فصلنامه امنیت ملی
سال نهم، شماره ۳۱، بهار ۱۳۹۸
مقاله هفتم از صفحه ۱۷۳ الی ۱۹۸

ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران[۱]

جمشید نصرت‌آبادی[۲]
حمیدرضا لشکریان[۳]
محمد مردانی شهربابک[۴]
محمدرضا موحدی صفت[۵]

تاریخ دریافت: ۱۳۹۷/۱۰/۱۸ تاریخ پذیرش: ۱۳۹۷/۱۲/۲۱

چکیده:
با توجه به موقعیت راهبردی جمهوری اسلامی ایران و گسترش سلطه‌طلبی ابرقدرت‌ها، ارزیابی قدرت سایبری باعث بهبود قدرت گردیده و دستیابی به قدرت سایبری مطلوب در نیروهای مسلح را تسریع می‌نماید؛ بنابراین فقدان یک الگوی ارزیابی راهبردی، به‌منظور سنجش قدرت سایبری، می‌تواند نیروهای مسلح را در سطوح تصمیم‌گیری دچار چالش نماید. در همین راستا هدف این تحقیق دستیابی به الگوی راهبردی سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران است.
این پژوهش با استناد به منابع کتابخانه‌ای و پژوهش‌های میدانی به دنبال پاسخ به این سؤال است که مهم‌ترین متغیرها و شاخص‌های شکل‌دهنده به الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران کدام است؟ بر این اساس، ابتدا در بخش مطالعات کتابخانه‌ای و با مراجعه به منابع معتبر، مهم‌ترین شاخص‌ها و متغیرهای مؤثر بر ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران استخراج گردید و با توجه به ماهیت و نقش آن‌ها و همچنین طی مصاحبه‌ای عمیق با نخبگان سایبری، این متغیرها در ابعاد آفند، پدافند و تاب‌آوری سایبری طبقه‌بندی گردیدند. در ادامه پرسشنامه‌ای طراحی و در اختیار صاحب‌نظران، خبرگان و کارشناسان سایبری قرار گرفت. بر اساس تجزیه‌وتحلیل پرسشنامه‌ها، مهم‌ترین متغیرها و شاخص‌های ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران احصاء گردید. درنهایت با توجه به یافته‌های کتابخانه‌ای و میدانی و همچنین تجزیه‌وتحلیل‌های صورت پذیرفته، الگوی مفهومی پیشنهادی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران پس از تأیید نهایی نخبگان سایبری، در قالب سه بعد، یازده مؤلفه و پنجاه‌وپنج شاخص ارائه گردید.

کلیدواژه‌ها: الگوی ارزیابی، فضای سایبری، قدرت سایبری، نیروهای مسلح جمهوری اسلامی ایران

۱- مقاله علمی- پژوهشی برگرفته از رساله دکتری می‌باشد.

۲- دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول)
nosratabadi110@chmail.ir
۳- استادیار دانشگاه امام حسین (ع)- Dr.lashkarian@chmail.ir
۴ - استادیار دانشگاه امام حسین (ع)- Mardani_dr@yahoo.com
۵- استادیار دانشگاه عالی دفاع ملی- Movahedi@snd.ac.ir

مقدمه:

قدرت در جهان امروزی معنای گذشته خود را از دست داده است و این تغییر مفهوم از قدرت به دلیل رشد سریع فضای سایبر و ایجاد زمینه‌های جدید و مهم در سیاست است. امروزه توانایی نفوذ در فضای سایبر به‌عنوان یکی از مهم‌ترین منابع قدرت در قرن ۲۱ محسوب می‌شود، لذا بازیگران دولتی و غیردولتی برای دست یافتن به اهداف نظامی، ایدئولوژی و اجتماعی فضای سایبر یا فضای فیزیکی از این فضاء استفاده می‌کنند (*Kristin, 2011,20*).

ویژگی‌های حوزه سایبری همچون گمنامی و نامتقارن بودن موجب شده، بسیاری از کشورها در عصر کنونی بر قدرت سایبری تمرکز کنند، به‌خصوص اینکه بازیگران کوچک‌تر در فضای سایبر نسبت به حوزه‌های سنتی، ظرفیت و توان بیشتری برای اعمال قدرت سخت و نرم دارند و برخی از اختلافات قدرت بین بازیگران را کاهش داده و نمونه مناسبی از پراکندگی قدرت که ویژگی سیاست جهانی در قرن حاضر به شمار می‌آید را به نمایش می‌گذارند. این موضوع موجب می‌شود، قدرت‌های بزرگ در عرصه سایبری هیچ‌گاه نتوانند به‌اندازه حوزه‌هایی چون دریا و خشکی مسلط شده و قدرت‌نمایی کنند (*joseph nye, 2010*).

در همین راستا تحولات سریع و عمیق ناشی از توسعه فضای سایبر در حوزه‌های مختلف، ازجمله حوزه‌های نظامی و دفاعی، باعث شده که ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران به‌عنوان یکی از موضوعات مهم در زمینه ارتقاء بهره‌وری نیروهای مسلح مطرح گردد. در این تحقیق، با بررسی رویکردهای تک متغیره و ترکیبی و همچنین مدل‌های مختلف ارزیابی قدرت، درنهایت یک الگوی راهبردی برای ارزیابی قدرت سایبری نیروهای مسلح مورد توجه قرار گرفته است.

ضعف سیستم‌های ارزیابی و نظام کسب بازخورد، امکان تبادل اطلاعات لازم را برای رشد، توسعه و بهبود فعالیت‌های یک سازمان غیرممکن کرده و زمینه‌های بروز بحران‌های مدیریتی را در آن‌ها افزایش می‌دهد و تداوم آن انحلال و شکست سازمان‌ها را به دنبال دارد. مراکز سایبری در ساختار نظامی – راهبردی نیروهای مسلح یک سازمان مهم به‌حساب می‌آیند و نتایج عملکرد آن نقش حیاتی در عملکرد و کارآمدی نیروهای مسلح خواهد داشت. از این رو پایش عملکرد آن‌ها بر اساس الگوهای نوین ارزیابی، یکی از وظایف مهم فرماندهان عالی نیروهای مسلح به‌حساب می‌آید. از طرفی با وجود تشکیل قرارگاه و فرماندهی‌های سایبری مختلف در نیروهای مسلح و سازمان‌های تابعه و گسترش روزافزون آن در همه ابعاد، هیچ‌گونه نظام و الگوی ارزیابی جامعی

به‌منظور سنجش قدرت سایبری نیروهای مسلح وجود ندارد و لازم است معیارها و ابزارهای دقیقی برای ارزیابی و قضاوت در خصوص اثربخشی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران طراحی گردد؛ بنابراین مسئله اصلی مقاله پیش رو، عدم وجود یک الگوی راهبردی ارزیابی به‌منظور سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران می‌باشد.

اهمیت و ضرورت تحقیق:

ارزیابی قدرت سایبری نیروهای مسلح موجب ارتقاء اثربخشی در حوزه سایبری نیروهای مسلح و همچنین محیط‌های عملیاتی دیگر می‌گردد که دستاوردها و مزایای عمده حاصل از انجام این پژوهش را می‌توان به‌صورت خلاصه در موارد زیر دانست:

با ارزیابی‌های راهبردی می‌توان تأثیرات تحولات محیطی بر نیروهای مسلح در حوزه سایبری را شناسایی و کنترل کرد.

دستیابی به یک الگوی علمی- راهبردی برای ارزیابی قدرت سایبری در سطح نیروهای مسلح، می‌تواند بهره‌وری سازمانی را ارتقاء دهد.

طراحی الگوی ارزیابی با استفاده از روش علمی دقیق، می‌تواند باعث جلوگیری از اعمال سلایق شخصی و تصمیمات غیر کارشناسی در این حوزه گردد.

هدف اصلی؛ دستیابی به الگوی راهبردی سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران بوده و سؤال اصلی مقاله نیز الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران کدام است؟ می‌باشد.

پیشینه تحقیق: با توجه به موضوع تحقیق، بررسی‌های مختلفی بر روی پژوهش‌های علمی و مرتبط با موضوع صورت پذیرفت که در زیر به برخی از مهم‌ترین موضوعات که در مؤلفه‌ها و متغیرهایی با موضوع تحقیق مشترک هستند؛ اشاره شده است.

یک پروژه تحقیقاتی مشترک با عنوان «چارچوب ارزیابی راهبردهای امنیت سایبری ملی[1]» در مرکز خبرگی امنیت اطلاعات و شبکه اتحادیه اروپا انجام‌شده است. این تحقیق که در سال ۲۰۱۴ صورت پذیرفته است در واقع یک نقشه راه برای ارزیابی راهبردهای امنیتی ارائه می‌نماید و اهداف کلیدی که این تحقیق دنبال می‌کند، عبارت است از توسعه قابلیت‌ها و سیاست‌های دفاع سایبری،

1-An evaluation Framework for National Cyber Security Strategies

دست یافتن به تاب‌آوری سایبری، کاهش جرائم سایبری، حمایت از صنعت در امنیت سایبری و امن سازی زیرساخت‌های اطلاعات حیاتی (*Enisa,2014*).

رساله‌ای با عنوان قدرت و اشکال آن: سخت، نرم، هوشمند در اکتبر ۲۰۱۱ توسط ماتئو پالاور[1] در دانشکده روابط بین‌الملل دانشگاه اقتصاد و علوم سیاسی لندن، انجام شده است. در این رساله ابعاد و ویژگی‌های نوع خاصی از قدرت به نام قدرت هوشمند مورد بررسی قرار گرفته و در ادامه نظریات لیبرالیستی در مورد قدرت نیز بررسی شده است. در چارچوب نظری این رساله به استدلال در مورد اهمیت قدرت هوشمند به‌عنوان شکل جدید قدرت پرداخته شده است. نتایج رساله نشان می‌دهد اتحادیه اروپا در سال‌های گذشته به توسعه قابلیت‌های نظامی (ابزارهای قدرت سخت) توجه داشته است. درصورتی‌که ایالات‌متحده با توجه به درس‌هایی که از جنگ عراق و افغانستان گرفته رویکرد خود را بر روی ابزارهای قدرت نرم متمرکز نموده است. افزایش بودجه دفاعی آمریکا نیز متوجه حمایت از دیپلماسی و قدرت نرم بوده است (پالاور، ۲۰۱۱).

مقاله‌ای با عنوان «مدل ارزیابی سطح امنیت سیستم‌های اطلاعاتی مبتنی بر رویکرد منطقی»[2] در سال ۲۰۱۵ توسط کریسمیر سلیک[3] و همکاران انجام گردید. این مدل قادر است سطح بالایی از انعطاف‌پذیری و قابلیت اجرا را برای سیستم‌های مختلف اطلاعات و سازمان‌های کسب‌وکار فراهم آورد؛ دارای ارتقاء پذیری به‌روز با توجه به مسائل امنیتی فعلی و تهدیدات جدید بوده و این انطباق‌پذیری بالا، موجب توانمندی در ارزیابی همه جنبه‌های ممکن امنیت شبکه مانند مسائل مربوط به سخت‌افزار و نرم‌افزار، نفوذ انسانی، سیاست‌های امنیتی، طرح‌های بازسازی و استفاده از تئوری دامپستر- شفر[4] موجب امکان ارزیابی ترکیبی کیفی و کمی شده است.

مقاله‌ای تحت عنوان «بلوک‌های سازنده قدرت سایبر ملی» در مارس ۲۰۱۶ در دانشگاه بوستون ایالات‌متحده ارائه شده است. در این مقاله با تجزیه‌وتحلیل عناصر فضای سایبر به‌عنوان بخشی تأثیرگذار در امنیت ملی به بررسی عوامل مؤثر بر قدرت ملی در فضای سایبر و استخراج مؤلفه‌های قدرت سایبر ملی پرداخته شده است. ازآنجا که قدرت سایبری یک پدیده چندوجهی است با در نظر گرفتن لایه‌های مختلف برای آن، ضمن بررسی روابط مطرح‌شده در مورد قدرت

1-Matteo Pallaver
2-An ontology the information systems security level assessment model based on and evidential reasoning approach
3-Kresimir Solic
4-Dumpester-Shafe

سایبری، به ارائه روابطی برای بررسی عوامل مؤثر بر قدرت سایبری به‌عنوان راهی برای دستیابی به قدرت ملی در قالب قدرت سایبری قابل درک پرداخته شده است (*Jc jansen van vuuren, 2016*).

مبانی نظری:

فضای سایبری: روسیه و آمریکا به‌صورت مشترک فضای سایبر را یک رسانه الکترونیکی که از طریق آن اطلاعات تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می‌شوند؛ معرفی نموده‌اند (*K.F. Rauscher and V. Yaschenko, 2011*). چهار مؤلفه کلیدی برای فضای سایبری وجود دارد که آن را یکتا می‌سازد و برای پاسخگویی به بسیاری از پرسش‌های مرتبط با آن مهم هستند.

مؤلفه سیستمی: شامل جنبه‌های فنی، زیرساختی و معماری فضای سایبری است. این مؤلفه شامل سخت‌افزار و نرم‌افزارهای کاربردی است که کاربران برای ذخیره‌سازی، انتقال و پردازش اطلاعات در فضای سایبری به آن‌ها اتکاء دارند.

مؤلفه محتوا و کاربرد: به محتوا و اطلاعات ارجاع دارد که در فضای سایبری وجود داشته و ابزارهایی که برای دستیابی و پردازش این اطلاعات مور داستفاده قرار می‌گیرد. مؤلفه محتوا و کاربرد به مؤلفه سیستمی اتکاء دارد و کاربردها را در راستای مدیریت و اشتراک اطلاعات برای کاربران فراهم می‌کند.

مؤلفه انسانی و اجتماعی: به ارتباطات و تعامل‌ها بین انسان‌ها در فضای سایبری و به اطلاعاتی که به اشتراک می‌گذارند، ارجاع دارد. دو مؤلفه قبلی امکان رشد مؤلفه انسانی و اجتماعی را با تسهیل ایجاد انجمن‌ها در فضای سایبری برای دسترسی و اشتراک اطلاعات مابین کاربران را فراهم نمودند.

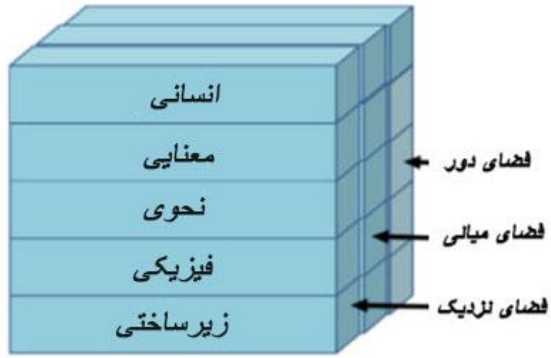
مؤلفه حاکمیتی: همه مؤلفه‌های قبلی فضای سایبری را تحت تأثیر قرار می‌دهد. این مؤلفه مشخصات فناوری (مؤلفه سیستمی)، استانداردسازی برای قالب‌بندی و تبادل داده‌ها (مؤلفه محتوایی و کاربردی) و چارچوب‌های قانونی کشورها برای کاربران فضای سایبری (مؤلفه انسانی و اجتماعی) را تحت تأثیر قرار می‌دهد (*Shaw, 2010:5*).

قدرت سایبری: «جوزف. اس. نای»[1]، استاد برجسته دانشگاه هاروارد آمریکا در مقاله‌ای که در سایت مرکز علوم و امور بین‌الملل بلفر- دانشکده کندی دانشگاه هاروارد- منتشر نموده به تبیین

1-Josehf. S. nye

قدرت سایبری در جهان امروز می‌پردازد و دراین‌باره می‌نویسد: قدرت در جهان امروزی معنای گذشته خود را از دست داده است و این تغییر مفهوم از قدرت به دلیل رشد سریع فضای سایبر و ایجاد زمینه‌های جدید و مهم در سیاست است (*Nye, 2010*). برخی کشورها همچنین ممکن است قدرت سایبری را به‌عنوان یک ابزار مؤثر علیه رقباء دنبال کنند. قدرت سایبر به‌عنوان ابزار راهبردی، جذاب و برترساز است، زیرا می‌تواند در هماهنگی با سایر ابزارها به‌تنهایی مورد استفاده قرار گیرد (فرانکلین، ۱۳۹۳). قدرت سایبری توانایی تولید یک نیروی سایبری ماهر، باکیفیت، یکپارچه، پاسخگو و معتبر، توان بالقوه برای اثربخشی سایبری را ایجاد می‌کند. با این وجود، چنین اثری بستگی به این دارد که چگونه این نیروها مورد استفاده قرار گیرند. ابزارهایی که کشورها با توسعه فنی، استفاده تاکتیکی، زمینه عملیاتی و فرماندهی راهبردی به‌عنوان متغیرهای اصلی مداخله‌گر در سراسر چارچوب ارزیابی، رویکردشان را با آن سازمان‌دهی می‌کنند. این درنهایت یک دولت را در وضعیت ایجاد قدرت سایبری قرار می‌دهد (*Jake bebber, 2017*).

ارتباط لایه‌های فضای سایبری با قدرت سایبری: تقسیم فضای سایبری به فضای نزدیک، فضای میانی و فضای دور، فرصتی برای حفظ آگاهی وضعیت سایبری و توانایی مقابله در برابر حملات سایبری ارائه می‌دهد. همچنین از طریق پیش‌بینی، جذب، سازگاری و بازیابی از حملات، به تاب‌آوری به عنوان عامل مهم در ایجاد قدرت سایبری کمک می‌کند. ترکیب آگاهی وضعیتی با ارزیابی لایه‌های مختلف فضای سایبری می‌تواند فهم فضای سایبری و نحوه برنامه‌ریزی قدرت سایبری را بهبود بخشد. از آنجا که از فضای سایبر برای اعمال قدرت سخت از طریق تهدید و اجبار نیز استفاده می‌شود؛ اولویت‌بندی و تخصیص منابع برای بهره‌برداری از این فضاء نیز اهمیت زیادی دارد. شلدون فضای سایبر را در یک مدل سه‌بعدی برحسب سه لایه افقی و پنج لایه عمودی مطابق شکل زیر در نظر گرفته است: (*Sheldon, 2011*).



شکل ۱: مدل سه‌بعدی فضای سایبر (*Sheldon, 2011*)

جدول ۱: سه لایه افقی فضای سایبر (*Sheldon, 2011*)

لایه	توصیف
فضای نزدیک Near space	شبکه‌های محلی و سیستم‌هایی که برای پشتیبانی زیرساخت ملی حیاتی است و به‌صورت پیش‌فرض توسط مؤسسات دولتی یا ملی کنترل و محافظت می‌شوند.
فضای میانه Mid space	شبکه‌ها و سیستم‌های حیاتی برای دسترسی به فضای سایبر جهانی که کنترل یا محافظت محلی روی آن‌ها وجود ندارد. معمولاً این‌ها ممکن است از نظر جغرافیایی در فاصله دوری قرار گرفته باشند و متعلق به یک شرکت تجاری خارجی یا یک دولت سوم (شخص ثالث) باشند.
فضای دور Far space	شبکه‌ها و سیستم‌هایی که فضای نزدیک رقیب یا دشمن را تشکیل می‌دهند و باید به‌عنوان بخشی از صحنه نبرد به‌منظور طرح‌ریزی قدرت و نفوذ از طریق فضای سایبر کنترل‌شده یا تحت تأثیر قرار گیرند.

از نظر شلدون قدرت روی یکی از این لایه‌ها، قدرت روی همه را نتیجه نمی‌دهد. متغیرهای قابل سنجش در هر لایه، شاخص مهمی در اندازه‌گیری و مقایسه قدرت است و ضعف در هرکدام از این شاخص‌ها، نیازمند تمرکز برای بهبود عملکرد آن لایه است.

تهاجم سایبری و ویژگی‌های آن: حمله یا آفند سایبری، مجموعه اعمالی است که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات در شبکه‌های موجود در فضای سایبری انجام می‌شود. حملات سایبری با استفاده از مقیاس پیچیدگی بر اساس لایه‌های فضای مجازی،

اندازه‌گیری می‌شوند. پیچیدگی با توجه به شش ویژگی، تداوم، انتشار، نوآوری، دقت و صحت، ضربه مؤثر و انتساب دادن حملات اندازه‌گیری می‌شود.

تداوم: تداوم به جهت تلاشی که از سمت مهاجم صورت می‌پذیرد، ارزیابی می‌گردد. امتیاز یک حمله انکار ویروس که نیاز به ادامه فعالیت از طرف مهاجم دارد، کمتر از امتیاز یک ویروس است که نیازمند دخالت انسانی برای انتشار است. بر همین اساس، امتیاز یک ویروس کمتر از یک کرم خود تکرارکننده است که پس از تحویل اولیه، نیاز به هیچ تعامل سازنده‌ای ندارد.

انتشار: بر اساس تلاشی که برای رساندن بدافزار به هدف صورت می‌گیرد، اندازه‌گیری می‌شود. امتیاز یک حمله موفقیت‌آمیز بر روی یک سیستم که به اینترنت متصل نیست، بالاتر از یک سیستم است که به‌راحتی قابل دسترسی است.

نوآوری: به لحاظ منحصربه‌فرد بودن تکنیک مورداستفاده در حمله و میزان تلاش در توسعه آن سنجیده می‌شود. استفاده از بهره‌برداری‌های ناشناخته، نمره بالا را دریافت می‌کند.

دقت و صحت: به لحاظ دقت حمله در دستیابی به یک هدف خاص اندازه‌گیری می‌شود. حمله‌ای که روی یک هدف منحصربه‌فرد در زمان خاص تمرکز می‌کند، دارای امتیاز بالاتری نسبت به حملات گسترده و عمومی است.

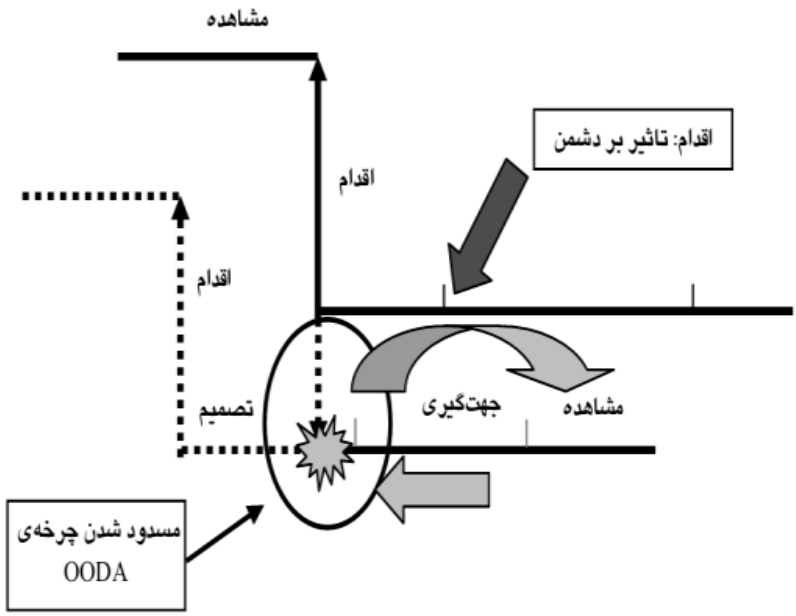
ضربه: ضربه به لحاظ اثربخشی حمله سنجیده می‌شود که بستگی به ارزش روان‌شناختی و تأثیر واقعی روی هدف دارد. ضربه همچنین می‌تواند برحسب اثر موقتی سنجیده شود. امتیازدهی تحت تأثیر محققان امنیت سایبری قرار می‌گیرد که جزییات حملاتی که به‌صورت عمومی منتشر نشده‌اند را شناسایی می‌کنند. ضربه بیشتر امتیاز بالاتری دارد.

انتساب (نسبت دادن): به لحاظ توانایی شناسایی منشأ حملات مورد ارزیابی قرار می‌گیرد. منشأ ممکن است ناشناسی کلی را دنبال کند یا ممکن است به گروه یا کشوری دیگر به‌منظور پنهان ماندن تحقیقات اشاره کند. ناشناسی بزرگ‌تر امتیاز بیشتری دارد (*Venables, 2015*).

آگاهی وضعیتی[1]: مزیت‌های اصلی شبکه محوری مانند سرعت، دقت و چابکی از راه‌های مختلفی می‌توانند فرآیند تصمیم سازی طرف مقابل را مختل سازند. یکی از این راه‌ها افزایش تعداد محرک‌ها در طول زمان است. هرچه تواتر و فراوانی محرک‌ها بیشتر باشد، احتمال اینکه آن‌ها در یک نقطه زمانی مناسب، بتوانند منجر به تأثیر مورد نظر بر فرآیند تصمیم‌سازی دشمن

1 -Situation Awareness

شوند، بیشتر می‌گردد؛ یعنی کوتاه کردن زمان کلی چرخه تولید محرک در فضای رزم، باعث چند برابر شدن تأثیر این محرک‌ها بر فرآیند تصمیم‌سازی دشمن در فاصله زمانی محدود می‌شود. در نتیجه احتمال مختل نمودن چرخه تصمیم‌گیری حریف توسط یکی از آن‌ها مطابق با شکل زیر افزایش می‌یابد.



شکل ۲: انسداد و اختلال حلقه بوید (قاسم‌زاده، ۱۳۹۲)

راه دیگر نفوذ به فرآیند تصمیم‌سازی دشمن با الزام استفاده از مزیت‌های شبکه محوری مانند خود هماهنگی و آگاهی وضعیتی، ایجاد هم‌زمان محرک‌ها در حجمی گسترده است. در این حالت تأثیر محرک‌های متعدد و هم‌زمان انسجام شناختی و روانی دشمن را بر هم می‌زند. در رویکرد تأثیر محور آگاهی وضعیتی جامع از شرایط فضای رزم دررسیدن به پیروزی بسیار حائز اهمیت است، اما ماهیت این آگاهی نزد همه بازیگران یکسان نیست (قاسم‌زاده، ۱۳۹۲).

تاب‌آوری در برابر حملات سایبری: در ره نگاشت راهبردی برای رویارویی با سه سناریوی محتمل سایبری در آینده باید به موضوعات راهبردی آمادگی نهادی، خط‌مشی سایبری، فهم جامعه و ساختار سیستماتیک ریسک‌های سایبری پرداخته شود. حرفه‌های سنتی امنیت سایبری رفته‌رفته

جای خود را به حرفه «تاب‌آوری سایبری» می‌دهند، زیرا بسیاری از سازمان‌های جهانی به این نتیجه رسیده‌اند که برخی حملات سایبری اجتناب‌ناپذیر هستند و به‌جای صرف زمان هنگفت برای حرفه‌های پیشگیرانه امنیت سایبری که در خصوص حملات سایبری اجتناب‌ناپذیر کمکی نمی‌کنند، می‌توان بر انعطاف‌پذیری سایبری سرمایه‌گذاری کرد. همکاری بخش‌های مختلف، گسترش ابزار حملات سایبری را محدود ساخته و منجر به ساخت قابلیت‌های نهادی شده است و همچنین به نوآوری انگیزه می‌بخشد (زواری، ۱۳۹۵).

مؤلفه‌های تاب‌آوری سایبری:

حس تشخیص: حس تشخیص، توانایی سازمان‌ها برای پیش‌بینی و تشخیص تهدیدات سایبری است. سازمان‌ها به استفاده از هوش تهدید سایبری و دفاع فعال برای پیش‌بینی تهدیدات یا حملات پیش رو نیاز دارند. قبل از موفق شدن حملات، آن‌ها به دانستن آنچه اتفاق می‌افتد، نیاز دارند و همچنین آن‌ها نیاز به تجزیه‌وتحلیل‌های پیچیده برای دستیابی زودهنگام به هشدارهای سایبری دارند.

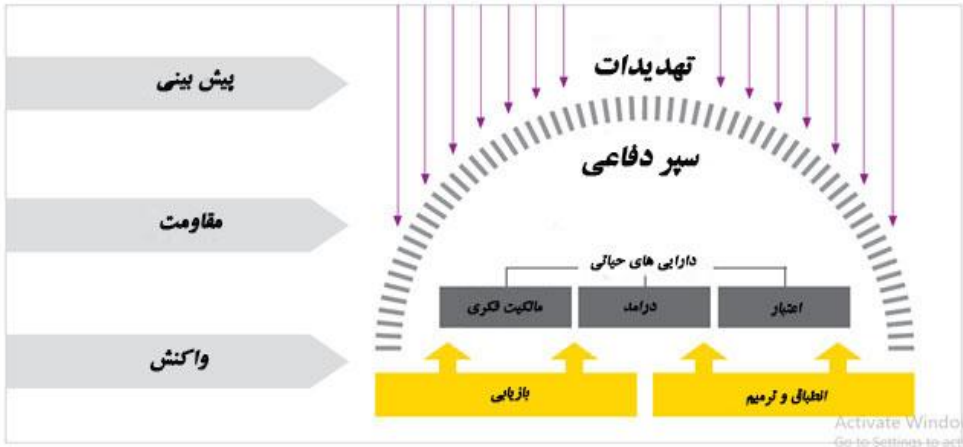
مقاومت: مکانیسم‌های مقاومت به‌طور اساسی سپری برای شرکت (سازمان) هستند که با مقداری ریسک در سازمان شروع می‌شود و سازمان سعی می‌کند آمادگی خود را با ایجاد سه لایه دفاعی دنبال نماید:

اولین لایه دفاعی: اجرای اقدامات کنترلی در عملیات روزمره

دومین لایه دفاعی: توسعه توابع نظارتی (کنترل‌های اینترنتی، بخش قانونی، مدیریت ریسک و امنیت سایبری)

سومین لایه دفاعی: استفاده قوی از بخش ممیزی داخلی

واکنش و ترمیم: اگر تشخیص با شکست مواجه شد (سازمان متوجه بروز تهدید نشد) و یک شکست در مقاومت به وجود آمد (اقدامات کنترلی به‌اندازه کافی قوی نبود) سازمان‌ها نیاز به آمادگی برای مقابله با اختلال، پاسخگویی به حوادث و مدیریت بحران دارند. آن‌ها همچنین نیاز به حفظ ادله دیجیتال (فارنزیک) برای بررسی رخنه سایبری دارند که اگر مهاجمین شناسایی شدند سازمان علیه آن‌ها ادعا نماید. در پایان آن‌ها همچنین نیاز به آمادگی برای برگرداندن سازمان به مأموریت‌های معمول در سریع‌ترین زمان ممکن دارند. یادگیری ازآنچه اتفاق افتاده است و سازگاری و سازمان‌دهی مجدد سازمان، کمک به بهبود تاب‌آوری است (*EY,2016*).



شکل ۳: اجزای تاب‌آوری در سازمان‌ها (*EY,2016*)

رویکردها و مدل‌های ارزیابی قدرت:

رویکردهای تک متغیره: در ارزیابی و سنجش قدرت، برخی اندیشمندان پس از بررسی عوامل مختلف بر روی یک عامل به‌عنوان ملاک و معیار اندازه‌گیری قدرت تأکید کرده و به‌وسیله آن به ارزیابی قدرت پرداخته‌اند. کسانی که فقط یک متغیر را در نظر گرفته‌اند؛ معمولاً متغیر انتخاب‌شده خود را نماینده قدرت ملی دانسته و سعی نکرده‌اند وانمود کنند که متغیر انتخابی آن‌ها در واقع، شاخص جامع قدرت ملی است. به‌طورکلی رویکردهای تک متغیره سنجش قدرت ملی را می‌توان به دودسته تقسیم کرد: دسته اول صاحب‌نظرانی که عوامل نظامی را مظهر قدرت ملی دانسته‌اند و گروه دوم افرادی که عوامل اقتصادی را مهم‌تر دانسته و آن‌ها را معیار ارزیابی قدرت ملی کشورها دانسته‌اند. بسیاری از تحلیلگرانی که خواهان ارزیابی توانمندی‌های ملی موجود هستند، توانمندی نظامی صرف را مظهر قدرت می‌دانند. دانشمندان علوم سیاسی مانند آینیس کلاد و کارل دیوچ، ازجمله این تحلیلگرانند. کسان دیگری مانند نورمن الکاک و آلن نیوکامب از هزینه‌های نظامی و برخی دیگر از نیروهای نظامی خاص استفاده کرده‌اند (*Tellis &Others ,2000*)

نقد رویکرد تک متغیره ارزیابی قدرت ملی: شاخص‌های رویکرد تک متغیری به دلیل سادگی و آسان بودن کار و یا در دسترس بودن آسان داده‌های آن‌ها رواج گسترده‌ای داشته است. افرادی که از چنین شاخص‌هایی طرفداری می‌کنند، معمولاً در مورد ارزش شاخص‌های چند متغیره

(ترکیبی) متقاعد نشده‌اند. با توجه به این دریافت، بسیاری از حامیان متغیرهای واحد ظاهراً از متغیرهایی که برای هدف موردنظر خود برگزیده‌اند، راضی هستند و کشورها را بر طبق توانایی ملی آن‌ها درجه‌بندی می‌کنند. مهم‌ترین نقدی که بر این نوع شاخص‌ها می‌توان وارد دانست، این است که این نوع شاخص‌های تک متغیری، نگرش محدودی به قدرت ملی کشورها دارند و نمی‌توانند بیانگر قدرت واقعی کشورها و جایگاه حقیقی آن‌ها در نظام ژئوپلیتیک جهانی باشند (*kadera,2004*).

رویکردها و مدل‌های چند متغیره (ترکیبی) محاسبه قدرت ملی: یکی دیگر از روش‌های محاسبه قدرت استفاده از چند متغیر و ترکیب آن‌ها و طراحی یک مدل چند متغیره است. طراحی مدل‌های ترکیبی (چند متغیره) توسط صاحب‌نظران به دو شکل متفاوت مدل‌های ریاضی و مدل‌های مفهومی صورت گرفته است. در شکل اول یعنی سنجش قدرت ملی کشورها بر اساس یک مدل ریاضی، ابتدا متغیرهای مورد نظر انتخاب می‌شود و سپس با طراحی یک مدل ریاضی نوع رابطه و ترکیب متغیرها مشخص می‌شود. درنهایت بر اساس این مدل ریاضی قدرت ملی کشورها مورد سنجش قرار می‌گیرد. به‌عنوان نمونه می‌توان به مدل‌هایی که توسط کلیفورد جرمن و فوکس طرح‌شده اشاره کرد. در نوع دوم یعنی مدل‌های مفهومی، چند متغیر به‌عنوان مهم‌ترین عوامل مؤثر بر قدرت ملی کشورها توسط طراح مدل انتخاب شده و سپس قدرت کشورها بر اساس امتیازات کسب شده در آن گروه از متغیرها مورد سنجش قرار می‌گیرد. البته در این روش فرمول خاصی که نشان‌دهنده نحوه ترکیب و نوع رابطه متغیرها باشد ارائه نمی‌شود (زرقانی، ۱۳۸۹).

ارزیابی قدرت سایبری بر اساس مؤلفه‌های آن: در جدیدترین کار انجام‌شده توسط جی وورن، مؤلفه‌های زیر برای قدرت سایبری در نظر گرفته‌شده است:

مؤلفه محیطی: مانند توزیع جغرافیایی جمعیت کاربران سایبری

مؤلفه اقتصادی: مانند فناوری‌های مربوط به دسترسی و توسعه زیرساخت ارتباطی، پشتیبانی و کارشناسان سایبری

مؤلفه نظامی: مانند ورود نیروهای نظامی به فضای سایبر و استفاده از قابلیت‌های آن برای حمله و دفاع سایبری

مؤلفه راهبردی: شامل راهبردهای سایبری به‌منظور پیشگیری از جرائم سایبری، امنیت سایبری و سامانه‌های آموزشی سایبر

مؤلفه شناختی: شامل اراده و درک سیاستمداران و تصمیم‌گیران در مواجهه با چالش‌های سایبری

بر این اساس وی رابطه زیر را برای ارزیابی قدرت سایبری ارائه داده است:

قدرت سایبری = {(مؤلفه محیطی+ مؤلفه اقتصادی+ مؤلفه نظامی)* (مؤلفه شناختی + مؤلفه راهبردی)} + رابطه متقابل مؤلفه‌های (محیطی، اقتصادی، نظامی)

کنار هم قرار گرفتن مؤلفه شناختی و راهبردی و ضریب قرار گرفتن آن‌ها در رابطه نشان‌دهنده اهمیت آن‌ها در محاسبه و ارزیابی قدرت سایبری است. از دیدگاه وی قدرت سایبری در محاسبه قدرت ملی به‌صورت زیر ضریب سایر مؤلفه‌ها قرار می‌گیرد:

قدرت ملی = {(جغرافیا+ جمعیت + منابع)+ مؤلفه اقتصادی+ مؤلفه نظامی + مؤلفه اطلاعاتی} * (مؤلفه سیاسی + مؤلفه روان‌شناختی) * قدرت سایبری. (*vuuren.2016*)

روش تحقیق:

این تحقیق با توجه به اینکه ابزار و راهنمایی برای سیاست‌گذاری در حوزه سایبری نیروهای مسلح جمهوری اسلامی ایران پیشنهاد می‌کند و امکان ارزیابی قدرت سایبری و در صورت نیاز بازنگری را فراهم می‌سازد، کاربردی است و با توجه به ارائه الگوی ارزیابی قدرت سایبری و توسعه دانش در این زمینه، توسعه‌ای هست؛ بنابراین این تحقیق با توجه به موضوع و هدف تحقیق، از نوع کاربردی- توسعه‌ای است. همچنین روش تحقیق به کار گرفته‌شده در این پژوهش، روش آمیخته (کیفی و کمی) است.

جامعه آماری تحقیق، حجم نمونه و روش نمونه‌گیری: جامعه آماری این تحقیق به دو دسته تقسیم گردید، دسته اول در مرحله نخست تحقیق (انجام مصاحبه) شامل تعداد ۱۰ نفر از خبرگان و صاحب‌نظران حوزه سایبری نیروهای مسلح می‌باشند و در مرحله دوم به‌منظور اعتبار سنجی اجزاء الگو (شاخص‌ها، مؤلفه‌ها و ابعاد الگو و تحلیل روابط بین آن‌ها) جامعه آماری را فرماندهان، خبرگان، متخصصان، اساتید و صاحب‌نظران سایبری نیروهای مسلح به تعداد ۶۵ نفر تشکیل دادند. جامعه خبرگی به‌منظور مصاحبه به تعداد ۱۰ نفر به کمک روش تمام شمار انتخاب شدند که در مرحله اول، حجم نمونه همان حجم جامعه است و در مرحله بعدی بر اساس جدول مورگان چنانچه حجم جامعه ۶۵ نفر در نظر گرفته شود، حجم نمونه نیز برابر با ۶۵ نفر خواهد بود. بر

همین اساس تعداد ۶۵ پرسشنامه برای جامعه نمونه ارسال گردید و تعداد ۳ عدد به دلایل نقصی که داشت کنار گذاشته شد و داده‌ها با تعداد ۶۲ پرسشنامه جمع‌آوری و تحلیل گردید.

ابزار گردآوری داده‌ها و روایی و پایایی آن‌ها: برای گردآوری داده‌ها در این رساله از دو روش کتابخانه‌ای و میدانی استفاده گردیده که در روش میدانی، ابزارهای مصاحبه و پرسشنامه به‌کار گرفته شده است. روایی منطقی پرسشنامه‌ها از دو جنبه روایی ظاهری و محتوایی به جهت روشن و بدون ابهام بودن گویه‌ها و همچنین کفایت کمیت و کیفیت آن‌ها توسط خبرگان و صاحب‌نظران و اساتید دانشگاه تأیید گردید. به‌منظور بررسی روایی شاخص‌های پرسشنامه ابتدا یک نمونه ۱۵ تایی بین جامعه هدف توزیع و جمع‌آوری گردید، پس از دسته‌بندی داده‌ها به کمک فن تحلیل عاملی، میزان روایی تک‌تک شاخص‌ها مورد بررسی قرار گرفت. در این فن چنانچه بار عاملی هر گویه کمتر از میزان ۰/۴ به دست آید نشان‌دهنده روایی پایین گویه است. همچنین برای محاسبه پایایی، از روش آلفای کرونباخ به شرح ذیل استفاده گردید:

جدول ۲: میزان آلفای کرونباخ حاصله

ردیف	پرسشنامه	میزان آلفای کرونباخ حاصله	رتبه پایایی
۱	قابلیت آفند سایبری	۰/۸۶۹	خیلی خوب
۲	قابلیت پدافند سایبری	۰/۹۲۳	عالی
۳	قابلیت تاب‌آوری سایبری	۰/۹۴۸	عالی

تجزیه‌وتحلیل:

ابتدا در بخش مطالعات کتابخانه‌ای و با مراجعه به منابع معتبر، مهم‌ترین شاخص‌ها و متغیرهای مؤثر بر ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران استخراج گردید و با توجه به ماهیت و نقش آن‌ها و همچنین طی مصاحبه‌ای عمیق با نخبگان سایبری، این متغیرها در ابعاد آفند، پدافند و تاب‌آوری سایبری طبقه‌بندی گردیدند. در ادامه پرسشنامه‌ای طراحی و در اختیار صاحب‌نظران، خبرگان و کارشناسان سایبری قرار گرفت. بر اساس تجزیه‌وتحلیل پرسشنامه‌ها، مهم‌ترین متغیرها و شاخص‌های ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران احصاء گردید. در همین راستا ابتدا به بررسی چگونگی توزیع داده‌های به دست آمده به کمک پرسشنامه، به جهت نرمال بودن یا غیر نرمال بودن پرداخته شد. سپس فرضیات مطرح شده مورد آزمون قرار گرفت که نتایج به شرح ادامه است:

نرمال بودن داده‌های مربوط به متغیرها

فرضیه: *H0*: توزیع داده‌های مربوط به متغیرهای (آفند سایبری، پدافند سایبری و تاب‌آوری سایبری) نرمال است.

H1: توزیع داده‌های مربوط به متغیرهای (آفند سایبری، پدافند سایبری و تاب‌آوری سایبری) نرمال نیست.

جدول ۳: آزمون کولموگروف- اسمرینوف

آزمون	متغیرها	میانگین	انحراف معیار	مقدار K-S محاسبه شده	سطح معناداری	نتیجه آزمون
کولموگروف- اسمرینوف	آگاهی وضعیتی	۴	.۳۶۸	.۲۱۰	/۰۰۰	نرمال نیست
	تسلیحات سایبری	۴,۶۲	.۲۹۹	.۱۸۲	/۰۰۰	نرمال نیست
	عامل انسانی	۴,۱۲	.۲۹۵	.۲۱۵	/۰۰۰	نرمال نیست
	پیچیدگی سایبری	۴,۰۶	.۲۹۵	.۲۱۲	/۰۰۰	نرمال نیست
	مصون‌سازی	۳,۹۲	.۴۴۱	.۲۱۱	/۰۰۰	نرمال نیست
	دیپلماسی سایبری	۳,۷۱	.۴۹۳	.۲۴۹	/۰۰۰	نرمال نیست
	حقوق سایبری	۴,۱۲	.۳۸۳	.۲۴۱	/۰۰۰	نرمال نیست
	پیش‌بینی	۴,۶۸	.۲۹۸	.۲۶۹	/۰۰۰	نرمال نیست
	مقاومت سایبری	۳,۸۶	.۴۴۰	.۲۰۱	/۰۰۰	نرمال نیست
	واکنش	۳,۹۶	.۳۹۲	.۱۶۳	/۰۰۰	نرمال نیست
	ترمیم	۳,۷۲	.۲۸۶	.۱۹۵	/۰۰۰	نرمال نیست
*P<0/05 ،**P<0/01 و N =۶۲						

جدول فوق، چون سطح معناداری برای همه متغیرها بیشتر از میزان خطای ۰۵/ به دست آمده فرضیه *H0* مورد تأیید است و این بدان معناست که توزیع داده‌ها نرمال نیست؛ بنابراین برای بررسی تأثیر متغیرها بر الگو که نرمال نیستند، از معادل آزمون *T* یک نمونه‌ای در آزمون‌های ناپارامتریک، یعنی آزمون توزیع دوجمله‌ای (*Binomeal*) استفاده می‌کنیم.

آزمون توزیع دوجمله‌ای ابعاد ارزیابی

فرضیه:

H0: ابعاد (آفند، پدافند و تاب‌آوری سایبری) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر ندارند.

H1: ابعاد (آفند، پدافند و تاب‌آوری سایبری) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر دارند.

جدول ۴: آزمون توزیع دوجمله‌ای ابعاد ارزیابی

آزمون	متغیرها	طبقات	حجم نمونه	درصد پاسخ مشاهده شده	سطح معناداری	نتیجه آزمون
توزیع دوجمله‌ای	آفند سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	پدافند سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	تاب‌آوری سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	**۶۲**	**۱۰۰**		
N =۶۲ و P<0/01، P<0/05***						

مطابق خروجی جدول، چون سطح معناداری (*sig*) برای کلیه متغیرها از میزان خطای ۰۵/ کمتر به دست آمده است می‌توان گفت فرضیه *H1* مورد تأیید واقع می‌گردد؛ بنابراین از نظر جامعه پاسخ‌دهنده ابعاد یاد شده با اطمینان ۹۵٪ بر الگو تأثیرگذار هستند.

آزمون توزیع دوجمله‌ای مؤلفه‌های آفند سایبری

فرضیه:

H0: مؤلفه‌های آفند سایبری (آگاهی وضعیتی، تسلیحات سایبری، عامل انسانی، پیچیدگی سایبری) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر ندارند.

H1: مؤلفه‌های آفند سایبری (آگاهی وضعیتی، تسلیحات سایبری، عامل انسانی، پیچیدگی سایبری) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر دارند.

جدول ۵: آزمون توزیع دوجمله‌ای مؤلفه‌های آفند سایبری

آزمون	متغیرها	طبقات	حجم نمونه	درصد پاسخ‌های مشاهده شده	سطح معناداری	نتیجه آزمون
توزیع دوجمله‌ای	آگاهی وضعیتی	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	تسلیحات سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	عامل انسانی	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	پیچیدگی سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
*P<0/05 ،**P<0/01 و N =۶۲						

آزمون توزیع دوجمله‌ای مؤلفه‌های پدافند سایبری

فرضیه:

H0: مؤلفه‌های پدافند سایبری (مصون‌سازی، دیپلماسی سایبری، حقوق سایبری) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر ندارند.

H1: مؤلفه‌های پدافند سایبری (مصون‌سازی دیپلماسی سایبری، حقوق سایبری) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر دارند.

جدول ۶: آزمون توزیع دوجمله‌ای مؤلفه‌های پدافند سایبری

آزمون	متغیرها	طبقات	حجم نمونه	درصد پاسخ‌های مشاهده شده	سطح معناداری	نتیجه آزمون
توزیع دوجمله‌ای	مصون‌سازی	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	دیپلماسی سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	حقوق سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
*P<0/05 ،**P<0/01 و N =۶۲						

آزمون توزیع دوجمله‌ای مؤلفه‌های تاب‌آوری سایبری

فرضیه:

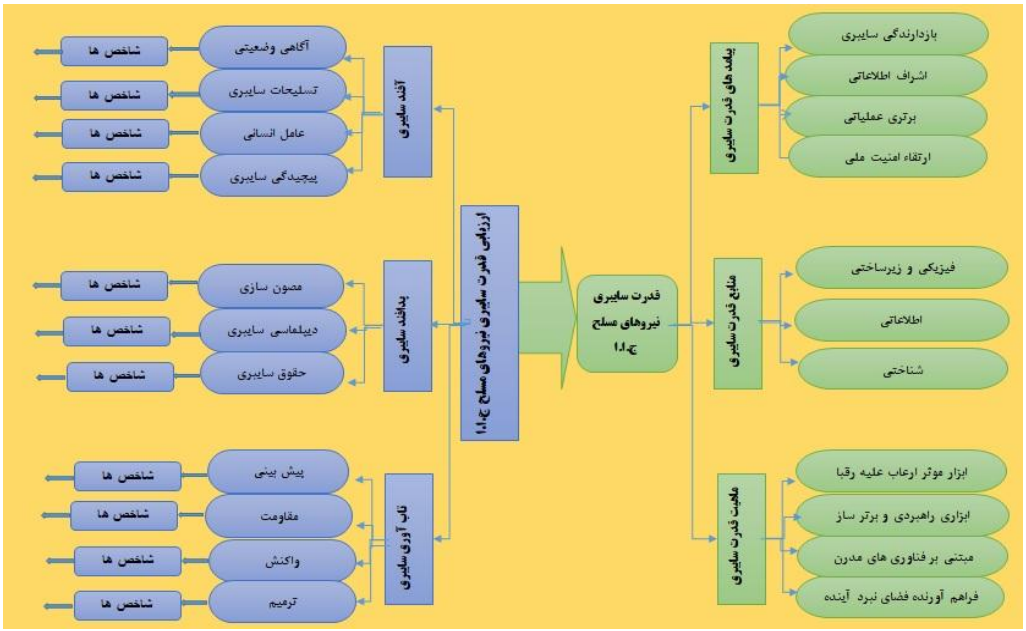
H0: مؤلفه‌های تاب‌آوری سایبری (پیش‌بینی، مقاومت سایبری، واکنش و ترمیم) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر ندارند.

H1: مؤلفه‌های تاب‌آوری سایبری (پیش‌بینی، مقاومت سایبری، واکنش و ترمیم) بر الگوی راهبردی ارزیابی قدرت سایبری تأثیر دارند.

جدول ۷: آزمون توزیع دوجمله‌ای مؤلفه‌های تاب‌آوری سایبری

آزمون	متغیرها	طبقات	حجم نمونه	درصد پاسخ‌های مشاهده شده	سطح معناداری	نتیجه آزمون
توزیع دوجمله‌ای	پیش‌بینی	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	مقاومت سایبری	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	واکنش	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
	ترمیم	<= 3	۰	۰	/۰۰۰	تأیید H1
		> 3	۶۲	۱۰۰		
*P<0/05 ،**P<0/01 و N =۶۲						

نتایج فوق بیانگر این است که همه متغیرهای احصایی بر الگوی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران تأثیر دارند. برای این منظور با مطالعه اسناد بالادستی، مبانی نظری و پیشینه تحقیق، متغیرهای مؤثر بر ارزیابی قدرت سایبری نیروهای مسلح در هر بخش احصاء و سپس توسط محقق در مؤلفه‌ها دسته‌بندی گردید که مؤلفه‌های تعیین شده با توجه به ادبیات تحقیق و مصاحبه انجام شده با صاحب‌نظران سایبری در نیروهای مسلح، در ابعاد آفند، پدافند و تاب‌آوری سایبری لحاظ گردیدند. همچنین منابع قدرت، ماهیت و پیامدهای آن، با مطالعات کتابخانه‌ای و میدانی برابر چارچوب مفهومی زیر شناسایی گردیدند.



شکل ۴: چارچوب مفهومی ارزیابی راهبردی قدرت سایبری

نتیجه‌گیری:

در طراحی الگوی راهبردی ارزیابی قدرت سایبری با توجه به پیچیدگی موضوع، پس از تعیین مهم‌ترین متغیرها و عوامل مؤثر از طریق روش اکتشافی و بررسی ارتباط و تأثیر آن‌ها بر الگوی مذکور از طریق تجزیه‌وتحلیل داده‌ها، محقق در پی پاسخ به سؤالات تحقیق و ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران است که بر اساس یافته‌های تحقیق به سؤالات این پژوهش پاسخ داده می‌شود:

سؤال فرعی اول: منابع، ماهیت و پیامدهای مختلف قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران کدام است؟

با توجه به یافته‌های کتابخانه‌ای و میدانی منابع، ماهیت و پیامدهای مختلف قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران شامل موارد زیر است:

منابع قدرت: فیزیکی و زیرساختی، اطلاعاتی، شناختی

ماهیت قدرت: ابزار مؤثر ارعاب علیه رقبا، ابزاری راهبردی و برترساز، مبتنی بر فناوری‌های مدرن، فراهم آورنده فضای نبرد آینده

پیامدهای قدرت: بازدارندگی سایبری، اشراف اطلاعاتی، برتری عملیاتی، ارتقاء امنیت ملی

سؤال فرعی دوم: ابعاد، مؤلفه‌ها و شاخص‌های سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران کدام است؟

با توجه به تجزیه‌وتحلیل‌های صورت پذیرفته، سنجش قدرت سایبری با سه بعد، یازده مؤلفه و پنجاه‌وپنج شاخص، به شرح زیر قابل انجام است:

جدول ۸: ابعاد، مؤلفه‌ها و شاخص‌های الگوی راهبردی ارزیابی قدرت سایبری جمهوری اسلامی ایران

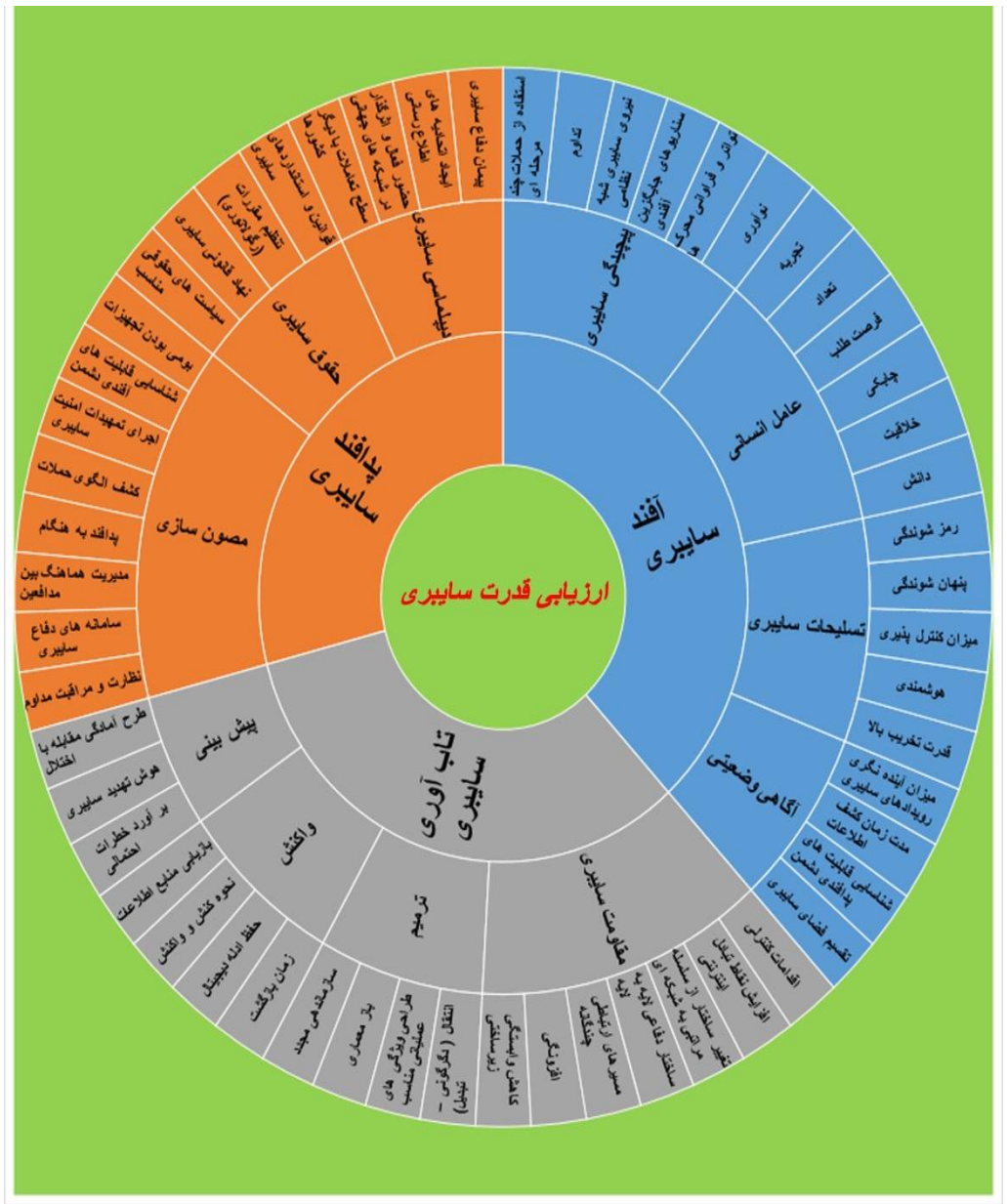
ردیف	ابعاد	مؤلفه‌ها	شاخص‌ها
۱	آفند سایبری	عامل انسانی	چابکی
۲			فرصت‌طلب
۳			خلاقیت
۴			دانش
۵			تعداد
۶			تجربه
۷		آگاهی وضعیتی	میزان آینده‌نگری رویدادهای سایبری
۸			شناسایی قابلیت‌های پدافندی دشمن
۹			مدت‌زمان کشف اطلاعات
۱۰			تقسیم فضای سایبری
۱۱		تسلیحات سایبری	میزان کنترل‌پذیری
۱۲			پنهان شوندگی
۱۳			رمز شوندگی
۱۴			قدرت تخریب بالا
۱۵			هوشمندی
۱۶		پیچیدگی سایبری	تداوم
۱۷			نوآوری
۱۸			میزان تواتر و فراوانی محرک‌ها
۱۹			حملات چندمرحله‌ای
۲۰			سناریوهای جایگزین آفندی
۲۱			نیروی سایبری شبه‌نظامی

ردیف	ابعاد	مؤلفه‌ها	شاخص‌ها
۲۲	پدافند سایبری	مصون‌سازی	بومی بودن تجهیزات
۲۳			کشف الگوی حملات
۲۴			سامانه‌های دفاع سایبری مبتنی بر انطباق الگو (شناسایی و ممانعت)
۲۵			میزان اجرای تمهیدات امنیت سایبری
۲۶			مدیریت هماهنگ بین مدافعین
۲۷			نظارت و مراقبت مداوم
۲۸			شناسایی قابلیت‌های آفندی دشمن
۲۹			پدافند به هنگام
۳۰		دیپلماسی سایبری	پیمان دفاع سایبری
۳۱			حضور فعال و اثرگذار در شبکه‌های جهانی
۳۲			ایجاد اتحادیه‌های اطلاع‌رسانی با کشورهای همسو
۳۳			سطح تمایلات با دیگر کشورها
۳۴		حقوق سایبری	تنظیم مقررات (رگلاتوری)
۳۵			سیاست‌های حقوقی مناسب
۳۶			استانداردهای سایبری
۳۷			نهاد قانونی سایبری
۳۸	تاب‌آوری سایبری	پیش‌بینی	هوش تهدید سایبری
۳۹			برآورد خطرات احتمالی (شناسایی، دسته‌بندی و ارزش‌گذاری تهدیدات سایبری)
۴۰			طرح آمادگی مقابله با اختلال
۴۱		مقاومت سایبری	کاهش وابستگی زیرساختی
۴۲			افزونگی
۴۳			مسیرهای ارتباطی چندگانه
۴۴			ساختار دفاعی لایه به لایه
۴۵			تغییر ساختار از سلسله مراتبی به شبکه‌ای
۴۶			افزایش نقاط تبادل اینترنتی
۴۷			اقدامات کنترلی

ردیف	ابعاد	مؤلفه‌ها	شاخص‌ها
۴۸		واکنش	بازیابی منابع اطلاعات
۴۹			نحوه کنش و واکنش (هدایت اوضاع)
۵۰			حفظ ادله دیجیتال (فارنزیک)
۵۱			زمان بازگشت
۵۲		ترمیم	سازمان‌دهی مجدد
۵۳			باز معماری
۵۴			طراحی ویژگی‌های عملیاتی مناسب
۵۵			انتقال (دگرگونی و تبدیل)
۵۵			انتقال (دگرگونی و تبدیل)

سؤال فرعی سوم: ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران چگونه است؟

ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران در قالب سه بعد، ده مؤلفه و هشتاد شاخص مطابق شکل زیر ارائه می‌گردد:



شکل ۵: الگوی ارزیابی قدرت سایبری

پیشنهادات:

با توجه به تأیید الگو، پیشنهاد می‌شود مدل عملیاتی این الگو بـه همـراه راهبـرد و برنامـه‌هـای اقدام طراحی گردد.

با مقایسه وضعیت موجود قدرت سایبری نیروهای مسلح جمهوری اسـلامی ایـران بـا الگـوی ارائه شده، پیشنهاد می‌گردد با ایجاد مراکز اشتراک و تحلیل اطلاعـات نسـبت بـه افـزایش قـدرت سایبری نیروهای مسلح جمهوری اسلامی ایران اقدام لازم صورت پذیرد.

با توجه به وضعیت نظام جمهوری اسلامی ایران و تقابل دائمی آن با اسـتکبار جهـانی و نظـام سلطه، تسریع در ارتقاء قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران که منجر بـه برتـری عملیاتی و ارتقاء امنیت ملی می‌شود، پیشنهاد می‌گردد.

منابع:

- فرانکلین و کرامر، (۱۳۹۳)، ***قدرت سایبری و امنیت ملی***، ترجمه احدی، محمد؛ ساوه‌درودی، مصطفی، تهران: انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.
- خاکی، غلامرضا، (۱۳۹۰)، ***روش تحقیق با رویکردی به پایان‌نامه نویسی***، تهران: انتشارات بازتاب.
- قاسم‌زاده، اردشیر و همکاران، (۱۳۹۳)، ***ارائه مدل ارزیابی میزان اثربخشی حملات سایبری با رویکرد عملیات تأثیر محور مبتنی بر اصول جنگ شناختی***، هشتمین کنفرانس ملی انجمن فرماندهی و کنترل تهران: دانشگاه علوم و فنون هوایی شهید ستاری.
- پالاور، ماتئو، (۲۰۱۱)، ***قدرت و اشکال آن: سخت، نرم، هوشمند***، دانشکده روابط بین‌الملل دانشگاه اقتصاد و علوم سیاسی لندن.
- مرکز خبرگی امنیت اطلاعات و شبکه، (۲۰۱۴)، ***یک چارچوب ارزیابی برای راهبردهای امنیت سایبری ملی***، آژانس اتحادیه اروپا.
- کریسمیر سلیک و همکاران، (۲۰۱۵)، ***مدل ارزیابی سطح امنیت سیستم‌های اطلاعاتی مبتنی بر رویکرد منطقی***، مجله رایانه‌ها و امنیت.
- زواری، مجید، (۱۳۹۵)، ***سناریوهای محتمل حملات سایبری و ضرورت ایجاد ره‌نگاشت***، ماهنامه نامه افق آینده‌پژوهی راهبردی، شماره ۱۱.
- زرقانی، سیدهادی، (۱۳۸۹)، ***نقد و تحلیل مدل‌های سنجش قدرت ملی***، فصلنامه ژئوپلیتیک، سال ششم، شماره اول، دانشگاه فردوسی مشهد.
- حافظ‌نیا، محمدرضا، (۱۳۹۲)، ***مقدمه‌ای بر روش تحقیق در علوم انسانی***، چاپ نوزدهم، تهران: انتشارات سمت.

- Lord,Kristin M. & Sharp, Travis (2011), American cyber future Security and prosperity in the Information Age, center for a new American Security, Volume I
- Nye, Joseph s. (2010); "Cyber Power", Belfer Center for Science and International Affairs.Peritz, AkiJ & Sechrist, Michael (2010); "Protecting Cyberspace and the U.S. National Interest", Belfer Center for Science and International Affairs.
- K.F. Rauscher and V. Yaschenko (Eds.), Russia U.S. Bilateral on Cybersecurity Critical Terminology Foundations, EastWest Institute and the Information Security Institute of Moscow State University, 2011
- Jake Bebber (2017), Cyber power and cyber effectiveness: An analytic Framework, U.S. Cyber Command, Norfolk, VA, USA

- Spade, J. M. (2012), China’s cyberpower and America’s national security. Carlisle Barracks, PA: US ARMY WAR COLLEGE
- Adrian Venables, Siraj Ahmed Shaikh and James Shuttleworth, (2015), A MODEL FOR CHARACTERIZING CYBERPOWER, 9th International Conference on Critical Infrastructure Protection (ICCIP)
- Sheldon, J.B. (2011).Deciphering Cyberpower: Strategic Purpose in peace and war. Restricted from: http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf
- R. E. Overill. Information Warfare: Battles in Cyber space, Computing & Control Engineering Journal, Vol. 12, no.3, pp. 125-128, 2001
- EY Global advisory cyber security leader, (2016), Path to cyber resilience, EY’s 19th Global Information Security Survey 2016-17
- Kadera, M.kelly (2004), Measuring National Power, International Intractions, Taylor& francis.
- Ashley J. Tellis, & others (2000), Measuring National Power in the postindustrial Age.Rond:New York
- Jc jansen van vuuren, (2016), “Building Blocks for National Cyberpower” Boston University of the United States
- Shaw,2010, cyber space: what senior military leaders need to know, http://handle.dtic.mil/100.2/ADA520146