Supreme National Defense University
Quarterly Journal of Strategic Management Research in National Defense
https://issk.sndu.ac.ir E-ISSN: 2980-8219
Vol. 9, No. 1, Issue. 33, Spring 2025 **Received:** 2023/03/27 **Accepted:** 2024/05/14
Research paper

Proposing a Cyber Power Framework for the Islamic Republic of Iran Army

Hossein Moslemi
Faculty Member, AJA University of Command and Staff, Tehran, Iran.
Davod Azar
PhD Student, AJA University of Command and Staff, Tehran, Iran (Corresponding Author).
Email: davodazar@yahoo.com

Abstract

New and emerging technologies have provided unprecedented capabilities while simultaneously transforming the strategic environment. In the contemporary era, concepts such as hard power, soft power, and smart power reflect a shift of influence toward cyberspace. From a military perspective, cyber power has emerged as a critical strategic tool in recent decades, and its performance assessment using modern frameworks constitutes a key responsibility for senior commanders. The primary research question of this study is: What is the cyber power model of the Islamic Republic of Iran Army? The objective is to identify the directional elements, dimensions, and interrelations within this model. This applied and developmental research employs a case-study approach with both qualitative and quantitative methods. The statistical population consists of 75 personnel of the Islamic Republic of Iran Army, each holding a master's degree or higher in cyber-related fields and possessing at least 15 years of experience in command, staff, or technical positions in cyberspace operations. Qualitative and quantitative analyses identified 11 key indicators for the directional elements, 8 key indicators for the dimensions of cyber power, and 4 key indicators for the relationships among dimensions. Using these indicators, a comprehensive model of the cyber power of the Islamic Republic of Iran Army is proposed, detailing its components and dimensions.

Keywords: Cyber Operations, Cyber Power, Cyber Defense, Dimensions of Cyber Power

فصلنامه مطالعات مدیریت راهبردی دفاع ملی

سال نهم، شماره یکم (پیاپی ۳۳)، بهار ۱۴۰۴، صص. ۴۳-۷۶

تاریخ دریافت: ۱۴۰۲/۰۱/۰۷ ـ تاریخ پذیرش: ۱۴۰۳/۰۲/۲۵

مقاله پژوهشی

ارائه الگوی قدرت سایبری ارتش جمهوری اسلامی ایران

حسین مسلمی

عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران.

داود آذر

دانشجوی دکتری دانشگاه فرماندهی و ستاد آجا، تهران، ایران (نویسنده مسئول).

Email: davodazar@yahoo.com

چکیده

فناوری‌های جدید و نوظهور، قابلیت‌ها و توانمندی‌های جدیدی را در اختیار قرار داده و هم‌زمان محیط راهبردی را تغییر می‌دهند؛ در دوران معاصر، ظهور مفاهیمی مانند، قدرت سخت، قدرت نرم و هوشمند، بیانگر جابه‌جایی و چرخش قدرت به‌سوی سایبری است. به لحاظ نظامی، قدرت سایبری، از ابزارهای نوظهور چند دهه گذشته است. در تمام سطوح منازعه، قدرت سایبری، عامل حتمی و گریزناپذیر توانمندی‌های نظامی است. ازاین‌رو پایش عملکرد آن‌ها بر اساس الگوهای نوین، یکی از وظایف مهم فرماندهان عالی نیروهای مسلح به شمار می‌آید. سؤال اصلی این تحقیق عبارت است از: الگوی قدرت سایبری ارتش جمهوری اسلامی ایران کدام است؟ که در پاسخ به این سؤال ارکان جهت‌ساز، ابعاد و روابط بین ابعاد الگوی قدرت سایبری ارتش جمهوری اسلامی ایران تعیین می‌شود. نوع پژوهش کاربردی و توسعه‌ای، روش پژوهش، موردی-زمینه‌ای و اقدام‌پژوهی و همچنین رویکرد تحقیق، کمّی و کیفی است. جامعه آماری این تحقیق، شامل ۷۵ نفر کارکنان ارتش جمهوری اسلامی ایران است که دارای مدرک تحصیلی کارشناسی ارشد و بالاتر در رشته‌های مرتبط با علوم سایبری بوده و دارای حداقل ۱۵ سال سابقه خدمت در مشاغل فرماندهی، ستادی و فنی در حوزه فضای سایبر بوده‌اند. نتایج حاصل از تجزیه‌وتحلیل کیفی و کمی این پژوهش، احصای الگویی برای قدرت سایبری ارتش با ۱۱ شاخص اصلی برای ارکان جهت‌ساز، ۸ شاخص اصلی برای ابعاد قدرت سایبری و ٤ شاخص اصلی برای روابط بین ابعاد قدرت سایبری است و با استفاده از این شاخص‌ها، مؤلفه‌ها و ابعاد الگو ارائه شده است.

کلیدواژه‌ها: عملیات سایبری، قدرت سایبری، پدافند سایبری، ابعاد قدرت سایبری.

مقدمه

فضای سایبر همانند دیگر قلمروهای حکومتی از اهمیت راهبردی برای حفظ تمامیت ارضی و تأمین‌کننده امنیت ملی کشورها به شمار می‌آید. به‌نحوی‌که سازمان‌های نظامی ازجمله ارتش جمهوری اسلامی ایران، خط‌مشی‌ها، قوانین و مقررات، تدابیر و روش‌های بهره‌برداری خاص و ویژه‌ای را برای برتری و کسب قدرت در این فضا اتخاذ می‌کنند. از سوی دیگر مفاهیم نوینی مانند عملیات سایبر، جنگ سایبر، عملیات شبکه رایانه‌ای، سایبر الکترومغناطیس، سلاح‌های سایبری و تاب‌آوری سایبری مطرح شده که کاربرد آن‌ها در فضای سایبری باعث شکل‌گیری مفهوم قدرت سایبری در سازمان‌های نظامی و ارتش جمهوری اسلامی ایران است. امروزه قدرت سایبری در حوزه اطلاعات سایبری، عملیات سایبری و زیرساخت سایبری مورد مطالعه قرار می‌گیرد که هرکدام از این حوزه‌ها هم به صورت‌های تک‌بُعدی و چندبُعدی دارای عناصر و روابط بین آن‌ها هستند. بر اساس کارکردهای نوین سایبری، قدرت سایبری می‌تواند به یک منبع قدرت سخت تبدیل شود که توانایی وارد کردن صدمه به اهداف فیزیکی در یک کشور دیگر را دارد؛ برای مثال بیشتر صنایع پیشرفته و خدمات دولتی فرایندهایی دارند که توسط رایانه‌های متصل به سامانه‌های کنترل نظارتی و جمع‌آوری داده پردازش می‌شوند. نرم‌افزار مخربی که به این سامانه‌ها وارد می‌شود، می‌تواند برای خاموش کردن فرایندی که آثار کاملاً فیزیکی دارد برنامه‌ریزی شده باشد؛ نظیر برق یک شهر مانند شیکاگو یا مسکو را قطع کند که این خاموشی گسترده می‌تواند خساراتی بیشتر از بمباران این شهرها وارد کند (نای، ۲۰۱۰: ٤). به لحاظ نظامی نیز، قدرت سایبر، یکی از مهم‌ترین ابزار نوظهور چند دهه گذشته است. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبر، عامل حتمی و گریزناپذیر توانمندی‌های نظامی است و این توانمندی بر پایه فناوری‌های پیشرفته شکل گرفته است. قدرت سایبر روزبه‌روز به‌عنوان یک عامل تأثیرگذار در سیاست‌گذاری حوزه‌های ملی از اقدامات ضدتروریستی گرفته تا سامان دادن سیاست، اقتصاد و حتی روابط با سایر کشورها، توسعه می‌یابد (زابلی زاده، ۱۳۹۷: ۵۳).

با پیشرفت فناوری و توسعه زیرساخت‌های فضای سایبر، این فضا به‌راحتی و برای همه در دسترس هستند و هرگونه عملیات سایبری شامل عملیات خدمات‌رسانی، تراکنش‌های مالی، اقدام‌های مجرمانه و غیره در آن شکل می‌گیرد که این عملیات دارای آثار گسترده‌ای هم برای ارتش و هم برای جامعه به همراه خواهد داشت. به‌طور همه‌جانبه در خصوص قدرت سایبری ارتش جمهوری اسلامی ایران باید گفت که علاوه بر محافظت و دفاع از حریم فضای سایبری و سرمایه‌های اطلاعاتی حساس، مهم و حیاتی خود، باید قادر باشند تا از فرصت‌های بی‌شمار این فضا در پیشبرد مأموریت و اهداف نظامی خود بهره‌مند گردند و در این جهت لازم است که قابلیت‌های پدافند، آفند و تاب‌آوری را در فضای سایبری ایجاد کنند. ارتش جمهوری اسلامی ایران به سبب نبود الگوی قدرت سایبری برای استفاده از تسهیلات و کسب برتری، ضرورت دارد که از یک الگوی مناسب با شرایط و مختصات زمانی و مکانی مناسب برخوردار باشد. فضای سایبری به‌عنوان یکی از عوامل نامحسوس، به‌مثابه یک توانمندساز و تسهیل‌کننده، تأثیر بسزایی در قدرت ملی کشورها دارد. در دوران معاصر، جهت‌گیری اولویت‌های راهبردی کشورها، برای نیل به قدرت فائقه، به سمت بهره‌برداری از فضای سایبر تغییر یافته و فناوری‌های پیشرفته سایبری، زمینه‌ساز تجدید بنای قدرت ملی در قالب قدرت سایبری شده است (ولوی، ۱۳۹۹:۱۹۰-۱۹۲). وجود تعاریف و قرائت‌های مختلف از مفاهیم قدرت سایبری و نامشخص بودن عناصر اصلی قدرت سایبری ارتش و شکل‌گیری روابط نامشخص و نامعتبر بین این عناصر و بروز ناهماهنگی در کارکردهای قدرت سایبری موجب می‌شود تا وجود الگویی مدون احساس شود. الگوی قدرت سایبری، مستلزم شناسایی ارکان جهت‌ساز و ابعاد و روابط بین ابعاد است و با وجود تشکیل قرارگاه و فرماندهی‌های سایبری مختلف در آجا و سازمان‌های تابعه و گسترش روزافزون آن در همه ابعاد، الگوی جامعی جهت قدرت سایبری وجود ندارد. سؤال اصلی پژوهش حاضر، این است که الگوی قدرت سایبری ارتش جمهوری اسلامی ایران کدام است؟ این پژوهش در جهت ارائه الگوی قدرت سایبری ارتش جمهوری اسلامی ایران انجام شده است.

۱. مبانی نظری و پیشینه تحقیق

۱-۱. ارکان جهت‌ساز قدرت سایبری

ارکان جهت‌ساز قدرت سایبری، فرامین و رهنمودهای مقام معظم رهبری (مدظله‌العالی) در مورد قدرت و قدرت سایبری، اسناد بالادستی، راهبردها و اهداف است (هلیلی،۱۳۹۷: ۱٤٤). موضوع ارتقای قدرت سایبری یک موضوع فرا سازمانی و ملی است که تدوین این ارکان برای آن مستلزم شناخت مؤلفه‌های مرتبط با سیاست‌های ابلاغی، قانون اساسی و اسناد بالادستی این حوزه است. در این بخش، به مروری بر فرامین و رهنمودهای مقام معظم رهبری (مدظله‌العالی) و اسناد بالادستی می‌پردازیم که مهم‌ترین عوامل مؤثر در نحوه شکل‌گیری و تدوین ارکان جهت ساز قدرت سایبری کشور هستند.

۱-۲. سیاست‌های قدرت سایبری

فضای سایبر در کنار فرصت‌های بی‌بدیل خود، منشأ تهدیدات و مخاطرات فراوانی است که در صورت عدم تسلط و مهار آن‌ها، ابزاری برای براندازی نظام اسلامی تلقی می‌شود. مروری بر دیدگاه‌های رهبری در سال‌های اخیر، نشان می‌دهد برای مدیریت این فضا، هم رویکرد فرصت‌محور و هم رویکرد تهدیدمحور را نباید از نظر دور داشت. فضای سایبر به خاطر دارا بودن تمامی مؤلفه‌های قدرت در ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، علم و فناوری، دفاعی-امنیتی و حقوقی-قضایی فرصت مناسبی را برای تداوم و افزایش قدرت ملی، فراهم کرده است. درعینِ‌حال بهره‌گیری از فناوری‌های نوین فضای سایبر، به‌ویژه رسانه‌های سایبری به همان میزان که در افزایش قدرت نرم کارگشا است، می‌تواند به ابزاری برای کاهش قدرت ملی تبدیل شود. قدرت سایبری نوع متأخر قدرت است که در سال‌های اخیر، توجه نظریه‌پردازان را به خود جلب کرده است. مقام معظم رهبری نیز در سال ۱۳۹٤ در بند سوم از حکم اعضای دوره دوم شورای عالی فضای مجازی، با اشاره به «ارتقای جمهوری اسلامی ایران به قدرت سایبری در تراز قدرت‌های تأثیرگذار جهانی» بر آن صحه گذاشتند. از دیدگاه ایشان، برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در

جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه در ارتقای قدرت سایبری باید سرلوحه عمل قرار گیرد. باید به این نکته مهم توجه داشت که دستیابی به قدرت سایبری در نگاه ایشان، مبتنی بر مبانی دینی و جهت اعتلای فرهنگ و تعالی بشریت است که در تلاش برای رسیدن به قدرت هسته‌ای و پرهیز از رسیدن به سلاح هسته‌ای نیز به چشم می‌خورد؛ اما از دیدگاه دشمن، قدرت سایبری ایران برای انجام جنگ سایبری، ایجاد اختلال در سامانه‌های موشکی، فرماندهی، کنترل و غیره است و همچنان ایران‌هراسی را در این حوزه القا می‌کنند. مروری بر بیانات در سال‌های گذشته در حوزه قدرت و قدرت ملی، سیر تکامل نظریات ایشان از منابع و ابزارهای قدرت سنتی به قدرت سایبری را نشان می‌دهد. بنابراین مفهوم‌سازی و تبیین دکترین این چهره نوین از قدرت، برای تدوین راهبردها و در پیش گرفتن رویکردهای مناسب، در راستای عمل به سیاست‌های کلان ابلاغ شده توسط ایشان امری ضروری به‌نظر می‌رسد.

۱-۳. اسناد بالادستی

برای پیدا کردن ارتباط این اسناد با مقوله قدرت و قدرت سایبری برخی از مهم‌ترین اسناد اشاره شده، مورد بررسی قرار گرفته که نتایج آن در جدول زیر آمده است:

جدول ۱: موارد احصا شده از اسناد بالادستی در مورد قدرت

ردیف	عنوان سند و منبع (مرجع و سال تصویب)	موارد مرتبط احصا شده
۱	سند چشم‌انداز ۲۰ ساله (قانون اساسی، ۱۳۸۲)	در این سند، ایران در افق ۱۴۰۴ کشوری توسعه‌یافته با جایگاه اول اقتصادی، علمی و فناوری در سطح منطقه، با هویت اسلامی و انقلابی، الهام‌بخش در جهان اسلام و با تعامل سازنده و مؤثر در روابط بین‌الملل توصیف شده است که دارای امنیت، استقلال، اقتدار با سامانه دفاعی مبتنی بر بازدارندگی همه‌جانبه است.
۲	برنامه چهارم توسعه (مجلس شورای اسلامی، ۱۳۸۴)	در این برنامه، در ماده ۱۱۲ به ارتقای ابتکار عمل و توان مقابله مؤثر در برابر تهدیدها و حفاظت از منافع ملی، منابع حیاتی و انقلاب اسلامی و در ماده ۱۹۱ به تعمیق شناخت مؤلفه‌های قدرت ملّی و

ردیف	عنوان سند و منبع (مرجع و سال تصویب)	موارد مرتبط احصا شده
		ترویج روحیه دفاع از منافع ملّی و مخالفت با ظلم و سلطه‌گری اشاره شده است.
۳	سند راهبردی پدافند غیرعامل (سازمان پدافند غیرعامل، ۱۳۸۶)	ایفای نقش اساسی در حراست و حفظ استقلال، تمامیت ارضی و سرمایه‌های ملی در چرخه نظام دفاعی امنیتی کشور و افزایش ضریب امنیت ملی و قدرت بازدارندگی ملی و ارتقای آستانه تحمل ملی در برابر تهدید در بیانیه مأموریت این سند راهبردی، آمده است.
۴	سند راهبردی نظام جامع فناوری اطلاعات کشور (هیئت وزیران، ۱۳۸۷)	یکی از سناریوهای مورد توجه در این سند، سناریوی سلطه جهانی است که با مدیریت قدرت‌های سلطه‌گر و اداره جهان مبتنی بر جهانی‌سازی در ابعاد مختلف اقتصاد، سیاست و فرهنگ مطرح است. طراحان این سناریو، فناوری اطلاعات را مهم‌ترین ابزار برای تحقق اهداف خویش می‌دانند؛ بنابراین برای مقابله با آن، سناریوی توانمندسازی ملی برای ارتقاء قدرت رقابت‌پذیری صنعتی و فنی در عرصه جهانی و تأمین نیازهای ملی در حوزه فناوری مورد توجه قرار گرفته است.
۵	سند راهبردی امنیت فضای تولید و تبادل اطلاعات (هیئت وزیران، ۱۳۸۷)	در چشم‌انداز این سند، تأمین امنیت فضای تولید و تبادل اطلاعات کشور برای صیانت از حاکمیت و اقتدار ملی در افق ۱۴۰۴ معرفی شده و بر صیانت از منافع، اسرار و اقتدار ملی در فضای تولید و تبادل اطلاعات تأکید شده است. دستیابی به این چشم‌انداز، در قالب قدرت سایبری و تعامل فرامرزی در فضای سایبر، قابل تحقق است.
۶	برنامه پنجم توسعه (مجلس شورای اسلامی، ۱۳۸۹)	در این برنامه توسعه بر ارتقای توانمندی‌های دفاعی و قدرت بازدارندگی بر مبنای استفاده بهینه از فناوری اطلاعات و ارتباطات تأکید شده همچنین در ماده ۱۹۶ به پشتیبانی و کمک به مقابله با جنگ نرم در حوزه‌های مختلف با اولویت حضور فزاینده در فضای مجازی و رایانه‌ای (سایبری) با رویکرد بومی اشاره شده است. این موارد نشان از لزوم توجه به قدرت سخت و نرم سایبر را در سیاست‌های کلان نشان می‌دهد.
۷	سیاست‌های ابلاغی اقتصاد مقاومتی (مجمع تشخیص مصلحت نظام، ۱۳۹۲)	سیاست اقتصاد مقاومتی از منظر مقام معظم رهبری (مدظله‌العالی) می‌تواند با حفظ دستاوردهای کشور در زمینه‌های مختلف و تداوم پیشرفت و تحقق آرمان‌ها و اصول قانون اساسی و سند چشم‌انداز بیست‌ساله، اقتصاد متکی به دانش و فناوری، عدالت بنیان، درون‌زا و

ردیف	عنوان سند و منبع (مرجع و سال تصویب)	موارد مرتبط احصا شده
		برون‌گرا، پویا و پیشرو را محقق سازد. پیشتازی اقتصاد دانش‌بنیان، پیاده‌سازی اجرای نقشه جامعه علمی کشور و شناسایی ظرفیت‌های علمی، فنی و اقتصادی برای دسترسی به توان آفندی و اقدامات مناسب ازجمله سیاست‌هایی است که به‌کارگیری آن در نیل به قدرت سایبری باید سرلوحه عمل قرار گیرد.
۸	سیاست‌های ابلاغی علم و فناوری (مجمع تشخیص مصلحت نظام، ۱۳۹۳)	علم و فناوری یکی از ابعاد مهم قدرت سایبری است که در سیاست‌های ابلاغی مقام معظم رهبری سیاست‌های کلی آن مطرح شده است. دستیابی به علوم و فناوری‌های پیشرفته، برنامه‌ریزی و نظارت راهبردی در حوزه علم و فناوری و تقویت عزم ملی و افزایش درک اجتماعی نسبت به اهمیت توسعه علم و فناوری با اهتمام بر انتقال فناوری و کسب دانش طراحی و ساخت برای تولید محصولات داخلی ازجمله مواردی است که در این سیاست‌ها به آن اشاره شده و می‌تواند در بعد علم و فناوری قدرت سایبری مورد توجه قرار گیرد.
۹	حکم مقام معظم رهبری در انتصاب اعضای دوره دوم شورای عالی فضای مجازی (شهریور ۱۳۹۴)	مأموریت‌هایی ازجمله رصد وضعیت جاری و آینده‌نگری تحولات، تثبیت جایگاه مرکز ملی فضای مجازی مواجهه هوشمندانه و مقتدرانه با تحولات پرشتاب فضای مجازی در این حکم مدنظر قرار گرفته است.
۱۰	برنامه ششم توسعه (مجلس شورای اسلامی اسفند ۱۳۹۵)	در این برنامه به کسب جایگاه برتر منطقه در توسعه دولت الکترونیک و افزایش ظرفیت‌های قدرت نرم و دفاع سایبری توجه شده است. به‌عنوان مثال در ماده ۱۰۵ بر بهره‌برداری از دیپلماسی عمومی و روش‌ها و ابزارهای نوین و کارآمد اطلاع‌رسانی در گستره فرامرزی برای تبیین دیدگاه‌های جمهوری اسلامی ایران در ابعاد گفتمانی و معنایی و ارتقای جایگاه ایران در افکار عمومی جهان تأکید شده است. در ماده ۱۰۷ نیز طرح جامع توسعه قدرت نرم دفاعی و سایبری با مشارکت ستاد کل نیروهای مسلح و شورای عالی فضای مجازی مطرح شده است. در ماده ۱۰۹ ایجاد سامانه پدافند سایبری در سطح ملی به‌منظور ارتقاء قدرت رصد، پایش تشخیص و هشداردِهی و

ردیف	عنوان سند و منبع (مرجع و سال تصویب)	موارد مرتبط احصا شده
		مصون‌سازی تهدیدات از وظایف دولت برشمرده شده است. این موارد به‌عنوان مؤلفه‌هایی از قدرت سایبری باید مد نظر قرار گیرد.

۱-٤. مطالعات پژوهشی سایر کشورها در حوزه قدرت سایبر

در بخش بررسی اسنادی قدرت سایبری، کشورهای مختلفی مورد مطالعه و بررسی قرار گرفتند که از میان آن‌ها آمریکا، انگلیس، روسیه، چین، گرجستان، رژیم اشغالگر قدس، ترکیه و اتحادیه اروپا با توجه به دلایل زیر مورد بررسی قرار گرفت: ۱. مرتبط بودن اسناد منتشره با موضوع تحقیق؛ ۲. در دسترس بودن اسناد؛ ۳. اهمیت نظامی و امنیتی کشور مورد نظر.

البته بدیهی است که این بررسی بر اساس اسناد منتشره است و ممکن است تمامی موارد مذکور به‌صراحت در اسناد ذکر نگردیده باشند. مضامین راهبردی تعدادی از کشورها به شرح جدول زیر است (بوز، آلن، همیلتون، ۲۰۱۳):

جدول ۲: جمع‌بندی مطالعات قدرت سایبر کشورها

کشور	اهداف	راهبرد	اقدامات	ساختار
آمریکا	اهداف آفندی نیز ذکرشده	توجه به نخبه پروری از سوی وزارت دفاع در حوزه سایبری	شاخص گذاری سلامت فضای سایبر- ایجاد زیرساخت ملی هشدار	دفاع سایبری زیر نظر ارتش است و برخی هم در حیطه امنیت داخلی همکاری نزدیک دفاع و امنیت داخلی وابسته بودن امنیت آمریکا به هوش مصنوعی
انگلیس	توجه ویژه به امنیت فضای کسب‌وکار و عدم ذکر سیاست‌های دفاعی	دولت نقش هماهنگی و همراهی راهبردها را دارد تا دخالت مستقیم	ایجاد یک مرجع برای آگاهی‌رسانی به مردم	دفتر امنیت سایبری (متولی امنیت سایبری راهبردی) و مرکز عملیات امنیت سایبری است، زیر نظر سرفرماندهی ارتباطات دولتی

ساختار	اقدامات	راهبرد	اهداف	کشور
حضور بخش خصوصی در ایجاد امنیت همراه با بخش‌های امنیتی	عملیات شناسایی سایبری در زمان صلح با شناسایی قابلیت‌های هجومی دشمن و سپس توانایی‌های دفاع سایبری	سرکوب سایبری و تأثیرگذاری حملات سایبری، کسب برتری از طریق مختل کردن توان	توجه به نقش جدی مردم در ایجاد امنیت	روسیه
یک واحد ویژه در ستاد کل ارتش با بودجه و ساختار مستقل	ارزیابی ریسک و تعیین تهدیدات توسط سازمان ملی امنیت اطلاعات و توجه به مانیتورینگ محتوا	توجه به رمزنگاری و ترویج آموزش‌ها از سطوح ابتدایی و کنترل و نظارت شدید دولت	دنبال کردن استراتژی ناتو در تقویت دفاع سایبری	ترکیه
واحد ۸۲۰۰ محرمانه‌ترین ساختار درون امان است که مسئول شنودها و دریافت ارتباطات الکترونیکی	مدیریت ریسک همکاری بین ارتش (نیروهای مسلح) و دیگر سازمان‌های امنیتی و بخش خصوصی	جذب سرمایه‌گذاری بودجه‌ای شرکت‌های خارجی فعال صنعت فاوا و افتا	همکاری و ادغام تلاش‌ها در میان واحدهای هر بخش، مانند یکپارچه‌سازی فعالیت‌ها و اشتراک دانش بین ارتش (نیروهای مسلح) و دیگر سازمان‌های امنیتی	رژیم صهیونیستی
توسعه رمزنگاری ارتقای استانداردهای راهنمای صنعت برای کیفیت عملکرد شرکت‌ها در امنیت سایبر و ارتقای اطلاعات قابل‌دسترسی برای عموم، به‌وسیله توسعه برچسب‌های امنیتی یا نشانه‌های درجه‌بندی که به مصرف‌کننده در ارزیابی بازار کمک کند.		برابر افق ۲۰۲۰ اتحادیه اروپا ابزارها و ادوات مبارزه با فعالیت‌های تروریستی که فضای سایبر را هدف گرفته‌اند توسعه داده است.		اتحادیه اروپا

۱-۵. مفهوم شناسی قدرت سایبری

در فضای سایبر، شکل‌گیری جوامع شبکه‌ای، موجب تغییر ساختار سلسله‌مراتبی قدرت و ایجاد ساختار شبکه‌ای تقویت شده که از آن، تحت عنوان پراکندگی قدرت نام برده می‌شود.

تغییر موازنه قدرت، تقسیم قدرت میان بازیگران مختلف و کاهش قدرت مرکزی دولت‌ها از پیامدهای این پدیده است. فناوری‌های پیشرفته فضای سایبر، الگوهای قدرت سنتی را درهم‌شکسته و با تغییر در مفهوم و کارکردهای قدرت، بنیان اقتدار رایج در دولت‌ها را به چالش کشیده است. رسانه‌های اینترنتی و شبکه‌های اجتماعی مجازی، امروزه کارایی خود را در تسلیم دولت‌ها به خواسته‌های عمومی مردم نشان داده است. هر کشور، برای حفظ موجودیت خود و نقش‌آفرینی مؤثر در عرصه جهانی، نیازمند به تعامل و انعطاف‌پذیری لازم، برای تطبیق خود با محیط بین‌الملل است. چنانچه دولت‌ها قادر به تطبیق خود با شرایط جدید نباشند، بقا و دوام آن‌ها با چالش روبه‌رو خواهد شد. در فضای سایبر، درک قواعد بازی و سیاست‌گذاری مناسب جهت بهره‌برداری از فرصت‌ها و قابلیت‌های فضای سایبر، از اهداف مهم کسب قدرت تلقی می‌شود و می‌توان آن را در قالب قدرت سایبری مورد توجه قرار داد. از نظر تیم جردن[1]، استاد بریتانیایی فعال در حوزه فرهنگ رقومی در کتاب خود با عنوان «قدرت سایبری: فرهنگ و سیاست‌های فضای سایبر» فضای سایبر را از منظر اجتماعی، فرهنگی و سیاسی مورد بررسی قرار داده است. وی معتقد است باوجود ماهیت پویا و متغیر فضای سایبر، روابط و الگوهای به نسبت پایداری از سبک زندگی در فضای سایبر در حال شکل‌گیری است. بنابراین بااینکه قدرت در فضای سایبر موضوعی پیچیده است؛ اما می‌توان پیامدهای آن را در حوزه‌های اجتماعی، فرهنگی و سیاسی در نظر گرفت. از دیدگاه وی، قدرت سایبری، در سه حوزه فردی، اجتماعی و تخیلی وابسته به هم، تشکیل شده است. در حوزه فردی و فضای اطلاعاتی در مالکیت افراد است، در حوزه اجتماعی، قدرت در قالب سلطه نمایانگر می‌شود و در بُعد تخیل، قدرت به‌عنوان مؤلفه مهم نظم اجتماعی، می‌تواند آرمان‌شهر و یا ویران‌شهر را به وجود آورد.

1. Tim Jordan

۱-٦. آفند سایبری

گونه‌ای از عملیات سایبری (عملیات سایبری شامل حمله، دفاع و تاب‌آوری سایبری) هستند که برای تأمین قدرت در فضای سایبری یا از طریق فضای سایبری طراحی شده‌اند. عملیات سایبری تهاجمی ممکن است منحصراً عملکردهای فضای سایبری دشمن را هدف قرار دهد و یا اثرات درجه‌یک را در فضای سایبری ایجاد کند تا با کنترل دقیق اثرات در حوزه‌های فیزیکی بر سامانه‌های تسلیحاتی، فرایندهای فرماندهی و کنترل، گره‌های لجستیکی، اهداف با ارزش بالا و غیره تأثیر بگذارد. برخی از مأموریت‌های عملیات سایبری تهاجمی می‌توانند شامل اقداماتی باشد که منجر به به‌کارگیری نیرو با تخریب یا انهدام فیزیکی سامانه‌های دشمن شود. تأثیرات خاص ایجاد شده به زمینه وسیع‌تری مانند وجود یا قریب‌الوقوع بودن خصومت‌های آشکار و ملاحظات سیاست ملی بستگی دارد.

۱-۷. پدافند سایبری

تعریف پدافند سایبری: مأموریت‌هایی برای حفظ توانایی استفاده از قابلیت‌های فضای مجازی آبی و محافظت از داده‌ها، شبکه‌ها، دستگاه‌های دارای فضای مجازی و سایر سامانه‌های تعیین شده با شکست فعالیت‌های مخرب در حال انجام یا قریب‌الوقوع فضای مجازی (فرهنگ لغت وزارت دفاع آمریکا، ۲۰۲۱: ٦۰).

۱-۸. تاب‌آوری سایبری

عبارت است بخشی از قدرت سایبری که توانایی یک سازمان برای مقاومت واکنش و بازیابی از تهدیدهای که بر روی اطلاعات است تأثیر خواهد داشت که به آن اطلاعات در انجام کسب‌وکار نیاز است. تاب‌آوری سایبری عبارت از توانایی آمادگی و سازگاری برای تغییر شرایط و تحمل و بازیابی سریع پس از اختلال‌ها است. بازیابی شامل توانایی تحمل و بازیابی از حملات عمدی، رویدادها یا تهدیدهای طبیعی یا حوادث است. تاب‌آوری سایبری، به‌عنوان توانایی سامانه‌ها و سازمان‌ها برای مقاومت در برابر حوادث سایبری تعریف می‌شود. تاب‌آوری سایبری، قابلیت سازمانی برای مقاومت در برابر تأثیرات منفی، باتوجه به تهدیدهای

شناخته شده، قابل پیش‌بینی، ناشناخته، غیرقابل پیش‌بینی، نامشخص و غیرمنتظره از فعالیت‌ها در فضای سایبری است. تاب‌آوری، توانایی دارایی‌ها، شبکه‌ها و سامانه‌ها برای پیش‌بینی، جذب و انطباق و یا بازیابی سریع از رویداد مخرب است (تقی‌پور، ۱۳۹۷: ۱۹۳).

۱-۹. راهبردهای پدافندی قدرت سایبری

پدافند سایبری توانایی‌های سازمان‌دهی شده برای محافظت در برابر حمله‌ها، کاستن خسارت‌های ناشی از آن‌ها و بازگشت سریع به وضعیت عادی در مقابل حمله سایبری است. این امر به فعالیت‌هایی اشاره دارد که از سوی یک‌طرف برای محافظت از منافعش در برابر یک حمله، صورت می‌گیرد. دفاع مؤثر در سامانه‌های الکترونیکی اغلب بر مبنای تشخیص، جداسازی، گزارش‌دهی، بازگشت به وضعیت عادی و خنثی‌سازی قرار دارد. توانایی دفع یک حمله، می‌تواند راهبرد دفاعی مؤثری باشد. یک حمله تنها هنگامی مؤثر است که یک ضعف واقعی را مورد هدف قرار دهد. برای داشتن دفاع سایبری همه‌جانبه و یکپارچه در سراسر کشور، بایستی چهار دسته توانمندی‌ها را در کشور تولید و تقویت نماییم:

۱. توانمندی‌های راهبردی: شامل تدوین سیاست‌ها، برنامه‌های راهبردی؛
۲. دستورالعمل‌های اجرایی: ایجاد وحدت فرماندهی در بخش سایبری، ایجاد ساختار سازمانی، توسعه بخش آموزشی و تخصیص بودجه به تمام قسمت‌های یاد شده؛
۳. توانمندی‌های علمی: لازمه دستیابی به دانش علمی، مطالعات بنیادی و نظریه‌پردازی در این زمینه است. همچنین ایجاد ساختارهای لازم و زیرساخت‌های آموزشی و پژوهشی می‌تواند دستیابی به چنین توانمندی مهمی را تسهیل نماید؛
٤. توانمندی عملیاتی: در این بخش بایستی توان دستگاه‌های کارفرما و نیز سایر دستگاه‌ها را به میزان کافی بالا برد تا بتوان توانمندی‌های عملیاتی را ارتقا داد (اسدالله‌زاده، ۱۳۹٤: ۱٤۸).

۱-۱۰. اهداف قدرت سایبری

۱-۱۰-۱. تقسیم‌بندی اهداف

اهداف برحسب سازمان، سطح و زمان تقسیم‌بندی‌های متعددی می‌شود در تقسیم‌بندی زمانی اهداف، تأکید بیشتر به رسیدن به هدف در بازه زمانی مشخص است.

این تقسیم‌بندی را می‌توان به دو دوره زمانی کوتاه‌مدت و بلندمدت تقسیم کرد (حسن بیگی، ۱۳۹۱: ۲۳۰-۲۲۰). دوره کوتاه‌مدت تا ۳ یا ۵ سال است و دوره بلندمدت بیشتر از ۵ سال.

به‌طور معمول برنامه‌های توسعه برحسب اهداف سالیانه و ۵ ساله «کوتاه‌مدت» و بیست‌ساله «چشم‌انداز- بلندمدت» دیده می‌شود.

فناوری‌های نوین فضای سایبر افق‌های نوینی را پیشِ روی دولت‌ها برای مدیریت این چالش‌ها فراهم نموده است. تحقق کارآمدی از مهم‌ترین دغدغه‌های دولتمردان و اندیشمندان برای توجیه حقانیت و مشروعیت قدرت سایبری است. کارآمدی مفهومی انتزاعی نیست بلکه مفهومی عملی است که نیازمند انجام اقدامات لازم و قانونی در حوزه‌های مطرح شده است.

از دیگر اهداف قدرت سایبری بازدارندگی است که همچون سایر عوامل بازدارندگی در نوع خود بیانگر نوعی از اقتدار را جلوه می‌کند (قیصری و قربانی،۱۳۹٤: ۱٤۸-۲۹).

جدول ۳: اهداف بلندمدت قدرت سایبری

اهداف بلندمدت	توصیف
پیش‌بینی[1]	برای جلوگیری از مواجهه عملکرد مأموریت با شرایط نامطلوب احتمالی وضعیت آمادگی آگاهانه را حفظ کنید.
مقاومت[2]	عملکردهای اساسی مأموریت را باوجود شرایط نامساعد ادامه دهید.
بازیابی[3]	عملکردهای مأموریت را در طی شرایط نامساعد و بعد از آن بازیابی کنید.
بهبود[4]	عملکردهای مأموریت و یا قابلیت‌های پشتیبانی را تغییر دهید تا تأثیرات نامطلوب ناشی از شرایط نامطلوب واقعی یا پیش‌بینی‌شده به حداقل برسد.

1. Anticipate
2. Withstand
3. Recover
4. Evolve

اهداف میان‌مدت عبارت‌های مشخص‌تری از نتایج مورد نظر است که به‌منظور تسهیل ارزیابی بیان شده است. یک هدف میان‌مدت را می‌توان با یک هدف نهایی واحد شناسایی کرد؛ اما ممکن است دستیابی به اهداف نهایی متعدد را امکان‌پذیر کند. اهداف میان‌مدت به‌عنوان پلی بین تکنیک‌ها و اهداف نهایی عمل می‌کنند. آن‌ها بیان می‌شوند تا ارزیابی را تسهیل کنند. آن‌ها ذی‌نفعان مختلف را قادر می‌سازند تا اولویت‌های مختلف خود را بر اساس مأموریت اعلام کنند. جدول زیر اهداف میان‌مدت قدرت سایبری را بیان می‌کند.

جدول ٤: اهداف میان‌مدت قدرت سایبری

اهداف میان‌مدت	توصیف
درک	نمایش‌های مفیدی از وابستگی‌های مأموریت و وضعیت منابع را با توجه به مشکلات احتمالی حفظ کنید
آمادگی	مجموعه‌ای از اقدامات واقع‌بینانه را حفظ کنید که مشکلات پیش‌بینی‌شده یا پیش‌بینی‌نشده را برطرف می‌کند
اجتناب-جلوگیری	جلوگیری از اجرای موفقیت‌آمیز حمله یا تحقق شرایط نامطلوب
تداوم	به حداکثر رساندن مدت‌زمان و دوام عملکردهای اساسی مأموریت در شرایط نامطلوب
مهار کردن	آسیب ناشی از شرایط نامساعد را محدود کنید
به حال اول برگرداندن	مجدداً منابع را برای ارائه به‌عنوان رقابت مجموعه‌ای از قابلیت‌های مأموریت به دلیل شرایط نامطلوب، مجدداً به‌کار گیرید
انتقال	جنبه‌های رفتار سازمانی را در پاسخ به شرایط نامطلوب قبلی، فعلی یا احتمالی یا حمله تغییر دهید
بازطراحی	اصلاح ساختارها برای ارتقای تاب‌آوری

اهداف کوتاه‌مدت در قالب فنون دفاع سایبری در چهارچوب مهندسی سایبری در جدول (۵)، مشخص و تعریف‌شده است.

جدول ۵: رابطه بین اهداف و روش دفاع سایبری در چهارچوب مهندسی سایبری

اهداف کوتاه‌مدت (روش)	توصیف
پاسخ انطباقی	به‌طور مناسب و پویا به موقعیت‌های خاص پاسخ دهید، با استفاده از حوادث غیرمترقبه عملیاتی چابک و جایگزین برای حفظ حداقل توانایی‌های عملیاتی، به‌منظور محدود کردن عواقب و جلوگیری از بی‌ثباتی، اقدامات پیشگیرانه را در صورت لزوم انجام دهید.
نظارت تحلیلی	مداوم برای استفاده از هوش تهدید، شناسایی آسیب‌پذیری‌ها، یافتن نشانه‌هایی از شرایط نامطلوب بالقوه و شناسایی آسیب‌های بالقوه یا موجود به‌طور مداوم داده‌ها جمع‌آوری، تلفیق و تجزیه‌وتحلیل کنید.
دفاع هماهنگ	سازوکارهای چندگانه و متمایز (دفاع در عمق) را برای محافظت از منابع حیاتی، در میان زیرسامانه‌ها، لایه‌ها، سامانه‌ها و سازمان‌ها هماهنگ کنید.
فریب	دشمن را گیج، فریب و گمراه کنید.
تنوع	برای به حداقل رساندن خرابی‌های معمول (ازجمله حملات سوءاستفاده از آسیب‌پذیری‌های رایج) از مجموعه‌ای ناهمگن از فناوری‌ها، منابع داده، مکان‌های پردازش و مسیرهای ارتباطی استفاده کنید.
موقعیت‌یابی پویا	توزیع و جابجایی پویا عملکردها و دارایی‌ها
نمایندگی پویا	آگاهی و پاسخ‌گویی به وضعیت مأموریت را با استفاده از نمایش‌های پویا از اجزاء، سامانه‌ها، خدمات، فعالیت‌های خصمانه و سایر موقعیت‌های نامطلوب و اثرات اقدامات جایگزین پشتیبانی کنید.
عدم ثبات و پایداری	اطلاعات، خدمات و ارتباطات را برای مدت‌زمان محدودی حفظ کنید، درنتیجه قرار گرفتن در معرض خرابی، دخل و تصرف را کاهش دهید.
محدودیت امتیاز	طراحی برای محدود کردن امتیازات اختصاص‌یافته به کاربران و نهادهای سایبری و تنظیم شرایط لازم برای امتیازات بر اساس اهمیت
تجدیدنظر	منابع را قادر می‌سازد تا با وظایف اصلی مأموریت هماهنگ شوند (دوباره تنظیم شوند)، بنابراین سطح حمله، احتمال عواقب ناخواسته و احتمال خرابی‌های ناگهانی را کاهش می‌دهد.
افزونگی	چندین نمونه محافظت‌شده از اطلاعات و منابع حیاتی فراهم کنید تا از عواقب تلفات کاسته شود.
تقسیم‌بندی- جداسازی	برای محدود کردن گسترش آسیب، اجزا (منطقی یا فیزیکی) را بر اساس حساسیت و اعتبار جدا کنید.

اهداف کوتاه‌مدت (روش)	توصیف
یکپارچگی ثابت‌شده	مکانیسم‌هایی را برای اطمینان از خرابی خدمات مهم، بانک‌های اطلاعاتی، جریان اطلاعات و اجزای سازنده فراهم کنید.
غیرقابل‌پیش‌بینی بودن	مرتباً و به‌طور تصادفی تغییراتی ایجاد کنید تا سطح حمله غیرقابل‌پیش‌بینی شود.

جدول (٦)، رابطه بین اهداف و فنون سایبری در چهارچوب قدرت سایبری را نشان می‌دهد.

جدول ٦: ایجاد ارتباط بین فنون سایبری با اهداف جزئی

	درک	آمادگی	پیشگیری	تحمیل کردن	تداوم	بازیابی	انتقال	بازطراحی
پاسخ مناسب				❊	❊	❊		
نظارت تحلیلی	❊	❊		❊		❊		
دفاع هماهنگ		❊	❊	❊	❊	❊		
فریب	❊		❊		❊			
تنوع			❊		❊			❊
موقعیت‌یابی پویا	❊		❊		❊			❊
نمایندگی پویا	❊	❊					❊	
عدم ثبات و پایداری			❊	❊	❊			❊
محدودیت امتیاز			❊	❊				
تجدیدنظر				❊			❊	
افزونگی					❊	❊		
تقسیم‌بندی / جداسازی			❊	❊				
یکپارچگی ثابت‌شده	❊			❊	❊	❊		
غیرقابل‌پیش‌بینی بودن	❊		❊		❊			

۲. روش‌شناسی تحقیق

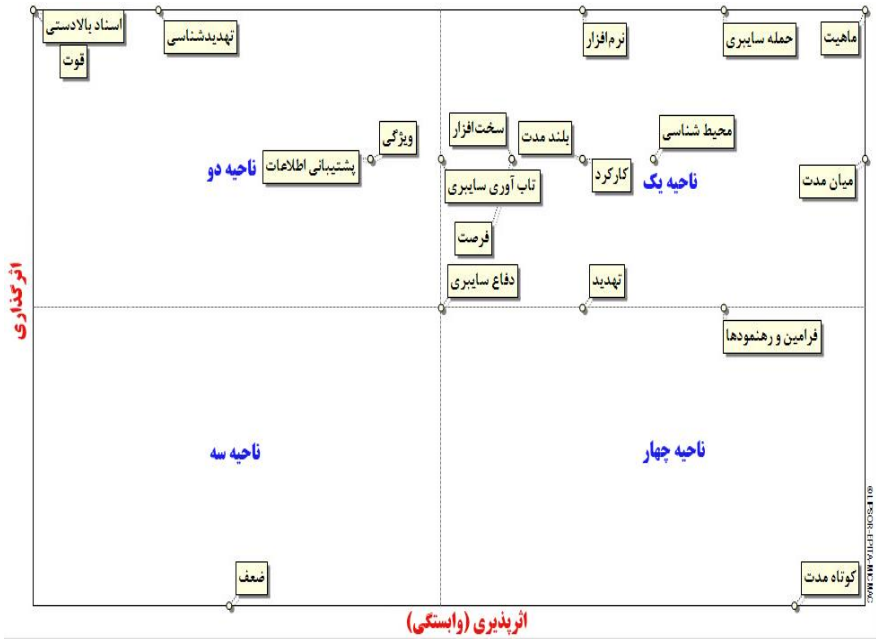
روش اجرای پژوهش توصیفی-تحلیلی است، نوع این تحقیق کاربردی است و رویکرد این تحقیق آمیخته است. صاحب‌نظران انتخاب‌شده همگی از فرماندهان و مسئولین و متخصصین آگاه در حوزه سایبری هستند که به موضوع تحقیق آشنایی کامل دارند؛ سؤال‌ها به‌گونه‌ای طراحی شده است که تمام ابعاد موضوع را پوشش دهد و محقق را در دستیابی به هدف تحقیق یاری دهد. سؤالات مصاحبه به گروهی از صاحب‌نظران در زمان‌های متفاوت ارائه شده و پاسخ‌های ارائه شده برای سنجش روایی سؤالات مصاحبه مقایسه شدند. از اسناد و مدارک معتبر موجود در کتابخانه‌ها و مقاله‌های علمی از سایت‌های اینترنتی معتبر استفاده شده است و همچنین با استفاده از منابع متعدد پر ارجاع بر میزان اعتبار منابع افزوده شده و برای اطمینان از اعتبار منابع از نظرات متخصصین موضوع و اساتید محترم استفاده شده است.

۳. تجزیه‌وتحلیل داده‌ها

روش تحلیل داده‌ها به این شکل بود که در گام نخست با بهره‌گیری از تحلیل محتوای ابعاد نظری تحقیق مفاهیم استخراج شد. در گام دوم تحلیل مضمون با کمک نرم‌افزار مکس‌کیودا انجام شد. در گام سوم برای احصای شاخص‌ها، نسبت به پالایش یا ادغام مفاهیم کلیدی پرداخته شد. در گام چهارم طی یک فرایند علمی و خبرگی، شاخص‌ها از جهت وجوه تشابه و تفاوت باهم مقایسه شدند سپس شاخص‌هایی که حول یک محور مشترک قرار داشتند و می‌توانستند اجزای تشکیل‌دهنده ارکان جهت‌ساز و ابعاد باشند در یک طبقه سازمان‌دهی شدند و بر اساس این فرایند علمی، استخراج شد. در گام پنجم مؤلفه‌هایی که دارای یک مفاهیم مشترک و مشابه بودند در ذیل یک طبقه سازمان‌دهی شدند.

تحلیل نتیجه ماتریس اثر متقابل در دو سطح انجام می‌گیرد؛ تحلیل اثرات متقابل مستقیم و تحلیل اثرات متقابل غیرمستقیم. تحلیل اثرات متقابل مستقیم نحوه اثرگذاری و اثرپذیری متغیرهای موضوع مطالعه را ارزیابی می‌کند به‌نحوی که پس از محاسبات صورت گرفته، هر یک از متغیرها در یکی از نواحی محور مختصات که دارای مفاهیم معنی‌داری هستند قرار

می‌گیرند؛ اما در تحلیل اثرات متقابل غیرمستقیم هم تأثیر متقابل و هم تأثیر متغیرها در نواحی چهارگانه حاصل از محاسبات دقیق‌تری است. شکل(۲)، پراکنش شاخص‌ها را بر اساس نظرات خبرگان در نواحی چهارگانه نشان می‌دهد.



شکل ۱: پراکنش شاخص‌ها در نواحی چهارگانه

بر اساس پراکنش شاخص‌ها که در شکل فوق مشاهده می‌شود و بر اساس این اصل که این پراکنش به شکل حرف L لاتین در نیامده است، نظام از وضعیت ناپایداری برخوردار است و کمترین تغییر در متغیرهای خطر که در محدوده شمال غربی نمودار قرار می‌گیرند؛ نظام دچار دگرگونی می‌شود یعنی تغییر شاخص‌ها منجر به بر هم خوردن پایداری نظام می‌شود.

بر اساس شکل تحلیل‌های مطرح شده برای خروجی میک مک که توسط گوردون[1] عنوان شده است چهار ناحیه نشان داده شده در شکل (۳)، به‌صورت زیر تحلیل می‌شوند:

متغیرهای دو وجهی (ناحیه یک نمودار و پراکنش شاخص‌ها): این متغیرها در ناحیه شمال شرقی نمودار قرار دارند و دارای خاصیت تأثیرگذاری-تأثیرپذیری بالایی هستند و طبیعت آن‌ها با عدم پایداری آمیخته است. این متغیرها قابل دست‌کاری و کنترل هستند و بر پویایی و تغییر نظام تأثیر می‌گذارند یعنی شاخص‌های ناپایداری را تشکیل می‌دهند. متغیرهایی که بالای خط قطری این ناحیه قرار می‌گیرند، متغیرهای ریسک نامیده می‌شوند متغیرهایی که زیرخط قطری این ناحیه قرار می‌گیرند متغیرهای «هدف» نامیده می‌شوند و نتایج نظام را به نمایش می‌گذارند. به عبارت دیگر، با دست‌کاری این متغیرها نظام تغییرات تکاملی را در پیش خواهد گرفت. با این توصیف متغیرهایی را که تأثیر بالایی دارند ولی قابل‌کنترل نیستند، به‌عنوان متغیر راهبردی محسوب نمی‌شوند. این متغیرها خود به دو دسته متغیرهای ریسک و متغیرهای هدف تقسیم می‌شوند. متغیرهای خطر حول‌وحوش خط قطری شمال شرقی هستند و از ظرفیت بالایی برای تبدیل به بازیگر کلیدی برخوردارند. بر اساس شکل فوق عواملی که در این گروه قرار می‌گیرند، عبارت‌اند از: نرم‌افزار، ماهیت، حمله سایبری، محیط‌شناسی، اهداف بلندمدت، سخت‌افزار، کارکرد، فرصت و تاب‌آوری. این شاخص‌ها با توجه به اینکه نظام ناپایدار است همان شاخص‌های اصلی مد نظر پژوهش هستند که در این ناحیه قرار می‌گیرند و نیروهای پیشران کلیدی نظام را تشکیل می‌دهند. این‌که این شاخص‌ها به‌عنوان نیروهای پیشران اصلی شناخته شده‌اند، نشان می‌دهد که بایستی در تدوین الگوی قدرت سایبری آجا این شاخص‌ها در اولویت اول قرار بگیرند. متغیرهای هدف نیز در زیر ناحیه خط قطری شمال شرقی و نزدیک به محور ایکس‌ها قرار دارند که در مطالعه حاضر شاخص‌های تهدید، فرامین و رهنمودها و اهداف میان‌مدت جزو متغیرهای هدف هستند، این شاخص‌ها امکان تبدیل شدن به نیروهای پیشران کلیدی را دارا می‌باشند و با اندک تغییراتی در آن‌ها قابلیت تبدیل به پیشران‌های کلیدی را دارند.

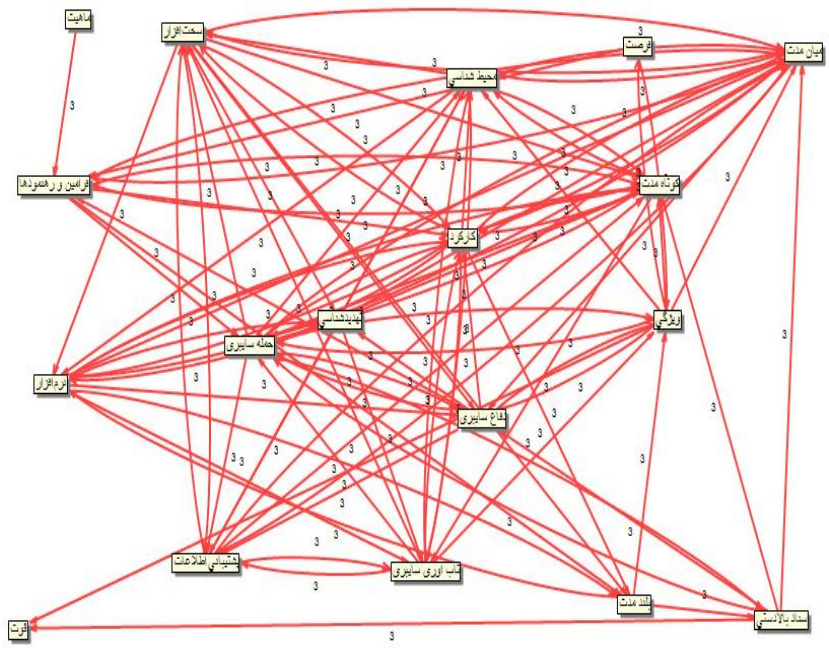
1. Gordon

متغیرهای تأثیرگذار (ناحیه دو نمودار و پراکنش شاخص‌ها): این متغیرها در قسمت شمال غربی نمودار قرار می‌گیرند و مهم‌ترین مؤلفه‌های تأثیرگذار در نظام هستند. برنامه‌ریزان به‌ندرت قادر به تغییر در متغیرهای قرارگرفته در ناحیه دو هستند. متغیرهای مزبور در قسمت شمال غربی نمودار نمایش داده می‌شوند. به‌عنوان بحرانی‌ترین و کلیدی‌ترین مؤلفه‌ها، بیشتر تأثیرگذار و کمتر تأثیرپذیر هستند و متغیرهای ورودی محسوب می‌شوند. متغیرهای محیطی عموماً در این قسمت قرار می‌گیرند که توسط نظام قابل کنترل نیستند. از آنجا که نظام ناپایدار است، بایستی تعداد کمی از شاخص‌های شناسایی شده در این ناحیه قرار بگیرد، که پراکنش نشان داده این مورد را اثبات می‌کند و همان‌گونه که می‌بینیم شاخص‌های تهدیدشناسی، اسناد بالادستی، قوت ویژگی و پشتیبانی اطلاعات در این محدوده قرار گرفته‌اند که این شاخص‌ها از توان تأثیرگذاری بالایی بر نظام برخوردارند.

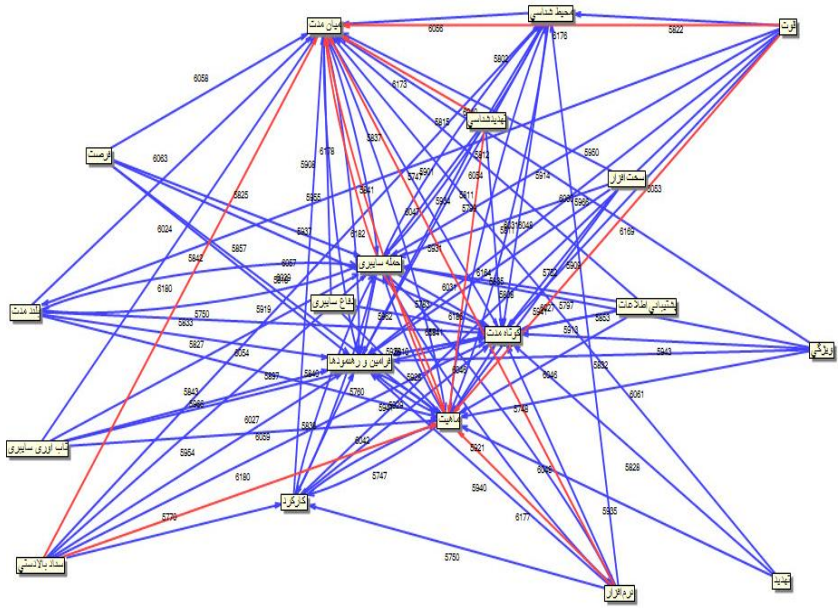
متغیرهای مستقل (ناحیه سه نمودار و پراکنش شاخص‌ها): متغیرهای مستقل در قسمت جنوب غربی نمودار قرار دارند. این‌ها نه بسیار تأثیرگذارند و نه بسیار تأثیرپذیر. به عبارتی، آن‌ها نه باعث توقف یک متغیر می‌شوند و نه موجب تکامل آن. که با توجه به پراکنش نشان داده شده، شاخص «ضعف» به‌عنوان تنها شاخص مستقل معرفی می‌شود که در این بخش قرار دارد. متغیری با کمترین میزان تأثیرگذاری و تأثیرپذیری و طبیعی است که این متغیرها ارزش تحلیلی نداشته و اهمیتی برای آن در نظام متصور نیستند ازاین‌رو در تدوین الگوی قدرت سایبری آجا از جایگاه مهمی برخوردار نخواهد بود البته این بدان معنی نیست که نبایستی به آن توجه نمود.

متغیرهای وابسته (ناحیه چهار نمودار و پراکنش شاخص‌ها): ربع پایینی سمت راست محل استقرار متغیرهایی با تأثیرپذیری بالا و تأثیرگذاری پایین است. این شاخص‌ها که با عنوان شاخص‌های وابسته نظام نیز شناخته می‌شوند، از این بابت که در اثر تغییرات نظامی بیشترین تغییر در آن‌ها رخ خواهد داد اهمیت دارند. لکن خود این متغیرها منشأ اثر و ایجاد تغییر در نظام نیستند. این شاخص‌ها به دلیل وابستگی شدید به سایر شاخص‌ها خاصیت راهبردی ندارند و بیشتر از سایر شاخص‌ها نتیجه می‌شوند و به‌عنوان شاخص‌های وابسته

تعریف می‌شوند با توجه به پراکنش نشان داده شده، شاخص «اهداف کوتاه‌مدت» جزو شاخص‌های وابسته به نظام معرفی می‌شود و معنی آن این است که در تدوین الگوی قدرت سایبری آجا به‌عنوان یک شاخص وابسته با سایر شاخص‌ها تلقی می‌شود که البته این دور از ذهن نیز نیست چرا که در مبحث امنیت سایبری اهداف کوتاه‌مدت وابسته به سایر عوامل هستند و در بخش شاخص‌های مربوط به اهداف میان‌مدت و بلندمدت از اعتبار بالاتری برخوردارند. یکی دیگر از خروجی‌های نرم‌افزار میک‌مک گراف تأثیرات مستقیم و گراف غیرمستقیم شاخص‌هاست که در شکل‌های زیر ترسیم شده‌اند که این تصاویر نحوه ارتباط مستقیم و غیرمستقیم تأثیرات متقابل شاخص‌های (متغیرها یا بازیگران) دخیل بر تدوین الگوی قدرت سایبری آجا را نمایش می‌دهند.



شکل ۲: گراف تأثیرات مستقیم شاخص‌ها



شکل ۳: گراف تأثیرات غیرمستقیم شاخص‌ها

بر اساس دو تصویر نشان داده شده در شکل‌ها، شاخص «کارکرد» به‌عنوان مرکزی‌ترین شاخص الگو معرفی می‌شود؛ زیرا در مرکز نمودار قرار دارد و توجه سایر شاخص‌ها به آن معطوف است و این به دلیل تأثیرگذاری بسیار بالایی است که این شاخص می‌تواند داشته باشد؛ اما شاخص «اهداف کوتاه‌مدت» به‌عنوان وابسته‌ترین شاخص تعیین می‌شود؛ زیرا در مرکز شکل قرار گرفته و تقریباً از تمامی شاخص‌ها تأثیر می‌پذیرد.

رتبه‌بندی میزان اثرگذاری و اثرپذیری عوامل، بر اساس نرم‌افزار میک مک انجام شد که تحلیل نتیجه‌ای که حاصل رتبه‌بندی است، در جدول (۷)، آورده شده است. مثبت بودن نشانه اثرگذاری بیشتر یک متغیر در تدوین الگوی قدرت سایبری آجا و منفی بودن شاخص نهایی نشانه اثرپذیری بیشتر یا همان وابستگی آن متغیر در تدوین الگوی قدرت سایبری آجا است.

جدول ۷: رتبه‌بندی میزان اثرگذاری و وابستگی متغیرهای اصلی

در تدوین الگوی قدرت سایبری آجا

ردیف	متغیر	اثرگذاری	وابستگی	شاخص نهایی
۱	فرامین و رهنمودها	۴۷	۵۱	-۴
۲	اسناد بالادستی	۴۹	۴۱	+۸
۳	ماهیت	۴۹	۵۳	-۴
۴	کارکرد	۴۸	۴۹	-۱
۵	ویژگی	۴۸	۴۶	+۲
۶	فرصت	۴۸	۴۸	۰
۷	تهدید	۴۷	۴۹	+۲
۸	قوت	۴۹	۴۱	+۸
۹	ضعف	۴۵	۴۴	+۱
۱۰	بلندمدت	۴۸	۴۹	-۱
۱۱	میان‌مدت	۴۸	۵۳	-۵
۱۲	کوتاه‌مدت	۴۵	۵۲	-۷
۱۳	حمله سایبری	۴۹	۵۱	-۳
۱۴	دفاع سایبری	۴۷	۴۷	۰
۱۵	تاب‌آوری سایبری	۴۸	۴۷	+۱
۱۶	محیط‌شناسی	۴۸	۵۰	-۲
۱۷	پشتیبانی اطلاعات	۴۸	۴۶	+۲
۱۸	تهدیدشناسی	۴۹	۴۳	+۶
۱۹	نرم‌افزار	۴۹	۴۹	۰
۲۰	سخت‌افزار	۴۸	۴۸	۰
	مجموع	۹۵۷	۹۵۷	{ +۸ ..... -۷ }

متغیرهای اسناد بالادستی و قوت بیشترین اثرگذاری را در بحث تدوین الگوی دفاع سایبری آجا دارند و پیشران اصلی در موضوع مورد پژوهش به شمار می‌آیند. پس از آن‌ها تهدیدشناسی قرار گرفته است. در بخش متغیرهایی نهایی، یعنی متغیرهای وابسته و اثرپذیر، اهداف کوتاه‌مدت به‌عنوان اثرپذیرترین عامل، شناسایی شده و پس از آن، ماهیت، فرامین و رهنمودها و اهداف میان‌مدت قرار دارند.

٤. نتیجه‌گیری

براساس مطالعات انجام شده در این تحقیق بسیاری از کشورها در صدد دستیابی به قدرت سایبری است و شناسایی فضای سایبری و استفاده از ابزارها، فرایندها و غیره نیازمند پیاده‌سازی یک الگوی مدوّن در ارتش جمهوری اسلامی ایران است. اگرچه وجود الگو به تنهایی برای رسیدن به این قدرت در ارتش جمهوری اسلامی کافی نیست ولی برای هماهنگ کردن ابزارها و فعالیت‌ها در راستای اسناد راهبردی مرتبط با آمادگی رزمی الکترونیکی آجا لازم است. علاوه بر این تهدیدها از نظر تنوع و پیچیدگی به‌طور مستمر هم از نظر زمانی و هم از نظر نوع و شدت گسترش در حال تغییر و توسعه هستند که این خود نیازمند بررسی عوامل محیطی و مطالعه و رصد دائم تهدیدها و به‌تبع آن، ارائه الگوی قدرت سایبری ارتش جمهوری اسلامی ایران است.

ازاین‌رو الگوی مورد بحث باید پویایی و تناسب در به‌کارگیری ابزارهای تهدید شناسی و مقابله–مدیریت در این فضا را دارا باشد. بنابراین نتایج این تحقیق را می‌توان در پاسخ به سؤال‌های زیر ارائه نمود:

سؤال اول: ارکان جهت‌ساز قدرت سایبری ارتش جمهوری اسلامی ایران کدامند؟

همان‌گونه که در ادبیات این تحقیق به نقل از هلیلی (۱۳۹۷) تعریف و تقسیم‌بندی برای ارکان جهت‌ساز شامل اسناد بالادستی، راهبردها و اهداف است. البته بنا به مطالعات انجام شده و افتراق بین مفاهیم مجازی و سایبری و غیره مفاهیم نیز بخشی از این ارکان جهت ساز پیشنهاد شده است که در ادامه تحقیق مفاهیم نیز به تائید جامعه آماری و صاحب‌نظران

رسید. برای دستیابی به این مهم، از روش استقرایی مؤلفه‌هایی که دارای یک مفاهیم مشترک و مشابه بودند در ذیل یک طبقه قرار داده و سازمان‌دِهی شدند، سپس نسبت به نام‌گذاری هر یک از طبقات (ابعاد) اقدام شد. بنابراین بر اساس این فرایند به شرح جدول ذیل استخراج شد. همان‌گونه که در ادبیات این تحقیق بیان شد به نقل از حسن بیگی (۱۳۹۱) اهداف را به صورت‌های مختلف می‌توان تقسیم کرد که در این تحقیق اهداف برای برنامه‌ریزی در سطوح مختلف تقسیم‌بندی اهداف بر حسب زمان (بلندمدت (راهبردی)، میان‌مدت (عملیاتی) و کوتاه‌مدت (اجرائی) تقسیم‌بندی شده است.

جدول ۸: ارکان جهت‌ساز قدرت سایبری آجا

ارکان جهت‌ساز										
اهداف			راهبردها				مفاهیم		سیاست‌ها	
کوتاه‌مدت	میان‌مدت	بلندمدت	ضعف	قوت	تهدید	فرصت	ویژگی	کارکرد	ماهیت	اسناد بالادستی	فرامین و رهنمودها

سؤال دوم: ابعاد قدرت سایبری ارتش جمهوری اسلامی ایران کدامند؟

تجزیه‌وتحلیل کیفی داده‌ها و منابع مطالعه شده ابعاد زیر از شناسایی گردید و برای تعیین ابعاد قدرت سایبری از جهت وجوه تشابه و تفاوت باهم مقایسه شدند سپس شاخص‌هایی که حول یک محور مشترک قرار داشتند و می‌توانستند اجزای تشکیل‌دهنده یک بُعد باشند، در یک طبقه سازمان‌دهی شدند، سپس نسبت به نام‌گذاری هریک از ابعاد قدرت سایبری اقدام شد. بنابراین بر اساس این فرایند ابعاد به شرح جدول ذیل استخراج شد.

جدول ۹: ابعاد قدرت سایبری آجا

ابعاد قدرت سایبری ارتش جمهوری اسلامی ایران							
زیرساختی		اطلاعاتی			عملیاتی		
سخت‌افزار	نرم‌افزار	تهدیدشناسی	پشتیبانی اطلاعاتی	محیط‌شناسی	تاب‌آوری سایبری	دفاع سایبری	حمله سایبری

سؤال سوم: روابط میان ابعاد قدرت سایبری ارتش جمهوری اسلامی ایران چگونه است؟

بخش سوم تحقیق برابر تعریف ارائه شده از الگو به نقل از مرادیان به محاسبه روابط بین عناصر (ابعاد) الگو می‌پردازد. برای دستیابی پاسخ به این هدف، با کمک نرم‌افزار میک‌مک و ارسال پرسش‌نامه به جامعه آماری یافته‌های به شرح زیر استخراج شد.

- ارکان جهت‌ساز قدرت سایبری ارتش جمهوری اسلامی ایران کدام است؟
- ابعاد الگوی قدرت سایبری ارتش جمهوری اسلامی ایران کدام است؟
- روابط بین ابعاد الگوی قدرت سایبری ارتش جمهوری اسلامی ایران چگونه است؟
- ارکان جهت ساز قدرت سایبری ارتش جمهوری اسلامی ایران کدام است؟

از نتایج آماری به‌دست‌آمده درباره سیاست‌ها دو فرامین و رهنمودها، قوانین و مقررات دارای میانگین بالاتر از ٤ هستند. در حوزه مفاهیم سه شاخص کارکردها، ماهیت و ویژگی‌ها با میانگین بالاتر از ٤ مورد تأیید پرسش‌شوندگان هستند.

نتایج کمی گویای این مطلب است که شاخص‌های ارائه شده برای قدرت سایبری ارتش جمهوری اسلامی ایران، از سطح متوسط به بالا مورد تأیید جامعه آماری است. در ضمن چون میانگین شاخص‌ها بالاتر از ٤ است، امکان بهره‌برداری از آن به میزان زیاد به بالا است.

نتایجی که از تجزیه‌وتحلیل کیفی و کمی برای نیل به هدف احصای ارکان جهت‌ساز قدرت سایبری ارتش جمهوری اسلامی ایران حاصل شده است، حاکی از آن است که ۱۲ شاخص از شاخص‌های بررسی شده با میانگین بالاتر از ٤ برای ارکان جهت‌ساز قدرت سایبری در اولویت هستند و می‌توانند مد نظر قرار گیرند ترتیب اولویت این شاخص‌ها براساس نظر گروه پرسش‌شوندگان و میانگین شاخص‌ها به شرح جدول است:

جدول شماره ۱۰: شاخص‌های مناسب برای ارکان جهت‌ساز قدرت سایبری آجا

شاخص‌های مناسب برای ارکان جهت ساز قدرت سایبری آجا			
اولویت	**شاخص**		**میانگین**
۱	سیاست‌ها	فرامین و رهنمودها	۴,۴۲
۲		اسناد بالادستی	۴,۳۹
۳	مفاهیم	ماهیت	۴,۳۳
۴		کارکرد	۴,۳۲
۵		ویژگی	۴,۳۲
۶	راهبردها	فرصت	۴,۲۸
۷		تهدید	۴,۲۵
۸		قوت	۴,۲۵
۹		ضعف	۴,۲۴
۱۰	اهداف	بلندمدت	۴,۱۹
۱۱		کوتاه‌مدت	۴,۱۳
۱۲		میان‌مدت	۴,۰۶

جدول ۱۱: اولویت‌بندی ابعاد، مؤلفه قدرت سایبری آجا

مفهوم	ابعاد	مؤلفه‌ها	امتیاز آزمون میانگین	اولویت
الگوی قدرت سایبری آجا	عملیات قدرت سایبری	حمله سایبری	۴,۲۵	۱
		دفاع سایبری	۴,۲۵	۲
		تاب‌آوری سایبری	۴,۲۴	۳
		محیط‌شناسی	۴,۱۹	۴

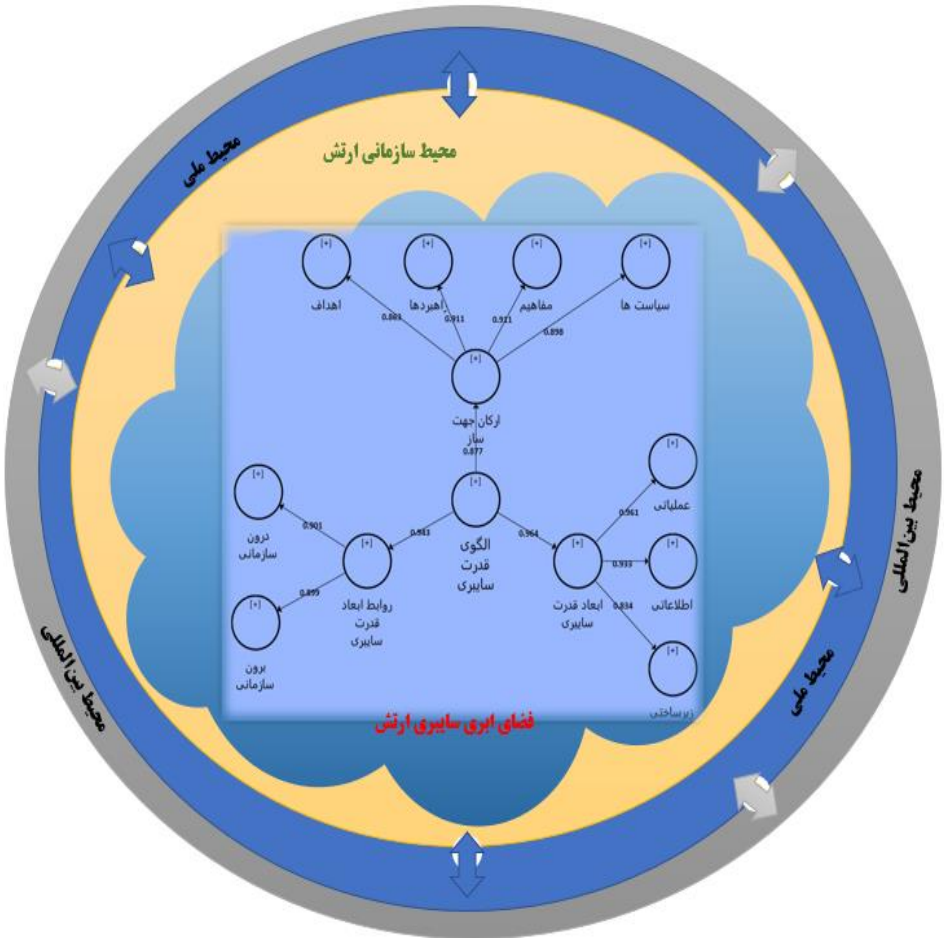
مفهوم	ابعاد	مؤلفه‌ها	امتیاز آزمون میانگین	اولویت
	اطلاعات قدرت سایبری	پشتیبانی اطلاعات	۴,۱۳	۵
		تهدیدشناسی	۴,۰۶	۶
	زیرساخت قدرت سایبری	سخت‌افزار	۴,۰۳	۷
		نرم‌افزار	۴,۰۳	۸

پاسخ به سؤال سوم

روابط بین ابعاد الگوی قدرت سایبری ارتش جمهوری اسلامی ایران چگونه است؟

با توجه به توضیحات پیشین در زمینه چگونگی احصای ابعاد و مؤلفه‌ها، در ادامه به‌منظور بررسی ارتباط بین آن‌ها، تأیید متغیرهای شناسایی‌شده و همچنین تأثیری که بر قدرت سایبری ارتش جمهوری اسلامی ایران دارند، پس از احصای ابعاد، مؤلفه‌ها و شاخص‌ها با استفاده از روش کیفی فراترکیب و تحلیل مضمون، پرسش‌نامه‌ای طراحی و در اختیار ۷۵ نفر از صاحب‌نظران، خبرگان و کارشناسان سایبری در آجا قرار گرفت که پس از تجزیه‌وتحلیل انجام شده برابر فصل قبل (چهارم) و انجام مصاحبه‌ای عمیق به‌منظور اعتبار سنجی نتایج، ارتباط بین ابعاد، مؤلفه‌ها و شاخص‌ها ارائه گردید، همچنین لازم به ذکر است در الگوی ارائه‌شده، از مؤلفه‌ها و شاخص‌هایی استفاده شده است که از اولویت بالاتری نسبت به دیگر ابعاد برخوردار بوده است. تحلیل حاصل از روابط ابعاد قدرت سایبری که ارتباط میان ابعاد عملیاتی، اطلاعاتی و زیرساختی با متغیرهای درون و برون‌سازمانی شامل درون سازمانی: معاونت عملیات، اطلاعات، فاوا و قرارگاه جنگ‌های نوپدید و برون‌سازمانی: وزارت دفاع و پشتیبانی ن.م وزارت اطلاعات وزارت فناوری اطلاعات و ارتباطات و شورای فضای مجازی همگی وجود داشته و از تأثیر بالا و بسیار بالا برخوردار هستند.

در نهایت با توجه به موارد بالا الگوی قدرت سایبری آجا که پاسخ به سؤال اصلی تحقیق است به‌صورت شکل (٤)، به دست می‌آید.



شکل ٤: الگوی قدرت سایبری ارتش جمهوری اسلامی ایران

فهرست منابع

- احمدی، سیروس (۱۳۹۹). ***نبرد سایبری کالبدشکافی امنیت جهانی***، چاپ اول، تهران، انتشارات دافوس.
- آذر، داود؛ ملکی، علیرضا (۱۳۹۸). ***جنگ سایبر و راه‌های مقابله با حملات سایبری***، تهران، انتشارات دافوس.
- اکبری، حمید و همکاران (۱۳۹۸). ***آگاهی وضعیتی حملات منع خدمت توزیع شده بر اساس پیش‌بینی (تجسم آینده نزدیک) صحنه نبرد مبتنی بر نظریه شواهد دمپستر- شافر و بیزین***، نشریه علمی پدافند الکترونیکی و سایبری، ۷(۱)، ۷۷-۹٤
- داداش‌تبار احمدی، کوروش و همکاران (۱۳۹۳). ***ارائه یک معماری جدید برای تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا در فرماندهی و کنترل سایبری***، مجله پدافند الکترونیکی و سایبری، ۲(۱)، ۱-۱٤
- ربیعی، بهزاد و همکاران (۱۳۹۹). ***معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج.ا. ایران***، فصلنامه علمی راهبرد دفاعی، سال هجدهم، شماره ٦۹.
- رشیدی، علی جبار (۱۳۹٦). ***آگاهی وضعیتی سایبری***، چاپ اول، تهران، انتشارات دانشگاه صنعتی مالک‌اشتر.
- زابلی زاده، اردشیر (۱۳۹۷). ***قدرت بازدارندگی در فضای سایبر***، دوفصلنامه علمی - پژوهشی رسانه و فرهنگ، ۸(۱)، ٤۷-۷٤
- سجادی اصیل وحید؛ آذر، داود (۱۳۹۹). ***عملیات سایبری در طرح‌ها و برنامه‌های وزارت دفاع آمریکا***، تهران، انتشارات دافوس آجا.
- شوشیان، کیانوش و همکاران (۱۳۹۹). ***مدل‌سازی حملات سایبری مبهم مبتنی بر فن جایگزین حمله***، نشریه علمی پدافند الکترونیکی و سایبری، ۸(۱) ۱، ٦۷-۷۷
- مسلمی، حسین و همکاران (۱۳۹٤). ***چگونگی ارتقای استفاده مطلوب آجا از فضای سایبر در پشتیبانی از مأموریت‌های مصرحه***، گروه مطالعاتی شماره ٦، دافوس آجا.
- نصرت‌آبادی، جمشید و همکاران (۱۳۹۷). ***ارائه الگوی ارزیابی قدرت سایبری ارتش جمهوری اسلامی ایران***، فصلنامه علمی- پژوهشی امنیت ملی، دانشگاه عالی دفاع ملی،۸(۲)، ۱۷۳-۱۹۸
- حکم مقام معظم رهبری در تشکیل شورای عالی فضای مجازی کشور دوره دوم سال ۹٤

- سند جامع سایبری نیروهای مسلح، تدوین‌کننده معاونت علوم تحقیقات و فناوری ستاد کل نیروهای مسلح، اداره علوم سایبری و هوش مصنوعی، اسفندماه ۱۳۹
- سند راهبردی پدافند سایبری کشور (۱۳۹٤). سازمان پدافند غیرعامل کشور و مرکز پدافند سایبری کشور.
- قانون ارتش جمهوری اسلامی ایران (۱۳٦٦). مجلس شورای اسلامی، شماره انتشار ۱۲٤٤۱، تاریخ تصویب ۱۳٦٦/۰۷/۰۱
- هلیلی، خداداد و همکاران (۱۳۹۷). ***قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر***، فصلنامه امنیت ملی، سال هشتم، شماره بیست و نهم، پاییز ۱۳۹۷.

References

- Andress, Jason, Winterfeild, Steve (2011). Cyber warfare Teechniques. Tactics and Tools for Security practitioners. USA.
- Ankang, Ju, Guo and others (2019). Research Article. HeteMSD: A Big Data Analytics Framework forTargeted Cyber-Attacks Detection Using Heterogeneous Multisource Data. Zhengzhou Institute of Information Science and Technology.China.
- Department of Army, (2017). FM 3-12, Cyberspace And Electronic Warfare Operations, Washington
- DOD (2018). JP 3-12, Cyberspace Operations
- Liivoja, Rain, Väljataga, Ann (2021). Autonomous Cyber Capabilities under International Law, NATO CCDCOE Publications
- Nye, Joseph S (2010). Cyber Power (The future of power in the 21th century). MIT-Harvard Minerva Project, Harvard Kennedy School.
- Olofintuyi, Sunday Samuel (2021). Cyber Situation Awareness Perception Model for Computer Network, (IJACSA) International Journal of Advanced Computer Science and Applications. Vol. 12, No. 1.
- Ph Stoecklin, Marc and others (2018). DeepLocker: How AI Can Power a Stealthy New Breed of Malware <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/>.
- Ross, Ron, and others (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. Draft NIST Special Publication800.Volume 2.
- Tadda. G, and others, (2006). Realizing situation awareness in a cyberenvironment, Proceedings of SPIE, Defense and Security Symposium, vol.
- Trusilo, Daniel and Burri, Thomas (2021). Ethical Artificial Intelligence: An Approach to Evaluating Disembodied Autonomous Systems. Autonomous Cyber Capabilities under International Law. Chapter 4. by NATO CCDCOE Publications.
- U.S.AIR FORCE, (2011). DOCTRINE PUBLICATION (AFDP) 3-12 CYBERSPACE OPERATIONS
- Zac, Rogers (2021). the promise of strategic Gain in the Digital Information Age. THE CYBER DEFENSE REVIEW. Army Cyber Institute. Vol 6. No.1.