فصلنامه علمی مطالعات بین‌رشته‌ای دانش‌راهبردی
سال سیزدهم، شماره ۵۱، تابستان ۱۴۰۲، صفحه ۹۰- ۶۱

مقاله پژوهشی: پیامدهای فضای سایبری برای راهبرد و امنیت دریایی کشورها

رحمان نجفی سیار[۱]

تاریخ دریافت: ۱۴۰۱/۰۳/۱۲ تاریخ پذیرش: ۱۴۰۱/۰۹/۱۵

چکیده

نقش فضای سایبری در محیط دریایی کشورها بسیار برجسته بوده و دربردارنده پیامدهای مهمی برای امنیت کشورها است. در این راستا، سوال مقاله حاضر این است که نقش‌آفرینی نیروهای دریایی در حوزه فضای سایبری چیست و متقابلاً این فضا چه پیامدهایی (فرصت‌ها و چالش‌هایی) برای امنیت و راهبرد دریایی کشورها دارند؟ در پاسخ به این سوال، با بهره‌گیری از روش توصیفی- تحلیلی و ابزار اسنادپژوهی، به این فرضیه رسیدیم که فضای سایبر، هسته اصلی موفقیت در مأموریت‌های دریایی است و اساس کنترل و فرماندهی نیروهای دریایی را تشکیل می‌دهد. سامانه‌ها و سامانه‌های مبتنی بر اطلاعات، آگاهی از فضای نبرد، جمع‌آوری اطلاعات، هدف‌گیری و قابلیت‌های دیگر را امکان‌پذیر می‌سازند. هدف نیروهای دریایی مدرن، حفظ آزادی مانور و سلب آزادی عمل دشمن در دریا است که این قابلیت را تجهیزات و توانمندی‌های سایبری فراهم می‌آورند. قابلیت‌های سایبری دشمنان همانند هدف‌گیری دقیق و حملات دوربرد به کشتی‌ها به این معنا است که نیروهای دریایی در دریا نسبت به گذشته پیوند محکم‌تری با یکدیگر دارند و در عین حال آسیب‌پذیرتر شده‌اند. موازنه سنتی قوا بین نیروهای دریایی و دشمنان به دلیل گسترش قابلیت‌های سایبری بر هم خورده است، که این امر باعث ایجاد عدم تقارن شده است. قابلیت‌های سایبری، همچنین نیروهای دریایی کوچک‌تر و بازیگران غیردولتی را به طور نامناسبی قدرتمندتر می‌کند. مقاله حاضر در راستای تبیین یافته‌های فوق، به ترسیم ساختار یا لایه‌های فضای سایبری مرتبط با مأموریت‌های نیروی دریایی، تبیین راهبرد نیروهای دریایی بین‌المللی برای فضای سایبری و مهم‌تر از همه، تبیین پیامدهای فضای سایبری برای امنیت دریایی در سه سطح راهبردی، عملیاتی و تاکتیکی پرداخته است.

کلیدواژه‌ها: فضای سایبر، راهبرد و امنیت دریایی، فرصت‌ها و چالش‌ها.

[۱] – استادیار روابط بین‌الملل دانشگاه عالی دفاع ملی؛ ایمیل political19@gmail.com

مقدمه

در شرایط جدید جهانی، به‌واسطه پیدایش فناوری اطلاعات و ارتباطات، سازمان‌های نظامی کشورها به‌طور اساسی دچار تحول شده‌اند. بسیاری از مفاهیم و فنون فرماندهی، سازمان‌دهی و تجهیزات، دچار تغییر شده و فضای تهدید و چگونگی عملیات‌های رزمی تحت تأثیر پیشرفت این حوزه قرار گرفته‌اند. کیفیت و مفاهیم نظامی شامل دکترین، سازمان، آموزش، تجهیزات و تسلیحات، رهبری و مدیریت، مهارت‌ها و نیروهای نظامی نیز به شدت تحت تأثیر این روند قرار گرفته‌اند. (کاویانی و دیگران، ۱۳۹۹: ۲۷۴)

حضور سامانه‌های پیچیده ارتباطی و الکترونیکی نوین، سناریوی نبردهای آینده را طوری تغییر داده که از یک‌سو این سامانه‌ها به فرماندهان در تصمیم‌سازی بر اساس تصاویر و اطلاعات زمان حقیقی نبرد کمک کرده و از سوی دیگر وابستگی به سامانه‌های الکترونیکی و ریزپردازنده‌ها، آنان را در برابر تهدیدات و نبردهای فضای سایبری بسیار آسیب‌پذیر کرده است (یادگاری و دیگران، ۱۳۹۶: ۳).

بر این اساس، امنیت سایبری[1] به یکی از مقوله‌های بسیار مهم در امنیت چندپارچه سازمان‌های نظامی تبدیل شده است؛ در واقع، این مقوله، زیربنای قابلیت‌های جدید نیروهای مسلح کشورها را تشکیل می‌دهد. یکی از سازمان‌های نظامی که امروزه به‌شدت مبتنی بر مقوله‌های امنیت سایبری و قابلیت‌های آن است، نیروی دریایی است. در این زمینه، توانایی‌ها و قابلیت‌های اطلاعاتی در ناوگان‌های مختلف نیروی دریایی ادغام شده و به‌طور مداوم توسط فضای سایبری بهبود می‌یابد. بنابراین، این امر باعث تقویت کنترل و فرماندهی، آگاهی از فضای جنگ، جمع‌آوری اطلاعات و هدف‌گیری دقیق می‌شود که برای موفقیت در یک عملیات ضروری است. در عصر نوین، نیروهای دریایی باید بتوانند به‌طور آزادانه انجام عملیات در فضای سایبری را برای خود حفظ کرده و از آن دفاع کنند تا بتوانند نیروهای تأثیرگذاری در عرصه دریا باشند. همان‌طور که وزیر دفاع سابق آمریکا «لیون پانتا» می‌گوید: «بدون داشتن اطلاعات و شبکه‌های ارتباطی معتبر و دسترسی مطمئن به فضا و فضای سایبری، نیروهای مسلح مدرن قادر به انجام عملیات‌های سریع و موثر نخواهند بود». (Navy Cyber Power 2020, 32)

بدین ترتیب، اهمیت فضای سایبری برای عملیات‌ها و راهبردهای جدید دریایی بر کسی پوشیده نیست، زیرا این فضا، کنترل و فرماندهی نیروهای دریایی مورد لزوم برای تمامی عملیات‌ها را پوشش می‌دهد. هدف نیروهای دریایی در آینده، حفظ آزادی عمل و سلب آزادی عمل دشمن در دریا است که بیشتر از طریق فضای سایبری انجام می‌شود. از طریق این بستر، آگاهی از فضای نبرد، جمع‌آوری

[1] Cyber Security

اطلاعات، هدف‌گیری و سایر اهداف موردنیاز که برای پیروزی در عملیات‌های دریایی ضروری است، امکان‌پذیر می‌شود.

بنابراین، قبل از هر چیز درک نقشی که فضای سایبری در محیط عملیات دریایی ایفا می‌کند، برای فهم پیامدهای فضای سایبری برای نیروی دریایی مهم است. این مقاله، ساختار یا لایه‌های فضای سایبری برای شناسایی حوزه‌های بیشتر که در آن نیروهای دریایی به فضای سایبری وابسته هستند را مورد بررسی قرار می‌دهد. سپس، پیامدهای فضای سایبری را در سطوح جنگ راهبردی، عملیاتی و تاکتیکی مورد بررسی قرار می‌دهد. در ادامه مقاله، فرصت‌های بالقوه و چالش‌های فضای سایبری به محققین و سیاست‌گذاران علاقه‌مند به امنیت و راهبرد دریایی ارائه شده است.

پیشینه‌شناسی و ادبیات تحقیق

الف) پیشینه‌شناسی

تاکنون در ارتباط با «پیامدهای فضای سایبری برای راهبرد و امنیت دریایی» به‌خصوص در متون داخلی، پژوهش معتبری منتشر نشده، اما با این حال، در زمینه تهدیدات فضای سایبری، ماهیت، ویژگی و جایگاه آن در راهبرد برخی کشورها پژوهش‌هایی منتشر شده که اهم آن به شرح ذیل است:

محمدکاظم صیاد، آرمین امینی و ابوالقاسم طاهری در مقاله‌ای با عنوان «تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران»؛ با ذکر این مقدمه که استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای تهدیدات امنیتی ازجمله خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته است، به این نتیجه رسیدند که فضای سایبر از یک‌سو فرصت‌هایی را به وجود آورده و امکان دسترسی افراد به اطلاعات را بسیار آسان کرده و از سوی دیگر تهدیدات متعددی را به وجود آورده و فضای تا حدی ناامن را در اختیار سودجویان برای آسیب زدن به زیرساخت‌های ملی به وجود آورده است. بنابراین، برخی از کشورها بر آن شده‌اند تا محیط سایبری خود را تا حد زیادی امن کرده و میزان خسارت ناشی از تهدیدات فضای سایبر را به حداقل ممکن برساند. ایالات متحده امریکا از جمله کشورهایی است که در این زمینه به موفقیت‌های رسیده است. ایجاد توانایی ضربه زدن به تأسیسات حیاتی بازیگران رقیب در فضای نبردهای سایبر از متغیرهای مهم در به تصویر کشیدن جایگاه فضای سایبر در راهبرد امنیتی آمریکاست و اقدامات صورت‌گرفته برای تحقق این هدف شامل هنجارسازی‌های بین‌المللی در زمینه سایبر و ایجاد همکاری‌های بین‌المللی با محوریت آمریکا است. در واقع، این نوع هنجارسازی‌ها به ایالات متحده این فرصت را می‌دهد تا علیه

کشورهای متخاصم خود از جمله جمهوری اسلامی ایران از همه گزینه‌های خود ازجمله گزینه نظامی استفاده کند.

دکتر «علی خلیلی‌پور» و «یاسر نورعلی‌وند» در مقاله‌ای با عنوان «تهدیدات سایبری و تاثیر آن بر امنیت ملی»، این پرسش را مطرح کرده‌اند که تهدیدات سایبری چگونه بر امنیت ملی تأثیر می‌گذارد و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد در پاسخ به این سوال به این نتیجه رسیده‌اند که تهدیدات فضای سایبر به علت برخورداری از ویژگی‌هایی به‌مانند قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام «انتشار قدرت» را به وجود آورده است که نه تنها باعث شده دولت‌های کوچیک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان‌یافته و افراد به معادلات قدرت جهانی شده است. بنابراین، این پدیده امنیت ملی را از ابعاد مفهومی امنیت، دولت‌محوری در امنیت، بُعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها و شیوه مقابله با تهدیدها و تعداد بازیگران در این عرصه تحت تأثیر قرار داده است.

«محمدعلی عسگری» در سال ۱۳۹۶ در پایان‌نامه کارشناسی ارشد خود با عنوان «بررسی جایگاه نبرد سایبری در راهبرد امنیتی آمریکا بعد از ۱۱ سپتامبر» به این نتیجه رسید که به طور کلی ایالات متحده در ارتباط با بسیاری از خدمات مهم و حیاتی به اینترنت و سامانه‌ها و داده‌های فضای مجازی متکی است. برتری نظامی آمریکا در کنار وابستگی ارکان دفاعی و اطلاعاتی این کشور به فضای سایبری موجب گشته برخی کشورها روی به ابزارهای غیرمتقارن جهت به چالش کشیدن آن ارکان بیاورند تا از این طریق میزان آسیب‌پذیری آمریکا را افزایش دهند. بنابراین، تهدیدها و حملات سایبری در راهبرد امنیت ملی آمریکا جایگاه پر اهمیتی دارد.

«علی اصغر بوژمهرانی» و «محمدرضا مهدوی حاجی» در مقاله‌ای با عنوان «واکاوی تهدیدات نوین سایبری در نیروهای مسلح»، به این نتیجه رسیده‌اند که گرچه جنگ سایبری به معنای واقعی تابه‌حال صورت نگرفته است ولی حملات روزانه سایبری حکایت از چشم‌انداز مخوف جنگ سایبری در آینده دارد. با پیشرفت روزافزون این حوزه و وابستگی نیروهای مسلح کشورها به این تکنولوژی می‌توان به این حقیقت رسید که جنگ دهه‌های آینده جنگ سایبری خواهد بود. نگارندگان این مقاله در پی پاسخ به سوال تهدیدات نوین سایبری علیه نیروهای‌مسلح و راهکارهای مقابله با آن، پیشنهاداتی همچون افزایش توانمندی نیروهای مسلح، ارتقاء مهارت سایبری، تربیت نیروهای زبده، شناخت تهدیدات نوین‌سایبری و چالش‌های آن در جنگ‌های اطلاعاتی آینده سایبری، برای مقابله با تهدیدهای امنیتی، را به عنوان مهم‌ترین راهکار برای حفظ منافع ملی و زیرساخت‌های حیاتی در فضای سایبری برشمرده‌اند.

پیشینه‌های فوق ضمن برشمردن تعاریف دقیق از تهدیدات و نبردهای سایبری و برخی مصادیق آن به تبیین ویژگی‌های تهدیدات فضای سایبری، به‌ویژه پدیده «انتشار قدرت» در جهان پرداخته‌اند که این امر امنیت ملی کشورها را از بعد مفهومی، دولت‌محوری، بُعد جغرافیایی تهدید، و گستردگی آسیب‌پذیری‌ها و شیوه مقابله تحت تأثیر قرار داده است. در این مقاله ضمن استفاده از برخی ادبیات پژوهش‌های فوق، به‌طور ویژه بر موضوع »پیامدهای فضای سایبری بر امنیت دریایی» متمرکز شده و سطوح تأثیرگذاری آن در سطح تاکتیکی، عملیاتی و راهبردی را برای نیروهای دریایی کشورها برشمرده است. از این حیث، مقاله حاضر هم به لحاظ موضوعی، هم محتوایی و نیز سطح تحلیل اثری بدیع محسوب می‌شود.

ب) مفاهیم و ادبیات تحقیق

فضای سایبری:

اصطلاح «فضای سایبر»[1] نخستین‌بار توسط «ویلیام گیبسون»[2] در سال ۱۹۸۴ مورد استفاده قرار گرفت. فضای سایبر در این تعریف، شبکه‌هایی است که از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم متصل‌اند و تمام اطلاعات راجع به افراد، فرهنگ‌ها، کشورها، و به‌طور کلی هر آنچه که در کره خاکی به‌طور فیزیکی و ملموس وجود دارند، در این فضا به شکل دیجیتالی وجود داشته و قابل استفاده و در دسترس کاربران بوده و از طریق رایانه، اجزای آن به شبکه‌های بین‌المللی مرتبط می‌باشند. فضای سایبری از سوی برخی کارشناسان نیز به عنوان «تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی و یا کاربران آن شکل می‌گیرد» تعریف شده است (Lord and Sharp, 2011: 10).

به صورت ویژه، «فضای سایبر»، حوزه جهانی از شبکه‌های به هم متصل و وابسته است که از طیف‌های الکترونیکی و الکترومغناطیسی برای تولید، ذخیره‌سازی، اصلاح، مبادله و بهره‌برداری از اطلاعات بهره می‌برد. این فضا از چهار لایه عملیاتی تشکیل شده است که برای ارایه قابلیت‌هایی که در مجموع به «فضای سایبری» معروف هستند با یکدیگر همکاری می‌کنند. «اجزای فیزیکی» فضای سایبر شامل رایانه‌ها، سرورها، دکل مخابراتی، کابل‌های فیبر نوری، ماهواره و طیف‌های الکترومغناطیس می‌شود. «لایه منطقی» فضای سایبر که وظیفه مسیریابی اطلاعات از منبع به مقصد را بر عهده دارد، برای جابجایی واقعی اطلاعات به لایه فیزیکی وابسته است. «لایه اطلاعات» جایی است که محتوا (مانند عکس، دیدئو، متن و اسناد) تولید، ذخیره، انتقال و تبدیل می‌شود. لایه نهایی فضای سایبری، لایه «کاربر» است که در آن

[1] Cyber Space
[2] -William Gibson

مردم و گروه‌ها با یکدیگر تعامل دارند و تجربه فضای سایبری را از طریق ارتباطات، برنامه‌ریزی و تصمیم‌گیری شکل می‌دهند(Choucri and Clark, 2021:87).

تهدید سایبری:

در همایشی که در ۲ مارس ۲۰۱۰ از سوی مؤسسه بین‌المللی CACI و مؤسسه مطالعاتی نیروی دریایی ایالات متحده با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، تهدیدهای سایبری[1] به صورت وقایعی که صورت طبیعی و یا توسط انسان (به صورت عمدی یا غیرعمدی) بر فضای مجازی تأثیرگذار باشد یا حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد» تعریف شد(Kuehl, 2019: 28).

ویژگی‌های تهدیدهای سایبری

تهدیدات سایبری ویژگی‌های منحصر به فردی دارند. از یک‌سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، سبب شده بازیگران زیادی به این عرصه وارد شوند(احدی، شاهمحمدی، ۱۳۹۷: ۲۲۷). بنابراین، یکی از ویژگی‌های مهم تهدیدهای سایبری، «تعدد بازیگران» در این فضا است. هزینه کم فناوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا کسب نرم‌افزارهای مخرب به این معناست که تقریباً هر کسی می‌تواند به این فضا ورود کند. این بازیگران شامل افراد، گروه های سازمان‌یافته جنایی، گروه های تروریستی، شرکت‌های خصوصی و دولت–ملت هستند(Charney,2019:6-5). از دیگر ویژگی‌های تهدیدات سایبری، «صرف زمان اندک» و سرعت بالای اقدام» است. در این زمینه، هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در نتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد. البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است. «عدم قابلیت ردیابی و ناشناس ماندن بازیگران» نیز از دیگر ویژگی‌های تهدیدات سایبری است. فضای سایبر به عنوان سامانه نامتمرکز طراحی شده و کاربران آن، غالباً شناخته شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. «تأثیرگذاری شگرف و کمرنگ شدن نقش جغرافیا» نیز از جمله ویژگی‌های مهم تهدیدات سایبری است. فضای سایبر سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است. بنابراین، تهدیدکنندگان قادر به فراتررفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان

[1] Cyber Threats

با تأثیرات شگرف هستند. «دامنه چندپارچه و مشترک» تهدیدات سایبری نیز یکی دیگر از ویژگی‌های تهدیدات در این فضا است. استفاده از این دامنه مشترک و یکپارچه این فضا توسط شرکت‌ها، دولت‌ها و سایر بازیگران به شیوه‌ای است که جداسازی آنها بسیار دشوار است. توانایی محدود برای جداکردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به تهدید را بسیار دشوارتر کرده است. از سوی دیگر ساختار پیچیده فضای سایبری، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات این فضا مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی‌ها و فناوری در حال تکامل برای پشتیبانی از سامانه‌های حیاتی است. در نهایت در فضای سایبر، «احتمال بازخواست اقدام‌های مجرمانه بازیگران» بسیار پایین است و همین امر تعقیب اقدامات مجرمانه سایر بازیگران را با چالش و دشواری مواجه می‌کند. بنابراین، سازمان‌ها و بازیگران دخیل در تهدیدات سایبری، این فضا را در مقایسه با گزینه‌های جایگزین غیرسایبری مطمئن‌تر و دارای خطرات کم‌تری می‌بینند (بوژمهرانی، ۱۳۹۲: ۱۰۴).

روش‌شناسی تحقیق

روش‌شناسی این پژوهش توصیفی-تحلیلی و از نظر هدف نیز کاربردی-توسعه‌ای است و روش گردآوری اطلاعات آن، مطالعه اسنادی-کتابخانه‌ای است. در مطالعه اسنادی، به‌طور ویژه از سایت نیروی دریایی آمریکا (سند «استراتژی سه‌گانه برتری در دریا»[1] (مصوب ۱۷ دسامبر ۲۰۲۰) و اسناد و گزارشات فرماندهی سایبری ارتش آمریکا[2] استفاده شده است. مهم‌ترین سندی که با راهبرد دریایی ارتباط دارد، «نقشه راه تسلط اطلاعاتی نیروی دریایی ایالات متحده ۲۰۱۳-۲۰۱۷»، «قدرت سایبری ۲۰۲۰»، «راهبرد دریایی برای دستیابی به تسلط اطلاعاتی ۲۰۱۳-۲۰۱۷» و «راهبرد نیروی سرمایه انسانی برای تسلط اطلاعاتی در نیروی دریایی ۲۰۱۲-۲۰۱۷» است که به‌طور ویژه در این تحقیق گزاره‌ها و دلالت‌های آن‌ها استخراج و بهره‌برداری شده است. علاوه بر این، گزارشات اسنادی برخی کشورها از جمله انگلستان، روسیه و کانادا نیز به اختصار بهره گرفته شده است. در تجزیه و تحلیل یافته‌ها از طریق مطالعه اسنادی، به‌طور ویژه بر فرصت‌ها و تهدیدهای فضای سایبری در سه سطح تحلیل (راهبردی، عملیاتی و تاکتیکی) تمرکز شده است.

بحث و یافته‌های تحقیق

۱- نقش‌آفرینی نیروهای دریایی در حوزه فضای سایبر

قابلیت‌های اصلی که نیروهای دریایی به دنبال دستیابی و ارایه آن هستند، قابلیت حضور قدرتمند

[1] The triple strategy of superiority at sea
[2] U.S. Army Cyber Command

و مداوم در آب‌های آزاد، قدرت بازدارندگی، کنترل دریایی، قدرت‌افکنی[1] و همچنین امنیت دریایی و کمک‌های بشردوستانه (با استانداردهای متفاوت) و واکنش در برابر فجایع می‌باشد(Kuehl, ۲۰۱۹: ۲۸).همه این قابلیت‌های اصلی به وسیله قابلیت‌های سایبری پشتیبانی و تقویت می‌شوند. بنابراین، طیف کاملی از عملیات‌های دریایی و راهبردهای دریایی متناظر با آن، مستلزم بهره‌مندی از قابلیت‌های سایبری است. برای نیروهای دریایی پیشرفته‌تر، این قابلیت‌های سایبری آن‌چنان در سامانه‌ها و سکوهای تسلیحاتی ادغام شده که وجود آن‌ها برای انجام هرگونه عملیات نظامی و رزمی ضروری است. برای نیروهای دریایی کم‌تر پیشرفته، قابلیت‌های سایبری از طریق تقویت فرماندهی و کنترل و افزایش‌دهنده نیرو در شرایط خاص، هنوز می‌تواند نقش مهمی در تقویت و ارتقاء توانایی‌های دیگر داشته باشد(Cyberspace Operations, February 5, 2019).

بنابراین، نیروهای دریایی، مسئول فراهم کردن قابلیت‌های عملیات فضای سایبری برای پشتیبانی از اهداف فرماندهان رزمی در دفاع از شبکه‌های اطلاعات ملی و استقرار ناوگان هستند. آن‌ها تأمین‌کنندگان عملیات‌های مشترک، پشتیبانی‌کنندگان از مأموریت‌های ملی و جنگجویان آب‌های آزاد هستند.

نیروهای دریایی یکی از چندین ابزار قدرت ملی و تنها یکی از شاخه‌های نیروهای مسلح هستند. علاوه بر وظایف دریایی خود، نیروهای دریایی مسئولیت پشتیبانی از عملیات‌های مشترک و بین سازمانی را بر عهده دارند. نقش نیروهای مسلح در امنیت ملی محدود به فعالیت در آب‌های آزاد نیست، اما در عین حال شامل راهبرد، سیاست و برنامه‌ریزی‌های حمایتی از تمامی اجزای امنیت ملی مانند فضای سایبری می‌شود. این یک مسئولیت چشمگیر برای نیروی دریایی و نیروهای دیگر است، بنابراین مباحث گسترده‌ای در مورد الگوهای نیروی جایگزین بالقوه وجود دارد. برای مثال، دریاسالار «جیمز استاواردیس» (از نیروی دریایی ایالات متحده) فرمانده عالی سابق اتحاد ناتو (۲۰۰۹-۲۰۱۳)، معتقد است که ستاد فرماندهی سایبری نباید از نیروهای مسلح سنتی به‌عنوان نیروی انسانی استفاده کند، بلکه باید یک نیروی مسلح کاملاً مجزا ایجاد کند که به جذب و آموزش نیروی متخصص امنیت سایبری بپردازد(Stavridis, 2017: 44).

[1] Power Project

۲- جایگاه فضای سایبر در راهبردهای دریایی

راهبردهای دریایی با توجه به فضای سایبر در یک دوره «گذار»[۱] قرار دارند. اکثر نیروهای دریایی اهمیت فضای سایبر به‌عنوان یک عامل توانمندساز حیاتی را می‌پذیرند، اما این یک شناخت در حال ظهور است که فضای سایبر چیزی بیش از آن است. بنابراین، فضای سایبر به‌عنوان یک عامل تحول‌آفرین و «تغییردهنده بازی»[۲] برای نیروهای دریایی و به‌طور کلی برای نیروهای امنیتی معرفی می‌شود. تمامی حالت‌ها و مراحل نبرد از مرحله برنامه‌ریزی گرفته تا مرحله تثبیت و بازسازی اکنون دارای ابعاد سایبری هستند. فضای سایبر تمامی سطوح جنگ از سطح راهبردی تا عملیاتی و تاکتیکی را در بر می‌گیرد. انواع مختلف جنگ‌ها و درگیری‌ها مانند جنگ در چهار حوزه دیگر (زمینی، دریایی، هوایی و فضایی) تحت تأثیر فضای سایبری قرار دارند(Dombrowski and Demchak, 2017: 73–6). در مورد نیروهای دریایی به طور خاص، فضای سایبر انواع جدیدی از ابزارهای جنگی را فراهم می‌کند، آگاهی موقعیتی را افزایش می‌دهد و فرماندهی و کنترل را تقویت می‌کند. فضای سایبر همچنین درها را به روی تهدیدهای جدیدی گشوده است: عملیات‌های ضد دسترسی/ منع منطقه‌ای[۳] بهبود توانایی‌های هدف‌گیری توسط دشمن و ارایه اهداف بیشتر برای حملات متعارف و حملات سایبری.

«سیاست‌های ملی» فضای سایبر، اهداف و مقاصد عملیاتی جدیدی در اختیار فرماندهان نیروی دریایی قرار می‌دهد و آن‌ها را با اهداف امنیت ملی مهم مرتبط می‌کند. «راهبردهای ملی»، دستورالعمل‌هایی را برای استفاده از انواع مختلفی از توانایی‌ها و قابلیت‌ها توسط نیروهای مسلح فراهم می‌کند و این دستورالعمل‌ها را به چارچوب قوانین ملی موجود برای عملیات‌ها و نبردهای تدافعی مرتبط می‌کند.

۳- راهبرد نیروی دریایی ایالات متحده برای فضای سایبر

وزارت دفاع ایالات متحده آمریکا و نیروی دریایی این کشور اسناد متعددی را در سال‌های اخیر

۱- Transitional

۲- game-changer

۳- «عملیات ضد دسترسی و منع منطقه‌ای» یک راهبرد نظامی با این ایده مرکزی است که بهترین راه برای غلبه بر یک دشمن دور، به‌ویژه اگر در قدرت نظامی کلی، برتر باشد، ممانعت از دسترسی و استقرار نیروهای آن به صحنه درگیری در منطقه خودی است.» به عبارت دیگر، این استراتژی برای جلوگیری از ورود یا اشغال یک صحنه عملیات طراحی می‌شود که به‌طور مؤثر توسط ارتش‌ها هنگام رویارویی با یک دشمن قوی‌تر مورد استفاده قرار می‌گیرد. از این استراتژی امروزه برای توصیف وضعیت »جنگ گرم» کنونی در دریای چین جنوبی بین آمریکا و چین استفاده می‌شود. عملیات‌های فضای سایبر نقش مهمی در استراتژی ضد دسترسی و منع منطقه‌ای دارد (نجفی سیار، ۱۴۰۱: ۱۲)

منتشر کرده‌اند که در مورد مواجهه با فضای سایبر، راهبرد سایبری و عملیات‌های سایبری منتشر شده‌اند. مهم‌ترین سند که با راهبرد دریایی ارتباط دارد، «نقشه راه تسلط اطلاعاتی نیروی دریایی ایالات متحده ۲۰۱۳-۲۰۱۷»[۱] «قدرت سایبری ۲۰۲۰»[۲]، «راهبرد دریایی برای دستیابی به اشراف اطلاعاتی ۲۰۱۳-۲۰۱۷»[۳] «راهبرد نیروی سرمایه انسانی برای اشراف اطلاعاتی در نیروی دریایی ۲۰۱۲-۲۰۱۷»[۴] و «راهبرد مشارکتی برای قدرت دریایی قرن بیست و یکم»[۵]. این اسناد راهبردی بر مبنای یک موضوع اصلی منتشر شده‌اند: فضای سایبر ۳ فرصت مهم و اساسی برای دستیابی به «اشراف اطلاعاتی» در اختیار ما قرار خواهد داد.

۱) تضمین دسترسی به فضای سایبر و فرماندهی و کنترل[۶](C2) مطمئن برای نیروهای مستقر، بدون توجه به محیط تهدید؛ ۲) آگاهی از فضای منطقه رزم برای درک بهتر محیط عملیاتی دریایی و اجتناب از غافلگیری راهبردی و ۳) تأثیرگذاری قاطعانه در فضای سایبر و آتش یکپارچه متحرک و غیرمتحرک برای توسعه و گسترش گزینه‌های رزمی برای فرماندهان نیروی دریایی و مشترک (U.S Navy Information Dominance Roadmap 2013–2028).

اولین فرصت که همان «تضمین فرماندهی و کنترل» است (C2)، به این معنی می‌باشد که نیروهای دریایی توانایی حفظ دسترسی به فضای سایبر برای تمامی کارکردهای ضروری و مورد نیاز مأموریت‌ها را دارد. همچنین هدف دیگر تأمین فرماندهی و کنترل انعطاف‌پذیر برای فرماندهان است. هدف دیگر فضای سایبر، حفظ توانایی اجرای فرماندهی و کنترل در یک محیط عملیاتی مورد مناقشه است، به ویژه هنگامی که دشمن محاصره اطلاعاتی یا سایبری انجام داده است. تضمین فرماندهی و کنترل برای فرماندهان بسیار اهمیت دارد، زیرا آن‌ها از این طریق می‌توانند اقدامات و مأموریت‌های موردنیاز در دریا، زمین، هوا و فضا و حتی فضای سایبر را برای پشتیبانی از طیف وسیعی از عملیات‌های نظامی هماهنگ‌سازی کنند. فرماندهی و کنترل تضمین شده نیازمند توانایی کنترل و فرماندهی نیروها در هر محیطی از جمله محیط‌های آسان، پیچیده یا بسیار پیچیده بدون توجه به تهدید موجود می‌باشد. علاوه بر نیروهای تحت فرمان، فضای سایبر همچنین باید

۱- U. S. Navy Information Dominance Roadmap 2013—2017

۲ Navy Cyber Power 2020

۳ Navy Strategy for Achieving Information Dominance 2013—2017

۴ Navy Information Dominance Corps Human Capital Strategy 2012—2017

۵ A Cooperative Strategy for 21st Century Seapower

۶ command and control

بتواند توانایی آتش نیروهای دوست در تمامی حوزه‌ها را هماهنگ کند، تا از این طریق به اثرات مطلوب دست یابند. در نهایت، نیروهای دریایی به فرماندهی و کنترل تضمین شده نیاز دارند تا از این طریق بتوانند در مورد مأموریت‌ها و وضعیت نیروهای دوست به ویژه هنگام انجام عملیات‌های نظامی، ارزیابی‌های دقیقی انجدم دهند (Navy Cyber Power 2020 : 1).

فرصت دوم، یعنی «آگاهی از فضای منطقه رزم توانایی نیروی دریایی در درک ویژگی‌ها و شرایط محیط عملیاتی» است. آنچه که برای دستیابی به این هدف لازم و ضروری است برخورداری از دانش در مورد مکان، فعالیت‌ها، اهداف و قابلیت‌های بالقوه دشمن؛ برخورداری از دانش کافی در مورد قابلیت‌ها، ظرفیت‌ها و وضعیت نیروی دریایی خودی؛ و برخورداری از دانش کافی در مورد محیط‌های واقعی و مجازی و تأثیر بالقوه آن‌ها بر اجرای مأموریت‌ها می‌باشد. این اجزای اطلاعاتی ابدی هستند- «سون تزو» این موضوع را ۲۵۰۰ سال پیش اشاره کرده و گفته است: «همه جنگ‌ها مبتنی بر فریب هستند»- اما قابلیت‌های فضای سایبر دیدگاه پیچیده‌تر، دقیق‌تر و یکپارچه‌تر از فضای جنگی مدرن را ترسیم کرده است که می‌تواند احتمال غافلگیری‌های ناخواسته را کاهش دهد. اجتناب از غافلگیری‌های راهبردی به معنای استفاده از مجموعه‌ها و تحلیل‌های اختصاصی اطلاعات سایبری و ادغام کامل و دقیق اطلاعات سایبری و هشدار تهدید در تصویر عملیاتی فرماندهان است(U.S Navy Information Dominance Roadmap 2013–۲۰۲۸: ۱۵).

فرصت سوم که «تأثیرگذاری سایبری هدفمند و دستیابی به آتش یکپارچه» است، نقطه اوج دو هدف قبلی است و امکان ارائه دقیق و به‌موقع اطلاعات به فرماندهان، یگان‌های مستقر و سامانه‌های تسلیحاتی را فراهم می‌کند. تأثیرگذاری سایبری هدفمند به معنای استفاده به‌موقع از قابلیت‌های سایبری در زمان و مکانی است که فرمانده در طیف کاملی از عملیات‌های نظامی انتخاب و معرفی می‌کند (Navy Cyber Power 2020: 1). از «طیف الکترومغناطیس» می‌توان برای ایجاد آتش متحرک متعارف و همچنین آتش غیرمتحرک مانند عملیات‌های سایبری تهاجمی، ایجاد پارازیت و تسلیحات انرژی هدایت شده استفاده کرد. از «آتش یکپارچه» می‌توان برای تقویت آتش نیروهای دریایی خودی یا دوست و همچنین ایجاد اختلال، مقابله و جلوگیری از نفوذ آتش نیروهای دشمن استفاده کرد. این نیروها قابلیت آن را دارند که در حوزه‌های مختلف با یکدیگر ترکیب شوند تا بتوانند بر دشمن غلبه کنند و به اهداف مطلوب دست یابند. یکی از نمونه‌های آتش یکپارچه و هماهنگ، حمله به گرجستان در جریان جنگ روسیه و گرجستان در سال ۲۰۰۸ است، که در طول آن نیروهای روسیه از طریق زمین، هوا و دریا به گرجستان حمله کردند،

درحالی که هم‌زمان وبسایت‌های سازمان‌های دولتی، خدمات مالی و سرویس‌های خبری گرجستان در معرض حملات محروم‌سازی سرورها از خدمات‌رسانی(DDoS)[1]قرار گرفتند. (Russell, 2018: ۹۸)

۴- راهبردهای دریایی بین‌المللی در فضای سایبری

کشورهای دیگر برای تقویت برخی از موضوعات، راهبردهایی برای فضای سایبری تدوین کرده‌اند. انگلستان، استرالیا، و روسیه همگی راهبردهای دریایی خاصی را تدوین کرده‌اند که به طریقی با فضای سایبر در ارتباط است. در ادامه برخی از این راهبردها به طور مختصر توضیح داده شده است.

راهبرد ملی انگلستان برای امنیت دریایی، حملات سایبری به زیرساخت‌ها و یا کشتی‌رانی دریایی انگلستان را به‌عنوان یکی از «مهم‌ترین خطرات» شناسایی می‌کند که «به احتمال بسیار زیاد آسیب‌ها و اختلال‌های قابل توجهی را برای انگلستان» ایجاد می‌کند. بر اساس این راهبرد، بیش از ۹۵ درصد از داده‌ها و اطلاعات بین قاره‌ای از مسیر کابل‌های زیرآبی منتقل می‌شود، بنابراین حفاظت از این جریان ضروری اطلاعات در برابر حملات سایبری یا فیزیکی بسیار اهمیت دارد؛ اطلاعاتی که اقتصاد جهانی به آن وابسته است. همچنین باید اطمینان حاصل کرد که کشورهای ساحلی بر اساس قوانین کنوانسیون حقوق دریاها اجازه استفاده آزادانه از دریا به عنوان بستری برای تبادل اطلاعات را می‌دهند(The UK National Strategy for Maritime Security, May 2019).

راهبرد دفاعی دریایی استرالیا بر قابلیت‌های سایبری به‌عنوان عملیات‌های توانمندساز و قابلیت مشترک تمرکز دارد. در نبردهای آینده و یا تشدید درگیری‌های آتی، یک دشمن می‌تواند از یک حمله سایبری علیه استرالیا برای بازدارندگی، تأخیر و یا جلوگیری از واکنش استرالیا و یا استقرار نیروها (نیروهای دفاعی استرالیا)[2]استفاده کند. این موضوع احتمالاً شامل هدف قرار دادن سامانه‌های اطلاعاتی، شبکه‌ها و زیرساخت‌های پشتیبانی گسترده می‌شود که به نظر می‌رسد برای تصمیم‌گیری و قابلیت‌های رزمی نیروهای دفاعی استرالیا ضروری است. پس از استقرار نیروها،

---

[1]- حمله (DDOS) روشی از حمله است که در آن حمله‌کننده با تعداد زیادی از کامپیوترها و شبکه‌هایی که در اختیار دارد، حمله را صورت می دهد. در این روش تمام کامپیوترها یکی از روش‌های حمله را که در ذیل ذکر شده اند را همزمان با هم انجام می‌دهند که ممکن است در برخی موارد خسارات جبران‌ناپذیری را به بار آورد. در این روش معمولا حمله کننده سیستم‌های زیادی را آلوده کرده و به آنها همرمان فرمان می‌دهد، به سیستم‌های آلوده‌شده zombie و به شبکه‌ای از این سیستم‌ها که تحت کنترل یک شخص هستند، botnet می‌گویند.

[2]- Australian Defense Force

آنها باید به‌عنوان شبکه‌ای از نیروها در یک محیط رقابتی عمل کنند (Department of Defense (Government of Australia, 2018: 20).

استرالیا یک مرکز عملیات امنیت سایبری[1]را در اداره سیگنال‌های استرالیا[2]برای شناسایی تهدیدهای سایبری و واکنش به رخدادهای فضای سایبر تأسیس کرده است. مدیریت شبکه و سامانه همراه با امنیت کارکنان و فیزیکی بخشی از راهبرد سایبری استرالیا است. در ژانویه ۲۰۱۳، دولت استرالیا یک شبکه امنیت سایبری جدید برای تقویت روابط بین سازمان‌های دولتی و صنایع خصوصی ایجاد کرد که هم‌اکنون به‌عنوان بستر مقابله با تهدیدات سایبری این کشور محسوب می‌شود (Ibid: 75–6).

روسیه نیز همانند سایر قدرت‌های بزرگ قابلیت‌های فضای سایبری پیشرفته‌ای برای خود ایجاد کرده است. راهبرد دریایی روسیه به طور مستقیم به فضای سایبری و امنیت سایبری به‌عنوان یک مسئولیت دریایی و یا نیروی دریایی نمی‌پردازد، بلکه اهمیت «پشتیبانی اطلاعاتی فعالیت‌های دریایی» را برای حفظ و توسعه سامانه‌های اطلاعاتی جهانی به رسمیت می‌شناسد که شامل سامانه‌های ناوبری، آب‌شناسی و انواع دیگر امنیت می‌شود(Maritime Doctrine of the Russian Federation, 2020)

بنابراین، فضای سایبر برای نیروهای دریایی کشورها از جمله آمریکا، روسیه، انگلستان و...) به‌عنوان یک عامل تحول‌آفرین و تغییردهنده بازی محسوب می‌شود که در تمامی سطوح جنگ از سطح راهبردی تا عملیاتی و تاکتیکی در حوزه‌های مختلف دیگر نقش‌آفرین می‌باشد.

۵- فرصت‌ها و چالش‌های امنیت و راهبرد دریایی در فضای سایبری

فضای سایبری مجموعه‌ای از چالش‌ها و فرصت‌ها را برای نیروهای دریایی، سیاست‌گذاران و استراتژیست‌های نظامی فراهم نموده است.

الف) فرصت‌ها

فضای سایبری فرصت‌های زیادی را برای راهبرد و امنیت دریایی ارایه می‌دهد. درحالی که آن‌ها را می‌توان به صورت مختصر در اینجا توضیح داد، اما نباید اهمیت بالای آن‌ها را نادیده گرفت. اولاً،

---

[1] Cyber Security Operations Center

[2]- اداره سیگنال‌های استرالیا (Defense Signals Directorate) یک سازمان اطلاعاتی گردآوری اطلاعات خارجی برای دولت استرالیا است. وظیفه این اداره، شنود الکترونیک و امنیت اطلاعات است. اداره سیگنال‌های استرالیا بخشی از جامعه اطلاعاتی استرالیا است. نقش اداره سیگنال‌های استرالیا در توافق یوکی‌یواس‌ای (فایو آیز) شنود الکترونیک در منطقه آسیای جنوبی و آسیای شرقی است. این اداره همچنین میزبان مرکز امنیت سایبری استرالیا است.

قابلیت‌های پیشرفته‌ای که از فضای سایبری به دست می‌آید منجر به تقویت و بهبود فرماندهی و کنترل و در نتیجه افزایش اثربخشی کلی نیروهای دریایی می‌شود. ثانیاً، افزایش آگاهی از فضای نبرد به نیروهای دریایی این امکان را می‌دهد تا درک بهتری از محیطی که در آن عملیات می‌کنند داشته باشند. ثالثاً، حملات سایبری و یکپارچه فرصت‌های جدیدی را برای اقدامات تهاجمی علیه دشمنان فراهم می‌کنند. رابعاً، فضای سایبری فرصت‌های جدیدی برای مدل‌سازی و شبیه‌سازی کمک به نیروهای دریایی برای آماده‌سازی و آموزش نیروها برای جنگ ارایه می‌دهد. خامساً، فضای سایبر به‌عنوان یک حوزه جدید فرصت‌هایی برای همکاری با کشورهای دوست به منظور توسعه، نگهداری و محافظت از این حوزه برای اطمینان از دسترسی ایمن و مطمئن شرکا و متحدان و در عین حال محدود کردن قدرت مانور دشمن در این حوزه ارایه می‌کند.

ب) چالش‌ها

فضای سایبر چالش‌های بسیاری ایجاد می‌کند. اولاً، عملیات‌های «ضد دسترسی و منع منطقه‌ای» مهم‌ترین چالش برای اهداف اصلی نیروهای دریایی و بازداشتن آزادی عمل دشمنان است. برای استفاده از هر قابلیتی در فضای سایبری، در ابتدا باید به این حوزه دسترسی داشت. یکی از اهداف اولیه نیروهای دریایی در فضای سایبر حفظ دسترسی مطمئن و آزادی عملیاتی است. اگر دشمن بتواند از طریق ایجاد یک محاصره سایبری و ابزارهای دیگر فضای سایبری را کنترل کند، در این صورت نیروهای دریایی با چالش‌های جدی در سراسر عملیات و نه صرفاً عملیات‌های سایبری مواجه خواهند شد(Russell, 2018: 103).

دوم، یک چالش مهم برای نیروهای دریایی و یا هر نیروی دیگری که در فضای سایبری فعالیت می‌کند این است که حمله یک مزیت محسوب می‌شود. تهدیدها در فضای سایبری سریع‌تر از آنکه نیروها بتوانند خود را در برابر آن‌ها محافظت کنند، گسترش می‌یابند. این حوزه پیوسته در حال تکامل است و نوآوری سامانه‌ها ابزارهای جدیدی را با سرعت بالایی تولید می‌کند. با خلق برنامه‌های کاربردی جدید، آسیب‌پذیری‌های جدید در درون سامانه‌ها پدید می‌آید. دشمنان به طور پیوسته در پی یافتن روش‌های جدید حمله و نفوذ هستند، درحالی که عملیات‌های سایبری تدافعی به دنبال مقابله با هجوم حملات سایبری دشمن هستند. تهدیدهای پیشرفته و مستمر(APTs)[1]

[1]- در حوزه امنیت اطلاعات، منظور از APTs مجموعه‌ای از حملات است که در یک الگوی دراز مدت حملات نفوذی پیچیده علیه دولت‌ها، شرکت‌ها و فعالان سیاسی استفاده می‌شود. این اصطلاح به گروهی که پشت این حملات است نیز اشاره می‌کند. تصور غلط رایج درباره APT این است که این نوع‌ها به‌طور ویژه دولت‌ها را هدف قرار داده‌است. فناوری APT توسط حمله کنندگان در بسیاری از کشورها به عنوان وسیله‌ای برای جمع‌آوری اطلاعات از فرد، گروه و افراد مشخص استفاده می‌شود. گفته می‌شود که برخی از گروه‌های درگیر در APT توسط منابع متعدد دولتی

حملات مستمر و پنهان به سامانه‌های رایانه‌ای هدف به منظور نظارت مداوم و استخراج داده- به طور خاص مسئله‌ساز هستند، زیرا شناسایی آنها بسیار مشکل است و می‌توانند آسیب‌های قابل توجهی وارد کنند. علاوه بر آن، سرعت انجام برخی حملات سایبری، موانع نسبتاً کمی که برای ورود به فضای سایبری وجود دارد، و تأثیر بالقوه یک حمله سایبری انگیزه زیادی را برای مهاجمان سایبری در حمله فراهم می‌کند. همگام کردن عملیات‌های تدافعی با اقدامات مهاجمان دشوار است و مقابله در برابر حملات آینده نیاز به نوآوری در این حوزه دارد(رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۲).

سوم اینکه، درحالی که نیروهای دریایی سال‌های طولانی است که از سامانه‌های سایبری استفاده می‌کنند، تعداد این سامانه‌ها و میزان وابستگی آن‌ها به فضای سایبری در حال گسترش است و این خود یک چالش است، زیرا هرچه تعداد سامانه‌های بیشتری به این فضا متصل باشند، میزان آسیب‌پذیری آن‌ها در فضای سایبری بیشتر خواهد بود. این سامانه‌ها معمولاً دارای قابلیت‌های مقاومت و تاب‌آوری درون سامانه‌ای هستند، اما این موضوع لزوماً به معنای ایمنی در برابر خطرات نیست و ممکن است این قابلیت‌ها اثربخشی مورد نظر را نداشته باشند. علاوه بر آن، آسیب‌پذیری‌های شناخته‌شده در درون سامانه‌ها را به آسانی نمی‌توان برطرف نمود. بروزرسانی‌ها و تبدیل‌ها باید به صورت مداوم و مستمر در برنامه‌های چرخه حیات سامانه‌ها ادغام شود و هنگام بروز آسیب‌پذیری‌ها از بروز رسانی مناسب استفاده شود.

چهارم، دفاع از شبکه‌های ملی در فضای سایبر و حفاظت از زیرساخت‌های حیاتی ملی همواره نیازمند منابع است. زمان، پول، مهارت و نیروی انسانی باید از حوزه‌های دیگر منحرف شود و به عملیات‌های فضای مجازی اختصاص داده شود(رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۲). درحالی که این موضوع در سطح ملی صحیح است، نیروهای دریایی از تقسیم بار هزینه‌های مربوط به دفاع از شبکه‌های خود و شبکه‌های ملی مستثنی نیستند. همانند زیرساخت‌های حیاتی سایبری، در بسیاری از موارد نیروهای دریایی خود را در یک جایگاه ممتاز برای حفاظت از زیرساخت‌های موجود در حوزه دریایی می‌یابند و مانع از دستیابی و دستکاری دشمن به فضای سایبری برای انجام عملیات‌های خرابکارانه می‌شوند. برای مثال، یک زیردریایی خارجی که به طور مخفیانه در سواحل یکی از کشورهای شمال شرقی اروپا گشت می‌زند، می‌تواند کابل‌های فیبر نوری که از بستر دریا عبور کرده است را دستکاری کرده و یا به آن‌ها آسیب بزند و یا اطلاعات مورد نیاز برای

به‌طور مستقیم یا غیرمستقیم حمایت می‌شوند.(Russell, 2018: 103)

تهدید آن کشور و یا کشورهای همسایه را به دست آورد.

پنجم، از آنجایی که فضای سایبر یک محیط تا حدی مصنوعی است، مکان‌نگاری آن دستخوش تغییر است و در نتیجه قابلیت‌ها و توانمندی‌های دشمنان نیز دائماً در حال تکامل است. این امر حفظ آگاهی وضعیتی بهینه در تمامی زمان‌ها را مشکل می‌کند، زیرا این حوزه دائماً در حال تکامل و تغییر است و تهدیدهای جدید می‌تواند انواع و شکل‌های مختلف به خود بگیرد. بنابراین، یک چالش بزرگ جلوگیری از غافلگیری راهبردی در فضای سایبری است. (Dombrowski and Demchak, 2017: 84–86)

ششم، نیروهای دریایی نیز در ارتباط با اصل نزدیکی و مجاورت با نیروهای دشمن، با چالش‌های بزرگی مواجه هستند. برای انجام حمله به دشمن، دیگر نیاز نیست که دشمنان در فاصله نسبتاً نزدیک با آن‌ها قرار داشته باشند. آن‌ها می‌توانند در آن سوی دنیا هم که باشند، حملات سایبری خود را علیه شبکه‌ها و سامانه‌های موجود در دریا و یا خشکی به دشمن انجام دهند. هدف‌گیری پیشرفته و آگاهی وضعیتی بهبود یافته این کار را امکان‌پذیر می‌کند. این موضوع باعث می‌شود تا نیروهای دریایی نسبت به توانایی خود در انجام عملیات‌های تأثیرگذار با نااطمینانی مواجه شوند. حتی اگر آن‌ها در محیط‌های منطقه‌ای خود با تهدید مواجهه نشوند، عملیات‌ها ممکن است نه‌تنها در آن سوی افق بلکه در سراسر جهان توسط نیروها به خطر افتد(Russell, 2018: 103).

هفتم اینکه، چالش مهم دیگر برای نیروهای دریایی ارتباط دادن است. ارتباط دادن در فضای سایبری می‌تواند بسیار دشوار باشد و در برخی موارد شناخت ارتباط بین یک بازیگر فضای سایبر با عامل حقیقی بسیار دشوار است. حتی در صورتی که بتوان این کار را انجام داد، در بسیاری از موارد زمان زیادی لازم است تا به طور دقیق مشخص کرد که یک حمله خاص از کجا نشأت گرفته است (کدام کشور یا منطقه)، چه کسی حمله را انجام داده است (هکر غیرنظامی، سازمان جنایی، کنشگر غیردولتی، سازمان نظامی یا دولتی درگیر)، و این حمله با مجوز چه کسی انجام شده است (فردی که با انگیزه شخصی این کار را انجام داده است یا مأمور دولتی بوده است). بدون داشتن این حقایق اولیه، نیروهای دریایی برای تعیین واکنش مناسب و اعمال قوانین و مقررات صحیح برای مداخله و استفاده از اصول مناسب دریایی کار سختی خواهند داشت.

هشتم، نیروهای دریایی در ارتباط با دقت سلاح‌های سایبری با چالش‌هایی مواجهه هستند. سلاح‌های سایبری می‌توانند از هر سلاح دیگری دقیق‌تر باشند، زیرا آن‌ها را می‌توان صرفاً در درون شبکه‌های خاص و بر روی برخی رایانه‌های خاص و تحت شرایط مشخص اجرا کرد. این

یک چالش جدید برای نیروی دریایی به حساب می‌آید، زیرا «دقت هدف‌گیری دیگر تنها شامل خط دید، آب‌های آزاد و یا قابلیت‌های نظامی روی خط افق»[1] نمی‌شود. مهاجمانی که دارای قابلیت‌های سایبری هستند می‌توانند دقت هدف‌گیری خود را از یک فرد خاص به یک شهر، منطقه و یا کل ملت را تغییر دهند(Dombrowski and Demchak, 2017: 83).

به لحاظ تاریخی، دقت در جنگ بسیار گران بوده است و بنابراین در دسترس تمامی کشورها نیست، چه برسد به گروه‌های غیر دولتی و یا افراد خاص. میزان دقت در سلاح‌ها مولفه سودمندی است، زیرا اثرگذاری سلاح را افزایش می‌دهد درحالی که به لحاظ نظری هزینه را کاهش می‌دهد. سلاح‌های دقیق‌تر به این معنا است که برای رسیدن به اثرات مطلوب نیاز به استقرار سامانه‌های تسلیحاتی کم‌تری است که این امر باعث کاهش هزینه‌های کلی عملیات می‌شود (نیروی انسانی، قدرت‌افکنی و غیره). تسلیحات دقیق همچنین به معنای کاهش احتمال صدمات جانبی غیرعمدی به غیرنظامیان می‌باشد، در نتیجه خطر عبور از خطوط قرمزی که منجر به تشدید درگیری‌ها می‌شود، را کاهش می‌دهد.

نهم، مقیاس حملات سایبری و تسلیحات سایبری برخلاف سلاح‌های متعارف و حملات در حوزه‌های دیگر است. به دلیل اینکه موانع ورود به فضای سایبری کم است، مهاجران سایبری می‌توانند حجم گسترده‌ای از آسیب‌ها را تنها با سرمایه‌گذاری‌های محدودی وارد کنند. همه حملات سایبری کم‌هزینه نیستند، حملات سایبری پیشرفته و رده بالایی وجود دارد که توسعه، آزمایش و اجرای آن‌ها بسیار پرهزینه است، اما بسیای از گزینه‌های دیگری در دسترس دولت‌ها، بازیگران غیردولتی و اشخاص وجود دارد که تحقیق و توسعه آن‌ها به سرمایه‌گذاری‌های گسترده و یا منابع قابل توجهی نیاز ندارد. حتی برای اجرای برخی از حملات سایبری، به مهارت‌های هک پیشرفته‌ای نیاز ندارد. برخی از سازمان‌های جنایی دارای مدل‌های تجاری هستند که نیازمند به‌کارگیری حملات سایبری است. از شبکه‌های رباتی می‌توان برای حمله به برخی اهداف خاص در یک دوره زمانی مشخص استفاده و سپس آن را خاموش کرد. به همین دلیل، سازمان‌های کوچک مانند گروه‌های تروریستی، بنگاه‌های جنایی و افراد خاص می‌توانند اثرات نامطلوبی در فضای سایبری ایجاد کنند. این مزیت‌های نامتقارن که در فضای سایبری وجود دارد، بازیگران کوچک‌تر را به شیوه‌ای بی‌سابقه قدرتمند می‌سازد. پیامدهای این امر برای نیروهای دریایی این است که آنها

[1] "precision in targeting is no longer constrained to line-of-sight, blue water, or over-the-horizon military capabilities"

باید طیف گسترده‌تری از تهدیدات را در مورد توجه قرار دهند. دشمنان دیگر نیازی به ساخت کشتی و رفتن به دریا ندارند، حتی موشک‌ها نیز دیگر ضروری نیستند، بلکه حملات سایبری می‌تواند به گروه‌های مختلفی که دارای ابزارها، مهارت‌ها و منابع سایبری مناسب هستند امکان دهد تا نیروهای دریایی را به طور مستقیم تهدید کنند.

دهم اینکه مرزهای ملی در فضای سایبر نیز وجود دارد، اما ماهیت جهانی فضای سایبری و انتقال تقریباً آنی و در لحظه اطلاعات می‌تواند آن را پشت سر نهاده و یا ارتباط آنها با این حوزه را کاهش دهد. مالکیت اطلاعاتی که در کسری از ثانیه در فضای سایبری جابجا می‌شود، چالش بزرگی برای مسئولین حاکم است. آیا دولتی که اطلاعات را دریافت کرده است مالک آن به حساب می‌آید یا دولتی که اطلاعات را ارسال کرده است مالک اصلی آن است؟ مسئولیت اطلاعات جابجا شده برای کشورهایی که در فرایند ارسال و دریافت اطلاعات دخیل هستند چیست؟ مرزهای سامانه دولتی مدرن با توجه به صلاحیت قانونی برای اطلاعاتی که با سرعت آنی در فضای سایبر منتقل می‌شود، مفید نیست.

یازدهمین چالش این است که مسائل مربوط به صلاحیت و کنترل در فضای سایبر نامشخص است که این موضوع برای نیروهای دریایی و همچنین سایر سازمان‌های امنیت ملی و مجری قانون مسئله‌ساز است. همچنین مشخص نیست که کدام اتفاق در فضای سایبر اقدام مجرمانه و کدام رویداد به طور بالقوه اقدام جنگی به حساب می‌آید. درحالی که نگرانی فزاینده‌ای از سوی برخی در مورد نظامی شدن فضای سایبری و هیاهوی جنگ سایبری وجود دارد، همچنین نیاز است تا حدود بین مسئولیت‌های اجرای قانون و دفاع ملی به طور دقیق مشخص شود. در برخی شرایط این تفاوت‌ها بر اساس مقیاس و ماهیت حمله مشخص خواهد بود، اما در بسیاری از موارد دیگر مسئولیت قانونی و قوانین مربوط به مداخله در جنگ باید به طور شفاف مشخص شود. (Susan, ۲۰۱۸: ۵۵)

دوازدهمین چالش این است که فضای سایبری چالش‌های زیادی را در ارتباط با همکاری بین بخش دولتی و خصوصی ارائه می‌دهد. برای مثال، نیروهای دریایی مجموعه‌ای از مأموریت‌ها و اختیارات قانونی متفاوتی (به طور کلی و با توجه به فضای سایبری) دارند که می‌تواند همکاری بین طرفین درگیر را دشوار کند. علاوه بر آن، همه شاخه‌های نیروی دریایی امنیت سایبری را اولویت بالایی نمی‌دانند که این موضوع هماهنگی و همکاری بین بخش خصوصی و دولتی را بیش از پیش دشوار می‌کند(Navy Cyber Power 2020: 7).

عملیات‌های فضای سایبری نیازمند همکاری بخش خصوصی نیز هست. از آنجایی که فضای

سایبری یک حوزه جنگی است، اما در عین حال تأمین امنیت آن منافع زیادی برای بخش خصوصی دارد. برای مثال، بخش گسترده‌ای از زیرساخت‌های فیزیکی فضای سایبری تحت مالکیت و اختیار شرکت‌های خصوصی است. نوآوری همچنین از بخش خصوصی نشأت می‌گیرد که این موضوع فرصت‌های جدیدی را برای نیروهای دریایی فراهم می‌کند تا از مزایای فناوری‌های نوین بهره‌مند شوند، اما در عین حال چالش‌هایی را ایجاد می‌کند، زیرا نیروهای دریایی نسبت به نوآوری واکنش نشان می‌دهند و آنها را هدایت نمی‌کنند. بنابراین، امنیت دریایی برای حفاظت از شبکه‌های موجود و ایجاد محصولات و فناوری‌های نوین به همکاری بخش خصوصی وابسته است.

چالش آخر این است که نیروهای دریایی با چالش‌هایی در لایه کاربری فضای مجازی مواجه هستند. اگر مسائلی مانند خرابکاری و یا جاسوسی عمدی را کنار بگذاریم، اکثر آسیب‌پذیری‌ها در لایه کاربری را می‌توان با هشیاری و اقدامات امنیتی دقیق تا حد زیادی کاهش داد. آموزش و تمرین برای تقویت عادات خوب بهداشت فضای سایبری راه درازی پیش روی خواهد داشت، اما اشتباهات و خطاهای گاه و بیگاه در قضاوت در هر سازمان بزرگی اجتناب‌ناپذیر است. این چالشی است که تمامی نیروهای دریایی با آن مواجه هستند؛ مهم نیست که سامانه‌ها و فناوری‌ها چقدر خوب هستند، اما هنوز هم ممکن است با خطای انسانی از کار بیفتند.

۶- پیامدهای فضای سایبری برای امنیت دریایی

الف) سطح عملیاتی

فضای سایبری پیامدهای روشنی برای امنیت دریایی در سطح عملیاتی جنگ دارد. فرمانده ناوگان سایبری/ فرماندهی ناوگان دهم نیروی دریایی ایالات متحده اظهار می‌دارد: «دفاع از شبکه‌ها و اطلاعات نیروی دریایی و وزارت دفاع ایالات متحده ضروری است و آن را نمی‌توان از سطح عملیاتی دریایی کلی جنگ جدا دانست»(Tighe, 3 May 2021).

فضای سایبر یکی از بخش‌های حساس، مهم و اصلی عملیات‌های دریایی طی دو دهه گذشته بوده است. تمامی بخش‌های عملیات دریایی و نیروی دریایی به قابلیت‌های سایبری وابسته است. فضای سایبر کنترل و فرماندهی و کنترل مطمئن، آتش یکپارچه، آگاهی از فضای نبرد، اطلاعات، حفاظت و پایداری را امکان‌پذیر می‌کند. فضای سایبر همچنین مانورهای دریایی را با پشتیبانی از موقعیت‌یابی، ناوبری و زمان‌بندی امکان‌پذیر می‌سازد. برای قدرت‌افکنی دریایی، در منظره‌ای که اغلب فاقد نشانه‌های راهنما و تابلوی اعلانات است، توانایی دستیابی به اطلاعات ناوبری دقیق و

آگاهی موقعیتی فراتر از خط دید اهمیت ویژه‌ای دارد. سامانه‌های موقعیت‌یاب جهانی سایبری و ماهواره‌ای و سامانه‌های ناوبری این توانایی و قابلیت‌ها را فراهم می‌کنند.

عملیات‌های فضای مجازی را می‌توان به سه طریق طبقه‌بندی کرد: اقدامات تهاجمی، اقدامات تدافعی و عملیات‌های شبکه‌ای.[1] عملیات‌های تهاجمی فضای سایبر برای قدرت‌افکنی از طریق بکارگیری نیرو در فضای سایبری طراحی شده است. عملیات‌های تدافعی فضای سایبر برای دفاع از سامانه‌ها یا زیرساخت‌های فضای سایبر ملی و یا کشورهای دوست به کار گرفته می‌شود. عملیات‌های شبکه‌ای برای طراحی، ساخت، پیکربندی، ایمن‌سازی و حفاظت از شبکه‌های اطلاعاتی و سامانه‌های ارتباطی و همچنین برای تضمین در دسترس بودن داده، یکپارچگی سامانه‌ها و محرمانه بودن آن‌ها به وجود آمده‌اند(Cyberspace Operations, 2019 : vii).

نهادهای تجاری و دانشگاهی که در قالب طراحی، ساخت، تحقیق و سایر محصولات و خدمات از ناوگان یا ارتش پشتیبانی می‌کنند، نیز بخشی از محیط گسترده‌تری برای امنیت دریایی هستند. بنابراین، امنیت دریایی و برتری جنگی تا حدودی به خنثی‌سازی حملات صورت گرفته بر سایت‌های نظامی و دولتی و همچنین تأمین امنیت اطلاعات حساس از سرقت و جاسوسی بستگی دارد. اطلاعات حساس، در دستان نادرست می‌تواند با بهبود هدفگیری نیروهای دریایی و افزایش دانش دشمن در مورد چگونگی آرایش، آموزش و تجهیز نیروهای خودی برای جنگ، اثربخشی عملیاتی ناوگان را تضعیف کند(Tighe, 3 May 2021).

ب) پیامدها در سطح تاکتیکی نبرد

در سطح تاکتیکی، فرماندهان نیروی دریایی باید از فناوری سایبری در تاکتیک‌های جنگی خود استفاده کنند. به طور عملی، این بدان معناست که قابلیت‌های سایبری تهاجمی و تدافعی باید در کنار اقدامات متحرک دیگر به کار گرفته شود. فضای سایبر می‌تواند تأثیرگذاری ابزارهای متحرک سنتی را از طریق تقویت دسترسی به اطلاعات و همچنین بهبود هدف‌گیری افزایش دهد. فضای سایبر همچنین چالش‌های جدیدی برای عملیات‌های دفاعی در حفاظت از سامانه‌ها از حملات سایبر و همچنین آتش‌های متحرک ارائه می‌دهد. فضای سایبر و قابلیت‌های سایبری نقش بسیار مهمی در پشتیبانی از سامانه‌های تسلیحاتی مبتنی بر شبکه مانند موشک‌های راهبردی- تاکتیکی «تاماهاک»[2] ایفا می‌کند، که داده‌های هدف‌گیری موردنیاز در جنگ را از مراکز کنترل و فرماندهی

[1] offensive action, defensive action, and network operations

[2] – تاماهاک بی جی ام-۱۰۹ موشک جنگی دوربرد مادون سرعت صوت از نوع موشک کروز است که قابلیت پرتاب

عملیات دریافت می‌کند. به همین طریق، برنامه‌های تعمیر و نگهداری از هواپیماها تا حد زیادی به فضای سایبر وابسته است تا آن‌ها را برای انجام مأموریت‌های مهم و حساس آماده کند. گزینه‌های دیگری برای برطرف کردن خطای سامانه‌ای وجود دارد، اما دسترسی به فضای سایبری مطمئن برای استقرار موفقیت‌آمیز این سامانه‌ها ضروری است. وابستگی به فضای سایبر در حال افزایش است، بنابراین نیاز به دسترسی ایمن به این فضا نیز در حال افزایش است(Navy Cyber Power ۲۰۲۰:۱۲).

امنیت نیروی دریایی همچنین تا حد زیادی به حفاظت از اطلاعات حیاتی در فضای سایبر بستگی دارد. به دلیل فراگیر بودن و همبستگی، فرصت‌های دسترسی غیرقانونی به اطلاعات فراوان است. این وظیفه نیروی دریایی است که آسیب‌پذیری خود را به حداقل برساند. تضمین امنیت اطلاعات مخاطرات مرتبط با استفاده، پردازش، ذخیره و انتقال داده‌ها و همچنین سامانه‌ها و فرایندهای مورد استفاده در پردازش را مدیریت می‌کند. راهبرد فضای سایبر برای حفاظت از دسترسی، یکپارچگی، اعتبار و محرمانگی داده طراحی شده است. به‌عنوان نسل بعدی امنیت عملیات‌ها، راهبرد فضای سایبر از اطلاعات مهم طبقه‌بندی شده و عادی حفاظت می‌کند. برای نیروهای دریایی، این فرایند حفاظت از اطلاعات ضروری به‌معنای آموزش رفتارهای مناسب سایبری به ملوانان و ادغام امنیت سایبر در چرخه حیات سامانه‌ها می‌باشد.

ج) پیامدها در درون ساختار فضای سایبر

روش دیگر برای درک پیامدهای فضای سایبر برای راهبرد و امنیت دریایی، ارزیابی ساختار فضای سایبر و یافتن فرصت‌هایی برای ایفای نقش راهبرد و امنیت دریایی است. چهار لایه فضای سایبر همان‌طور که در تعریف مفاهیم اشاره شد، عبارت‌اند از: لایه فیزیکی، منطقه، اطلاعاتی و لایه کاربر(Rattray, 2014: 33).

لایه فیزیکی[1]

لایه فیزیکی فضای سایبر از رایانه‌ها، سرورها، کابل‌های فیبر نوری، دکل‌های مخابراتی، ماهواره‌ها

و استفاده در همه شرایط آب و هوایی و جوی را دارد. این موشک در دهه ۱۹۷۰ برای پرتاب از زیردریایی‌ها به صورت دوربرد، ارتفاع پایین، و قابل شلیک از زیردریایی‌ها در شرکت جنرال داینامیکس آمریکایی طراحی شد. از آن زمان تا کنون این موشک چندین بار در شرکت‌های زیرمجموعه‌ای و غیرزیرمجموعه‌ای ارتقا یافته است و هم‌اکنون در شرکت ریتون ساخته می‌شود(Tighe, 3 May 2021).

[1] Physical layer

و اجـزای دیگـر زیرسـاخت فیزیکـی تشـکیل شـده اسـت کـه حـوزه جهـانی و همچنـین طیـف الکترومغناطیس را تشکیل می‌دهـد. ایـن عناصـر فیزیکـی در برابـر دسـتکاری، آسـیب و تخریـب آسیب‌پذیرند. کابل‌های زیردریایی از بستر دریاها عبور می‌کنند، برخی اوقات این کابل‌ها در اعماق دریا مدفون می‌شوند و در برخی موارد نه، و از سوی دیگر دریا بـه محـل‌هـای مشـخص شـده در ساحل وارد می‌شوند. اکثر آسیب‌های وارد شده به این کابل‌ها به صورت تصادفی صورت می‌گیرد، مانند آسیب‌های ناشی از سقوط لنگر کشتی و یا عبور کشتی‌ها در آب‌های کم‌عمـق کـه منجـر بـه آسیب‌زدن به کابل‌های زیر آب می‌شود. با این‌حال، دستکاری کابل‌های زیرآبـی مـی‌توانـد عمـدی باشد. برای مثال، در جنگ آمریکا و اسپانیا، کابل‌های تلگراف بـه‌عنـوان بخشـی از راهبـرد مختـل کردن پیوندهای ارتباطی فرا اقیانوسی نابود شد (Cheney Hyde, 1956: 77). در طول جنگ سـرد، ایالات متحده برای شنود به مکالمات تلفنی کـه در پـس پـرده آهنـین[1] اتفـاق مـی‌افتـاد، بـه شـبکه کابل‌های تلفن شوروی نفوذ کرد. در سال ۲۰۱۳ سه نفر به دلیل تلاش برای قطع کردن کابـل‌هـای زیردریایی در سواحل اسکندریه مصـر بازداشـت شـدند (BBC News ۲۷ مـارس ۲۰۱۵). ایـن دستکاری‌ها در کابل‌های زیردریایی در سال‌های بعد نیز ادامه داشت. به هر صورت، چه به صورت عمد یا غیرعمد، کابل‌های آسیب‌دیده می‌تواند کارآیی، اعتماد و امنیت شبکه جهانی را بـه مخـاطره بیفکند.

هیچ نیرویی وظیفه محافظت از این کابل‌ها را برعهده ندارد، اما نیروی دریایی به‌عنوان نیروی فعـال در حوزه دریایی حداقل وظیفه دارد که آسیبی به این کابل‌ها نرساند و حتی به طـور بـالقوه از ایـن زیرساخت‌های حیاتی در برابر آسیب‌رسانی و دسـتکاری دشـمن متخاصـم محافظـت کنـد. گـارد ساحلی و نیروی دریایی که بر انجام عملیات‌های ساحلی تمرکز دارند، مسئولیت بیشـتری در قبـال حفاظت از این زیرساخت‌های حیاتی عهده‌دار است، زیرا این کابل‌ها هنگامی که به ساحل نزدیـک می‌شوند هنگام ورود به لوله‌های محافظ ساحلی بیشترین میزان آسـیب‌پـذیری را دارنـد. بنـابراین، نیروهای مستقر در دریا که شامل نیروی دریایی و گارد ساحلی می‌شود، وظیفه نظارت و حفاظـت

[1] – پرده آهنین (Iron Curtain) نام بخش‌بندی مرزی اروپای پس از جنگ جهانی دوم –در ۱۹۴۵– و در جنگ سرد به دو بخش اروپای غربی و کشورهای عضو پیمان ورشو بود. با پایان جنگ سرد در ۱۹۹۱ پرده آهنین نیز برچیده شد. این اصطلاح کنایه‌ای است از تلاش‌های اتحاد جماهیر شوروی برای ممانعت از ارتباط آزاد خود و دولت‌های اقماری‌اش با کشورهای غیر کمونیستیِ غربی. این اصطلاح را نخستین بار وینستون چرچیل در سال ۱۹۴۵ ضمن بحث از مسائل سیاست خارجی در مجلس عوام به‌کار برد.

از زیرساخت‌های حیاتی فضای سایبری را عهده دارند (U.S. Department of Defense, February 5, 2019).

طیف الکترومغناطیسی(EM) یکی از عناصر تشکیل دهنده فضای سایبر و مولفه اصلی عملیات‌های دریایی است. برای دهه‌های متمادی، نیروهای دریایی عملیات‌های مختلفی را با استفاده از طیف الکترومغناطیس انجام داده‌اند و از تاکتیک‌های جنگ الکترونیک در پشتیبانی از عملیات‌های دریایی استفاده کرده‌اند. با توجه به اینکه فضای سایبر بخش قابل توجهی از محیط اطلاعاتی را تشکیل می‌دهد و طیف الکترومغناطیس یکی از اجزای اصلی فضای سایبر است، جنگ الکترونیک بخشی از فضای سایبر به حساب می‌آید. هدف از جنگ الکترونیک، «انکار برتری دشمن در طیف الکترومغناطیس و تضمین دسترسی بدون مانع نیروهای دوست به بخش طیف الکترومغناطیس محیط اطلاعاتی است». جنگ الکترونیک از تاکتیک‌های تهاجمی و تدافعی استفاده می‌کند تا از طریق شناسایی، انکار، فریب، اختلال، تخریب،حفاظت و انهدام دسترسی بدون مانع را تضمین کند. فعالیت‌های جنگ الکترونیک متعارف شامل رادارهای تولید پارازیت و نفوذ و ایجاد پیوندهای ارتباطی می‌شود. یک نمونه از سامانه‌های دریایی که در جنگ الکترونیک استفاده می‌شود هواپیمای نیروی دریایی ایالات متحده «پراولر»[1]است که با اختلال در فعالیت‌های الکترونیک دشمن، اطلاعات الکترونیک راهبردی از منطقه عملیات جمع‌آوری می‌کند(Haig, 2018: 8-12).

به گفته فرمانده عملیات‌های دریایی نیروی دریایی ایالات متحده، «در دو دهه آینده، محیط الکترومغناطیس ممکن است به حیاتی‌ترین عرصه جنگی ما تبدیل شود» (وزارت دفاع امریکا، ۵ فوریه ۲۰۱۹). کنترل اطلاعات که اکثر آن از طریق طیف الکترومغناطیس صورت می‌گیرد در حال حاضر از کنترل قلمرو در جنگ‌های مدرن اهمیت بیشتری دارد. جنگ الکترونیک و امروزه جنگ مانور الکترومغناطیس بر مدیریت و کنترل طیف الکترومغناطیس متمرکز است. قابلیت‌هایی که طیف الکترومغناطیس ارائه می‌دهد، برای مأموریت‌های دستیابی به آگاهی از فضای نبرد و آگاهی بهینه از حوزه دریایی اهمیت حیاتی دارد. عملیات‌های انعطاف‌پذیر و قابلیت مانور در فرکانس‌های

[1] – نورثروپ-گرومن ئی‌ای-۶بی پراولر (Northrop Grumman EA-6B Prowler) یک هواپیمای دوموتوره جهت ماموریت‌های جنگ الکترونیک می‌باشد که توسط شرکت نورثروپ و (بعدتر نورثروپ گرومن) آمریکا تولید گردیده است. این هواپیما از سال ۱۹۷۱ تاکنون در خدمت نیروهای مسلح ایالت متحده می‌باشد. ۴ نفر خدمه شامل یک خلبان یک متصدی اسلحه و دو نفر متصدی جنگ الکترونیک (جنگال) این هواپیما در سال ۲۰۱۵ قسمت اعظم جای خود را به هواپیمای جنگ الکترونیک پیشرفته ئی/آ-۱۸جی گراولر داد.

مختلف در طیف الکترومغناطیس به نیروهای دریایی امکان دسترسی ایمن و انجام عملیات در محیط جنگ الکترونیک را فراهم می‌کند(Cyberspace Operations, 2019 : vii).

لایه منطقی[۱]

لایه منطقی، سامانه عصبی مرکزی فضای سایبر است. این لایه مسئولیت مسیریابی بسته‌های داده به مقاصد نهایی خود معمولاً از طریق سامانه‌های نام دامنه یا دی‌ان‌اس (DNS)[۲]، پروتکل‌های اینترنتی، جستوگرها، وب‌سایت‌ها و نرم‌افزارها را بر عهده دارد. تمامی موارد ذکر شده به کابل‌های فیبر نوری و زیرساخت‌های فیزیکی وابسته است. حملات سایبری هدفمند می‌تواند لایه منطقی فضای سایبر را به روش‌های مختلفی هدف قرار دهد و باعث سوء عملکرد و یا از کار افتادن کامل آن شود تا مانع از جریان یافتن داده شود. یک نمونه از این نوع حملات، حمله استاکسنت[۳] است. حمله استاکسنت که به تسلیحات هسته‌ای ایران صورت گرفت از طریق یک کرم کامپیوتری انجام شد که کارکرد داخلی تجهیزات پیشرفته را مختل کرد و در عین حال اپراتورهای سامانه قادر به شناسایی عامل اصلی آن نبودند(Chiefs of Staff, November 27, 2021).

نیروهای دریایی با استفاده از تسلیحات سایبری تهاجمی و تدافعی در لایه منطقی فضای سایبر نقش‌آفرینی می‌کنند. بیشتر سلاح‌های سایبری شامل دستکاری ساختار «منطقی» فضای سایبر می‌شود. تغییر در این لایه می‌تواند منجر به اختلال و هدایت نادرست جریان اطلاعات، ایجاد مانع، نصب نقاط ورودی و خروجی مخفی و ایجاد اثرات جدید بدون رضایت طرف موردنظر شود. بنابراین، لایه منطقی جایی است که درگیری‌های سایبری معمولاً واقع می‌شود، دیوارهای سایبری آنجا ساخته می‌شود (برای مثال، دیوار آتش بزرگ چین)، و «جنگ سایبری» تعریف‌شده بین ماشین‌ها رخ می‌دهد.

جنگ اطلاعاتی(IW)[۴] لایه‌های فیزیکی و منطقی فضای سایبر را در برمی‌گیرد. جنگ اطلاعاتی به

۱- Logic layer

۲- domain name systems

۳ - اِستاکس‌نِت (Stuxnet) یک بدافزار رایانه‌ای (طبق نظر شرکت‌های نرم‌افزار امنیت رایانه‌ای: کرم رایانه‌ای یا تروجان) است که اولین‌بار در تاریخ ۱۳ ژوئیه ۲۰۱۰ توسط آنتی‌ویروس وی‌بی‌ای۳۲ شناسایی شد. براساس نظر کارشناسان شرکت سیمانتک، این بدافزار به دنبال خرابکاری در تأسیسات غنی‌سازی اورانیوم نطنز بوده‌است.

۴- Information Warfare

طور مستقیم در هر جنبه‌ای از عملیات‌های دریایی دخالت دارد، زیرا از طریق بهره‌برداری از شبکه‌ها از نقاط ضعف دشمن برای به دست آوردن اطلاعات مورد نیاز تصمیم‌گیرندگان استفاده می‌کند. جنگ اطلاعاتی از طیف کاملی از اطلاعات سایبری، رمزنگاری‌شده و سیگنال‌های اطلاعاتی، عملیات‌های اطلاعاتی، عملیات‌های شبکه‌های کامپیوتری و مأموریت‌های جنگ الکترونیک در حوزه‌های مختلف فضای سایبر و الکترومغناطیس بهره می‌برد. عملیات‌های جنگ الکترونیک مانند عملیات‌های شبکه کامپیوتری در این لایه از فضای سایبر واقع می‌شود. (Haig, ۲۰۱۸: ۸-۱۲)

لایه اطلاعات

لایه اطلاعات شامل کدها، متن‌ها، عکس‌ها و مطالب دیگری می‌شود که از طریق فضای سایبر تولید، ذخیره و منتقل می‌شود. در این لایه، اطلاعات توسط کاربران دریافت و به اشتراک گذاشته می‌شود و ادراک و دانش آن‌ها تحت تأثیر قرار می‌گیرد. برای نیروهای نظامی، محیط اطلاعاتی شامل جهان فیزیکی، اطلاعات و داده و ابعاد شناختی با محوریت انسان می‌شود. عملیات‌های اطلاعاتی (IO)[۱]عبارت است از «بکارگیری یکپارچه قابلیت‌های مرتبط با اطلاعات در عملیات‌های نظامی به همراه انواع دیگر عملیات‌ها برای تأثیرگذاری و ایجاد اختلال در تصمیم‌گیری دشمنان بالفعل و بالقوه و در عین حال حفاظت از زیرساخت‌های مورد نیاز جهت تصمیم‌گیری نیروهای دوست». قابلیت‌های مرتبط با اطلاعات شامل ابزارها، تکنیک‌ها و فعالیت‌هایی می‌شود که از داده، دانش و اطلاعات برای تأثیرگذاری در محیط اطلاعاتی بهره می‌برد. انواع عملیات‌های اطلاعاتی ممکن است شامل فریب و یا عملیات‌های روانی از طریق انتشار اطلاعات نادرست برای تأثیرگذاری بر درک شناختی نیروهای هدف شود(Navy Cyber Power 2020 : 1).

لایه کاربر[۲]

در نهایت، لایه کاربر فضای مجازی از مردم و افرادی تشکیل شده است که با این فناوری درگیر هستند تا در فضای مجازی جوامع و تجربه‌های جدیدی را خلق کنند. واضح است که عملیات‌های اطلاعاتی برای هدف قرار دادن کاربران طراحی شده‌اند، بنابراین این عملیات‌ها هر دو لایه را تحت تأثیر قرار می‌دهند. با این حال، از منظر نیروهای دریایی، امنیت عملیات[۳](OPSEC) در لایه کاربر

۱ Information operations
۲ User layer
۳ operations security

بسیار حساس و حیاتی است. امنیت اطلاعات فرایند حفاظت از داده‌هایی است که ممکن است برای دشمن فایده داشته باشد، و در اصل اطلاعات را از چشمان دشمن دور نگه می‌دارد. عملیات‌های نظامی که در آن‌ها از فضای سایبر استفاده می‌شود، نیازمند سطح بالایی از امنیت اطلاعات است، زیرا محیط سایبری همه جا وجود دارد و اطلاعات زیادی در مورد سامانه‌ها و حتی سامانه‌های طبقه‌بندی نشده در آن وجود دارد که می‌تواند به صورت بالقوه برای دشمنان مفید واقع گردد.

نتیجه‌گیری و پیشنهادات

الف– نتیجه‌گیری: فضای سایبر برای عملیات‌ها و راهبردهای جدید دریایی بسیار مهم و حیاتی است، زیرا کنترل و فرماندهی نیروهای دریایی که برای تمامی عملیات‌ها ضروری است را تشکیل می‌دهد. سامانه‌ها و سامانه‌های مبتنی بر اطلاعات که آگاهی فضای نبرد، جمع‌آوری اطلاعات، هدف‌گیری و قابلیت‌های دیگر را امکان‌پذیر می‌کند، هسته اصلی موفقیت در مأموریت‌های دریایی می‌باشند. قدرت مانور و آزادی عمل به همراه توانایی سلب آزادی عمل دشمن در فضای سایبر، برای موفقیت عملیات‌های نظامی و راهبردهای جنگی لازم است. بنابراین، هدف نیروهای دریایی در آینده، حفظ آزادی عمل و سلب آزادی عمل دشمن در دریا و فضای سایبر خواهد بود.

در این زمینه، افزایش آگاهی از فضای نبرد سایبر به نیروهای دریایی این امکان را می‌دهد تا درک بهتری از محیطی که در آن عملیات می‌کنند، داشته باشند. همچنین، آتش‌های سایبری و یکپارچه فرصت‌های جدید برای اقدامات تهاجمی علیه دشمنان فراهم می‌کنند. حفاظت از شبکه‌های اطلاعاتی ملی و دریایی مستلزم انجام عملیات‌های سایبری تدافعی برای جلوگیری از حملات نفوذی به سامانه‌های هدف است. برای برخی از کشورها، امنیت سایبری می‌تواند شامل عملیات‌های سایبری تدافعی برای جلوگیری از حملات دشمنان و واکنش به حملات سایبری بر سامانه‌های ملی و دریایی شود. حملات سایبری و قابلیت‌های سایبری دشمنان مانند هدف‌گیری دقیق و حملات دوربرد بر کشتی‌ها بدان معناست که نیروهای دریایی در دریا نسبت به گذشته پیوند محکم‌تری با یکدیگر دارند و در عین حال آسیب‌پذیرتر شده‌اند. موازنه سنتی قوا بین نیروهای دریایی و دشمنان به دلیل گسترش قابلیت‌های سایبری بر هم خورده است، که این امر باعث ایجاد عدم تقارن شده است و همچنین نیروهای دریایی کوچک‌تر و بازیگران غیردولتی را به طور نامناسبی قدرتمندتر می‌سازد.

بنابراین، فضای سایبری تهدیدات بی‌شماری برای نیروهای دریایی و راهبردهای آن‌ها پدید

می‌آورد. تهدیدها در فضای سایبر سریع‌تر از آنکه نیروهای دریایی بتوانند خود را در برابر آن‌ها محافظت کنند، گسترش می‌یابند. این حوزه پیوسته در حال تکامل است و نوآوری سامانه‌ها، ابزارهای جدیدی را با سرعت بالایی تولید می‌کند. فضای سایبر به دلیل اینکه تا حدی یک محیط مصنوعی است، مکان‌نگاری آن نیز دستخوش تغییر است. بنابراین، در این فضا، چالش غافلگیری راهبردی برای نیروهای دریایی وجود دارد. نیروهای دریایی در ارتباط با اصل نزدیکی و مجاورت با نیروهای دشمن نیز با چالش‌های بزرگی مواجه‌اند. برای حمله به دشمن در عرصه دریا، دیگر نیاز نیست که دشمنان در فاصله نسبتاً نزدیک با آن‌ها قرار داشته باشند. آن‌ها می‌توانند در آن سوی دنیا با فاصله بسیار دور، حملات سایبری خود را علیه شبکه‌ها و سامانه‌های دریایی دشمن انجام دهند.

دقت سلاح‌های سایبری نیز چالش‌هایی برای نیروهای دریایی ایجاد می‌کنند. سلاح‌های سایبری می‌توانند دقیق‌تر از سلاح‌های دیگر باشند، زیرا آنها در درون شبکه‌های خاص و بر روی برخی رایانه‌های خاص و تحت شرایط مشخص (کنترل‌شده) اجرا می‌شوند. مقیاس حملات سایبری و تسلیحات سایبری نسبت به هزینه آن، برخلاف سلاح‌های متعارف و حملات در حوزه‌های دیگر، بیشتر است. به دلیل اینکه موانع ورود به فضای سایبر اندک است، مهاجمان سایبری می‌توانند حجم گسترده‌ای از آسیب‌ها را با سرمایه‌گذاری‌های محدود وارد سازند. مسائل مربوط به صلاحیت و کنترل در فضای سایبری نیز برای نیروهای دریایی کشورها مسئله‌ساز است. مشخص نیست که کدام اتفاق در فضای سایبر در حوزه دریا اقدام مجرمانه و کدام رویداد به طور بالقوه اقدام جنگی محسوب می‌شود. این مسائل و چالش‌های پیش رو، پیشنهادهای خاصی می‌طلبد که در ادامه به برخی از مهم‌ترین آنها اشاره می‌شود:

ب–پیشنهاد:

– افزایش آگاهی از فضای سایبر در حوزه دریا به منظور درک بهتر از محیط عملیات سایبری یکپارچه در دریا؛

– نوآوری سامانه‌ها و ایجاد ابزارهای جدیدی در حوزه فضای سایبر دریایی با توجه به تهدیدات رو به تکامل در این حوزه؛

– ایجاد قرارگاه یکپارچه سایبری و عملیات‌های آفندی–پدافندی یکپارچه برای حفاظت از شبکه‌های اطلاعات ملی و دریایی.

– لزوم تدوین قوانین خاص در حوزه سایبری دریایی، همکاری‌های بین‌المللی در خصوص

جرم‌انگاری تهدیدات سایبری، و همکاری‌های بین بخشی (دولت‌ها، بخش خصوص، سازمان‌های نظامی دریایی و...).

منابع و مأخذ

فارسی:

- احدی، محمد، شاهمحمدی، محمد (۱۳۹۷)؛ طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی، ***فصلنامه مطالعات بین‌رشته‌ای دانش راهبردی***، سال هشتم، شماره ۳۱، تابستان ۱۳۹۷، صص ۲۵۲-۲۲۵
- بوژمهرانی، علی اصغر و مهدوی حاجی محمدرضا (۱۳۹۹)؛ واکاوی تهدیدات نوین سایبری در نیروهای مسلح، ***فصلنامه مطالعات جنگ***، دوره ۲، شماره ۶ ، آذر، صص:۱۰۰-۱۲۶
- خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند یاسر (۱۳۹۱)؛ تهدیدات سایبری و تأثیر آن بر امنیت ملی، ***فصلنامه مطالعات راهبردی***، سال پانزدهم، شماره دوم، تابستان، صص ۱۹۶-۱۶۷.
- کاویانی حسن، میرسپاسی ناصر و دیگران (۱۳۹۹)؛ طراحی مدل شایستگی کارکنان در حوزه امنیت سایبری، ***فصلنامه مطالعات بین‌رشته‌ای دانش راهبردی***، سال دهم، شماره ۴۱، زمستان ۱۳۹۹، صص ۲۹۸-۲۷۳.
- نجفی سیار، رحمان (۱۴۰۱)؛ ارزیابی راهبردهای جدید دریایی ایالات متحده در برابر چین؛ مزیت‌ها و چالش‌ها، ***فصلنامه روابط خارجی***، دوره ۱۵، شماره ۵۴، صص ۳-۲۷.
- یادگاری، وحید و دیگران (۱۳۹۶)؛ نقش امنیت فاوا در جنگ سایبری علیه سازمان‌های امنیتی با رویکرد پدافند غیرعامل، ***فصلنامه پژوهش‌های حفاظتی- امنیتی***، دانشگاه جامع امام حسین (ع) سال ۶، شماره ۲۱، صص ۱-۲۴.

منابع انگلیسی:

- Brenner, Susan (2018); ***Cyberthreats: The Emerging Fault Lines of the Nation State,*** New York: Oxford University Press.
- BBC News, (August 28, 2015); ***Egypt Arrests as Undersea Internet Cable Cut Off Alexandria,"*** Available at: www.bbc.com/news/world-middle-east-21963100.
- Choucri Nazli and David D. Clark, (2021); "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma, ***Harvard University and Massachusetts Institute for Technology,*** November 6–7.
- Choucri and Clark, (2021); ***Integrating Cyberspace and International Relations***, Cambridge Press.

- Charles Cheney Hyde, (1956); ***International Law,*** Chiefly as Interpreted and Applied by the United States , 2nd rev. edn., 3 vols. Boston, MA: Little, Brown.
- Daniel T. Kuehl, (2019); "From Cyberspace to Cyberpower: Defi ning the Problem," in *Cyberpower and National Security* , ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, ***Washington, DC: National Defense University Press*** and Potomac Books, Inc., p. 28.
- Cyberspace Operations, Joint Publication 3-12, ***U.S. Department of Defense,*** February 5, 2019.
- Dombrowski Peter and Chris C. Demchak, (Spring 2017), "Cyber War, Cybered Confl ict, and the Maritime Domain," ***Naval War College Review*** 67, 2, pp. 73–6.
- Defence White Paper 2018: ***Defending Australia and its National Interests ,*** Department of Defence, Government of Australia. Available at: www.defence.gov.au/whitepaper/docs/ WP_2013_web.pdf
- Impson, Nick (2020); ***The Next Warm War: How History's Anti-Access/Area Denial*** ,Campaigns Inform the Future of War, Address: https://smallwarsjournal.com/jrnl
- Navy Cyber Power 2020 ; ***U.S. Navy Information Dominance Roadmap 2013–2028,*** Deputy Chief of Naval Operations for Information Dominance, Director of Warfare Integration for Information Dominance,p. ii. Available at: www.defenseinnovationmarketplace.mil/resources/Information_Dominance_Roadmap.
- Navy Cyber Power 2020: Sustaining U.S. Global Leadership – Priorities for 21st Century Defens, Deputy Chief of Naval Operations for Information Dominance/Fleet Cyber Command/Tenth Fleet, ***Washington, DC, November 2020.*** Available at: www.defenseinnovationmarketplace.mil/resources/NavyCyberPlan2020.pdf
- Russell, Alison Lawlor; (2018); ***Cyber Blockades***, Washington, DC: Georgetown University Press.
- ***The UK National Strategy for Maritime Security,*** HM Government, May 2019, p. 19. Available at: www. gov.uk/government/publication.
- Rattray, Gregory J (2014); ***Strategic Warfare in Cyberspace,*** Cambridge, MA: MIT Press.
- Sherry Sontag and Christopher Drew, (2012); ***Blind Man's Bluff,*** New York: HarperCollins.
- Sherry Sontag and Christopher Drew,(1998); ***Blind Man's Bluff***, New York: Harper Collins.
- Stavridis, James "Time for a U.S. Cyber Force, ***Proceedings Magazine*** 140, 1/1331, January 2017.
- ***Maritime Doctrine of the Russian Federation 2020***, July 2001, Ocean Policy 2020, p. 16. Available at: www. oceanlaw.org/downloads/arctic/Russian_Maritime_Policy_2020.pdf

- U.S. Navy Information Dominance Roadmap 2013–2028 , pp. 7–8; ***Navy Cyber Power 2020***.
- VADM Jan E. Tighe, 3 (May 2021); "The Impact of Cyber on the Maritime Operational Level of War," ***MOC Warfighter***. Available at: www.usnwc.edu/mocwarfighter/Article.aspx?ArticleID=23
- Zsolt, Haig. (2018); ***Electronic Warfare in Cyberspace,*** Faculty of Military Sciences and Officer Training National University of Public Service, Budapest, Hungary.p6.