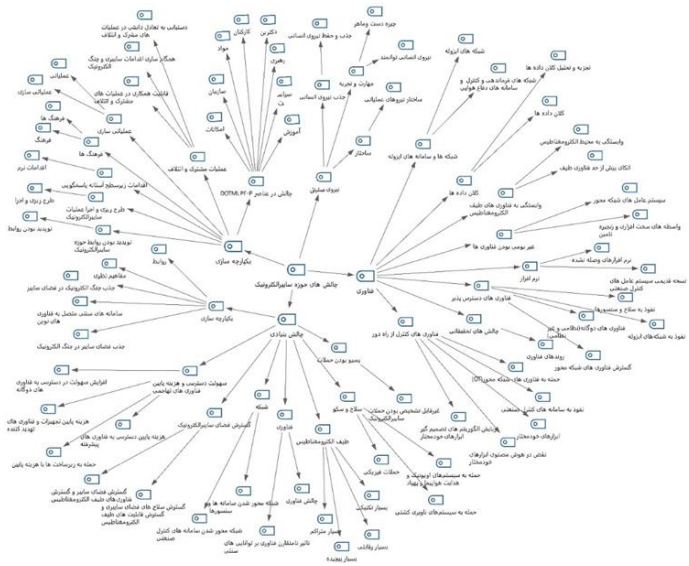
ارائه یافته‌ها

تجزیه و تحلیل یافته‌های حاصل از مطالعه و تحلیل اسناد، با استفاده از تحلیل محتوا، کدگذاری گردید، سپس با بررسی کدهای اولیه و باتوجه به محتوا و مضامین عبارات کدگذاری شده دسته‌بندی و به هر دسته یک کدمحور اختصاص داده شد. در نهایت با

آنالیز دقیق کدهای محور، مقوله‌های اصلی که بیان کننده چالش‌ها و تهدات حوزه سایبرالکترونیک می‌باشد، استخراج گردید. در این بخش از رویکرد فراترکیب، پس از انجام فرایندهای شش‌گانه، چالش‌ها و تهدیدات حوزه سایبرالکترونیک در سه لایه شامل مقوله‌ها، کدهای محور و شاخص‌های کلیدی در قالب شبکه مضامین (شکل۳) و ساختار درختی(شکل٤) استخراج گردید.



شکل(۳): شبکه مضامین چالش‌ها و تهدیدات حوزه سایبرالکترونیک



شکل(٤): ساختار درختی چالش‌های حوزه سایبرالکترونیک (کد، کد محور و مقوله)

٤. نتیجه‌گیری

مطابق طبقه‌بندی انجام شده از چالش‌ها و تهدیدات حوزه سایبرالکترونیک، چهار مقوله یکپارچه‌سازی، بنیادی، فناوری و نیروی عملیاتی مرتبط با این حوزه احصا گردیده است. باتوجه به ماهیت طیف الکترومغناطیس و فضای سایبر، و نوپدید بودن فناوری‌های سایبرالکترونیک، یک سری چالش‌ها و تهدیدات این حوزه، برگرفته از ماهیت این دو حوزه می‌باشد که این چالش‌ها و تهدیدات تحت عنوان «بنیادی» است، که معمولاً دارای ویژگی‌هایی همچون پسیو ، شبکه محور، تاثیر نامتقارن، سهولت دسترسی می‌باشند. مقوله دوم از چالش‌ها و تهدیدات، «فناوری» است، که می‌تواند برای میدان‌های نبرد ایجاد چالش و تهدید نمایند. از این مقوله‌های چالشی و تهدیدزا می‌توان به فناوری‌های کنترل از راه دور، فناوری کلان داده، فناوری‌های غیر بومی، فناوری‌های دوگانه اشاره نمود. مقوله سوم از چالش‌ها و تهدیدات که از در هم‌تنیدگی این دو حوزه خلق گردیده است در یکپارچه‌سازی حوزه سایبرالکترونیک نهفته شده است. این دسته از چالش‌ها بیشتر در عناصر DOTMLPF-P و یکپارچه‌سازی این دو حوزه در عملیاتی‌های مشترک و ائتلافی دیده می‌شود. آخرین مقوله از چالش‌ها و تهدیدات حوزه سایبرالکترونیک، که می‌توان گفت از مهمترین مقوله‌های چالش‌برانگیز این حوزه می‌باشد، «نیروی عملیاتی» است، نیروی عملیاتی در این حوزه باید خلاق، باهوش، توانمند و چیره دست باشد. اگر در حوزه‌های دیگر باهوش بودن و خلاقیت پارامتر چندم است در این حوزه باهوش بودن و خلاقیت در رتبه نخست پارامترهای انتخاب نیروی عمل کننده قرار می‌گیرد.

پیشنهادها

پیشنهادهای کاربردی:

سامانه‌ها و تجهیزات سنتی به‌ویژه تجهیزات کنترلی از قبیل اسکادا متصل به شبکه‌های محلی و اینترنت، به دلیل نداشتن مکانیزم‌های بروزرسانی پروتکل‌های امنیتی، یکی از چالش‌های اساسی در جوامع مدرن و در حال پیشرفت است.

باتوجه به چالش‌ها و تهدیدات سایبرالکترونیک مرتبط با این تجهیزات، باید نسبت به افزایش سطح آگاهی و هشدارهای لازم به کاربران این سامانه‌ها و تجهیزات، در برابر تهدیدات احتمالی اقدام نمود.

در آینده نزدیک، یکپارچه‌سازی و همزمان‌سازی فعالیت‌های سایبری و جنگ الکترونیک، یکی از چالش‌های پیش‌روی تصمیم‌سازان و تصمیم‌گیران این دو حوزه خواهد بود. لذا در راستای یکپارچه‌سازی و همزمان‌سازی کلیه فعالیت‌های سایبرالکترونیک، نسبت به تدوین دکترین، آیین‌نامه‌ها و راهبردهای حوزه سایبرالکترونیک در سطوح مختلف (راهبردی، عملیاتی و تاکتیکی) اقدام گردد.

پیشنهادهای راهبردی:

در حوزه سایبرالکترونیک، بکارگیری نیروی عملیاتی براساس ساختار سنتی یک چالش راهبردی است، در عرصه‌های دیگر مقوله کاربری سامانه‌های و تجهیزات صحنه نبرد از موقوله تحقیقاتی جداست و کسی منکر این نیست که ارتباط مابین آن‌ها به روند تحقیقاتی آن حوزه سرعت بیشتری می‌دهد. در حوزه سایبرالکترونیک، ارتباط مابین این دو، نسبت به حوزه‌های دیگر، بسیار نزدیک و در هم‌تنیده است. در این حوزه فاصله بین عنصر تحقیقاتی و کاربر عملیاتی یک چالش اساسی است. لذا در این حوزه باید دید که نیروی باهوش و خلاق عملیاتی باید دارای چه ویژگی‌هایی تحقیقاتی باشد؟ این نیروی باهوش و خلاق چه اختیاراتی (با توجه به این که عرصه‌های تحقیقات و عملیات در این حوزه در هم‌تنیده شده‌اند) باید داشته باشد؟. چه آموزش‌هایی (طولی و عرضی) باید ببیند؟ ابزارهای و نحوه مدیریت این نیرو چگونه است؟

امروزه، سرعت تغییر فناوری‌ها، یک چالش اساسی است. لذا در این حوزه باید دید که روند تغییرات فناوری‌ها در عرصه سایبرالکترونیک چگونه است؟ سرعت تغییرات فناوری در این حوزه چقدر است؟. آیا می‌توان به یک الگوی مدیریت فناوری‌های شالوده شکن و نوظهور رسید؟

فهرست منابع و مآخذ

الف. منابع فارسی

- آذرپی، بهمن (۱۳۸۵). ***جنگ‌های آینده***. فصلنامه علوم و فنون نظامی، ۲(۵)، ۱۱٤-۱۲٦.
- امیرصوفی، حشمت‌اله(۱۳۹۲). پدافند غیرعامل امن‌ترین راه برای ایستادگی در برابر دسیسه‌های دشمن. همایش آموزشی پدافند غیرعامل با رویکرد دفاع سایبری، سمنان
- حسنلو، خسرو(۱۳۹٦). ***اصول جنگ در عصر ناهمگونی‌ها***. فصلنامه مطالعات دفاعی استراتژیک، ۱۵(۷۰)، ۱۵۱-۱۷۸
- حیدری، کیومرث و عبدی، فریدون(۱۳۹۱). ***جنگ‌های آینده و مشخصات آن با تحلیلی بر دیدگاه برخی صاحب‌نظران نظامی غرب***. فصلنامه علمی-پژوهشی مدیریت نظامی، ۱۲(٤۸)، ٤۳-۷٦
- شهبازی سلطانی، محمد و صواتیان، سیاوش(۱۳۹٦). ***شناسایی ویژگی‌های معرف مدیر جهادی به روش فراترکیب***. فصلنامه علمی - پژوهشی مدیریت اسلامی،۵۲(۱)، ۱۹۹-۲۳۰
- فرح بخت، احمدرضا، و دهقانی، مهدی. (۱۳۹۸). ***همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان های نظامی***. فصلنامه امنیت ملی، ۹(۳۱)، ۲۱۹-۱۹۹.

ب. منابع انگلیسی

- Askin, O., Irmak, R., & Avsever, M. (2015, May). Cyber warfare and electronic warfare integration in the operational environment of the future: cyber electronic warfare. In Cyber Sensing 2015 (Vol. 9458, pp. 83-89). SPIE.
- AU Department of Defence. Science & Technology. (2016). Cyber and Electronic Warfare Division Strategic Plan 2016-2021
- Bommakanti, K. (2019). Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army. ORF Occasional Paper, 203.
- Choi, S., Cho, J., & Kwon, O. J. (2020). A Study on Battle Damage Assessment of Electronic Warfare associated with Cyber Warfare. Journal of Internet Computing and Services, 21(1), 201-210.

- Cole, H. T. (2014). Warfare in the Electromagnetic Spectrum and Cyberspace: United States Air Force Cyber/Electromagnetic Warfare Command Construct. Air War College, Air University Maxwell AFB United States.
- Cox, J., Bennett, D., Lathrop, S., Walls, C., LaClair, J., Tracy, C., & Esquibel, J. (2019). The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence. The Cyber Defense Review, 4(2), 81-102.
- Du Plessis, W. P. (2014, August). Software-defined radio (SDR) as a mechanism for exploring cyber-electronic warfare (EW) collaboration. In 2014 Information Security for South Africa (pp. 1-6). IEEE.
- Haig, Z. (2015). Electronic warfare in cyberspace. Security and Defence Quarterly, 7(2), 22-35.
- Henselmann, G., & Lehto, M. (2019, July). Where Cyber Meets the Electromagnetic Spectrum. In ECCWS 2019 18th European Conference on Cyber Warfare and Security (p. 209). Academic Conferences and publishing limited.
- Kim, S., Kim, S., Park, B. J., Jeong, U. S., Choo, H., Yun, J., & Kim, J. (2021). Cyber Electronic Warfare Technologies and Development Directions. The Journal of Korean Institute of Electromagnetic Engineering and Science, 32(2), 119-126.
- Leite Junior, W. C., de Moraes, C. C., de Albuquerque, C. E., Machado, R. C. S., & de Sá, A. O. (2021). A triggering mechanism for cyber-attacks in naval sensors and systems. Sensors, 21(9), 3195.
- Mallick, P. K. (2021). The PLA's Cyber Warfare Capabilities and India's Options. The Future of War in South Asia: Innovation, Technology and Organisation, 54.
- McCrory, D. (2020). Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States. The RUSI Journal, 165(7), 34-44.
- Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure.
- NATO STANDARD, AJP-3.20, (2020). ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS

- PVSM, L. G. D. R. P., & AVSM, V. (2017). CYBER ELECTRONIC WARFARE: THE MOTHER OF NON-KINETIC THREATS. Impact of Future Technologies on Warfare, 1.
- RAND Corporation. (2013). REDEFINING INFORMATION WARFARE BOUNDARIES FOR AN ARMY IN A WIRELESS WORLD
- Stouffer, K., Scarfone, K. (2013). Guide to Industrial Control Systems(ICS) Security. U.S. Department of Commerce
- Soesanto, S. (2021). A Digital Army: Synergies on the Battlefield and the Development of Cyber-Electromagnetic Activities (CEMA). CSS Cyberdefense Reports.
- UK Ministry of Defence. (2017). Future Force Concept. Development, Concepts and Doctrine Centre. Joint Doctrine Note 1/17.
- UK Ministry of Defence. (2018). Cyber and Electromagnetic Activities. Development, Concepts and Doctrine Centre. Joint Doctrine Note 1/18
- U.S. Department of the Army Headquarters. (2014). Cyber Electromagnetic Activities. Field Manual No. 3-38(FM 3-38).
- U.S. Department of the Army Headquarters, (2018). The U.S. Army Concept for Cyberspace and Electronic Warfare Operations (2025-2040).
- U.S. Department of the Army Headquarters. (2021). CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE. Field Manual No. 3-12(FM 3-12)
- V. L. Do, L. Fillatre, I. Nikiforov and P. Willett. (May 2017). Security of SCADA systems against cyber–physical attacks, in IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 5, pp. 28-45
- Yasar, N., Yasar, F. M., & Topcu, Y. (2012, May). Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield. In Cyber Sensing 2012 (Vol. 8408, pp. 151-159). SPIE.

ج. منابع عبری

- גיל ברעם ואופיר בראל(۲۰۲۰). לוחמת מידע בין המעצמות במאה ה־