آینده‌پژوهی دفاعی، سال هفتم، شماره ۲۷، زمستان ۱۴۰۱

تاریخ دریافت: ۱۴۰۱/۱۰/۰۳ تاریخ پذیرش: ۱۴۰۱/۱۲/۲۴

از صفحه ۶۳ تا صفحه ۸۲

راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران

داود آذر[۱*]

حسین مسلمی[۲]

نوع مقاله: پژوهشی

چکیده

به لحاظ نظامی، قدرت سایبری، شاید مهم‌ترین قدرت نوظهور چند دهه گذشته باشد. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. رهنامه‌های جدید نظامی بر اساس فضای سایبر تدوین می‌شوند. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبری، عامل حتمی و گریزناپذیر توانمندی‌های نظامی است، این توانمندی بر پایه فناوری‌های مدرن شکل‌گرفته است. مراکز سایبری در ساختار نظامی ارتش جمهوری اسلامی ایران یک سازمان مهم به‌حساب می‌آیند و نتایج عملکرد آن‌ها نقش حیاتی در عملکرد و کارآمدی ارتش خواهد داشت. ازاین‌رو تعیین عملکرد آن‌ها بر اساس راهبردهای نوین، یکی از وظایف مهم فرماندهان عالی ارتش جمهوری اسلامی ایران به‌حساب می‌آید. این تحقیق با هدف ارائه راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران انجام شده است. در این پژوهش بر اساس روشی تحلیلی- توصیفی و بهره گیری از منابع موجود در زمینه قدرت سایبری و نیز بررسی همه جانبه با استفاده از روش تحلیل SWOT نسبت به تعیین نقاط قوت، ضعف، فرصت‌ها و تهدیدها اقدام شده و در ادامه بر اساس نظر کارشناسان و مصاحبه شوندگان، وزن هر گزینه تعیین و پانزده راهبرد به عنوان مهم‌ترین راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران تعیین گردید.

واژه‌های کلیدی:

فضای سایبر، قدرت سایبری، آفند سایبری.

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

[۲] استادیار دانشگاه فرماندهی و ستاد آجا، تهران، ایران

[*] نویسنده مسئول: Email: d.azar@casu.ac.ir

DOI 10.22034/DFSR.2023.1983449.1667

مقدمه

با توسعه جوامع مجازی در اینترنت، حوزه‌های سرزمینی کاهش‌یافته و الگوهای حکمرانی توسعه پیدا کرده است و الگوی جدیدی برای جوامع و حاکمیت، در حال شکل‌گیری است. نقش دولت‌ها در زندگی مردم کم‌اهمیت‌تر شده است؛ افراد با چندین قرارداد داوطلبانه، زندگی خواهند کرد و با کلیک ماوس در جوامع مختلف وارد می‌شوند (Nye, 2010: 4).

به لحاظ نظامی، قدرت سایبر، شاید مهم‌ترین ابزار نوظهور چند دهه گذشته باشد. در حال حاضر اغلب نیروهای مسلح کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. رهنامه‌های جدید نظامی بر اساس فضای سایبر تدوین 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 مدرن شکل‌گرفته است. قدرت سایبر روزبه‌روز خود را به‌عنوان یک عامل تأثیرگذار در سیاست‌گذاری حوزه‌های ملی از اقدامات ضدتروریستی گرفته تا سامان دادن سیاست، اقتصاد و حتی روابط با سایر کشورها، توسعه می‌دهد (زابلی زاده، ۱۳۹۷: ۵۳).

اطلاعات در فضای سایبر به‌راحتی و برای همه به‌صورت یکسان در دسترس هستند. سیستمی که به ارتباطات الکترونیکی متکی است، در صورت تداخل یا ازبین‌رفتن توانایی برقراری ارتباط، می‌تواند بی‌فایده شود. از آنجاکه این اتکا بسیار کلی است، حمله سایبری به زیرساخت‌های اطلاعاتی می‌تواند تأثیرات گسترده‌ای هم برای ارتش و هم برای جامعه داشته باشد و چنین حملاتی می‌تواند از منابع مختلفی انجام شود، شناسایی برخی از آنها دشوار یا غیرممکن است (Zac, 2021: 83).

یکی از عرصه‌های قدرت، فضای سایبری می‌باشد، 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،... از جمله اقدامات عمده سازمان‌هاست تا بتوانند با گسترش قدرت سایبری، جایگاه خود را در سلسله مراتب توان جهانی ارتقاء بخشند (هلیلی، ۱۳۹۷: ۱۴۳).

کشور جمهوری اسلامی ایران در حوزه سایبری، اقدامات ارزشمندی را در جهت ارتقاء قدرت سایبری و ایجاد ظرفیت پاسخ‌گویی و مقابله با تهدیدهای سایبری انجام داده است، از طرفی اقدامات مذکور با توجه به گستردگی حوزه سایبر در حد جامع نبوده و لازم است راهبردهای قدرت سایبری آجا تدوین و مدون شود تا بر اساس آن سطح و عملکرد قدرت سایبری ارتش

مشخص گردد، که در صورت عدم یکپارچگی در اجزای قدرت سایبری در حوزه‌های تاب‌آوری، جنگ شناختی، جمع‌آوری اطلاعات سایبری، پدافند و آفند سایبری موجب همگرایی قدرت سایبری مؤثر در آجا می‌شود. همچنین نبود راهبردهای ارتقاء قدرت سایبری منتج شده از سنجش قدرت سایبری که سبب می‌گردد نقشه راه رسیدن از وضع موجود به وضع مطلوب در هاله‌ای از ابهام بماند (رمضان‌زاده، ۱۳۹۹: ۳).

راهبردهای سایبری توسط کشورهای مختلف ارائه‌شده اما راهبردهای مذکور نه‌تنها قابل بسط در ارتش جمهوری اسلامی ایران نمی‌باشد بلکه برای کشور هم مفید نمی‌باشد، زیرا راهبردها؛ متناسب با چشم‌انداز و اصول ارزشی کشورها تدوین‌شده و با عنایت به چشم‌انداز و اصول ارزشی مترقی و معنی محور در کشور جمهوری اسلامی ایران، بسط راهبردهای کشورهای دیگر کاری ناصواب می‌باشد (همان).

سؤال اصلی پژوهش حاضر، این است که راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران کدام است؟ بنابراین لزوم تعیین راهبردهای قدرت سایبری در ارتش ج ا ا جهت پوشش ضعف‌ها و جلوگیری از تهدیدها و استفاده از نقاط قوت و فرصت‌ها جهت برگرداندن به وضعیت عادی در کمترین زمان ممکن مد نظر بوده که در نهایت به نتیجه مطلوب در خصوص راهبردهای این حوزه خواهد شد.

مبانی نظری

فضای سایبر

فضای سایبر امکانات جدیدی در اختیار بشر قرار می‌دهد. انسان را از فاعل بودن در محیط اجتماعی، به سوژگی در محیط مجازی سوق می‌دهد؛ ایده‌ها را گسترش می‌دهد؛ دولت را به‌عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و اقتصادی خلع سلاح می‌کند. وجود پیوند میان فضای سایبر و قدرت در روابط بین‌الملل، در حال حاضر امر بدیهی محسوب می‌شود. وجوه قدرت در فضای فیزیکی متنوع است. این تعدد وجه، خود را در فضای سایبر نیز نشان می‌دهد. می‌توان از چند وجه قدرت در روابط بین‌الملل و جهان سیاست صحبت کرد. وجه سخت‌افزاری و وجه نرم‌افزاری قدرت در فضای سایبری، نیز می‌تواند نشانه‌های چنین وجوهی را جستجو کرد (زابلی زاده، ۱۳۹۷: ۵۶).

مهم‌ترین ویژگی‌های برقراری ارتباطات در فضای سایبری عبارت‌اند از:

- شبکه‌ای بودن
- قابلیت ایجاد اجتماعات
- ماهیت فنی

- وابستگی و ارتباطات متقابل
- آسیب‌پذیر بودن (Department of Army, 2017: PP I-15 - I-16)

نگاه راهبردی به قدرت سایبری

در یک تقسیم‌بندی می‌توان، راهبرد را در سه سطح راهبرد امنیت ملی، راهبرد دفاعی و راهبرد نظامی تعریف نمود. راهبرد نظامی عبارت است از توسعه و به‌کارگیری قدرت نظامی برای دستیابی به اهداف ملی از طریق توسل یا تهدید به‌زور. ازنظر آقای دکتر آقا محمدی راهبرد نظامی عبارت است از طرحی جامع و منسجم از روش‌های به‌کارگیری قدرت نظامی و منابع و ابزارهای نیل به اهداف نظامی، در راستای تأمین اهداف سیاسی، نظامی بر اساس پایش محیطی به‌منظور خلق و بهره‌برداری از فرصت‌ها، توسعه قابلیت‌ها و شایستگی‌های محوری، کاهش ضعف‌ها و خنثی‌سازی تهدیدهای نظامی. راهبرد نظامی بخشی از راهبرد فراگیر است (آقامحمدی، ۱۳۹۵).

معیارهای مطلوب برای قدرت سایبری

در کار انجام شده توسط جی وورن[1]، مؤلفه‌های زیر برای قدرت سایبری در نظر گرفته شده 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 (نصرت‌آبادی، ۱۳۹۷: ۱۸۵-۱۸۷).

مطلوبیت‌های قدرت سایبری ارتش جمهوری اسلامی ایران

مطلوبیت‌های شناسایی شده ارتش جمهوری اسلامی ایران که با تحقق آن‌ها می‌تواند مأموریت‌های آفند سایبری خود را ارتقا دهد عبارت‌اند از:

- طراحی، تولید، استقرار و به‌کارگیری محصولات بومی حوزه فاوا
- ارتقا تحصیلی کارکنان حوزه فاوا

[1] Jworn

- تولید نرم‌افزارهای امن داخلی
- برگزاری رزمایش‌های سایبری
- ایجاد و تقویت مراکز تولید سامانه‌های هوشمند (مسلمی حسین، ۱۳۹۴: ۲۱۶).

کشورها با توسعه فنی و استفاده تاکتیکی در زمینهٔ عملیاتی از نیروهای سایبری به‌عنوان متغیرهای اصلی مداخله‌گر در سراسر چارچوب ارزیابی سایبری، رویکردشان را سازماندهی می‌کنند و درنهایت یک سازمان نظامی را در وضعیت ایجاد قدرت سایبری قرار می‌دهند. اثربخشی قدرت سایبری بستگی به این دارد که چگونه نیروهای سایبری مورداستفاده و ارزیابی قرار گیرند (نصرت‌آبادی، ۱۳۹۷: ۱۷۳-۱۷۸).

اسناد و مدارک اصول پدافند سایبری کشوری

ارتش نیز از اصول و تاثیرات محیط پیرامونی خود مصون نبوده و بایستی همواره آن را مد نظر داشته و بر اساس آن اسناد و راه کارهای خود را تدوین نماید.

بر این اساس تدابیری که از سوی مقام معظم رهبری در سال۱۳۹۴ بیان گردید، فضای سایبری کشور هم که بخش مهمی از سرمایه‌های حیاتی و حساس کشور را در بردارد باید مصون و پایدار بماند.

جدول(۱) اصول پدافند سایبری کشور

۱. مصون سازی و پایداری فضای سایبر	۲. حفظ و صیانت از سرمایه‌های سایبری
۳. وحدت فرماندهی پدافند سایبری کشور	۴. پیش‌دستی در شناخت تهدیدها
۵. دفاع بومی، همه جانبه و بازدارنده	۶. اقتصادسازی
۷. هوشمندی در دفاع	۸. اشراف اطلاعاتی در فضای سایبری
۹. روزآمدی و آینده‌نگری	۱۰. دانش و فناوری بومی و مدیریت آن
۱۱. کاهش آسیب‌پذیری سایبری	۱۲. نفوذ ناپذیری و اقتدار
۱۳. حفظ تداوم کارکرد سامانه‌ها	۱۴. بهداشت سایبری
۱۵. آمادگی و پایداری	۱۶. رعایت قوانین بین المللی

عوامل محیطی چهارگانه نقاط قوت، ضعف، فرصت‌ها و تهدیدها پدافند سایبری کشور عبارتند از: (پدافند سایبری کشوری، ۱۳۹۹: ۲۷-۳۴)

قوت‌ها

۱. توجه جدی و حمایت‌های مسئولین عالی نظام به فضای سایبری، ظرفیت‌ها و مخاطرات آن
۲. درک مسئولین از تبعات تهدیدها و حملات سایبری قبلی دشمن به زیرساخت‌های کشور
۳. وجود ساختار پدافند غیر عامل سایبری برای دفاع از فضای سایبری کشور
۴. وجود ظرفیت‌های مناسب در اسناد بالادستی و حمایتی

۵. وجود سند افتا و ابلاغیات دولت در این حوزه
۶. وجود قوانین جزایی مربوط به جرایم رایانه‌ای
۷. وجود تجربیات مفید از تهدیدهای فضای سایبر در سازمان‌های نظامی، دولتی و خصوصی شکل‌گیری نسبی ساختارهای مصوب در عرصه امنیت سایبری کشور
۸. وجود ظرفیت‌های علمی، پژوهشی و صنعتی حوزه سایبری و افتا در بخش‌های دولتی و خصوصی کشور
۹. وجود رشته‌های دفاع سایبری در دانشگاه‌های کشور
۱۰. برخورداری نسبی از نیروی انسانی متعهد و متخصص در حوزه سایبری
۱۱. توانایی طراحی، تولید بومی و مهندسی معکوس نرم‌افزارها و سخت‌افزارهای پدافند سایبری
۱۲. توانایی طراحی و تولید الگوریتم‌های رمزنگاری بومی
۱۳. توانایی کشف و تحلیل آسیب‌پذیری‌های شناخته، ناشناخته در زیرساخت‌های سایبری کشور
۱۴. توانایی نسبی مقابله و پاسخ‌گویی به تهدیدهای سایبری
۱۵. وجود ظرفیت‌های ارتباطی پشتیبان برای پدافند سایبری از سرمایه‌های کشور

ضعف‌ها

۱. برخوردار نبودن از سند راه‌کاری پدافند سایبری
۲. تنوع دیدگاه‌های فرهیختگان نسبت به تهدیدهای فضای سایبری
۳. کم توجهی به استفاده از ظرفیت‌های بخش خصوصی در حوزه سایبری
۴. کمبود رشته‌ها، دروس و پایان نامه‌های دانشگاهی در حوزه تهدیدهای سایبری
۵. کندی رشد صنعت پدافند سایبری
۶. بهره‌برداری از تجهیزات غیربومی در حوزه سایبری
۷. پایین بودن سرعت رشد تجهیزات سخت‌افزاری و نرم‌افزاری بومی در فضای سایبری کشور
۸. کندی سرعت رشد دانش، فناوری، استانداردها و محصولات بومی حوزه سایبری
۹. قطع نشدن وابستگی به دانش، فناوری‌ها و استانداردهای غیر بومی در حوزه سایبری
۱۰. کمبود آزمایشگاه‌های مرجع سایبری

تهدیدها

۱. انگیزه دشمن برای تسلط بر فضای سایبری
۲. وجود راه‌کارهای تهاجمی دشمن در فضای سایبری

۳. وجود سازمان رزم سایبری در کشورهای متخاصم
۴. ساختارمند شدن تهدیدهای استکبار جهانی بر علیه ج. ا. ا. در فضای سایبری
۵. مخاطرات ناشی از به‌کارگیری بدافزارها و سلاح‌های سایبری توسط حریف
۶. تاثیرات شبکه‌های اجتماعی و فناوری‌های نوظهور دشمن در تضعیف امنیت ملی
۷. وجود شبکه‌ها و گروه‌های جاسوسی و نفوذی وابسته به دشمن در فضای سایبری
۸. توافقات و تفاهمات کشورهای متخاصم علیه ج. ا. ا.
۹. فقدان حقوق بین‌المللی عادلانه در حوزه سایبری
۱۰. بهره‌گیری دشمن از بلاتکلیفی قلمرو سایبری کشور
۱۱. تقدم راه‌کارهای جنگ سایبری نسبت به جنگ فیزیکی

فرصت‌ها

۱. امکان استفاده از ویژگی بی‌مرزی و گستردگی جهانی فضای سایبری در امر پدافند سایبری
۲. اتکای شدید دشمن به زیرساخت‌های اطلاعاتی، ارتباطی و پردازشی و سرویس‌های عمومی
۳. فعال شدن ظرفیت‌های دفاع سایبری به واسطه وجود تحریم‌ها و تهدیدها
۴. امکان بهره‌گیری از دانش و فناوری‌های نوظهور
۵. امکان ارتقا سطح همکاری‌های بین المللی و منطقه‌ای در زمینه پدافند سایبری
۶. رقابت کشورها، دولت‌ها و شرکت‌های چند ملیتی صاحب دانش و فناوری
۷. امکان همکاری‌های بین‌المللی در زمینه حقوق بین‌الملل و پیمان‌های همکاری و دفاع سایبری هم‌سو

بررسی مؤلفه‌های مؤثر در قدرت سایبری

عامل انسانی

در آفند سایبری با دو دسته عامل انسانی سروکار داریم:

بخش اول مهاجم: اغلب کارکنان و رزمندگان حاضر در آن، دارای تخصص و سوابق دیگری مثلاً امنیت، رایانه، ارتباط و رشته‌های محاسباتی و فنی هستند. نکته دیگر در این حوزه این است که برخلاف سایر رشته‌ها، اعتبارنامه‌ها و مدارک رسمی بسیار کم است. تجارب و مهارت‌ها در زمینه عملیات سایبری، در عین اهمیت بسیار زیاد، می‌توانند بسیار متفاوت باشند (سجادی اصیل، ۱۳۹۹: ۵۶).

بخش دوم جامعه هدف: بخش دوم که بخش روانی این حوزه است، در واقع شامل افرادی است که مخاطب فضای سایبر هستند و همیشه تحت‌تأثیر سناریوهای متخصصین روان‌شناسی و جامعه‌شناسی دشمن در بستر فضای سایبر قرار دارند.

به‌طورکلی مهارت‌های مورد نیاز در حوزه عملیات سایبری، به سه دسته مهارت‌های شناسایی، حمله و دفاع سایبری تقسیم می‌شود. مهارت‌های شناسایی سربازان سایبری را قادر به بررسی زیرساخت‌ها، سامانه‌ها و ترافیک می‌نماید. مهارت‌های تهاجمی بیشتر بر روی حمله تمرکز دارند و با سایر مباحث غیرامنیتی نیز هم‌پوشانی ندارند. مهارت‌های تدافعی به‌طورکلی در تمامی صنایع محاسباتی رایج هستند. این مهارت‌ها بیشتر در بخش فناوری اطلاعات وجود دارد. (Andress, 2011: 61-80).

تسلیحات سایبری

دسته‌بندی سلاح‌های سایبری به شرح زیر است.

- ✓ ابزارهای شناسایی
- ✓ ابزارهای پویش
- ✓ ابزارهای به‌دست‌آوردن دسترسی و بالابردن سطح آن
- ✓ ابزارهای خارج‌کردن غیرمجاز به اطلاعات
- ✓ ابزارهای حفظ دسترسی
- ✓ ابزارهای حمله
- ✓ ابزارهای ایجاد ابهام (سجادی اصیل، ۱۳۹۹: ۵۸-۶۰).

هنگام ارزیابی ویژگی‌های رفتاری یک سیستم، سلاح همچنین باید بتواند قابلیت اطمینان از رفتار سیستم را تضمین کند. در این راستا با ارزیابی قابلیت هدف‌گیری یک سیستم، باید بتوان با اطمینان گفت که یک سیستم آنچه را که برای او به‌عنوان هدف قرار داده شده است مورد هدف قرار می‌دهد. (Trusilo, 2021: 62)

می‌توان سلاح‌های سایبری را به دو دسته با بدنه و بدون بدنه خودمختار تقسیم کرد.

در مورد سیستم‌های دارای بدنه، وجود نوعی تجلی روباتیک، تصوری را در مورد مکان و محدودیت‌های سیستم ایجاد می‌کند. (Stoecklin, 2018: 82)

یک سیستم هوشمند دارای بدنه بر پنج محور استوار است که عبارت‌اند از: ۱. خودکامگی، ۲. استقلال از کنترل انسان، ۳. تعامل با محیط، ۴. یادگیری و ۵. تحرک. (Liivoja, 2021: 63)

پیشینه و سابقه پژوهش

نصرت‌آبادی (۱۳۹۷) در پژوهشی با عنوان ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران، منابع قدرت را منابع فیزیکی و زیرساختی، اطلاعاتی، شناختی، ماهیت قدرت را ابزار مؤثر ارعاب علیه رقبا، ابزاری راهبردی و برتر ساز، مبتنی بر فناوری‌های

مدرن، فراهم آورنده فضای نبرد آینده و پیامدهای قدرت را بازدارندگی سایبری، اشراف اطلاعاتی، برتری عملیاتی، ارتقای امنیت ملی معرفی می‌کند. در پایان عوامل مؤثر برای ارزیابی نیروهای مسلح در سه بعد آفند سایبری، پدافند سایبری و تاب‌آوری سایبری تقسیم‌بندی کرده است.

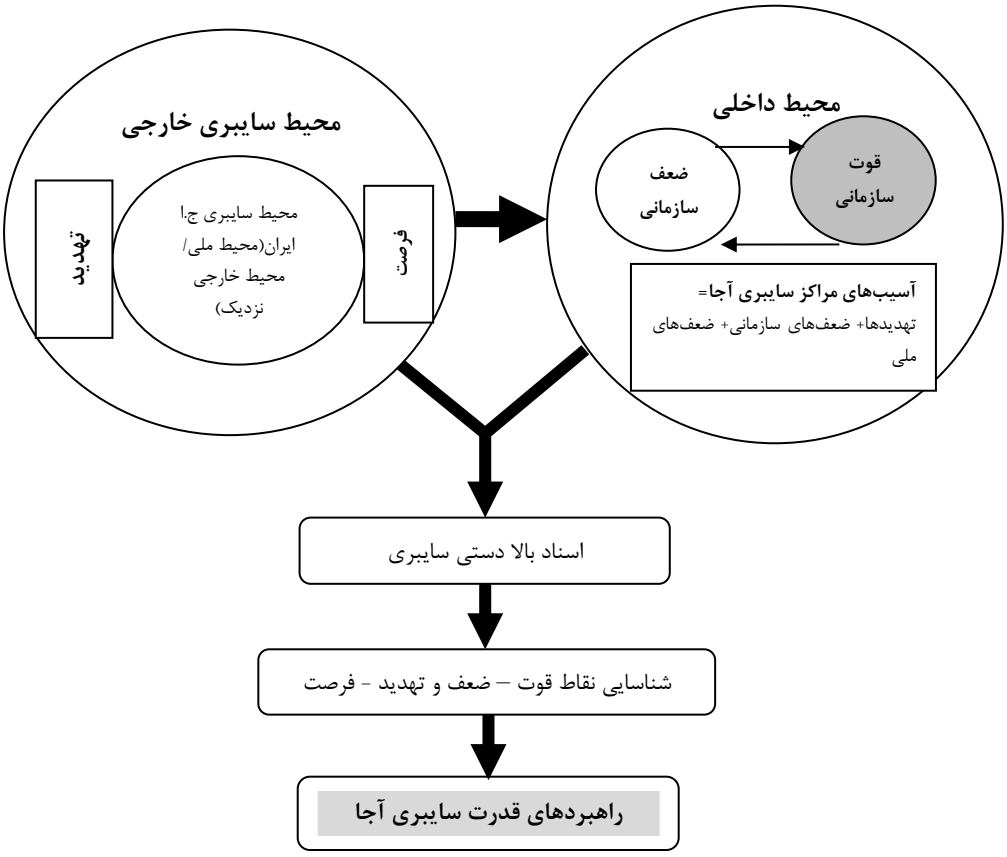
مطالعه تطبیقی راهبردهای قدرت سایبری کشورهای آمریکا، ترکیه، ناتو، کانادا، رژیم صهیونیستی، انگلیس محورهای مورد توجه گرفت و مضامین راهبردی از راهبردهای کشورهای فوق و استرالیا، کره جنوبی، اتریش، اتحادیه اروپا و چین به شرح جدول زیر جمع‌بندی شد:

جدول(۲) جمع‌بندی‌مطالعات قدرت سایبر سایر کشورها

ساختار	اقدامات	راهبرد	مأموریت	اهداف	چشم انداز	کشور
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 مردم	شاخص گذاری سلامت فضای سایبر- ایجاد زیرساخت ملی هشدار	توجه به نخبه پروری از سوی وزارت دفاع در حوزه سایبری	توجه به پدافند غیرعامل	اهداف آفندی نیز ذکرشده	پیوستگی میان چشم‌انداز و ارزش‌ها تصریح‌شده است	آمریکا
	ایجاد یک مرجع برای آگاهی‌رسانی به مردم	دولت نقش هماهنگی و همراهی راهبردها را دارد تا دخالت مستقیم		توجه ویژه به امنیت فضای کسب‌وکار و عدم ذکر سیاست‌ها ی دفاعی	توجه جدی به صنعت و اقتصاد برای امنیت ملی	انگلیس
حضور بخش خصوصی در ایجاد امنیت همراه با بخش‌های امنیتی			اصول راهنما: رهبری قوی برای مدیریت این فضا در سطح ملی	توجه به نقش جدی مردم در ایجاد امنیت		روسیه

ساختار	اقدامات	راهبرد	مأموریت	اهداف	چشم انداز	کشور
	ارزیابی ریسک و تعیین تهدیدها توسط سازمان ملی امنیت اطلاعات- توجه به مانیتورینگ محتوا	توجه به رمزنگاری و ترویج آموزش‌ها از سطوح ابتدایی- کنترل واردات رمزنگاری				ترکیه
	مدیریت ریسک همکاری بین ارتش (نیروهای مسلح) و دیگر سازمان‌های امنیتی و بخش خصوصی،	جذب سرمایه‌گذاری بودجه‌ای شرکت‌های خارجی فعال صنعت فاوا و افتا			عدم ذکر شفاف چشم‌انداز و دکترین	رژیم غاصب اسراییل
توسعه رمزنگاری ارتقاء استانداردهای راهنمای صنعت برای کیفیت عملکرد شرکت‌ها در امنیت سایبر و ارتقاء اطلاعات قابل‌دسترسی برای عموم، به‌وسیله توسعه برچسب‌های امنیتی یا نشانه‌های درجه‌بندی که به مصرف‌کننده در ارزیابی بازار کمک کند		کاهش شدید جرائم سایبری رونق بازار صنعت افتا ترویج تعامل و هماهنگی بین بازیگران بخش نظامی و غیرنظامی در اتحادیه با تأکید بر تبادل بهترین تجارب، تبادل اطلاعات و پیش‌آگاهی، پاسخ به تهدیدها، ارزیابی تهدید، بالا بردن آگاهی و قائل شدن امنیت سایبر به‌عنوان یک اولویت			اتحادیه اروپا
		ایجاد زیرساخت ملی اطلاعات در جهت امنیت سایبری- تکیه‌بر مباحث رمزنگاری خصوصاً رمزنگاری بومی- تمرکز برافزایش آگاهی عمومی				چین

مدل مفهومی تحقیق



شکل(۱) مدل مفهومی تحقیق

روش‌شناسی پژوهش

روش اجرای پژوهش توصیفی-تحلیلی است، نوع این تحقیق کاربردی است و رویکرد این تحقیق آمیخته است. صاحب‌نظران انتخاب شده 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 به‌منظور 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.

تجزیه و تحلیل عوامل داخلی مؤثر بر قدرت سایبری آجا

برای سازماندهی عوامل داخلی در قالب مقوله قوت‌ها و ضعف‌های فراروی، با استفاده از عوامل درجه‌بندی و با توجه به اهمیت هر یک از قوت‌ها و ضعف‌ها و با توجه به میزان تأثیر گذاری هر یک از آنها بر قدرت سایبری آجا، محاسبه و به شرح جدول‌های زیر تعیین گردید:

جدول (۳) عوامل داخلی(قوت‌ها)

ردیف	نقاط قوت	میانگین
۱	وجود تدابیر و فرمان‌های صادره توسط فرماندهی معظم کل قوا در خصوص حوزه‌های مختلف سایبری	۴. ۱۸
۲	برخورداری از نگاه راهبردی در سلسله‌مراتب فرماندهی در حوزه سایبری	۴. ۳۳
۳	وحدت فرماندهی در امور سایبری آجا از طریق شورای عالی سایبری	۳. ۹۶
۴	ایجاد ساختارهای سازمانی مناسب در حوزه جنگ سایبری در سطح آجا	۴. ۲۰
۵	تأسیس و توسعه مراکز علمی و پژوهشی و رشته‌های دانشگاهی مرتبط با حوزه سایبر در سطح آجا	۴. ۲۵
۶	وجود اسناد بالادستی مناسب درزمینه‌ی قدرت سایبری	۳. ۹۹
۷	زیرساخت‌های فاوایی بومی، کارآمد، گسترده و فراگیر در سطح آجا و نیروهای مسلح	۳. ۹۷
۸	برخورداری از نیروی انسانی متعهد، متخصص با تحصیلات تکمیلی درزمینه‌ی سایبری	۴. ۰۳
۹	حرفه‌ای سازی و تخصصی شدن نیروهای مسلح با برگزاری رزمایش‌های سایبری متعدد در سطح نیروهای مسلح.	۳. ۹۷
۱۰	وجود ظرفیت‌ها و قابلیت‌های لازم برای پاسخگویی سریع جهت مقابله با حملات سایبری	۳. ۶۴
۱۱	برگزاری دوره‌های مختلف آموزشی طولی و عرضی درزمینه‌ی دفاع سایبری در سطح مراکز آموزشی تخصصی آجا	۳. ۷۶
۱۲	بهره‌مندی از ظرفیت‌ها و قابلیت‌های تعاملی در مشارکت‌پذیری و ایجاد کمک‌کننده به مأموریت‌های سایبری	۴. ۰۰
۱۳	ایجاد مراکز عملیات سایبری در سطح سازمان رزم آجا	۴. ۰۷
۱۴	نظم و انضباط و اطاعت‌پذیری مؤثر سازمانی	۳. ۹۷
۱۵	تدوین و به‌کارگیری آیین‌نامه‌ها و دستورالعمل‌های مختلف درزمینه‌ی به‌کارگیری فضای سایبری در مأموریت‌های آجا	۴. ۱۶
۱۶	به‌کارگیری نظام فرماندهی و کنترل در سطح آجا	۴. ۷۶
۱۷	تولید محتوا متناسب با مأموریت‌های آجا در فضای سایبری	۴. ۰۸
۱۸	ایمن‌سازی مراکز حساس و حیاتی آجا در برابر جاسوسی، نفوذ و خرابکاری	۳. ۹۵

جدول (۴) عوامل داخلی(ضعف‌ها)

ردیف	نقاط ضعف	میانگین
۱	عدم لحاظ قدرت سایبری در قدرت رزمی آجا	۳۹ .۴
۲	متناسب و به‌روز نبودن قوانین، مقررات، آئین‌نامه‌ها، دستورالعمل‌ها و استانداردهای تخصصی و عملیاتی با تغییرات سریع و متنوع درزمینه‌ی جنگ سایبری	۲۹ .۴
۳	عدم چابکی در تولید محصولات نرم‌افزاری بومی در سطح آجا	۱۶ .۴
۴	ضعف همگرایی و هماهنگی دو حوزه سایبر در رزم و رزم سایبری جهت افزایش تاب‌آوری و بازدارندگی سایبری	۰۹ .۴
۵	عدم بهره‌گیری مناسب از تجربیات و ظرفیت‌های بخش خصوصی فعال در حوزه سایبری	۱۵ .۴
۶	نبود سازوکار مناسب برای دیده‌بانی، جست‌وجو، پویش، شناسایی، کشف و پیش‌بینی و پیشگیری بحران‌های امنیتی در حوزه سایبری	۲۰ .۴
۷	پویا نبودن ساختار، تشکیلات و سازمان‌های شغلی در سطوح مختلف متناسب با گسترش تهدیدهای سایبری	۰۷ .۴
۸	نبود رابطه مناسب بین بخش‌های تحقیقاتی و پژوهشی با سازمان‌های عملیاتی و اجرایی و ضعف در بکار گیری نتایج پژوهش‌ها در حوزه سایبر	۱۶ .۴
۹	وابستگی به دانش، فناوری و استانداردهای غیربومی و داخلی در زمینه‌های مختلف سایبری	۱۱ .۴
۱۰	کندی رشد علوم، فناوری و تحقیقات حوزه سایبری در آجا	۱۷ .۴
۱۱	نبود آزمایشگاه مرجع دفاع سایبری در آجا	۱۶ .۴
۱۲	متناسب نبودن تجهیزات و فناوری موجود آجا با نیازها و تهدیدها حوزه سایبری	۱۲ .۴
۱۳	ناکافی بودن آموزش‌های تخصصی کارکنان در خصوص سایبر در رزم	۰۷ .۴
۱۴	کمبود اعتبارات و بودجه موردنیاز در حوزه دفاع سایبری	۹۷ .۳
۱۵	ضعف در تولید علم، فکر و ابتکار در راهبردها، تاکتیک‌ها و تکنیک‌های جنگ سایبری	۳۵ .۴
۱۶	ضعف در مدیریت دانش و انتقال تجارب فنی سایبری به نسل‌های آینده	۱۵ .۴
۱۷	کمبود استانداردهای امنیتی بومی مبتنی بر استانداردهای بین‌المللی موجود برای اهداف مأموریت‌های سایبری آجا	۴۰ .۴
۱۸	عدم شناخت مناسب از ظرفیت‌ها و ضعف در رویه‌های مدیریتی و ابزارهای انگیزشی لازم برای بهره‌گیری از متخصصان سایبری در آجا	۰۹ .۴

برای سازماندهی عوامل خارجی در قالب مقوله فرصت‌ها و تهدیدهای فراروی، با استفاده از عوامل درجه‌بندی و با توجه به اهمیت هر یک از فرصت‌ها و تهدیدها و با توجه به میزان تأثیر گذاری هر یک از آنها بر قدرت سایبری آجا، محاسبه و به شرح جدول‌های زیر تعیین گردید:

جدول (۵) عوامل خارجی(فرصت‌ها)

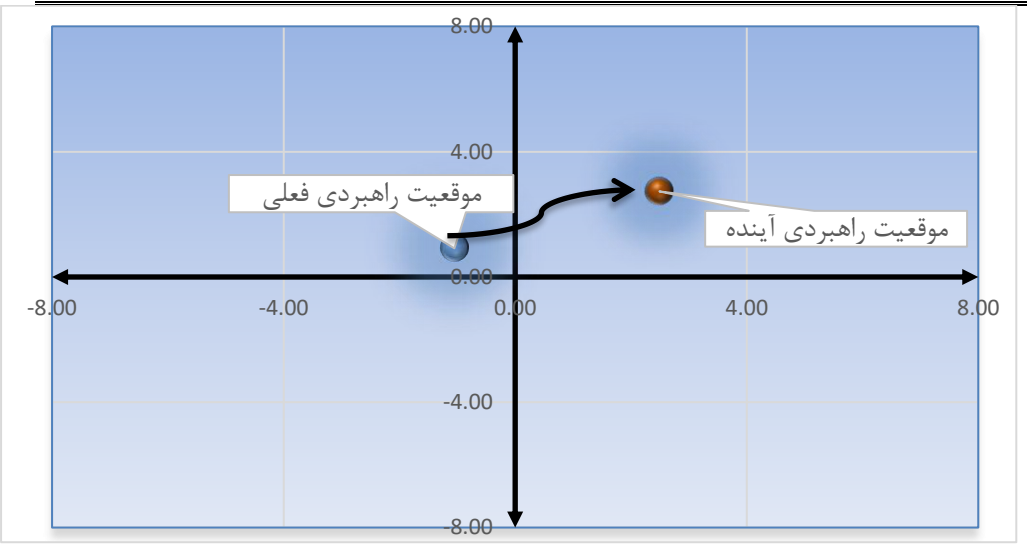
ردیف	فرصت‌ها	میانگین
۱	گستردگی جهانی و دسترسی بدون مرز برای عملیات جمع‌آوری، پدافندی و آفندی	۵۲ .۳
۲	ایجاد شورای عالی فضای مجازی در کشور	۵۸ .۴
۳	وابستگی شدید دشمن به زیرساخت‌ها و ابزارهای ارتباطی و قابلیت نفوذ بر آن	۰۸ .۴
۴	حمایت فرماندهی معظم کل قوا	۶۸ .۴
۵	وجود ظرفیت‌ها و قابلیت‌های سایر کشورهای دوست در انجام عملیات مشترک سایبری.	۳۷ .۳
۶	برخورداری از نیروی انسانی ولایتمدار، انقلابی، باهوش جوان، متخصص و تحصیل‌کرده در زمینه‌ی سایبر در سطح کشور	۱۱ .۴
۷	حمایت مسئولین ستاد کل و قرارگاه سایبری قرارگاه مرکزی حضرت خاتم (ص) از اقدامات قانونی آجا در حوزه قدرت سایبری	۹۳ .۳
۸	امکان استفاده و بهره‌برداری از مراکز علمی و پژوهش کشور و خارج از کشور جهت تعریف و اجرای پروژه‌های تحقیقاتی و پژوهشی و صنعتی موردنیاز درزمینه‌ی قدرت سایبری	۰۳ .۴
۹	وجود اسناد راهبردی، قوانین و مقررات متعدد مرتبط با فضای سایبری در سطح کشور	۷۹ .۳
۱۰	وجود زیرساخت ارتباطی مناسب مربوط به فناوری اطلاعات و ارتباطات در سطح کشور	۳۳ .۴
۱۱	افزایش سهم فضای سایبری در حفظ سرمایه‌های اجتماعی	۲۳ .۴
۱۲	اقبال ظرفیت‌های علمی، نخبگان و خبرگان برای تعامل و نقش‌آفرینی در حوزه سایبری	۶۱ .۳
۱۳	وجود شرکت‌های تخصصی سایبری در وزارت دفاع و پشتیبانی نیروهای مسلح	۸۲ .۳
۱۴	افزایش سواد رسانه‌ای جامعه نسبت به فضای سایبری و تهدیدهای آن	۵۶ .۴
۱۵	تولید محتوای مناسب و متناسب با آرمان‌های انقلاب اسلامی و فرهنگ اسلامی- ایرانی در فضای سایبری توسط افسران جنگ نرم کشور	۲۸ .۳
۱۶	ظرفیت‌های سایبری آموزشی، تحقیقاتی و عملیاتی در سطح ن. م	۵۸ .۴

جدول (۶) عوامل خارجی(تهدیدها)

ردیف	تهدیدها	میانگین
۱	توانمندی‌ها و قابلیت‌های دشمنان در بهره‌گیری از فناوری‌های برتری ساز در جنگ سایبری	۰۴ .۴
۲	سازمان‌دهی تهدیدهای سایبری از سوی دشمن و ایجاد و گسترش تهاجم‌ها در فضای سایبر در رزم و رزم سایبری	۲۴ .۴
۳	بلاتکلیفی فضای سایبری کشور و وجود مراکز متعدد تصمیم‌گیری	۲۳ .۴
۴	کمبود فناوری‌ها و تجهیزات فناورانه بومی در حوزه سایبر	۳۰ .۳
۵	برخورداری دشمنان از ساختارها و سازمان‌های گسترده، منسجم و یکپارچه رزمی درزمینه‌ی جنگ سایبری	۵۳ .۳
۶	بهره‌برداری حداکثری دشمنان از شبکه‌های اجتماعی فضای سایبری در عملیات روانی و جنگ نرم علیه نظام مقدس جمهوری اسلامی ایران	۳۶ .۳
۷	وابستگی روزافزون فعالیت‌های اجرایی به فضای سایبری غیربومی	۸۳ .۴
۸	ضعف قوانین و مقررات بین‌المللی در زمینه‌ی حملات سایبری	۵۹ .۳
۹	تغییرات سریع فناوری‌های سایبری	۵۳ .۳
۱۰	قابلیت دشمن در استفاده از تاکتیک‌ها و تکنیک‌های پیچیده سایبری	۷۵ .۳
۱۱	شکست‌های حفاظتی سایبری کارکنان	۸۱ .۳
۱۲	پیامدهای نامطلوب ناشی از حکمرانی نظام‌های بین‌المللی در موضوعات سایبری و مالکیت معنوی	۲۴ .۴

ارزیابی موقعیت و اقدام راهبردی آینده آجا

بر اساس ارزیابی کمی و کیفی عوامل داخلی و محیطی وضعیت و موقعیت اقدام راهبردی آجا در شرایط حال در محافظه‌کارانه و آینده تهاجمی مطابق شکل زیر است:



شکل (۲) موقعیت و اقدام راهبردی آینده آجا

تشکیل جدول SWOT و تعیین رابطه بین عوامل محیطی مؤثر بر قدرت سایبری آجا:

جهت تدوین راهبردهای ارتقای قدرت سایبری آجا ضروری است که نقاط قوت و ضعف سایبری آجا با فرصت‌ها و تهدیدهای سایبری آجا تقابل و انطباق داده شوند. یکی از رایج‌ترین ابزارهای مواجهه و تقابل نقاط قوت و ضعف با فرصت‌ها و تهدیدها در حوزه مدیریت راهبردی ماتریس SWOT می‌باشد. راهبردها بر اساس عوامل محیطی که بیشترین رابطه را باهم دارند:

نتیجه‌گیری

در جدول زیر تلاش گردیده است عوامل داخلی و خارجی قدرت سایبری آجا با تکیه بر روش تجزیه و تحلیل S. W. O. T ارایه گردد.

جدول (۷) ماتریس عوامل S. W. O. T

عوامل داخلی / عوامل خارجی	قوّت‌ها (S)	ضعف‌ها(W)
فرصت‌ها (O)	راه کار (S. O)- توسعه‌ای	راه کار (W. O)-ترمیمی
تهدیدها (T)	راه کار (ST)-بازدارندگی(تهاجمی)	راه کار (W. T)-اصلاحی(دفاعی)

جهت تعیین راهبردهای قدرت سایبری آجا ابتدا با توجه به ماتریس‌های ماتریس SWOT و IE راهبردهای قدرت سایبری آجا تدوین گردیده است. سپس بر اساس ماتریس برنامه‌ریزی راهبردی کمی، راهبردهای اولویت‌دار انتخاب گردیدند. جدول زیر راهبردهای اولویت‌دار قدرت سایبری آجا را نشان می‌دهد.

توضیح اینکه برابر نظر صاحب‌نظران و نویسندگان کتب و منابع تدوین راهبرد توصیه گردیده است که محقق صرفاً با توجه به نقطه راهبردی سازمان راهبردهای مربوط به همان منطقه را تدوین نماید، در این تحقیق با اجماع نظر و خواسته خبرگان تحقیق نظر به اهمیت توجه به کلیه تهدیدها و نقاط ضعف پیرامونی ۱۵راهبرد با اولویت بالا مشخص‌شده و مدنظر قرار گرفت.

جدول (۸) راهبردهای قدرت سایبری آجا

ردیف	نوع راهبرد	اولویت‌بندی راهبردها
۱	:(SO)۱	توسعه نظریه، دکترین و راهبردهای بلندمدت قدرت سایبری آجا با بهره‌گیری از ظرفیت‌های علمی و نیروی انسانی متعهد و متخصص درزمینه‌ی سایبری مبتنی بر دانش، علوم و فناوری‌های روز
۲	:(SO)۲	توسعه ظرفیت شورای عالی سایبری آجا در راستای عمق‌بخشی به هدایت، کنترل و نظارت بر اقدامات سایبری به‌منظور دستیابی به هماهنگی‌های فراگیر در انجام وظایف سایبری نیروهای تابعه آجا
۳	:(ST)۱	شبکه‌سازی هسته‌های مردمی و آماده‌سازی آن‌ها در راستای اقدامات عملیاتی، پدافندی، دفاعی، شناختی به‌منظور توسعه قابلیت سایبری آجا
۴	:(ST)۲	توسعه و یکپارچه‌سازی زیرساخت‌های اطلاعاتی امن و پایدار آجا به‌منظور صیانت از منابع سایبری آجا
۵	:(WT)۱	توسعه پروژه‌های کلان سایبری به‌منظور کسب قله‌های علم و فناوری جهت مقابله با راهبردهای تهاجمی دشمنان علیه نظام مقدس ج.ا در فضای سایبری
۶	:(WT)۳	متناسب‌سازی تجهیزات و فناوری‌ها و تکنیک‌های جنگ سایبری (سامانه‌های سایبری و سایبر پایه) در هر یک از حوزه‌های عملیاتی آجا (اعم از حوزه‌های فاوا، جنگال، شبکه‌های راداری، جنگنده‌ها، هواپیماهای ترابری، پهپادها، بالگردها، موشک‌ها، ناوها، ناوچه‌ها، زیردریایی، مهمات هوشمند) به‌منظور مقابله با فناوری‌ها و تجهیزات گسترده، منسجم و یکپارچه رزمی دشمن در حوزه نبرد سایبری
۷	(SO)5	ظرفیت‌سازی برای بهره‌گیری از تعامل و مشارکت سازمان‌های فعال کشوری و کشورهای دوست برای مقابله و اقدام سایبری علیه دشمنان
۸	:(SO)۳	توسعه ساختار سازمان سایبری آجا به‌منظور ظرفیت‌سازی انجام اقدامات رزم سایبری، سایبر در رزم و اشراف اطلاعاتی متناسب با مأموریت‌های سایبری آجا
۹	(SO)6	توسعه و کارآمدی مراکز علمی تحقیقاتی آجا در حوزه سایبر به‌منظور دستیابی به محصولات و سامانه‌های برتر ساز و کلیدی از طریق تعامل و همکاری با مراکز تحقیقاتی نیروهای مسلح، ملی و بین‌المللی
۱۰	:(ST)۳	توسعه ظرفیت‌های شورای عالی سایبری آجا در تعامل با قرارگاه سایبری س. ک ن. م به‌منظور یکپارچه‌سازی نظام تصمیم‌گیری و فرماندهی و کنترل سایبری آجا
۱۱	:(WT)۲	استفاده از ظرفیت‌های توانمند و متعهد مردمی در راستای ارتقاء توان، آمادگی و بهره‌وری جنگ شناختی و اشرافیت اطلاعاتی جهت افزایش قدرت نرم کشور.
۱۲	:(WO)۲	استفاده از ظرفیت شورای عالی سایبری آجا به‌منظور تلفیق قدرت سخت و قدرت نرم آجا در

ردیف	نوع راهبرد	اولویت‌بندی راهبردها
		محاسبه قدرت رزمی ارتش و عمق‌بخشی به سایبر در رزم و رزم سایبری
۱۳	(WO)۴:	بهره‌گیری از ظرفیت‌های همکاری و تعامل با کشورهای دوست و توانمندی‌های علمی- فنی موجود در سطح کشور به‌منظور بومی‌سازی و متناسب‌سازی تجهیزات و فناوری موجود آجا با نیازها و تهدیدهای حوزه سایبری
۱۴	(SO)۴:	توسعه مرکز عملیات سایبری در سطح آجا با تکیه‌بر ظرفیت‌های سایبری کشور به‌منظور رفع نیازهای عملیاتی آجا در حوزه‌های رزم سایبری، سایبر در رزم و اشراف اطلاعاتی.
۱۵	(WO)۱:	استفاده از ظرفیت‌های علمی- تحقیقاتی و آموزشی به‌منظور توسعه استانداردهای امنیتی مرجع درزمینه‌ی رزم سایبری و سایبر در رزم و اشراف اطلاعاتی

قدردانی

نویسندگان بر خود لازم می‌دانند از همه عزیزانی که با مشاوره خود نویسندگان را یاری نمودند مراتب تشکر و قدردانی خود را اعلام نمایند.

منابع

- احمدی، سیروس، (۱۳۹۹)، *نبرد سایبری کالبدشکافی امنیت جهانی*، چاپ اول، تهران، انتشارات دافوس.
- اکبری، حمید، و دیگران، (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)، ۷۷-۹۴.
- آذر، داود، ملکی، علیرضا، (۱۳۹۸)، *جنگ سایبر و راه‌های مقابله با حملات سایبری*، تهران، انتشارات دافوس.
- *حکم مقام معظم رهبری در تشکیل شورای عالی فضای مجازی کشور* ،دوره دوم، سال ۹۴.
- داداش‌تبار احمدی، کوروش، و دیگران، (۱۳۹۳)، ارائه یک معماری جدید برای تجسم اثرات حملات سایبری مبتنی بر ادغام اطلاعات سطح بالا در فرماندهی و کنترل سایبری، *مجله علمی – پژوهشی پدافند الکترونیکی و سایبری*، ۲(۱)، ۱-۱۴.
- ربیعی، بهزاد، و دیگران، (۱۳۹۹)، معرفی الگویی برای اندازه‌گیری و ارزیابی قدرت سایبری یک سازمان دفاعی در ج. ا. ایران، *فصلنامه علمی راهبرد دفاعی*، سال هجدهم، ۶۹، ۱-۲۸.
- رشیدی، علی جبار، (۱۳۹۶)، *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)، ۴۷-۷۴.
- سجادی اصیل، وحید، آذر، داود، (۱۳۹۹)، *عملیات سایبری در طرح‌ها و برنامه‌های وزارت دفاع آمریکا*، تهران، انتشارات دافوس آجا.
- *سند جامع سایبری نیروهای مسلح، تدوین‌کننده معاونت علوم تحقیقات و فناوری ستاد کل نیروهای مسلح*، اداره علوم سایبری و هوش مصنوعی، اسفندماه ۱۳۹۲.
- *سند راهبردی پدافند سایبری کشور، سازمان پدافند غیرعامل کشور و مرکز پدافند سایبری کشور*، ۱۳۹۴.
- شوشیان، کیانوش و دیگران، (۱۳۹۹)، مدل‌سازی حملات سایبری مبهم مبتنی بر فن جایگزین حمله، *نشریه علمی پدافند الکترونیکی و سایبری*، ۸(۱) ۱، ۶۷-۷۷.
- *قانون ارتش جمهوری اسلامی ایران*، مجلس شورای اسلامی، شماره انتشار ۱۲۴۴۱، تاریخ تصویب ۱۳۶۶/۰۷/۰۱.
- مسلمی، حسین و همکاران، (۱۳۹۴)، چگونگی ارتقای استفاده مطلوب آجا از فضای سایبر در پشتیبانی از مأموریت‌های مصرحه، *گروه مطالعاتی شماره ۶*، دافوس آجا.

- نصرت‌آبادی، جمشید، و دیگران، (۱۳۹۷)، ارائه الگوی ارزیابی قدرت سایبری ارتش جمهوری اسلامی ایران، *فصلنامه علمی - پژوهشی امنیت ملی*، دانشگاه عالی دفاع ملی، ۸(۲)، ۱۷۳-۱۹۸.

- Andress, Jason, Winterfeild, Steve (2011). *Cyber warfare Teechniques. Tactics and Tools for Security practitioner*s. 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. 6(1).