تاریخ دریافت: ۱۳۹۸/۱۰/۱۲
تاریخ پذیرش: ۱۳۹۹/۰۴/۱۱

فصلنامه علوم و فنون نظامی
سال شانزدهم، شماره ۵۱، بهار ۱۳۹۹
صص ۲۶- ۵

ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری ارتش آمریکا

وحید سجادی [۱*]
داود آذر [۲]

چکیده

در ادبیات نظامی ایالات‌متحده امریکا، فضای سایبر به‌عنوان حوزه پنجم عملیات نظامی معرفی و در اسناد راهبردی، بر ایجاد توانایی‌هایی برای عملیات سایبری مؤثر، اشاره گردیده است. ازاین‌رو، این پژوهش درصدد تبیین راه‌های ارتقای توان دفاع ارتش جمهوری اسلامی ایران در برابر عملیات سایبری ارتش امریکا، از طریق مطالعه اسناد و مدارک و نیز مصاحبه با صاحب‌نظران است. در این راستا، کارکنان پایور ارتش جمهوری اسلامی ایران دارای مدارک تحصیلی کارشناسی به بالا در رشته‌های مرتبط با فعالیت‌های سایبری و در محدوده درجات افسر ارشدی به بالا، به‌عنوان جامعه آماری، (با در نظر گرفتن ضریبی) به تعداد ۱۰۰ نفر در نظر گرفته شد و تمامی افراد جامعه (به‌صورت تمام شمار)، موردمطالعه قرار گرفتند. در تجزیه‌وتحلیل داده‌ها، در ابتدا اطلاعات به‌دست‌آمده بر پایه روش داده بنیاد، کدگذاری گردیده و بیشترین تکرارها مشخص گردید و در ادامه، تعداد ۲۶ سؤال در قالب پرسش‌نامه طراحی و در اختیار جامعه آماری قرار گرفت. نتایج حاصل از تجزیه‌وتحلیل اطلاعات جمع‌آوری‌شده، بیان‌گر آن است که با سطح اطمینان بسیار بالا می‌توان گفت که با انجام اقدامات بسترساز، توانمندساز و پشتیبانی اطلاعاتی، می‌توان توان مقابله ارتش جمهوری اسلامی ایران را در برابر عملیات سایبری ارتش امریکا ارتقا داد.

واژه‌های کلیدی:
فضای سایبری، عملیات تدافعی سایبری، عملیات تهاجمی سایبری، حمله سایبری، دفاع سایبری.

---

[۱]. کارشناس ارشد مدیریت دفاعی دانشگاه فرماندهی و ستاد آجا، تهران، ایران
[۲]. عضو هیئت‌علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران
[*] نویسنده مسئول: Email:v.d.sajadi@gmail.com

مقدمه

کسب توانایی مقابله با دشمن، مستلزم شناخت همه‌جانبه و آگاهی از نقاط ضعف و قوت آن است. آشنایی با رهنامه، ساختار و روندهای حاکم بر ارتش جهان، به‌ویژه ارتش‌هایی که در زمره ارتش‌های متخاصم احتمالی قرار دارند، در مطالعات نظامی کاربردی اهمیت فراوانی دارد. از سال ۲۰۱۱ که وزارت دفاع امریکا در سند راهبرد عملیات در فضای سایبر خود که با هدف تعیین اهداف راهبردی اولویت‌بندی شده و واقعی برای اقدامات سایبری وزارت دفاع و نیز مأموریت‌هایی که باید در ۵ سال آینده انجام می‌شد را منتشر کرد، فضای سایبر به‌عنوان حوزه پنجم عملیات نظامی وزارت دفاع امریکا – در کنار حوزه‌های چهارگانه زمین، هوا، دریا و فضا- معرفی گردید (Mudrinich,2012:4). بر این اساس، در سال ۲۰۱۲، وزارت دفاع شروع به ایجاد نیروی مأموریت سایبری[1] کرد و پیش‌بینی گردید که زمانی که این نیرو به‌طور کامل عملیاتی شود، ۶۲۰۰ نفر کارکنان نظامی، غیرنظامی و قراردادی خواهد داشت. نیروی مأموریت سایبری شامل کارکنانی است که در ۱۳۳ تیم، با عنوان تیم محافظت سایبری برای تکمیل اقدامات سنتی پدافندی و دفاع از شبکه‌های اولویت‌دار وزارت دفاع در برابر تهدیدات اولویت‌دار؛ نیروی مأموریت ملی و تیم‌های پشتیبانی اختصاص‌یافته به آن، برای محافظت از امریکا و منافع آن در برابر پیامدهای قابل‌توجه حملات سایبری؛ و نیروی مأموریت رزمی و تیم‌های پشتیبانی اختصاص‌یافته به آن، برای پشتیبانی از فرماندهان رزمی، از طریق پشتیبانی از طرح‌های عملیاتی و عملیات نظامی، سازمان‌دهی خواهند شد. ازآنجاکه استفاده تمام‌عیار از فضای سایبری در زمان‌های صلح و نبرد، یکی از راهبردهای اصلی امریکا بوده و در سال‌های اخیر نیز به‌خوبی نمود پیدا کرده است، به‌منظور ارتقای توان مقاومت در برابر عملیات سایبری امریکا، لازم است با نگاهی موشکافانه، نسبت به شناسایی و کسب اطلاعاتی کامل و جامع در خصوص ابعاد مختلف عملیات سایبری امریکا اقدام و متناسب با آن، سیاست‌ها و اقدامات مناسب برای ارتقای توان دفاع در برابر آن پیش‌بینی و اجرا گردد.

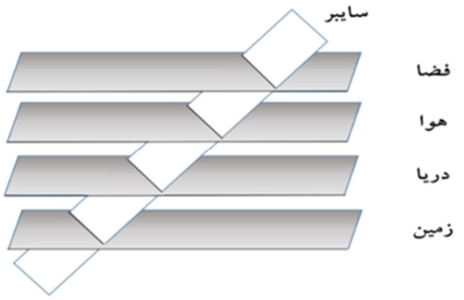
این پژوهش درصدد تبیین راه‌های ارتقای توان دفاع ارتش جمهوری اسلامی ایران (در تمام ابعاد تهاجمی، تدافعی و امنیتی) در برابر عملیات سایبری ارتش امریکا (اعم از عملیات سایبری تهاجمی، عملیات سایبری تدافعی و عملیات شبکه‌های اطلاعاتی وزارت دفاع) است که در این راستا، "تبیین راه‌های ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری ارتش آمریکا" به‌عنوان هدف اصلی و "راه‌های ارتقای توان مقابله ارتش جمهوری اسلامی ایران

[1] Cyber Mission Force

با عملیات سایبری ارتش آمریکا چیست؟" به‌عنوان سؤال اصلی این پژوهش در نظر گرفته شده است.

فضای سایبری

فضای سایبری یک دامنه فراگیر در محیط اطلاعاتی متشکل از شبکه‌های وابسته به زیرساخت‌های فناوری اطلاعات و داده‌های مقیم است که دربرگیرنده اینترنت، شبکه‌ها و سامانه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده‌ها و کنترل‌کننده‌های جاسازی‌شده است. نیروهای مسلح عملیات فضای سایبری را در قالب عملیات مستقل و مشترک انجام می‌دهند. (JP1-02,2010:86)



شکل (۱) رابطه حوزه سایبر با سایر حوزه‌های نبرد

گرچه فضای سایبر، یک دامنه مستقل در کنار دیگر دامنه‌ها است؛ اما قلمروهای فیزیکی را به هم پیوند می‌دهد. بنابراین ضمن اینکه فضای سایبری به‌تنهایی به‌عنوان یک عرصه مستقل جنگ پذیرفته‌شده است، موفقیت عملیات‌ها در عرصه‌های فیزیکی نیز مستلزم توانمندی و آمادگی همه‌جانبه در فضای سایبری است. آزادی مانور در فضای سایبر، قابلیت‌های فرماندهان را برای آزادی عمل و اِعمال فرماندهی در حوزه‌های دیگر، افزایش می‌دهد. (فرح بخت و دهقانی، ۱۳۸۹:۳۵)

رویکرد ایالات‌متحده امریکا به فضای سایبری

در ۲۰ سپتامبر ۲۰۱۸، کاخ سفید آخرین نسخه راهبرد سایبری خود را با عنوان راهبرد سایبری ملی[1] منتشر کرد. یک هفته پس از انتشار این سند، در سپتامبر ۲۰۱۸، کریستوفر پینتر[2]، هماهنگ‌کننده وقت امور سایبری وزارت امور خارجه امریکا، در یادداشتی در انستیتو

[1] National Cyber Strategy (NCS)
[2] Christopher Painter

سیاست‌های راهبردی استرالیا، نوشت که "هماهنگی و ادامه اقدامات گذشته،... پیامی محکم مبنی بر تداوم و پایداری رویکرد ایالات‌متحده را برای عموم و شرکای آمریکا می‌فرستد." مایکل دانیل[1]، هماهنگ‌کننده وقت امنیت سایبری کاخ سفید نیز در توییتر گفت که انطباق این رویکردها نشان می‌دهد که فضای سایبر، یک مسئله غیر حزبی است.

در راهبرد جدید سایبری ملی دولت امریکا، تهدیدات مبتنی بر فضای سایبر به‌عنوان یک تهدید جاری و دائمی علیه ایالات‌متحده امریکا در نظر گرفته شده است. برای محافظت از "شیوه زندگی آمریکایی"، امنیت سایبری به‌عنوان عنصری حیاتی در این راهبرد معرفی شده است.(www.cfr.org)

این سند شامل ۴ رکن اساسی است که عبارت‌اند از:

- *محافظت از مردم امریکا، سرزمین و شیوه زندگی آمریکایی* از طریق برقراری امنیت اطلاعات و شبکه‌های فدرال، امن سازی زیرساخت‌های حیاتی، مبارزه با جرائم سایبری و ارتقای گزارش دهی رخدادها.
- *ارتقای رفاه آمریکایی* از طریق تقویت یک اقتصاد دیجیتال پر جنب‌وجوش و پایدار(برگشت-پذیر)، رشد و محافظت از مهارت و قوه نبوغ امریکا، توسعه نیروی کار امنیت سایبری برتر.
- *حفظ صلح مقتدرانه* از طریق افزایش ثبات سایبری، نسبت دادن و مقابله با رفتارهای غیرقابل‌قبول در فضای سایبری.
- *پیشبرد نفوذ امریکا* از طریق ترویج اینترنت نامحدود، متقابل، مطمئن و امن و ایجاد ظرفیت‌های سایبری بین‌المللی. (National Cyber Strategy, 2018:15-26)

به‌کارگیری گسترده فناوری‌های سایبری (ازجمله پروتکل‌های ارتباطی، زیرساخت‌های شبکه‌ای، نرم‌افزارها و سخت‌افزارها) در تأمین اهداف ذکرشده، موجب وابستگی امریکا به حوزه سایبر شده است. این وابستگی، با در نظر گرفتن آسیب‌پذیری‌ها و گستردگی و توزیع آن‌ها در تمامی حوزه‌های نظامی و غیرنظامی، تمامی ابعاد زیرساختی، اداری، نظامی، اقتصادی، اجتماعی و ... را در معرض آسیب قرار داده است. بنابراین اگرچه توان تهاجمی دشمن در این حوزه ارتقا یافته و در حد بالایی قرار دارد، توان دفاعی و شناسایی این کشور در تناسب با دیگر کشورها، به دلیل گسترش استفاده از فضای سایبری، پایین است. (ابوالحسینی، ۱۳۹۲: ۸۲)

[1] Michael Daniel

رویکرد وزارت دفاع امریکا به فضای سایبری

در ۱۷ آوریل ۲۰۱۵، وزارت دفاع امریکا، سند راهبرد سایبری سال ۲۰۱۵ خود را منتشر کرد. سندی که به گفته اشتون کارتر وزیر دفاع آمریکا، هدف آن هدایت فرآیند توسعه نیروهای سایبری وزارت دفاع و تقویت وضعیت دفاع سایبری و بازدارندگی سایبری است و وزارت دفاع باید در طول پنج سال، آن‌ها را محقق کند. پنج سال پیش از انتشار این سند، وزارت دفاع امریکا در گزارش چهارساله نظامی خود،[1] بر اساس راهبرد امنیت ملی سال ۲۰۱۰ امریکا که تهدیدات فضای سایبر را به‌عنوان یکی از چالش‌های مهم امنیت ملی، امنیت عمومی و اقتصادی معرفی کرده بود، فضای سایبری در کنار زمین، هوا، دریا و فضا، به‌عنوان یکی از حوزه‌های نبرد معرفی شده است (Theohary, 2015:1). در این سند به شکل‌گیری یک نیروی مأموریت سایبری جدید اشاره‌شده بود. از سال ۲۰۱۲، وزارت دفاع شروع به ایجاد این نیروی مأموریت سایبری در داخل خود کرده بود. نیروی مأموریت سایبری نشان‌دهنده یک سرمایه‌گذاری عمده وزارت دفاع و دولت امریکا است و هدف اصلی از آن، تعیین اهداف خاص و مشخص برای هدایت و توسعه نیروی مأموریت سایبری و نیروهای کاری دیگر وزارت دفاع در محافظت و دفاع از منافع امریکا بیان شده بود. ساختار این نیرو در قالب ۱۳۳ تیم شامل **نیروی محافظت سایبری**، **نیروی مأموریت ملی سایبری** و **نیروی رزمی مأموریت سایبری** سازمان‌دهی گردید.

در سال ۲۰۱۳، به‌منظور دستیابی به همکاری در حوزه‌های دیگر و اطمینان از آمادگی رزمی نیروی مأموریت سایبری در نیرو و نیز ساختار سازی مجدد نیروهای کاری نظامی و غیرنظامی و زیرساخت‌ها برای اجرای مأموریت‌های وزارت دفاع، وزارت، شروع به تجمیع نیروی مأموریت سایبری در یک نیروی چند مأموریتی نظامی بزرگ‌تر کرد. در طول اجرای این راهبرد، وزارت دفاع به ایجاد نیروی مأموریت سایبری و تکمیل فرایند فرماندهی و کنترل و ایجاد سازمان‌دهی موردنیاز برای عملیات‌های مؤثر، ادامه داد(DoD, 2015:6) . سه سال بعد از انتشار سند راهبرد سایبری ۲۰۱۵، وزارت دفاع امریکا، رویکرد جدید سایبری خود را با عنوان "راهبرد سایبری ۲۰۱۸ وزارت دفاع امریکا" تدوین کرد. اهداف سایبری وزارت دفاع امریکا بر اساس این سند عبارت‌اند از:

۱- اطمینان از توانایی نیروهای مشترک، در دستیابی به اهداف خود در یک محیط رقابتی در فضای سایبری

[1] Quadrennial Defense Review

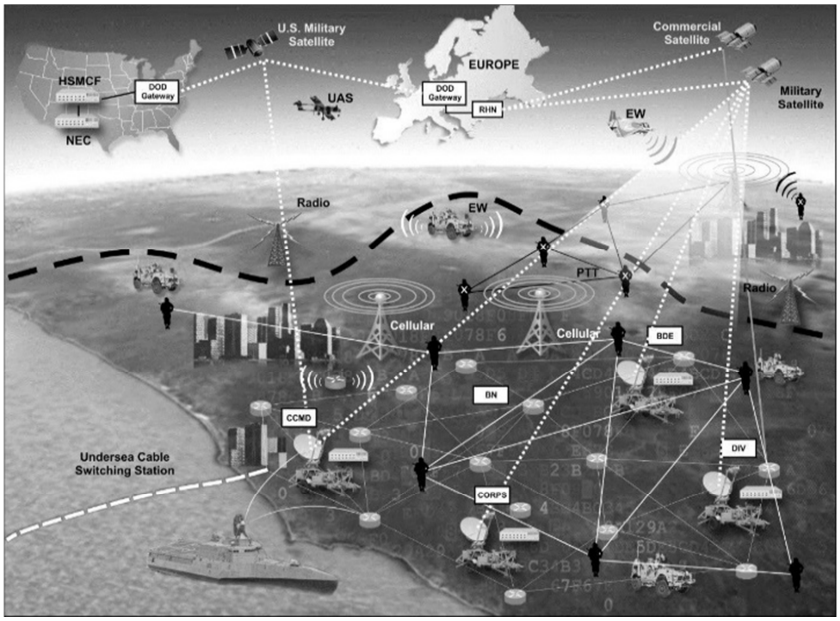
۲- تقویت نیروهای مشترک از طریق انجام عملیات سایبری که برتری نظامی امریکا را تسهیل می‌نماید.
۳- دفاع از زیرساخت‌های حیاتی امریکا از اقدامات سایبری مخرب که به‌تنهایی یا در کنار سایر اقدامات مخرب، می‌توانند منجر به بروز حوادث سایبری مهم شوند.
۴- امن کردن سیستم‌ها و اطلاعات وزارت دفاع در برابر اقدامات مخرب سایبری (که اطلاعات وزارت دفاع در سیستم‌هایی که متعلق به وزارت دفاع نیست را نیز دربر می‌گیرد.)
۵- توسعه همکاری‌های سایبری وزارت دفاع با همکاران بین سازمانی، صنایع و همکاران بین-المللی. (DoD, 2018:2)

بر پایه این سند و با فاصله‌ای اندک، فرماندهی سایبری ایالات‌متحده امریکا[1] -به‌عنوان متولی اصلی عملیات سایبری وزارت دفاع امریکا- سند جدید راهبرد خود را منتشر کرد. در تحلیلی که پروفسور ریچارد هارکنت[2] کمی بعد از انتشار این سند منتشر کرد، آمده است که فرماندهی سایبری بر این اعتقاد است که فضای سایبری، نسبت به زمان پایه‌گذاری این فرماندهی در سال ۲۰۰۹، دچار تغییرات اساسی شده است. بنابراین و بر اساس تجربیات حاصله طی هشت سال گذشته، فرماندهی سایبری امریکا یک رویکرد جدیدی را که با واقعیت‌های راهبردی که این فرماندهی می‌بایست با در نظر گرفتن آن‌ها، با موفقیت فعالیت کند، ارائه می‌دهد. این سند نشان‌دهنده پیشرفت قابل‌ملاحظه‌ای در عملیات سایبری و تفکر راهبردی است، که فرصتی برای به دست آوردن و ارتقای امنیت و ثبات، در محیط دیجیتال جهانی به‌هم‌پیوسته است.(www.lawfareblog.com)

با اشاره به سند راهبرد دفاعی سال ۲۰۱۸ ایالات‌متحده امریکا، مبنی بر توانایی فزاینده دشمنان در تأثیرگذاری و اخلال در جامعه، اقتصاد و قدرت نظامی امریکا (با توجه به رشد وابستگی و اتکای ایالات‌متحده امریکا به فضای سایبری)، مهم‌ترین و اساسی‌ترین نکته‌ای که در این سند به آن اشاره‌شده است، این است که: "برتری در حوزه‌های فیزیکی (زمین، دریا، هوا و فضا) در بخش‌های زیادی به برتری در فضای سایبری وابسته است." در سند راهبرد این فرماندهی، از فرماندهی سایبری به‌عنوان رزمندگان سایبری نام برده شده است که به‌صورت شبانه‌روزی مشغول به انجام عملیات در فضای سایبری در برابر دشمنان هستند و اکنون، آموخته‌اند که پیش از نفوذ دشمنان به محدوده دفاع سایبری خود و یا از بین بردن نیروهای

[1] United State Cyber Command (USCYBERCOM)
[2] Richard J. Harknett

نظامی امریکا، باید حملات را متوقف کنند؛ از طریق عملیات مداوم و یکپارچه، رفتار دشمن را تحت تأثیر قرار دهند؛ چابک باشند؛ همکاری‌هایشان عملیاتی و عملیاتشان مستمر باشد. وزارت دفاع با به‌کارگیری نیروهای نظامی، از جامعه آمریکا در مقابل تمام دشمنان خارجی یا داخلی حمایت و دفاع می‌کند. وزارت دفاع در کنار سایر مأموریت‌ها، آگاهی موقعیتی به اشتراک گذاشته‌شده را پیاده‌سازی و نگهداری کرده و عملیات دفاع از شبکه نظامی را هدایت می‌کند. (www.us-cert.gov)



BDE: تیپ زمینی	NEC: مرکز تشکیلات شبکه‌ای
BN: گردان زمینی	PTT: مکالمات تلفنی
CCMD: مقر فرماندهی جنگ	RHN: مرکز اصلی ارتباطات منطقه ای
DIV: لشکر زمینی	UAS: سیستم‌های هوایی بدون سرنشین
DOD: وزارت دفاع امریکا	HSMCF: مقر اصلی فرماندهی عملیات

شکل (۲) نمایش بصری فضای سایبری و طیف الکترومغناطیس در یک محیط عملیاتی

عملیات سایبری

طبق تعریف وزارت دفاع امریکا، عملیات فضای سایبر، عبارت از به‌کارگیری فضای سایبری با هدف اصلی دستیابی به اهداف، در فضای سایبری یا از طریق آن است. مأموریت‌های مربوط به فضای سایبری شامل عملیات سایبری تهاجمی، عملیات سایبری تدافعی و عملیات شبکه

اطلاعاتی وزارت دفاع است (DoD, 2017:GL-8). نوع و ماهیت عملیات سایبری و عواقبی که از این نوع عملیات متصور است، به‌گونه‌ای است که مشوق‌هایی برای اولویت دادن درگیری‌های سایبری نسبت به درگیری‌های نظامی ایجاد کرده است؛ به‌گونه‌ای که امروزه اگر ثابت شود که اهداف مدنظر از حمله به یک کشور یا سازمان، هم از طریق حملات نظامی و هم از طریق عملیات سایبری قابل تحقق است، به دلایل مختلف می‌توان ثابت کرد که راهکارهای سایبری انتخاب خواهد شد. (ابوالحسنی، ۱۳۹۲: ۹۸)

در آخرین نسخه نشریه مشترک عملیات سایبری وزارت دفاع امریکا، عملیات سایبری به سه حوزه عملیات سایبری تهاجمی، عملیات سایبری تدافعی و عملیات شبکه‌های وزارت دفاع تقسیم‌بندی شده است. عملیات نظامی در فضای سایبری در قالب مأموریت‌های اجرایی از طریق ترکیبی از اقدامات ویژه به‌منظور نیل به هدف‌های تعیین‌شده انجام می‌شود. نهادها و بخش‌های مختلفی در وزارت دفاع، اقدامات اطلاعاتی ملی، فعالیت‌های تجاری خرد و سایر فعالیت‌های سایبری را انجام می‌دهند که این فعالیت‌ها، تحت سیاست‌های مرتبط با عملیات سایبری وزارت دفاع هدایت می‌گردند. اغلب فعالیت‌های سایبری وزارت دفاع، به‌عنوان "اقدامات مرتبط سایبری"، از فضای سایبری برای فراهم کردن امکان اجرای سایر فعالیت‌های سایبری استفاده می‌کنند که توانمندی‌های فضای سایبری را برای تکمیل مأموریت‌ها به کار گیرد؛ اما به‌عنوان بخشی از سه نوع عملیات سایبری (عملیات سایبری تهاجمی، عملیات سایبری تدافعی و عملیات شبکه اطلاعاتی وزارت دفاع) طبقه‌بندی نمی‌شوند. این کاربردها شامل فعالیت‌هایی مثل اجرای یک سامانه فرماندهی و کنترل یا پشتیبانی، ارسال یک پیام الکترونیکی برای پشتیبانی از یک هدف اطلاعاتی یا استفاده از اینترنت برای تکمیل یک دوره آموزشی می‌شود. اغلب از طریق چنین کاربردهایی است که آسیب‌پذیری‌ها یا نفوذها علیه شبکه اطلاعاتی وزارت دفاع ایجاد می‌شود.(DoD, 2018:II-1)

تمام فعالیت‌هایی که در فضای سایبری انجام‌شده و در زمره اقدامات مرتبط سایبری قرار نمی‌گیرند، به‌عنوان بخشی از یکی از سه نوع عملیات سایبری (عملیات سایبری تهاجمی، عملیات سایبری تهاجمی تدافعی و عملیات شبکه اطلاعاتی وزارت دفاع) اجرا می‌شوند. این سه نوع عملیات، به‌طور کامل تمامی فعالیت‌های نیروهای سایبری را پوشش می‌دهند. مأموریت‌ها و فعالیت‌های فضای سایبری به هم وابسته و مرتبط هستند. فعالیت‌های سایبری، پشتیبان و حمایت‌کننده مأموریت‌های سایبری هستند. فعالیت‌های سایبری از عملیات شبکه اطلاعاتی وزارت دفاع، عملیات سایبری تهاجمی و عملیات سایبری تدافعی یا هر ترکیبی از آن‌ها پشتیبانی می‌کنند. اجرای فعالیت‌های سایبری در هر رده‌ای، به هماهنگی، توانایی و مجوزهای

مربوطه وابسته است. این فعالیت‌ها به هم وابسته و مرتبط بوده و انجام موفق یک مأموریت، ممکن است نیازمند اجرای چندین فعالیت سایبری باشد.(U.S.ARMY, 2017:I-6)

عملیات سایبری تدافعی

هدف اصلی از دفاع، هدایت تمامی فعالیت‌های دشمن به خارج از سامانه‌های خودی است. اهدافی ازجمله توانایی بازسازی پذیری[1]، انسجام و توانایی حفظ اعتماد نیز اهدافی حقیقی در این زمینه به شمار می‌آیند. مجموعه تلاش‌های سازمان‌یافته و هدایت‌شده برای جلوگیری از آسیب رساندن مهاجمان به توانایی‌های نظامی در عرصه فناوری‌های سایبری، در قالب عملیات سایبری تدافعی طبقه‌بندی می‌شوند. تاکتیک‌های مورداستفاده نیروهای مسلح در این حوزه، با روش‌های مورداستفاده توسط سایر سازمان‌ها و نهادها برای دور نگه‌داشتن متجاوزین بسیار شبیه است. چراکه ابزارهای مورداستفاده در این حوزه، در بسیاری از موارد مشترک هستند. به‌عنوان‌مثال، از همان سامانه‌های دیواره آتش که در محیط‌های نظامی استفاده می‌شود، در محیط‌های غیرنظامی و سایر سازمان‌ها و نهادها نیز استفاده می‌گردد. (ناصری، ۱۳۸۷: ۳۳)

در آخرین نسخه نشریه مشترک عملیات سایبری در سال ۲۰۱۸، عملیات سایبری تدافعی به‌عنوان مأموریت‌هایی که برای دفاع از شبکه اطلاعاتی وزارت دفاع -یا سایر نیروهای سایبری وزارت دفاع که دستور دفاع از آن‌ها صادرشده باشد- در برابر تهدیدات فعال در فضای سایبری انجام می‌شود، تعریف شده است. مأموریت‌های عملیات سایبری تدافعی، به‌طور خاص به حفظ توانمندی نیروهای خودی و محافظت از داده‌ها، شبکه‌ها، تجهیزات مرتبط سایبری و سایر تجهیزات و توانمندی‌هایی که در معرض مواجهه با تهدیدات سایبری هستند، اختصاص داده‌شده‌اند. این اقدامات درواقع برای زمان‌هایی که تهدیدات جاری، موفق به شکستن یا دور زدن اقدامات امنیتی و ایمنی اجراشده در قالب عملیات شبکه اطلاعاتی وزارت دفاع شده و یا احتمال شکست یا دور زدن آن‌ها توسط تهدیدات وجود دارد، طراحی و اجرا می‌گردند. عملیات سایبری تدافعی، تهدید محور بوده و به‌طور متناوب از اهداف عملیاتی پشتیبانی می‌کنند. هدف اصلی عملیات سایبری تدافعی، دفع تهدید جاری و/یا بازگرداندن یک شبکه در معرض خطر به شرایط امنیتی و کارکرد عادی است.

اجزای عملیات سایبری تدافعی عبارت‌اند از:

- اقدامات دفاعی داخلی عملیات سایبری تدافعی[2]

---

[1] Recoverability

[2] DCO Internal Defensive Measures (DCO-IDM)

- فعالیت‌های واکنشی عملیات سایبری تدافعی[1]
- دفاع از فضای سایبری غیر وزارت دفاع[2] (DoD, 2018:II-4)

عملیات سایبری تهاجمی

عملیات سایبری تهاجمی، گونه‌ای از عملیات سایبری هستند که بر اساس استفاده از قدرت در فضای سایبر، یا از طریق آن طرح‌ریزی شده‌اند. همانند عملیات تهاجمی در حوزه‌های فیزیکی، عملیات سایبری تهاجمی، بر اساس دستور و مجوزهای صادرشده، انجام می‌شود. عملیات سایبری تهاجمی، نیاز به تطبیق با سیاست‌های جاری و کسب مجوز از مقامات ذیصلاح دارد. این عملیات، از نوع مأموریت‌هایی است که به‌منظور نمایش و اعمال قدرت در فضای سایبری خارجی (غیرخودی) یا به‌واسطه آن، از طریق فعالیت‌های انجام‌شده در پشتیبانی از فرماندهان رزمی یا اهداف ملی انجام می‌شوند. عملیات سایبری تهاجمی می‌تواند منحصراً علیه فعالیت‌های سایبری دشمنان هدف‌گیری شوند یا آثار ابتدایی را در فضای سایبری، به‌منظور شروع تأثیرات متوالی دقیق کنترل‌شده در حوزه‌های فیزیکی، با هدف تأثیرگذاری بر سامانه‌های جنگی، فرایندهای فرماندهی و کنترل، نقاط آمادی و تدارکات، آتش‌های دارای ارزش بالا و ... دشمن ایجاد نماید.

همانند فعالیت‌های واکنشی عملیات سایبری تدافعی، برخی مأموریت‌های عملیات سایبری تهاجمی می‌تواند شامل اقداماتی باشد که منجر به به‌کارگیری نیرو با تخریب یا انهدام فیزیکی سامانه‌های دشمن شود. مأموریت‌های عملیات سایبری تهاجمی نیاز به دستور نظامی هماهنگ شده مناسب و ملاحظات دقیق سطوح مأموریت، نقش‌ها و وظایف شرکت‌کنندگان و نیز اهداف قابل‌اندازه‌گیری دارد. (DoD, 2018:II-5)

حملات سایبری ممکن است از خارج از شبکه و از طریق هکرها، یا از درون شبکه و به‌وسیله سازه‌ها و اجزای مخرب صورت گیرند. این فعالیت‌ها که به‌دقت با سایر آتش‌های طرح‌ریزی‌شده در حوزه فیزیکی هماهنگ و هم‌زمان هستند، شامل فعالیت‌های انکار (نفی) و دست‌کاری (تحریف) است. (همان: II-6)

[1] DCO Response Actions (DCO-RA)
[2] Defense of Non-DOD Cyberspace

عملیات شبکه اطلاعاتی وزارت دفاع

مأموریت عملیات شبکه اطلاعاتی وزارت دفاع[1]، شامل فعالیت‌های عملیاتی است که برای امن سازی، پیکربندی، عملیات، توسعه، نگهداری و پایداری فضای سایبری وزارت دفاع امریکا و نیز ایجاد و حفظ جنبه‌های امنیتی (یکپارچگی، دسترس‌پذیری و اعتمادپذیری) شبکه اطلاعاتی وزارت دفاع، در فضای سایبری انجام می‌شود. این فعالیت‌ها شامل اقدامات امنیتی سایبری است که آسیب‌پذیری‌های شبکه اطلاعاتی وزارت دفاع یا بخش‌هایی از آن را مشخص می‌کند. علاوه بر آن، برپایی شبکه‌های تاکتیکی به‌منظور توسعه شبکه‌های موجود توسط نیروهای گسترش‌یافته، اقدامات نگهداری و سایر اقدامات غیرامنیتی لازم برای نگهداری شبکه اطلاعاتی وزارت دفاع و نیز عملیات تیم‌های قرمز و سایر اشکال آزمون و ارزیابی، جزء سایر مأموریت‌های عملیات شبکه اطلاعاتی وزارت دفاع است.

عملیات شبکه اطلاعاتی وزارت دفاع، متمرکز بر شبکه و تهدید محور است. نیروهای سایبری و نیروهای کار اختصاص داده‌شده به این مأموریت تلاش می‌کنند از تأثیرگذاری تهدیدات بر شبکه‌ها و سامانه‌های خاصی که محافظت از آن‌ها را بر عهده دارند، جلوگیری نمایند. آن‌ها از تمامی اطلاعات موجود درباره هر تهدید بخصوص، برای ارتقای وضعیت امنیتی شبکه بهره می‌گیرند. ازآنجاکه پایه و اساس انجام تمامی توانمندی‌ها و کارکردهای سرویس‌های رزمی وزارت دفاع شبکه اطلاعاتی وزارت دفاع است، عملیات شبکه اطلاعاتی وزارت دفاع را احتمالاً می‌توان مهم‌ترین و پیچیده‌ترین نوع عملیاتی دانست که وزارت دفاع به‌طور روزانه انجام می‌دهد. (همان: II-2)

نقش‌ها و مسئولیت‌ها در عملیات سایبری وزارت دفاع امریکا

فرماندهی سایبری ایالات‌متحده[2]

در ۲۳ ژوئن ۲۰۰۹، به دستور وزیر دفاع وقت امریکا در زیرمجموعه فرماندهی راهبردی برای تمرکز بر عملیات سایبری نظامی، با ادغام چندین واحد از بخش‌های امنیت شبکه وزارت دفاع تشکیل و از ۳۱ اکتبر ۲۰۱۰، به‌طور رسمی مشغول به فعالیت گردید. در ۱۸ اوت ۲۰۱۷، رئیس‌جمهور آمریکا، دونالد ترامپ، توصیه وزیر دفاع مبنی بر انتزاع فرماندهی سایبری از فرماندهی راهبردی ایالات‌متحده و تأسیس فرماندهی رزمی مستقل/یکپارچه مسئول عملیات

[1] DODIN Operations
[2] US Cyber Command(USCYBERCOM)

های سایبری[1] را پذیرفت و از ۴ می ۲۰۱۸ ، فرماندهی سایبری ایالات‌متحده امریکا، به دهمین فرماندهی رزمی مستقل/یکپارچه[2] تبدیل شد."ژنرال پاول ناکاسون" از ۴ می ۲۰۱۸، به‌عنوان فرمانده فرماندهی سایبری امریکا معرفی و جایگزین "دریاسالار مایکل راجرز" شد که از سال ۲۰۱۴ این مسئولیت را به عهده داشت (https://www.cybercom.mil). این فرماندهی طرح-ریزی، هماهنگی، تجمیع و هدایت فعالیت‌ها به‌منظور جهت‌دهی عملیات و دفاع از شبکه‌های اطلاعاتی اختصاصی وزارت دفاع؛ آماده‌سازی و (بنا به دستور) هدایت و اجرای عملیات سایبری نظامی همه‌جانبه به‌منظور ایجاد توانمندی فعالیت در همه حوزه‌ها؛ تضمین آزادی عمل امریکا و متحدانش در فضای سایبر؛ و جلوگیری از اقدام مشابه دشمنان و رقبا را بر عهده دارد. "دستیابی و حفظ تفوق در فضای سایبر، به‌منظور تأثیرگذاری بر رفتار دشمن، ارائه مزایای راهبردی و عملیاتی به نیروهای مشترک؛ و دفاع و پیشرفت منافع ملی" به‌عنوان چشم‌انداز فرماندهی سایبری امریکا تعیین‌شده است.

فرماندهی سایبری نیروی زمینی/ ارتش دوم[3]

در اول اکتبر سال ۲۰۱۰، فرماندهی سایبری نیروی زمینی، به‌عنوان یک رده عملیاتی نیروی زمینی، تحت نظارت مستقیم ستاد نیروی زمینی، تشکیل گردید. این فرماندهی، مسئولیت مستقیم مأموریت‌ها، اقدامات و فعالیت‌های مرتبط با فضای سایبر در نیروی زمینی را بر عهده دارد. فرماندهی سایبری نیروی زمینی، عملیات سایبری همه‌جانبه را به‌منظور اطمینان از آزادی عمل در فضای سایبر و مانعت از اقدام مشابه دشمن، اجرا می‌نماید. این فرماندهی، وظیفه هدایت و انجام جنگ الکترونیک یکپارچه، عملیات اطلاعاتی و عملیات سایبری (در صورت تصویب و بنا به دستور) را برای تضمین آزادی عمل در فضای سایبر یا محیط اطلاعاتی و یا با استفاده از آن و جلوگیری از استفاده مشابه دشمن از آن را بر عهده دارد. (www.arcyber.army.mil)

فرماندهی سایبری نیروی دریایی / ناوگان دهم [4]

ناوگان دهم امریکا، نیروی عملیاتی فرماندهی سایبری است. این ناوگان، هدایت عملیاتی را از مرکز عملیات دریایی واقع در مریلند انجام می‌دهد. مأموریت فرماندهی سایبری ناوگان دهم،

[1] Unified Combatant Command responsible for cyberspace operations
[2] Unified Combatant Command (CCMD)
[3] Army Cyber Command/Second Army (USARCYBER)
[4] Fleet Cyber Command/Tenth Fleet (Navy)

ایفای نقش مرکز عملیات برای شبکه‌ها، عملیات رمزنگاری و اطلاعات سیگنالی، عملیات اطلاعاتی، عملیات سایبری، جنگ الکترونیک و عملیات فضایی برای پشتیبانی از نیروها، در دریا و ساحل؛ هدایت عملیات سایبری جهانی نیروی دریایی برای مقابله و دفاع در برابر تجاوز و اطمینان از آزادی عمل در دستیابی به اهداف نظامی در درون فضای سایبر یا با استفاده از آن؛ سازمان‌دهی و هدایت عملیات رمزنگاری جهانی و پشتیبانی از عملیات اطلاعاتی و طراحی و عملیات فضایی (بنا به دستور)؛ اجرای مأموریت‌های سایبری (بنا به دستور)؛ هدایت، فعالیت، نگهداری، امن سازی و دفاع از بخش‌های مرتبط به نیروی دریایی شبکه‌های اطلاعاتی وزارت دفاع؛ توسعه، همکاری، تجهیز و اولویت‌بندی نیازمندی‌های عملیات اطلاعاتی، سایبری، رمزنگاری/ جمع‌آوری اطلاعات سیگنالی نیروی دریایی است. (https://www.public.navy.mil)

فرماندهی سایبری نیروی هوایی[1]

نیروی ۱۶هوایی امریکا، ساختار عملیاتی رزمی نیروی هوایی است که برای حصول اطمینان از حفظ برتری رزمی نیروهای خودی، عملیات سایبری همه‌جانبه را اجرا می‌کند. مأموریت این نیرو، عملیات، توسعه و دفاع از شبکه‌های اطلاعات نیروی هوایی، دفاع از سامانه‌های کلیدی مأموریتی و ارائه توانمندی‌ها و قابلیت‌های سایبری همه‌جانبه، برای نیروهای رزمی مشترک، در فضای سایبر یا با استفاده از آن است. بیش از ۵۴۰۰ نفر کارکنان نیروی هوایی و ۱۱۰۰۰نفر کارکنان رزرو، عملیات سایبری امریکا در سطح جهان را پشتیبانی می‌نمایند. (https://www.16af.af.mil)

فرماندهی سایبری تفنگداران دریایی[2]

فرماندهی سایبری تفنگداران دریایی، یک نیروی کاربردی از تفنگداران دریایی برای محافظت از زیرساخت‌های حیاتی در مقابل حملات سایبری است. این فرماندهی، بخش تفنگداران دریایی فرماندهی سایبری امریکا است که مقر آن در فورت مید مریلند واقع شده است. این فرماندهی، هم‌زمان با فرماندهی سایبری نیروی دریایی و فرماندهی سایبری نیروی هوایی، در اکتبر ۲۰۰۹ ایجاد شده است (https://www.candp.marines.mil) . مأموریت فرماندهی سایبری تفنگداران دریایی، طراحی، هماهنگی، تجمیع و یکپارچه‌سازی و هدایت عملیات یکپارچه سایبری تفنگداران است. این مأموریت، هر سه بخش عملیات سایبری را دربر می‌گیرد. (http://www.candp.marines.mil)

---

[1] AIR FORCE CYBER COMMAND /24th AIR FORCE

2 U.S. Marine Corps Cyberspace Command

نیروی مأموریت سایبری

از سال ۲۰۱۲، وزیر دفاع و رئیس ستاد مشترک ارتش امریکا[1]، نیروی مأموریت سایبری را برای سازمان‌دهی و استفاده از نیروی موردنیاز برای انجام مأموریت‌های کلیدی سایبری ایجاد کردند. فرمانده فرماندهی سایبری امریکا، از نیروی مأموریت سایبری به‌عنوان زیرمجموعه‌ای از نیروهای وزارت دفاع، برای انجام عملیات سایبری بهره‌برداری می‌کند. واحدهای مختلف تاکتیکی فضای سایبر از نیروها (سرویس‌های) گوناگون که به فرماندهی سایبری اختصاص‌یافته است، شامل سه گروه زیر است:

نیروی محافظت سایبری[2]. نیروی محافظت سایبری، عملیات سایبری برای محافظت داخلی از شبکه اطلاعاتی وزارت دفاع یا سایر دارایی‌های سایبری را طبق دستور انجام می‌دهد. این نیرو، از ۶۸ تیم محافظت سایبری که برای دفاع در فضای سایبر در همکاری یا پشتیبانی از صاحبان بخش‌ها، ارائه‌دهندگان خدمات امنیت سایبری و کاربران، سازمان‌دهی شده، آموزش-های لازم را فرا گرفته و به‌طور کامل تجهیز شده‌اند، تشکیل شده است.

نیروی عملیات ملی سایبری [3]. نیروی عملیات ملی سایبری، عملیات سایبری برای مقابله با تهدیدات فضای سایبر قابل‌توجه علیه شبکه اطلاعاتی وزارت دفاع و (بنا به دستور) علیه منافع ملی و متوقف کردن حملات سایبری و فعالیت‌های مخرب سایبری را انجام می‌دهد. این نیرو از چندین تیم مختلف مأموریت ملی، تیم‌های پشتیبانی ملی اختصاص‌یافته و تیم‌های پشتیبانی سایبری سطح ملی برای محافظت از فضای سایبر غیر شبکه‌های وزارت دفاع تشکیل شده است. نیروی مأموریت ملی سایبری، شامل ۱۳ تیم مأموریت ملی است که توسط ۸ تیم پشتیبانی ملی پشتیبانی می‌شوند و برای دفاع از کشور در برابر حملات سایبری علیه منافع امریکا طراحی شده‌اند.

نیروی رزمی عملیات سایبری[4]. نیروی رزمی عملیات سایبری، عملیات سایبری را در پشتیبانی از مأموریت‌ها، طرح‌ها و اولویت‌های فرماندهان رزمی و جغرافیایی انجام می‌دهد. این نیرو از چندین تیم مختلف مأموریت رزمی سایبری و تیم‌های پشتیبانی رزمی اختصاص داده‌شده تشکیل شده است. نیروی مأموریت رزمی سایبری، شامل ۲۷ تیم مأموریت رزمی است

---

[1] Chairman of the Joint Chiefs of Staff (CJCS)
[2] Cyber Protection Force (CPF)
3 Cyber National Mission Force (CNMF)
4 Cyber Combat Mission Force (CCMF)

که توسط ۱۷ تیم پشتیبانی رزمی پشتیبانی می‌شوند و تمرکز آن‌ها بر نیازمندی‌های سایبری فرماندهی‌های رزمی است.(DoD, 2018:I-9)

روش اجرای پژوهش

ازآنجاکه در این پژوهش، پژوهشگران درصدد بودند تا با استفاده از روش‌های علمی، راه‌های ارتقای توان دفاع سایبری آجا در برابر عملیات سایبری ارتش امریکا را ارائه نماید، این پژوهش از نوع کاربردی است. با توجه به اینکه در این پژوهش ابعاد مختلف عملیات سایبری ارتش امریکا، آن‌گونه که هست، با تمرکز به زمان حال (وضعیت فعلی) با در نظر گرفتن رویدادها و آثار گذشته -که به شرایط موجود مربوط می‌شوند- موردبررسی، توصیف و تفسیر گردیده است، پژوهش از نوع توصیفی است.

در این پژوهش، پژوهشگران با استفاده از ادبیات نظری و مصاحبه با خبرگان و متخصصان مربوطه، اطلاعات و داده‌های موردنیاز را با ابزارهای اسناد و مدارک، مصاحبه و پرسشنامه جمع‌آوری (روش توصیفی) نموده و ابتدا با انجام تحلیل کیفی و انسجام دهی و خلاصه کردن، نتایج موردنظر اهداف پژوهش را به دست آورده، سپس بر اساس دیدگاه و نگرش جامعه نمونه، نتایج پرسشنامه را تحلیل کمی نموده و درنهایت با روش تحلیل آمیخته به نتیجه‌گیری و ارائه راه‌کارهای مناسب دست یافته است.

تجزیه‌وتحلیل اطلاعات جمع‌آوری‌شده

برای شناسایی راه‌های ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری ارتش آمریکا، با در نظر گرفتن یافته‌های حاصله از ادبیات پژوهش و نظرات صاحب‌نظران، تعداد ۲۳ سؤال در قالب پرسش‌نامه طراحی و در اختیار جامعه آماری قرار گرفت. پس از تجزیه‌وتحلیل اطلاعات جمع‌آوری‌شده از طریق پرسشنامه، مصاحبه با صاحب‌نظران و بررسی اسناد و مدارک در رابطه با موضوع پژوهش که به روش توصیفی و با استفاده از جداول توزیع فراوانی و آمار استنباطی نتایج زیر حاصل گردید.

ایالات‌متحده امریکا از حدود دو دهه پیش، به اهمیت فضای سایبری و نقش آن در نبردهای آینده پی برده است و به همین دلیل شروع به سیاست‌گذاری در این حوزه نموده است. بر این اساس، ضمن تدوین راهبردهای سایبری در سطوح ملی و وزارت دفاع، نیروهای مربوطه سایبری در سطح وزارت دفاع (و سایر سازمان‌ها، نهادها و ارگان‌ها) پیش‌بینی، ایجاد و عملیاتی شده است. در این رابطه، پس از تعریف فضای سایبری به‌عنوان یک حوزه عملیاتی

برای وزارت دفاع امریکا، تمامی وظایف عملیات سایبری در قالب عملیات سایبری تدافعی، تهاجمی و عملیات سایبری توسط نیروهای سایبری اشاره‌شده، طرح‌ریزی و اجرا می‌گردد.

با توجه به موارد بالا، عمده نتایج به‌دست‌آمده از تجزیه‌وتحلیل ادبیات پژوهش و نظرات صاحب‌نظران، حاکی از این است که برای ارتقای توان مقابله ارتش جمهوری اسلامی ایران در برابر عملیات سایبری امریکا، لازم است که *ضمن به رسمیت شناختن فضای سایبری به‌عنوان یک حوزه نبرد*، *انجام انواع عملیات سایبری در فضای سایبری یا با استفاده از فضای سایبری، توسط ارتش جمهوری اسلامی ایران*، مدنظر قرار داده شود. پس از انجام این مراحل، مهم‌ترین اقدامات لازم برای ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری امریکا، اولاً *رصد مستمر و مداوم وضعیت امنیت سایبری خودی* در کنار *رصد مستمر و مداوم عملیات سایبری امریکا* و ثانیاً *ارتقای توانمندی انفرادی و سازمانی افراد و یگان‌های مرتبط در ارتش جمهوری اسلامی ایران از طریق تجهیز، آموزش و شبیه‌سازی عملیات سایبری امریکا در قالب رزمایش‌های سایبری* است.

نتایج به‌دست‌آمده از تجزیه‌وتحلیل اطلاعات، گویای این مطلب است که بیش از ۹۲٪ افراد جامعه نمونه، شاخص‌های ارائه‌شده را در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش آمریکا در سطح متوسط به بالا مورد تأیید می‌دانند. و در ضمن چون میانگین این مؤلفه ۴/۰۴ (۵ >۴/۰۴> ۴) است، امکان بهره‌برداری از آن به میزان زیاد به بالا است.

جدول(۱) اولویت اقدامات برای ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا بر اساس آزمون فریدمن

اولویت	شاخص	رتبه میانگین
۱	آموزش کارکنان سایبری برای انجام اقدامات سایبری تهاجمی مناسب و متناسب با اقدامات تدافعی ارتش امریکا	۴,۶۹
۲	تدوین یا به‌روزرسانی اسناد بالادستی در آجا برای لحاظ کردن فضای سایبری به‌عنوان یک حوزه انجام عملیات نظامی یا با اهداف نظامی در کنار سایر حوزه‌های فیزیکی موجود (زمین، هوا، دریا و فضا)	۴,۵۲
۳	تدوین یا به‌روزرسانی اسناد بالادستی در آجا برای انجام عملیات سایبری در آجا و پیش‌بینی نقش تهاجمی برای آجا در فضای سایبری یا با استفاده از آن در رویارویی‌های احتمالی پیش رو	۴,۱۹

۴	شبیه‌سازی اقدامات دفاعی وزارت دفاع امریکا از طریق انجام رزمایش‌های سایبری	۴,۱۵
	میانگین	۴,۳۹

✓ نتایج به‌دست‌آمده از تحلیل کیفی و کمی، در خصوص دستیابی به هدف "شناسایی راه-های مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا"

تعداد ۴ شاخص از شاخص‌های موردبررسی قرارگرفته با میانگین بیش از ۴، به شرح زیر، به-عنوان اقدامات دارای اولویت در راستای ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا احصاء گردید:

۱. آموزش کارکنان سایبری برای انجام اقدامات تهاجمی سایبری مناسب و متناسب با اقدامات تدافعی ارتش امریکا که با کسب میانگین ۴,۶۹ از نظر صاحب‌نظران حائز بالاترین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا شده است. ۹۵٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا مفید است.

۲. تدوین یا به‌روزرسانی اسناد بالادستی در آجا برای لحاظ کردن فضای سایبری به‌عنوان یک حوزه انجام عملیات نظامی یا با اهداف نظامی در کنار سایر حوزه‌های فیزیکی موجود (زمین، هوا، دریا و فضا)که با کسب میانگین ۴,۵۲ از نظر صاحب‌نظران حائز دومین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا شده است. ۹۱٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا مفید است.

۳. تدوین یا به‌روزرسانی اسناد بالادستی در آجا برای انجام عملیات سایبری در آجا و پیش‌بینی نقش تهاجمی برای آجا در فضای سایبری یا با استفاده از آن در رویارویی‌های احتمالی پیش‌رو که با کسب میانگین ۴,۱۹ از نظر صاحب‌نظران حائز سومین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا شده است. ۷۷٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا مفید است.

۴. شبیه‌سازی اقدامات دفاعی وزارت دفاع امریکا از طریق انجام رزمایش‌های سایبری که با کسب میانگین ۴,۱۵ از نظر صاحب‌نظران حائز چهارمین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا شده است. ۷۹٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا مفید است.

✓ نتایج به‌دست‌آمده از تحلیل کیفی و کمی، در خصوص دستیابی به هدف شناسایی راه‌های مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا

تعداد ۸ شاخص از شاخص‌های موردبررسی قرارگرفته با میانگین بیش از ۴، به شرح زیر، به‌عنوان اقدامات دارای اولویت در راستای ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تدافعی ارتش امریکا احصاء گردید:

۱. بازنگری و به‌روزرسانی رهنامه دفاعی آجا و تعریف عملیات سایبری به‌عنوان یک حوزه عملیاتی در مقابل عملیات سایبری تهاجمی ارتش امریکا که با کسب میانگین ۴,۶ از نظر صاحب‌نظران حائز بالاترین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۹۵ ٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.

۲. بازتعریف ابعاد محیط عملیاتی و لحاظ کردن محیط عملیات سایبری به‌عنوان بخشی از محیط عملیاتی در مقابله با عملیات سایبری تهاجمی ارتش امریکا که با کسب میانگین ۴,۴۸ از نظر صاحب‌نظران حائز دومین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است.۸۹٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.

۳. ارائه آموزش‌های لازم در حوزه امنیت و دفاع سایبری متناسب با تهدید، در تمامی سطوح (مدیران سازمانی، مدیران شبکه و کاربران سامانه‌ها) که با کسب میانگین ۴,۴۳ از نظر صاحب‌نظران حائز سومین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۸۴٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.

۴. تشکیل، تقویت و به‌روزرسانی مراکز عملیات امنیت در آجا به‌منظور رصد رخدادهای امنیتی که با کسب میانگین ۴,۳ از نظر صاحب‌نظران حائز چهارمین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۸۶٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.
۵. شبیه‌سازی اقدامات تهاجمی وزارت دفاع امریکا از طریق انجام رزمایش‌های سایبری که با کسب میانگین ۴,۱۵ از نظر صاحب‌نظران حائز پنجمین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۶۴٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.
۶. اجرایی کردن نظامات پدافند غیرعامل سایبری کشور با رویکرد مصون‌سازی فضای سایبری آجا که با کسب میانگین ۴,۱۵ از نظر صاحب‌نظران حائز ششمین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۸۰٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.
۷. تشکیل، تقویت و به‌روزرسانی مستمر گروه‌های "آپا" در رده‌های مختلف در سطح آجا که با کسب میانگین ۴,۰۵ از نظر صاحب‌نظران حائز هفتمین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۷۷٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.
۸. طراحی و پیاده‌سازی سازوکار مناسب برای رصد مستمر آخرین وضعیت و اقدامات سایبری امریکا به‌منظور کشف و شناسایی طرح‌ها و روش‌های تهاجمی که با کسب میانگین ۴ از نظر صاحب‌نظران حائز هشتمین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۷۷٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا مفید است.

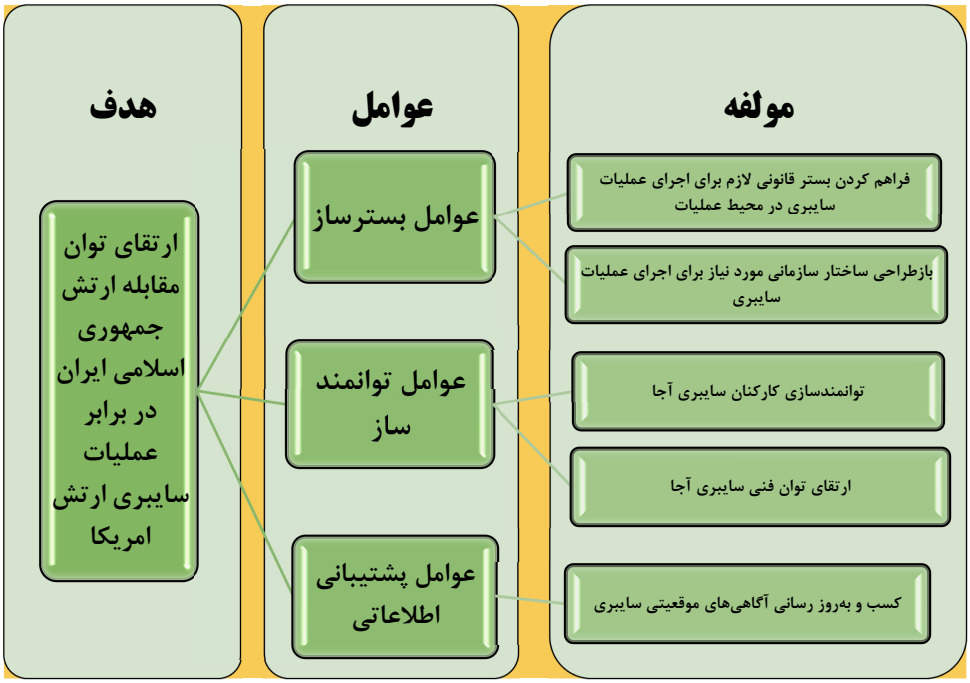
✓ نتایج به‌دست‌آمده از تحلیل کیفی و کمی، در خصوص دستیابی به هدف شناسایی راه‌های مقابله ارتش جمهوری اسلامی ایران با عملیات شبکه اطلاعاتی وزارت دفاع امریکا

تعداد ۲ شاخص از شاخص‌های موردبررسی قرارگرفته با میانگین بیش از ۴، به شرح زیر، به‌عنوان اقدامات دارای اولویت در راستای ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات شبکه اطلاعاتی وزارت دفاع امریکا احصاء گردید:

۱. تقویت توان فنی سایبری تهاجمی خودی در هر دو حوزه حمله سایبری و بهره‌گیری سایبری به‌منظور انجام اقدامات تهاجمی علیه شبکه اطلاعاتی وزارت دفاع امریکا که با کسب میانگین ۴,۴ از نظر صاحب‌نظران حائز بالاترین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات سایبری تهاجمی ارتش امریکا شده است. ۸۷٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات شبکه اطلاعاتی وزارت دفاع امریکا مفید است.

۲. راه‌اندازی، تقویت و هدایت نهادهای مسئول رصد و پایش اقدامات امنیتی سایبری به‌منظور شناسایی و جمع‌آوری اطلاعات مرتبط که با کسب میانگین ۴,۰۲ از نظر صاحب‌نظران حائز دومین اولویت در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات شبکه اطلاعاتی وزارت دفاع امریکا شده است. ۷۱٪ از جامعه آماری معتقد بودند که این شاخص به میزان خیلی زیاد و زیاد در ارتقای توان مقابله ارتش جمهوری اسلامی ایران با عملیات شبکه اطلاعاتی وزارت دفاع امریکا مفید است.

با در نظر گرفتن موارد اشاره‌شده بالا می‌توان استنباط کرد که بر اساس ادبیات پژوهش و نیز نظر صاحب‌نظران، ارتقای توان مقابله ارتش جمهوری اسلامی ایران در برابر عملیات سایبری ارتش امریکا، می‌تواند در قالب چارچوب مفهومی زیر انجام شود.



نمودار ۰(۱): چارچوب مفهومی ارتقای توان مقابله ارتش جمهوری اسلامی ایران در برابر عملیات سایبری ارتش امریکا

منابع

- ابوالحسینی، علیرضا (۱۳۹۲). *معرفی و برآورد تهدیدات سایبری*. تهران: انتشارات دیده‌بان.
- فرح بخت، احمدرضا و دهقانی، مهدی (۱۳۹۸). همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی. *فصلنامه امنیت ملی*، ۹ (۳۱): ۶۵-۳۴.
- ناصری، علی، ریاضی، عبدالمجید (۱۳۸۷). *جنگ اطلاعات (چگونه از حملات سایبری درامان باشیم)*. تهران: انتشارات دانشگاه عالی دفاع ملی.
- Department Of Defense (2012), *Sustaining U.S. Global Leadership: Priorities For 21st Century*, Washington, DoD.
- Department Of Defense (2013), *JP 3-12 [R], Cyberspace Operation*, Washington, DoD.
- Department Of Defense (2015), *The Department Of Defense Cyber Strategy*, Washington, DoD.
- Department Of Defense (2018), *JP 3-12, Cyberspace Operation*, Washington, DoD.
- Department Of The Army, (2017), *FM 3-12, Cyberspace And Electronic Warfare Operations*, Washington, Department Of The Army.
- Mudrinich, E. M. (2012). *Cyber 3.0: The department of defense strategy for operating in cyberspace and the attribution problem*. AFL Rev., 68, 167.
- Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.
- The White House,(2015), *U.S. National Security Strategy*, Washington,The White House.
- The White House,(2018), *The National Cyber Strategy Of The United States Of America*, Washington,The White House.
- Theohary, Catherine ,(2015), *Cyber Operations In DOD Policy And Plans*: Issues For Congress, USA, Congressional Research Service .
- Wilson E. Burke (Major General), (2015), *Military Cyber Programs and Posture, Presentation To The Senate Armed Services Committee Subcommittee On Emerging Threats And Capabilities United States Senate*, Washington, 24th Air Force.