

تعیین جایگاه دفاع پیش‌کنش‌گرانه در فضای سایبری جمهوری اسلامی ایران

محمود کاظمی^۱، محمدرضا ولوی^۲

تاریخ دریافت: ۱۴۰۴/۰۲/۰۶

تاریخ پذیرش: ۱۴۰۴/۰۵/۰۸

چکیده

توسعه روز افزون فضای سایبری و ویژگی‌های خاص و منحصر به فردی که واجد آن گردیده، آن را به یکی از قلمروهای درگیری بین کشورها تبدیل کرده است. لذا امروزه مسئله جنگ و دفاع سایبری، اهمیت ویژه‌ای پیدا کرده است و کشورهای مختلف، تعاریف و ساختارهای متفاوتی را برای ایجاد امنیت و شکل دادن به چارچوب دفاع سایبری خود ارائه کرده‌اند. در این بین وجود شاخص‌هایی که بتوان بر اساس آن‌ها، این روش‌ها را از یکدیگر تفکیک نموده، نقش‌ها و وظایف هر یک از بازیگران خودی را مشخص کرد، محل مناقشه بوده است. در این تحقیق که از نوع کاربردی است و به صورت توصیفی و موردی‌زمینه‌ای انجام شده است تلاش گردیده تعاریف مربوط به هریک از انواع دفاع سایبری، تبیین گردد و شاخص‌هایی برای فاصله‌گذاری بین آن‌ها ارائه شود. بر اساس نتایج به دست آمده، سه شاخص زمان، نوع اقدام و فضای مقابله، انواع دفاع سایبری را که مشتمل بر دفاع غیرفعال، تاب‌آور، مستحکم، فعال، فرافعال و پیش‌کنش‌گرانه است از یکدیگر تفکیک می‌نماید.

واژگان کلیدی: دفاع سایبری، دفاع غیرفعال، دفاع فعال، دفاع فرافعال، دفاع پیش‌کنش‌گرانه.

^۱ دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول) mkazemi@ihu.ac.ir

^۲ دانشیار و عضو هیئت علمی دانشگاه صنعتی مالک اشتر Valavi@mut.ac.ir

۱. مقدمه

مسئله جنگ در فضای سایبری و دفاع در برابر حملات و تهدیدات سایبری به یک عبارت آشنا برای همه متخصصین و اندیشمندان تبدیل شده است. کتاب‌ها و مقالات متعددی در خصوص جنگ سایبری، میدان نبرد سایبری، حملات سایبری، دفاع سایبری و دیگر موضوعات این حوزه تالیف شده [۲-۷] و از زوایای مختلف به آن‌ها پرداخته شده است. به عبارتی قلمرو سایبری، به‌عنوان پنجمین قلمرو و بعد از قلمروهای زمینی، دریایی، هوایی و فضایی، کانون درگیری بین کشورها، دولت‌ها و حتی گروه‌های تروریستی با کشورها شده است. همین امر باعث شده است کشورهای مختلف در دفاع سایبری خود رویه‌ها، ساختارها و راهکشی‌های مختلفی ازجمله دفاع سایبری فعال، دفاع سایبری تاب‌آور و دفاع روبه‌جلو را اتخاذ نمایند. استفاده از فضای سایبری برای تحمیل اراده زیر آستانه جنگ و درگیری نظامی، امری معمول شده است و واقعیت‌های روز دنیا به خوبی گویای این موضوع است. نمونه‌ها و مثالهای دور و نزدیک زیادی برای جنگ سایبری و یا استفاده از فضای سایبری برای ضربه به حاکمیت کشورها و یا تحمیل اراده در ابعاد دیگر سیاسی، اقتصادی، نظامی و اطلاعاتی وجود دارد. طراحی بدافزار استاکسنت برای ایجاد اختلال در چرخه استفاده صلح‌آمیز از انرژی هسته‌ای جمهوری اسلامی ایران و بهره‌برداری از این رخداد برای فشار بر ایران در جریان مذاکرات هسته‌ای، نزدیک‌ترین نمونه این حملات در بعد سیاسی است. اختلال در جایگاه‌های عرضه سوخت و تلاش برای ایجاد آشوب در کشور، نمونه دیگر این موضوع است. حملات علیه رژیم اشغالگر قدس نیز که در سال‌های گذشته و بخصوص در جریان نبرد طوفان الاقصی شدت پیدا کرده است نیز از دیگر نمونه‌هاست. حملات سایبری عمدتاً توسط گروه‌های هکتیویست و در جریان نبرد طوفان الاقصی علیه رژیم صهیونیستی گزارش شد که شامل موارد زیر بودند: حمله به زیرساخت‌های حیاتی، حمله به وب‌سایت‌های دولتی و نظامی، نفوذ به سیستم‌ها، جنگ روانی و انتشار اطلاعات جعلی و حمله به شبکه‌های اجتماعی. آنچه بیش از سایر وجوه مهم است این است که از تهاجم سایبری در

ترکیب با نبرد در سایر مولفه‌های قدرت (سیاسی، نظامی، فرهنگی، امنیتی و اقتصادی) بهره‌برداری می‌شود و اثرگذاری مولفه مذکور را تشدید می‌کند. نمونه دیگر این موضوع را به روشنی می‌توان در جنگ روسیه و اوکراین مشاهده کرد. حملات سایبری گسترده ازجمله حملات انکار سرویس توزیع‌شده^۱ و حملات باج‌افزاری در ایام منتهی به شروع حمله روسیه به زیرساخت‌های حیاتی اوکراین صورت گرفت. همچنین در ۲۴ فوریه ۲۰۲۲، هم‌زمان با شروع تهاجم نظامی روسیه، یک حمله سایبری به ماهواره‌های ارتباطی Viasat انجام شد که باعث اختلال در خدمات اینترنت ماهواره‌ای در اوکراین و بخش‌هایی از اروپا گردید و ارتباطات نظامی و غیرنظامی اوکراین را تحت تأثیر قرار داد و نشان داد که زیرساخت‌های فضایی نیز در معرض تهدیدات سایبری هستند.

نبردهای سایبری به‌عنوان جدیدترین و پیچیده‌ترین نبردها در جنگ پست مدرن به شمار می‌آیند. حملات سایبری به دلیل بکر بودن، درصد هزینه و فایده بالا، عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید و عدم توانایی در تعیین میزان و دامنه خسارات وارد شده در مراحل اولیه شروع حمله، موردتوجه کشورهای متخاصم به ویژه در جنگهای پنهان قرار گرفته است [۸]؛ بنابراین بدیهی است که کشورها به فکر ایجاد ساختار دفاعی خود در فضای سایبری باشند و با توجه به سرعت پیشرفت و نوشوندگی تهدیدات در این فضا، راهبردها و راهکشی‌های دفاعی نیز دستخوش تغییرات قرار می‌گیرند که به‌عنوان نمونه می‌توان به سند راهبرد دفاع سایبری وزارت دفاع آمریکا اشاره کرد که در طول سال‌های ۲۰۱۳ تا ۲۰۲۳ از دفاع پیشگیرانه به سمت دفاع روبه‌جلو حرکت کرده است [۹-۱۱].

این تغییرات بیانگر آن است که در صورت انتظار برای رسیدن تهدید و یا حمله سایبری به سرمایه‌های حیاتی و حساس و دیگر سرمایه‌های سایبری، فرصت و امکان مقابله لازم با آن‌ها از دست خواهد رفت؛ بنابراین بسنده کردن به اقدامات غیرفعال و مقاوم‌سازی زیرساخت‌ها، به‌تنهایی کافی نیست و باید رویکردهایی را در نظر داشت که تهدید را در مبدا شناسایی نموده و با آن مقابله کند [۹، ۱۱].

^۱ DDoS

از سوی دیگر بررسی برخی از مفاهیم دفاع سایبری نشان می‌دهد که این مفاهیم، ابتدا در فضای حقیقی مطرح بوده‌اند و آرام آرام و بعد از شکل‌گیری فضای سایبری و وقوع تهدیدات و حملات، در این فضا نیز تعریف‌شده و با ویژگی‌های خاص این فضا منطبق شده‌اند. به‌عنوان نمونه دفاع در عمق، یکی از موضوعاتی است که از دیرباز در فضای حقیقی و به‌خصوص در قلمرو زمینی مطرح بوده است. دفاع در عمق (دفاع عمیق، انعطاف‌پذیر یا کشسان) یک استراتژی نظامی است که به‌جای ممانعت از پیشروی مهاجم، سعی در به تأخیر انداختن آن، خریدن زمان و تحمیل تلفات بیشتر با تسلیم کردن فضا به مهاجم دارد [۱۲]. همین مفهوم از مدت‌ها قبل (همچنانکه در ادامه همین مقاله گفته خواهد شد) در فضای سایبری نیز شکل گرفته و در موضوع امنیت شبکه‌ها از این استراتژی دفاعی بهره‌برداری شده است. اتفاق مشابهی برای سایر مفاهیم حوزه دفاع سایبری رخ داده است.

نکته حائز اهمیت در اینجا این است که عدم تعریف درست و اجماع نظر پیرامون مفاهیم این حوزه مانند دفاع غیرفعال، دفاع فعال، دفاع پیشگیرانه و دفاع پیش‌کنش‌گرانه و سایر مفاهیم و جایگاه و موقعیت آن‌ها نسبت به یکدیگر، موجب اشکال در سیاست‌گذاری و شکل‌دهی راهبردها خواهد شد؛ بنابراین در ادامه با بررسی مفاهیم فضای سایبری و ویژگی‌های آن، جنگ سایبری، تهدید و تهدید سایبری، شاخص‌هایی برای تفکیک انواع دفاع در فضای سایبری ارائه و پس از تعریف انواع دفاع در فضای سایبری، بر اساس شاخص‌های پیش‌گفته به تعیین جایگاه آن‌ها نسبت به یکدیگر پرداخته خواهد شد.

۲. مبانی نظری پژوهش

۱.۲. فضای سایبر

فضای سایبری به مجموعه‌ای اطلاق می‌گردد که شامل زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی آن و سامانه‌های رایانه‌ای است. فضای سایبری یا فضای مجازی ترکیبی از ده‌ها هزار رایانه به‌هم‌پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سویچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سامانه جامع فراهم می‌آورد [۱۳]. بر اساس این تعریف و آنچه در ادامه همین تعریف در

مقاله مورد اشاره آمده است، فضای سایبری دارای مؤلفه سخت‌افزار، مجازی (داده و نرم‌افزار) و شناختی (کاربران و اشخاص) است. فضای سایبری جمهوری اسلامی ایران شامل مجموعه‌ای از ارزش‌ها، منافع و دارایی‌های ملی در فضای سایبری بوده و جهت ارائه خدمات در راستای اهداف نظام جمهوری اسلامی ایران است. این فضا محدود به مرزهای جغرافیایی نیست [۱۴]. دَن کوهل نیز فضای سایبری را این‌گونه تعریف می‌کند: فضای سایبری عبارت است از یک قلمرو عملیاتی که ویژگی متمایز و منحصر به فرد آن این است که با به‌کارگیری الکترونیک و طیف الکترومغناطیس برای ایجاد، ذخیره، تغییر، تبادل و بهره‌جویی از اطلاعات از طریق دستگاه‌های به هم متصل مبتنی بر فناوری اطلاعات و ارتباطات و زیرساخت‌های آن‌ها، شکل می‌گیرد [۱۵]. سازمان پدافند غیرعامل نیز فضای سایبری را این‌گونه تعریف می‌کند: شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات. این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه‌شده باشد [۱۶].

از جمع‌بندی این تعاریف درمی‌یابیم که اولاً فضای سایبری یک زیست‌بوم را تشکیل می‌دهد که مشتمل بر موضوعاتی همچون آموزش، پژوهش، صنعت، فناوری و ... می‌شود و بسیاری از نیازمندی‌های بشر امروزی در امور اجتماعی، فرهنگی، سیاسی، اقتصادی و دفاعی - امنیتی در این زیست‌بوم قابل تأمین است و بخش زیادی از جامعه، عملاً در این فضا زیست می‌کنند و ثانیاً فضای سایبری دارای سه بعد فیزیکی (زیرساخت‌های فناوری اطلاعات و ارتباطات)، بعد منطقی (داده و نرم‌افزار) و بعد ادراکی یا شناختی - اجتماعی (تعامل انسان و دو بعد دیگر این فضا) [۱۷] است و ثالثاً هریک از این ابعاد دارای ویژگی‌هایی است که در تعاریف، به بخش‌هایی از آن‌ها

عملیات نظامی، این منطقه، هدفی است که باید به‌طور موقت یا دائم تحت نفوذ و یا کنترل قرار گیرد [۲۱].

در تعریف و دسته‌بندی دفاع سایبری، از این بعد فضای سایبری نیز فارغ از لایه‌بندی که برای فضای سایبری مطرح کرده استفاده شده است.

۲.۲. ویژگی‌های فضای سایبر

فضای سایبری واجد ویژگی‌هایی است که جنگ و دفاع در و از طریق آن را به‌شدت از جنگ و دفاع در فضای حقیقی متمایز کرده است. ویژگی‌های فضای سایبری از حیث مباحث امنیتی عبارت‌اند از:

- تقدم اقدام پیش‌کنش‌گری فعال و آفندی بر دفاع: با توجه به ویژگی‌های فضای سایبری، ابتکار عمل برای مهاجم بسیار بیشتر از مدافع خواهد بود و پیش‌دستی در تهاجم، کشورهای هدف را متحمل خسارات و صدمات بیشتری می‌نماید.

- انتساب حمله (گمنامی و ناشناسی): با توجه به تاکتیک‌ها و روش‌های متعدد در ایجاد گمنامی در زمان اجرای حملات سایبری، طراحی حمله به شکلی صورت می‌گیرد که تشخیص منشأ حمله مشکل است.

- سرعت عمل در فضای سایبر: با توجه به پتانسیل‌های بالای این فضا برای اختفاء تسلیحات سایبری در حوزه هدف، سرعت عمل در فضای سایبری به‌شدت افزایش می‌یابد.

- تفاوت در نوع فرماندهی و مدیریت: با توجه به ویژگی‌های خاص فضای سایبری، فرآیند و نظام مدیریت در فضای سایبری از سبک‌های خاص و متفاوتی نسبت به سایر قلمروها برخوردار هست.

- عدم قطعیت و نامشخص بودن تهدیدات: در شرایط حاضر کشورها با زنجیره و طیفی از تهدیدهای نامشخص، مستمر و فراگیر که پتانسیل و قابلیت مخاطره را دارا است مواجه هستند [۲۲].

همچنین دسترس‌پذیری، هوشمندی و نوآوری، فراگیرندگی و تأثیرگذاری و نیز انعطاف‌پذیری هم‌زمان با پیچیدگی، تنوع و تحولات سریع پدیده‌ها، محاسبه و پردازش و پیش‌بینی و شبیه‌سازی از دیگر ویژگی‌های فضای سایبری به شمار می‌رود و در بسیاری از موضوعات بشر با درنوردیدن ابعاد زمان و مکان،

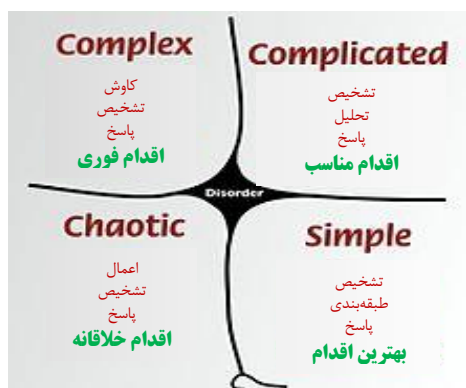
اشاره شده است. در [۱۸] به تفصیل در خصوص مدل‌های مختلف فضای سایبری بحث شده است. مدل سه لایه‌ای، در سند ۳-۱۲ JP [۱۹] و دکترین سایبری نیروی هوایی [۲۰] مورد اشاره و استفاده قرار گرفته است و سایر مدل‌های ارائه شده، قابل تجمیع در همین مدل هستند. مدل‌های با لایه‌های بیشتر، تلاش کرده‌اند جزئیات بیشتری را در برخی لایه‌ها به نمایش بگذارند. در این مقاله از مدل سه لایه‌ای (فیزیکی، اطلاعاتی، شناختی) استفاده شده است. از سوی دیگر، یکی از مدل‌های ارائه شده برای فضای سایبری، موقعیت جغرافیایی را نیز به مدل وارد کرده (شکل ۱) و تعریف فضای دور، میانه و نزدیک را این‌گونه مطرح می‌کند که فضای نزدیک، در سطح ملی، شبکه‌ها و سامانه‌هایی است که برای پشتیبانی از زیرساخت‌ها و خدمات ملی، حیاتی هستند و عمدتاً توسط سازمان‌های دولتی، کنترل و محافظت می‌شوند. در سطح محلی نیز، فضای نزدیک عنصری از شبکه است که پیکربندی و مالکیت آن‌ها متعلق به شرکت‌ها و کاربران فردی است.



شکل ۱. مدل سه‌بعدی فضای سایبری [۲۱].

این سازمان‌ها و افراد، نوع نرم‌افزارها و دستگاه‌هایی که در این شبکه‌ها، نصب و استفاده می‌شوند را کنترل می‌کنند. فضای نزدیک در سطح شخصی نیز، شامل دستگاه‌های الکترونیکی شخصی است که به اینترنت متصل هستند. فضای میانی، به عنوان شبکه‌ها و سامانه‌هایی تعریف می‌شوند که برای دسترسی به فضای سایبری جهانی حیاتی هستند اما هیچ کنترل یا محافظت محلی یا شخصی روی آن‌ها وجود ندارد. به‌طور معمول، این زیرساخت‌ها ممکن است از نظر جغرافیایی دور بوده و متعلق به یک شرکت تجاری خارجی یا یک دولت ثالث باشند. در ادامه، فضای دور به معنی شبکه‌ها و سامانه‌هایی است که به مقصد مرتبط هستند و یا جایی که دشمن ممکن است در آن قرار داشته باشد و به عنوان فضای نزدیک وی در نظر گرفته می‌شود. در

دیدگاه بسیاری از نظریه‌پردازان و نویسندگان، دوره قطعیت و قابل پیش‌بینی بودن به پایان رسیده است و عدم قطعیت، آشوب و تغییر پارادایمی در حال اتفاق است [۲۵]. این موضوع در چارچوب کانوین^۱ (شکل ۲) که در مسئله تصمیم‌گیری مورد استفاده قرار می‌گیرد به‌خوبی قابل مشاهده است.



شکل ۲. دامنه‌های چارچوب کانوین در تفکیک محیطها [۲۶].

هر ابزار دیجیتال، سیستم‌عامل، نرم‌افزار، مسیر انتقال، فایل و کاربر، چندین بردار حمله^۲ (مسیر رسیدن به هدف) و سطح حمله^۳ (که می‌توان به آن حمله کرد) دارد. وقتی دستگاه‌ها راه‌اندازی می‌شوند، کاربران وارد سیستم می‌شوند، برنامه‌ها را راه‌اندازی می‌کنند، ایمیل‌ها را باز می‌کنند، وب‌سایت‌ها را مرور می‌کنند، فایل‌ها را دست‌کاری می‌کنند یا اطلاعات را منتقل می‌کنند، این اقدامات بردارهای حمله را باز نموده و سطوح حمله را در معرض دید قرار می‌دهند و در نتیجه فرصت‌های حمله فراهم می‌شوند. با این توصیف، حتی اگر محیط پیرامونی به‌دقت مورد احصا قرار گیرد، زمان، هزینه و مهارت لازم برای بستن تمام حفره‌ها و بسته نگاه‌داشتن آن‌ها وجود نخواهد داشت. چنانچه به این موضوع، تهدیدات غیرقابل پیش‌بینی و پیچیده پویا نیز اضافه شود وضعیت پیچیده‌تر خواهد بود و با این وصف که تعریف ارائه‌شده از محیط پیرامونی، تنها مربوط به لایه بیرونی دفاع است؛ بنابراین حتماً دفاع در عمق مورد نیاز است [۲۷] و این نتیجه‌گیری در تحقیق [۲۸] نیز آمده است. در تحقیق مذکور با بررسی انواع دفاع سایبری و با استفاده از عبارات دفاع مستحکم - مبتنی بر محیط دفاعی - و دفاع تاب‌آور - تضمین

واقعیت‌های مجازی و تخیلات را با افزایش سرعت، دقت و کاهش هزینه و زمان عینیت بخشیده است [۲۳].

۱.۲.۲. پیچیدگی فضای سایبر

متخصصان امنیت سایبری صراحتاً اذعان می‌کنند که رویکردهای سنتی برای امن سازی اطلاعات و فضای سایبری موفقیت‌آمیز نیستند و عمده‌تأ شکست می‌خورند و تعریف قدیمی امنیت با محیط عملیاتی امروزی مطابقت ندارد [۳، ۲۴] زیرا فضای سایبری و محیط تهدید و به‌تبع آن‌ها، امنیت و دفاع سایبری به طرز عجیب و غیرقابل مدیریتی، پیچیده شده است. یکی از نکاتی که در خصوص دفاع از یک سرمایه سایبری مطرح است، محیط پیرامونی است. برای محافظت از اطلاعات از طریق کنترل دسترسی به آن‌ها، باید یک محیط پیرامونی برای آن‌ها تعریف کنیم و از این محیط محافظت کنیم. در گذشته این کار با محافظت فیزیکی قابل انجام بود چون عمده‌تأ رایانه‌ها، مستقل بودند. برای تصور پیچیدگی محیط، مثال زیر را در نظر بگیرید. یک سیستم مین‌فریم در یک ساختمان قرار دارد - محیط کاملاً تحت کنترل. همین سیستم به چند رایانه دیگر داخل همان ساختمان که هرکدام پردازنده، ذخیره‌ساز، درگاه‌های ورودی/خروجی و نرم‌افزارهای مربوط به خود را دارند متصل می‌شود - محیط پیرامونی تغییر می‌کند. حال به این مجموعه رایانه‌های قابل حمل که برای خارج محیط فیزیکی مورد اشاره در نظر گرفته شده‌اند را اضافه کنید. متعاقباً با افزودن یک شبکه محلی، عناصر محیط فیزیکی که می‌توانند مستعد ضربه خوردن و استراق سمع احتمالی باشند اضافه می‌شود که اکنون باید از آن‌ها نیز دفاع کرد. توسعه شبکه به یک شبکه گسترده، اجزا محیط را که شامل کابل‌ها و سوییچ‌های افراد می‌شود افزایش می‌دهد - که تا اینجا مربوط به دهه ۱۹۸۰ است. به این‌ها، درایوهای ذخیره‌ساز قابل حمل با ظرفیت بالا و حجم بسیار کم و سپس شبکه‌های رادیویی را در قالب‌های مختلف مانند شبکه‌های سلولی، وایفای، بلوتوث و ... اضافه کنید - و این‌ها مربوط به دهه ۱۹۹۰ است. همان‌طور که مشاهده می‌شود، محیط پیرامونی، دیگر قابل احصا و بنابراین قابل دفاع با رویکردهای خطی گذشته نیست. بر اساس

^۲ Attack surface

^۱ Cynefin Framework

^۳ Attack vector

می‌تواند رویکردهای دفاع سایبری موجود که شامل پیشگیری از حمله (نسل اول)، شناسایی و پاسخ (نسل دوم) و تحمل و تاب‌آوری (نسل سوم) می‌شود را از محدودیت‌های خود عبور دهد [۲۹-۳۱].

این به‌نوبه خود مستلزم نیاز به در نظر گرفتن پارادایم‌های جدیدی است که می‌تواند مبنایی برای نسل بعدی (چهارمین) رویکردهای دفاع سایبری فراهم کند [۲۹].

۳.۲. جنگ سایبری

جنگ سایبری، ترکیبی از حمله و دفاع در شبکه‌های کامپیوتری و عملیات‌های فنی خاص است [۷]. بر اساس تعریف سازمان پدافند، جنگ سایبر عبارت است از استفاده از رایانه‌ها به‌عنوان یک اسلحه یا به‌عنوان ابزاری برای انجام کارهای خشونت‌بار جهت ترساندن یا تغییر عقیده یک گروه یا کشور. جنگ سایبر به‌قصد کارهای سیاسی و آرمانی انجام می‌گیرد و مکان‌ها و تأسیسات حیاتی مانند انرژی، حمل‌ونقل، ارتباطات و سرویس‌های ضروری (مانند پلیس و خدمات پزشکی) را هدف قرار می‌دهد و از شبکه‌های رایانه‌ای به‌عنوان بسترهایی جهت انجام این اعمال خرابکارانه استفاده می‌کند [۸]. همچنین [۸] در تعریفی دیگر، جنگ سایبری را بالاترین سطح تهاجم سایبری می‌داند و در تعریف تهاجم سایبری این‌گونه عنوان می‌کند که به هرگونه اقدام غیرمجاز سایبری که باهدف نقض سیاست امنیتی یک سرمایه سایبری و ایجاد خرابی یا خسارت، ایجاد اختلال در عملکرد یا از کاراندازی خدمات و یا دستیابی به اطلاعات سرمایه ملی سایبری مذکور انجام گیرد، تهاجم سایبری اطلاق می‌گردد.

بر اساس تعریف اول و دوم، جنگ سایبر، درون خود فضای سایبری صورت می‌گیرد. درحالی‌که در تعریف سوم، بخشی که اشاره به نقض سیاست امنیتی یک سرمایه سایبری می‌کند می‌تواند یک اقدام جنبشی خارج از فضای سایبری علیه بعد فیزیکی سرمایه سایبری را نیز شامل شود که با توجه به جهت‌گیری این مقاله که دفاع پیش‌کنش‌گرانه در فضای سایبری را مدنظر دارد، از تعاریف اول و دوم تبعیت نموده و اقدام فیزیکی علیه بعد فیزیکی سرمایه‌های سایبری از شمول این بحث خارج می‌شود

تداوم خدمات - به‌جای عبارت کلی دفاع غیرفعال و تعریف دفاع فعال، این‌ها را مستقل از یکدیگر ندانسته و عنوان می‌کند در سه‌گانه‌ای مکمل از رویکردهای سیاستی برای دستیابی به امنیت سایبری عمل می‌کنند. آنچه در بالا در قالب یک مثال عنوان شد به‌عنوان دلایل پیچیدگی فضای سایبری در [۲۹] مورد اشاره قرار گرفته است. پیشرفت‌های اخیر در اینترنت اشیا و به‌طور کلی، تحقیقات مرتبط با محاسبات توزیع‌شده که منجر به تحقق مزایای استفاده از گره‌های لبه (دستگاه‌های کم‌مصرف و همچنین دستگاه‌های شبکه میانی و سرورها) برای ذخیره‌سازی و پردازش جانبی شده است، باعث پیدایش پارادایم‌های مختلف محاسباتی لبه‌گرا می‌شود که به دنبال آوردن «قدرت» رایانش ابری به لبه شبکه هستند. سیستم‌هایی که به این پارادایم‌های لبه‌گرا پایبند هستند (مانند مه / لبه / ابر متحرک و غیره) و IoT را نیز در بر می‌گیرند، ویژگی‌هایی را از خود بروز می‌دهند که مشکلات مرتبط با دفاع سایبری سنتی برای سیستم‌های توزیع‌شده را تشدید می‌کند. این ویژگی‌ها عبارت‌اند از مقیاس بسیار بزرگ و ناهمگونی، محدودیت‌های جدی منابع، پویایی غیرقابل صرف‌نظر سیستم از جمله تحرک و تمرکززدایی کامل یا جزئی که همه این‌ها منجر به پیچیدگی بالای سیستم می‌شود.

محیط‌های تاکتیکی مدرن که در آن سیستم‌های لبه‌گرای فوق‌الذکر ممکن است به اجرای عملیات بپردازند، مشکلات مربوط به دفاع سایبری را از این هم بیشتر تشدید می‌کنند [۲۹]. به‌ویژه، محیط‌های متخاصم بدون ساختار، ناپایدار، به‌سرعت در حال تغییر و آشوبناک اینترنت اشیا / نظامی / صحنه نبرد (IoMT/IoBT)، حاکی از طیفی از عوامل استرس‌زای اضافی است که در محیط‌های عملیاتی سازمانی یا عمومی وجود ندارند. به‌عنوان مثال (۱) نرخ بسیار بالاتری از حملات باهدف برهم زدن یکپارچگی و دسترس‌پذیری؛ (۲) عدم قطعیت اطلاعات (از جمله از طریق حملات اطلاعات نادرست)؛ (۳) پیش-بینی‌ناپذیری بالا؛ (۴) دامنه‌های با سطوح اعتماد متفاوت و درهم که شبکه‌های با طبقه‌بندی متفاوت را اداره می‌کنند و (۵) ارتباطات ضعیف.

افزایش پیچیدگی سیستم و محیط (بر اساس موارد فوق) هنگامی که با پیچیدگی روزافزون فن‌های مهاجم ترکیب می‌شود

چه اینکه چنین اقدامی ذیل قوانین جنگ قابل رسیدگی و اقدام متقابل خواهد بود.

۴.۲. تهدید

ارائه یک تعریف دقیق از تهدید به دلیل چندوجهی بودن و ارتباط آن با امنیت، منافع، اهداف و راهبردها، پیچیده و مشکل است. تهدید در لغت، معانی مختلف اما نزدیک به هم دارد. فرهنگ لغات آن را به ترساندن، بیم دادن و بیم عقوبت دادن معنا کرده است [۳۲]. تهدید از نظر لغوی به معنای ترساندن و در اصطلاح به هرگونه نیت، قصد و اقدامی که ثبات و امنیت یک سازمان یا کشور را به خطر اندازد گفته می‌شود. فرهنگ معین تهدید را ترسانیدن و بیم معنی کرده است و لرز تهدیدات را عبارت از هر چیزی که بتواند ثبات و امنیت را در یک کشور به خطر اندازد، دانسته و معتقد است تهدیدات، منافع را هدف قرار می‌دهند. مفهوم تهدید در نگرش سیستمی، عدم تعادل در سیستم، بیان شده است؛ یعنی عاملی که اجازه نمی‌دهد سیستم به اهداف خویش برسد. در پاره‌ای از متون نیز تهدید به معنای توانایی‌ها، نیت و اقدامات دشمنان بالفعل و بالقوه برای ممانعت از دستیابی خودی به مقاصد امنیتی، تعریف شده است [۳۳]. بر اساس این تعریف، به‌غیر از اقدامات، نیت و توانایی‌های دشمن نیز می‌توانند جزو محورهای تهدید قرار گیرند و این همان چیزی است که در دفاع پیشدستانه و پیشگیرانه مورد توجه و استناد قرار می‌گیرد. «فرهنگ آکسفورد تهدید را این‌گونه تعریف می‌کند: امکان به وحشت انداختن، ترساندن یا انجام فاجعه برای یک فرد یا جامعه، آسیب زدن به کسی یا چیزی، نتایج ناخوشایند به بار آوردن» [۳۴]. در یک تعریف عمومی، تهدید عبارت است از «فقدان امنیت؛ ایجاد اختلال در توانایی‌های کشور در کسب اهداف ملی؛ اقداماتی که کمیت و کیفیت زندگی مردم یک کشور یا دامنه اختیارات حکومت را به‌طور جدی کاهش دهد». تهدید ذاتاً مبهم و نامعلوم بوده و شناسایی آن بسیار دشوار است. اکثر تهدیدات موجود در صحنه جهانی شامل تعداد زیادی عوامل پیچیده‌اند که برآیند و نتایج آن‌ها را به‌شدت نامعلوم می‌سازد.

به‌طور کلی تهدید دارای دو مرحله است؛ مرحله ذهنی و مرحله عملیاتی (عینی). در مرحله ذهنی، دشمن یا کشور تهدیدکننده ابتدا نقاط آسیب‌پذیر جامعه هدف را شناسایی

می‌کند، ابزارهایش را می‌شناسد و سپس هدف‌گذاری و سرمایه‌گذاری می‌کند و در نهایت آن را عملیاتی می‌نماید. تقسیم‌بندی تهدید بر دو بعد ذهنی و عملیاتی برای پیشگیری تهدید است. باید این را بدانیم برای مقابله با تهدید در کدام مرحله پادزهر را تزریق کنیم [۳۵]. این تعریف از تهدید تا حد زیادی بر مدل چهار مرحله‌ای اودا منطبق است.

همان‌گونه که در تعریف اخیر مشخص است مفهوم تهدید، بر عبارت آسیب‌پذیری تکیه دارد. درواقع دشمن با شناسایی آسیب‌پذیری‌های آماج تلاش می‌کند از این آسیب‌پذیری در جهت تهدید و ضربه به وی استفاده نماید. از سوی دیگر، تعریف تهدید، واژه دیگری را نیز به ذهن متبادر می‌نماید و آن امنیت است. از دیدگاه علوم سیاسی و روابط بین‌الملل، تهدید و امنیت به‌وسیله یکدیگر تعریف می‌شوند. امنیت درواقع نبود تهدید است و باوجود تهدید، امنیت مخدوش بوده و کاهش می‌یابد. از آنجاکه امنیت، امری ذهنی است [۳۶] بنابراین تهدید نیز یک بعد ذهنی خواهد داشت. امنیت به وضعیتی اطلاق می‌شود که در آن نسبت به منافع بازیگر، تهدیدی وجود نداشته باشد و یا در صورت وجود، امکان مدیریت مؤثر آن برای بازیگر مورد تهدید واقع‌شده، وجود داشته باشد. امنیت در اینجا، وضعیت مبتنی بر نبود تهدید برای منافع بازیگر است که با رویکرد سلبی ارائه شده است؛ اما از حیث ایجابی امنیت به وضعیتی اطلاق می‌شود که در آن بین خواسته‌ها و داشته‌ها در یک واحد سیاسی معین، متناسب با ضریب ایدئولوژیک (آن واحد)، تعادلی وجود دارد که نزد بازیگران (آن واحد) تولید رضایت می‌نماید [۳۷].

با توجه به مطالب و دیدگاه‌های مختلف در خصوص تهدید، آن را این‌گونه تعریف می‌کنیم: هرگونه نیت، قصد و یا اقدامی که از سوی یک کنشگر (اعم از فرد، گروه یا کشور) علیه ثبات، امنیت و منافع یک بازیگر، ناظر به آسیب‌پذیری‌ها و ضعف‌های داخلی بازیگر به وجود آید، تهدید نامیده می‌شود.

چند نکته را در این تعریف باید مدنظر داشت. نکته اول اینکه ثبات و امنیت و همچنین تهدید، معطوف به سطح بازیگر است و چنانچه بازیگر را یک کشور در نظر بگیریم، طبیعتاً موضوع امنیت ملی مطرح خواهد بود و منظور از تهدید، تهدید امنیت ملی و یا هر یک از اجزای آن است. به عبارتی تهدید

داشته باشند، هویت مشترک بیشتری دارند و به همین دلیل ادراک آن‌ها از نیت تهاجمی طرف مقابل به شدت کاهش می‌یابد [۳۸]. بررسی معیارهای چهارگانه بالا در تقابل نظام جمهوری اسلامی با نظام سلطه به سرکردگی آمریکا نشان می‌دهد نیت تعرضی غرب به وضوح علیه جمهوری اسلامی وجود دارد: در راهبرد دفاع سایبری وزارت دفاع آمریکا به همراه کره شمالی و پس از روسیه و چین به عنوان تهدیدات اصلی، از ایران به عنوان یکی از تهدیدات این کشور نام برده شده است [۹]. از عمر آمریکا اندکی بیش از ۲۴۰ سال می‌گذرد در حالی که از این مدت بیش از ۲۲۰ سال آن را در جنگ گذرانده، در ۲۲۷ جنگ، شرکت داشته و فهرست کشورهایی که آمریکا به آن‌ها حمله کرده، بسیار زیاد است [۳۹، ۴۰]. سوابق تهدید، تعرض، حمله و مداخله در امور داخلی ایران از سوی آمریکا و هم‌پیمانانش نیز دیگر بر کسی پوشیده نیست [۴۰] و در خصوص آخرین معیار نیز باید گفت هیچ‌گونه هویت مشترکی بین ایران و آمریکا نه از لحاظ مذهبی، نه تاریخ و تمدن، نه نظام ارزشی و نه ساختارهای اقتصادی و سیاسی وجود ندارد. کشور ایران به دلیل موقعیت ژئوپلیتیکی خود و واقع شدن در منطقه جنوب غرب آسیا با مخاطرات و چالش‌های عمده‌ای در نظام محیط بین‌الملل روبه‌روست و بروز اختلاف‌ها و تقابل چندساله بین ایران و غرب که از بدو انقلاب اسلامی [و حتی پیش از آن] تاکنون از حیث آرمان، ارزش، ایدئولوژی، ژئوپلیتیک، اقتصاد و فرهنگ به وجود آمده، کشور ایران را همواره در معرض تهدیدات استکبار جهانی قرار داده است [۲۲]. طراحی، پیاده‌سازی، هماهنگی و اجرای حمله استاکسنت توسط آمریکا با همراهی رژیم جعلی صهیونیستی، یکی از شاخص‌ترین اقدامات تهاجمی سایبری در دنیا بوده است که علیه جمهوری اسلامی ایران انجام گرفت.

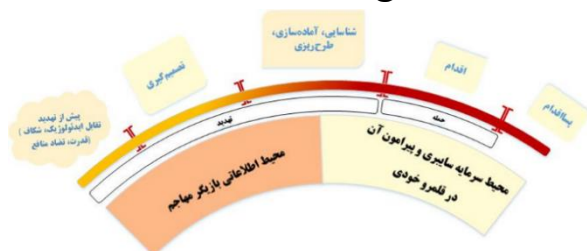
اکنون و پس از تعریف تهدید، فرآیند شکل‌گیری تهدید را بررسی می‌نماییم. از خلال تعاریف و مباحثی که در بالا به آن‌ها اشاره شد، این‌گونه استنباط می‌شود که پس از به وجود آمدن دلایل تهدید (که از آن به مرحله پیش از تهدید یاد شد و شامل دلایلی همچون تقابل ایدئولوژیک، شکاف قدرت و یا تضاد منافع می‌شود و شکل‌دهنده نیت تهاجمی است)، بازیگر تهدیدکننده، درصدد ایجاد اختلال در امنیت آماج (برای تحمیل

زیرساخت‌های حیاتی یک کشور نیز، تهدید امنیت ملی محسوب می‌شود. نکته دوم اینکه مرحله پیش از تهدید در این تعریف آورده نشده است. درواقع اینکه تضاد ایدئولوژیک باعث به وجود آمدن تهدید شده است یا تضاد منافع و یا شکاف قدرت، در اصل شکل‌گیری تهدید، تأثیری نخواهد داشت هرچند ممکن است در ماهیت تهدید شکل گرفته مؤثر باشد. به همین ترتیب، اینکه منشأ به وجود آمدن تهدید، جدید است یا از دیرباز وجود داشته است نیز در تعریف فوق مؤثر نخواهد بود. لکن چنین مواردی ممکن است در برخی ویژگی‌های تهدید، مؤثر واقع شوند. به عنوان مثال، تقابل ایدئولوژیک، می‌تواند یک تهدید را به عنوان تهدید دائمی مشخص نماید و یا میزان شکاف قدرت، بر روی سطح تهدید و یا احتمال تهدید اثرگذار باشد.

رویکرد نیت تهاجمی و تهدیدات امنیتی بر پایه عوامل چهارگانه «استفان والت» قرار گرفته است. با تغییر موازنه از قدرت به تهدید، وی چهار عامل را در شکل‌گیری تهدید بیان کرده است که عبارت‌اند از: قدرت نظامی، توان تهاجم، نزدیکی جغرافیایی و نیت تهاجمی. به نظر می‌رسد در میان این چهار عامل، نیت تهاجمی، شرط کافی و لازم در تولید یا ایجاد تهدید باشد [۳۸]. اولین معیار در محک وجود و میزان نیت تعرضی کشوری بر ضد کشور دیگر نظریه امنیتی یا رهنامه امنیتی دو کشور است. معیار دوم چگونگی شهرت بین‌المللی بازیگر مقابل است. برای مثال چنانچه بازیگر مقابل - که بازیگر خودی در معرض ادراک تهدیدات از ناحیه آن قرار دارد - در نزد ملت‌ها و دولت‌ها به‌طور کلی کشوری جنگ‌طلب، تجاوزکار و اشغالگر شناخته شود، خودبه‌خود، تقویت‌کننده ادراک نیت تهاجمی و تهدیدآمیز از سوی طرف مقابل خواهد بود. معیار سوم تاریخچه منازعات میان دو بازیگر متعامل یا متقابل است. اگر میان کشور درک‌کننده تهدید و کشوری که عامل تهدید شناخته شده است سوابق درگیری و جنگ وجود داشته باشد، در چنین وضعیتی احتمال بالا رفتن ادراک از نیت تعرضی افزایش می‌یابد. هویت مشترک، چهارمین و آخرین منبع تعیین تکلیف نیت تعرضی است. بر این اساس، هراندازه دو کشور از لحاظ مذهب، ساختار اقتصادی، ساختار سیاسی، قومیت و زبان، نظام ارزشی، تاریخ و تمدن و مواردی مانند این، نزدیکی و اشتراک روزافزون‌تری

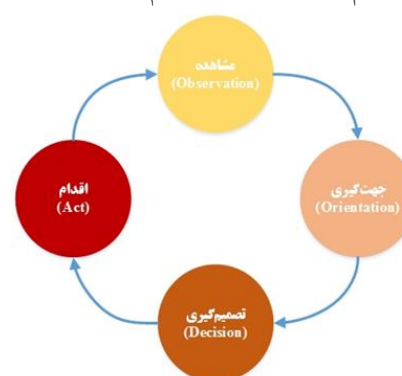
آن، تصمیم لازم اتخاذ می‌شود، مهم بوده و عنوان و محتوای دفاع را دستخوش تغییر قرار می‌دهد و نکته مهم‌تر که باید بر آن تأکید داشت این است که دفاع در هر یک از مراحل مورد اشاره، به معنی بی‌نیازی از سایر مراحل نیست و دفاع در هر مرحله، مکمل دفاع کلی از سرمایه مورد بحث خواهد بود هر چند تشخیص حمله در مراحل ابتدایی شکل‌گیری تهدید، قطعاً مانع از ایراد خسارات بیشتر خواهد بود و معمولاً هزینه بیشتری نیز به همراه دارد.

با توجه به فرآیند مورد اشاره برای شکل‌گیری تهدید، می‌توان دید که موقعیت اعمال تهدید از جانب بازیگر مهاجم نیز در هر یک از مراحل این فرآیند متفاوت است. به عنوان مثال، مرحله اقدام، متوجه خود سرمایه سایبری است (فضای نزدیک (شکل ۱))؛ در حالی که مرحله شناسایی، آماده‌سازی و طرح‌ریزی هم می‌تواند در محیط سرمایه مورد نظر انجام شود و هم بخش‌هایی از آن در محیط پیرامونی آن (فضای میانی (همان)) و یا حتی در محیط خود بازیگر مهاجم (فضای دور (همان))؛ و بالعکس، مرحله تصمیم‌گیری، به‌طور کامل در محیط اطلاعاتی مهاجم قرار دارد و وارد محیط بازیگر آماج نشده است (شکل ۶). از آنجاکه هنوز به فضای تعریف تهدید سایبری وارد نشده‌ایم، می‌توان گفت اقدامی که در این مرحله ممکن است علیه سرمایه سایبری صورت گیرد هم می‌تواند در بعد فیزیکی فضای سایبری باشد و هم در بعد اطلاعاتی و هم در بعد شناختی. به عبارتی هم می‌توان اقدامی فیزیکی (به عنوان مثال انفجار در خود سرمایه مورد نظر یا خرابکاری در منبع تأمین برق آن) برای نابودی یا از کار انداختن سرمایه سایبری را متصور شد و هم می‌توان انتظار یک عملیات سایبری (به عنوان مثال نفوذ و ایجاد اختلال در عملکرد) را علیه سرمایه سایبری مدنظر داشت و هم یک عملیات شناختی برای تغییر در محاسبات آماج.



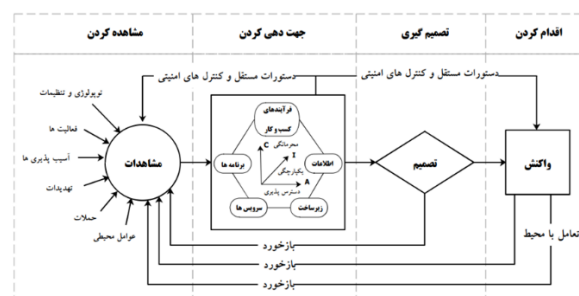
شکل ۶. محدوده صورت‌بندی تهدید (محقق).

قدرت، اراده و تصمیم) برمی‌آید. به عبارتی در این مرحله هدف‌گذاری صورت می‌گیرد. با تعیین هدف، اقدام به شناسایی نقاط ضعف و آسیب‌پذیری در آماج نموده و برای نفوذ و رخنه از طریق این آسیب‌پذیری‌ها، به دنبال ایجاد مقدمات، ابزارها و تسلیحات لازم خواهد بود و پس از فراهم‌سازی ابزارها، دست به اقدام خواهد زد. در چرخه فرماندهی و کنترل اودا (شکل ۳) نیز همین مراحل وجود دارد: مشاهده (شناسایی)، جهت‌گیری (انتخاب)، تصمیم (آماده‌سازی) و اقدام.



شکل ۳. چرخه اودا [۴۱].

البته مدل‌های دیگری نیز برای چرخه اودا در فضای سایبری ارائه شده است که به‌طور نمونه می‌توان به مدل وینسنت لندرز (شکل ۴) اشاره کرد [۴۲].



شکل ۴. مدل وینسنت لندرز [۴۳].

شکل ۵، توالی مراحل مورد اشاره در شکل‌گیری و عملیاتی سازی تهدید را نشان می‌دهد.



شکل ۵. فرآیند شکل‌گیری تهدید ناظر به چرخه اودا (محقق).

همان‌گونه که پیش‌ازین نیز اشاره شد، اینکه در کدام یک از این مراحل، تهدید مورد شناسایی قرار می‌گیرد و برای مقابله با

۵.۲. تهدید سایبری

تعاریف و برداشت‌های متعددی از تهدید سایبری ارائه شده است که بعضاً با مفاهیمی همچون مخاطره، آسیب‌پذیری، رخداد یا حادثه و رویداد نیز اشتراک معنایی پیدا کرده و شاید همین برداشت‌های مختلف باعث اختلاف در تعیین و تبیین مفهوم دفاع سایبری گردد [۴۴]. بر اساس تعریف سازمان فناوری اطلاعات، مخاطرات موجود در فضای سایبری را تهدید سایبری گویند. تهدید سایبری یک عامل بالقوه (پتانسیل) برای نقض امنیت در فضای سایبری است. تهدید سایبری در صورتی وجود خواهد داشت که یک پیشامد، قابلیت، کنش یا رخداد که می‌تواند در امنیت سایبری رخنه ایجاد نموده و منجر به صدمه شود به وجود بیاید. این بدان معنی است که یک تهدید سایبری، یک خطر بالقوه است که ممکن است منجر به بهره‌برداری از یک آسیب‌پذیری امنیتی شود [۸].

طبق تعریف ENISA، آسیب‌پذیری، وجود ضعف یا خطا در طراحی یا پیاده‌سازی است که می‌تواند به رویداد ناگهانی و نامطلوب منجر شود و باعث به خطر انداختن امنیت و نقض سیاست‌های امنیتی سامانه، شبکه، نرم‌افزار یا پروتکل می‌شود. نفوذ با سوءاستفاده از آسیب‌پذیری‌ها صورت می‌گیرد [۴۵] و البته این ضعف‌ها، ذاتی است [۴۶] و در هر سامانه، نرم‌افزار و یا شبکه به‌مرور کشف و برطرف می‌شود و ممکن است تا قبل از برطرف شدن مورد سوءاستفاده یا اصطلاحاً بهره‌جویی قرار گیرد.

بر اساس استاندارد ISO ۲۷۰۰۱ [۴۷] که استاندارد پیشرو در بحث اجرای «سیستم‌های مدیریت امنیت اطلاعات» است سه نوع مختلف از مسائل امنیتی ممکن است وجود داشته باشد که در هنگام تلاش برای حل و فصل حوادث امنیتی باید به‌دقت شناسایی شوند. این تفکیک از این جهت مهم است که اقدامات و راهکارهای در نظر گرفته‌شده در مواجهه با هر یک از این مسائل ممکن است متفاوت باشد. این مفاهیم تحت عنوان رویدادها، حوادث و عدم انطباق‌ها شناخته می‌شوند.

یک رویداد امنیتی زمانی رخ می‌دهد که واقعه‌ای به وجود بیاید که ممکن است بر سطوح مخاطره تأثیر بگذارد؛ مانند عدم انطباق سیاست‌ها و شکست کنترل‌های تعیین‌شده. این رویدادها

نباید لزوماً بر کسب‌وکار و یا اطلاعات شرکت تأثیرگذار باشند [۴۸]. یک رویداد امنیتی تغییر در رفتار عادی یک سیستم، فرآیند، محیط یا گردش کار معین است. به عبارت دیگر وقتی چیزی اتفاق می‌افتد (مثبت یا منفی)، یک رویداد خواهیم داشت.

حادثه زمانی رخ می‌دهد که یک یا چند رویداد امنیتی به سطحی برسند که در آن، هم عملیات تجاری و هم امنیت اطلاعات به خطر افتاده باشد (و این به معنی از دست دادن اطلاعات خواهد بود). در چنین مواردی برای جلوگیری از تأثیرات منفی بر سازمان، نیاز به اقدام در مقابل حادثه وجود دارد [۴۸]. در زیر (شکل ۷) مثال‌هایی از رویداد امنیتی در مقایسه با حادثه امنیتی متناظر آورده شده است. همچنین بر اساس استاندارد ISO ۲۷۰۰۱، عدم انطباق به هر وضعیتی که در آن الزامی وجود دارد و آن الزام برآورده نمی‌شود اطلاق می‌شود (به‌عنوان مثال عدم ایجاد نسخه‌های پشتیبان در صورت نیاز، همان‌طور که در خط‌مشی پشتیبان‌گیری تعیین شده است). هم یک رویداد امنیتی و هم یک حادثه امنیتی را می‌توان به‌عنوان یک عدم انطباق تلقی کرد [۴۸]. همچنین می‌توان گفت هر حادثه امنیتی، یک رویداد است اما هر رویدادی، لزوماً یک حادثه نیست (شکل ۸).



شکل ۷. مقایسه حادثه و رویداد امنیتی [۴۸].

سازمان پدافند غیرعامل، همه موارد یادشده بالا را در قالب تهدید عنوان کرده و با تعریف عاملی تحت عنوان شدت تهدید، فاصله‌گذاری بین این مفاهیم را مدیریت کرده است. لذا تهدیدات سایبری علیه سرمایه‌های ملی سایبری در پنج سطح دسته‌بندی می‌شود: خیلی زیاد (فاجعه)، زیاد (بحران)، متوسط (حادثه امنیتی عمده)، کم (حادثه امنیتی) و خیلی کم (رویداد امنیتی) [۱۶].

در مبحث دسته‌بندی رخدادها سایبری در آمریکا، این رخدادها به‌صورت مشابهی تحت عنوان طرح بررسی شدت

رخداد سایبری دسته‌بندی شده‌اند [۴۹]. در این رویکرد با مقیاس‌گذاری و امتیازدهی که بر روی ۸ مؤلفه صورت می‌گیرد،



شکل ۸ مقایسه رویداد، عدم انطباق و حادثه سایبری [۴۸].

حوادث دسته‌بندی می‌شوند: تأثیر عملکردی، فعالیت مشاهده‌شده، محل فعالیت مشاهده‌شده، ویژگی‌های بازیگر، تأثیر اطلاعات، قابلیت بازیابی، وابستگی بین بخشی و تأثیر بالقوه. وضعیت مشابهی برای دسته‌بندی حوادث سایبری در فرانسه وجود دارد [۵۰].

بر اساس تعریف موسسه ملی استاندارد و فناوری آمریکا، هر شرایط یا رویدادی با قابلیت تأثیر نامطلوب بر عملیات سازمانی (شامل مأموریت، عملکرد، تصویر یا شهرت)، دارایی‌های سازمانی یا افراد از طریق یک سیستم اطلاعاتی به‌وسیله دسترسی غیرمجاز، تخریب، افشا، دست‌کاری اطلاعات و/یا انکار سرویس، تهدید سایبری نام دارد. همچنین، توانایی بالقوه یک منبع تهدید برای بهره‌جویی موفقیت‌آمیز از یک آسیب‌پذیری خاص سیستم اطلاعاتی نیز در تعریف تهدید سایبری قرار می‌گیرد [۵۱]. سازمان پدافند غیرعامل نیز دقیقاً همین تعریف از تهدید را اتخاذ کرده است [۱۶]. همان‌گونه که از این تعاریف برمی‌آید، در فضای سایبری نیز تهدید، بر مفهوم آسیب‌پذیری تکیه دارد و به معنای آسیب و ایراد قطعی خسارت نیست و با توجه به بالقوه بودن امکان نقض امنیت در فضای سایبری، سخن از طیفی از اقدامات در قالب تهدید به میان می‌آید. از سوی دیگر برای پی بردن به مفهوم تهدید سایبری و مرز قائل شدن بین تهدید، آسیب‌پذیری و مخاطره در فضای سایبری، باید ماهیت دارایی سایبری را شناسایی کرد. دارایی‌ها مشتمل بر اشخاص، اشیاء و اطلاعات می‌شود. اشخاص هم به کارمندان و هم به ذینفعان یک شرکت یا یک زیرساخت اشاره می‌کند. اشیاء مشتمل بر دارایی‌های مشهود و نامشهود دارای

ارزش سازمان می‌شود (میزان ارزش در اینجا موضوع بحث نیست). اطلاعات نیز به هر نوع داده مربوط به آن دارایی مانند حساب‌های کاربری، رکوردها و ... برمی‌گردد. این سه منبع، موضوع تهدید، مخاطره و آسیب‌پذیری قرار می‌گیرند. بر این اساس تهدید عبارت از اقدامی است که احتمال آسیب، صدمه، خطر یا پیامدهای منفی را برای یک شخص، گروه، سازمان یا موجودیت مطرح می‌کند. همچنین تهدید ممکن است به یک خطر یا مخاطره قریب‌الوقوع اشاره کند که می‌تواند باعث آسیب یا صدمه به دارایی‌های مورد اشاره شود. تهدیدها می‌توانند از منابع مختلفی از جمله افراد، گروه‌ها یا رویدادهای طبیعی ناشی شوند و ممکن است عمدی یا غیرعمدی باشند؛ بنابراین سه نوع اصلی تهدید وجود دارد:

- تهدیدات طبیعی مانند سیل، طوفان، گردباد، زلزله
- تهدیدهای ناخواسته مانند دسترسی اشتباه یک کارمند به اطلاعات اشتباه
- تهدیدهای عمدی مانند نرم‌افزارهای جاسوسی، بدافزار یا اقدامات یک کارمند ناراضی [۴۸].

۶.۲. دفاع سایبری

به‌کارگیری اقدامات حفاظتی مؤثر برای به دست آوردن یک سطح مناسب از امنیت سایبری به‌منظور تضمین عملکرد و عملیات دفاعی را دفاع سایبری می‌گویند. این موضوع به‌وسیله اقدامات حفاظتی مناسب برای کاهش مخاطره امنیتی به یک سطح قابل‌پذیرش حاصل می‌شود. دفاع سایبری از وظایف و تکالیف حفاظت، کشف، پاسخ و بازیابی تشکیل شده است [۵۲]. همچنین دفاع سایبری عبارت است از قابلیت‌های سازمان‌یافته برای محافظت در مقابل حمله سایبری یا کاهش و بازیابی سریع اثرات آن [۵۳]. درجایی دیگر دفاع سایبری اعمالی است که به‌وسیله یک‌طرف ارتباطی انجام می‌شود که دارایی‌هایش را در مقابل وقوع حمله محافظت می‌کند. دفاع مؤثر در سامانه‌های الکترونیکی نوعاً مبتنی است بر شناسایی، مجزا سازی، گزارش، بازیابی و خنثی‌سازی [۵۴]. پدافند سایبری عبارت است از بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیر سایبری کشور به‌منظور ایجاد بازدارندگی، پیشگیری، ممانعت از انجام، تشخیص به‌موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم

گشت زنی در جلوگیری و غلبه بر جنایتکارانی که می‌توانند دیده شوند، مؤثر هستند. ولی برای مقابله با جنایات پیچیده‌ای که در پشت درهای بسته که مورد گشت زنی قرار نمی‌گیرند انجام شود، به‌تنهایی مؤثر نیستند. برای این‌گونه جنایتکاران حرفه‌ای، شهرها نیاز به استفاده از کارآگاه‌های ماهر دارد. کارآگاهان به‌جای گشت زنی و نظارت در سطح شبکه، اطلاعات را جمع‌آوری، بررسی و شواهد را تجزیه و تحلیل نموده و به‌طور فعالانه و هوشمند مظنونین را کشف می‌کنند. دفاع سایبری عامل در سطح فضای سایبری، عملکردی مشابه عملکرد کارآگاهان دارد و این منافاتی با حضور افسران پلیس در سطح شهر ندارد [۱۳]؛ بنابراین می‌توان گفت هم‌زمان دفاع عامل و غیرعامل در فضای سایبری ضرورت دارد و هر یک کارکرد خود را دارند و مکمل یکدیگر هستند و پرداختن به هر یک از این عناوین، به معنای نفی دیگری نیست [۱۳، ۲۸، ۵۷، ۵۸].

تقسیم دفاع سایبری به فعال و غیرفعال، تنها تقسیم‌بندی این حوزه نیست و همان‌گونه که برخی منابع ذکر کرده‌اند، این تقسیم‌بندی، تقسیم‌بندی دقیقی نیست. در ادامه به تقسیم‌بندی‌های مختلف اشاره خواهیم کرد. ذکر این نکته در اینجا ضروری به نظر می‌رسد که عبارت Active Defense به دو معنا ممکن است بکار رود. چنانچه عبارت مورد اشاره در برابر عبارت Passive استفاده شود، به معنای عامل بکار خواهد رفت و اگر در قیاس با عبارت Reactive مورد استفاده قرار گیرد به معنای دفاع فعال خواهد بود [۵۹] به عبارتی، معنای اول ناظر به اقدامات مورد استفاده در یک چارچوب دفاعی است و معنای دوم، خود چارچوب دفاعی را مدنظر دارد.

یک تقسیم‌بندی دیگر، دفاع سایبری را به دفاع فعال، دفاع مستحکم و دفاع تاب‌آور تقسیم می‌کند [۲۸]. در این تقسیم‌بندی، از منظر نوع اقداماتی که در مقابله با تهدید در نظر گرفته می‌شود به مسئله دفاع، نگرسته می‌شود. در این دیدگاه دفاع سایبری را می‌توان در محدوده وسیعی از اقدامات، از پیشگیری و پاسخ تا بازدارندگی و بازجویی گسترش داد [۵۸].

یک نگاه دیگر به مسئله دفاع سایبری، نگاشت آن به موضوع امنیت و سپس تقسیم‌بندی آن است. در این مدل، بر اساس آنچه گارتنر به تصویر می‌کشد (شکل ۹)، هر چه از امنیت فناوری

سایبری به سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخصصین سایبری اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم و گروه‌های تحت حمایت پنهان دولت‌های متخاصم به‌نحوی که امکان تهاجم سایبری را از کلیه متخصصین سلب نماید [۱۶]. از سوی دیگر دفاع سایبری، مجموعه اقدامات بازدارنده، رفع کننده، دفع کننده و بازیابی کننده که به‌منظور پیشگیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری انجام می‌گیرد تعریف شده است [۵۵]؛ و در جای دیگر دفاع سایبری عبارت است از یک مکانیسم دفاعی شبکه رایانه‌ای که شامل پاسخ به اقدامات و حفاظت از زیرساخت‌های حیاتی و تضمین اطلاعات برای سازمان‌ها، نهادهای دولتی و سایر شبکه‌های ممکن است و علاوه بر پیشگیری و شناسایی (آشکارسازی) روی تولید پاسخ به‌موقع به دو چیز، حملات و تهدیدات تمرکز می‌کند به‌نحوی که هیچ زیرساخت یا اطلاعاتی دچار تغییر (دست‌کاری) نشود [۵۶].

آنچه از تعاریف ارائه شده استفاده می‌شود این است که دو محور کلی در دفاع سایبری مدنظر است: کشف و پاسخ. دقت در عبارات فوق، روشن می‌سازد که موضوع کشف یا به‌صورت مستتر در تعریف آورده شده و یا با عباراتی مثل شناسایی، تشخیص و هشدار، برجسته می‌شود و موضوعاتی همچون جمع‌آوری اطلاعات، اشراف اطلاعاتی، آگاهی وضعیتی سایبری و تحلیل اطلاعات در این بخش قرار می‌گیرد. همچنین مقوله پاسخ نیز طیف وسیعی از مفاهیم را در خود جای داده است. مفاهیمی همچون حفاظت، رفع کردن، دفع کردن، بازیابی، بازدارندگی، پیشگیری و ممانعت از انجام نیز ذیل پاسخ قرار می‌گیرند. تفکیک انواع مختلف پاسخ همچنان که در ادامه خواهیم دید با شاخص‌های چندگانه (زمان، نوع و فضای اقدام) صورت می‌گیرد.

مقایسه جالبی بین فضای سایبری و محیط شهروندی عمومی در بحث دفاع در کار اصغری و همکاران صورت گرفته است. نظارت امنیتی بر شبکه‌ها و ابزارهای انتهایی، کاری مشابه فرستادن افسرها به سطح شهرها جهت اعمال محدودیت‌های لازم و مراقبت از وقوع جرم است. در دنیای واقعی، نیروهای

تفاوت‌های اساسی

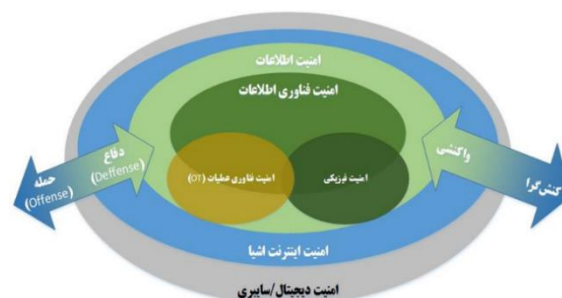
- تمرکز راهبردی: هدف امنیت سایبری جلوگیری از حوادث از طریق سیاست‌ها، آگاهی کاربر، کنترل‌های دسترسی و پلتفرم‌هایی است که نفوذ را دشوارتر می‌کند و درواقع تمرکز بر این است که آسیب‌پذیری‌ها را قبل از اینکه مورد سوءاستفاده قرار گیرند، ببندند و یا برطرف کنند. در مقابل، دفاع سایبری با این طرز فکر کار می‌کند که دشمنان مصمم و مشخص، بدون توجه به کنترل‌های امنیتی، بالاخره راه‌هایی برای نفوذ پیدا خواهند کرد. لذا این رویکرد بر روی شناسایی سریع ناهنجاری و تهدید، در کنار اجرای طرح‌های پاسخ برای به حداقل رساندن اثرات رخنه تمرکز می‌کند.

- مجموعه ابزارهای پشتیبانی: در انواع ابزارهای مورد استفاده، به‌ویژه در مورد ابزارهای حفاظتی مانند ضدبدافزارها، فایروال‌ها و سامانه‌های پیشگیری از نفوذ (بین دفاع و امنیت) همپوشانی‌هایی وجود دارد. بااین‌حال، در مورد استقرار و پیکربندی این سامانه‌ها بر اساس یک تفکر امنیتی یا تفکر دفاعی، انگیزه‌ها متفاوت خواهد بود. گروه‌های امنیتی، ممیزی، اسکن و آزمون‌های نفوذ را به‌صورت پیش‌کنش‌گرانه انجام می‌دهند - یعنی سعی می‌کنند آسیب‌پذیری‌ها را قبل از وقوع حوادث، شناسایی و اصلاح کنند. حال‌آنکه ابزارهای دفاعی مانند SIEM ها بیشتر بر روی شناسایی حملات فعال به‌صورت واکنشی تمرکز می‌کنند.

محدوده عملکردی: امنیت سایبری دامنه عملکردی گسترده‌ای را که شامل آگاهی، مدیریت آسیب‌پذیری، مدیریت هویت و دسترسی، حفاظت از داده‌ها و کنترل‌های امنیتی برنامه است در بر می‌گیرد. قابلیت‌های دفاع سایبری به‌صورت محدود و باریک، بیشتر بر اطلاعات تهدید، تجزیه و تحلیل رفتار برای شناسایی ناهنجاری‌ها و هماهنگ‌سازی پاسخ‌ها از طریق طرح‌ها و رویه‌های پاسخ به حادثه متمرکز است. در یک رابطه متقابل، امنیت پایه قوی به دفاع سایبری اجازه می‌دهد تا تلاش‌ها را فقط بر روی تهدیدات واقعاً پیچیده متمرکز کند و در مقوله دفاع سایبری، اطلاعات تهدید به بهبود مستمر برنامه‌های امنیتی کمک می‌کند. اساساً وجود عبارتی تحت عنوان «امنیت سایبری دفاعی» حکایت از عام بودن امنیت بر دفاع است و به معنی تمرکز بر

اطلاعات به سمت امنیت سایبری حرکت می‌کنیم، اقدامات امن سازی نیز از حالت واکنشی به سمت اقدامات کنشی، سوق پیدا می‌کند و یا به عبارتی از حالت دفاعی به وضعیت هجومی تغییر شکل پیدا می‌کند [۶۰].

البته ذکر یک نکته در اینجا خالی از لطف نیست و آن اینکه مرزهای بین دفاع فعال و غیرفعال و یا تقسیم‌بندی‌های دیگری که ارائه می‌شود، اغلب روشن نیست و دارای ابهام بوده، بستگی به فناوری‌های خاص مورد استفاده در فرآیند دفاع یا در عملیات دفاعی سایبری دارد [۶۱].



شکل ۹. مدل امنیت فناوری اطلاعات از دیدگاه گارتنر [۴۴].

قاسمی گل در مقاله خود [۶۲] جهت ارائه چارچوبی برای سامانه‌های پاسخ به نفوذ، دو مقوله مدیریت هشدار و سامانه پاسخ را اساسی‌ترین ارکان سامانه‌های حفاظت از امنیت در فضای سایبری عنوان می‌کند و در ادامه با مروری جامع بر تقسیم‌بندی‌های ارائه‌شده از پاسخ به حملات سایبری در مقالات، دسته‌بندی از سامانه‌های پاسخ ارائه می‌دهد که در شکل ۱۰ آورده شده است.

۱.۶.۲. امنیت و دفاع سایبری

امنیت سایبری و دفاع سایبری دو رشته به‌هم‌پیوسته را نشان می‌دهند که بر حفاظت از دارایی‌ها و زیرساخت‌های سایبری متمرکز شده‌اند. امنیت سایبری بیشتر بر پیشگیری - کاهش سطوح حمله و مقاوم‌سازی سیستم‌ها در برابر خطر اشغال و دفاع سایبری بر تشخیص تهدید و به حداقل رساندن تأثیرات در هنگام وقوع حوادث متمرکز است. سیاست‌های امنیت سایبری و قابلیت‌های دفاع سایبری درحالی‌که از نظر دامنه متفاوت هستند، برای ایجاد حفاظت لایه‌ای، به‌خصوص برای اهداف با ارزش بالا همکاری نزدیکی دارند. بر این اساس می‌توان وجوه اشتراک و افتراق زیر را بین این دو مقوله برشمرد [۶۳].

تفاوت در این است که دفاع سایبری، راهبرد به کار گرفته شده برای محافظت از سیستمها و اطلاعات و داده‌های موجود در آن‌ها و تمرکز امنیت سایبری بر نحوه اجرای این راهبردهاست. درواقع نمی‌توان امنیت سایبری را از دفاع سایبری جدا کرد. هر دو مؤلفه‌های لازم برای محافظت از اطلاعات در برابر هکرها و سایر انواع شکست‌های امنیتی هستند.

۲.۶.۲. شاخص‌های تفکیک انواع دفاع سایبری

در [۵۷] چهار شاخص برای ارزیابی و تفکیک انواع دفاع فعال سایبری ارائه می‌کند. این شاخص‌ها عبارت‌اند از دامنه تأثیرات (داخلی، خارجی)، درجه همکاری (مشارکتی و غیر مشارکتی)، انواع تأثیرات (اشتراک‌گذاری اطلاعات تهدید یا حمله، جمع‌آوری، مسدودسازی و پیش‌دستی یا پیشگیری) و درجه خودکارسازی (خودکار و دستی). از بین شاخص‌های مورد اشاره، دامنه تأثیرات با توجه به تعریفی که از فضای دور و فضای نزدیک قبلاً ارائه شد [۲۱] مورد توجه قرار خواهد گرفت. همچنین انواع تأثیرات را در قالب شاخص نوع اقدام مدل‌سازی می‌نماییم و به دو دسته تقسیم می‌شوند: عامل و غیرعامل و منظور از اقدام عامل، اقدامی است که در مواجهه با یک حمله مشخص جاری صورت می‌گیرد و اقدام غیرعامل، اقداماتی است که در برابر رخدادهای عمدتاً غیرعمدی صورت می‌گیرد و مواجهه با حمله سایبری ندارد [۵۷].

چنانچه از منظر بردار زمانی به مسئله دفاع پرداخته شود دفاع به سه مقوله دفاع قبل از حمله، دفاع حین حمله و دفاع پس از حمله تقسیم می‌شود [۵۹]. البته باید در اینجا این نکته را یادآور شد که میان تهدید و حمله، اشتراک معنایی در نظر گرفته شده است و چنانچه از این اشتراک معنایی صرف‌نظر شود، می‌توان گفت دفاع قبل از حمله، درواقع دفاع در برابر تهدید است (که می‌تواند قریب‌الوقوع و یا غیرمحمتمل باشد (شکل ۶)) و براساس آنچه در مورد تهدید، بیان شد ناظر به بعد ذهنی تهدید نیز خواهد بود. درواقع برای یک حمله سایبری، یک فرآیند در نظر گرفته می‌شود که به «زنجیره کشتار سایبری» [۶۵] معروف است و کل این فرآیند در چرخه اودا (شکل ۳) در مرحله اقدام قرار می‌گیرد.

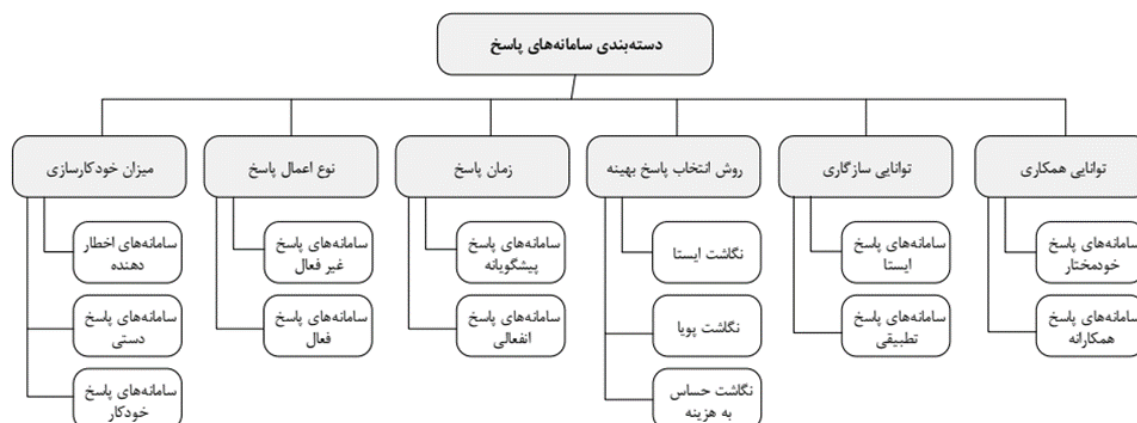
ساخت و نگهداری سیستم‌های انعطاف‌پذیری است که از تهدیدات جلوگیری، آن‌ها را شناسایی و درنهایت به آن‌ها پاسخ می‌دهند. اگرچه ممکن است ساده به نظر برسد اما امنیت دفاعی دقیقاً همان‌طور که از اسم آن به نظر مارسد عمل می‌کند: ایجاد امنیت با یک رویکرد دفاعی که برای جلوگیری از وقوع حمله در همان گام اول طراحی شده است [۶۴].

مشترکات کلیدی

امنیت سایبری و دفاع سایبری در عین داشتن مراکز ثقل متفاوت، مشترکات قابل توجهی نیز دارند [۶۳]:

- وابستگی متقابل: پیشگیری قوی که توسط امنیت سایبری هدایت می‌شود، اختلال و موارد مثبت کاذبی را که راه‌حل‌های دفاع سایبری باید مدیریت کنند، کاهش می‌دهد. کنترل‌های دسترسی دقیق و تنظیمات مقاوم‌شده، به ابزارهای دفاعی اجازه می‌دهد تا تشخیص‌ها را فقط روی رفتارهای واقعاً غیرعادی تنظیم کنند. به همین ترتیب، دید گسترده‌تر به تهدیداتی که دفاع سایبری ارائه می‌کند، گروه‌های امنیتی را راهنمایی می‌کند تا کنترل‌ها و سیاست‌ها را برای تطبیق بهتر بر حملات دنیای واقعی از طریق ویژگی‌هایی مانند فهرست‌های اعتبار IP، فهرست بندی نقطه پایانی مجاز برای مسدود کردن ابزارهای مخرب و به‌روزرسانی‌های آموزش آگاهی کاربر را تطبیق دهند.
- استقرارهای یکپارچه: برای محافظت جامع در برابر طیف وسیعی از تهدیدات، از پایه تا پیشرفته، کنترل‌های پیشگیرانه امنیت سایبری نیاز به تقویت از طریق قابلیت‌های دفاع سایبری فعال مانند نظارت بر شبکه، تمرین‌های شکار تهدید و فرآیندهای واکنش به حادثه دارند. هیچ پشته امنیتی ایستایی نمی‌تواند در مقابل هر بردار حمله به‌ویژه تهدیدات جدید جلوگیری کند. دفاع سایبری دید و کنترل لازم را برای پاسخگویی پویا به هر چیزی که از کنترل‌های پایه فرار می‌کند، ارائه می‌کند.

ادغام هر دو دیدگاه تحت پلتفرم‌های تحلیل و هماهنگی مشترک، اشتراک‌گذاری یکپارچه اطلاعات، پاسخ هماهنگ به تهدید، تنظیمات بهینه سیستم و گزارش یکدست را امکان‌پذیر می‌کند؛ بنابراین در پاسخ به این سؤال که تفاوت بین امنیت سایبری و دفاع سایبری چیست؟ به بیان ساده می‌توان گفت:



شکل ۱۰. دسته‌بندی سامانه‌های پاسخ بر اساس دیدگاه‌های مختلف [۶۲].

اشاره کرد. اشناير در کتاب‌ها و مقالات خود به اهمیت و کیفیت لایه‌بندی در دفاع سایبری اشاره می‌کند [۶۷-۶۹]. همچنین برخی استانداردها با در نظر گرفتن همین راهبرد دفاعی تدوین شده‌اند مانند NIST SP ۸۰۰-۵۳ [۷۰] و ISO ۲۷۰۰۱ [۴۷]. در استاندارد NIST SP ۸۰۰-۵۳ واپایش‌های متعددی وجود دارد که با دفاع در عمق مرتبط هستند از جمله: کنترل دسترسی به سیستم‌ها و اطلاعات بر اساس سیاست‌های امنیتی (AC-۳)، محدود کردن دسترسی فیزیکی به تأسیسات و تجهیزات (PE-۳)، حفاظت از مرزهای سیستم با استفاده از فایروال‌ها و سیستم‌های تشخیص نفوذ (SC-۷)، ارزیابی آسیب‌پذیری (RA-۵) و استفاده از آنتی‌ویروس و سایر ابزارهای امنیتی برای مقابله با بدافزارها (SI-۳). در استاندارد ISO ۲۷۰۰۱ نیز مدیریت حقوق دسترسی (A.۹.۲.۳)، کنترل دسترسی فیزیکی (A.۱۱.۱.۱)، مدیریت آسیب‌پذیری‌ها (A.۱۲.۱.۳) و کنترل‌های شبکه (A.۱۳.۱.۱) از مصادیق وجود لایه‌های مختلف دفاعی یا همان دفاع در عمق هستند.

بنابراین مجدداً بر این نکته تأکید می‌شود که مطرح کردن یک راهبرد یا رویکرد در دفاع سایبری، به معنی نفی سایر رویکردها و راهبردها نیست و بر اساس میزان اهمیت و حیاتی بودن یک سرمایه سایبری، می‌توان از لایه‌های مختلف دفاعی برای محافظت از آن در برابر تهدیدات استفاده کرد.

۲.۷.۲. دفاع غیرفعال

دفاع غیرفعال عبارت است از: دیوار آتش، بهداشت (سایبری) - آموزش یک نیروی کار تحصیل کرده تا در برابر

بنابراین از این منظر دفاع قبل از حمله باید دربرگیرنده مرحله تصمیم و ماقبل آن نیز باشد و دفاع در حین و پس از حمله، مرحله اقدام را در برمی‌گیرد. آنچه [۶۵] در خصوص مقابله مرحله‌به‌مرحله با حملات سایبری (نفوذ سایبری) توضیح می‌دهد در سطح تاکتیکی و برگرفته از دکترین هدف‌گیری نظامی وزارت دفاع آمریکا است [۶۶] که فرآیندی مشتمل بر مراحل «یافتن، تثبیت، ره‌گیری، هدف‌گیری، درگیری و ارزیابی» است و معادل آن در فضای سایبری عبارت خواهد بود از: «شناسایی، تسلیح، تحویل، بهره‌جویی، نصب، فرماندهی و کنترل، اقدام». در هر یک از این مراحل می‌توان حمله را شناسایی نموده (دفاع حین حمله) و مانع از اجرای گام‌های بعدی شد.

۲.۲. انواع دفاع سایبری

بر اساس شاخص‌های بیان‌شده بالا و مطالبی که در مقدمه به آن‌ها اشاره شد، در ادامه به تبیین انواع دفاع سایبری که در مقالات مورد استفاده و اشاره قرار گرفته‌اند پرداخته می‌شود.

۱.۷.۲. دفاع در عمق سایبری

همان‌گونه که قبلاً عنوان شد، دفاع در عمق، یک راهبرد نظامی قدیمی است که به معنای ایجاد خطوط مختلف دفاعی و دشوار کردن مسیر مهاجم برای دستیابی و تصرف اهداف است. بااین‌حال، کاربرد این مفهوم در حوزه امنیت سایبری به‌طور رسمی در دهه‌های اخیر (از ۱۹۸۰ به این‌طرف) و با گسترش فناوری‌های اطلاعاتی و افزایش تهدیدات سایبری مطرح شده است. ازجمله دانشمندانی که ایده دفاع در عمق را در فضای سایبری مطرح کرده‌اند می‌توان به بروس اشناير و ریچارد کلارک

خطاها یا تخلفاتی که می‌تواند منجر به نفوذ سایبری شود مراقبت و محافظت نماید- فناوری شناسایی، «ظرف‌های عسل» یا فریب‌هایی که به‌عنوان منحرف‌کننده ایفای نقش می‌کنند و مدیریت مخاطرات فضای سایبری از طریق دفاع جمعی، مشارکت‌های هوشمند، آموزش اطلاعات، آگاهی وضعیتی برتر و ایجاد محیط‌های شبکه‌ای ایمن و تاب‌آور [۷۱]. همچنین دفاع غیرفعال سایبری به کلیه اقداماتی غیر از دفاع فعال سایبری گفته می‌شود که برای به حداقل رساندن اثربخشی تهدیدات سایبری علیه نیروها و دارایی‌های خودی انجام می‌شود [۵۷] و مصادیق آن نیز عبارت‌اند از فایروال‌ها، سامانه‌های کشف نفوذ و ابزارهای ضد بدافزار [۷۲] و نیز رمزنگاری، پنهان نگاری، مدیریت امنیت و تأیید، مدیریت و نظارت پیکربندی، ارزیابی مخاطره، پشتیبان گیری داده و بازیابی داده از دست‌رفته و ارائه آموزش‌های کلاسیک و مهارتی به کاربران [۵۷].

۳.۷.۲. دفاع تاب‌آور

تاب‌آوری یک فرآیند، توانایی و یا پیامد سازگاری موفقیت‌آمیز با شرایط تهدیدکننده است [۷۳]. تاب‌آوری سایبری، توانایی یک سیستم، سازمان، مأموریت یا فرآیند تجاری برای پیش‌بینی، مقاومت، بازیابی و تطبیق قابلیت‌ها در مواجهه با شرایط خصمانه، فشارها یا حملات به منابع سایبری است که برای عملکرد به آن نیاز دارد [۷۴]. تاب‌آوری سایبری ناظر به توانایی یک سامانه سایبری در ارائه مستمر نتایج مورد انتظار به‌رغم رویدادهای سایبری نامطلوب است. به بیان ساده، سامانه‌های سایبری باید بتوانند حتی در صورت وجود حملات سایبری مخرب به فعالیت خود ادامه دهند [۷۵]. در مقایسه با دیگر انواع دفاع سایبری و به‌جای جستجوی تهاجمی عاملان نقض امنیت و یا به‌جای ایجاد استحکامات در اطراف دارایی‌های کلیدی سایبری، می‌توان بر این موضوع تمرکز کرد که زیرساخت‌ها و خدماتی که بر ارتباطات شبکه‌ای متکی هستند به کار خود ادامه می‌دهند و خدماتی را که برای آن طراحی شده‌اند ارائه می‌کنند. لذا به‌جای دفاع سایبری تهاجمی یا مستحکم، یک رویکرد بالقوه عمل‌گرایانه‌تر نسبت به امنیت سایبری، دفاع سایبری تاب‌آور است. تاب‌آوری به‌خودی‌خود مبتنی بر پذیرش این اصل است که با توجه به آسیب‌پذیری‌های ذاتی فضای

سایبری، حوادث سایبری قطعاً رخ خواهند داد و تمرکز بر توانایی بازیابی از این حوادث یا بازگشت به حالت اولیه یا ایجاد انطباق با یک وضعیت جدید و تنظیم‌شده است. به‌عبارت‌دیگر، دفاع تاب‌آور، مربوط به شرایط پس از حمله و یا پس از کشف حمله است. دفاع سایبری تاب‌آور یک وجه مشترک با دفاع مستحکم دارد و آن این است که کاملاً معطوف به محیط داخل یا شبکه محلی مدافع است و با بیرون از این شبکه ارتباطی ندارد. در این رویکرد، مدیران شبکه و سیاست‌گذاران باید مطمئن شوند که سیستم‌ها و شبکه‌ها تاب‌آور هستند و می‌توانند در برابر حوادث مقاومت کنند. ایجاد تدابیر امنیتی در این سیستم‌ها، یک ویژگی اساسی و مهم برای رسیدن به چنین آمادگی محسوب می‌شود؛ بنابراین دفاع سایبری تاب‌آور را می‌توان به این صورت تعریف کرد: تضمین تداوم عملکرد سیستم و ارائه خدمات با ساخت شبکه‌های ارتباطی و اطلاعاتی باقابلیت درونی برای مقاومت یا انطباق همه‌جانبه با حوادث عمدی یا غیرعمدی [۲۸].

۴.۷.۲. دفاع مستحکم

همان‌طور که در تعریف دفاع غیرفعال بحث شد، اقداماتی مانند ایجاد دیوارهای آتش، نرم‌افزارهای ضد بدافزار، فناوری‌های تشخیص و دیگر اقداماتی که به آن‌ها اشاره شد، توسط برخی از متخصصین به‌عنوان اشکال دفاع غیرفعال و یا واکنشی نام‌گذاری شده است. باین‌حال، اگر به هدف نهایی این اقدامات توجه شود، مجموعه اقدامات مربوطه را نمی‌توان دقیقاً و صرفاً به‌عنوان غیرفعال نام‌گذاری کرد. هدف دیوارهای آتش و فیلترها و هر اقدام دیگری که برای جلوگیری از دسترسی مخرب به دارایی‌های کلیدی در نظر گرفته شده است، دقیقاً همین است: جلوگیری از دسترسی [۷۱]؛ یعنی اقداماتی انجام می‌شود که احتمال موفقیت هرگونه نفوذ یا حمله در رسیدن به اهداف خود را کاهش می‌دهد. مثالی از این دسته اقدامات در فضای حقیقی، ساخت قلعه‌ها و دژهاست. ایجاد چنین استحکاماتی به معنی وقوع حمله یا در برابر حمله در حال وقوع نیست بلکه باهدف محافظت از افراد داخل این استحکامات در برابر مهاجمان خارجی ساخته شده‌اند. روش‌هایی مانند نصب دیوارهای آتش یا قرار دادن فیلترها و اسکرین‌ها بر روی کابل‌های تبادل داده، همگی برای جلوگیری از دسترسی کد، اطلاعات یا

عوامل مخرب به سیستم‌های شبکه و سوءاستفاده از دارایی‌های موردنظر هستند؛ بنابراین می‌توان گفت این اقدامات، اقدامات غیرفعالی نیستند که در واکنش به یک حادثه انجام شده باشند بلکه اقداماتی هستند که برای ساختن استحکامات مجازی طراحی شده‌اند. علاوه بر نصب دیوارهای آتش و نرم‌افزارهای ضد بدافزار، دفاع سایبری مستحکم (FCD) را می‌توان با ایجاد امنیت در زیرساخت‌های پشتیبانی‌کننده فضای سایبری یعنی نرم‌افزارها، رایانه‌ها، مسیرها و سایر عناصر موردنیاز برای فعال کردن دامنه‌های برخپ نیز به دست آورد. ماهیت غیرقابل پیش‌بینی و شکننده شبکه‌های کامپیوتری گسترده بین‌المللی، یک ناامنی ذاتی و سامانمند در فضای سایبری ایجاد نموده [۷۶] و زیرساخت‌های آن را در برابر حوادث طبیعی، تصادفی یا مخرب و عمدی، آسیب‌پذیر می‌کند. به‌عنوان مثال بسته‌های داده ممکن است در حین انتقال به دلیل عبور از کابل‌های معیوب و خط‌پذیر، خراب شوند، رایانه‌های فردی ممکن است به‌مرورزمان خراب شوند و نرم‌افزارها ممکن است از کار بیافتند. ایجاد تدابیر امنیتی در تمام عناصر موردنیاز برای عملکرد شبکه‌های ارتباطی بین‌المللی، این آسیب‌پذیری‌های سامانه‌ای و قابل سوءاستفاده را کاهش می‌دهد. با توجه به موارد فوق می‌توان دفاع سایبری مستحکم را این‌گونه تعریف کرد: ایجاد شبکه‌های اطلاعاتی و ارتباطی تماماً امن به‌منظور ایجاد محیط‌های دفاعی در اطراف دارایی‌های کلیدی و به حداقل رساندن حوادث و آسیب‌های عمدی یا غیرعمدی [۲۸].

۵.۷.۲. دفاع فعال

بر اساس فرمایشات فرماندهی معظم کل قوا، دفاع فعال به شدیدترین حالت در مرز صلح و جنگ (شدیدترین حالت بازدارندگی و در مرز درگیری با رقیب) اطلاق می‌گردد. در دفاع فعال، ساختار، نیروها و فناوری سازمانی، کاربردی ترکیبی دارند. هم‌چنین باوجودی که مقاصد کشور، بازدارندگی است، اما برخی اهداف، سیاست‌ها و استراتژی‌های سازمانی حالت تهاجمی دارند [۷۷]. به گفته دنینگ دفاع فعال سایبری، اقدام دفاعی مستقیمی است که برای از بین بردن، خنثی کردن یا کاهش اثربخشی تهدیدات سایبری علیه نیروهای دوست و به‌صورت مجموعه انجام می‌شود [۵۷]. دفاع فعال سایبری عبارت است از

قابلیت هم‌زمان و بلادرنگ کشف، شناسایی، تجزیه و تحلیل و کاهش تهدیدها. دفاع سایبری فعال با استفاده از حسگرها، نرم‌افزار و اطلاعات و با سرعت شبکه عمل می‌کند تا فعالیت‌های مخرب را قبل از اینکه بر شبکه‌ها و سیستم‌ها تأثیر بگذارد به‌طور ایدئال شناسایی و متوقف کند. در این تعریف دو ویژگی بارز دفاع فعال عنوان شده است: اول بلادرنگ بودن تشخیص و دوم کاهش تهدیدات اساسی قبل از ایراد خسارت یا خرابی. بر این اساس دو مورد از مصادیق دفاع فعال عبارت‌اند از: تولید و انتشار کرم سفید و پرش آدرس؛ بنابراین، دفاع فعال سایبری بر اقدامات پیش‌دستانه برای مقابله با اثرات فوری یک حادثه سایبری، چه از طریق شناسایی و خنثی‌سازی نرم‌افزارهای مخرب و چه با تلاش عمدی برای پنهان کردن حضور برخپ دستگاه‌های هدف برای جلوگیری و مقابله با جاسوسی، تأکید می‌کند. البته اقدامات تهاجمی‌تری نیز وجود دارد که می‌توان برای دفاع از سیستم‌ها و شبکه‌ها مدنظر قرار داد. درحالی‌که کرم‌های سفید را می‌توان برای جستجو و مبارزه با نرم‌افزارهای مخرب استفاده کرد، [۷۸] و [۶] توضیح می‌دهند که چگونه می‌توان از آن‌ها برای تبدیل ابزارهای هکرها و متجاوزان احتمالی علیه خود آن‌ها و شناسایی نه‌تنها نرم‌افزار مهاجم، بلکه حتی سرورها و سایر دستگاه‌های سخت‌افزاری میزبان و توزیع‌کننده کد حمله نیز استفاده کرد. فرآیند اخیر در مقالات به‌عنوان «هک بک» شناخته می‌شود [۷۹، ۸۰]. هنگامی که دستگاه‌های منبع نفوذ یا حمله شناسایی شدند، می‌توان اقداماتی را انجام داد که آن دستگاه‌ها غیرفعال شوند یا از انجام اهداف آن‌ها جلوگیری شود. آنچه این اقدامات را قابل توجه می‌کند این است که آن‌ها فن‌هایی تهاجمی و آفندی هستند که فراتر از مرزهای شبکه مدافع عمل می‌کنند و با مهاجم مبارزه می‌کنند. بر اساس این تعریف می‌توان گفت که دفاع سایبری فعال درواقع یک پارادایم امنیتی است که از دو روش استفاده می‌کند: یکی شناسایی و کاهش تهدیدات به‌صورت بلادرنگ در شبکه‌های مدافع و دیگری، توانایی انجام اقدامات متقابل تهاجمی آفندی بیرونی [۲۸]. از آنجاکه بخش دوم یا روش‌های مورد استفاده در بخش دوم با توجه به ویژگی‌های فضای سایبری ازجمله گمنامی، می‌تواند دارای آثار و تبعات حقوقی بین‌المللی باشد، لذا می‌توان آن را تحت عنوان دفاع

فرافعال از مقوله دفاع فعال جدا کرد که در ادامه همین بخش به آن پرداخته خواهد شد. دفاع فعال را این‌گونه نیز تعریف کرده‌اند: اصطلاحی دربرگیرنده مجموعه اقدامات لازم امنیت سایبری میان تهاجم و تدافع غیرفعال سنتی است. این فعالیت‌ها در ۲ دسته کلی قرار می‌گیرند؛ دسته اول، تعامل‌های فنی بین یک مدافع و یک مهاجم را شامل می‌شود. دسته دوم اقدامات دفاع فعال شامل عملیات‌هایی برای توانمندسازی مدافعان در جمع‌آوری اطلاعات مربوط به عوامل تهدید، شاخص‌های موجود در اینترنت و دیگر ابزارهای سیاسی مانند تحریم‌ها، اتهامات و راه‌حل‌های تجاری است که می‌توانند رفتار عوامل مخرب را تغییر دهند. اصطلاح دفاع فعال مترادف با هک متقابل نیست و این دو نباید بجای یکدیگر به کار روند [۸۱].

ویژگی شاخص دفاع فعال در تعاریفی که از آن بیان شد، انجام اقدام تهاجمی در بیرون از شبکه خانگی مدافع است درحالی‌که در دفاع مستحکم، ویژگی اصلی، تمرکز پیشگیرانه و درون‌نگر این رویکرد به‌منظور به حداقل رساندن دسترسی به سیستم‌ها و شبکه‌های هدف است.

در این مقاله با توجه به ارائه نوع دیگری از دفاع تحت عنوان دفاع فرافعال، تمرکز دفاع فعال را بر اقداماتی قرار می‌دهیم که در قلمرو مدافع عمل می‌کنند اگرچه برای رصد حملات و پیشگیری از آن‌ها، می‌توان از شاخص‌ها و نشانه‌هایی که در فضای میانی وجود دارند استفاده کرد.

۶.۷.۲. دفاع فرافعال

همان‌گونه که گفته شد رویکردهای مختلفی به دفاع سایبری وجود دارد و تقسیم‌بندی‌های مختلفی برای آن ارائه می‌شود. در [۵۶] دفاع سایبری به سه دسته که مکمل یکدیگر هستند تقسیم می‌شود: غیرفعال، فعال و فرافعال. بر همین اساس، فعالیت‌های فرافعال، محیط سایبری را مقاوم و سخت می‌کند و حداکثر کارایی را برای زیرساخت‌های سایبری و همچنین عملکردهای مأموریتی حفظ می‌کند و به دنبال افزایش هزینه حمله برای مهاجم و کاهش مخاطرات برای محیط هدف است. وضعیت فرافعال، متکی به دفاع‌های سنجیده و پویا از طریق اطلاعات و شواهد به‌دست‌آمده از اطلاعات به مقابله با تهدیدات واقعی و بالقوه می‌پردازد. در حالت ایدئال، این رویکرد بر طیف کاملی از

قابلیت‌ها و توانمندی‌های یک سازمان - از دفاع شبکه، روابط عمومی، تلاش‌های حقوقی و دیگر عملیات تجاری - متکی است. موقعیت‌یابی فرافعال همچنین بر درک جامع و دقیق (و تا حد امکان، بلادرنگ) از شبکه خودی و همچنین توانایی جمع‌آوری و ادغام منابع اطلاعاتی خارج از آن شبکه برای ارزیابی کامل محیط تهدید تکیه دارد [۸۲]. در مقالات غیر مرتبط با فضای سایبری، عبارت فرافعال را به‌عنوان پیش‌کنش‌گرانه معنا کرده‌اند لکن در فضای سایبری، به‌جای آن عبارات دیگری نیز استفاده شده است. در [۶۲]، عبارت پیشگویانه به‌جای فرافعال بکار رفته و در تعریف آن، سامانه‌هایی که امکان پیش‌بینی حمله قبل از وقوع آن را می‌دهند ذکر شده است. این پیشگویی، عموماً دشوار بوده و مبتنی بر احتمالات و آنالیز کاربران فعلی و رفتار سامانه است. پاسخ پیشگویانه نیازمند ارتباط نزدیک شیوه تشخیص و شیوه پاسخ است به‌طوری‌که به‌محض تشخیص حمله، پاسخ صادر شود.

در [۱۳] دفاع فرافعال را به کنش‌گرایانه معنا کرده و بر اساس مراجع مورداستفاده، معادل دفاع فعال در نظر گرفته است. [۸۳] دو ویژگی را برای امنیت سایبری فرافعال در نظر می‌گیرد: اول شناسایی حملات بالقوه قبل از به ثمر نشستن آن‌ها و دوم ایجاد اقدامات متقابل پیشگیرانه بر اساس این شناخت. فن‌های دفاع سایبری فرافعال، در مقالات، نیاز به سطحی از تجزیه و تحلیل داده‌ها دارند. این روش‌های تحلیلی عمدتاً شامل تحلیل ترافیک شبکه، تشخیص ناهنجاری، تحلیل شبکه اجتماعی برای رفتار گروهی، تحلیل شبکه اجتماعی برای پیش‌بینی حمله سایبری و رویکردهای سری زمانی برای نظارت و شناسایی حملات سایبری را پوشش داده‌اند [۸۴]. یکی از ویژگی‌های دفاع فرافعال، این است که حیطه عمل آن در خارج از شبکه مورد دفاع قرار دارد. همچنان‌که در [۸۵] بیان می‌کند، وزارت دفاع آمریکا به‌جای آنکه منتظر حملات سایبری باشد و در هنگام وقوع، به آن‌ها پاسخ دهد باید به‌صورت فرافعال در بیرون از فضای سایبری آمریکا، به مانور پرداخته و با مشاهده و درک دشمنان در حال رشد و با دریافت مجوز، عملیات اطلاعاتی را برای اختلال، انکار یا تخریب توانایی‌ها و زیرساخت‌های آن‌ها قبل از رسیدن به اهداف موردنظر هدایت کند. شرکت‌های پیشرو

در حوزه سایبری نیز این رویکرد را در ساختار دفاعی خود وارد کرده‌اند. به عنوان مثال IBM رویکرد فرافعال را در بحث اطلاعات سایبری مدنظر قرار داده و به جای اینکه تنها اطلاعات فنی سایبری را بررسی کند، هم‌زمان به دنبال یافتن انگیزه‌ها، قابلیت‌ها، نیات، اهداف، آسیب‌پذیری‌ها و حتی در صورت امکان هویت بازیگران تهدید است [۸۶].

دفاع فرافعال سایبری، به نوعی تلاش فعالانه برای شناسایی حملات (قبل و حین وقوع حمله) و پاسخ هجومی علیه مهاجم یا منشأ شکل‌گیری تهدید است و اغلب در محیط پیرامونی و بیرونی شبکه (خارج از مرز دفاعی شبکه) یا سازمان مورد هدف است. دفاع سایبری که هدف خنثی نمودن عوامل خارجی تهدید را دارد دفاع فرافعال سایبری می‌نامند. هدف در این عملیات، شناسایی، رفتارشناسی و اقدام فرافعال (هجومی و کنترل‌شده) نسبت به عملکرد مهاجم یا مهاجمین سازمان‌یافته در محدوده دفاعی مرزهای جغرافیایی است. عنصر اطلاعات (جمع‌آوری و بهره‌برداری از اطلاعات و تولید اطلاعات تهدید) و فریب از مفاهیم اصلی در این رویکرد هست [۸۷]. در اغلب مقالات مورد مطالعه، دفاع فرافعال به عنوان بخشی از دفاع فعال سایبری عنوان شده است و ویژگی‌هایی از جمله هماهنگی، ممانعت، حفاظت، کاهش و بازیابی را شامل می‌شود [۸۸].

۷.۷.۲. دفاع روبه‌جلو

وزارت دفاع آمریکا، اولین بار در سال ۲۰۱۳ سند راهبرد سایبری خود را ارائه و سپس در سال‌های ۲۰۱۵، ۲۰۱۸ و نهایتاً ۲۰۲۳ آن را به‌روزرسانی کرده است. هرچند، بخشه‌ای قابل‌توجهی از آخرین راهبرد سایبری آمریکا، تغییر نکرده و تعجب خواننده را به خود جلب نمی‌کند اما در سند راهبردی که وزارت دفاع در سال ۲۰۱۸ منتشر کرده است یک مفهوم عملیاتی جدید وارد ادبیات فضای سایبری شده و این مفهوم عبارت است از «دفاع روبه‌جلو». در سند ۲۰۲۳ نیز مجدداً بر این مفهوم تأکید شده است. این مفهوم و یا به عبارتی اصطلاح، چهار بار در طول سند مورد اشاره به‌کاررفته و در تبیین آن گفته‌شده که دفاع روبه‌جلو به معنی مقابله با تهدیدات قبل از رسیدن به شبکه‌های ایالات متحده است. همین راهبرد در سند ۲۰۲۳ نیز دنبال شده است. درواقع آمریکا بر این باور است که پیش‌ازاین که تهدید و

نه حمله، به زیرساخت موردنظر در خاک آمریکا برسد، می‌بایست شناسایی شود و از عملیاتی شدن آن جلوگیری به عمل آید. این مفهوم در برابر کشورهایی که علیه آمریکا عملیات سایبری خصمانه انجام داده بودند اما اقدام آن‌ها در سطحی پایین‌تر از یک حمله مسلحانه و نظامی بوده است مطرح شد. همان‌گونه که مشخص است در این سند نیز بر مفهوم تهدید تکیه شده و مبنای انجام اقدام دفاعی، شناسایی تهدید عنوان‌شده است.

مفهوم دفاع روبه‌جلو از راهبرد «درگیری مداوم» آمریکا پشتیبانی می‌کند. در تبیین این مفهوم توضیح داده‌شده است که برتری از طریق استمرار، ابتکار عمل را در فضای سایبری با رقابت مداوم با دشمنان حفظ می‌کند و باعث عدم اطمینان آن‌ها در هرکجا که مانور می‌دهند، می‌شود. این چشم‌انداز درواقع توصیف می‌کند که «فرماندهی سایبری» چگونه (عملیات آفندی و پدافندی توأمان در یک فضای جنگی پیوسته)، کجا (در سطح جهان و تا حد ممکن در نزدیکی دشمنان)، چه زمان (به‌طور مداوم) و چرا (ایجاد برتری عملیاتی برای خود ضمن ممانعت از کسب برتری عملیاتی دشمن) در فضای سایبری اقدام به عملیات می‌کند. به بیانی دیگر درگیری مداوم، به معنی حضور فرماندهی سایبری در همه‌جا، همه زمان و استفاده از همه ابزارها است [۸۹]. با این توصیف، درگیری مداوم چند ویژگی دارد:

۱. استراتژی دفاع سایبری آمریکا را از «آماده بودن» یا پاسخ نسبت به یک بحران به یک عملیات مداوم و نامحدود تبدیل می‌کند.
۲. به‌منزله افزایش نقش و سهم فرماندهی سایبری در دفاع از زیرساخت‌های حیاتی (و بیرون از شبکه‌های وزارت دفاع) علاوه بر شبکه‌ها و سامانه‌های اطلاعاتی وزارت دفاع است.
۳. به‌مثابه چتر استراتژیکی است که ذیل آن دفاع روبه‌جلو تعریف می‌گردد.
۴. اشاره و اطمینان دارد که عملیات سایبری زیر حد اقدام مسلحانه رخ می‌دهد (همان).

دفاع روبه‌جلو به‌ضرورت نبرد ماندگار برای جلوگیری از عملیات سایبری خصمانه متناوب علیه آمریکا اشاره دارد. به نظر می‌رسد که برای آمریکا، مسئله به این صورت است که برخی

برای غلبه بر دیگر ویژگی‌های فضای سایبری و پیشگیری از غافلگیری به رسمیت شناخته می‌شود.

نکته دیگری که از سایر اسناد تشریح کننده این راهبرد به دست می‌آید این است که این مفهوم یک مفهوم دکترینی است و برای فهم بهتر آن لازم است از زبان مشابهی که وزارت دفاع آمریکا در رابطه با چنین مفاهیمی استفاده می‌کند بهره برد. بر این اساس، شاید نزدیک‌ترین عبارت به دفاع روبه‌جلو، «دفاع فعال» باشد که برای سایر حوزه‌های رزم بکار می‌رود و به معنی به‌کارگیری ضد حملات و اقدامات آفندی محدود جهت انکار یک منطقه یا موقعیت مورد مناقشه با دشمن است. لذا دفاع روبه‌جلو را می‌توان یک «دفاع فعال پیشرفته» تعبیر کرد یعنی دفاع فعالی با عرض جغرافیایی بیشتر و محدودیت کمتر در ویژگی‌های آفندی و تهاجمی [۹۰].

نکات دیگری نیز پیرامون این راهبرد وجود دارد از جمله مدت‌زمان حمله، قابلیت بازدارندگی، اثربخشی، دقت در هدف‌گیری دشمن، زمان ورود به درگیری و لکن برای عملیاتی سازی دفاع روبه‌جلو، سه اقدام اساسی، ضروری دانسته شده است که عبارت‌اند از تضعیف توان رزم دشمن، تلفیق توانایی‌های سایبری با دیگر ابزارهای نظامی و غیرنظامی و کسب اشراف اطلاعاتی و حفظ دسترسی اطلاعاتی علیه اهداف مشخص [۹۱].

۸.۷.۲ دفاع پیش‌کنش‌گرانه سایبری

توانایی و آمادگی جنگ آن‌قدر حائز اهمیت است که قرآن کریم می‌فرماید: «وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ» هر نیرویی در توان دارید، برای مقابله با آن‌ها [= دشمنان] آماده‌سازید و (همچنین) اسب‌های ورزیده (برای میدان نبرد) تا به‌وسیله آن، دشمن خدا و دشمن خویش را بترسانید (قرآن کریم). اشاره قرآن کریم به آنچه در توان دارید را می‌توان ناظر به ابعاد مختلف قدرت و جنبه‌های مختلف دفاع تفسیر کرد و بر این اساس، می‌توان گفت حفظ و ارتقاء آمادگی‌های رزمی و دفاعی در فضای سایبری نیز، مشمول این آیه خواهد بود. امیرالمؤمنین علی (علیه‌السلام) نیز در همین راستا در فرازی از خطبه ۳۷ نهج‌البلاغه می‌فرمایند: «وَقُلْتُ لَكُمْ أَغْزَوْهُمْ قَبْلَ أَنْ يَغْزَوْكُمْ فَوَاللَّهِ مَا غَزَى قَوْمٌ قَطُّ فِي عَقْرِ دَارِهِمْ إِلَّا

کشورها همواره در پی دشمنی با آمریکا هستند و از هر فرصتی برای ضربه زدن به منافع آمریکا استفاده می‌کنند (همان‌طور که در بخشی از سند به این کشورها اشاره هم می‌شود) و تهدید دائمی محسوب می‌شوند؛ بنابراین، آمریکا نیز می‌بایست برای انجام اقدام مناسب و در لحظه آمادگی لازم را داشته باشد. هرچند عبارت کلی دفاع روبه‌جلو و شرح مختصر آن در توضیحات پنتاگون خیلی کوتاه است اما از سه مفهوم بسیار کلان و عمیق تشکیل شده است:

۱. موقعیت‌یابی برای تخریب و تخفیف عملیات سایبری
 ۲. هشدار دهی به معنای جمع‌آوری اطلاعات در مورد تهدیدها و اطلاع به بخش‌های دفاعی
 ۳. نفوذ در ساختارها و زیرساخت‌های اطلاعاتی، حساس و حیاتی دشمنان به‌منظور دلسرد کردن آن‌ها از طرح‌ریزی و اجرای عملیات سایبری علیه آمریکا (اقتدار سایبری).
- برای پاسخ به نیازهای فوق و درواقع، فراهم کردن الزامات پاسخ مناسب به تهدیدات با توجه به ویژگی‌های فضای سایبری، الزامات مختلفی برای داشتن دفاع روبه‌جلو عنوان می‌شود:
- اول اینکه آمریکا برای داشتن دفاع روبه‌جلو، نیازمند هدایت عملیات فضای سایبری به سمت توسعه و ارتقاء توانمندی‌های نظامی سایبری و جاسوسی و جمع‌آوری اطلاعات سایبری (از جنس Intelligence) است تا بتواند از آن‌ها برای زمان بحران و یا درگیری استفاده کند.

دومین نکته تمرکزی است که در سند موردبحث به آن اشاره می‌کند. درواقع با توجه به دشمنی دیرینه‌ای که روسیه و چین در فضای سایبری با آمریکا داشته‌اند، تأکید شده است که باید بر این دولت‌ها تمرکز داشت.

نکته سومی که در مقایسه با سند راهبردی سایبری سال ۲۰۱۳ می‌توان برداشت کرد این است که وزارت دفاع، دامنه عملیات سایبری را که قبلاً به شبکه‌ها و سامانه‌های وزارت دفاع آمریکا محدود می‌شد، هم به شبکه‌های خارج از وزارت دفاع و هم به خارج از آمریکا نیز توسعه داده است [۹۰] و به عبارتی، اگرچه مرز جغرافیایی آن‌گونه که در فضای حقیقی رسمیت دارد شاید در فضای سایبری، به رسمیت شناخته نشود اما در اینجا و

دُلُوا؛ و گفتم پیش از آن که آن‌ها با شما بجنگند با آنان نبرد کنید، به خدا سوگند، هر ملتی که درون خانه خود مورد هجوم قرار گیرد، ذلیل خواهد شد (نهج البلاغه). مقام معظم رهبری طی سخنرانی خود در دانشگاه افسری امام علی «علیه السلام» مورخ ۱۳۹۰/۸/۱۹، بیان داشتند که: «ما اهل تجاوز به هیچ ملتی و هیچ کشوری نیستیم، ما هرگز اقدام به جنگ خونین نمی‌کنیم، ملت ایران این را به اثبات رسانده است، اما ما ملتی هستیم که هرگونه تجاوز را، بلکه هرگونه تهدید را، با استواری و با قدرت کامل پاسخ خواهیم داد. ما ملتی نیستیم که بنشینیم تماشا کنیم قدرت‌های پوشالی مادی که از درون کرم‌خورده و موریانه خورده‌اند، ملت استوار و پولادین ایران را تهدید کنند. ما در مقابل تهدید، تهدید می‌کنیم.» [۹۲]. از سوی دیگر دکتترین سایبری جمهوری اسلامی که در [۲۲] تدوین شده است، مبتنی بر سه اصل استقلال سایبری، اقتدار سایبری و تواضعی، موارد زیر را الزام می‌کند:

- استقرار حاکمیت اسلامی ایرانی با نقش‌آفرینی مقتدر و مؤثر
 - گسترش مرزهای جغرافیایی به مرزهای سایبری
 - دفاع و امنیت همه‌جانبه پایدار مردمی با محوریت محتوا
 - تاب‌آوری، بازدارندگی و تهاجم ترکیبی سایبری در جغرافیای مؤثر بر امنیت ملی
 - رزم سایبری مقتدرانه و پشیمان کننده
 - سایبر در رزم (زیرساخت سایبری) با فناوری‌های نوین بومی
 - صیانت از سازوکار مادی و معنوی سایبری
- بر این اساس، اکتفا به دفاع سایبری در قلمرو سایبری جمهوری اسلامی و مبتنی بر انواع پیش‌گفته، طبق فرمایش امیرالمؤمنین (ع)، نمی‌تواند عزتمندی را برای کشور به همراه داشته باشد و احکام عملی دکتترین سایبری جمهوری اسلامی ایران را تأمین نماید. لذا نوع دیگری از دفاع سایبری که بتواند پاسخگوی تهدید (یعنی تهدید در برابر تهدید) باشد و پیش از رسیدن تهدید به مرزهای سایبری کشور، بازیگر تهدید را منصرف نماید مورد نیاز است.

در منابع فارسی از عبارت پیش‌کنش‌گرانه در دفاع سایبری استفاده نشده است و برخی تلاش کرده‌اند محتوای یادشده در دفاع فرافعال را به عنوان دفاع پیش‌کنش‌گرانه مطرح کنند. لکن

این دو عبارت قدری با یکدیگر تفاوت دارند. دو مقوله مدیریت هشدار و سامانه پاسخ، اساسی‌ترین ارکان سامانه‌های دفاع و حفاظت از امنیت در فضای سایبری هستند که عمدتاً این دو مقوله از یکدیگر جدا در نظر گرفته می‌شوند [۶۲]. یکی از مهم‌ترین ویژگی‌های دفاع پیش‌کنش‌گرانه این است که مدیریت هشدار، رصد، شناسایی و پیش‌بینی تهدیدات سایبری کاملاً در تعامل با پاسخ تعریف می‌شود. از سوی دیگر و با توجه به ویژگی‌های پیش‌گفته فضای سایبری مؤثر بر حمله و دفاع در این فضا، از آنجاکه در حملات سایبری زمان تشخیص به‌شدت مهم است، هدف در دفاع پیش‌کنش‌گرانه، پیش‌بینی تهدیدات از طریق رصد، پایش و تحلیل مداوم اطلاعات تهدید و نه حمله است. درواقع به‌جای انتظار برای رسیدن حمله به سرمایه سایبری خودی و آشکارشدن نشانه‌های حمله، خواستار درک زودهنگام و فهم هشدارهای اولیه (یا نشانک‌های) شکل‌گیری اقدامات (و تهدیدات) در مبدأ و در سمت سرمایه سایبری دشمن هستیم. در گام بعدی، سناریوهای مقابله و اقدامات پاسخ و زمینه‌های آن باید از قبل فراهم باشد چراکه نیازمندی‌های پاسخ می‌بایست از قبل آماده‌شده باشد؛ بنابراین دفاع پیش‌کنش‌گرانه عبارت است از «رصد، شناسایی، پیش‌بینی و تحلیل تهدیدات محتمل سایبری و اشراف اطلاعاتی، برنامه‌ریزی، طرح‌ریزی و اقدام باهدف اختلال، تغییر، انحراف، تخریب یا نابودی تهدید - در دو بعد ذهنی و عینی - (قبل از به فعلیت رسیدن تهدید) که شامل شناسایی موجودیت‌ها و بازیگران مؤثر مرتبط با صحنه نبرد سایبری می‌شود. طرح‌ریزی و اقدام در دفاع پیش‌کنش‌گرانه از جنس تهدیدات پیشرفته ماندگار است. به عبارتی مطابق با زنجیره کشتار سایبری، گام‌های اولیه حمله انجام می‌شود و در زمان مقتضی، اقدام نهایی برای اختلال، تغییر، انحراف و یا تخریب موردنظر صورت می‌پذیرد.

۳. روش تحقیق

از آنجاکه این مقاله به دنبال سامان دادن به یکی از مباحث مهم در نیروهای مسلح و همچنین در فضای سایبری جمهوری اسلامی است، نوع تحقیق ازلحاظ هدف، کاربردی محسوب می‌شود. همچنین تحقیق حاضر به‌صورت توصیفی و موردی-زمینه‌ای انجام شده است. از آنجاکه این تحقیق برای گردآوری

اطلاعاتی که مدون نشده به کار می‌رود، توصیفی است و با این روش، توصیف واقعی و منظم موضوعات صورت می‌گیرد و از آنجا که مطالعه عمیق روی نمونه‌هایی از یک پدیده (دفاع سایبری) در محیط واقعی صورت می‌گیرد، موردی-زمینه‌ای محسوب می‌شود.

در این تحقیق، با استفاده از روش کتابخانه‌ای و با جمع‌آوری و مطالعه منابع گوناگون شامل کتاب‌ها، مقالات، گزارش‌ها، اسناد راهبردی سایر کشورها و اسناد بالادستی کشور، ادبیات نظری جمع‌آوری شده و با به‌کارگیری مصاحبه عمیق از خبرگان دفاع سایبری، اطلاعات و داده‌های موردنیاز جمع‌آوری گردیده است. تعداد خبرگان مشارکت‌کننده به‌صورت تمام شمار تا رسیدن به اشباع نظری ادامه یافت. ویژگی موردنظر برای جامعه مشارکت‌کننده علاوه بر داشتن مدرک کارشناسی ارشد یا دکترا در رشته‌های مرتبط با تحقیق، داشتن حداقل ۱۰ سال سابقه مدیریتی در سطوح راهبردی یا عملیاتی دفاع سایبری نیز هست. نتایج مستخرج از پژوهش در دو مرحله توسط هیئت اندیشه‌ورز از نخبگان و خبرگان حوزه سایبری به تأیید رسیده است.

همان‌گونه که در این شکل مشخص است سه محور برای افراز در نظر گرفته می‌شود که عبارت‌اند از زمان، نوع اقدام و فضای مقابله. محور زمان به سه بخش پیش از حمله، حین حمله و پس از حمله تقسیم می‌شود. نوع اقدام، مشتمل بر عامل و غیرعامل است و فضای مقابله دربرگیرنده فضای دور و فضای نزدیک خواهد بود. یادآور می‌شود با توجه به اینکه ورود به فضای میانی و اقدام عامل در این فضا، دارای آثار و تبعات حقوقی است و از این حیث با فضای دور، مشابهت دارد، با فضای دور یکی، در نظر گرفته می‌شود.

فضای سایبری، با عنایت به رشد و توسعه خیره‌کننده آن و پیشرفت فناوری‌های مورد استفاده در آن، از یک فضای ناشناخته و پیچیده، به سمت یک فضای آشوبناک حرکت کرده است که پیچیدگی و عدم قطعیت در آن به شدت بالاست. اقتضای عمل در محیط‌های آشوبناک، برخلاف سایر محیط‌ها که ابتدا درک از محیط صورت می‌گیرد و سپس تصمیم به اقدام اتفاق می‌افتد، این است که اقدام مقدم باشد و در ادامه وضعیت محیط، مورد بررسی قرار گیرد. مسئله دفاع سایبری نیز با توجه به سیر تطوری که برای آن عنوان گردید از این قاعده مستثنا نبوده و به سمت پیش‌دستی و پیش‌کش‌گری در این فضا حرکت کرده است و به عبارتی برای دفاع موفق در این فضا، مدافع همواره باید یک گام از مهاجم جلوتر عمل کند. هرچند این کار در عمل بسیار سخت به نظر می‌رسد. از سوی دیگر با توجه به اینکه فضای سایبری، یک محیط ساخته دست بشر است لذا وجود آسیب‌پذیری در لایه‌های مختلف آن، گریزناپذیر است و فضای سایبری را مستعد تهدیدات و مخاطرات می‌نماید و اگرچه برای

با توجه به فاصله‌گذاری که با دفاع فعال دارد در خارج از قلمرو مدافع و در فضای دور خواهد بود.

دفاع روبه‌جلو تنها در راهبرد دفاع سایبری آمریکا مورد اشاره و استفاده قرار گرفته است و مشتمل بر اقدامات عامل علیه منشأ تهدید (فضای دور) پیش از وقوع حمله است.

دفاع پیش‌کنش‌گرانه سایبری نیز وضعیتی مشابه دفاع روبه‌جلو خواهد داشت؛ یعنی به لحاظ سایبری (چراکه طبق تعریف آن می‌تواند اقدامات غیرسایبری را نیز در بر گیرد)، اقدامات عامل در محدوده زمانی پیش از حمله (و در زمان تهدید) و در قلمرو دور را شامل می‌شود.

۵. نتیجه‌گیری

بر اساس یافته‌های تحقیق، انواع دفاع در فضای سایبری عبارت‌اند از دفاع در عمق، دفاع غیرفعال، دفاع تاب‌آور، دفاع مستحکم، دفاع فعال، دفاع فرافعال و دفاع پیش‌کنش‌گرانه که برای تفکیک آن‌ها از سه شاخص زمان، فضای اقدام و نوع اقدام بهره‌گیری شد. جمع‌بندی موارد یاد شده در جدول ۱ آورده شده است.

در ادامه و برای کارهای آتی پیشنهاد می‌شود الگوی راهبردی دفاع پیش‌کنش‌گرانه تدوین شود. همچنین بر اساس تفکیک صورت گرفته، طرح راهبردی دفاع سایبری با هدف‌گذاری نگاهت نهادی برای انواع دفاع در نیروهای مسلح و سازمان‌های امنیتی و اطلاعاتی صورت گیرد.

مجموعه اقدامات در نظر گرفته‌شده برای آن‌ها در بخش مربوطه صورت می‌پذیرد.

اکنون به تشریح این موضوع خواهیم پرداخت که هر یک از انواع دفاع مطرح‌شده در بخش دوم مقاله در کدام محدوده از شکل ۱۱ قرار خواهند گرفت.

دفاع در عمق، به معنای وجود لایه‌های مختلف دفاعی است و از این حیث، کل فضای افراز دفاع سایبری را در بر خواهد گرفت.

اقدامات دفاع غیرفعال با توجه به تعریف صورت گرفته، در محدوده غیرعامل شکل ۱۱ واقع خواهد شد و تنها در میدان نزدیک کاربرد دارد و از نظر زمانی، مشمول محدودیت نمی‌شود.

دفاع تاب‌آور نیز در محدوده غیرعامل، در میدان نزدیک قرار می‌گیرد و همان‌گونه که در تعریف آن ذکر شده، از نظر زمانی مربوط به شرایط پس از حمله و حین حمله (در صورت کشف آن پیش از پایان حمله) است.

دفاع مستحکم با توجه به مصادیق و تعریفی که برای آن ارائه گردید، هم شامل اقدامات عامل و هم غیرعامل است ولی از نظر زمانی، معطوف به حین حمله و پیش از حمله خواهد بود و تنها در محیط نزدیک قابل اجرا و پیاده‌سازی است.

دفاع فعال مشتمل بر اقدامات عاملی است که در حین و پس از حمله برای یافتن و تعقیب مهاجم در فضای نزدیک صورت می‌گیرد.

دفاع فرافعال، نیز از حیث نوع اقدام در محدوده عامل قرار دارد و از نظر زمانی مربوط به حین حمله است و حیطه اقدام آن

جدول ۱. مقایسه انواع دفاع سایبری.

دفاع در عمق								
دفاع غیرفعال	دفاع تاب‌آور	دفاع مستحکم	دفاع فعال	دفاع فرافعال	دفاع روبه‌جلو	دفاع پیش‌کنش‌گرانه	اقدام (ت)	قبل از حمله
✓	✓	✓	✓	✓	✓	✓		
✓	✓	✓	✓	✓	✓	✓		حین حمله
✓	✓	✓	✓	✓	✓	✓	✓	بعد از حمله
✓	✓	✓	✓	✓	✓	✓	✓	عامل
✓	✓	✓	✓	✓	✓	✓	✓	غیرعامل
✓	✓	✓	✓	✓	✓	✓	✓	فضای دور
✓	✓	✓	✓	✓	✓	✓	✓	فضای نزدیک

۶. منابع

- [۲۱] A. Venables, "Modelling Cyberspace to Determine Cybersecurity Training Requirements," *Frontiers in Education*, vol. ۶, p. ۷۶۸۰۳۷, ۱۱/۱۶ ۲۰۲۱, doi: ۱۰.۳۳۸۹/educ.۲۰۲۱.۷۶۸۰۳۷.
- [۲۲] M. Moradi, "Developing the Cyber Doctrine of the Islamic Republic of Iran in the Defense-Security Field," PhD, National Defense University, Iran - Tehran, ۲۰۲۲ (in persian).
- [۲۳] H. Yazdani and G. Jalali-Farahani, "Key Human Resources Variables in Strengthening the Cyber Defense of the Islamic Republic of Iran," *National Security*, vol. ۷, no. ۲۶, p. ۱۶, ۲۰۱۷ (in persian).
- [۲۴] B. Donohue, "Experts Tell Senate: Government Networks Owned, Resistance Is Futile," *ThreatPost*, U.S.A., ۲۰۱۲.
- [۲۵] P. W. Brodbeck, "Complexity theory and organization procedure design," *Business Process Management* vol. ۸, no. ۴, p. ۲۶, ۲۰۰۲, doi: <https://doi.org/10.1108/14637100210435026>.
- [۲۶] Wikipedia, "Cynefin framework", at https://en.wikipedia.org/wiki/Cynefin_framework.
- [۲۷] D. Kruger, "Radically Simplifying Cybersecurity," in *Applied Cyber-Physical Systems*, S. C. Suh, U. J. Tanik, J. N. Carbone, and A. Eroglu Eds.: Springer New York, NY, ۲۰۱۲, ch. ۵.
- [۲۸] R. S. Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence," in ۱th International Conference on Cyber Conflict, Tallinn, Estonia, M. M. P. Brangetto, J. Stinissen, Ed., ۲۰۱۴.
- [۲۹] A. V. Uzunov, S. Nepal, and M. B. Chhetri, "Proactive Antifragility: A New Paradigm for Next-Generation Cyber Defence at the Edge," in ۲۰۱۹ IEEE ۵th International Conference on Collaboration and Internet Computing (CIC), ۱۲-۱۴ Dec. ۲۰۱۹, pp. ۲۴۶-۲۵۵, doi: ۱۰.۱۱۰۹/CIC48460.۲۰۱۹.۰۰۳۹.
- [۳۰] V. Tzavara and S. Vassiliadis, "Tracing the evolution of cyber resilience: a historical and conceptual review," *International Journal of Information Security*, vol. ۲۲, no. ۲, pp. ۱۶۵-۱۷۱, ۲۰۲۴/۰۶/۰۱ ۲۰۲۴, doi: ۱۰.۱۰۰۷/s1۰۲۰۷-۰۲۳-۰۰۸۱۱-x.
- [۳۱] S. Ahmadi, "Next Generation AI-Based Firewalls: A Comparative Study," *International Journal of Computer (IJC)*, vol. ۴۹, pp. ۲۴۵-۲۶۲, ۱۲/۳۱ ۲۰۲۳.
- [۳۲] H. Amid, "Amid Culture," Tehran: Amirkabir Publications, ۲۰۰۳ (in persian).
- [۳۳] A. Panahi, "Investigating the Impact of Electronic Threats from Own Forces on the Decision-Making Process of Jungle Operations in Unequal Battles," *Quarterly Journal of Military Sciences and Technologies*, vol. ۱۵, no. ۵۰, p. ۲۷, ۲۰۱۹ (in persian).
- [۳۴] S. Rahpik, "Explanation of indicators, manifestations and dimensions of threats in the components of national power," National Defense University, Tehran, ۲۰۰۸ (in persian).
- [۳۵] A. Mehraban, "The Relationship Between Threats and Damages in the Field of National Security with a View to Sanctions (Case Study of the Sanctions Resolution against the Islamic Republic of Iran)," *Strategic Defense Studies Quarterly*, vol. ۱۷, no. ۷۶, p. ۲۴, ۲۰۱۹ (in persian).
- [۳۶] H. Ameri, *Principles of International Relations*. Tehran: Agah Publications, ۱۹۹۱ (in persian).
- [۳۷] A. Eftekhari, *Security*. Tehran: Imam Sadeq University, ۲۰۱۲ (in persian).
- [۳۸] A. Bahmani, H. Khodadi, and M. Fathi Zadeh, "Reviewing and Assessing America's Aggressive Intentions and Security Threats after the Islamic Revolution of Iran," *Quarterly Journal*
- [۱] M. Ahadi and M. Shahmohammadi, "The Strategic Plan of Cyber Defense of the Islamic Republic of Iran in the Field of Deterrence," *Quarterly Scientific Research Journal of Interdisciplinary Studies in Strategic Knowledge*, vol. ۸, pp. ۲۲۵-۲۵۲, ۲۰۱۸ (in persian).
- [۲] C. Whyte and B. Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy*, ۲nd ed. London: Routledge, ۲۰۲۳, p. ۳۶۴.
- [۳] D. Barrett, "U.S. Outgunned in Hacker War", ed: Wall Street Journal, ۲۰۱۲.
- [۴] N. Dyer and S. Matviyenko, *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. Minnesota University, ۲۰۱۹.
- [۵] J. P. Farwell and R. Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy*, vol. ۵۴, no. ۴, p. ۱۴, ۲۰۱۲.
- [۶] K. E. Heckman, M. J. Walsh, F. J. Stech, T. A. O'Boyle, S. R. DiCato, and A. F. Herber, "Active cyber defense with denial and deception: A cyber-wargame experiment," *Computers & Security*, vol. ۳۷, pp. ۷۲-۷۷, ۲۰۱۳/۰۹/۰۱/ ۲۰۱۳, doi: <https://doi.org/10.1016/j.cose.۲۰۱۳.۰۳.۰۱۵>.
- [۷] R. C. Parks and D. P. Duggan, "Principles of Cyberwarfare," *IEEE Security & Privacy*, vol. ۹, pp. ۳۰-۳۵, ۲۰۱۱.
- [۸] P. Hosseini and H. Zarifmanesh, "Comparative Study of the Cyber Defense Structure of Countries," (in persian), *Defense and Security Research*, vol. ۵, no. ۲, pp. ۱۹-۴۶, ۲۰۱۳. [Online]. Available: <https://www.noormags.ir/view/fa/articlepage/۱۰۷۴۸۲۵>.
- [۹] DEPARTMENT OF DEFENSE CYBER STRATEGY, ۲۰۱۸
- [۱۰] DEPARTMENT OF DEFENSE CYBER STRATEGY, ۲۰۱۳
- [۱۱] DEPARTMENT OF DEFENSE CYBER STRATEGY, ۲۰۲۳
- [۱۲] M. Healy, "Cannae ۲۱۶ BC: Hannibal smashes Rome's Army (Campaign)". Osprey Publishing, ۱۹۹۴.
- [۱۳] R. Asghari, H. Bagheri, and M. Mirzazadeh, "Providing a Framework for Active Cyber Defense Against Advanced Cyber Attacks," *Scientific-Research Journal of Electronic and Cyber Defense*, vol. Special Issue of the Conference on Combinatorics, Cryptography and Computing, p. ۱۵, ۲۰۱۹ (in persian).
- [۱۴] R. Taghipour, M. Ramak, H. Amirli, V. Ghorbani, M. Haghi, M. Kazemi, M. Ramazaniyarandi, A. Esmaili, S. Yazdani, A. Malaee, "Designing the country's cyber defense system and formulating its strategies," Group study, ۲۰۱۶ (in persian).
- [۱۵] F. D. Kramer, S. H. Starr, and L. K. Wentz, *Cyberpower and National Security*. Washington, D.C., United States: POTOMAC BOOKS: National Defense University Press, ۲۰۰۹, p. ۶۶۴.
- [۱۶] Cyber defense Strategic document, ۲۰۱۵ (in persian)
- [۱۷] A. Ghasemzadeh and M. Dehghani, "Presenting a ۲D Cyberspace Model Based on a ۲D Physical, Informational, and Cognitive Command and Control Model," presented at the ۸th National Iranian Command and Control Conference (C4I), Tehran, ۲۰۱۴ (in persian).
- [۱۸] S. Tabatabaei Manesh, "Comparative Review of Models and Theories Regarding Cyberspace Partitioning," presented at the Fourth National Conference on Cyber Defense, Maragheh, ۲۰۲۳ (in persian).
- [۱۹] Joint Publication JP ۳-۱۲ *Cyberspace Operations*. (۲۰۱۸)
- [۲۰] CYBERSPACE OPERATIONS ۳-۱۲ (۲۰۲۳)

- [۵۷] D. E. Denning, "Framework and principles for active cyber defense," *Computers & Security*, vol. ۴۰, pp. ۱۰۸-۱۱۳, ۲۰۱۴, doi: ۱۰.۱۰۱۶/J.COSE.۲۰۱۳.۱۱.۰۰۴.
- [۵۸] T. P. Wong, "Active cyber defense: enhancing national cyber defense," *Naval Postgraduate School Monterey, CA*, ۲۰۱۱.
- [۵۹] H. Rahimov and M. Movahedisefat, "Presenting a Conceptual Model for National Cyber Defense", *Quarterly Journal of Strategic Cyberspace Studies*, vol. ۲, no. ۳, pp. ۶۹-۸۸, ۲۰۲۲. [Online]. Available: https://ssc.sndu.ac.ir/article_۲۵۵۳.html. (in persian)
- [۶۰] Gartner. "https://twitter.com/Gartner_inc/status/۷۳۹۸۴۵۳۱۶۸۰۸۱۷۹۷۱۳".
- [۶۱] K. Hartmann and K. Giles, "Net Neutrality in the Context of Cyber Warfare," in *۱۰th International Conference on Cyber Conflict CyCon X: Maximising Effects*, Tallinn, Estonia, R. J. T. Minárik, L. Lindström, Ed., ۲۰۱۸: CCD COE.
- [۶۲] M. Ghasemigol, "A Future-oriented Framework for Intrusion Response Systems in Computer Networks," *Electronic and Cyber Security Research Journal*, vol. ۳, pp. ۱۳-۲۴, ۲۰۱۸. (in persian)
- [۶۳] E. Rodriguez, "Cyber Defense vs. Cyber Security: Understanding the Varied Approaches to Digital Protection," ed: LinkedIn, ۲۰۲۴.
- [۶۴] A. Chesbrough. "What is the Difference Between Offensive and Defensive Security." *BreachLock*. <https://www.breachlock.com/resources/blog/what-is-the-difference-between-offensive-and-defensive-security/> (accessed ۲۰۲۴).
- [۶۵] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," ۲۰۱۰.
- [۶۶] Joint Publication ۳-۶۰ Joint Targeting. ۲۰۰۷, [Online] Available: http://www.dtic.mil/doctrine/new_pubs/jp۳_۶۰.pdf.
- [۶۷] B. Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Copernicus, ۲۰۰۳, p. ۳۰۴.
- [۶۸] B. Schneier, *Schneier on Security*, ۱ ed. John Wiley & Sons, ۲۰۰۸, p. ۳۳۶.
- [۶۹] S. Fitz-Gerald, "Schneier on Security, B. Schneier. J. Wiley (۲۰۰۸), ۳۲۸ pp., ISBN: ۹۷۸۰۴۷۰۳۹۵۳۵۶," *International Journal of Information Management*, vol. ۳۰, pp. ۳۷۴-۳۷۵, ۰۸/۰۱ ۲۰۱۰, doi: ۱۰.۱۰۱۶/j.jinfomgt.۲۰۱۰.۰۵.۰۰۴.
- [۷۰] NIST SP ۸۰۰-۵۳ Rev. ۵, NIST, ۲۰۲۰. [Online]. Available: <https://csrc.nist.gov/pubs/sp/۸۰۰/۵۳/r۵/upd۱/final>
- [۷۱] R. J. D. a. R. Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," presented at the *International Political Sociology*, ۲۰۱۰.
- [۷۲] W. Lu, S. Xu, and X. Yi, "Optimizing Active Cyber Defense," in *International Conference on Decision and Game Theory for Security: GameSec ۲۰۱۳*, Cham, ۲۰۱۳: Springer International Publishing, in *Decision and Game Theory for Security*, pp. ۲۰۶, ۲۲۵.
- [۷۳] R. Ramezani Dehghi and A. M. Aminzadeh, "Cyber resilience model of defense systems and products," *Military Science and Technology*, vol. ۱۹, no. ۶۴, pp. ۹۱-۱۱۰, ۱۴۰۲, doi: ۱۰.۲۲۰۳۴/qjmst.۲۰۲۳.۵۵۱۷۵۵.۱۶۹۲. (in persian)
- [۷۴] D. Galinec and W. Steingartner, "Combining cybersecurity and cyber defense to achieve cyber resilience," in *۲۰۱۷ IEEE ۱۴th International Scientific Conference on Informatics*, ۲۰۱۷: IEEE, pp. ۸۷-۹۳.
- [۷۵] B. Bet Sheken, "A Review of Resilience Engineering in Cyberspace," presented at the *Third National Conference on* of Islamic Revolution Studies, vol. ۹, no. ۳۰, p. ۲۰, ۲۰۱۲. (in persian)
- [۳۹] yjc, "List of America's Failed Wars in the World," in *Young Journalists Club*, ed, ۲۰۱۸. (in persian)
- [۴۰] A. Shirazi, "A Long List of America's Crimes Against the People of the World," in *Mashreq News*, ed, ۲۰۲۲. (in persian)
- [۴۱] M. Sahraei, M. Velvi, B. Bayat, and A. Tarqi, "Presenting a Native Model for Cyber Surveillance, Monitoring, and Warning Based on the Oda Cycle," *National Security Journal*, vol. ۱۰, no. ۳۷, p. ۲۸, ۲۰۱۹. (in persian)
- [۴۲] M. Ramak, "Presenting a strategic model for international cooperation to enhance cyberspace security based on the national interests of the Republic of Iran with the approach of combating cybercrime," Ph.D., Faculty of National Defense, National Defense University, Tehran, ۲۰۱۹.
- [۴۳] V. Lenders, A. Tanner, and A. Blarer, "Gaining an Edge in Cyberspace with Advanced Situational Awareness," *IEEE Security & Privacy*, vol. ۱۳, no. ۲, pp. ۶۵-۷۴, ۲۰۱۵, doi: ۱۰.۱۱۰۹/MSP.۲۰۱۵.۳۰.
- [۴۴] A. Klimburg and H. Tiirmaa-Klaar, "Cybersecurity and Cyberpower: Concepts ,Conditions and Capabilities for Cooperation for Action within the EU," *European Parliament, Belgium*, ۲۰۱۱. [Online]. Available: <http://www.europarl.europa.eu/committees/en/sede/studies/download.html?languageDocument=EN&file=۴۱۶۴۸>
- [۴۵] A. Sh. Jabarrashidi, Mohammad "Modeling and Simulation of Cyber Battlefield," (in fa), *Information Technology Management*, vol. ۹, no. ۴, p. ۲۰, ۲۰۱۷, doi: ۱۰.۲۲۰۵۹/jitm.۲۰۱۷.۲۳۴۷۰۹.۲۰۶۰. (in persian)
- [۴۶] Z. E. Mrabet, N. Kaabouch, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges " *Computers & Electrical Engineering*, vol. ۶۷, p. ۱۴, ۲۰۱۸.
- [۴۷] Information technology — Security techniques — Information security management systems ISO, ۲۰۱۸. [Online]. Available: <https://www.iso.org/standard/۷۳۹۰۶.html>
- [۴۸] S. Velasquez. "https://www.linkedin.com/pulse/differences-between-security-event-incident-non-compliance-". LinkedIn. (accessed).
- [۴۹] NATIONAL CYBER INCIDENT RESPONSE PLAN. [Online] Available: https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
- [۵۰] OSCE, "CYBER INCIDENT CLASSIFICATION. A Report on Emerging Practices within the OSCE region," Vienna, ۲۰۲۲.
- [۵۱] FIPS ۲۰۰, NIST, United States, ۲۰۰۶.
- [۵۲] H. Amirli and R. Taghipour, "Presenting a Process Model for Native Cyber Defense," *National Security Quarterly*, vol. ۱۰, no. ۳۷, p. ۳۴, ۲۰۱۹. (in persian)
- [۵۳] Critical Terminology Foundations ۲ ;Russia-U.S. Bilateral on Cybersecurity .
- [۵۴] Information Technology Organization , Cyber Defense System, ۲۰۱۱ (in persian)
- [۵۵] R. Taghipour and A. Esmaeili, "Designing a Conceptual Model of the Cyber Defense Pattern of the Islamic Republic of Iran," *Journal of National Security*, vol. ۸, pp. ۱۸۱-۲۰۲, ۲۰۱۸. (in persian)
- [۵۶] D. Galinec, D. Možnik, and B. Guberina, "Cybersecurity and cyber defence: national level strategic approach," *Automatika*, vol. ۵۸, no. ۳, pp. ۲۷۲-۲۸۶, ۲۰۱۷/۰۷/۰۳ ۲۰۱۷, doi: ۱۰.۱۰۸۰/۰۰۵۱۱۴۴.۲۰۱۷.۱۴۰۷۰۲۲.

- [۸۴] I. Ruth, "Multi-dimensional structural data integration for proactive cyber-defence," in ۲۰۱۷ International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), ۲۰۱۷: IEEE, pp. ۱-۹.
- [۸۵] P. J. Murphy and E. Borghard, "To Defend Forward, US Cyber Strategy Demands a Cohesive Vision for Information Operations," *Cyber Defense Review*, vol. ۵, no. ۳, p. ۱۵, ۲۰۲۰. [Online]. Available: <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/۲۴۲۰۱۷۶/to-define-forward-us-cyber-strategy-demands-a-cohesive-vision-for-information-o/>
- [۸۶] C. Uthoff, "Current and Emerging Trends in Cyber Operations Policy, Strategy and Practice," in *Palgrave Studies in Cybercrime and Cybersecurity*, F. Lemieux Ed., no. ۱): Palgrave Macmillan UK, ۲۰۱۵, ch. ۱۳, sec. IV, pp. XIII, ۲۵۴.
- [۸۷] Cyberelectronic, "Explanation of the comprehensive model of cyber defense radar and pay-fund", ۲۰۲۰.
- [۸۸] J. B. Brazell, "The Need for a Transdisciplinary Approach to Security of Cyber Physical Infrastructure," in *Applied Cyber-Physical Systems*, S. C. Suh, U. J. Tanik, J. N. Carbone, and A. Eroglu Eds. New York Springer, ۲۰۱۴, ch. ۲, p. ۲۵۶.
- [۸۹] J. G. Schneider. "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy." *Lawfare Institute* <https://www.lawfaremedia.org/article/persistent-engagement-foundation-evolution-and-evaluation-strategy> (accessed).
- [۹۰] W. Dave, "The Pentagon's New Cyber Strategy: Defend Forward", ۲۰۱۸.
- [۹۱] Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior, ۲۰۲۰. [Online] Available: <https://www.lawfaremedia.org/article/operationalizing-defend-forward-how-concept-works-change-adversary-behavior>
- [۹۲] Supreme Leader, "Supreme Leader's Statement at Imam Ali (PBUH) Military University," ed, ۲۰۱۱
- Computer Science, Engineering and Information Technology, ۲۰۱۷. [Online]. Available: <https://civilica.com/doc/۶۷۶۸۵۵>.(in persian)
- [۷۶] L. Hansen and H. Nissenbaum, "Digital disaster, cyber security, and the Copenhagen School," *International studies quarterly*, vol. ۵۳, no. ۴, pp. ۱۱۵۵-۱۱۷۵, ۲۰۰۹.
- [۷۷] M. Barari and A. Mohammadi, "Defense in Cyberspace Based on the Recommendations of Imam Khamenei" presented at the Explanation of Imam Khamenei's Defense Thought, ۲۰۱۴. [Online]. Available: <https://www.noormags.ir/view/fa/articlepage/۱۸۶۶۲۴۷>.(in persian)
- [۷۸] J. C. Mitchell, "Active Defence," *ITNOW*, vol. ۵۴, no. ۴, pp. ۲۶-۲۷, ۲۰۱۲, doi: ۱۰.۱۰۹۲/itnow/bws۱۰۳.
- [۷۹] P. Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures," *Journal of International Law*, vol. ۴۷, p. ۱۳, ۲۰۱۳. [Online]. Available: <https://ssrn.com/abstract=۲۲۷۰۶۷۳> or <http://dx.doi.org/۱۰.۲۱۳۹/ssrn.۲۲۷۰۶۷۳>.
- [۸۰] S. McGee, R. V. Sabett, and A. Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense," *Business & Technology Law*, vol. ۸, no. ۱, p. ۴۷, ۲۰۱۳. [Online]. Available: <https://digitalcommons.law.umaryland.edu/jbtl/vol۸/iss۱/۳>.
- [۸۱] D. C. Blair, M. Chertoff, F. J. Cilluffo, and N. O'Connor, "Into the Gray Zone: The Private Sector and Active Defense against Cyber Threats," *Center for Cyber and Homeland Security*, George Washington University ۲۰۱۶.
- [۸۲] T. Mattern, J. Felker, R. Borum, and G. Bamford, "Operational levels of cyber intelligence," *International Journal of Intelligence and CounterIntelligence*, vol. ۲۷, no. ۴, pp. ۷۰۲-۷۰۴, ۲۰۱۴, ۷۱۹.
- [۸۳] H.-M. Chen, R. Kazman, I. Monarch, and P. Wang, "Can Cybersecurity Be Proactive? A Big Data Approach and Challenges," in *Hawaii International Conference on System Sciences*, ۲۰۱۷.