فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره۳، تابستان ۱۴۰۱
مقاله سوم، از صفحات ۶۹-۸۸

مقاله پژوهشی:

ارائه الگوی مفهومی برای دفاع سایبری ملی

هانی رحیم‌اف[۱]، محمدرضا موحدی‌صفت[۲]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۰ **تاریخ پذیرش:** ۱۴۰۰/۱۰/۱۶

چکیده

امروزه حملات و تهدیدات سایبری نسبت به گذشته با تأثیر و پیچیدگی بیشتری به انجام می‌رسند. بر این اساس راهکارهای دفاع سایبری نیز متنوع‌تر شده و علاوه بر رویکرد پدافندی، به سمت حذف تهدید رفته است. ازآنجاکه ایجاد هرگونه نظام کارآمد دفاع سایبری مستلزم طراحی الگوی مفهومی آن بوده و تنوع روش‌های دفاعی و تفاوت اجرایشان چشم‌گیر است؛ پژوهشگران را بر آن داشته تا با ارائه الگوی مفهومی دفاع سایبری، راهکارهای موجود در دنیا را با نگاه کلان به فضای سایبر و در تعامل با یکدیگر بررسی نموده و دسته‌بندی نوین و جامعی را در این خصوص ارائه نمایند.

تحقیق حاضر به‌صورت توصیفی و از نوع توسعه‌ای- کاربردی است. پژوهشگران با استفاده از روش کتابخانه‌ای، مبانی نظری را بررسی نموده و با به‌کارگیری روش عقلایی و انجام مصاحبه عمیق با خبرگان به الگوی مفهومی دفاع سایبری دست‌یافته‌اند. در تحقیق حاضر، روش‌های دفاعی پیش‌کنشانه، پیشگیرانه، پیش‌دستانه، پیش‌بینانه، فعال، واکنشی، به‌کارگیری سامانه و تجهیزات امنیتی و فریب، نصب وصله‌های امنیتی، هشداردهی و آگاه‌سازی امنیتی، ایمن‌سازی اطلاعات و ارتباطات، وضع سیاست امنیتی، قطع ارتباطات مشکوک، جلوگیری از تداوم و گسترش حمله، جرم‌یابی و برطرف نمودن آسیب‌پذیری‌ها، در دو بخش دفاع سایبری عامل و غیرعامل بررسی‌شده و با شاخص‌گذاری حمله، به پیش، حین و پس از حمله سایبری تقسیم‌بندی شده‌اند.

کلیدواژه‌ها: دفاع سایبری، الگوی مفهومی، دفاع عامل سایبری، دفاع غیرعامل سایبری

۱. دانش‌آموخته دکترای دانشگاه عالی دفاع ملی – نویسندهٔ مسئول h.rahimov۹۸@sndu.ac.ir
۲. دانشیار دانشگاه عالی دفاع ملی – movahedi۲۵@sndu.ac.ir

مقدمه

گستردگی و سهولت دسترسی به شبکه اینترنت باعث شده است، هرساله بر تعداد افراد بهره‌بردار آن اضافه شود. با ایجاد و گسترش اینترنت اشیاء مخاطرات آن نیز روند افزایشی داشته است. تعداد دستگاه‌های متصل به اینترنت در سال ۲۰۱۲ از ۸.۸ میلیارد دستگاه به ۲۰.۱ میلیارد دستگاه در سال ۲۰۱۷ رسیده و پیش‌بینی می‌شود که این آمار در سال ۲۰۲۵ به ۷۵.۳ میلیارد دستگاه برسد (اروارل[۱], ۲۰۱۸, ص. ۲۷۰). با افزایش ضریب نفوذ اینترنت بر تعداد حملات سایبری نیز افزوده شده است. سال‌هاست که دولت‌ها به‌منظور دفاع سایبری و امن‌سازی زیرساخت خود، هزینه قابل‌توجهی را مصرف می‌کنند؛ اما همچنان کسب‌وکارها و زیرساخت‌های دولتی به‌طور مکرر هدف حملات سایبری قرار می‌گیرند. بر اساس گزارش سال ۲۰۲۰ آژانس امنیت سایبری اتحادیه اروپا[۲] در بازه زمانی ژانویه ۲۰۱۹ تا آوریل ۲۰۲۰ به‌طور متوسط روزانه ۲۳۰۰۰۰ بدافزار جدید تولید شده است. ٦۰ درصد حملات سایبری، جرائم سازمان‌دهی شده بوده و ١٦ درصد آن‌ها مرتبط با دولت‌ها می‌باشد؛ همچنین اطلاعات طبقه‌بندی شده نظامی و دولتی دومین هدف جرائم سایبری در این مدت بوده‌اند (انیسا[۳], ۲۰۲۰, صص. ۹–۱۵).

حملات سایبری در دهه ۸۰ میلادی ترکیب و پیچیدگی ساده‌ای داشت؛ اما رفته‌رفته پیچیدگی آن‌ها افزایش یافت تا در دهه ۲۰۱۰ شاهد نسل جدیدی از حملات باشیم و پیش‌بینی می‌شود حملات سایبری در دهه ۲۰۲۰ به حملات با سطح راهبردی تبدیل شوند (اروارل, ۲۰۱۸, ص. ۲۷٦)؛ درواقع پشتیبانی دولتی از حملات سایبری باعث پیچیدگی زیاد حملات شده و دفاع سایبری را نیز سخت‌تر از گذشته نموده است. دولت‌ها جهت رسیدن به اهداف خود و پرهیز از تبعات جنگ فیزیکی، اقدام به انجام حملات سایبری نموده و در عین دستیابی به هدف خود، با بهره‌گیری از ویژگی‌های فضای سایبر و به‌کارگیری روش‌های پیچیده تلاش می‌نمایند تا هویتشان را نیز مخفی نمایند، حتی در حملاتی که بر اساس ادله فنی، هویت عاملین حمله اثبات شود، نیز

---

۱. Ervural
۲. The European Union Agency for Cybersecurity (ENISA)
۳. Enisa

دولت‌ها دست داشتن خود در حملات را انکار می‌نمایند. ضعف قوانین بین‌المللی در جلوگیری، اثبات و برخورد با حملات سایبری نیز باعث شده است تا دولت‌ها تلاش نمایند با ایجاد و تربیت نیروی متخصص تهاجم سایبری و تولید تسلیحات گوناگون سایبری، قدرت تهاجم سایبری‌شان را بدون بر جای گذاشتن هرگونه رد پا تقویت نمایند. «امروزه، افراد بسیاری جنگ سایبری را یکی از ارکان چنگ‌ها در امروز و آینده می‌دانند؛ بنابراین باید سازوکاری را برای مقابله با تهاجمات پیش رو دنبال کرد.» (تقی‌پور ، اسماعیلی, ۲۰۱۹, صص.۲-۳) جمهوری اسلامی ایران نیز همواره از قربانیان حملات سایبری بوده است. حملات سایبری علیه کشور به حدی جدی بوده که «پس از حمله استاکس‌نت علیه تأسیسات هسته‌ای ایران، حتی برخی از کشورهای پیشروی سایبری نیز در ساختار دفاع سایبری خود تجدیدنظر نمودند» (دنینگ , ۲۰۱۲, ص. ۱۱).

در شرایطی که حمله سایبری از دیدگاه برخی از کشورها به‌عنوان حمله نظامی تلقی و زمینه‌های جدی جنگ‌های فیزیکی نظامی را فراهم خواهد نمود و در این خصوص نیز مراکز دفاع سایبری پیشرفته‌ای راه‌اندازی شده است؛ به‌روشنی می‌توان دریافت که جنگی جدی در فضای سایبر در حال شکل‌گیری است. جنگی که به‌شدت زیرساخت‌های سایبری و غیر سایبری کشور را در تمامی ابعاد تهدید می‌کند؛ ازاین‌رو اهمیت دفاع سایبر با نگاه راهبردی بیش از هر موضوع دیگری خودنمایی می‌کند (مقدسی لیچاهی و همت, ۱۳۹۷, ص .۲). پیشرفته شدن حملات سایبری باعث شده است تا راه‌حل‌های دفاعی نیز پیشرفت نموده و فراتر از راهکارهای گذشته عمل نمایند. ازآنجایی‌که روش‌ها و فناوری‌های کنونی حمله سایبری پیچیده‌تر و مداوم‌تر شده است، سامانه‌های تشخیص و شناسایی متعارف برای دفاع سایبری کارآمد نبوده و در مواقع خطر، امنیت لازم را برای رویدادهای بحرانی فراهم نمی‌کنند (باقری و همکاران، ۱۳۹۶, ص. ۲). هرچند درگذشته رویکرد دفاع سایبری عموماً بر امن‌سازی و رفع آسیب‌پذیری‌های داخلی تمرکز داشته؛ اما امروزه نگاه کل‌نگرانه‌ای نسبت به روش‌های دفاعی شکل‌گرفته که تنها بر نگاه به محیط داخل متمرکز نبوده و بر حذف تهدید سایبری نیز توجه دارد. پیشرفت دفاع سایبری و تنوع روش‌ها و راهکارهای آن باعث شده است، تا نیاز به الگوی مفهومی دقیق و علمی که تمامی جنبه‌های دفاعی در آن مدنظر قرارگرفته باشد؛ بیش از پیش احساس گردد. به‌وسیله الگوی مذکور می‌توان

به‌صورت کل‌نگرانه و به‌طور جامع به دفاع سایبری پرداخت و علاوه بر اجتناب از مغفول ماندن برخی روش‌ها، می‌توان تمامی راهکارهای دفاعی را در ساختاری چندلایه به‌کارگیری نمود. پژوهشگران در این مقاله در تلاش‌اند تا با گردآوری روش‌های دفاع سایبری در لایه‌های فیزیکی و اطلاعاتی فضای سایبر و بررسی آن‌ها در تعامل با یکدیگر، دسته‌بندی جدیدی را در قالب الگوی مفهومی دفاع سایبری که دربرگیرنده تمامی راهکارهای دفاعی است، ارائه نماید؛ تا بر اساس آن متولیان دفاع سایبری بتوانند، به‌طور جامع‌نگرانه وظایف خود را به انجام برسانند. پیاده‌سازی دفاع سایبری چندلایه و همه‌جانبه باعث خواهد شد تا مهاجمان سایبری در اجرای حملات خود ناکام مانده و از تهاجمات آتی منصرف و دلسرد گردند؛ درنتیجه تهدیدات سایبری کاهش‌یافته و پیامد آن افزایش قدرت سایبری کشور خواهد بود.

تعاریف

عملیات سایبری[۱]: وزارت دفاع آمریکا، عملیات سایبری را به‌کارگیری فضای سایبر باهدف اصلی دستیابی به اهداف در این فضا یا از طریق آن تعریف می‌کند(DoD JP ۳-۰, ۲۰۱۸, p. GL-۸). بر اساس دستورالعمل شماره ۲۰ سیاست اجرایی رئیس‌جمهور آمریکا، عملیات سایبری به‌عنوان مجموعه‌ای از عملیات جمع‌آوری سایبری، عملیات سایبری تدافعی و عملیات سایبری تهاجمی تعریف‌شده است (کاخ سفید[۲], ۲۰۰٤, ص. ۳)؛ اما بر اساس تعریف جدید وزارت دفاع آمریکا، مأموریت‌های مربوط به فضای سایبری شامل: عملیات سایبری تهاجمی، عملیات سایبری تدافعی و عملیات شبکه اطلاعاتی وزارت دفاع می‌باشد (DoD JP ۳-۱۲, ۲۰۱۸, p. x). ناتو نیز عملیات سایبری را این‌گونه تعریف می‌کند که:«انجام اقدامات در یا از طریق فضای سایبری برای حفظ آزادی عمل دوستانه در فضای سایبری و / یا ایجاد اثر برای دستیابی به اهداف فرماندهان می‌باشد» (AJP-۳,۲۰, ۲۰۲۰, □. ٤).

۱. cyberspace operations
۲. The White House

عملیات تدافعی سایبری[۱]: مأموریت‌هایی برای حفظ توانایی جهت بهره‌برداری از قابلیت‌های دوستانه فضای سایبر و محافظت از داده‌ها، شبکه‌ها، دستگاه‌های موجود در فضای سایبر یا سایر سامانه‌هایی که جهت حفاظت از شکست امنیتی یا جلوگیری از فعالیت‌های قریب‌الوقوع مخرب سایبری طراحی‌شده‌اند، می‌باشد (DoD JP ۳-۱۲, ۲۰۱۸, p. GL-٤). در تعریفی دیگر، عملیات و فعالیت‌ها و برنامه‌های مرتبط (غیر از دفاع شبکه‌ای یا جمع‌آوری سایبری) که توسط دولت آمریکا یا با مجوز دولت در فضای سایبر به‌منظور ایجاد پیامدهای سایبری در خارج از شبکه‌های دولتی آمریکا با هدف دفاع یا محافظت در برابر تهدیدات قریب‌الوقوع یا حملات جاری یا فعالیت‌های مخرب سایبری، علیه منافع ملی در درون یا بیرون از فضای سایبری انجام می‌شود، به‌عنوان عملیات سایبری تدافعی نامیده می‌شود (کاخ سفید, ۲۰۰٤, ص. ۳). ناتو نیز عملیات تدافعی سایبری را این‌گونه تعریف می‌نماید که: «اقدامات دفاعی در یا از طریق فضای سایبری برای حفظ آزادی عمل دوستانه در فضای سایبری است»(AJP-۳,۲۰, ۲۰۲۰, p. ٤).

عملیات تهاجمی سایبری[۲]: عملیاتی است که برای قدرت‌نمایی با به‌کارگیری قدرت در یا از طریق عرصه سایبری انجام می‌شود و مجموعه اقدامات متنوعی را در فضای سایبری در برمی‌گیرد؛ این اقدامات شامل حملات انکار سرویس (مثل تنزل کیفیت سرویس، قطع سرویس و یا تخریب کامل سرویس) و حملات دست‌کاری اطلاعات هستند که بعضاً یا مخفی مانده، یا پیامدهای آن‌ها در عرصه‌های فیزیکی ظاهر می‌شوند. در حقیقت هدف حمله سایبری ایجاد مزیت نسبی در عرصه سایبری یا دیگر عرصه‌های فیزیکی برای نیروهای خودی با به‌کارگیری توان رزم سایبری است (ویلیامز[۳], ۲۰۱٤, ص. ۱۹). عملیات تهاجمی سایبری عملیاتی است که برای اعمال قدرت با استفاده از زور در فضای سایبر یا از طریق آن، انجام می‌شود. (DoD JP ۳-۱۲, ۲۰۱۸, p. GL-٥) عملیات [تهاجمی] سایبری با درجه بالایی از گمنامی و انکارپذیری قابل‌قبول، همراه بوده و نتایج حاصل از آن عموماً نامشخص است که شامل طیف وسیعی از گزینه‌ها و نتایج احتمالی می‌شود؛ همچنین ممکن است در مقیاس زمانی از دهم ثانیه تا چندین سال به طول بیانجامد

۱. defensive cyberspace operations
۲. offensive cyberspace operations
۳. Williams

(اسمیتز و ورک[1]، ۲۰۲۰، ص. ۲). بر اساس دستورالعمل شماره ۲۰ سیاست اجرایی رئیس‌جمهور آمریکا، عملیات و برنامه‌ها و فعالیت‌های مرتبط (غیر از دفاع شبکه‌ای، جمع‌آوری سایبری و عملیات سایبری تدافعی) چه توسط دولت آمریکا یا با مجوز دولت در فضای سایبری باهدف ایجاد آثار سایبری در خارج از شبکه‌های دولتی آمریکا انجام شود؛ به‌عنوان عملیات سایبری تهاجمی تعریف می‌گردد.(کاخ سفید، ۲۰۱٤، ص. ۳) ناتو عملیات تهاجمی سایبری را اقداماتی در یا از طریق فضای سایبری که قدرت ایجاد اثراتی را برای دستیابی به اهداف نظامی طرح‌ریزی می‌کند؛ می‌داند(AJP-۳,۲۰, ۲۰۲۰, p. ٤).

حمله سایبری[2]: یک اقدام سایبری است که تأثیرات مختلف – مانند کاهش، قطع، تخریب یا دست‌کاری– برای منع استفاده از فضای سایبر ایجاد می‌کند و می‌تواند به‌صورت پنهان یا آشکار در قلمروهای فیزیکی صورت گیرد (DoD JP ۳-۱۲, ۲۰۱۸, p. GL-٤).

دفاع سایبری[3]: شامل اقداماتی است که معمولاً درون فضای سایبر وزارت دفاع برای امن‌سازی، عملیاتی‌سازی و دفاع از شبکه اطلاعاتی وزارت دفاع در برابر تهدیدات خاص انجام می‌گیرد. اهداف دفاع سایبری شامل اقدامات جلوگیری، آشکارسازی، تشخیص، مقابله و کاهش تأثیرات تهدیدات است (DoD JP ۳-۱۲, ۲۰۱۸, p. GL-٤).

مبانی نظری و پیشینه پژوهش

بر اساس تعریف جدید وزارت دفاع آمریکا، مأموریت‌های مربوط به فضای سایبری شامل عملیات سایبری تهاجمی، عملیات سایبری تدافعی و عملیات شبکه اطلاعاتی وزارت دفاع است(DoD JP ۳-۱۲, ۲۰۱۸, p. x)؛ اما ناتو در این تقسیم‌بندی با ایالات‌متحده موافق نبوده و عملیات سایبری را تنها بر دو قسمت تهاجمی و تدافعی طبقه‌بندی نموده است (AJP-۳,۲۰, ۲۰۲۰, p. ۱٦).

در سند عملیات سایبری سال ۲۰۱۳ وزارت دفاع آمریکا، عملیات سایبری تدافعی به دو بخش زیر تقسیم شده است:(DoD JP ۳-۱۲, ۲۰۱۳, p. ۲٤)

---

۱. Smeets, M. & Work
۲. cyberspace attack
۳. cyberspace defense

- عملیات در داخل شبکه وزارت دفاع [غیرعامل] که شامل کشف تهدیدات داخلی پیشرفته و پاسخ‌های داخلی به این تهدیدها هستند.
- عملیات در خارج از شبکه‌های وزارت دفاع [عامل] که شامل اقدامات دفاعی جهت از بین بردن تهدیدهای مداوم یا قریب‌الوقوع بوده و ممکن است تا سطح استفاده از نیرو نیز پیش رود؛ اما همانند حوزه‌های فیزیکی، تأثیر اقدامات متقابل محدود بوده و معمولاً فعالیت‌های دشمن را بجای شکست، کاهش می‌دهد.

در سند عملیات سایبری سال ۲۰۱۹ وزارت دفاع آمریکا، در خصوص عملیات تدافعی سایبری این‌گونه بیان‌شده است که باهدف اصلی دفع تهدید جاری و یا بازگرداندن یک شبکه در معرض خطر به شرایط امنیتی و کارکرد عادی انجام می‌شود؛ همچنین تأکید شده است که یک ویژگی کلیدی فعالیت‌های عملیات سایبر تدافعی وزارت دفاع، دفاع عامل سایبری است. بر اساس این سند، عملیات تدافعی سایبری به سه بخش ذیل تقسیم‌بندی می‌شود (DoD JP ۳-۱۲, ۲۰۱۸, pp. ۳۷–۳۹).

۱- اقدامات دفاعی داخلی عملیات سایبری تدافعی: طی آن فعالیت‌های دفاعی مجاز در یک بخش یا شبکه دفاع شده انجام می‌شود؛ این اقدامات شامل فعالیت‌های دفاعی پویای سایبری، جهت حفظ یا برقراری مجدد امنیت فضای در معرض تهدید سایبری وزارت دفاع، به‌منظور حصول اطمینان از دسترسی –برای انجام مأموریت‌های نظامی– به فضای سایبر است. اغلب مأموریت‌های عملیات سایبری تدافعی از نوع اقدامات داخلی هستند که شامل ردیابی تهدیدات تجاری و پیشرفته تهاجمی داخلی در کنار اقدامات عامل و فعالیت‌های ضد تهدید داخلی واکنشی، برای مقابله با تهدیدات و کاهش اثرات مخرب آن‌ها است؛

۲- فعالیت‌های واکنشی عملیات سایبری تدافعی: این فعالیت‌ها در خارج از شبکه یا بخش دفاع شده فضای سایبر انجام می‌شوند و عموماً بدون کسب اجازه از مالک سامانه یا شبکه تحت تأثیر قرارگرفته‌شده، صورت می‌پذیرند. بعضی از مأموریت‌های واکنشی عملیات سایبری تدافعی شامل اقداماتی است که منجر به استفاده از نیرو برای تخریب یا انهدام فیزیکی دشمن –بسته به سطح مأموریت– می‌شوند؛ البته برای این‌گونه مأموریت‌ها نیاز به دستور صریح نظامی و

ملاحظات دقیق در سطوح مأموریت می‌باشد. فعالیت‌های واکنشی عملیات سایبری تدافعی – همانند عملیات سایبری تهاجمی– نیازمند جمع‌آوری اطلاعاتی برای کسب اطلاعات تهدید است؛ این فعالیت‌ها ممکن است، شامل استفاده از اقدامات مقابله‌ای غیر مخرب باشد. بر این اساس، منبع تهدید شناسایی‌شده و از تکنیک‌های غیر نفوذی برای مقابله با کاهشی تهدید استفاده می‌شود. نیروهای مشترک می‌توانند پشتیبانی از فعالیت‌های واکنشی عملیات سایبری تدافعی را به فرماندهان رزمی در رده‌های تیپ و پایین‌تر بسپارند؛

۳– دفاع از فضای سایبری غیر وزارت دفاع: در این قسمت، فعالیت‌های وزارت دفاع به بخش‌های متعدد خارج از وزارت دفاع –شامل بخش‌های خصوصی و شبکه‌های همکار مأموریتی– متکی است. حفاظت از این شبکه‌ها و سامانه‌های خارج از وزارت دفاع می‌تواند عنصری حیاتی در تضمین موفقیت مأموریت باشد؛ بنابراین در صورت لزوم با هماهنگی کامل با وزارت امنیت داخلی آمریکا و سایر وزارتخانه‌ها و نهادهای مرتبط، نیروهای سایبری وزارت دفاع می‌توانند فعالیت‌های واکنشی و اقدامات داخلی دفاعی عملیات سایبری تدافعی را به‌منظور دفاع از این نهادها یا سایر بخش‌های سایبری خارج از وزارت دفاع انجام دهند.

با توجه به مطالب فوق‌الذکر؛ هرچند مأموریت‌های وزارت دفاع آمریکا در سند ۲۰۱۹ نسبت به سند ۲۰۱۳ تکمیل‌شده است؛ اما عملیات سایبری تدافعی را به دو بخش اقدامات عامل و غیرعامل در حوزه فضای سایبری تقسیم‌بندی نماید.

در سند راهبرد سایبری وزارت دفاع آمریکا –که در سال ۲۰۱۸ منتشر گردید– بیان‌شده است که: «ما به‌منظور مقابله یا ضربه زدن به فعالیت‌های مخرب سایبری، اقدام به دفاع در خط مقدم تهدید[۱] خواهیم نمود.» (راهبرد سایبری وزارت دفاع آمریکا[۲], ۲۰۱۸, ص. ۱) در این سند یکی از اقسام دفاع در خط مقدم تهدید، عملیات سایبری پیش‌کنشانه[۳] نامیده شده است.

آخرین سند دکترین عملیات سایبری ناتو بیان می‌دارد که عملیات سایبری تدافعی می‌تواند شامل ارزیابی آسیب‌پذیری، مدیریت ریسک و اقدامات ممکن جهت پاسخ در راستای نیازهای

۱. Defend Forward
۲. DoD Cyber Strategy
۳. Proactive Defense

عملیاتی باشد؛ این اقدامات می‌تواند اثرات سایبری حاکمیتی بر متحدان ایجاد نماید و چالش هماهنگی فضای سایبری را برای فرمانده ایجاد کند (AJP-۳,۲۰, ۲۰۲۰, p. ۱۷) از مطالب ناتو چنین برداشت می‌شود که عملیات سایبری تدافعی را به دفاع عامل و غیرعامل تقسیم‌بندی می‌نماید.

در مقاله (اسمیتز[۱], ۲۰۲۰) ضمن دسته‌بندی فضای سایبر به مناطق آبی، خاکستری و قرمز، برای ایالات‌متحده آمریکا این حق را قائل شده است که در هر سه منطقه، حضور فعال داشته و حتی بتواند بر اساس قانون داخلی آمریکا و بدون هماهنگی با کنگره، جهت مقاصد دفاعی، عملیات تخریبی سایبری انجام دهد. ژنرال ناکاسون[۲] - فرماندهی سایبری آمریکا و به‌طور همزمان مدیر آژانس امنیت ملی و رئیس سرویس امنیت مرکزی ایالات‌متحده که پیش از این نیز فرماندهی سایبری ارتش آمریکا را عهده‌دار بوده است– در مقاله‌ای می‌نویسد: اگر ما تنها در «فضای آبی» دفاع کنیم بازنده خواهیم بود. در عوض ما باید به‌صورت یکپارچه در فضای داخلی به‌هم‌پیوسته جهانی تا حد ممکن به مخالفان و عملیات آن‌ها نزدیک شویم و به‌طور مداوم فضای جنگ را شکل دهیم تا مزیت عملیاتی برای خودمان ایجاد و از دشمنانمان سلب کنیم (اسمیتز, ۲۰۲۰, صص. ۱–۲).

مقاله (گوتالز و هانت[۳], ۲۰۱۹) نیز به صراحت عملیات دفاعی سایبری را به دو بخش عامل و غیرعامل تقسیم‌بندی می‌کند (گوتالز و هانت, ۲۰۱۹, ص. ۱).

یکی از رویکردهای دفاع عامل، دفاع پیش‌کنشانه است. تمایل زیادی جهت حرکت به سمت این رویکرد وجود دارد. در دفاع پیش‌کنشانه، پیش از اینکه رخدادهای امنیتی آسیبی وارد نمایند، از آن‌ها جلوگیری شده یا از شدت تأثیر آن‌ها کاسته می‌شود. راهکار این رویکرد استفاده از اطلاعات تهدیدات سایبری، آگاهی وضعیتی سایبری، همکاری و اشتراک‌گذاری اطلاعات و سایر روش‌های مستخرج از تحقیق و توسعه است (هوساک و همکاران[۴], ۲۰۲۱، ص. ۱).

۱. Smeets
۲. Paul M. Nakasone
۳. Goethals & Hunt
۴. Husák et al.

در چاپ دوم کتاب (استرند و همکاران[۱]، ۲۰۱۷) به دفاع عامل سایبری در حین انجام حمله سایبری و پیش از اتمام آن پرداخته‌شده و آن را دفاع فعال[۲] نامیده است. در این کتاب برای انجام دفاع فعال، از سه مرحله آزار[۳] جهت اتلاف وقت مهاجم، انتساب[٤] جهت شناسایی منشأ اصلی حمله و دور زدن راهکارهای گمنام‌سازی مهاجم و حمله[٥] به‌منظور نفوذ معکوس به سیستم مهاجم نام‌برده شده و به‌تفصیل به آن پرداخته است؛ همچنین از تله سایبری[٦] به‌عنوان زیرساخت موردنیاز دفاع فعال نام‌برده شده است (استرند و همکاران، ۲۰۱۷؛ صص. ٢٤–١٣٤).

بخشی از مقاله (روفل و همکاران[۷]، ۲۰۱٤) به نقش گروه‌های آپا[۸] یا CSIRT[۹] در دفاع غیرعامل سایبری قبل، حین و پس از تهاجم سایبری پرداخته است و خدمات واکنشی این گروه‌ها را هشداردهی، رسیدگی به حادثه، رسیدگی به آسیب‌پذیری و رسیدگی به رویداد نامیده است (روفل و همکاران، ۲۰۱٤, ص. ۲۰).

بر اساس مطالب بیان‌شده، هر یک از بخش‌های عامل و غیرعامل دفاع سایبری را می‌توان به سه قسمت پیش، حین و پس از حمله سایبری دسته‌بندی نمود.

در مقاله (رمضان زاده، ۱۳۹۹) نیز پنج مانع در مسیر دفاع سایبری شمرده‌شده است؛ که عبارتند از: «غیرقابل‌پیش‌بینی و غیرقابل‌کشف بودن حمله، انکار نتایج دفاع به‌دلیل محدود بودن آن در فضای سایبر، وجود سطوح پیچیده دفاع، چند تکه شدن دفاع بین بخش خصوصی و دولتی که باعث پیچیده‌تر شدن یکپارچگی دفاع می‌شود؛ درنهایت ریسک‌های زنجیره تأمین در دنیای کنونی هیچ کشوری زنجیره تأمین اقلام سایبری خود را به‌صورت کامل در دست نداشته و ضروری است تا بخشی از این تجهیزات، از خارج از کشور تأمین شوند. در هر مرحله این

۱. Strand et al.
۲. Active Defense
۳. Annoyance
٤. Attribution
٥. Attack
٦. Honeypot
۷. Ruefle et al.
۸. آگاهی، پشتیبانی، امداد
۹. Computer Security Incident Response Team

زنجیره تأمین، سازمان‌های اطلاعاتی خارجی می‌توانند بخشی از سیستم‌ها را بدون اطلاع کشور هدف آلوده کرده و در نتیجه بدافزارهای موردنظر را وارد شبکه نمایند»(رمضان‌زاده ، ۱۳۹۹، صص. ۳-٤).

روش‌شناسی پژوهش

این تحقیق به‌صورت توصیفی و موردی- زمینه‌ای انجام می‌شود. از این‌جهت توصیفی است که برای گردآوری اطلاعاتی که مدون نشده به‌کار می‌رود و با این روش، توصیف عینی، واقعی و منظم موضوعات انجام می‌گردد. از این‌جهت موردی- زمینه‌ای است که در این مقاله، مطالعه عمیق روی نمونه‌هایی از یک پدیده در محیط واقعی صورت می‌گیرد.

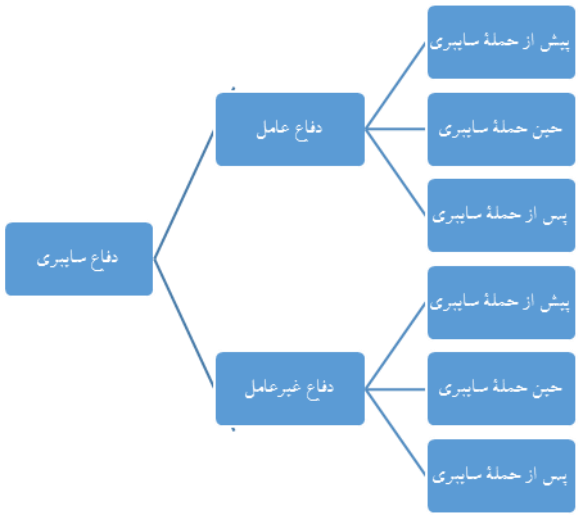
همچنین ازآنجا که در این پژوهش پژوهشگران درصدد بوده‌اند تا با استفاده از روش‌های علمی الگوی مفهومی دفاع سایبری را ارائه نمایند؛ پژوهش حاضر از نوع کاربردی بوده و در زمینه شناخت الگوی مفهومی دفاع سایبری، توسعه‌ای خواهد بود؛ بنابراین توسعه‌ای- کاربردی است.

در این تحقیق، پژوهشگران با استفاده از روش کتابخانه ادبیات نظری را جمع‌آوری نموده و با به‌کارگیری روش عقلایی و انجام مصاحبه عمیق با خبرگان دفاع سایبری، اطلاعات و داده‌های موردنیاز را جمع‌آوری کرده‌اند. به‌منظور اخذ نظر خبرگان جهت ارائه الگوی مفهومی پژوهش، مصاحبه عمیق با جامعه آماری صورت پذیرفت. با توجه به جدول مورگان و فرمول کوکران، انجام مصاحبه به‌صورت تمام‌شمار تا رسیدن به اشباع نظری ادامه یافت. ویژگی مشترک جامعه آماری، علاوه بر داشتن مدرک کارشناسی‌ارشد یا دکترا در رشته‌های مرتبط با تحقیق، داشتن حداقل ۱۰ سال سابقه مدیریتی در سطوح راهبردی یا عملیاتی دفاع سایبری نیز می‌باشد.

یافته‌های پژوهش

با توجه به اینکه محور اصلی دفاع سایبری، دفاع در برابر حملات سایبری است؛ بر اساس نظر خبرگان، دفاع سایبری به سه بخش پیش از حمله سایبری، حین حمله سایبری و پس از حمله سایبری تقسیم‌بندی می‌شود. از سویی طبق یافته‌های بخش مبانی نظری، دفاع سایبری به دو

قسمت عامل و غیرعامل دسته‌بندی می‌گردد؛ این دسته‌بندی‌ها شش ناحیه را مطابق شکل ۱ مشخص می‌کنند.



شکل ۱) افراز دفاع سایبری

دفاع عامل سایبری – پیش از حمله سایبری

هدف دفاع عامل پیش از حمله سایبری، از بین بردن تهدیدات از طریق انجام عملیات سایبری است؛ درواقع به تهدید سایبری اجازه بالفعل شدن داده نشده و با آن مقابله می‌شود. به نظر می‌رسد دفاع در خط مقدم تهدید که استراتژی اصلی آمریکا در سند عملیات سایبری ۲۰۱۸ وزارت دفاع این کشور است و در سخنان مقامات مسئول آمریکایی، بارها بر آن تأکید شده است؛ دربرگیرنده تمامی انواع دفاع عامل پیش از حمله سایبری است؛ این نوع از دفاع سایبری به زیر بخش‌های ذیل تقسیم‌بندی می‌شود:

- دفاع سایبری پیش‌کنشانه[۱]: در این نوع دفاع سایبری، احتمال حمله سایبری فوری و قریب‌الوقوع دشمن وجود دارد؛ اما این احتمال به قطعیت تبدیل نشده است. در این نوع دفاع، دو عنصر احتمال حمله و قریب‌الوقوع بودن آن نقش اصلی را بر عهده دارند؛
- دفاع سایبری پیش‌گیرانه[۲]: در این نوع دفاع سایبری نیز احتمال حمله سایبری وجود دارد

۱. Proactive cyberspace defense
۲. Preventive cyberspace defense

و این احتمال قطعیت نیافته است. تفاوت آن با دفاع سایبری پیش‌کنشانه در این است که احتمال حمله سایبری در آینده وجود دارد. آینده‌ای که در این دفاع سایبری بحث می‌شود، شامل آینده نزدیک یا دور می‌گردد؛ درواقع دفاع سایبری پیش‌گیرانه شامل دفاع سایبری پیش‌کنشانه نیز می‌باشد و از نظر زمانی بازه بیشتری را در بر می‌گیرد؛

- دفاع سایبری پیش‌دستانه[۱]: در این نوع دفاع سایبری، حمله فوری و قریب‌الوقوع دشمن قطعی است؛ بنابراین در دفاع از خود، پیش‌دستی صورت پذیرفته و با آن مقابله می‌شود؛ این نوع دفاع سایبری بر اساس بند ۵۱ منشور سازمان ملل متحد مشروع شناخته‌شده و در حقوق بین‌الملل بر سر آن اتفاق نظر وجود دارد. دو عنصر قطعیت حمله و قریب‌الوقوع بودن آن در دفاع سایبری پیش‌دستانه، نقش اصلی را بر عهده‌دارند. به این نوع دفاع سایبری، دفاع سایبری پیش‌نگرانه[۲] نیز گفته می‌شود؛
- دفاع سایبری پیش‌بینانه[۳]: در این نوع دفاع سایبری، بر اساس شواهد و قرائن، پیش‌بینی می‌شود که حمله دشمن در آینده قطعی است و از وقوع آن اطمینان وجود دارد. مشابه دفاع سایبری پیش‌گیرانه، آینده‌ای که در این نوع دفاع سایبری بحث می‌شود، شامل آینده نزدیک یا دور می‌گردد؛ این دفاع سایبری محیط بر دفاع سایبری پیش‌دستانه بوده و آن را نیز در بر می‌گیرد.

دفاع عامل سایبری – حین حمله سایبری

مهاجمان سایبری جهت مخفی ماندن خود از روش‌های مختلفی استفاده می‌کنند. در این صورت، هویت و محل استقرار مهاجمان، گمنام مانده و از مجازات قانونی در امان خواهند بود؛ آن‌ها پس از انجام حمله سایبری ردپاهای برجای‌مانده را پاک نموده و تلاش می‌کنند تا هرگونه رهگیری را غیرممکن سازند. به همین دلیل شناسایی مهاجمین در حین انجام حمله سایبری، ساده‌تر از زمانی است که حمله به پایان رسیده باشد. راهکار دفاع عامل در حین انجام حمله سایبری، دفاع فعال نامیده می‌شود. به‌دلیل اینکه عموماً زمان حملات سایبری محدود می‌باشد؛ در دفاع فعال از روش‌هایی استفاده می‌شود که مهاجم به‌ناچار مدت حمله سایبری را افزایش دهد تا

۱. Preemptive cyberspace defense
۲. Anticipatory self-defense
۳. Predictive cyberspace defense

از این طریق مدافع بتواند زمان بیشتری به مهاجم دسترسی داشته باشد. به‌طور مثال مدافع، سامانه فریبی مانند تله سایبری را آماده نموده و به‌جای اینکه آن را نسبت به حمله SQL Injection آسیب‌پذیر نماید، به Blind SQL Injection آسیب‌پذیر می‌کند تا از این طریق مهاجم مجبور شود کاراکتر به کاراکتر اطلاعات پایگاه داده SQL را استخراج کرده و زمان بیشتری را صرف انجام حمله سایبری کند. در مرحله بعد مدافع تلاش می‌نماید تا به رایانه مهاجم نفوذ کرده و اختیار آن را به دست گیرد و یا بتواند موقعیت مکانی آن را فارغ از روش‌های گمنام‌سازی مورد استفاده مهاجم به دست آورد. یک نمونه موفق دفاع عامل، حین حمله سایبری، توسط کشور گرجستان با کمک ناتو صورت پذیرفت و به‌وسیله دفاع فعال توانستند حمله گسترده‌ای که به شبکه برق این کشور صورت گرفته بود را، از طریق نفوذ به رایانه مهاجمین و به‌دست گرفتن دوربین آن و سپس انتشار تصاویر مهاجمین، خنثی نمایند.

دفاع عامل سایبری – پس از حمله سایبری

همان‌طور که بیان شد، مهاجمین سایبری با روش‌های مختلفی تلاش می‌نمایند تا هویت و موقعیت خود را مخفی نگه دارند؛ اما IP آخرین تجهیزی که مهاجم از طریق آن حمله خود را اجرا نموده است در سامانه، هدف حمله ثبت می‌گردد. در دفاع واکنشی، مدافعین می‌توانند با استفاده از نفوذ معکوس[۱] تلاش نمایند تا به تجهیزات مورداستفاده مهاجمین رخنه نموده یا از طرق قانونی، آن‌ها را ردیابی نمایند. هدف این کار، شناسایی منشأ اصلی حمله و اقدامات لازم جهت تنبیه و جلوگیری از تکرار حمله است؛ این اقدامات، شامل طیف گسترده‌ای از تصمیمات می‌شود؛ به‌طور مثال می‌توان به انهدام و تخریب تجهیزات به‌کارگیری شده در حمله، انجام اقدام تلافی‌جویانه، وضع تحریم‌های اقتصادی، کاهش روابط دیپلماتیک، ثبت شکایت حقوقی در مراجع بین‌المللی –درصورتی‌که حمله سایبری مورد حمایت دولت باشد اشاره نمود.

با توجه به اینکه مهاجمین از دانش نفوذ آگاهی داشته و تجهیزات به‌کار رفته در حمله سایبری را امن‌سازی و سپس امحاء می‌نمایند؛ احتمال موفقیت این نوع دفاع سایبری زیاد به نظر نمی‌رسد.

---

۱ . Hack Back

دفاع غیرعامل سایبری – پیش از حمله سایبری

بیشتر اقدامات دفاعی کشورها و هزینه‌های مصرف‌شده، در دفاع غیرعامل سایبری و پیش از وقوع هرگونه تهاجمی انجام می‌شود. این نوع از دفاع سایبری شامل کلیه اقداماتی می‌شود که احتمال حمله موفق دشمن را کاهش داده یا دشمن را به‌دلیل احتمال پایین موفقیت، از انجام حمله سایبری منصرف می‌نماید. تمامی تجهیزات امنیت سایبری مانند سامانه‌های SOC[1] و CSOC[2]، دیواره‌های آتش، سامانه‌های تشخیص یا جلوگیری از نفوذ و غیره، تجهیزات فریب مانند تله‌های سایبری، هشداردهی‌ها و آگاه‌سازی‌های امنیتی، نصب وصله‌های امنیتی، ایمن‌سازی اطلاعات و ارتباطات سایبری، تعیین سیاست‌های امنیتی و غیره جزء اقدامات دفاعی غیرعامل پیش از انجام یک حمله سایبری است.

دفاع غیرعامل سایبری – حین حمله سایبری

عمده اهداف حملات سایبری با پشتیبانی دولتی، زیرساخت کشور هدف است. زیرساخت‌های یک کشور بر اساس اهمیت به ترتیب به زیرساخت‌های حیاتی، حساس و مهم تقسیم‌بندی می‌شود. دسترسی و حمله به این زیرساخت‌ها تأثیر گسترده‌ای از خود بر جای می‌گذارد؛ لذا دفاع از آن‌ها از اهمیت ویژه‌ای برخوردار است. یک راهکار دفاعی مؤثر از زیرساخت‌های بیان‌شده، تهیه فهرست سفید ارتباطی است. از طریق این فهرست –که مرتباً بروز– رسانی می‌شود– ارتباطات مجاز سایبری به مراکز تعیین‌شده و تمامی ارتباطات خارج از فهرست، مشکوک تلقی شده و در دروازه اینترنتی کشور مسدود می‌گردد. با انجام این روش ساده امنیتی بدون ایجاد اختلال در کارکرد مراکز، بدون صرف هزینه یا انجام پردازش قابل‌توجه، از حجم حملات سایبری به زیرساخت‌های حیاتی، حساس و مهم کاسته می‌شود.

راهکار دیگری که در این نوع دفاع وجود دارد، اعزام گروه‌های واکنش سریع به حوادث امنیت سایبری[3] است تا بتوانند از تداوم حمله جلوگیری نموده و جلوی گسترش حمله سایبری به سایر تجهیزات را بگیرند.

---

۱ . Security Operation Center
۲ . Cyber Security Operations Centre
۳ . Computer Emergency Response Team (CERT)

دفاع غیرعامل سایبری – پس از حمله سایبری

انجام جرم‌یابی[۱] از اصلی‌ترین اقدامات دفاع سایبری پس از انجام یک حمله سایبری است. در جرم‌یابی سایبری تلاش می‌شود ردپای برجای‌مانده از مهاجمین بررسی‌شده و روش کارشان کشف گردد تا بتوان مصون‌سازی نسبت به روش مذکور و روش‌های مشابه را انجام داد؛ همچنین تلاش می‌شود بدافزار مورد استفاده مهاجمین کشف و مورد تحلیل پویا و ایستا قرار گیرد؛ تا از این طریق بتوان به اطلاعاتی مانند، به‌کارگیری نشان یا زبان خاص افشاکننده هویت یا ملیت نویسندگان بدافزار، کشف مسیر حمله، به‌دست آوردن فنون و آسیب‌پذیری‌های مورداستفاده در حمله، بررسی چگونگی نگارش بدافزار و انطباق آن با سایر بدافزارهای کشف‌شده در دنیا جهت برقراری ارتباط حملات سایبری با یکدیگر و بسیاری از موارد دیگر دست یافت.

گروه واکنش سریع به حوادث امنیت سایبری نیز می‌تواند با برطرف نمودن آسیب‌پذیری مورد استفاده در حمله، پاک‌سازی سامانه‌های آلوده و راه‌اندازی مجدد سامانه‌های آسیب‌دیده حمله سایبری به دفاع سایبری پس از انجام حمله سایبری کمک نماید.

نتیجه‌گیری و پیشنهادها

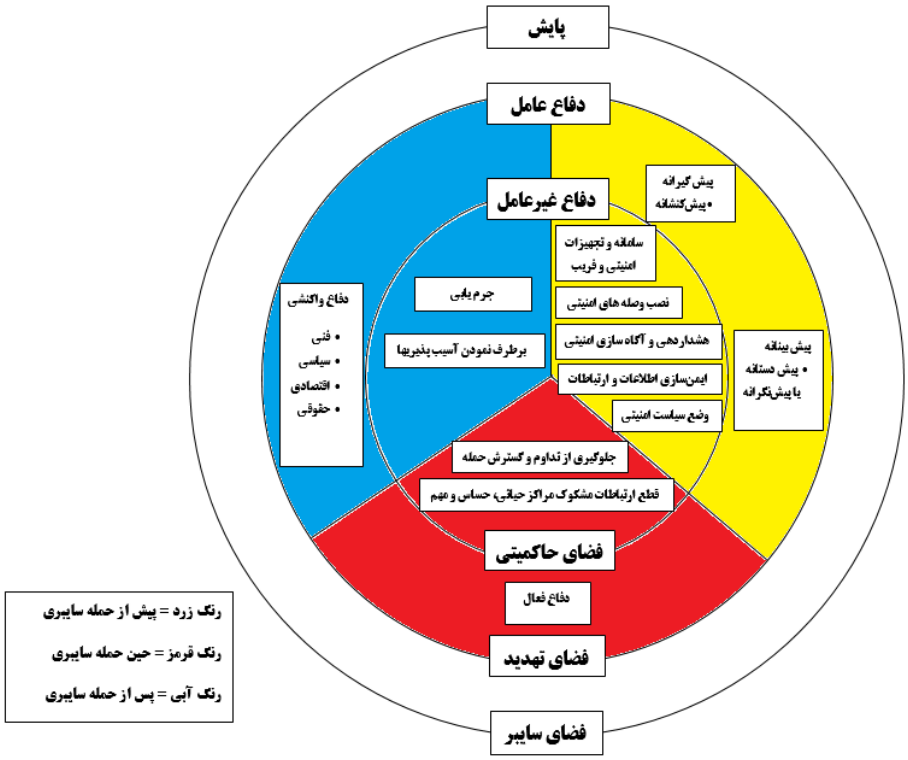
همان‌گونه که در قلمروهای زمین، دریا، هوا و فضا، دفاع به‌منظور بازدارندگی و جلوگیری از نیل متجاوزین به اهداف خرابکاری، بهره‌جویی، بهره‌برداری اطلاعاتی، نفوذ به سیستم‌های نظامی و غیره انجام می‌شود؛ در فضای سایبر نیز –که از آن به‌عنوان بعد پنجم عملیات نظامی نام برده می‌شود– باید با بهره‌گیری از تمامی روش‌های متنوع دفاعی، از دستیابی متجاوزین به سرمایه‌های ملی ممانعت به عمل آورد. به همین دلیل در تحقیق حاضر، الگوی مفهومی نوینی که در برگیرنده انواع دفاع سایبری و روش‌های هریک است، ارائه گردید تا با توجه به آن، راهکارهای دفاعی گوناگون در تصمیم‌گیری‌های راهبردی دفاع سایبری جمهوری اسلامی ایران، مدنظر قرار گیرد.

با توجه به یافته‌های تحقیق، دفاع سایبری به دو بخش عامل و غیرعامل دسته‌بندی می‌گردد. هریک از این دو دفاع نیز با شاخص‌گذاری حمله سایبری، به پیش از حمله، حین حمله و پس از

---

۱. Forensic

حمله سایبری تقسیم می‌شوند. بر این اساس دفاع عامل پیش از حمله سایبری به چهار دسته دفاع سایبری پیش‌کنشانه، دفاع سایبری پیش‌گیرانه، دفاع سایبری پیش‌دستانه و دفاع سایبری پیش‌بینانه بخش‌بندی می‌شود. دفاع عامل حین حمله سایبری نیز با دفاع فعال سایبری انجام می‌گردد و درنهایت دفاع عامل پس از حمله سایبری به دفاع واکنشی در حوزه‌های فنی، سیاسی، اقتصادی و حقوقی دسته‌بندی می‌شود. دفاع غیرعامل پیش از حمله سایبری نیز به سامانه و تجهیزات امنیتی و فریب، نصب وصله‌های امنیتی، هشداردهی و آگاه‌سازی امنیتی، ایمن‌سازی اطلاعات و ارتباطات و وضع سیاست امنیتی دسته‌بندی می‌شود. دفاع غیرعامل حین حمله سایبری به قطع ارتباطات مشکوک مراکز حیاتی، حساس و مهم و جلوگیری از تداوم و گسترش حمله دسته‌بندی می‌شود و درنهایت دفاع غیرعامل پس از حمله سایبری نیز به جرم‌یابی و برطرف نمودن آسیب‌پذیری‌ها دسته‌بندی می‌گردد. با توجه به یافته‌های تحقیق و کسب نظر خبرگان دفاع سایبری، الگوی مفهومی دفاع سایبری در شکل ۲ ارائه می‌گردد.



شکل ۲ الگوی مفهومی دفاع سایبری

به‌عنوان پیشنهاد، جهت ادامه این تحقیق می‌توان ارائه الگوی راهبردی دفاع عامل سایبری، ارائه الگوی راهبردی دفاع پیش‌گیرانه و پیش‌کنشانه، ارائه الگوی راهبردی دفاع فعال سایبری و ارائه الگوی راهبردی دفاع غیرعامل سایبری را پیشنهاد نمود؛ همچنین می‌توان برای هر یک از الگوهای فوق‌الذکر، طرح راهبردی را نیز ارائه کرد. از سوی دیگر برای شناسایی زودهنگام تهدید سایبری، ارائه الگو و طرح راهبردی و عملیاتی پیشنهاد می‌شود. درنهایت نیز جهت پایش فضای سایبر و رصد عوامل تهدید نیاز به ارائه الگو و طرح راهبردی و عملیاتی است که تحقیق در این زمینه، دستاوردهای چشم‌گیری برای دفاع سایبری جمهوری اسلامی ایران خواهد داشت.

فهرست منابع و مآخذ

الف- منابع فارسی

- باقری، ح؛ طرحانی، ف؛ اصغری، ر (۱۳۹۶)، رویکردی نوین برای ارتقای پدافند سایبری مبتنی بر دفاع سایبری فعال In ، *دومین کنفرانس ملی رویکردهای نوین در آموزش و پژوهش* .undefined . .۷۰۲۱۲۷https://civilica.com/doc/
- تقی پور، ر؛ اسماعیلی، ع (۲۰۱۹)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، *فصلنامه علمی امنیت ملی*، *۸*(۳۰)، ۱۸۱-۲۰۲. https://ns.sndu.ac.ir/article_۳۴۹.html.
- رمضان زاده، م؛ غیوری ثالث، م؛ احمدوند، ع. م؛ آقایی، م؛ نظری فرخی، ا (۱۳۹۹)، ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی سایبری، *مدیریت نظامی*، ۲۰(۷۸ ,(۹۲-۶۱) ۰۰۱۳۰۷#r https://www.sid.ir/fa/Journal/ViewPaper.aspx?id=۵۵۱۶۶۵.
- مقدسی لیچاهی، ا. ح؛ & همت، ح (۲۰۱۸)، ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه، *آینده‌پژوهی دفاعی*، ۳(۱۰)، ۱۰۳-۱۲۰_http://www.dfsr.ir/article .۳۴۲۸۴.