تاریخ دریافت:۱۴۰۱/۰۱/۱۸ پژوهشنامه علوم دفاعی، شماره ٦، تابستان ۱۴۰۱
تاریخ پذیرش:۱۴۰۱/۰٤/۲۷ ص ص ٤١ تا ٦٤

تدوین راهبردهای ارتقاء قدرت سایبر در نیروهای مسلح جمهوری اسلامی ایران با تاکید بر حوزه‌های رزم سایبری و سایبر در رزم

مجتبی رمضان زاده[۱]، ابراهیم نظری فرخی[۲]

چکیده

در عصر کنونی، دنیا در حال گذر از جنگ‌های سنتی به جنگ‌های سایبری هست. نیروهای مسلح جمهوری اسلامی ایران در حوزه سایبری، اقدامات ارزشمندی را در جهت ارتقاء قدرت نظامی و ایجاد ظرفیت پاسخ‌گویی و مقابله با تهدیدات سایبری انجام داده است، ولی اقدامات مذکور با توجه به گستردگی حوزه سایبر در حد جامع نبوده و لازم است که فعالیت‌های فراوان دیگری در جهت رزم سایبری و سایبر در رزم صورت پذیرد تا به قدرت سایبری در تراز قدرت‌های تأثیرگذار جهانی و برخوردار از ابتکار عمل و قدرت تعامل با دیگر کشورها محقق شود. لذا تدوین راهبردها با تمرکز با رزم سایبری و سایبر در رزم جهت ارتقاء قدرت سایبری و جلوگیری از غافلگیری راهبردی، ضروری است. در این پژوهش، پس از مروری اجمالی بر مفاهیم قدرت به مفهوم‌سازی قدرت سایبری پرداخته شده و با تحلیل محیطی روندهای فضای سایبر، مطالعه اکتشافی قدرت سایبری در برخی از کشورها و اسناد بالادستی و برگزاری جلسات متعدد با خبرگان مدل مفهومی قدرت سایبری، ارائه شده است. روش تحقیق ازنظر هدف؛ کاربردی توسعه‌ای، ازنظر ماهیت؛ توصیفی همبستگی و از نظر روش تجزیه وتحلیل داده‌ها؛ آمیخته است. نتایج این تحقیق نشان می‌دهد با توسعه رویکرد عملیات سایبری در ابعاد شش‌گانه زیرساخت فاوایی، قابلیت‌های سایبری، تاب‌آوری سایبری، جمع‌آوری اطلاعات سایبری، رزم سایبری و سایبر در رزم از طریق راهبردهای تدوین شده، قدرت سایبری نیروهای مسلح به میزان ۲۷,۲٤ درصد ارتقاء پیدا خواهد کرد و عملاً در سطحی از اقتدار قرار می‌گیرد که قادر خواهد بود با حضوری مقتدرانه به اجرای مأموریت بپردازد.

کلمات کلیدی: قدرت، قدرت سایبری، راهبرد، رزم سایبری، سایبر در رزم، نیروهای مسلح.

---

۱. عضو هیئت‌علمی دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران. ایمیل: bmr.1398@yahoo.com
۲. عضو هیئت علمی دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران: e60_itmytn@yahoo.com

مقدمه

در نگرش اسلامی، قدرت هم‌افق با حکومت تعریف شده و مبتنی بر آیات قرآن کریم و روایات معصومان، منشأ قدرت از آنِ خداوند تبارک و تعالی بوده که برای ایجاد حکومت الهی برای دستیابی به اهداف برتر است (جعفری پناه و میراحمدی، ۱۳۹۱: ۱۰۷). در این راستا ابعاد و ویژگی‌های یک حکومت الهی با ابعاد و ویژگی قدرت مشروع بیان می‌شود (مفتح، ۱۳۹۰: ١٤).

امروزه فضای سایبری بعد مهمی از زیست‌بوم جهـانی را شـکل می‌دهد (زابلی زاده و وهاب پور، ۱۳۹۷: ۵۱)، کشورها به عنوان بازیگران اصلی در عرصه‌ی سایبری از لحاظ قدرت سایبری دارای ظرفیت‌های متعددی هستند، یکی از مهم‌ترین بازیگران این عرصه در کشورهای مختلف، سازمان‌های نظامی هستند. قدرت سایبری، مفاهیم سنتی امنیت نظامی و غیرنظامی را تغییر می‌دهد، زیرا فضای سایبری معنای مرزهای ملی را از بین می‌برد. فضای سایبری، نباید فقط از منظر فناوری مورد توجه قرار گیرد، فضای سایبری به‌عنوان پدیده‌ای که در زندگی روزمره و کارکردهای جوامع ما تأثیر روزافزون دارد، باید نگاه شود. قدرت سایبری باعث ایجاد تعویض بازیگران در سیستم قدرت جهانی شده است. از این پس حملات سایبری و اقدامات ضد سایبری بخشی از سامانه‌های دفاعی ملی و دکترین نظامی کشورها خواهد بود. اندازه‌گیری قدرت سایبری برای نیروهای مسلح دشوار است زیرا متکی به ارزیابی مأموریت‌ها، تهدیدات و محیط عملیاتی یگان‌های عمل‌کننده است (الوعده و بیراگبارا[1]، ۲۰۲۰: ۱۱). اهمیت موضوع سایبر، امنیت سایبر و دفاع سایبر از بیانات مقام معظم رهبری به‌وضوح قابل‌مشاهده است:

"فضای مجازی به‌اندازه انقلاب اسلامی اهمیت دارد." (سایت فارسی مقام معظم رهبری).

"فضای مجازی، واقعاً یک دنیای روبه رشدِ غیرقابلِ توقّف است، یعنی واقعاً آخر ندارد؛ آدم هرچه نگاه می‌کند، آن چیزِ اوّل بلا آخر، فضای مجازی است. هر چه انسان پیش می‌رود در این فضا، این همین‌طور، ادامه دارد. این‌یک فرصت‌های بزرگی در اختیار هر کشوری

[1] Aluede, Biragbara

می‌گذارد، تهدیدهایی هم درکناش دارد؛ ما بایستی کاری کنیم که از آن فرصت‌ها، حداکثر استفاده را بکنیم." (سایت فارسی مقام معظم رهبری).

ظهور روندها و پارادایم‌های نوین فناوری اطلاعات و ارتباطات نظیر شیءگرایی، شبکه محوری، محاسبات ابری، اینترنت اشیاء، انقلاب صنعتی چهارم،... تأثیرات و تحولات عمیقی بر تهیه چشم‌اندازها، جهت‌گیری‌ها، سیاست‌ها و راهبردهای دولت‌ها و سازمان‌های نظامی داشته است، برنامه‌ریزی راهبردی و سیاست‌گذاری کلان در این حوزه، نیازمند تدوین اصول راهنما، به منظور هدایت و راهبری فعالیت‌ها و اقدام‌های لازم جهت دستیابی به اهداف و منافع ملی است که در قالب رهنامه قدرت سایبری به دست می‌آید (هلیلی، ولوی، موحدی صفت، باقری،۱۳۹۷: ١٦). در نیروهای مسلح جمهوری اسلامی ایران آمادگی رزمی و توان رزمی توسط متولیان عملیات محاسبه می‌گردد ولی در محاسبات، مؤلفه‌های قدرت سایبری به‌وضوح دیده نمی‌شود زیرا دو مفهوم رزم سایبری و سایبر در رزم به صورت کامل در قدرت رزمی تبیین نشده و در ادامه ابعاد قدرت سایبری احصاء نشده و عملاً الگو جامع برای ارزیابی برای قدرت سایبری وجود ندارد.

در این مقاله، الگوی قدرت سایبری و راهبردهای ارتقاء آن در نیروهای مسلح جمهوری اسلامی ایران ارائه می‌شود تا با دسترسی به قدرت سایبری در تراز جهانی، قدرت بازدارندگی نیروهای مسلح جمهوری اسلامی ایران به‌منظور صیانت از تمامیت ارضی کشور در سطح نظام بین‌الملل افزایش یابد.

مبانی نظری

برای دستیابی و حفظ منافع ملی کشورها، وجود امنیت ملی لازم است، برای ایجاد امنیت ملی پایدار، قدرت در حوزه مختلف سیاسی، اقتصادی، فرهنگی، دفاعی و زیست‌محیطی ضروری است. قدرت به مفهوم تأثیرگذاری بر رفتار دیگران است، به‌نحوی‌که آنچه می‌خواهیم اتفاق بیفتد (بلیک، گلشن پژوه، ۱۳۸۹: ۱۲۷). به دلیل ارزان بودن، اثربخشی، نداشتن تلفات، پنهان بودن رزم سایبری و سایبر در رزم، جنگ در این بستر یکی از عرصه‌های قدرت، است،

کنش‌های سایبری در سال‌های اخیر رو به گسترش بوده و فعالیت‌هایی نظیر ایجاد نهادهای سیاست‌گذار در فضای سایبر، تشکیل کمیته‌های امنیت سایبری، بازتعریف دکترین سایبری، ایجاد واحدهای جدید سایبری در سطوح بالای سازمانی مانند فرماندهی سایبری، مراکز دفاع سایبری، ... ازجمله اقدامات عمده کشورها هست تا بتوانند با گسترش قدرت سایبری، جایگاه خود را در سلسله مراتب توان جهانی ارتقاء بخشند (هلیلی، ولوی، موحدی صفت، باقری،۱۳۹۷: ۳۲).

قدرت سایبری می‌تواند از منظر نظامی بازتعریف شود به نحوی که قدرت سایبری نظامی به کارکردهای عملیاتی با استفاده از ابزار فضای سایبر برای تحقق اهداف و مأموریت‌های نظامی از طریق فضای سایبر اطلاق می‌گردد. کشور جمهوری اسلامی ایران در حوزه سایبری به ویژه رزم سایبری، اقدامات ارزشمندی را در جهت ارتقاء قدرت سایبری و ایجاد ظرفیت پاسخ‌گویی و مقابله با تهدیدات سایبری انجام داده است، ولی اقدامات مذکور با توجه به گستردگی حوزه سایبر به ویژه در سایبر در رزم در حد جامع نبوده و عدم یکپارچگی در اجزای قدرت سایبری در حوزه‌های رزم سایبری و سایبر در رزم باعث عدم بروز قدرت سایبری مؤثر بر قدرت سخت گردیده است و به علت عدم شناسایی جامع و مانع ابعاد قدرت سایبری بر میزان اثربخشی آن کاسته است و در نتیجه نقشه راه ارتقاء قدرت سایبری قابل‌اتکا نخواهد بود.

رزم سایبری

رزم سایبری عبارت است از انجام یا آماده شدن برای انجام عملیات نظامی مطابق با اصول مربوط به اطلاعات. رزم سایبری یعنی ایجاد اختلال و نابودی سامانه‌های اطلاعاتی و ارتباطی که دشمن برای دانستن خود به آن‌ها تکیه می‌کند. در رزم سایبری تلاش می‌شود تا همه‌چیز را درباره دشمن بدانیم و درعین‌حال اجازه داده نشود او چیزی درباره ما بداند. به بیان دیگر، هدف اصلی از رزم سایبری برهم زدن موازنه اطلاعات و دانش به نفع نیروهای خودی است. رزم سایبری زیرمجموعه‌ای از جنگ اطلاعاتی است که شامل اقدام‌هایی

می‌شود که در دنیای سایبر رخ می‌دهد. رزم سایبر اَشکال متعدد داشته و از انواع فناوری‌های پیشرفته بهره می‌برد (ناظمی اردکانی و همکاران، ۱۳۹۵، ۲۲).

سایبر در رزم

سایبر در رزم استفاده از فضای سایبری به‌عنوان بستر و توان‌افزایی رزم مرسوم به صورت شبکه محور و متصل به هم انجام می‌شود. وجه تشابه دو اصطلاح رزم سایبری و سایبر در رزم، استفاده از بستر فضای سایبری است به نحوی که هر دو حوزه، بستر ایجاد قدرت، محیط الکترونیکی است که از طریق آن اطلاعات تولید، ارسال، دریافت، ذخیره، پردازش و حذف می‌شود اما تفاوت آن‌ها در نوع تجهیزات است به نحوی که در تجهیزات سایبری، رزم سایبری معنی پیدا می‌کند و در تجهیزات سایبرپایه، سایبر در رزم معنی پیدا می‌نماید. این دو تعریف نشان می‌دهد که حوزه رزم سایبری و سایبر در رزم در ارتقای توان رزمی نیروهای مسلح تأثیر مستقیم دارند و باید موردتوجه جدی قرار گیرد.(سند جامع سایبری نیروهای مسلح،١٤٠٠). سایبر در رزم عبارت است از به‌کارگیری سامانه‌های متکی به سایبر با رویکرد فیزیکی، اطلاعاتی و شناختی در نیروهای عملیاتی زمینی، هوایی، دریایی و فضایی به‌منظور انجام مأموریت‌های محوله آفندی، پدافندی، اطلاعاتی و امنیتی که سامانه اصلی نیرو در حوزه عملیات وابسته به سایبر است (قرارگاه سایبری و تهدیدات نوین).

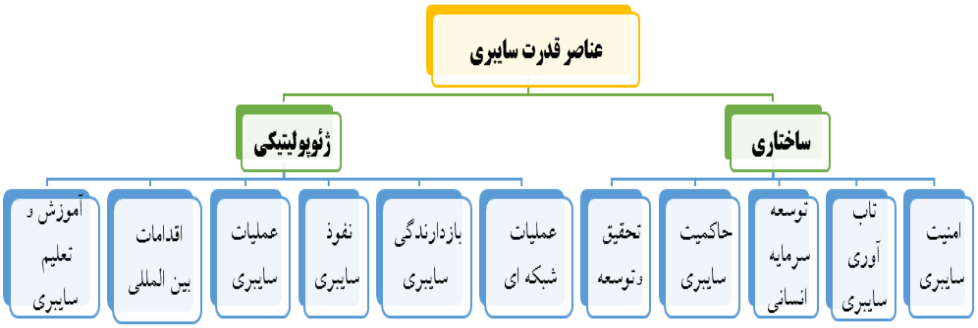
اجزاء قدرت سایبری

هدف کلی از قدرت سایبری نیروهای مسلح تحقق منویات و مطالبات سایبری فرماندهی معظم کل قوا (مدظله‌العالی) از طریق ایجاد نظام هماهنگ، جامع، کارآمد، به‌روز، هوشمند و مؤثر در بخش‌های مختلف سایبری نیروهای مسلح و ارتقاء توانمندی‌ها، قابلیت‌ها و آمادگی‌ها به‌منظور دستیابی و ارتقای قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران در همه ابعاد است. برای احصاء همه ابعاد قدرت سایبری، شناسایی اجزاء قدرت سایبری ضروری است.

نتایج مطالعات اکتشافی

نتایج مطالعه تطبیقی راهبردهای قدرت سایبری کشورهای آمریکا، روسیه، چین، رژیم صهیونیستی، انگلیس محورهای موردتوجه در اتخاذ راهبرد سایبری موفق به شرح زیر حاصل‌شده است:

- ✓ شناخت و فهم عمیق از محیط سایبر
- ✓ سرمایه‌گذاری بودجه‌ای گسترده بر امور زیربنایی سایبری
- ✓ داشتن مراکز و نیروهای سایبری کارآمد
- ✓ تأکید بر اصل هماهنگی و همگرایی
- ✓ چندجانبه گرایی در عین خوداتکایی
- ✓ همکاری سایبری گسترده با بخش خصوصی
- ✓ جایگاه و اهمیت سازمان‌های نظامی، اطلاعاتی و امنیتی



شکل شماره ۱- چارچوب راهبردی عناصر قدرت سایبری (کرامر، ۲۰۱۰)

حوزه‌ها و مؤلفه‌های تأثیرگذار بر قدرت رزم سایبری و سایبر در رزم

با توجه به نتایج حاصل از مصاحبه با خبرگان، ارکان و الگوهای تجزیه‌وتحلیل محیط‌های داخل و پیرامون و جمع‌آوری اطلاعات از روش‌های کتابخانه‌ای و میدانی ۲۵ مؤلفه تأثیرگذار

بر ارتقای قدرت سایبری مرتبط با این ٦ حوزه تعیین گردیدند. کلیه عوامل مرتبط با حوزه‌های شش‌گانه استخراج‌شده (زیرساخت فاوایی، قابلیت‌های سایبری، تاب‌آوری سایبری، جمع‌آوری اطلاعات، رزم سایبری، سایبر در رزم) شامل ۲۵ مؤلفه است که در جدول زیر، نشان داده شده است. جدول زیر، مبین این مطلب است که ازنظر جامعه خبره، این حوزه‌ها، دارای بیشترین و اساسی‌ترین تأثیر بر ارتقای قدرت سایبری است؛ بنابراین در این تحقیق فرآیند تعیین وضعیت موجود قدرت و تدوین طرح راهبردی ارتقای آن با در نظر گرفتن این حوزه‌ها صورت خواهد گرفت.

جدول (۱): مؤلفه‌های قدرت سایبری

ردیف	مؤلفه	حوزه
۱	بسترهای ارتباط	زیرساخت فاوایی
۲	بستر فناوری اطلاعات	
۳	امنیت و کنترل امنیت	
٤	فرماندهی و کنترل	قابلیت‌های سایبری
٥	اسناد راهبردی	
٦	معماری سازمان	
۷	آموزش سایبری	
۸	تجهیزات سایبری	
۹	منابع انسانی	
۱۰	همکاری سایبری	
۱۱	انسداد سایبری	تاب‌آوری سایبری
۱۲	بازرسی مداوم	
۱۳	مقاومت سایبری	
١٤	دیپلماسی سایبری	

ردیف	مؤلفه	حوزه
۱۵	برآورد اطلاعات سایبری	جمع‌آوری اطلاعات سایبری
١٦	اشرافیت سایبری خودی	
۱۷	یکپارچه‌سازی اطلاعات	
۱۸	جمع‌آوری اطلاعات سایبری دشمن	
۱۹	تجمیع و داده‌کاوی اطلاعات سایبری	
۲۰	پدافند غیرعامل رزم سایبری	رزم سایبری
۲۱	پدافند عامل رزم سایبری	
۲۲	آفند رزم سایبری	
۲۳	پدافند غیرعامل سایبر در رزم	سایبر در رزم
۲٤	پدافند عامل سایبر در رزم	
۲۵	آفند سایبر در رزم	

پیشینه تحقیق

جهت بررسی پیشینه تحقیق و مطالعات گذشته، محقق در بانک اطلاعات رساله‌ها و مطالعات گروهی دانشگاه عالی دفاع ملی، سامانه پژوهشگاه علوم و فناوری ایران، بانک اطلاعات پژوهشی نیروهای مسلح و سایر پایگاه‌های علمی داخلی و خارجی اقدام به جستجو در موضوعات مرتبط با عنوان پژوهش نمود که عناوین آن در قالب جداول ذیل ارائه می‌گردد:

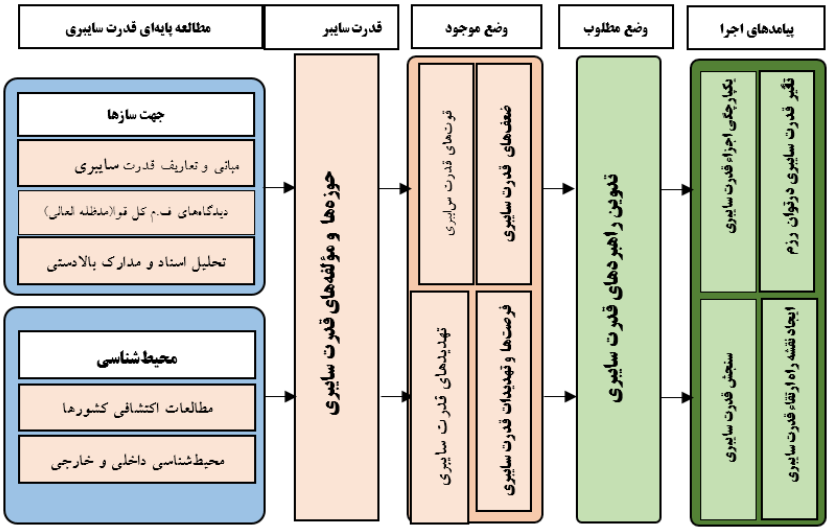
جدول (۲): پیشینه تحقیق

عنوان	نتایج
سند راهبردی پدافند سایبری کشور	تعریف چشم‌انداز پدافند سایبری در افق ١٤٠٤ دست‌یافته به زیست‌بوم ملی سایبری امن. افزایش پیچیدگی سامانه‌ها در فضای سایبری چالش‌های امنیتی برای کشور در بردارد. با توجه به آسیب‌پذیری ذاتی موجود در فضای سایبری و روند رو به رشد مهاجرت از دنیای سنتی به این فضا ریسک سامانه‌های فناوری اطلاعات را که برای اقتصاد کشور حیاتی هست را افزایش داده است.
امنیت ملی در فضای سایبر	با توجه به اینکه بنیان‌های اقتصادی و حتی سیاسی، فرهنگی و نظامی به‌گونه‌ای بر بستر فضای سایبر قرارگرفته و یا در حال قرار گرفتن است. ازاین‌رو ایجاد هرگونه اشکال در این فضا می‌تواند چالش‌های پیچیده و فلج‌کننده‌ای برای نظام پدید آورد. این چالش‌ها می‌تواند امنیت ملی را مخدوش کند. برای تأمین امنیت ملی باید از حوزه شناخت خودی صیانت نمود و بر حوزه شناخت دشمن اثر گذاشت. این کار با بهره‌گیری از فضای سایبر انجام می‌شود. بهره‌برداری از فضای سایبر در این حوزه انتخابی نیست بلکه اجباری است. (واحدی & صنیعی، ۱۳۹۲)

طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران	بازدارندگی از ابعاد اساسی دفاع سایبری است که مانع ذهنی محکمی را برای حریفان ایجاد می‌نماید تا با افزایش هزینه‌های تهاجمات سایبری، در مرحله طرح‌ریزی و قبل از آن، عاملان عملیات تهاجم را با تشتت و تزلزل مواجه سازد. استحکام چنین مانعی بستگی به میزان قابلیت، توانمندی و ظرفیت‌های بالقوه پاسخگویی دارد که به نسبت بین قدرت سایبری در مقایسه با دشمن بستگی دارد. با توجه به وضعیت نظام جمهوری اسلامی ایران و تقابل دائمی استکبار جهانی و نظام سلطه با آن، تهیه و تأمین تجهیزات سایبری، از مشکلات اساسی در حوزه دفاع سایبری است و ضرورت دارد اقدامات لازم درزمینه‌ی بومی‌سازی تجهیزات ساخت افزاری و نرم‌افزاری به‌ویژه در بخش دفاع و ایجاد زنجیره تأمین امن صورت پذیرد (تقی پور، اسماعیلی ۱۳۹۷).
طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی	اصول حاکم در برابر تهدیدهای سایبری در حوزه بازدارندگی عبارت‌اند از: آسیب‌ناپذیری، تحمیل هزینه‌بر دشمن، پاسخ به حملات دشمن، حفظ ارتقای بازدارندگی، پشیمان کنندگی، القای پیام اقتدار و برخورداری از فناوری بومی برتر. ارزش‌ها عبارت‌اند از اقتدار و نمایش قدرت، آمادگی دفاعی، ارعاب دشمن. چشم‌انداز عبارت‌اند از برخورداری از ساختار دفاعی آسیب‌ناپذیر و نفوذناپذیر در حوزه‌های حیاتی و حداقل آسیب‌پذیری در مقابل تهدیدها و حملات سایبری با ویژگی‌های تاب‌آوری، قابلیت کاهش خسارت و زمان ترمیم، انعطاف در گزینش و ترجیح شیوه دفاع لایه‌ای (احدی، شاه محمدی ۱۳۹۷).
Offense-defense theory analysis of Russian cyber capability	قابلیت روسیه در فضای سایبری بر مبنای نظریه‌ی جرویس آفندی است ولی نمای بیرونی و ظاهری آن‌هم آفندی و هم پدافندی است (Medvedev, 2015).

Cyber Power and the International System	باوجوداینکه بازدارندگی در فضای سایبری مانند فضاهای دیگر معنی ندارد ولی به دلایلی مانند مسئله‌ی نسبت‌دهی (به‌سختی می‌توان منبع حملات را مشخص نمود و به کشور نسبت داد) در آن موردتوجه کشورها درزمینه‌ی بازدارندگی قرارگرفته است. عملیات سایبری معمولاً به‌صورت مخفیانه و غیرعلنی انجام می‌گیرند یعنی تا حد ممکن بازیگران قدرت در این عرصه سعی می‌کنند از رویارویی مستقیم پرهیز کنند. فضای سایبری ماهیتاً به دلیل مسئله‌ی نسبت‌دهی کمتر در معرض خطر رویارویی دولت‌هاست ولی معمولاً پاسخگویی در همین فضا صورت نمی‌گیرد بلکه پاسخگویی به حملات سایبری در یک زمینه‌ی چند فضایی صورت می‌پذیرد (William, 2017).
ارائه الگوی راهبردی ارتقاء قدرت سایبری ایران در تراز جهانی	پس از مروری بر مفاهیم قدرت و قدرت سایبری، ارکان جهت سازی قدرت سایبری احصاء و ابعاد قدرت سایبری تدوین و الگوی راهبردی ارائه گردید (هلیلی، ولوی،۱۳۹۷).
بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا	مطابق نظریه‌ی رئالیسم ساختاری کشورها تمایل به افزایش قدرت تهاجمی خود در عرصه‌ی سایبری دارند. به همین دلیل بسیار از اندیشمندان بر این باورند که ویژگی بازدارندگی در فضای سایبری با دیگر فضاها متفاوت است و در این فضا باید مباحثی مانند هنجار سازی، انکار، تلافی و گرفتار سازی را درزمینه‌ی بازدارندگی در نظر گرفت (دهقانی، ۱۳۹۷).
قدرت بازدارندگی در فضای سایبری	سه مؤلفه‌ی اساسی درزمینه‌ی بازدارندگی در فضای سایبری به دست آمد که شناسایی مؤلفه‌ی کلیدی در این حوزه به شمار می‌رود. همچنین نتیجه‌ی دیگر این است که بدون عملیات تلافی‌جویانه بازدارندگی در فضای سایبری چندان مؤثر نیست (زابلی‌زاده، وهاب‌پور، ۱۳۹۷).

Cyber Power and Cyber Effectiveness: An Analytic Framework	در این مقاله یک چارچوب نظری برای بررسی متغیرهای قدرت سایبری یک حکومت و همین‌طور اثربخشی آن ارائه‌شده است. *(Bebber, 2017)* قدرت بالقوه سایبری دولت: روابط عمومی خصوصی- نهادهای سیاسی فرهنگ و جامعه: فرهنگ اطلاعات- جامعه اطلاعاتی- جرائم اقتصاد: صنعت فناوری نظامی: روابط دولتی – نوع آوری، انتشار و انطباق بین‌المللی: هنجارهای جهانی- مشارکت خارجی



شکل (۲): مدل مفهومی تحقیق

مدل مفهومی تحقیق

با عنایت به ادبیات تحقیق و مصاحبه‌های خبرگی انجام‌شده، مدل مفهومی تحقیق احصاء گردید. در مدل ارائه شده بالا، مطالعه پایه‌ای قدرت سایبری شامل جهت‌سازها و محیط‌شناسی انجام گرفته است. سپس به حوزه‌ها و مفاهیم و مؤلفه‌های قدرت سایبری پرداخته شد. در

ادامه وضع موجود در قالب بررسی نقاط قوت، ضعف، فرصت و تهدید مورد مطالعه قرار گرفت. مطالعه وضع مطلوب از طریق تدوین راهبردهای قدرت سایبری صورت گرفت و در نهایت پیامدهای اجرا به عنوان خروجی این مدل، خواهد بود.

روش‌شناسی پژوهش

روش تحقیق ازنظر هدف؛ کاربردی توسعه‌ای، ازنظر ماهیت؛ توصیفی همبستگی و از نظر روش تجزیه‌وتحلیل داده‌ها؛ آمیخته است.

قلمرو تحقیق (زمانی، مکانی و موضوعی)

- قلمرو زمانی تحقیق سال جاری (۱٤۰۰) است.
- قلمرو مکانی ندارد اما کاربرد آن ابتدا در ایران و باورمندان به انقلاب اسلامی است.
- قلمرو موضوعی، فضای سایبر از منظر رزم در سایبر و سایبر در رزم است.

روش نمونه‌گیری و حجم آن

حجم نمونه در بخش کیفی با توجه به خبرگان و صاحب‌نظران تا حد اشباع نظری در حوزه‌های قدرت سایبری و نظریه‌پردازی است. در بخش کمی، جامعه آماری مورد مطالعه، متشکل از کلیه کارکنانی که در حوزه قدرت سایبری و رزم در سایبر و سایبر در رزم که در امر آموزشی و پژوهشی مشغول انجام‌وظیفه هستند، می‌باشند. جامعه آماری با رعایت ملاحظات امنیتی متشکل از ۹۵ نفر است که حجم نمونه با ضریب اطمینان ۹۵٪ و سطح خطای ۰/۰۵ درصد با استفاده از فرمول کوکران، به شرح زیر محاسبه می‌گردد: با توجه به تنوع محل خدمتی جامعه آماری، حجم نمونه بر اساس فرمول کوکران به تعداد ۷۵ نفر و از طریق روش طبقاتی و به‌صورت زیر تعیین می‌گردد. جهت بررسی پایایی پرسشنامه، از روش محاسبه ضریب آلفای کرونباخ استفاده شده است، هر چه این ضریب به عدد یک نزدیک‌تر باشد؛ نشان‌دهنده پایایی مناسب ابزار است. میزان پایایی در پژوهش حاضر با استفاده از نرم‌افزار *SPSS* برابر با ۰,۷ شده است که نشان می‌دهد آزمون از پایایی قابل قبولی برخوردار است.

جدول (۳): توزیع جامعه آماری و نمونه ازنظر محل خدمت

ردیف	محل خدمتی جامعه آماری	حجم نمونه
۱	ستاد کل نیروهای مسلح	۱۵
۲	ارتش جمهوری اسلامی ایران	۱۳
۳	سپاه پاسداران انقلاب اسلامی	۱۲
٤	نیروی انتظامی	۱۰
۵	وزارت دفاع و پشتیبانی نیروهای مسلح	۱۰
۱۰	سایبری سازمان‌های ن.م	۱۵
جمع		۷۵

ازآنجاکه تک‌تک سؤالات پرسشنامه مبتنی بر ادبیات پژوهش به‌دست‌آمده است، این پرسشنامه دارای روایی لازم است. علاوه بر آن به منظور حصول اطمینان بیشتر از روایی پرسشنامه، نقطه نظرات خبرگان و تأیید آنان نیز اخذ شده است.

- **توصیف جمعیت شناختی پاسخ‌دهندگان**

عوامل مؤثر در طراحی مدل تحقیق، بر اساس طیف لیکرت با یک مقیاس نگرش سنج ۵ گزینه‌ای از خیلی زیاد تا خیلی کم در قالب پرسش‌نامه در بین ۷۵ نفر به‌صورت هدفمند توزیع گردید. در این قسمت اطلاعات حاصل از پرسش‌نامه درزمینه مشخصات فردی شامل نوع تخصص، جایگاه خدمتی، سابقه خدمتی، سطح تحصیلات، سازمان یا محل خدمت در جداولی منعکس و تشریح شده است.

۱) نوع تخصص: توزیع فراوانی پاسخگویان برحسب نوع تخصص در چهار دسته (فاوا، سایبر، جنگال و امنیت شبکه) دسته‌بندی و ارزیابی گردیده است. بر اساس نتایج بدست آمده درصد فراوانی مربوط به فاوا ۲۸٪، سایبر ۳۳٪، جنگال ۲۲٪ و امنیت ۱۷٪ هستند.

۲) جایگاه خدمتی:

توزیع فراوانی پاسخگویان برحسب جایگاه خدمتی در پنج گروه (١٤،١٥،١٦،١٧،١٨) دسته‌بندی و ارزیابی‌شده که نتایج آن نمایش داده شده است. بر اساس نتایج بدست‌آمده تعداد پاسخگویان در جایگاه خدمتی (١٥) به تعداد ٧ نفر معادل ١٢٪، در جایگاه خدمتی (١٦) به تعداد ٨ نفر معادل ١٣٪، در جایگاه خدمتی (١٧) به تعداد ٢٢ نفر معادل ٣٧٪، در جایگاه خدمتی (١٨) به تعداد ١٨ نفر معادل ٣٠٪ و در جایگاه خدمتی (١٩) به تعداد ٥ نفر معادل ٨٪ از کل پاسخگویان است.

٣) سابقه خدمتی:

پاسخ‌دهندگان به پرسش‌نامه از سابقه خدمتی مناسب برخوردار بوده به‌طوری‌که توزیع فراوانی پاسخگویان برحسب سابقه خدمتی به ٦ دسته از ٥ تا ١٠ سال، ١٠ تا ١٥ سال، ١٥ تا ٢٠ سال، ٢٠ تا ٢٥ سال، ٢٥ تا ٣٠ سال و بالای ٣٠ سال تقسیم شدند. بر اساس نتایج بدست‌آمده فراوانی پاسخگویان از ٥ تا ١٠ سال به تعداد ٨ نفر معادل ١٣٪، از ١٠ تا ١٥ سال به تعداد ١٢ نفر معادل ٢٠٪، از ١٥ تا ٢٠ سال به تعداد ٧ نفر معادل ١٢٪، از ٢٠ تا ٢٥ سال به تعداد ١٣ نفر معادل ٢٢٪، از ٢٥ تا ٣٠ سال به تعداد ١٢ نفر معادل ٢٠٪ و بالاتر از ٣٠ سال به تعداد ٨ نفر معادل ١٣٪ از کل پاسخگویان است.

٤) سطح تحصیلات:

توزیع فراوانی پاسخگویان برحسب مدرک تحصیلی در سه گروه کارشناس، کارشناس ارشد و دکترا دسته‌بندی و ارزیابی گردیده است. بر اساس نتایج بدست‌آمده فراوانی، ١٠ نفر معادل ١٧٪ دکترا و ٣٢ نفر معادل ٥٣٪ کارشناس ارشد و در سطح کارشناس به تعداد ١٨ نفر معادل ٣٠٪ هستند. کلیه پاسخگویان از سطح تحصیلات حداقل کارشناس برخوردار بودند.

٥) محل خدمت:

توزیع فراوانی پاسخگویان برحسب محل خدمت از مجموع ٧٥ پاسخ‌دهنده، از ستاد کل ١٥ نفر معادل ٢٥٪، از ارتش جمهوری اسلامی ایران به تعداد ١٣ نفر معادل ٢١٪، از سپاه پاسداران انقلاب اسلامی به تعداد ١٢ نفر معادل ٢٠٪، از نیروی انتظامی به تعداد ١٠ نفر معادل ١٧٪ و

وزارت دفاع و پشتیبانی نیروهای مسلح به تعداد ۱۰ نفر معادل ۱۷٪ به پرسشنامه این تحقیق پاسخ دادند.

تحلیل توصیفی داده‌ها و تعیین میزان مطلوبیت

پرسشنامه با مقیاس ۵ درجه‌ای طیف لیکرت با رتبه‌های «خیلی خوب، خوب، متوسط، کم و خیلی کم» طراحی گردید. برای تبدیل پاسخ‌های کیفی به کمی از روش وزن دهی استفاده شد. برای تعیین میزان مطلوبیت از طیف سه‌بخشی استفاده شد. در این تحقیق، طیف سه‌بخشی با توجه به مقیاس ۵ درجه‌ای پرسشنامه مطابق زیر مقابل ترسیم گردید و بر اساس آن میزان مطلوبیت عامل‌های پرسشنامه محاسبه گردید. ۵ حوزه از ٦ حوزه مورد بررسی در محدوده مطلوب و حوزه آفند سایبری، در محدوده نسبتاً مطلوب قرار گرفت و به همین روش مطلوبیت مؤلفه‌های حوزه‌های مختلف نیز احصاء و تائید شده است.

جدول (٤): محاسبه میانگین وزنی و میزان مطلوبیت ابعاد

ابعاد	فراوانی گزینه‌ها					وزن کلی	میانگین وزنی	کیفیت شاخص		
	خ.ز	ز	م	ک	خ.ک			مطلوب	نسبتاً مطلوب	نامطلوب
جمع‌آوری اطلاعات سایبری	٤٠	٢٧	٤	٣	١	٣٢٧	٤,٣٦	*		
پدافند سایبری	٢٩	٢٨	١٢	٥	١	٣٠٤	٤,٠٥	*		
آفند سایبری	٣٠	١٨	١٢	١٠	٥	٢٨٣	٣,٧٧		*	
زیرساخت فاوا	٣٥	٢٦	١٠	٣	١	٣١٦	٤,٢١	*		
الزامات سایبری	٣٣	٢٥	١٢	٣	٢	٣٠٩	٤,١٢	*		
تاب‌آوری سایبری	٤٠	٢٠	١٢	٣	٠	٣٢٢	٤,٣٠	*		

تحلیل محیطی

پس از مطالعه مبانی نظری ابتدا مؤلفه‌های اساسی محیط داخلی و خارجی احصاء گردیده، سپس به تفکیک هر مؤلفه نقاط قوت و ضعف و فرصت و تهدید قدرت سایبری احصاء شده و پس از تأیید خبرگان برای اعضای جامعه آماری ارسال گردید. پس از اصلاح و تأیید نقاط قوت و ضعف و فرصت و تهدید قدرت سایبری، نتایج حاصل از ارزیابی محیطی در بخش زیر نشان داده شده است.

نقاط قوت

- ✓ وجود تدابیر و فرمان‌ها صادره توسط فرماندهی معظم کل قوا در خصوص حوزه‌های مختلف سایبری
- ✓ برخورداری از نگاه راهبردی در سلسله مراتب فرماندهی در حوزه سایبری
- ✓ وحدت فرماندهی در امور سایبری نیروهای مسلح از طریق ستاد کل نیروهای مسلح
- ✓ وجود اسناد بالادستی مناسب درزمینه قدرت سایبری
- ✓ زیرساخت‌های فاوایی کارآمد، گسترده و فراگیر در سطح نیروهای مسلح
- ✓ برخورداری از نیروی انسانی متعهد، متخصص با تحصیلات تکمیلی در زمینه سایبری
- ✓ بهره‌مندی از ظرفیت‌ها و قابلیت‌های تعاملی در مشارکت‌پذیری و ایجاد کمک‌کننده به مأموریت‌های سایبری
- ✓ حرفه‌ای سازی و تخصصی شدن نیروهای مسلح با برگزاری رزمایش‌های سایبری متعدد در سطح نیروهای مسلح.

نقاط ضعف

- ✓ ضعف همگرایی و هماهنگی ساختارهای متولی سیاست‌گذاری، تصمیم‌گیری، اجرا و نظارت در موضوع سایبری
- ✓ عدم احصاء و شناخت دقیق تجهیزات رزمی سایبرپایه خودی و دشمن
- ✓ عدم وجود طرح عملیاتی آفندی و یا پدافندی برای تجهیزات سایبرپایه خودی و دشمن

- ✓ عدم بهره‌گیری مناسب از تجربیات و ظرفیت‌های بخش خصوصی فعال سایبری
- ✓ کمبود استانداردهای امنیتی بومی برای تجهیزات سایبرپایه
- ✓ وابستگی به دانش، فناوری و استانداردهای غیربومی و داخلی در زمینه‌های سایبری
- ✓ ناکافی بودن آموزش‌های تخصصی کارکنان در خصوص سایبر در رزم

نقاط فرصت

- ✓ حمایت فرماندهی معظم کل قوا
- ✓ گستردگی جهانی و دسترسی بدون مرز برای عملیات جمع‌آوری، پدافندی و آفندی
- ✓ وجود ظرفیت‌ها و قابلیت‌های سایر کشورهای دوست در انجام عملیات مشترک سایبری.
- ✓ وابستگی شدید دشمن به تجهیزات سایبرپایه و قابلیت نفوذ بر آن
- ✓ داشتن تجربه مطلوب در حوزه رزم سایبری و قابلیت توسعه آن به حوزه سایبر در رزم
- ✓ اقبال ظرفیت‌های علمی، نخبگان و خبرگان برای تعامل و نقش آفرینی در حوزه سایبری

نقاط تهدید

- ✓ توانمندی‌ها و قابلیت‌های دشمنان در بهره‌گیری از فناوری‌های برتری ساز در جنگ سایبری
- ✓ سازمان‌دهی تهدیدات سایبری از سوی دشمن و ایجاد و گسترش تهاجم‌ها در فضای سایبر در رزم و رزم سایبری
- ✓ ضعف قوانین و مقررات بین‌المللی درزمینه حملات سایبری

راهبردهای قدرت سایبری (با تمرکز بر رزم سایبری و سایبر در رزم)

جهت تدوین راهبردهای ارتقای قدرت سایبری ضروری است که نقاط قوت و ضعف سایبری با فرصت‌ها و تهدیدات سایبری تقابل و انطباق داده شوند. یکی از رایج‌ترین ابزارهای مواجهه و تقابل نقاط قوت و **ضعف** با فرصت‌ها و تهدیدات در حوزه مدیریت راهبردی ماتریس *SWOT* است. بر این اساس راهبردها بر اساس عوامل محیطی که بیشترین رابطه را با هم دارند به شرح ذیل تدوین گردیدند:

۱. تدوین نظریه، دکترین، آرمان، سیاست و رهنامه و برنامه‌ریزی راهبردی قدرت سایبری به‌عنوان اسناد جهت ساز و هادی فعالیت‌های سایبری.
۲. توسعه رویکرد عملیات سایبری فعال در سطح نیروهای مسلح منظور افزایش تاب‌آوری سایبری سامانه‌ها و زیرساخت‌های حیاتی
۳. توسعه تجهیزات و فناوری‌ها و تکنیک‌های رزم سایبری و سایبر در رزم ناهمطراز و غیر وابسته به منظور مقابله با فناوری‌ها و تجهیزات گسترده، منسجم و یکپارچه رزمی دشمن در حوزه نبرد سایبری
٤. توسعه کارکردهای سایبر در رزم در هر رده (اعم از حوزه‌های فاوا، جنگال، شبکه‌های راداری، جنگنده‌ها، هواپیماهای ترابری، پهپادها، بالگردها، موشک‌ها، ناوها و ناوچه‌ها، زیردریایی، مهمات هوشمند) و ... به‌منظور عملیات آفندی و پدافندی در تجهیزات سایبرپایه
۵. توسعه و ارتقای نظام فرماندهی و کنترل سایبری با استفاده از امکانات فضای سایبر در دو حوزه رزم سایبری و سایبر در رزم
٦. بهره‌مندی از ظرفیت‌های کشور و مراکز علمی تحقیقاتی در سطح ملی و ن. م به منظور طراحی، پیاده‌سازی و توسعه نظام فرماندهی و کنترل سایبری
۷. توسعه تسلط و اشراف جامع بر فضای سایبری در حوزه مأموریتی با طراحی و اجرای سامانه‌های جامع پویش و پایش تهدیدات سایبری به منظور افزایش مصون‌سازی سامانه‌ها و زیرساخت‌های حیاتی
۸. توسعه همکاری‌های علمی – آموزشی در سطح ملی و بین‌المللی در راستای ساماندهی، ارتقای دانش فنی و کیفی سازی دوره‌های آموزشی داخلی به منظور افزایش توانمندهای نیروی انسانی متخصص درزمینه سایبری
۹. برگزاری رزمایش‌های سایبری مشترک و مرکب در سطح ملی و بین‌المللی با مجموعه سازمان‌های ن. م و نیز کشورهای دوست و متحد به‌منظور حفظ و ارتقای قابلیت‌های سایبری

نتایج حاصل از احصاء راهبردهای منتخب در قالب جدول میزان تأثیر راهبرد بر ارتقای قدرت سایبری تنظیم و به کارشناسان سایبری جهت نمره دهی بر اساس طیف لیکرت ۱ الی ۹ ارسال شد و با توجه به نمرات ضریب اهمیت هرکدام از راهبردها، امتیاز موزون و سپس مجموع نمرات میزان تأثیر راهبرد بر قدرت سایبری محاسبه گردید که نتایج آن به شرح جدول (۵) ارائه گردید.

جدول (۵): نتایج و امتیاز مولفه های قدرت سایبری

ردیف	راهبردها	میزان اهمیت	قدرت سایبری			
			در شرایط موجود		در شرایط آتی	
			امتیاز	عدد موزون	امتیاز	عدد موزون
۱	تدوین نظریه، دکترین، آرمان، سیاست و رهنامه و برنامه‌ریزی راهبردی قدرت سایبری به‌عنوان اسناد جهت‌ساز و هادی فعالیت‌های سایبری.	٦/۲۳	۵/۱۲	۳۱/۹۰	٦/۱۲	۳۸/۱۳
۲	توسعه رویکرد عملیات سایبری فعال در سطح نیروهای مسلح منظور افزایش تاب‌آوری سایبری سامانه‌ها و زیرساخت‌های حیاتی	۷/۲۸	٤/۲۳	۳۰/۷۹	۷/۱٦	۵۲/۱۲
۳	توسعه تجهیزات و فناوری‌ها و تکنیک‌های رزم سایبری و سایبر در رزم ناهمطراز و غیر وابسته به‌منظور مقابله با فناوری‌ها و تجهیزات گسترده، منسجم و یکپارچه رزمی دشمن در حوزه نبرد سایبری	۷/٦۹	٤/۱۱	۳۱/٦۱	۵/۹٤	٤۵/٦۸
٤	توسعه کارکردهای سایبر در رزم در هر رده (اعم از حوزه‌های فاوا، جنگال، شبکه‌های راداری، جنگنده‌ها، هواپیماهای ترابری، پهپادها، بالگردها، موشک‌ها، ناوها و ناوچه‌ها، زیردریایی، مهمات	۸/۲۹	٤/۹۹	٤۱/۳۷	۷/۱۲	۵۹/۰۲

	هوشمند) و ... به‌منظور عملیات آفندی و پدافندی در تجهیزات سایبر پایه					
٥	توسعه و ارتقای نظام فرماندهی و کنترل سایبری با استفاده از امکانات فضای سایبر در دو حوزه رزم سایبری و سایبر در رزم	٨/٣٥	٣/٢٦	٢٧/٢٢	٦/٩٣	٥٧/٨٧
٦	بهره‌مندی از ظرفیت‌های کشور و مراکز علمی تحقیقاتی در سطح ملی و ن. م به‌منظور طراحی، پیاده‌سازی و توسعه نظام فرماندهی و کنترل سایبری	٦/٥٤	٤/١٥	٢٧/١٤	٦/١٩	٤٠/٤٨
٧	توسعه تسلط و اشراف جامع بر فضای سایبری در حوزه مأموریتی با طراحی و اجرای سامانه‌های جامع پویش و پایش تهدیدات سایبری به‌منظور افزایش مصون‌سازی سامانه‌ها و زیرساخت‌های حیاتی	٧/١٢	٣/١٨	٢٢/٦٤	٧/٢٣	٥١/٤٨
٨	توسعه همکاری‌های علمی – آموزشی در سطح ملی و بین‌المللی در راستای ساماندهی، ارتقای دانش فنی و کیفی سازی دوره‌های آموزشی داخلی به‌منظور افزایش توانمندهای نیروی انسانی متخصص درزمینه سایبری	٥/١٩	٤/٨٩	٢٥/٣٨	٦/٩٨	٣٦/٢٣
٩	برگزاری رزمایش‌های سایبری مشترک و مرکب در سطح ملی و بین‌المللی با مجموعه سازمان‌های ن. م و نیز کشورهای دوست و متحد به‌منظور حفظ و ارتقای قابلیت‌های سایبری	٧/١٦	٥/١٢	**٦/٦٦**	٧/١٨	٥١/٤١
		٦٣/٨٥	٣٩/٠٥	٢٧٤/٧١	٦٠/٨٥	٤٣٢/٤٢

شکل (۳): ارتقای قدرت سایبری در افق برنامه

نتیجه گیری و پیشنهادات

جمهوری اسلامی ایران و نیروهای مسلح، اقدامات ارزشمندی را جهت ایجاد و ظرفیت پاسخ‌گویی و مقابله با تهدیدات سایبری انجام داده ولی اقدامات مذکور با توجه به گستردگی حوزه‌های نبردی سایبری جامع نبوده و لازم است که فعالیت‌های دیگری در جهت ارتقای قدرت سایبری در حوزه‌های مختلف همانند سایبر در رزم، مقاومت سایبری، مصون‌سازی منابع و ایجاد قابلیت‌های دفاع فعال انجام گیرد. جهت ارتقای قدرت سایبری رویکرد راهبردی در ایجاد مزیت‌های رقابتی نقش بسزایی دارد به نحوی که با استفاده از فرصت‌ها و قوت‌ها و پرهیز از ضعف‌ها و نقص‌ها، راهبردهای لازم جهت ارتقای قدرت سایبری تدوین گردید. ارزیابی راهبردها نشان می‌دهد که در یک دوره زمانی پنج ساله می‌توان قدرت سایبری را به میزان ۲۷ درصد افزایش داد و سطح بلوغ قدرت سایبری را در سطح قدرت تراز منطقه‌ای قرار داد. با ارزیابی انجام شده میزان اثربخشی راهبردهای تدوینی نمایان می‌گردد.

پیشنهاد می‌شود پژوهشگران آتی:

الف- متناسب با راهبردهای ارائه شده، سیاست‌ها و الزامات اجرایی متناسب با هر راهبرد را تدوین نمایند.

ب- بر اساس ابعاد و مولفه‌های احصاء شده، پژوهشگران آتی مدل سنجش قدرت سایبری را با نگاه سطح بلوغ تدوین و موقعیت راهبردی قدرت سایبری را به صورت سالیانه تعیین و به تصمیم‌گیران ارائه نمایند.

منابع

بلیک، ژ و گلشن پژوه، م. (۱۳۸۹). قدرت نرم. تهدید نرم: پیشنهادی در راستای سیاست سازی. راهبرد, ۱۹(۵۵) (بخش ویژه بررسی‌های بین‌الملل), ۱۲۳-۱۳۷.

جعفری پناه، م.، و میراحمدی، م. (۱۳۹۱). مؤلفه‌های قدرت نرم جمهوری اسلامی ایران با رویکرد اسلامی. معرفت سیاسی, ٤(۲), ۱۰۵-۱۲۲.

خداداد هلیلی، محمدرضا ولوی، محمدرضا موحدی صفت، مسعود باقری، (۱۳۹۷). قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر، نشریه امنیت ملی، ۸(۲۹).

زابلی زاده، ا.، و وهاب پور، پ. (۱۳۹۷). قدرت بازدارندگی در فضای سایبر. مطالعات بین‌رشته‌ای در رسانه و فرهنگ (رسانه و فرهنگ), ۸(۱ (پیاپی ۱۵)), ٤٧-٧٤.

مفتح، محمدهادی،(۱۳۹۰). گزارش تحلیلی از کتاب نظریه قدرت برگرفته از قرآن و سنت، فصلنامه کتاب نقد، ۱۳(۵۹)، ۱۱۳.

مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، (۱۳۹۰). راهبردهای امنیت فضای سایبری در سه کشور انگلستان، آلمان و آمریکا. چاپ اول، تهران، ناشر: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی حوزه هسته‌های نوآوری دفاعی.

نصرت‌آبادی، جمشید، لشکریان، حمیدرضا، مردانی، محمد، موحدی صفت، محمدرضا. (۱۳۹۸). ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران، فصلنامه علمی امنیت ملی، (۳۱)۹، ۱۹۸-۱۷۳.

Aluede, L. O., & Biragbara, E. P. B. (2020). CYBER ATTACK: AN EMERGING WAR. GSJ, 8(1)

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., & Dolan, T. (2014). Cybersecurity capability maturity model (C2M2). Department of Homeland Security, 1-76.

Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). CYBER READINESS INDEX 2.0.

Hamilton, B. A. (2011). Cyber power index: findings and methodology. Retrieved January, 6, 2013.

Hanson, F., Uren, T., Ryan, F., Chi, M., Viola, J., & Chapman, E. (2017). Cyber maturity in the Asia Pacific region 2017.

https://farsi.khamenei.ir/others-dialog?id=19272
https://farsi.khamenei.ir/speech-content?id=34162
Kramer. D. Franklin.(2016) . CyberPower and National Security. USA National Defence Uneversity.
Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.
Minges, (2017), Global Cybersecurity Index (GCI), the Internatonal Telecommunication Union (ITU)
Nye, J. S. (2021). Soft power: the evolution of a concept. Journal of Political Power, 14(1), 196-208.
Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. Scitech Lawyer, 10(4), 16.
Starr, Stuart H. (2008), developing a theory of cyber power, in FD Kramer, S. Starr, L.K. Wentz (ed.) Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity, pp. 127–135
Van Veenendaal, E., & Wells, B. (2012). Test maturity model integration (TMMi). TMMI Foundation (www. tmmifoundation. org), Uitgeverij Tutein Nolthenius.