فصلنامه مدیریت و پژوهش‌های دفاعی

۱۰۳

سال بیست و سوم
بهار ۱۴۰۳

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۲/۰۷/۲۱
تاریخ پذیرش:
۱۴۰۳/۰۳/۳۰
صص: ۳۷-۱۱

شاپا چاپی: ۶۱۲۱-۲۰۰۸
الکترونیکی: ۵۲۱۸-۲۶۴۵

نقش ظرفیت فضای سایبری در ارتقای سطح آگاهی وضعیتی مراکز فرماندهی و کنترل

سعید کافی [۱]

چکیده

در سال‌های اخیر بشر با رشد فن‌آوری اطلاعات و ارتباطات متوجه کارکردهای فضای سایبری در جنگ‌ها شده است. از جمله این کارکردها به بهره‌گیری سازمان‌های نظامی از ظرفیت‌های فضای سایبری در فرماندهی و کنترل به منظور افزایش آگاهی وضعیتی اشاره می‌شود. آگاهی وضعیتی یکی از کارکردهای مراکز فرماندهی و کنترل است و هر چه سطح این آگاهی بیشتر شود، اشراف اطلاعاتی بیشتری برای نیروهای عمل کننده تحت پوشش مراکز فرماندهی و کنترل فراهم می‌شود. نقطه قوت هر مرکز فرماندهی و کنترل سطح آگاهی وضعیتی آن است. در این پژوهش چند سناریوی واقعی از رزمایش‌های نظامی در دنیا معرفی شده است که به موجب آن کارکردهای فرماندهی و کنترل در فضای سایبری مشخص می‌شود. در این سناریوها تلاش شده است تا کارکرد آگاهی وضعیتی به خوبی به صورت مثال‌هایی بیان شود. در نهایت یک مدل پیشنهادی فرماندهی و کنترل با الهام از ظرفیت‌های فضای سایبری ارائه شده است. این پژوهش به روش توصیفی – تحلیلی اجرا شده و به این جمع بندی می‌رسد که با توجه به گسترش فن‌آوری اطلاعات و ارتباطات ظرفیت فضای سایبری نقش مهمی در ارتقای سطح آگاهی وضعیتی دارد و مانع از غافلگیری یگان‌های نظامی می‌شود.

کلیدواژه‌ها: مراکز فرماندهی و کنترل، فضای سایبری، آگاهی وضعیتی.

DOR: 20.1001.1.20086121.1403.23.103.1.6

۱. استادیار، دکتری هوافضا، مدیریت راهبردی، فرماندهی و ستاد، دانشگاه جامع امام حسین(ع)، تهران، ایران
dr.saeedkafi@gmail.com

مقدمه

یکی از نیازهای اساسی هر عملیات نظامی بهره‌گیری از کارکردهای مراکز فرماندهی و کنترل است. وجود این مراکز برای ایجاد آگاهی وضعیتی و هماهنگی نیروهای عمل کننده و در نهایت تحقق مأموریت‌ها حیاتی به شمار می‌آید. فرماندهی و کنترل موجب هماهنگی کارکردهای نظامی مانند اطلاعات، مانور، قدرت آتش، پشتیبانی خدمات رزم و اقدامات تأمینی می‌شود و به کارایی و اثربخشی نیروهای نظامی کمک شایانی می‌نماید. فرماندهی و کنترل در بستر ۵ متغیر قابل تحلیل است: "چه کسی، چه چیزی، چه زمانی، کجا و چگونه". پژوهش حاضر از این ۵ متغیر تمرکز خود را بر روی "چگونگی" یا به عبارتی نحوه اجرای عملیات به منظور برخورداری از بیشترین سطح آگاهی وضعیتی گذاشته است.

فضای سایبری قلمرو پنجم درگیری‌های بشری بعد از زمین، هوا، دریا و فضا محسوب می‌شود. همان طور که زمانی با توسعه درگیری‌ها نیاز به تولید مفاهیم مرتبط با جنگ‌های زمینی و پس از آن هوایی، دریایی و فضایی بود، امروزه نیز نیاز به تولید مفاهیم مشابه در فضای سایبری است. فضای سایبری روز به روز در جنگ‌ها نقش مهم‌تری را پیدا می‌کند و این به دلیل ویژگی‌های خاص و برتر این فضا نسبت به فضاهای سنتی مورد اشاره است. از جمله این ویژگی‌ها به هزینه‌های کمتر عملیات در این فضا، کاهش عده نفرات مورد نیاز از سطح تیپ و لشکر به سطح افراد معدود (حتی کمتر از تعداد افراد متشکل از یک دسته نظامی) اما متخصص، بی نیازی به تجهیزات و ادوات رایج نظامی، گمنامی نفرات در این فضا، امکان اجرای عملیات از هر نقطه از کره زمین در صورت وجود زیرساخت‌های مرتبط، سرعت غافلگیری و اجرای عملیات بدون وجود شواهد و قرائن عملیات پیش از اجرای عملیات در فضاهای سنتی و بسیاری از موارد مشابه اشاره می‌شود. (Ministry of Defense of the Netherlands, 2012)

فضای سایبری محیطی متشکل از شبکه وابسته به یکدیگر در زیرساخت فن‌آوری دیجیتالی است که شامل پلتفرم‌ها، اینترنت، شبکه ارتباطی، سامانه‌های رایانه‌ای، پردازشگرها و کنترلرهای درون‌زا می‌شود و اطلاعات در این فضا به صورت فیزیکی و مجازی و در قلمرو شناختی که خود قلمرو ششم نبردها است، به گردش در می‌آید. آگاهی وضعیتی[1] درک حوزه خاص، مسأله یا

1 Situational Awareness (SA)

موقعیتی است که در چارچوب محدودیت‌های زمانی و مکانی قرار دارد. آگاهی وضعیتی در ۳ مرحله مورد استفاده قرار می‌گیرد. این ۳ مرحله شامل وضعیت نیروهای خودی، شرایط محیطی و جغرافیایی و در نهایت وضعیت نیروهای دشمن می‌شود. توسعه ابزارهای ارتباطی و وابستگی‌های دیجیتالی در ارتش‌ها موجب شده است تا نقش فضای سایبری در افزایش آگاهی وضعیتی بیش از پیش شود.

حجم زیاد اطلاعاتی که به کمک سامانه‌های اطلاعاتی تولید می‌شود، این پتانسیل را دارد که برای افزایش آگاهی وضعیتی مورد استفاده قرار گیرد. کلان داده‌ها از نظر حجم، شدت و تنوع داده در فضای سایبری ظرفیت تحلیلی مراکز اطلاعاتی را اشباع کرده‌اند. ماهیت خارج از محدودیت مرزهای جغرافیایی در فضای سایبری موجب شده است تا هم دسترسی‌ها بدون محدویت مرزی باشد و هم تهدیدها به صورت فرامرزی خود را نشان دهد. بهره‌گیری از این اطلاعات به شکل فیلتر شده و بدون عوامل تهدیدزا در سامانه فرماندهی و کنترل شرایطی را به وجود می‌آورد که فرمانده به اطلاعات بیشتری دست پیدا کند و تصمیمات بهتری اتخاذ نمایند. فن‌آوری‌های اطلاعاتی این امکان را دارد تا از انواع تجهیزات حسگرها در فرماندهی و کنترل به منظور شناسایی، تعیین موقعیت، ردیابی، نظارت و غیره استفاده نماید. هم اکنون، ارتش‌های عضو پیمان نظامی ناتو از طرح ابتکاری کاربردهای علم و فن‌آوری در محیط محاسبات ابری و میزبانی حسگرهای اینترنت اشیاء، تجهیزات و توانمندی‌های اطلاعاتی و یکپارچه سازی منابع اطلاعاتی در این بستر استفاده می‌کنند. این ادغام و یکپارچه سازی در رزمایش نیروهای عضو پیمان ناتو در سال ۲۰۲۱ مشاهده شد. (Congressional Research Service, 2021)

اما فرماندهی بنا به تعریف اختیاری است که به یک فرد برای انجام وظیفه یا مأموریت مشخصی واگذار شده است و کنترل مجموعه اقداماتی است که فرد با استفاده از آنها می‌تواند از اجرای فرامین خود مطمئن شود. از جمله این اقدامات می‌توان به فرآیندها یا روش‌های جاری عملیاتی اشاره کرد. (Simoens, 2021)

عباراتی مانند سامانه فرماندهی و کنترل سایبری یا سامانه مدیریت پدافند شبکه‌ای برای توصیف سامانه‌هایی بکار می‌رود که در مدیریت از راه دور دیوارهای آتش، سامانه کشف رخنه و سایر زیرسامانه‌ها و اجزای شبکه کاربرد دارند. واژه سامانه فرماندهی و کنترل مورد استفاده در

پژوهش حاضر معنا و مفهوم متفاوتی دارد. مدیریت از راه دور دیوار آتش سامانه‌های کشف رخنه و سایر موارد بخشی از سامانه فرماندهی و کنترل است. مفهوم فرماندهی و کنترل در این پژوهش مشابه فرماندهی و کنترل در جنگ‌های فیزیکی است.

در حملات فیزیکی پس از گزارش حمله به یکی از دستگاه‌ها به سایر دستگاه‌ها و سازمان‌ها نیز هشدار حملات مشابه داده می‌شود. کارشناسان تضمین اطلاعات[1] حملات را به عنوان بخشی از فرآیند کاری خود تحلیل می‌کنند. در سلسله مراتب فرماندهی هنگامی که فرمانده اطلاعات هدف را دریافت می‌کند، دستورات را در خصوص چگونگی مقابله با تهدید به سلسله مراتب زنجیره فرماندهی زیرامر صادر می‌نماید. در نهایت، اقدامات لازم برای ارزیابی آسیب پذیری به صورت دقیق انجام می‌شود و آسیب‌پذیری‌ها برای کاهش مخاطرات رفع می‌شود. در صورتی که اقدامات ارزیابی آسیب‌پذیری به موقع انجام نشود، مخاطرات حمله متوجه نقاطی می‌شود که آسیب‌پذیری‌های آن به موقع مرتفع نشده است. گاهی زمان برای کشف و واکنش نسبت به حمله از چند ساعت تا چندین روز طول می‌کشد و برای اتخاذ هر گونه اقدامی باید منتظر ماند تا دستورات از رأس سلسله مراتب فرماندهی دریافت شود. اتخاذ برخی از اقدامات مانند جداسازی شبکه یا قطع خدمات خاص نیز نیازمند کسب دستور است. (Mani, et al. 2020)

این سبک از فرماندهی و کنترل که متکی بر تهیه گزارش وضعیت و ارسال آن به رأس سلسله مراتب فرماندهی برای اخذ تصمیم و برگشت دستور در زنجیره فرماندهی است، در پدافند سایبری کارایی چندانی ندارد. جنگ‌های سایبری گاهی ظرف چند ثانیه یا چند دقیقه رخ می‌دهند و این در حالی است که جنگ‌های فیزیکی پیش از وقوع دارای شواهد و قرائنی هستند که روزها یا ماه‌ها قبل از جنگ قابل مشاهده و بررسی می‌باشند. حتی سمت حمله و اهداف حمله نیز قابل پیش بینی است. تمام این موارد نشان می‌دهد که استفاده از نظام فرماندهی و کنترل جنگ‌های فیزیکی کارایی مطلوبی در جنگ سایبری ندارد. از سوی دیگر، ساختار فرماندهی و کنترل جنگ‌های سنتی در هنگام ادغام فرماندهی و کنترل سایبری در فرماندهی و کنترل فیزیکی قابل استفاده است. (Simoens, 2021)

---

۱. تضمین اطلاعات (Information Assurance) مجموعه اقداماتی است که با هدف تضمین دسترس‌پذیری، یکپارچگی، احراز هویت، محرمانگی و عدم منع استفاده از اطلاعات و سیستم‌های اطلاعاتی به عمل می‌آید.

در بیان اهمیت پژوهش حاضر و با عنایت به مطالب پیش گفته در صورت پرداختن به پژوهش حاضر می‌توان ساختار مراکز فرماندهی و کنترل را مطابق با تهدیدهای فضای سایبری به روز کرد و آگاهی وضعیتی را ارتقاء داد و در صورت بی توجهی به پژوهش حاضر آگاهی وضعیتی مراکز فرماندهی و کنترل کمتر شده و به همین شکل نیروهای عمل کننده قادر به درک واقعیات صحنه نبرد نخواهند بود.

در نتیجه، دغدغه و هدف پژوهش حاضر بررسی نقش ظرفیت فضای سایبری در ارتقای سطح آگاهی وضعیتی مراکز فرماندهی و کنترل است.

مبانی نظری

بررسی قیاسی مراکز فرماندهی و کنترل فیزیکی و سایبری

پیش از ورود به بررسی قیاسی مراکز فرماندهی و کنترل فیزیکی و سایبری واژه آگاهی وضعیتی[1] مورد بررسی و تبیین قرار می‌گیرد. آگاهی وضعیتی بنا به تعریف عبارت است از درک محیط، عوامل محیطی و چگونگی تغییر این عوامل در فرآیند زمانی یا سایر عناصر تأثیرگذار است. وجود آگاهی وضعیتی برای اخذ تصمیم مؤثر در محیط‌های مختلف حائز اهمیت است. یک تعریف دیگر از آگاهی وضعیتی به قرار زیر است: "درک عناصر در محیط در محدوده زمانی و مکانی، مفهوم سازی این عناصر و ترسیم وضعیت محیط در آینده نزدیک."

آگاهی وضعیتی پایه حیاتی در اخذ هر تصمیم گیری موفق آمیز است. بسیاری از دستاوردهای آگاهی وضعیتی منتج به حفظ جان انسان‌ها و دارایی‌های مهم می‌شود. آگاهی وضعیتی در هر محیطی اعم از فرودگاه‌ها و کنترل ترافیک هوایی، مراکز نظامی و امنیتی و ناوبری دریایی، هوایی و زمینی کاربرد دارد و بی شک یکی از کاربردهای مهم آن در مراکز فرماندهی و کنترل است. نبود آگاهی وضعیتی منجر به اخذ تصمیمات اشتباه و در نتیجه بروز صدمات و تلفات می‌شود. آگاهی وضعیتی در ۳ مرحله توصیف می‌شود: "درک عناصر محیطی، شناخت موقعیت خود و دشمن و ترسیم موقعیت در آینده". آنچه علاوه بر موارد فوق حائز اهمیت است همجوشی اطلاعاتی به منظور مفهوم سازی آنچه می‌گذرد و آنچه خواهد آمد است. هر چه این همجوشی

1 Situational awareness or situation awareness (SA)

بیشتر شود، به همان اندازه قدرت اخذ تصمیم گیری از حالت واکنشی به پیش کنشی است. آگاهی وضعیتی علاوه بر سه مرحله فوق مبتنی بر سه عنصر انسانی، تجهیزاتی و فرآیندی است. عناصر انسانی با استفاده از تجهیزات لازم در قالب فرآیندهای مرتبط به درک عناصر محیطی، شناخت موقعیت خود و دشمن و ترسیم موقعیت در آینده می‌رسند. در آگاهی وضعیتی به صورت تیمی نیاز است تا تیم به یک سطح از آگاهی مشترک وضعیتی برسند. (Simoens, 2021)

فضای سایبری نیز یک مفهوم فردی، ملی و بین‌المللی است که به موجب آن فن‌آوری دیجیتال و کارد آن توصیف می‌شود. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.

اصطلاح اینترنت اشیا نیز به ارتباط بین دستگاه‌های محاسباتی، ماشین‌های مکانیکی و دیجیتال در بستر اینترنت بدون نیاز به دخالت انسان اشاره دارد. در این دستگاه‌ها قطعات هوشمندی برای ایجاد ارتباط با سیستم مرکزی و جمع‌آوری و ارسال داده‌های دریافتی از محیط اطراف تعبیه شده است.

داده‌هایی که حسگرها جمع‌آوری می‌کنند به نوع دستگاه و وظیفه آن بستگی دارد. دستگاه‌ها داده‌های اساسی را برای اجرای یک عمل مشخص، انتخاب می‌کنند تا از آن‌ها برای تصمیم‌گیری کمک بگیرند. برای مثال حسگرهای صدا، داده‌های مربوط به تغییر سطح صدا را جمع‌آوری و به مرکز پردازش داده ارسال می‌کنند تا میزان سر و صدای محیط اندازه گیری شود.

در خصوص کارکردهای اینترنت اشیاء در مراکز فرماندهی و کنترل سایبری و ارتقای سطح آگاهی وضعیتی آنها منابع کمی در دسترس است. معدود منابع موجود در این خصوص از طرف ارتش‌های عضو پیمان نظامی ناتو منتشر شده است. ناتو در این خصوص اسناد چندانی منتشر نکرده است، اما پژوهشگران پژوهش‌هایی را حول این موضوع انجام داده‌اند و در نشریات علمی بین‌المللی تا حدودی نشر پیدا کرده است. پژوهش حاضر با بررسی این منابع و سایر منابعی که می‌تواند به فهم این مسأله کمک کند، به نگارش درآمده است. برخی از منابع در دسترس در این خصوص در فهرست مأخذ اثر حاضر آمده است.

فرماندهی و کنترل جنگ‌های فیزیکی بر پایه مفهوم سلولی در هر سطح از سلسله مراتب فرماندهی عمل می‌کند. برای مثال، در ساختار سلسله مراتب فرماندهی و کنترل پدافند هوایی یک

سلول به نام مرکز عملیات پدافند هوایی وجود دارد که در رأس سلسله مراتب فرماندهی و کنترل است. در زیر مجموعه نیزسلول‌های دیگر قرار دارند که به نام مرکز عملیات پدافند هوایی در نواحی جغرافیایی کشور پراکنده شده‌اند. این سلول‌ها به سلول مادر یعنی مرکز عملیات پدافند هوایی متصل هستند و گزارش‌های خود را به آن ارائه می‌دهند. نوع ارتباط در بستر فیبر نوری یا ارتباطات بی سیم به شکل رمزگذاری شده صورت می‌گیرد. به این شکل یک شبکه یکپارچه تشکیل شده است. اما همین شبکه در برابر اختلالات الکترونیکی، فریب الکترونیکی، قطع کامل ارتباط یا دستکاری در داده جاری در شبکه آسیب‌پذیر است و هر آن ممکن است یکی از حلقه‌های نیروهای عملیاتی این شبکه به دلیل حمله الکترونیکی یا فریب دست به اقدامی بزند که به تصور خود درست است. هر یک از سلول‌ها در یک موقعیت فیزیکی قرار گرفته‌اند و پدافند نیز به صورت توزیعی صورت می‌گیرد. یک عامل پدافند در یک لحظه نمی‌تواند به صورت فیزیکی در تمام نقاط حضور داشته باشد. حال هر یک از سلول‌ها یک بخش از پازل را برای ترسیم تصویر کلی فراهم می‌کنند و در نهایت تصویر کلی در سلول مادر شکل می‌گیرد.(Jani, N., 2020)

اما در مقابل سلول‌های فیزیکی یک مدل سازمانی جنگ سایبری مبتنی بر سلول‌های مجازی یا به عبارتی سلول‌های منطقی ارائه می‌شود. سلول‌های مجازی در فضای سایبری مرکز فرماندهی و کنترل وجود دارند. یک نیروی مهاجم سایبری بر خلاف محیط فیزیکی می‌تواند به طور هم زمان در چند سلول مجازی حضور داشته باشد. همین حضور هم زمان در چند سلول ویژگی قدرتمندی به فرماندهی و کنترل سایبری می‌دهد و دیگر نیازی نیست که همانند فرماندهی و کنترل فیزیکی گزارش به صورت سلسله مراتبی ارائه شود. فرماندهان جنگ سایبری می‌توانند اعضای چند سلول مجازی رده پائین‌تر و هم عرض خود باشند و در صورتی که مجاز دانسته شود، عضو سلول رده بالاتر از خود نیز باشند. (Jurcut, 2019)

در فرماندهی و کنترل فیریکی تنها یک ساختار سازمانی حاکم است که از آن به زنجیره فرماندهی یاد می‌شود. گزارش‌دهی در این ساختار در سلسله مراتب فرماندهی صورت می‌گیرد و نوع رابطه بر اساس "بسیار با یکی"[1] است. همان طور که پیش از این اشاره شد در ساختار فرماندهی و کنترل پدافند هوایی بسیاری از مراکز عملیات منطقه‌ای و مراکز کنترل و گزارش با

1 Many to One Relationship

یک مرکز عملیات پدافند هوایی در ارتباط هستند. اما سلول‌های مجازی بر اساس رابطه عضویت سازماندهی می‌شوند و نوع رابطه بر اساس "بسیاری با بسیاری"[1] است. عملیات در ساختار متمرکز فرماندهی و کنترل به صورت شبکه محور اجرا می‌شود و هر یک از سلول‌ها به سلول مرکز عملیات منطقه‌ای گزارش می‌دهد، با این تفاوت که در صورت انهدام مرکز عملیات سایر سلول‌ها دچار از هم گسیختگی شده و وحدت تلاش خود را از دست می‌دهند. اما در مدل "بسیاری با بسیاری" تنها هنگامی کارایی رزمی سلول‌ها از دست می‌رود که کل آنها مورد هدف قرار گیرند و انهدام یک یا چند مورد از آنها بی فایده است. بنابراین، در مدل "بسیاری با بسیاری" ضریب تاب آوری بیشتر خواهد بود. در نتیجه، یک ساختار سازمانی برای جنگ سایبری که روابط زنجیره فرماندهی در آن نهفته است، وجود دارد. (Finn, 2017)

با این توصیف ساختار سازمانی جنگ سایبری با ساختار سازمانی جنگ فیزیکی ادغام می‌شود تا زنجیره فرماندهی متعارف برای مقاصد فرماندهی حفظ شود و ویژگی‌های لازم برای اجرای عملیات سایبری نیز ایجاد شود.

اما کاربرد فرماندهی و کنترل فراتر از ایجاد ارتباط در زنجیره فرماندهی است. برای مثال، از کارکردهای سامانه‌های فرماندهی و کنترل برای تدوین راهبرد، اجرای تاکتیک، ایجاد تصویر مشترک، ارائه راه کار و حفظ جریان اطلاعاتی استفاده می‌شود. (Simoens, 2021)

در جنگ سنتی فیزیکی مرسوم است که حرکات، تاکتیک‌ها و تسلیحات دشمنان بالقوه با هدف تدوین راهبردها و تاکتیک‌های آنها پیش از آغاز جنگ بررسی شود. این راهبردها شامل درک هنر عملیاتی از جمله سازماندهی برای جنگ، شیوه‌های برقراری ارتباطات در درون سازمان، رویدادهای احتمالی در جنگ آینده، راه کارهای مطلوب برای مقابله با رویدادها، نحوه دریافت اطلاعات رزمی و کسب آگاهی وضعیتی و امثال آن می‌شود. هر عنصر راهبردی جنگ سنتی دارای یک عامل موازی در جنگ سایبری است.

کارشناسان پدافند سایبری استفاده چندانی از راهبردها و تاکتیک‌های نظامی نمی‌برند. فرماندهان نظامی می‌دانند که زمان‌هایی پیش می‌آید که بهترین راهبرد پدافندی آفند است. آنها به ارزش تاکتیک‌های فریب و مانور آگاه هستند. این واقعیت که راهبرد پدافند در عمق از عملیات

1 Many to Many Relationship

آفندی یا مانور و فریب استفاده نمی‌کند، موجب می‌شود که مدافع همانند مهاجم در عملیات خود مؤثر واقع نشود. راهبردهای پدافند سایبری جاری بیشتر استاتیک هستند و تاکتیک‌های آنها جنبه واکنشی دارند. هدف راهبرد پدافند در عمق ایجاد لایه‌های متعدد پدافندی به این امید است که شکست حملات دست کم در یکی از لایه‌ها رخ دهد. هنگامی که این راهبرد با شکست مواجه شود، اقدامات واکنشی آغاز می‌شود و مکان حمله و کشف رخنه مد نظر قرار می‌گیرد و وصله‌های امنیتی برای توقف حملات و رخنه‌های آتی مورد استفاده قرار می‌گیرد و سامانه به وضعیت اولیه برگردانده می‌شود. (Beni, 2020)

اکثر حملات در دنیای امروز از یک نوع هستند. برای مثال، یک بدافزار که به پیوست یک ایمیل ارسال می‌شود یا حمله منع خدمات که علیه یک نوع خاص از سرور با آسیب پذیری معین صورت می‌گیرد. در اکثر موارد این حملات هماهنگ نبوده و با یک راهبرد مشخص آسیب و خسارات معینی را به سامانه‌های متعدد در شبکه وارد می‌کند. در زمان جنگ این احتمال مطرح است که حملاتی از طرف بازیگران دولتی به صورت هماهنگ به چندین هدف با استفاده از انواع حملات صورت گیرد. این حملات متعدد با هدف عبور از لایه‌های چندگانه پدافند در عمق به صورت همزمان انجام می‌شود و پس از آن حملات گسترده اصلی آغاز می‌شوند که موجب وارد آوردن خسارات عمده به شبکه شده و احیای خدمات در بستر شبکه شاید مستلزم صرف روزها یا ماه‌ها زمان باشد. این حملات در طبقه‌بندی حملات فاجعه آمیز قرار می‌گیرد. حال سامانه فرماندهی و کنترل پیشنهادی باید به شکلی معماری شود که قادر به پاسخگویی به چنین حملاتی به صورت سریع و هماهنگ در یک مکانیزم پدافندی پویا باشد و ضمن فریب مهاجم بتواند راه کارهای از پیش تعیین شده را بر مبنای نظارت بر حملات واقعی و اجرای حملات پیچیده به طور همزمان ارائه دهد. (Jurcut, 2019)

بنابراین، سامانه فرماندهی و کنترل باید پویا بوده و امکان خلق و بکارگیری راهبردهایی را که از تاکتیک پشتیبانی می‌کند، بدهد. راهبردها و تاکتیک‌های جنگ فیزیکی هم پویا و هم قابل پیش بینی هستند. این ویژگی‌ها قابل استفاده در فرماندهی و کنترل سایبری هستند. برای مثال، در جنگ فیزیکی از تاکتیک مانور و فریب استفاده می‌شود و از تاکتیک و عملیات آفندی و پدافندی استفاده به عمل می‌آید. حال برای اتخاذ چنین تاکتیکی در فضای سایبری باید از منابع سایبری

متنوع و توانایی هماهنگی منابع به منظور مانور در برابر دشمن برخوردار بود و آن را فریب داد. (Finn, 2017)

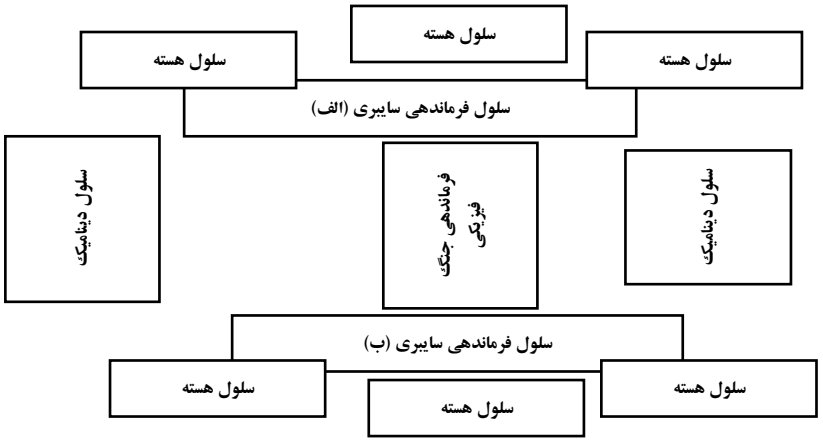
مدل عملیاتی فرماندهی و کنترل سایبری

در این مدل تصاویر دایره، بیضی و غیره معرف سلول هستند. هنگامی که دو سلول با یکدیگر برخورد می‌کنند، نشاندهنده آن است که حداقل یک عضو را به اشتراک دارند. به این معنی که یک سرباز سایبری در هر دو سلول به طور همزمان حضور دارد. در نظریه مجموعه‌ها در ریاضیات مجموعه را بر اساس روابط آن تعریف می‌کنند. به این معنی که مجموعه بر اساس این که چه عنصری عضو مجموعه است، تعریف می‌شود. یک سلول مجازی به عنوان مجموعه‌ای از اعضای سلول است.

برخلاف نظریه مجموعه‌ها سلول‌های مجازی همواره از اعضای یکسانی برخوردار نیستند. اعضای سلول‌ها تغییر می‌کنند. برای مثال، سلول‌های مجازی برای مدت ۲۴ ساعت در روز فعالیت می‌کنند و در طول روز چندین بار احتمال تغییر آنها است. با تغییر شیفت کاری کلیه اعضاء نیز تغییر می‌کنند. این سلول‌های مجازی بنا به مأموریت ممکن است تشکیل شوند و بعد از اتمام آن دیگر وجود نداشته باشند. سلول‌های هسته همواره در فرماندهی و کنترل سایبری حضور دارند، اما سلول‌های دینامیک بنا به موارد اقتضایی تشکیل می‌شوند. هر سلول هسته دارای یک فرمانده سلول است. سامانه‌های فرماندهی و کنترل سایبری باید در ۲۴ ساعت روز عملیاتی باشند و به همین دلیل باید از فرماندهان سایبری به صورت شیفت سایبری استفاده شود. حال فرمانده سلول در جنگ فیزیکی می‌تواند فرمانده صحنه باشد. فرمانده این اختیار را دارد که مسئولیت فرماندهی را به یک افسر ارشد تفویض کند. فرمانده صحنه عملیات فیزیکی بر اینترفیس سامانه فرماندهی و کنترل جنگ سایبری با سامانه فرماندهی و کنترل جنگ فیزیکی نظارت می‌کند. (Parunak, F., 2021)

حال در شرایطی که فرمانده صحنه عملیات فیزیکی بر عملیات نظارت دارد، فرماندهی و کنترل واقعی جنگ سایبری بر عهده فرماندهان جنگ سایبری منطقه‌ای است. هر فرمانده صحنه جنگ سایبری بر یک سلول منطقه‌ای فرماندهی می‌کند. در شکل شماره ۱ دو منطقه الف و ب نشان داده شده است. در عمل هر تعدادی از این مناطق را می‌توان ایجاد کرد و این بستگی به تعداد مناطق در فرماندهی و کنترل جنگ فیزیکی دارد. تطابق تعداد مناطق سایبری با فیزیکی به علت لزوم

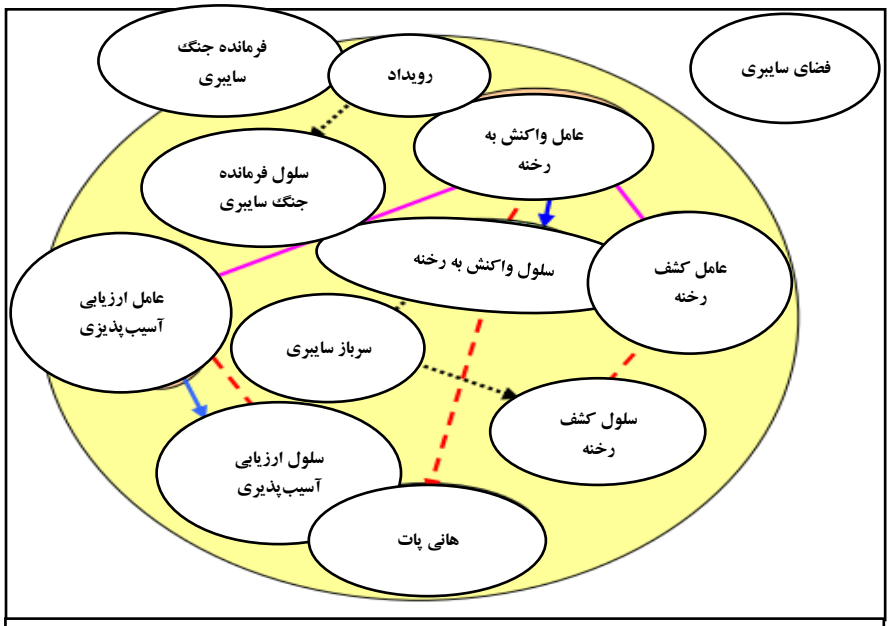
پشتیبانی فرماندهی و کنترل سایبری از مناطق فیزیکی است. آنچه که یک منطقه را شکل می‌دهد، بستگی به عواملی مانند سطح سامانه فرماندهی و کنترل (تاکتیکی، عملیاتی و ...)، ابعاد صحنه و توپولوژی شبکه فرماندهی و کنترل دارد. (پاروناک، ۲۰۰۳: ۱۲) با تقاطع سلول فرماندهی و کنترل جنگ فیزیکی و سلول فرماندهی و کنترل جنگ سایبری می‌توان به این نتیجه دست یافت که یکی از اعضای فرماندهی و کنترل جنگ فیزیکی عضو فرماندهی و کنترل جنگ سایبری است. در سامانه‌های فرماندهی و کنترل توزیع یافته یک فرمانده جنگ فیزیکی قادر به نظارت بر تمام سلول‌های منطقه‌ای نخواهد بود. یک قاعده کلی برای تمام سلول‌ها عبارت است از این که یک فرمانده سلول در هر سطحی کسی را کنترل می‌کند که عضوی از سلول است. حال این فرض در نظر گرفته می‌شود که فرمانده جنگ فیزیکی به تمام فرماندهان جنگ سایبری اجازه عضویت در سلول جنگ فیزیکی را می‌دهد. هر چند در مواردی ممکن است این فرض نقض شود.



شکل ۱. مدل فرماندهی و کنترل سایبری

هر فرمانده جنگ سایبری مورد حمایت سایر سلول‌ها قرار دارد. برخی از آنها در شکل ۲ شامل سلول‌های کشف رخنه، سلول‌های پاسخ به رخنه و سلول‌های ارزیابی آسیب پذیری می‌شود. سلول دیگر مربوط به سلول بستر تست است که برای تست ایده‌ها یا نرم‌افزارهای جدید بکار می‌رود. سلول‌های دیگر نقش سلول دینامیک پ و ت را دارند. سلول‌های دینامیک در صورت نیاز به پشتیبانی از وظایف فرماندهی و کنترل یا عملیات ایجاد می‌شوند. هر فرمانده سلول می‌تواند

ایجاد سلول جدید را مورد تأیید قرار دهد. همان فردی که مسئولیت ایجاد یک سلول جدید را بر عهده دارد، مسئولیت تعیین فرمانده سلول جدید را نیز به دوش می‌کشد. (Munoz, MF., 2020)



شکل ۲. مدل عملیاتی سیستم فرماندهی و کنترل جنگ سایبری

مدل عملیاتی که در تصویر زیر آمده است، یک مدل فرماندهی و کنترل جنگ سایبری است. حال به شرح راهبرد دینامیک و تاکتیک‌های پیش بینی کننده این مدل پرداخته می‌شود. برخی از وظایف عملیاتی این مدل به شرح زیر است:

- تحلیل اطلاعات سایبری. برای مثال: تحلیل اطلاعات رویدادهای مرتبط با رخنه و ردپای حملات، تطابق رویدادهای رخنه، تأیید حمله، وضعیت فرماندهی و کنترل شبکه و هشدارباش سایبری به سایر سازمان‌ها.
- مدیریت عملیات سایبری. برای مثال: حفظ یک تصویر علمیات سایبری، نمایش ترتیب نیروی سایبری و نمایش وضعیت حملات و ارائه راه کار برای پاسخ به حمله.
- کنترل عملیات سایبری. برای مثال: نظارت بر حملات و راه کارها، اعزام عوامل سیار، جابجایی کارکردهای حیاتی و کشاندن مهاجم به هانی پات‌ها.

شکل ۲ برخی از کارکردهای سلول‌های شکل ۱ را نشان می‌دهد. در رأس تصویر، فرمانده جنگ سایبری دیده می‌شود که به سلول فرماندهی جنگ سایبری ملحق شده است. در میانه تصویر سلول واکنش به رخنه، ارزیابی آسیب پذیری و سلول کشف رخنه آمده است که فرمانده جنگ سایبری را پشتیبانی می‌کنند. سلول ارزیابی آسیب پذیری عامل گشت سیار را برای کشف آسیب پذیری‌ها مانند مودم‌ها یا پلتفرم‌های غیر مجاز اعزام می‌کند.

یکی از عوامل پیامی را به سلول بررسی آسیب پذیری ارسال می نماید. خطوط فلش خط چین نشان دهنده اعزام عامل سیار است. خطوط فلش غیر خط چین نشاندهنده آن است که پیام‌های عامل سیار به یکی از سلول‌های مجازی ارسال شده است. شکل بیضی که برچسب ندارد، نشان دهنده پلتفرم های داخل شبکه فرماندهی و کنترل به عنوان محل حضور عوامل سیار است. در تصویر مشاهده می شود که سلول واکنش به رخنه یک عامل سیار را در واکنش به برخی از رویدادهای رخنه اعزام کرده است و این عامل اطلاعات حاصل را با سلول واکنش به رخنه و سایر سلول‌ها در میان می‌گذارد. سلول سیار واکنش به رخنه فرآیند جاری در پلتفرم را به ظن خصمانه بودن آن متوقف می‌کند. (Simoens, 2021)

یک الگوریتم تصادفی با تضمین پوشش یکپارچه تجهیزات فرماندهی و کنترل اعزام عوامل گشتی را کنترل می‌نماید. ویژگی تصادفی بودن الگوریتم متضمن آن است که هم رخنه کننده و هم کاربر مشروع اطلاعی از زمان و مکان (گره) حضور عامل اعزامی ندارند. در نتیجه، رخنه کننده به سختی می‌تواند از لایه‌های امنیتی عبور کند و کاربر مشروع نیز نمی‌تواند سیاست‌های امنیتی را نقض نماید. دشمنان نیز در این شرایط قادر به آماده سازی اطلاعاتی میدان نبرد در فضای سایبری فرماندهی و کنترل نخواهند بود، چرا که سلول‌های سیار و عوامل سیار تصویر متفاوتی از سازمان منطقی و فیزیکی سیستم‌های فرماندهی و کنترل در مقابل رقیب قرار می‌دهند. (U.S. Department of Defense, 2019)

شناسایی حملات و کشف رخنه

سلول کشف رخنه اطلاعات رخنه در شبکه میزبان را از انواع منابع دریافت می‌کند. ابتدا اطلاعات رخنه را از اسکنرها، سیستم های کشف رخنه میزبان پایه و عوامل گشتی در سیستم فرماندهی و کنترل می‌گیرد. اطلاعات رویداد از دیوار آتش موجود در سامانه فرماندهی و کنترل

بدست می‌آید. علاوه بر این، اطلاعات مربوط به هشدار و سایر اطلاعات در خصوص حملات از سایر سازمان‌ها دریافت می‌شود. تمام اطلاعات موجود با یکدیگر تقاطع داده می‌شود تا احتمال وقوع حمله مشخص شود. در تقاطع اطلاعاتی نقش انسان در چرخه بیشتر می‌شود.

اطلاعات پس از تقاطع گیری به سلول واکنش به رخنه ارسال می‌شود تا نوع اقدام ضروری مشخص شود. در مدل عملیاتی تقاطع اطلاعات رویداد بدون آن که اطلاعات در دیتا بیس مشترک تجمیع شود، تقاطع گیری می‌شود. اما در سامانه‌های فرماندهی و کنترل جنگ فیزیکی همانند اطلاعات حاصل از ردگیری یک هدف (برای مثال هدف هوایی در فرماندهی و کنترل پدافند هوایی) ابتدا اطلاعات مراکز عملیات پدافند هوایی در یک دیتابیس مشترک که همان مرکز عملیات پدافند هوایی است، تجمیع می‌شود. در مدل عملیاتی در زمان صرفه جویی می‌شود و واکنش در زمان کوتاه‌تری صورت می‌گیرد. در فرماندهی و کنترل سایبری صرفه‌جویی در زمان عامل مهمی در واکنش به موقع به تهدیدها است.

واکنش به رخنه و ضد حمله

سلول واکنش به رخنه عملکرد چندگانه دارد. واکنش به رخنه دارای حیطه عملکردی گسترده‌ای است که شامل واکنش فوری به منظور مهار حمله، واکنش کمتر فوری به منظور توقف حملات و اطلاع رسانی به فرمانده جنگ سایبری در صورت وقوع رویداد، ضد حمله، مشاوره در خصوص راه کارها به فرمانده جنگ سایبری و فرمانده جنگ فیزیکی و برآورد خسارات حملات می‌شود. اعضای سلول واکنش در تدوین راهبرد و تاکتیک و راه کارها نقش دارند.

سلول واکنش به رخنه عوامل سیار را برای از بین بردن فرآیندهای منتخب، پیکربندی دیوار آتش و در صورت لزوم رفع یا محدودسازی کاربران مشکوک اعزام می‌کند. حملات آفندی یا عوامل پنهانی در راستای تدابیر عملیاتی فرماندهی و کنترل سایبری در واکنش به تهدیدهای سایبری گسترش پیدا می‌کنند. عوامل سیار در خارج از محدوده شبکه عمل نمی‌کنند. (Beni, 2020)

سناریوهای برگرفته از رزمایش‌های واقعی در دنیا

در ادامه به معرفی و طرح چند سناریوی واقعی برگرفته از رزمایش‌های واقعی در دنیا با تکیه بر فن‌آوری سایبری در فرماندهی و کنترل به منظور به تصور کشیدن کارکرد و اهمیت فضای سایبری در ارتقای سطح آگاهی وضعیتی پرداخته می‌شود. (Bonabeau, 2018)

سناریوی پست ایست و بازرسی: در این سناریو نقاط ایست و بازرسی در خارج از منطقه امنیتی در نظر گرفته می‌شود. منطقه امنیتی مانند پایگاه نظامی است. در این سناریو از سخت افزارهای نظامی بهره گرفته می‌شود. در نقاط ایست و بازرسی چندین حسگر اینترنت اشیاء نصب شده است. این حسگرها به طور خودکار می‌توانند خودروهای در حال نزدیک شوندگی به مقر ایست و بازرسی را شناسایی کرده و حتی نوع خودرو، نوع موتور آن، وزن و رنگ خودرو و هویت سرنشینان آن را مشخص نمایند. شناسایی هویت سرنشینان خودرو از طریق تشخیص چهره و صدا انجام می‌شود. در صورتی که خودرو از نظر مشخصات آن و سرنشینان از نظر هویت و سطح دسترسی مجاز تشخیص داده شود، اجازه ورود به محدوده مقر به آن داده می‌شود. در صورتی که خودرو مجاز دانسته نشود و توقف نیز نکند، یک پهپاد بلافاصله به سمت آن می‌رود و اطلاعات این حادثه را از طریق پروتکل رادیویی برد بلند به مرکز فرماندهی و کنترل ارسال می‌کند.

سناریوی کمک‌های بشردوستانه و امداد و نجات: در این سناریو یک شهر هوشمند در معرض بلایای طبیعی مانند زمین لرزه، طوفان یا سیل قرار گرفته است. این سناریو در مدیریت بحران در رزمایش دور میزی مورد استفاده قرار گرفته است. در این سناریو از نیروهای نظامی درخواست می‌شود تا به دولت محلی در امدادرسانی اضطراری مانند آواربرداری یا امداد پزشکی کمک کنند. در این حالت هدف فرماندهان افزایش منابع اطلاعاتی خود به منظور ارتقای سطح اشراف اطلاعاتی، دریافت خدمات آمادی در زمان حقیقی برای بهبود برنامه‌ریزی، نظارت بر بهداشت عمومی منطقه و تقویت اطلاعات نیروها از طریق دریافت و پردازش اطلاعات است. نیروهای نظامی از اطلاعات سامانه‌های باقی مانده شهر هوشمند برای تقویت خوراک اطلاعاتی خود بهره می‌برند. زیرساخت‌های شهر هوشمند شامل حسگرها و تجهیزات ارتباطی از جمله دوربین‌های شهری، حسگرهای سنجش آلودگی و شرایط جوی، شبکه حمل و نقل هوشمند و شبکه هوشمند برق می‌شود. نیروهای نظامی با استقرار حسگرهای خود در نقاط حساس به تقویت منابع اطلاعاتی کمک می‌کنند. حال اطلاعات حاصل از حسگرهای شهر هوشمند و اطلاعات حسگرهای نظامی به صورت مشترک برای ایجاد آگاهی وضعیتی مشترک قابل استفاده نظامیان و مقامات محلی است. برخی از حسگرهای نظامی شامل حسگرهای حرکتی، حسگرهای انتشار گاز، حسگرهای فرکانس رادیویی، حسگرهای کیفیت هوا و حسگرهای دوربینی کشف و شناسایی اشیاء می‌شود. (Brambilla, 2019)

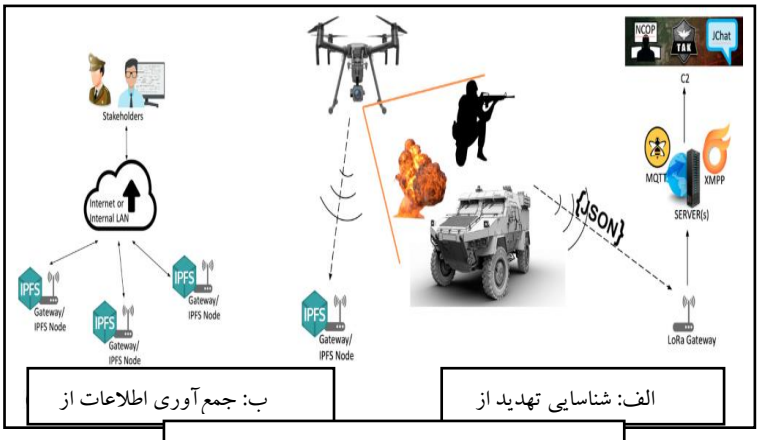
سناریوی پایگاه هوشمند: سناریوی پایگاه هوشمند یکی از سناریوهایی است که به موجب آن فن‌آوری اینترنت اشیاء می‌تواند ارزش افزوده قابل توجه‌ای ایجاد کند. پایگاه هوشمند دارای ویژگی‌های مشابه بسیاری با شهر هوشمند است. برای مثال، نظارت بر جریان برق، کشف نواقص کارکردی تجهیزات، فعال سازی نگهداری پیشگیرانه، نظارت بر آماد و مدیریت تجدید تدارکات برخی از موارد مشابه کارکردهای شهر و پایگاه هوشمند است.

سناریوی شبکه توزیع شده سربازان متصل به یکدیگر: در این سناریو یگان‌های مختلفی از سربازان با مأموریت مشخص مانند گشت رزمی در نظر گرفته می‌شود. برای بهبود سطح آگاهی وضعیتی در خصوص شرایط بهداشتی سربازان علائم حیاتی آنها به طور مستمر تحت نظارت قرار می‌گیرد. این علائم در حفظ سطح هوشیاری سربازان و کاهش احتمال بروز سوانح ایمنی و تأمینی حائز اهمیت است. حسگرهای پوشیدنی مانند حسگرهای کاردیوگرافی یا اکسیژن سنج خون اطلاعات حاصل از علائم حیاتی بدن را جمع‌آوری کرده و این اطلاعات را به فرستنده اطلاعات برای ارسال به مرکز دریافت اطلاعات سربازان می‌فرستند. حسگرها از طریق ارتباطات بلوتوث به گوشی هوشمند سرباز متصل هستند. اطلاعات در گوشی به عنوان بانک داده جمع‌آوری می‌شود. اطلاعات دیگر مانند اطلاعات حاصل از موقعیت جغرافیایی سرباز نیز در این بانک داده ذخیره می‌شود. راه دوم ارسال اطلاعات استفاده از یک گره ارتباطی است که اطلاعات را به گره امن دیگری برای به اشتراک گذاری در اطلاعات حاصل از هر سرباز یا یگان به یک گره "گیت وی" امن ارسال می‌شود تا اطلاعات در کل شبکه قابل دسترسی باشد. علاوه بر این، در معماری ساختار ذخیره سازی اطلاعات به شکلی کار شده است که افزونگی به عنوان یک اقدام پدافند غیرعامل در آن رعایت شده باشد. (Alam, 2021) اطلاعاتی که به این شکل بدست می‌آید، قابل استفاده و اشتراک گذاری برای سایر یگان‌های هم عرض، مافوق یا زیرامر است. هم اکنون، ارتش‌های عضو ناتو از تصویر عملیاتی مشترک در مجموعه نیروهای مسلح زیرپوشش فرماندهی آن استفاده می‌کنند. یکی از مزایای غیرقابل انکار تصویرسازی مشترک در مجموعه عملیاتی نیروهای مسلح افزایش ضریب تاب آوری نیروها است. کاهش حداکثری نقطه شکست[1]، احتمال غافلگیری و مواردی از این دست از مزایای دیگر شبکه‌سازی است. هنگامی که نیروها در پوشش یک شبکه

1 Point of Failure

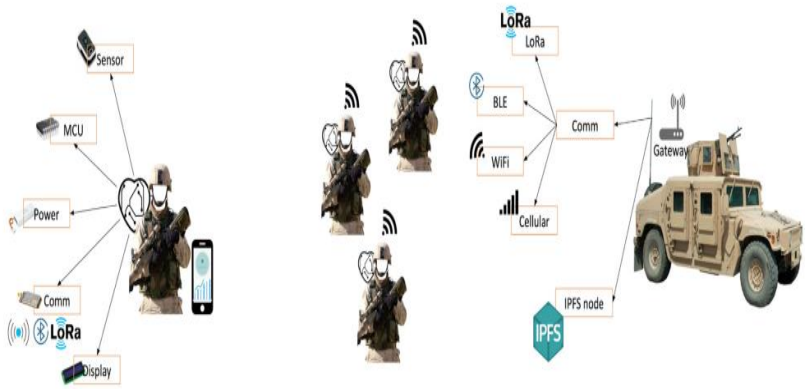
عمل می‌کنند، سطح آگاهی وضعیتی آنها افزایش پیدا می‌کند و به یک یادگیری جمعی می‌رسند. حال مجموعه کاملی از اطلاعات سربازان شامل وضعیت علائم حیاتی بدن آنها مانند سطح استرس، کوفتگی و عدم هوشیاری ذهنی و امثال آن که در عملکرد آنها تأثیر مستقیم دارد، قابل بررسی و در دسترس است. (Brambilla, 2021)

شناسایی تهدید: این سناریو در ادامه سناریوی شبکه توزیع شده سربازان متصل به یکدیگر قرار دارد. حال در نظر بگیرید که یگانی در حین گشت متوجه صدای انفجار در مجاورت موقعیت خود یا آتش دشمن به سمت یگان‌های خودی می‌شود. از چندین سامانه برای اشراف اطلاعاتی و آگاهی وضعیتی استفاده به عمل می‌آید. برای مثال، از یک پهپاد مانند پهپادهای مجهز به حسگر حرارتی برای شروع عملیات شناسایی در محیط پیرامون استفاده می‌شود. تصاویر حاصل از این شناسایی با استفاده از تجهیزات مکمل که در آزمایشگاه‌ها است، قابل بررسی و تحلیل خواهد بود. از بانک اطلاعات موجود برای شناسایی بر اساس چهره نیز می‌توان در پهپادها استفاده کرد. حال پهپادی که در حال گشت زنی است می‌تواند تهدید را کشف کرده و اطلاعات آن را به نزدیک‌ترین گره ارتباطی برای ذخیره سازی ارسال کند یا اطلاعات را با استفاده از نرم‌افزارهای مرتبط به گوشی‌های هوشمند سربازان ارسال نماید.



الف: شناسایی تهدید از ب: جمع‌آوری اطلاعات از

تصویر۴: اطلاعات عملیاتی اینترنت اشیاء برای



الف: یگان‌ها و سربازان متصل به

ب: سربازان متصل به

شکل ۳: اطلاعات عملیاتی اینترنت اشیاء برای فرماندهی و کنترل

مهم‌ترین مزیت این سناریو حفظ جان سربازان است. (DeLoach, 2020)

ردیابی مجروحین: این سناریو شامل ردیابی سربازان مجروح می‌شود. در این سناریو تمام سربازان دارای برچسب شناسایی فرکانس رادیویی هستند. هر برچسب فرکانس رادیویی معرف یک سرباز است. علاوه بر این، تجهیزات همراه سربازان نیز مجهز به ردیاب تعیین موقعیت جغرافیایی هستند که در وقفه‌های زمانی موقعیت آنها را به مرکز ارسال می‌کند. سربازان پس از تشخیص نیاز به خدمات درمانی به مرکز درمانی مشخص اعزام می‌شوند و سوابق سلامتی آنها ثبت می‌شود. علاوه بر این، میزان مراجعه مجروحین به یک مرکز درمانی مشخص قابل سنجش خواهد بود و این که چه خدماتی آنها دریافت می‌کنند و چه نتایجی در پی داشته است، در بانک اطلاعاتی ثبت می‌شود. این بررسی‌ها می‌تواند به تحلیل‌گران و فرماندهان رزمی کمک کند تا نسبت به تشخیص بیشترین آسیب‌ها در نقاط مختلف منطقه نبرد اطلاع پیدا کنند و ضمن بررسی علت آن تحلیل بهتری از اطلاعات رزمی داشته و طرح‌ریزی عملیات را اصلاح کنند. (Bachrach, 2019),

سامانه فرماندهی و کنترل: چندین سامانه فرماندهی و کنترل عملیاتی شناسایی شده است که قادر به تصویرسازی و پردازش اطلاعات حاصل از اینترنت اشیاء است. برای مثال، در ارتش کشورهای عضو ناتو سامانه هماهنگی و اطلاعات پزشکی دارای ۱۲ ماژول است که ابزارهای

مختلفی را در طرح‌ریزی کمک‌های پزشکی، مدیریت بهداری، پشتیبانی کلینیکی، نظارت بر وضعیت سلامت و اطلاعات پزشکی دارد. این سامانه داده‌های مورد نیاز را برای ایجاد تصویر مشترک عملیاتی با تبادل اطلاعات به صورت خودکار در میان ارتش‌های عضو ناتو انجام می‌دهد. این اقدام با استفاده از یک برچسب هوشمند به عنوان فن‌آوری اینترنت اشیاء بر روی بیمار به جای استفاده از بارکد یا برچسب شناسایی فرکانس رادیویی انجام می‌شود.

در تمام این سامانه‌ها تلاش می‌شود تا دایره اطلاعاتی با استفاده از منابع متعدد گسترش پیدا کند. اطلاعات عملیاتی، آمادی، رزم در هوا، زمین و دریا و غیره از جمله اطلاعاتی است که در سامانه فرماندهی و کنترل مورد توجه قرار می‌گیرد. اطلاعاتی که از منابع متعدد به دست می‌آید در یک تصویر بزرگ مد نظر قرار می‌گیرد تا امکان اخذ تصمیم در زمان و مکان صحیح فراهم آید.

پیشینه پژوهش

در پیشینه پژوهش به پژوهش‌هایی اشاره می‌شود که در قالب مقالات در حوزه موضوع پژوهش حاضر مطرح است. از جمله این موارد مقاله‌ای با عنوان "آگاهی وضعیتی در دفاع سایبری فعال، راهبردی به منظور مقابله با حملات پیشرفته امروزی" است. این مقاله به قلم حامد رادی نیا و علی جباررشیدی در سال ۱۴۰۱ در کنفرانس ملی فن‌آوری‌های نوین در مهندسی برق و کامپیوتر ارائه شده است. در این مقاله نقش آگاهی وضعیتی در بهبود دفاع سایبری فعال مورد بررسی قرار گرفته است و برای خواننده مشخص شده است که در صورت وجود آگاهی وضعیتی در سطح قابل قبول امکان دفاع بهتری در فضای سایبری در برابر تهدیدهای مترتب به وجود خواهد آمد. مطالعه این مقاله به نگارنده در نگارش ادبیات آگاهی وضعیتی کمک شایانی کرد. پرداختن به آگاهی وضعیتی در این مقاله وجه مشترک با پژوهش حاضر را تشکیل می‌دهد و وجه افتراق آن را باید در تمرکز پژوهش حاضر بر حوزه فرماندهی و کنترل دانست. به عبارتی، پژوهش حاضر به دنبال وام گرفتن از ادبیات فضای سایبری در راستای ارتقای سطح آگاهی وضعیتی حوزه فرماندهی و کنترل است.

عنوان مقاله دوم "ارائه یک معماری جدید برای تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا در فرماندهی و کنترل سایبری" است. این مقاله به قلم نویسندگان داداش

تباراحمدی کوروش و جباررشیدی علی و براری مرتضی در سال ۱۳۹۳ در نشریه پدافند الکترونیک و سایبری دوره دوم شماره چهارم منتشر شده است. مقاله فوق متمرکز معماری جدیدی برای تجسم آثار حملات سایبری است و در این خصوص به دنبال ادغام اطلاعات در فرماندهی و کنترل است. مطالعه این مقاله تا حدودی موجب برخورداری نگارنده از یک نگرش مطلوب در خصوص مراکز فرماندهی و کنترل شد. نقطه اشتراک مقاله فوق با مقاله نگارنده در وجود ادبیات سایبری است و نقطه افتراق در پرداختن مقاله نگارنده به مراکز فرماندهی و کنترل فیزیکی در مقابل مراکز فرماندهی و کنترل سایبری است که هدف مقاله فوق است.

مقاله سوم با عنوان "مدل سازی و شبیه سازی صحنه نبرد سایبری" در سال ۱۳۹۶در نشریه مدیریت فن‌آوری اطلاعات دوره دوم شماره چهارم منتشر شده است. مقاله فوق حاوی اطلاعاتی در خصوص صحنه نبرد سایبری است و مطالعه آن به بسط دانش نویسنده پژوهش حاضر در ترسیم فضای سایبری کمک نمود. وجه اشتراک این مقاله با مقاله نگارنده در استفاده از مفاهیم فضای سایبری است و وجه افتراق آن در پرداختن مقاله نگارنده به آگاهی وضعیتی و ارتقای آن در مراکز فرماندهی و کنترل است و این در حالی است که مقاله فوق تنها مختص شبیه سازی صحنه نبرد سایبری است.

مقاله چهارم با عنوان " تجسم حملات سایبری با تخمین خسارت و ترکیب قابلیت و فرصت مهاجم بر اساس مدل انتقال باور" در سال ۱۳۹۷ در نشریه پدافند الکترونیک و سایبری در دوره ششم شماره چهارم منتشر شده است. این مقاله همانند مقاله پیشین به بسط دانش نویسنده پژوهش حاضر در خصوص مفاهیم فضای سایبری کمک شایانی نمود. وجه اشتراک این مقاله با مقاله نگارنده پژوهش حاضر در مفاهیم سایبری است و وجه افتراق در آگاهی وضعیتی و مراکز فرماندهی و کنترل است که در مقاله فوق به آنها پرداخته نشده است و در پژوهش حاضر به آنها پرداخته شده است.

روش‌شناسی پژوهش

روش پژوهش در این مقاله توصیفی – تحلیلی از نوع کاربردی است. تلاش شده است علاوه بر تصویرسازی آنچه هست به تشریح و تبیین دلایل چگونه بودن و چرایی وضعیت مسئله و ابعاد

آن پرداخته شود. تکیه‌گاه استدلالی بحث از طریق جستجو در ادبیات و مباحث نظری تحقیق و تدوین گزاره‌ها و قضایای کلی موجود فراهم شده است. جزئیات مربوط به مسئله تحقیق با گزاره-های کلی مربوطه ارتباط داده شده و به نتیجه‌گیری ختم شده است. راهبرد جمع آوری داده‌ها در پژوهش حاضر متکی بر مطالعات اسنادی، فیش برداری و ایجاد ارتباط منطقی میان داده با استفاده از قیاس عقلی بوده است. پس از جمع‌آوری داده‌ها و بهره‌گیری از اسناد متنوع علمی برای تحقق یک نتیجه گیری مناسب اقدام به تحلیل داده‌ها و سپس استنباط و تفسیر داده‌ها شده است.

سؤال پژوهش

نقش ظرفیت فضای سایبری در ارتقای سطح آگاهی وضعیتی مراکز فرماندهی و کنترل چیست؟

داده پردازی و یافته‌های پژوهش

فرماندهی و کنترل بر مبنای ۵ متغیر چه کسی، چه چیزی، چه زمانی، کجا و چگونه عمل می‌کند. در پژوهش حاضر به متغیر چگونگی اعمال فرماندهی و کنترل پرداخته می‌شود. قلمرو سایبری قلمرو پنجم جنگ‌ها محسوب می‌شود. اعمال فرماندهی و کنترل بدون وجود آگاهی وضعیتی غیر ممکن است و در دنیایی که فن‌آوری‌های ارتباطی و اطلاعاتی گسترش قابل توجه‌ای پیدا کرده است و فضای سایبری بر تمام محیط‌های سنتی مانند عملیات در زمین، دریا، هوا و فضا مسلط شده است، نقش این فضا در افزایش آگاهی وضعیتی غیر قابل چشم پوشی است. این نقش به دلیل ویژگی‌های این فضا است که برخی از آنها عبارتند از کاهش هزینه‌های اجرای مأموریت، بی نیازی به تجهیزات و ادوات پر هزینه نظامی، گمنامی نفرات، اجرای مأموریت از هر نقطه از کره زمین، سرعت غافلگیری، نبودن شواهد و قرائن عملیات پیش از اجرا و موارد مشابه. آگاهی وضعیتی در ۳ مرحله اطلاع از وضعیت خودی، شرایط محیطی و جغرافیایی و وضعیت نیروهای دشمن قابل اجرا و بهره برداری است. فضای سایبری به دلیل توسعه روزافزون این ظرفیت را دارد تا در هر ۳ مرحله سطح آگاهی وضعیتی را در نیروهای خودی به موجب انتقال اطلاعات به مراکز فرماندهی و کنترل بالا ببرد. از طرف دیگر، توسعه اینترنت اشیاء و توسعه شهرهای هوشمند و حتی پایگاه‌های نظامی هوشمند شرایطی را به وجود آورده است تا به موجب آن امکان بهره‌برداری

بیشتر از فضای سایبری برای ارتقای سطح آگاهی وضعیتی فراهم شود. زمان در فضای سایبری به سمت صفر (به دلیل ماهیت پویا و وقوع تهدیدها در کسری از ثانیه در این فضا) و مکان به سمت لامکان (به دلیل مطرح نبودن محدودیت‌های فیزیکی و جغرافیایی در فضای سایبر) پیش می‌رود. به عبارتی، تهدیدها از هر نقطه از کره زمین به موجب توسعه فضای سایبری قابل وقوع و شکل‌گیری است و زمان تحقق آن در کسری از ثانیه است. به همین نسبت هر مرکز فرماندهی و کنترلی که از ظرفیت فضای سایبری برای ارتقای آگاهی وضعیتی خود استفاده کند، امکان برخورداری از اطلاعات از هر نقطه از سطح کره زمین در کمترین زمان ممکن فراهم می‌شود. مدل فرماندهی و کنترل سنتی در جنگ‌های فیزیکی بر مبنای "یکی در برابر همه" است. یک فرمانده در رأس است و سلسله مراتب فرماندهی ذیل آن قرار می‌گیرد. اما در مدل فرماندهی و کنترل متکی به ظرفیت‌های سایبری "همه در برابر همه" قرار می‌گیرند. تمرکز زدایی موجب افزایش سطح تاب آوری مراکز فرماندهی و کنترل و افزایش سطح آگاهی وضعیتی می‌شود. در مدل بسیاری با بسیاری انهدام یک عنصر راه به جایی نمی‌برد و سامانه همچنان فعال است، اما در مدل یکی با بسیاری در صورت انهدام عامل اصلی فرماندهی و کنترل وحدت تلاش از بین می‌رود. در "پدافند سایبری در عمق"، لایه‌های متعدد به منظور ممانعت از رخنه دشمن ایجاد می‌شود. حال در پدافند به صورت فیزیکی در صورت شکست راهبرد پدافند اقدام آفندی در دستور کار قرار می‌گیرد. در سامانه فرماندهی و کنترل پیشنهادی تلاش شده است تا به این نقص توجه شود و از چابکی در تغییر تاکتیک پدافند به آفند استفاده به عمل آید. سلول‌های هسته همواره در مرکز فرماندهی و کنترل حضور دارند، اما سلول‌های دینامیک بنا به موارد اقتضایی در مرکز فرماندهی و کنترل حضور پیدا می‌کنند.

بر اساس آنچه که شرح داده شد، می‌توان دریافت که ظرفیت‌های فضای سایبری یک جایگاه مهم در مراکز فرماندهی و کنترل برای افزایش آگاهی وضعیتی دارد. دامنه اطلاعات در این حوزه به دلیل تنوع منابع اطلاعاتی بیشتر می‌شود و شرایط برای تطابق اطلاعات با یکدیگر و تقاطع گیری فراهم می‌شود. به همین دلیل اعتبارسنجی اطلاعات به شیوه دقیق‌تری صورت می‌گیرد و در نهایت افزایش اشراف و آگاهی وضعیتی بدست می‌آید. به این شکل غافلگیری نیروها کمتر خواهد شد و واکنش آنها به تحولات و تهدیدهای محیط پیرامون بیشتر می‌شود. علاوه بر این، کاربردهای

اینترنت اشیاء بسیار متنوع است. از نقاط ایست و بازرسی تا تعیین وضعیت علائم حیاتی سربازان و بسیاری از اطلاعات با ارزش قابل دریافت و بررسی است. دامنه این اطلاعات می‌تواند تا سطح خسارات رزمی که به ادوات نظامی وارد می‌شود، گسترش یابد.

در سامانه‌های فرماندهی و کنترل جنگ‌های فیزیکی نیاز به افزایش منابع اطلاعاتی به ویژه در ظرفیت‌های جدیدی فضای سایبری مانند اینترنت اشیاء است. در سامانه‌های فرماندهی و کنترل جنگ‌های سایبری نیز این نیاز بدیهی است. بنابراین، در کلیه جنگ‌های سنتی و سایبری نیاز است تا همگام با توسعه تهدیدها در فضاهای جدید منابع اطلاعاتی نیز گسترش و توسعه پیدا کند و یکی از منابع مهم فرصت‌های فضای سایبری برای افزایش آگاهی وضعیتی است. با توسعه روز افزون شهرهای هوشمند و حتی مقرهای نظامی هوشمند لزوم توسعه راه‌های ارتباط دهی و ارتباط گیری مطرح شده است.

در جنگ‌های امروزی تمامی عوامل انسانی و تجهیزاتی به یکدیگر متصل شده‌اند و عضوی را نمی‌توان یافت که خارج از چارچوب شبکه عمل کند. شبکه سازی یعنی فعالیت تیمی و گروهی و افزایش هم افزایی در میان نیروهای عملیاتی که این خود به افزایش کارایی رزمی منجر می‌شود. این مهم چه در عرصه فیزیکی و چه در عرصه سایبری حائز اهمیت است و در سرعت تصمیم گیری هر طرف مؤثر است. درگیری‌ها در قلمروهای چندگانه جنگ به سرعت از قلمرویی به قلمروی دیگر منتقل می‌شود و کسی نمی‌تواند با یک نگاه تک بعدی و مراکز فرماندهی و کنترل تک قلمرویی به تمام تهدیدهای متوجه کشور بپردازد. بنابراین، سامانه فرماندهی و کنترل باید پویا بوده و امکان خلق و بکارگیری راهبردهایی را که از تاکتیک پشتیبانی می‌کند، بدهد. سلول‌های مجازی در فضای سایبری مرکز فرماندهی و کنترل وجود دارند. یک نیروی مهاجم سایبری بر خلاف محیط فیزیکی می‌تواند به طور هم زمان در چند سلول مجازی حضور داشته باشد. همین حضور هم زمان در چند سلول ویژگی قدرتمندی به فرماندهی و کنترل سایبری می‌دهد و دیگر نیازی نیست که همانند فرماندهی و کنترل فیزیکی گزارش به صورت سلسله مراتبی ارائه شود. فرماندهان جنگ سایبری می‌توانند اعضای چند سلول مجازی رده پائین‌تر و هم عرض خود باشند و در صورتی که مجاز دانسته شود، عضو سلول رده بالاتر از خود نیز باشند. این الگو قابل تسری در مراکز فرماندهی و کنترل فیزیکی است.

در فرماندهی و کنترل فیریکی تنها یک ساختار سازمانی حاکم است که از آن به زنجیره فرماندهی یاد می‌شود. گزارش‌دهی در این ساختار در سلسله مراتب فرماندهی صورت می‌گیرد و نوع رابطه بر اساس "بسیار با یکی" است. در ساختار فرماندهی و کنترل فیزیکی بسیاری از مراکز عملیات منطقه‌ای و مراکز کنترل و گزارش با یک مرکز عملیات در ارتباط هستند. اما سلول‌های مجازی بر اساس رابطه عضویت سازماندهی می‌شوند و نوع رابطه بر اساس "بسیاری با بسیاری" است. عملیات در ساختار متمرکز فرماندهی و کنترل به صورت شبکه محور اجرا می‌شود و در صورت انهدام مرکز عملیات سایر سلول‌ها دچار از هم گسیختگی شده و وحدت تلاش خود را از دست می‌دهند. اما در مدل "بسیاری با بسیاری" تنها هنگامی کارایی رزمی سلول‌ها از دست می‌رود که کل آنها مورد هدف قرار گیرند و انهدام یک یا چند مورد از آنها بی فایده است. با عنایت به آنچه بیان شد می‌توان از ویژگی‌های فضای سایبری برای افزایش کارآمدی مراکز فرماندهی و کنترل بهره برد که از آن جمله تغییر ساختار "یکی در برابر همه" به "همه در برابر همه" است. در چنین ساختار قدرت پاسخگویی مراکز فرماندهی و کنترل به تهدیدهای متنوع افزایش پیدا می‌کند. از سوی دیگر، به دلیل توسعه شبکه‌های ارتباطی و وابستگی اشیاء به اینترنت نیز می‌توان با بهره گرفتن از این ظرفیت حجم جمع آوری اطلاعات را افزایش داد. نکته دیگر حسگرهایی است که به موجب ظرفیت اینترنت اشیاء قابل استفاده در مراکز مختلف فرماندهی و کنترل است. همان طور که در سناریوهای مطرح آمد، این حسگرها می‌توانند در تشخیص سامانه‌های خودی یا دشمن (تشخیص دوست از دشمن) و در یک کلام افزایش آگاهی وضعیتی نقش بسزایی داشته باشد. با توجه به تنوع و تعدد طیف تهدیدها ضروری است تا مراکز فرماندهی و کنترل به منظور حفظ آگاهی وضعیتی خود از ساختارهای چابکی مانند ساختارهای سایبری بهره ببرند. جنگ‌ها خارج از شبکه عمل نمی‌کنند و زمان به شدت به سمت صفر شدن و مکان به سمت عدم محدودیت پیش می‌رود. حال ساختارهای فیزیکی مراکز فرماندهی و کنترل قدرت پاسخگویی به تهدیدها در چنین فضایی را ندارند و راهی جز بهره گرفتن از ساختارهای چابک فضای سایبری نیست. این چابکی به دلیل ضرورت پاسخگویی به تهدیدهای آنی در فضای سایبری است.

نتیجه‌گیری و پیشنهادها

در خاتمه نتیجه گرفته می‌شود که ظرفیت فضای سایبری حاوی الگوهای مناسبی برای بکارگیری در ساختار فرماندهی و کنترل جنگ‌های فیزیکی است. گسترش شهرها و پایگاه‌های هوشمند به شکلی شده است که بهره گیری از مزایای فضای سایبری و از جمله اینترنت اشیاء را تبدیل به امری ضروری کرده است. مهم‌ترین مزیت بهره‌گیری از فضای سایبری دستیابی به آگاهی وضعیتی است. شبکه‌سازی نیروها و تجهیزات و اتصال آنها به یکدیگر دامنه پوشش عملیاتی نیروها را گسترش داده است و امکان اجرای عملیات هماهنگ و بدون اصطکاک بین نیروها را فراهم آورده است. در این میان، ضرورت چند منظوره‌سازی و ایجاد قابلیت منعطف و عملکرد چند قلمرویی در مراکز فرماندهی و کنترل محسوس است. نیروها، سامانه‌ها و ساختارهای مراکز فرماندهی و کنترل باید به شکلی معماری شوند که توان پاسخگویی به نیازهای محیط عملیاتی از قلمرویی به قلمرو دیگر را داشته باشند. در گذشته مراکز فرماندهی و کنترل به نیازهای قلمروهای فیزیکی در زمین، دریا، آسمان و فضا پاسخ می‌دادند. اما در حال حاضر قلمرو پنجم به این ابعاد اضافه شده است و همانند اکسیژن در تمام آنها حاضر است و به عنوان یک عامل اثرگذار عمل می‌کند. در نتیجه، مراکز فرماندهی و کنترل نیز باید همپای این تحول متحول شوند تا توان پاسخگویی به نیازهای صحنه نبرد را همچنان داشته باشند. یکی از اقدامات مهم در این خصوص بهره‌گیری از ظرفیت فضای سایبری است تا آگاهی وضعیتی به عنوان یکی از کارکردهای مهم مراکز فرماندهی و کنترل افزایش یابد. بهره گیری از این ظرفیت به برخورداری از اطلاعات در لحظه در خصوص خسارات رزمی به تجهیزات و ادوات، جراحات و مجروحین، آمادگی روحی و روانی سربازان، تحولات میدان نبرد در قلمروهای فیزیکی و سایبری، وضعیت زیرساخت‌های حیاتی مانند شبکه برق، گاز و انرژی (به عنوان نیروی پیشران ادوات خودرویی ارتش‌ها) و بسیاری از موارد مشابه کمک شایانی می‌کند. علاوه بر این، استفاده از این ظرفیت به تشخیص به هنگام تهدیدها به ویژه در مناطق نا آرام و بی ثبات و پست‌های ایست و بازرسی کمک می‌کند و ضمن شناسایی هویت نفرات و سرنشینان، نوع خودرو و مشخصات آنها را با اطلاعات موجود تطبیق می‌دهد. وجود چنین قابلیتی به ویژه در محیط جنگ‌های شهری همانند لیبی، سوریه یا عراق

که با خودروهای انتحاری مواجه هستند، بسیار حائز اهمیت است. با وجود قابلیت فضای سایبری بانک اطلاعاتی مراکز فرماندهی و کنترل به عنوان با ارزش‌ترین سرمایه و دارایی آنها غنی شده و در لحظه اطلاعات آن به روز می‌شود. تغییر ساختار از "یکی به همه" به "همه به همه" یکی از دستاوردهای مهم الگوبرداری از فضای سایبری در ساختار فرماندهی و کنترل جنگ‌های فیزیکی است. به این شکل، تاب‌آوری نیروها افزایش یافته و سطح باززیستی به شکل چشمگیری ارتقاء می‌یابد. انهدام یک عامل یا مرکز در این ساختار نمی‌تواند موجب انهدام همه شود.

منابع اطلاعاتی در دنیای امروز متعدد و متنوع است و در ساختار شبکه‌ای مبتنی بر تمام قلمروها امکان استفاده از تمام ظرفیت‌ها برای افزایش آگاهی وضعیتی در مراکز فرماندهی و کنترل طبق الگوی اتصال به تمامی مراکز حائز اهمیت در جنگ وجود دارد. فضای سایبری دارای ظرفیت جمع‌آوری و انباشت داده و کلان داده است. این ظرفیت می‌تواند در اختیار مراکز فرماندهی و کنترل برای افزایش آگاهی وضعیتی قرار گیرد.

پیشنهاد می‌شود مراکز فرماندهی کنترل به ظرفیت‌های سایبری موجود در کشور متصل شوند و نهایت استفاده را از داده‌های موجود در دیتا بیس‌ها و نیز تبعیت از ساختارهای غیر سلسله مراتبی و "همه به همه" ببرند.

فهرست منابع

Alam, T., (2021), Block chain and its Role in the Internet of Things, Int J Sci Res in Comp Sci, Eng and Inf Tech

Bachrach, J., (2019), Composable continuous-space programs for robotic swarms. Neural Comput Appl.;19(6):825–47.

Beni, G., (2020), Swarm Intelligence in Cellular Robotic Systems. Robot Biological Systems Towards a New Bionics? NATO ASI Ser Vol102.

Bonabeau, E., (2018), Agent-based modeling: methods and techniques for simulating human systems. Proc Natl Acad Sci [Internet].;99(suppl. 3):7280–

Brambilla M., (2019), Swarm robotics: A review from the swarm engineering perspective. Swarm Intell.

Brambilla M., (2021), Property-driven design for swarm robotics. AAMAS 2012 Int Conf Auton Agents Multiagent Syst [Internet]. (June): in-press

Congressional Research Service, (2021), Defense primer: What is command and control?

DeLoach SA, (2020), Wood MF, Sparkman CH. Multiagent Systems Engineering. Int J Softw Eng Knowl Eng.

Finn, A., (2017), Developments and challenges for autonomous unmanned vehicles. Berlin: Springer.

Jani, N., (2020), IoT and Cyber Security: Introduction, Attacks, and Preventive Steps, IGI Global, Ch. 10.

Jurcut, P., (2019), Introduction to IoT Security, Wiley, , Ch. 2.

Kara, C. S., (2019), The Internet of Robotic Things, Tech. Rep. 5, ABI Research.

Mani, D., (2020), Data Science for IoT, in: Int Conf on Comp Net and Comm Tech.

Ministry of Defense of the Netherlands, (2020), Command and control, Joint Doctrine Publication.

Munoz, MF., (2020), Agent-based simulation and analysis of a defensive UAV swarm against an enemy UAV swarm. Naval Postgraduate School.

Parunak, F., (2021), HVD. Making Swarming Happen. In: Conference on Swarming and C4ISR, Tysons Corner, VA.

Simoens, M., (2021), The Internet of Robotic Things: A review, Int J Adv Robotic Sys 15 (02).

U.S. Department of Defense, (2019), Unmanned Systems Integrated Roadmap.

Weiskopf F., (2018), Control of cooperative, autonomous unmanned aerial vehicles. In: AIAA’s 1st Technical Conference and Workshop on Unmanned Aerospace Vehicles. Portsmouth, VA.