آینده‌پژوهی دفاعی، سال ششم، شماره ۲۳، زمستان ۱۴۰۰

تاریخ دریافت: ۱۴۰۰/۰۶/۲۷ تاریخ پذیرش: ۱۴۰۰/۱۱/۳۰

از صفحه ۱۵۳ تا صفحه ۱۷۶

تدوین راهبردهای دفاع سایبری کشور در برابر تهدیدهای آتی دشمن در افق چشم‌انداز ۱۴۰۵

نوع مقاله: پژوهشی

محمد سپهری*[۱]

چکیده

تهدیدهای سایبری طی سال‌های اخیر بر علیه جمهوری اسلامی ایران از روند رو به رشدی برخوردار شده است. فضای سایبری، اگر چه پس از زمین، دریا، هوا و فضا، به عنوان بعد پنجم نبردهای نظامی در نظر گرفته شده، لیکن بواسطه برخورداری از تفاوت‌های عمده‌ای همچون؛ تغییرات بسیار سریع، گسترده و مداومِ، گمنامی کاربران، بی‌مرزی، آشوبناکی و ترکیب آن با سایر ابعاد جنگ‌ها، نسبت به سایر محیط‌های عملیاتی، از ویژگی‌های منحصر به فردی برخوردار است. هدف اصلی مقاله دستیابی به راهبردهای دفاع سایبری کشور در برابر تهدیدهای سایبری دشمن در افق چشم‌انداز ۱۴۰۵ می‌باشد که پس از ارائه مطالبی مربوط به شناخت تهدیدها و توانمندی‌های سایبری دشمن، راه کارهای لازم جهت مقابله با تهدیدهای آنان به بررسی عملکرد کشور در استفاده از فناوری‌های دفاع سایبری می‌پردازد. این پژوهش کاربردی و توسعه‌ای، روش تحقیق آن آمیخته از نوع موردی-زمینه‌ای، روش گردآوری اطلاعات اسنادی و پیمایشی و ابزار آن مصاحبه و جامعه آماری ۶۰ نفر تعیین شده که با استفاده از ماتریس SWOT جهت تجزیه و تحلیل محیط داخل و خارج و تدوین راهبردها و از نرم‌افزار TOPSIS در تعیین اولویت‌بندی راهبردهای دفاع سایبری کشور در مقابله با تهدیدهای سایبری دشمن استفاده گردیده و مهمترین راهبرد آن بومی‌سازی و هوشمندسازی سامانه‌های نرم‌افزاری و سخت‌افزاری سایبری کشور از منظر فرآیندها، نظامات، استانداردها، پروتکل‌ها، رویه‌ها و روال‌ها با استفاده از توان و ظرفیت‌های علمی دانشگاه‌ها و مراکز تحقیقاتی کشور با هدف مصون‌سازی و افزایش بازدارندگی سایبری در برابر تهدیدها و حمله‌های سایبری دشمن است.

واژه‌های کلیدی:

حمله سایبری، دفاع سایبری، جنگ سایبری، پشتیبانی سایبری، تهدیدهای سایبری.

---

[۱]. استادیار و عضو هیات علمی دانشگاه پدافند هوایی خاتم‌الانبیاء(ص).

* نویسنده مسئول: Email: sepehri377@chmail.ir

DOI: 10.22034/DFSR.2022.539210.1541

مقدمه

با پیدایش و گسترش سریع فضای سایبر و اتکاء روزافزون کشورها به قابلیت‌های بی‌شمار آن، روز به روز به تهدیدها، آسیب‌پذیری‌ها و جرایم این فضا نیز افزوده شده و جنگ بین کشورها از فضای واقعی به فضای سایبری کشیده و شکل جنگ‌ها درکنار جنگ‌های سخت به جنگ سایبری با عنوان بعد پنجم جنگ‌ها تغییر یافته است. در سال‌های اخیر اکثرکشورها اقدام به تشکیل و راه‌اندازی سازمان‌ها و واحدهای مختلف دفاع سایبری در سطوح مختلف عملیاتی، راه‌کنشی و راهبردی نمودند، جمهوری اسلامی ایران نیز اقدامات بسیار خوبی در حوزه‌های نرم افزاری و سخت‌افزاری در بخش کشوری و لشکری نموده است. فضای آشوبناک و بدون مرز فیزیکی سایبر با تمام چالش‌ها و پیچیدگی‌های موجود در آن مانند یک جریان آب شدیدی است که نمی‌توان برخلاف آن حرکت کرد. همانطور که مقام معظم رهبری(مدظله) فرمودند: "فضای مجازی واقعاً یک دنیای رو به رشدِ غیرقابل توقّف است، یعنی واقعاً آخر ندارد؛ آدم هرچه نگاه می‌کند، آن چیزِ اوّل بلا آخر، فضای مجازی است. هرچه انسان پایش می‌رود در این فضا، این همین طور ادامه دارد. این یک فرصت‌های بزرگی در اختیار هر کشوری می‌گذارد، تهدیدهایی هم در کنارش دارد؛ ما بایستی کاری کنیم که از آن فرصت‌ها حداکثر استفاده را بکنیم، از این تهدیدها تا آنجایی که ممکن است خودمان را برکنار نگه بداریم."بنابراین باید فضای سایبری را مدیریت نمود.

بنابراین مسئله‌ی اصلی و دغدغه این تحقیق مدّون نمودن راهبردهای دفاع سایبری جهت مقابله با تهدیدهای سایبری دشمن[1] می‌باشد. شناخت ساختار و توانمندی‌های سایبری دشمن در سطوح عملیاتی، راه‌کنشی و راهبردی از اهمیت بسیار بالایی برخوردار بوده و باعث ارتقاء توانمندی‌های سایبری کشور، افزایش بازدارندگی،کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری سایبری، ارتقاء پایداری ملی و مصون‌سازی زیرساخت‌های سایبری کشور در برابر تهدیدهای سایبری دشمن می‌شود که در صورت نپرداختن به آن باعث غافلگیری و فلج‌سازی عملیاتی، راه‌کنشی و راهبردی، عدم رشد و توسعه فناوری‌های سایبری کشور، بالا رفتن هزینه‌های دفاعی، ضربه خوردن از نقاط آسیب‌پذیر سایبری و تصمیم‌گیری نامناسب و ناکارآمد در حوزه‌های مختلف سایبری کشور می‌شود. دستیابی به راهبردهای دفاع سایبری کشور در برابر تهدیدهای سایبری دشمن در افق چشم‌انداز ۱۴۰۵هدف اصلی، شناسایی تهدیدها، توانمندی‌های سایبری دشمن و نقاط قوت و ضعف سامانه‌های سایبری کشور از اهداف فرعی این تحقیق می باشد.

[1]. در این مقاله منظور از دشمن فقط تهدیدهای سایبری آمریکا مد نظر می‌باشد.

مبانی نظری و پیشینه‌های پژوهش

جنگ سایبری

بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری(عملیات سایبری) است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی های این نوع از تهاجم های سایبری، برای آن که دولت ها آنها را جنگ علیه منافع ملی خود تلقی نمایند.(سند پدافند سایبری کشور:۱۳۹۴، ۵)

تهدیدهای راهبردی فضای سایبر

هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از ایجاد اختلال در ارائه خدمت، تهدید راهبردی سایبری گفته می‌شود.(ملائی و همکاران: ۱۳۹۷)

حمله سایبری (تهاجم سایبری)

اقدامی سایبری که تأثیرات مختلف مانند کاهش، قطع، تخریب یا دستکاری برای منع استفاده از فضای سایبر ایجاد می‌کند و می‌تواند به صورت پنهان یا آشکار در قلمروهای فیزیکی صورت گیرد. (JP 3-12(R), 2018, II-5)

دفاع سایبری

اقداماتی که معمولاً درون فضای سایبر وزارت دفاع برای امن سازی، عملیاتی سازی و دفاع از شبکه اطلاعاتی وزارت دفاع در برابر تهدیدات خاص انجام می‌گیرد. اهداف دفاع سایبری شامل اقداماتی جلوگیری، آشکارسازی، تشخیص، مقابله و کاهش تاثیرات تهدیدات می‌باشد.(FM 3-12, 2017, 1-9)

دفاع سایبری در اسناد بالادستی

الف- مهمترین اهداف کلان دفاع سایبری کشور در سند راهبردی پدافند سایبری عبارتند از:

۱. طراحی، پیاده‌سازی و اجرای نظام پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه به لایه، بومی، پیشگیرانه، شبکه‌ای، گسترش یافته و سلسله مراتبی، چابک و منعطف در سطح ملی، منطقه‌ای و استانی.

۲. ارتقای آمادگی دفاعی و بازدارندگی کشور در مقابل تهدیدات و حملات سایبری کشورهای متخاصم.

۳. طراحی، پیاده سازی و اجرای سامانه جامع رصد، پایش، مراقبت، کنترل و تشخیص و هشدار تهدیدات سایبری.

۴. طراحی، پیاده‌سازی و اجرای نظام جامع فرماندهی وکنترل یکپارچه و هوشمند پدافند سایبری.
۵. حفاظت، صیانت و پایدارسازی سرمایه‌های سایبری کشور درمقابل تهدیدات و حملات سایبری دشمنان.
۶. ارتقاء توانمندی فرماندهی و کنترل و مدیریت بحران سایبری در راستای تضمین تداوم خدمت رسانی ضروری به مردم و دستگاه‌های حیاتی و بازیابی و ضعیت عادی.
۷. آموزش، تربیت و توانمندسازی سرمایه‌های انسانی کارآمد متناسب با اقتضائات حال و آینده پدافند سایبری.
۸. تولید، مدیریت و بومی سازی دانش پدافند سایبری با بکارگیری ظرفیت‌های ملی.
۹. سازماندهی، آموزش، هدایت، کنترل و ارزیابی مداوم دستگاه‌های کشور در راستای ارتقای کارآیی دفاعی و نیل به بازدارندگی پدافندی از طریق فعال‌سازی قرارگاه پدافند سایبری.
۱۰. تعامل بین المللی در حوزه پدافند سایبری در چارچوب سیاست ها، مقررات و قوانین ابلاغی.
۱۱. ایجاد، استقرار، پیاده‌سازی و راهبری نظام دفاع حقوقی و قانونی از منافع ملی کشور در حوزه سایبری.
۱۲. فرهنگ‌سازی، آموزش عمومی، سازماندهی، تمرین و رزمایش و تولید آمادگی پدافند سایبری در دستگاه‌های اجرایی.
۱۳. طراحی، پیاده‌سازی و اجرای سامانه امن و پایدار خدمات سایبری به زیرساخت‌های حیاتی و حساس کشور در راستای مصونیت بخشی کامل به آنها. (سند راهبردی پدافند سایبری کشور۱۳۹۴ : ۱۵-۱۶)

ب- نظام جامع فناوری اطلاعات کشور(سند راهبردی امنیت فضای تولید و تبادل اطلاعات و ارتباطات[۱])

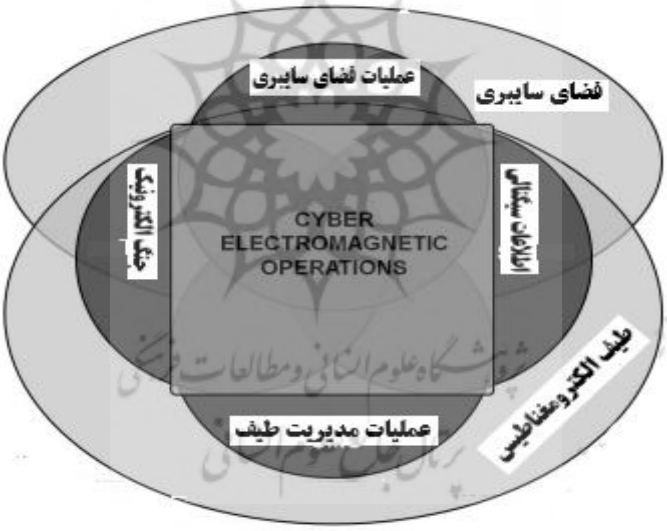
در راستای تحقق اهداف چشم انداز بیست ساله و دستیابی به جایگاه اول علمی، فناوری و اقتصادی منطقه و استمرار جامعه دانش پایه و دانایی محور در توسعه مدیریت فناوری اطلاعات در سطح ملی با تمرکز به سیاست‌گذاری و سامان‌دهی نظام نوآوری فناوری، بیانیه ماموریت فناوری اطلاعات کشور اینگونه ترسیم خواهد شد" فراهم آوردن امکان دسترسی مناسب همه اقشار جامعه به فناوری اطلاعات و آموزش فراگیر جامعه و تربیت منابع انسانی متخصص برای بکارگیریان در همه ابعاد زندگی و ایجاد فضای رقابتی خلاق برای سازماندهی جامعه شبکه‌ای و هوشمند که موجب تغییر الگو و روند توسعه ملی از منابع پایه به دانش پایه و شهروندان

۱. افتا

مسئولیت‌پذیر بالنده در تحصیل ارزش، جهت رفع شکاف دیجیتالی ملی با جامعه جهانی گردد".(ریاضی:۱۳۸۶،۱۱)

همگرایی جنگ سایبری، جنگ الکترونیک و اطلاعات سیگنالی

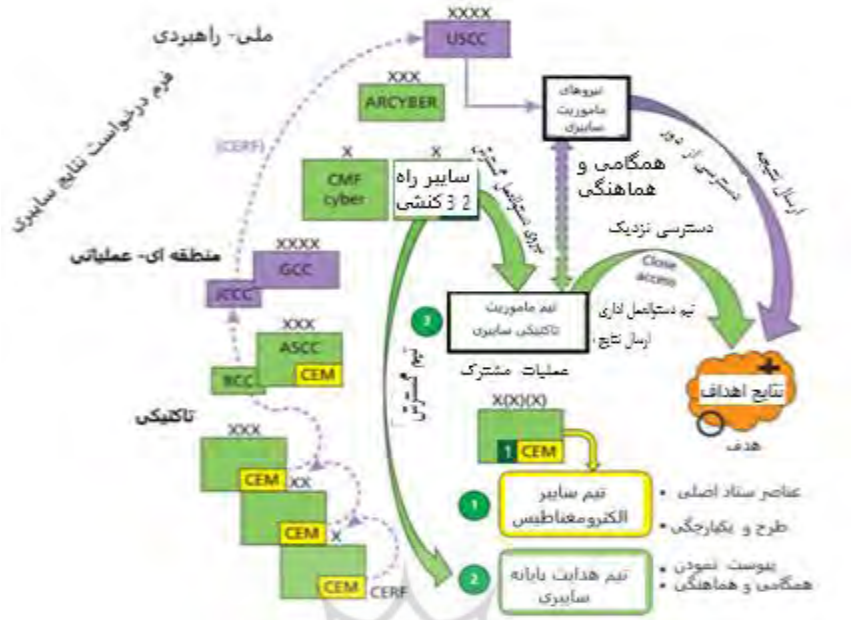
از اهداف و اولویت‌های اولیه فرماندهی سایبری ارتش آمریکا، ایجاد قابلیت سایبر الکترونیک برای تأثیرگذاری در فضای سایبری به منظور پشتیبانی از عملیات جنگ الکترونیک است که به صورت هماهنگ و هم‌زمان شده توسط سازمان رزم در منطقه عملیاتی اجرا می‌گردد. عملیات شبکه، جنگ شبکه، عملیات شبکه رایانه‌ای، برتری‌های فضائی و جنگ الکترونیک از جمله قابلیت‌های سایبرالکترونیک است که مورد توجه فرماندهان عملیات راه‌کنشی صحنه نبرد قراردارد. ایجاد یکپارچگی در مدیریت موضوعات سایبری، طیف الکترومغناطیس و اطلاعات باعث هم‌افزایی قابلیت‌های سازمان در اقدامات جنگ الکترونیک و عملیات شبکه خواهد شد. یگان‌هایی همچون فرماندهی امنیت و اطلاعات، فرماندهی شبکه[1] نیروهای مسلح و فرماندهی اعلام خطر و هشدار دهنده[2] در این فرآیند همکاری می‌نمایند.



شکل(۱) عملیات سایبری الکترونیک در ماموریت جدید سایبری امریکا (zslot, 2015)

ساختار سازمان سایبری ارتش آمریکا در سطوح راهبردی و راه‌کنشی

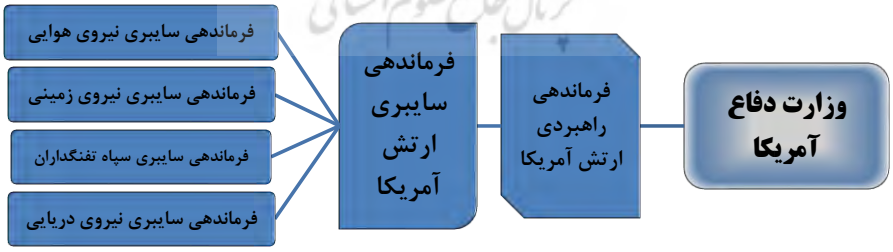
[1]. NETCOM
[2]. REDCOM



شکل (۲) ساختار سازمان سایبری ارتش آمریکا (JOINT PUBLICATION 3-13-1 :۲۰۰۷,12)

فرماندهی سایبری ارتش آمریکا

فرماندهی راهبردی نیروهای مسلح آمریکا، برای کنترل و مدیریت جنگ سایبری در زمین، هوا، فضا و دریا جهت مقابله با استفاده از مقدورات و توانمندی‌های کشورهای هدف در فضای مجازی مبادرت به سازماندهی و تشکیل یک فرماندهی، تحت عنوان فرماندهی سایبری در سطح نیروهای مسلح نموده است. فرماندهی سایبری نیروهای مسلح آمریکا متولی انجام ماموریت سایبری در نیروهای مسلح در کل جهان و مسئولیت سازماندهی، آموزش، تجهیز و اجرای خط‌مشی صادره از فرماندهی راهبردی ارتش امریکا را عهده‌دار است.



شکل (۳) ساختار فرماندهی سایبری نیروهای مسلح آمریکا(U.S ARMY CYBER COMMAND, 2011)

مهم‌ترین رویکردهای فضای سایبری در سند راهبردی آمریکا

الف- فناوری‌های شبکه‌ای، پتانسیل نیرومندی برای آینده آمریکا و جهان می‌باشد.

ب- رویکرد نظامی فضای سایبر انصراف و ممانعت می‌باشد. آمریکا در حالی حق دفاع از دارایی-های حیاتی را به عنوان سرمایه‌های ضروری خود محفوظ می‌داند که عوامل مخرب را منصرف و یا از عملکرد آن‌ها ممانعت می‌کند.

پ-آمریکا به تقویت دفاع شبکه‌ای و توانایی خود برای مقاومت و جبران اختلالات و سایر حملات، ادامه خواهد داد.

ت- در برابر آن دسته از حملات پیچیده‌ای که خسارت بار هستند، برنامه‌های واکنشی مفید و توسعه یافته‌ای را طراحی و به تفکیک و کاهش اختلال در دستگاه‌ها و محدود کردن تاثیرات در شبکه‌ها و تاثیرات متعاقب آن پرداخته می‌شود. زمانی که مجوز صادر شود، آمریکا به اقدامات در فضای مجازی پاسخ می‌دهد.

ث- منظور دفاع از کشور و هم پیمانان و شرکاء و منافع خود، حق استفاده از تمام ابزار دیپلماتیک، اطلاعاتی، نظامی و اقتصادی را مناسب و سازگار با قانون کاربردی بین‌المللی، برای خود محفوظ می‌داند. در چنین اقدامی، هر زمانی که بتوانیم تمام گزینه‌ها را پیش ازکاربرد فشار نظامی بررسی و با دقت هزینه‌ها و خطرات واکنش در مقابل هزینه‌های عدم واکنش برآورد خواهد کرد.

ج- ارتش سایبری امریکا، آمادگی برای چالش‌های امنیتی قرن۲۱، نیاز فزاینده ارتش به شبکه-های معتبر و ایمن را شناسایی و تعدیل خواهد کرد و اتحاد نظامی فعلی را برای مقابله با تهدیدات بالقوه در فضای سایبری ایجاد و افزایش خواهد داد.(همان،۱۱۴)

- **حوزه‌های مختلف تهدیدهای فضای سایبری کشور**

حوزه‌های مختلف تهدیدهای سایبری دشمن علیه کشورمان عبارت اند از:

شکل (۴) حوزه‌های تهدید فضای سایبری کشور (محمودزاده و همکار:۱۳۹۷)

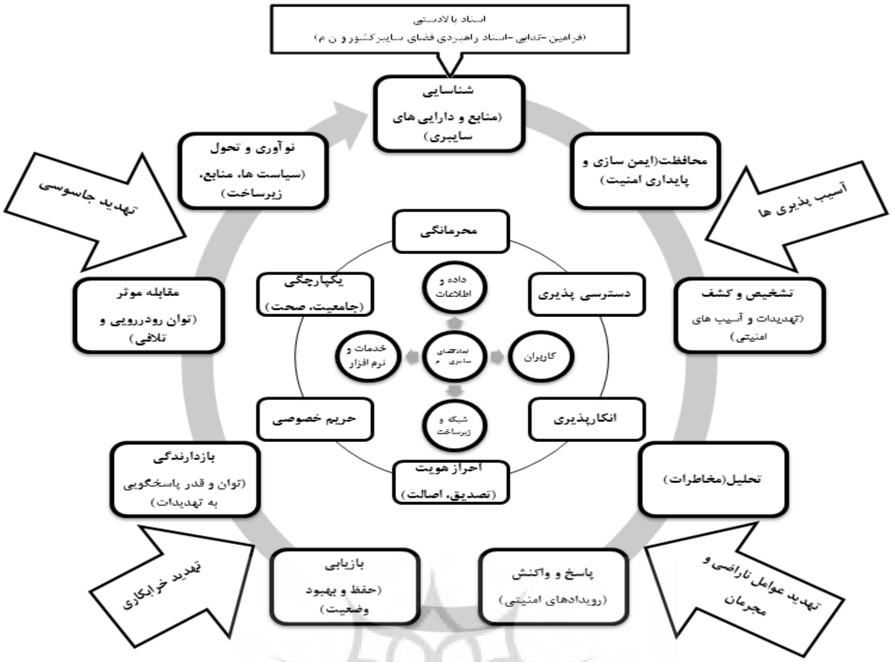
سطوح تهدیدهای سایبری کشور

سطوح تهدیدها و اقدامات موثر برعلیه سامانه‌های سایبری عبارتند از:

شکل(۵) سطوح تهدید سایبری. (پورابراهیم:۱۳۹۲، ۱۶)

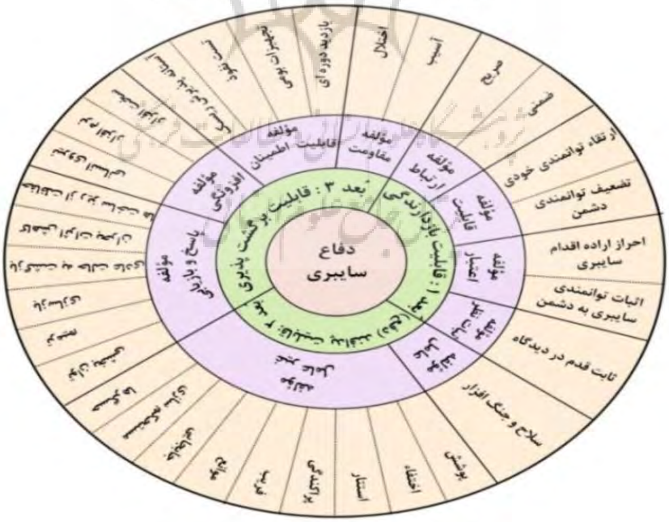
الگوی راهبردی صیانت امنیتی فضای سایبر

الگوی راهبردی صیانت امنیتی فضای سایبری کشور(نیروهای مسلح) بشرح ذیل می‌باشد:



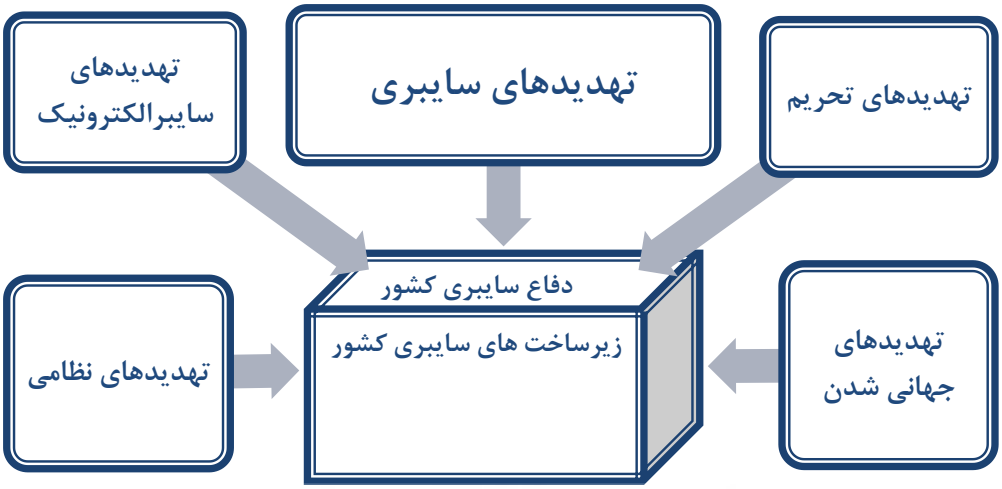
شکل(۶) الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح (محمودزاده و همکار:۱۳۹۷)

الگوی دفاع سایبری جمهوری اسلامی ایران



شکل (۷) مدل مفهومی الگوی دفاع سایبری ایران(تقی‌پور و همکار: ۱۳۹۷)

الگوی مفهومی تحقیق



شکل (۸) مدل مفهومی تحقیق

پیشینه‌های پژوهش

هرچند تحقیقات کامل و جامعی در ارتباط با تدوین راهبردهای دفاع سایبری کشور انجام نشده ولی با اینحال در چند تحقیق به بررسی ویژگی‌های دفاع سایبری پرداخته شده است. در مقاله‌ای آقای ملائی و همکاران(۱۳۹۷) به تدوین الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها با بهره‌گیری از بازی پویای علامت‌دهی با اطلاعات ناقص و تعادل نش پرداخته و راهبردهای مختلط در شش بعد و چهار مولفه اصلی و در پنج وضعیت منازعه، توازن، سلطه بازدارنده، سلطه تهدیدکننده و ضرر متقابل تدوین نموده وآقای محمودزاده و همکار(۱۳۹۷) در مقاله‌ای دیگر به تدوین الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح پرداخته که مهمترین مولفه در بُعد عوامل اصلی فضای سایبر نیروهای مسلح داده‌ها و اطلاعات، کاربران، شبکه و زیرساخت، خدمات و نرم افزار، مهم‌ترین مولفه در بُعد اهداف امنیتی فضای سایبری، محرمانگی، احراز هویت، یکپارچگی و صحت، دسترسی پذیری، انکارناپذیری و در نهایت حفاظت از حریم خصوصی سازمان و در بُعد اقدامات و راه‌کارهای صیانت امنیتی نیز مهم‌ترین مولفه‌ها؛ شناسایی منابع و دارایی‌های سایبری، محافظت، تشخیص و کشف، تحلیل، پاسخ و واکنش، بازیابی، بازدارندگی، مقابله موثر، نوآوری و تحول می‌باشد. پورابراهیمی و همکار(۱۳۹۴) در مقاله‌ی دیگری به امنیت قلب در فضای سایبر، مبانی و ارکان پرداخته که نتایج تحقیق حاکی از آن است که، غفلت سایبری، غفلت ناشی از فناوری سایبری بر زندگی و شئون مختلف آن است.

آقای احمدوند و همکار(۱۳۹۵) در مقاله‌ای به تدوین الگوی طرح دفاع سایبری در برابر تهدیدات سایبری حوزه اقتصاد پرداخته و نتیجه تحقیق حاکی از آن است که شاخص شبکه‌های بومی و امن به عنوان با ارزش‌ترین اصول، وابستگی به سامانه‌های بانکی بین‌المللی به عنوان اساسی‌ترین چالش، خرابکاری سیستم‌های نرم افزاری، سخت افزاری و داده‌ها به عنوان مهمترین تهدید، افزایش قابلیت‌های دفاعی نظام سایبری اقتصادی کشور به عنوان اصلی‌ترین راهبرد، استفاده از تحریم‌های دشمن برای تقویت اقتصاد و تولید داخلی به عنوان بهترین فرصت، وابستگی علمی سایبری در حوزه اقتصاد به خارج از کشور به عنوان مهمترین ضعف و بالاخره توسعه به کارگیری نرم افزارهای بومی در برخی زیرساخت‌های اقتصادی کشور به عنوان برترین قوت می باشند. آقای پورابراهیمی و همکار(۱۳۹۵) در مقاله‌ای دیگر به دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات جنگ روانی پرداخته و نتایج تحقیق حاکی از آن است که، هرچند تهدیدات وارده در عرصه فضای سایبری کشور در حوزه عملیات روانی، در ظاهر اقدامی نه چندان پیچیده به نظر می‌رسد، اما در صحنه عمل بسیار متفاوت و پیچیده‌تر از سایر روش‌هاست. آقای عبدالله‌خانی و همکار(۱۳۹۴) در مقاله‌ای دیگر به سنجش تهدیدات سایبری پرداخته که نتایج مقاله حاکی از آن است که با سنجش تهدیدات سایبری می‌توان توجه مسولین فضای سایبری را به قسمت‌هایی معطوف کرد که از نظر امنیتی در وضعیت مناسبی قرار نداشته و می‌توانند آسیب‌های جدی به اهداف مرجع و دارایی‌های کلیدی حوزه سایبری وارد نموده و پیامدهای خطرناکی را در پی داشته باشند.

آقای تقی‌پور و همکار(۱۳۹۷)در مقاله‌ای به طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران پرداخته که نتایج مقاله حاکی از آن است که با توجه به جایگاه خاص ایران سه مفهوم بازدارندگی، پدافند و برگشت‌پذیری به مثابه ابعاد اساسی دفاع سایبری مورد شناسایی قرار گرفته و مدل مفهومی دفاع سایبری طراحی گردیده است. آقای هلیلی و همکاران (۱۳۹۷) در مقاله‌ای دیگر به قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی پرداخته است. آقای یزادنیان و همکار(۱۳۹۶) در مقاله‌ای دیگر به متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران پرداختند و آقای فرحبخت (۱۳۹۸) در مقاله‌ای همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی پرداخته که نتایج مقاله حاکی از ادغام اقدامات جنگ‌الکترونیک و جنگ سایبری[1] و شکل‌گیری فعالیت‌های سایبرالکترونیک، قابلیت‌های جدید و ارتقاء یافته‌ای را ایجاد نموده است.

---

[1]. سایبرالکترونیک

جمع‌بندی مقالات انجام شده حاکی از آن است که تمامی تحقیق‌ها به تولید ادبیات فضای سایبری، بررسی موضوعی خاص سایبری پرداخته و یا تدوین الگوی دفاع سایبری در یک حوزه خاص پرداخته ولی هیچ یک به تدوین راهبردهای دفاع سایبری کشور در برابر تهدیدهای دشمن خاص نپرداخته که در این تحقیق به تدوین راهبردهای دفاع سایبری در سطوح مختلف کشور در برابر تهدیدات سایبری دشمن پرداخته شده است. نوآوری‌های انجام شده در این تحقیق شامل؛ تدوین راهبردهای دفاع سایبری کشور در برابر تهدیدهای آتی دشمن در افق چشم‌انداز ۱۴۰۵، تولید ادبیات دفاع سایبری کشور، احصاء نقاط قوت و ضعف سامانه‌های دفاع سایبری کشور و احصاء فرصت‌ها و تهدیدهای سامانه‌های سایبری دشمن می‌باشد.

روش‌شناسی پژوهش

این پژوهش از نظر هدف کاربردی، توسعه‌ای و روش تحقیق آمیخته از نوع موردی-زمینه‌ای، روش گردآوری اطلاعات کتابخانه‌ای با مطالعه اسناد و مدارک موجود و ابزار آن بررسی اسناد و مدارک، آرشیو، کتاب، رساله دکتری، استفاده از اطلاعات موجود در وبگاه اینترنت و مصاحبه با استفاده از پرسش‌نامه جهت اخذ نظر خبرگان می‌باشد. به منظور تجزیه و تحلیل و ارایه راهبردها از روش نوین تدوین راهبرد دیوید استفاده و سپس با استفاده از روش خبرگی عوامل محیطی(قوت، ضعف، تهدیدها و فرصت‌ها) احصاء و با استفاده از ماتریسSWOT جهت تدوین راهبرد و استفاده از نرم‌افزارTOPSIS در تعیین اولویت راهبردهای و سپس اقدام به تجزیه و تحلیل اطلاعات شده است. قلمرو زمانی پژوهش تهدیدهای پنج سال قبل تاکنون و پیشنهاداتی برای پنج سال آتی جهت افق چشم‌انداز ۱۴۰۵ می‌باشد. قلمرو مکانی زیرساخت‌های سایبری دو کشور جمهوری اسلامی ایران و آمریکا می‌باشد. جامعه آماری۶۰ نفر به صورت تمام شمار، شامل صاحب‌نظران، خبرگان و نخبگان، متخصصان، کارشناسان و اساتید دانشگاه در حوزه‌های دفاع سایبری و پدافند غیرعامل که حداقل دارای ۱۵سال سابقه اجرایی و مدیریتی و حداقل دارای مدرک تحصیلی کارشناسی ارشد(۶۹٪ دکتری و ۳۱٪ کارشناسی ارشد) می‌باشد. روایی پرسش‌نامه به تایید خبرگان و اساتید دانشگاه رسیده و پایایی آن با آزمون آلفای کُرُنباخ ۰/۸۷ بوده که نشانگر پایایی پرسش‌نامه می‌باشد.

تجزیه و تحلیل داده‌ها

ماتریس ارزیابی عوامل داخلی(IFE)

برای تحلیل محیطی با تهیه پرسش‌نامه و دریافت نقطه نظر خبرگان سایبری کشور و با توجه به عوامل اصلی و اثرگذار ماتریس مورد نظر و ارزش‌گذاری آنان نقاط قوت و ضعف خودی و فرصت‌ها و تهدیدهای دشمن به شرح ذیل احصاء گردید:

جدول(۱) نقاط قوت دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره قوت	نقاط قوت
S1	برخورداری از حمایت‌ها، تاکیدها و پشتیبانی‌های مقام معظم رهبری و سایر مسئولین نظام در حوزه‌ی دفاع سایبری کشور.
S2	وجود اسناد بالادستی(سیاست‌های کلی نظام در حوزه پدافند غیرعامل، سند راهبردی پدافند غیرعامل کشور، سند راهبردی دفاع سایبری و سند افتا و...) و امکانات و ظرفیت‌های مناسب در حوزه پدافند غیرعامل و دفاع سایبری کشور و همکاری سازمان‌های کشوری و لشکری در حوزه دفاع سایبری.
S3	وجود ساختار دفاع سایبری مناسب با تشکیل قرارگاه دفاع سایبری کشور در سازمان پدافند غیرعامل جهت رصد، پایش و مقابله با تهدیدات فضای سایبری کشور.
S4	قابلیت طراحی، ساخت و ارتقاء تجهیزات سایبری در کشور در حوزه نرم‌افزاری و سخت افزاری.
S5	وجود توان علمی، آموزشی، پژوهشی و صنعتی بسیار خوب و روند رو به رشد سایبری دانشگاه‌های نظامی و غیرنظامی کشور در طراحی، ساخت، بکارگیری و مهندسی معکوس نرم‌افزارها و سخت‌افزارهای بومی.
S6	برخورداری نسبی از نیروی انسانی متعهد و متخصص در حوزه دفاع سایبری کشور
S7	رشد و توسعه نسبی دانش و فناوری‌های نرم‌افزاری و سخت‌افزاری امنیت سایبری بومی
S8	وجود هم‌افزایی نسبی بین نخبگان نظامی و غیرنظامی در حوزه دفاع سایبری کشور.
S9	هشداردهی به سازمان‌های کشوری و لشکری از پیامدهای حملات، تهدیدات و آسیب‌های سایبری قبلی دشمن به زیرساخت‌های حیاتی، حساس و مهم کشور.
S10	فرهنگ‌سازی نسبی دفاع سایبری در سازمان‌های لشکری و کشوری به عنوان بعد پنجم جنگها.
S11	تشکیل مراکز امداد و نجات سایبری(مراکز آپا) در کشور.
S12	وجود و تشکیل شورای عالی فضای مجازی در کشور.
S13	وجود و تشکیل پلیس فتا و قوانین جزایی مربوط به جرایم و تهدیدات سایبری
S14	شکل‌گیری نسبی ساختار سازمانی دفاع سایبری در سازمان‌های لشکری، کشوری.
S15	وجود رشته‌های دفاع سایبری در مقطع کارشناسی ارشد و دکتری تخصصی در دانشگاه‌های کشور.
S16	توانایی طراحی، تولید و بکارگیری نرم افزارهای رمزنگاری بومی جهت بکارگیری در فضای سایبری کشور.
S17	توانایی کشف، شناسایی و تجزیه و تحلیل تهدیدها و آسیب پذیری‌های زیرساخت‌های حیاتی، حساس و مهم سایبری کشور.
S18	توانایی نسبی در رهگیری، شناسایی، موقعیت‌یابی و پاسخگویی سریع به تهدیدات سایبری دشمن.
S19	هم‌افزایی نسبی بین نخبگان و بخش‌های امنیتی سازمان‌های لشکری و کشوری در صیانت، پشتیبانی و دفاع از سرمایه‌های سایبری کشور (داده‌های کلان[1]، رایانش ابری[2] و...)

[1]. BIG DATA
[2]. CLOUD COMPUTING

جدول(۲) مقادیر عددی نقاط قوت دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره قوت	تطابق با عامل							وضع موجود(اهمیت)					میانگین(ضریب اهمیت)	نمره موزون عامل
	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها						
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد		
S1	۰	۲۰	۳۲	۷	۱	۲/۸۱۶۶۶	۰/۰۲۲۱۸۱	۰	۱۷	۳۲	۷	۴	۲/۹۶۶۶۶۷	۰/۰۶۵۸۰
S2	۰	۱۴	۳۶	۷	۳	۲/۹۸۳۳۳۳	۰/۰۲۳۴۹۴	۰	۲۰	۳۲	۶	۲	/۸۳۳۳۳۳ ۲	۰/۰۶۶۵۶۶
S3	۰	۱۶	۳۵	۷	۲	۲/۹۱۶۶۶۷	۰/۰۲۲۹۶۹	۰	۲۱	۳۲	۶	۱	/۷۸۳۳۳۳ ۲	۰/۰۶۳۹۳
S4	۰	۱۶	۴۰	۲	۲	۲/۸۳۳۳۳۳	۰/۰۲۲۳۱۳	۰	۲۳	۳۴	۲	۱	/۶۸۳۳۳۳ ۲	۰/۰۵۹۸۷۲
S5	۰	۶	۵۱	۲	۱	۲/۹۶۶۶۶۷	۰/۰۲۳۳۶۳	۰	۲۵	۳۱	۳	۱	۲/۶۶۶۶۶۷	۰/۰۶۲۳
S6	۰	۱۱	۴۲	۴	۳	۲/۹۸۳۳۳۳	۰/۰۲۳۴۹۴	۰	۲۱	۳۶	۲	۱	۲/۷۱۶۶۶۷	۰۶۳۸۲۵
S7	۰	۱۴	۴۴	۰	۲	۲/۸۳۳۳۳۳	۰/۰۲۲۳۱۳	۰	۱۵	۳۴	۹	۲	۲/۹۶۶۶۶۷	۰/۰۶۶۱۹۴
S8	۰	۱۲	۴۷	۰	۱	۲/۸۳۳۳۳۳	۰/۰۲۲۳۱۳	۰	۲۳	۳۵	۱	۱	۲/۶۶۶۶۶۷	۰/۰۵۹۵۰
S9	۰	۱۱	۴۱	۷	۱	۲/۹۶۶۶۶۷	۰/۰۲۳۳۶۳	۰	۱۷	۳۹	۲	۲	۲/۸۱۶۶۶۷	۰/۰۶۵۸۰۵
S10	۰	۱۰	۴۶	۲	۲	۲/۹۳۳۳۳۳	۰/۰۲۳۱۰	۰	۲۱	۳۳	۴	۲	/۷۸۳۳۳۳ ۲	۰/۰۶۴۲۹۵
S11	۰	۹	۴۸	۱	۲	۲/۹۳۳۳۳۳	۰/۰۲۳۱۱	۰	۱۹	۳۲	۷	۲	۲/۸۶۶۶۶۷	۰/۰۶۶۲۲
S12	۰	۱۱	۴۶	۰	۳	۲/۹۱۶۶۶۷	۰/۰۲۲۹۶۹	۰	۱۹	۳۴	۵	۲	/۸۳۳۳۳۳ ۲	۰/۰۶۵۰۷۹
S13	۰	۱۱	۴۶	۲	۱	۲/۸۸۳۳۳۳	۰/۰۲۲۷۰۶	۰	۲۴	۳۲	۳	۱	/۶۸۳۳۳۳ ۲	۰/۰۶۰۹۲۹
S14	۰	۱۹	۳۹	۱	۱	۲/۷۳۳۳۳۳	۰/۰۲۱۵۲۵	۰	۱۹	۳۵	۴	۲	۲/۸۱۶۶۶۷	۰/۰۶۰۶۲۹
S15	۰	۱۲	۴۵	۱	۲	۲/۸۸۳۳۳۳	۰/۰۲۲۷۰۶	۰	۲۱	۳۵	۳	۱	/۷۳۳۳۳۳ ۲	۰/۰۶۲۰۶۴
S16	۰	۱۳	۴۲	۲	۳	۲/۹۱۶۶۶۷	۰/۰۲۲۹۶۹	۰	۲۴	۳۳	۲	۱	۲/۶۶۶۶۶۷	۰/۰۶۱۲۵
S17	۰	۱۷	۴۰	۲	۱	۲/۷۸۳۳۳۳	۰/۰۲۱۹۱۹	۰	۲۰	۳۵	۳	۲	/۷۸۳۳۳۳ ۲	۰/۰۶۱۰۰۸
S18	۰	۱۳	۴۴	۱	۲	۲/۸۶۶۶۶۷	۰/۰۲۲۲۵۷	۰	۲۲	۳۴	۳	۱	۲/۷۱۶۶۶۷	۰/۰۶۱۳۲۹
S19	۰	۱۱	۴۵	۱	۳	۲/۹۳۳۳۳۳	۰/۰۲۳۱	۰	۲۴	۳۲	۳	۱	/۶۸۳۳۳۳ ۲	۰/۰۶۱۹۸۵
جمع						۵۴/۹۱۶۶۷	۰/۴۳۲۴۷۱						۵۲/۶۶۶۶۷	۱/۱۹۸۵۸۷

جدول (۳) نقاط ضعف دفاع سایبری کشور حاصل از یافته‌های تحقیق

ضعف	نقاط ضعف
W1	بومی نبودن اکثر نرم افزارها و سخت افزارها مورد استفاده در زیرساخت‌های سایبری کشور.
W2	پایین بودن سطح آگاهی و دانش دفاع سایبری مسئولین مختلف سازمان‌های کشوری، لشکری و عموم مردم.

W3	آسیب‌پذیری بودن سامانه‌های سایبری کشور در برابر انواع حملات مختلف سایبری دشمن.
W4	آسیب‌پذیری سامانه‌های سایبری کشور در برابر رهگیری و شنود سایبری دشمن.
W5	تعامل و همکاری سایبری پایین سازمان‌های کشوری و لشکری.
W6	نهادینه نشدن فرهنگ دفاع سایبری در سازمان‌های کشوری و لشکری.
W7	باور پایین اکثر مسولین سازمان‌های کشوری و لشکری نسبت به تهدیدات سایبری.
W8	همگرایی کم سازمان‌های لشکری و کشوری در زمینه دفاع سایبری کشور.
W9	رشد کم فناوری‌های دفاع سایبری پیشرفته بومی، نسبت به سایر فناوری‌ها.
W10	کمبود آزمایشگاه‌های مرجع بومی سامانه‌های مختلف سایبری در کشور.
W11	کم توجهی به سرمایه‌گذاری اندک در استفاده از ظرفیت‌های نرم افزاری و سخت‌افزاری بومی سایبری کشور .
W12	وجود تهدیدات بالقوه و بالفعل در بهره‌برداری از تجهیزات غیربومی سایبری ساخت کشورهای صاحب فناوری.
W13	روند کند طراحی، ساخت و بکارگیری تجهیزات سخت افزاری بومی سایبری در کشور.
W14	پایین بودن سرعت رشد و توسعه دانش، فناوری و استاندارد نرم افزارهای بومی در حوزه سایبری کشور.
W15	خودکفا و خوداتکا نبودن دانش، فناوری‌ها و استانداردهای نرم افزاری و سخت افزاری فضای سایبری کشور.
W16	کافی نبودن رشته‌ها، دروس، پایان‌نامه و رساله‌های دانشگاهی در حوزه‌های دانشی دفاع سایبری کشور.

جدول (۴) مقادیر عددی نقاط ضعف دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره ضعف	تطابق با عامل						وزن	وضع موجود(اهمیت)						نمره موزون عامل
	تعداد جواب‌ها					میانگین		میانگین(بر اهمیت)	تعداد جواب‌ها					
	کم خیلی	کم	متوسط	زیاد	زیاد خیلی				خیلی کم	کم	متوسط	زیاد	زیاد خیلی	
W1	۰	۰	۸	۱۰	۴۲	۴/۵۶۶۶۶۷	۰/۰۳۵۹۶۲	۴/۵۱۶۶۶۷	۰	۰	۸	۱۳	۳۹	۰/۱۶۲۴۳۲
W2	۰	۰	۵	۱۲	۴۳	۴/۶۳۳۳۳۳	۰/۰۳۶۴۸۸	/۶۸۳۳۳۳ ۴	۰	۰	۱	۱۷	۴۲	/۱۷۰۸۸۴ ۰
W3	۰	۰	۵	۲۲	۳۳	۴/۴۶۶۶۶۷	۰/۰۳۵۱۷۵	/۷۳۳۳۳۳ ۴	۰	۰	۰	۱۶	۴۴	۰/۱۶۶۴۹۶
W4	۰	۰	۷	۲۱	۳۲	۴/۴۱۶۶۶۷	**۰/۰۳۴۷۸۱**	/**۷۶۶۶۶۷** ۴	۰	۰	۱	۱۲	۴۷	/**۱۶۵۷۹۲** ۰
W5	۰	۰	۸	۲۱	۳۱	/۳۸۳۳۳۳ ۴	**۰/۰۳۴۵۱۹**	/**۵۶۶۶۶۷** ۴	۰	۰	۷	۱۲	۴۱	/**۱۵۷۶۳۷** ۰
W6	۰	۰	۷	۱۸	۳۵	/**۴۶۶۶۶۷** ۴	**۰/۰۳۵۱۷۵** ۰	/**۶۳۳۳۳۳** ۴	۰	۰	۲	۱۸	۴۰	/**۱۶۲۹۷۹** ۰
W7	۰	۰	۸	۱۸	۳۷	/**۶۸۳۳۳۳** ۴	**۰/۰۳۶۸۸۱**	/**۶۳۳۳۳۳** ۴	۰	۰	۶	۱۰	۴۴	/**۱۷۰۸۸۴** ۰
W8	۰	۰	۵	۲۱	۳۴	/**۴۸۳۳۳۳** ۴	**۰/۰۳۵۳۰۶**	/**۶۸۳۳۳۳** ۴	۰	۰	۲	۱۵	۴۳	/**۱۶۵۳۵۲** ۰
W9	۰	۰	۴	۲۴	۳۲	/**۴۶۶۶۶۷** ۴	**۰/۰۳۵۱۷۵**	/**۶۶۶۶۶۷** ۴	۰	۰	۲	۱۶	۴۲	/**۱۶۴۱۵۱** ۰
W10	۰	۰	۳	۲۰	۳۷	/**۵۶۶۶۶۷** ۴	**۰/۰۳۵۹۶۳**	/**۷۶۶۶۶۷** ۴	۰	۰	۱	۱۲	۴۷	/**۱۷۱۴۲۲** ۰
W11	۰	۰	۵	۲۱	۳۴	/**۴۸۳۳۳۳** ۴	**۰/۰۳۵۳۰۶**	/**۷۶۶۶۶۷** ۴	۰	۰	۱	۱۲	۴۷	/**۱۶۸۲۹۴** ۰

W12	۰	۰	۹	۱۷	۳۴	/۴۱۶۶۶۷	۰/۰۳۴۷۸۱	۰	۰	۱	۱۸	۴۱	/۶۶۶۶۶۷	/۱۶۲۳۱۴
W13	۰	۰	۳	۲۳	۳۴	/۵۱۶۶۶۷	۰/۰۳۵۵۶۹	۰	۰	۲	۱۲	۴۶	/۷۳۳۳۳۳	۰/۱۶۸۳۶
W14	۰	۰	۵	۱۸	۳۷	/۵۳۳۳۳۳	۰/۰۳۵۷	۰	۰	۲	۱۳	۴۵	/۷۱۶۶۶۷	/۱۶۸۳۸۶
W15	۰	۰	۴	۲۱	۳۵	/۵۱۶۶۶۷	۰/۰۳۵۵۶۹	۰	۰	۲	۱۶	۴۲	/۶۶۶۶۶۷	/۱۶۵۹۸۹
W16	۰	۰	۵	۲۲	۳۳	/۴۶۶۶۶۷	۰/۰۳۵۱۷۵	۰	۰	۴	۱۵	۴۱	/۶۱۶۶۶۷	/۱۶۲۳۹۲
جمع						۷/۰۶۶۶۷۲	۰/۵۶۷۵۲۹						۷/۸۱۶۶۷۴	/۶۵۳۷۶۳۲
جمع کل						۱۲/۹۸۳۳۶	۱						۱۲/۴۸۳۳۷	/۸۵۲۳۴۹۳

جدول(۵) خلاصه ماتریس عوامل داخلی(IFE)

عوامل محیط داخلی	میانگین موافقت	وزن عامل	میانگین وضع موجود(ضریب اهمیت)	نمره موزون
قوت‌ها	۵۴/۹۱۶۶۷	۰/۴۳۲۴۷۱	۵۲/۶۶۶۶۷	۱/۱۹۸۵۸۷
ضعف‌ها	۷۲/۰۶۶۶۷	۰/۵۶۷۵۲۹	۷۴/۸۱۶۶۷	۲/۶۵۳۷۶۳
جمع کل	۱۲۶/۹۸۳۳۴	۱	۱۲۷/۴۸۳۳۴	۳/۸۵۲۳۵

بر اساس نتایج حاصله، چون عدد ضعف‌ها بیشتر از عدد قوت‌ها می‌باشد، بنابراین که دفاع سایبری کشور در محیط داخلی با ضعف روبرو است.

ماتریس ارزیابی عوامل خارجی(EFE)

جدول(۶) نقاط فرصت دفاع سایبری کشور حاصل از یافته‌های تحقیق

فرصت	نقاط فرصت
O1	بی‌حد و مرز بودن و عدم وجود قوانین لازم و کافی جهانی در حوزه فضای سایبری.
O2	ارزان بودن هزینه سلاح های سایبری نسبت به سلاح های سخت نظامی.
O3	قابلیت مخفی ماندن و جعل هویت در فضای سایبری جهت انجام حملات سایبری به دشمن.
O4	ناهمتراز بودن شکل حملات سایبری.
O5	وابستگی بیش از حد دشمن به استفاده از فضای سایبری در کلیه فعالیت‌های نظامی و غیر نظامی.
O6	امکان رهگیری و شنود فضای سایبری دشمن با استفاده از سخت‌افزارها، نرم‌افزارها، بدافزارها و جاسوس افزارها.
O7	امکان حمله، اختلال و فریب سایبری در زیرساخت‌های حیاتی، حساس و مهم دشمن.
O8	امکان فلج‌سازی راه‌کنشی و راهبردی زیرساخت‌های حیاتی، حساس و مهم دشمن.
O9	امکان تجزیه و تحلیل و دستیابی آسان زیر ساخت‌های نرم افزاری و سخت افزاری دشمن.
O10	امکان بهره‌برداری از دانش و فناوری‌های نوظهور دفاع سایبری.
O11	گستردگی بسیار وسیع جهانی فضای سایبری و امکان دسترسی و استفاده آسان از آن در دفاع سایبری.
O12	امکان دستیابی به پروتوکل‌های ارتباطی مورد استفاده در فضای سایبری دشمن.
O13	امکان هم‌افزایی عملیاتی و راهبردی سایبری با کشورهای مسلمان و دوست برعلیه دشمن.

۴O1	هم‌افزایی و فعال سازی توانمندی‌ها و ظرفیت‌های دفاع سایبری کشور با وجود تحریم‌ها و تهدیدهای دشمن.

جدول(۷) مقادیر عددی نقاط فرصت دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره ضعف	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها					میانگین(ضریب اهمیت)	نمره موزون عامل
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد		
O_1	۰	۰	۰	۴۶	۱۴	233333/۴	۰/033585	۰	۱۵	۳۴	۱۱	۰	۲/933333	۰/098515
O_2	۰	۰	۰	۴۰	۲۰	333333/۴	۰/034378	۰	۱۱	۳۲	۱۵	۲	۳/133333	۰/107717
O_3	۰	۰	۰	۴۶	۱۴	233333/۴	۰/033585	۲	۱۲	۳۰	۱۵	۱	۳/016667	۰/101313
O_4	۰	۰	۱	۳۹	۲۰	316667/۴	۰/034246	۱	۱۶	۲۳	۱۸	۲	۳/066667	۰/10502
O_5	۰	۰	۲	۴۸	۱۰	133333/۴	۰/032791	۱	۱۳	۲۴	۱۹	۳	۳/166667	۰/103839
O_6	۰	۰	۳	۴۴	۱۳	166667/۴	۰/033056	۱	۱۵	۲۴	۱۳	۷	۳/166667	۰/104676
O_7	۰	۰	۱	۴۵	۱۴	216667/۴	۰/033452	۱۲	۱۰	۱۸	۱۷	۳	۲/816667	۰/094224
O_8	۰	۰	۲	۴۶	۱۲	166667/۴	۰/033056	۶	۸	۲۳	۲۱	۲	۳/083333	۰/101922
O_9	۰	۰	۲	۴۶	۱۲	166667/۴	۰/033056	۹	۱۱	۱۶	۲۱	۳	۲/966667	۰/098065
O_{10}	۰	۰	۳	۴۹	۸	083333/۴	۰/032395	۱۰	۳	۲۵	۲۰	۲	۳/016667	۰/097724
O_{11}	۰	۰	۱	۵۰	۹	133333/۴	۰/032791	۵	۱۰	۲۲	۲۲	۱	۳/066667	۰/10056
O_{12}	۰	۰	۲	۴۶	۱۲	166667/۴	۰/033056	۷	۱۳	۲۴	۱۳	۳	۲/866667	۰/09476
O_{13}	**0**	۰	۳	**32**	**25**	366667/۴	۰/034642	۲	**17**	**14**	۲۳	۴	۳/166667	۰/109701
O_{14}	**0**	۰	۱	**38**	**21**	333333/۴	۰/034378	۲	**16**	**15**	۲۰	۷	۳/233333	۰/111155
جمع						۵۹/05	۰/468465						۴۲/7	۱/42919

جدول(۸) نقاط تهدید دفاع سایبری کشور حاصل از یافته‌های تحقیق

تهدید	نقاط تهدید
T1	به‌کارگیری انواع مختلف حملات سایبری در کنار حمله و جنگ سخت توسط دشمن(جنگ ترکیبی).
T2	وجود تهدیدات نرم‌افزاری و سخت‌افزاری ناشی از زیر ساخت‌های بین‌المللی در بستر شبکه جهانی اینترنت.
T3	مالکیت و انحصارطلبی بیش از حد دشمن جهت تسلط نرم‌افزاری و سخت‌افزاری بر فضای سایبری جهانی.
T4	استقرار فرماندهی سایبری آمریکا در بخش‌هایی از جهان و تشکیل سازمان رزمی سایبری دشمن در قالب فرماندهی سایبری در بعضی از کشورهای همسایه ایران جهت تسلط به فضای سایبری ایران.
T5	آشوبناکی، پیچیده‌گی شیوه‌ها و روش‌های جمع‌آوری اطلاعات دشمن از طریق شبکه‌ها و گروه‌های جاسوسی و سرویس‌های اطلاعاتی نفوذی وابسته به دشمن در فضای سایبری.

T6	وابستگی زیرساخت‌های ملی، انرژی، پولی، سلامت کشور به بهره برداری از فضای سایبری
T7	بکارگیری فناوری مختلف سایبری در اکثر تسلیحات نظامی و امکان حملات سایبری بر روی آنها توسط دشمن.
T8	استفاده از سکوهای هوایی، زمینی، دریایی و فضایی هوشمند توسط دشمن جهت حمله، اختلال و شنود سایبری.
T9	بکارگیری سلاح سایبری توسط دشمن در کلیه حوزه‌ها به دلیل ارزانی و پیچیده‌گی آن.
T10	هم‌افزایی وسیع جهانی تهدیدهای دشمن در فضای سایبری بر علیه جمهوری اسلامی ایران.
T11	وجود تهدیدهای بدافزارها، باج‌افزارها و سلاح‌های سایبری دشمن بر علیه فضای سایبری ایران.
T12	فقدان حقوق و قانون بین‌المللی عادلانه در حوزه دفاع سایبری در دنیا و سوء استفاده دشمن از آن.
T13	تقدم راه‌کنشی و راهبردی جنگ سایبری نسبت به جنگ سخت و فیزیکی توسط دشمن.
T14	هم‌افزایی سایبری دشمنان با یکدیگر برعلیه زیرساخت‌های سایبری کشور.
T15	تأثیر بسیار زیاد شبکه‌های اجتماعی و فناوری‌های نوظهور دشمن در تضعیف امنیت ملی کشور.

جدول(۹) مقادیر عددی تهدیدهای دفاع سایبری کشور حاصل از یافته‌های تحقیق

شماره ضعف	تطابق با عامل							وضع موجود(اهمیت)							نمره موزون عامل
	تعداد جواب‌ها					میانگین	وزن	تعداد جواب‌ها					میانگین(نمره اهمیت)		
	خیلی کم	کم	متوسط	زیاد	خیلی زیاد			خیلی کم	کم	متوسط	زیاد	خیلی زیاد			
T1	۰	۰	۵	۲۲	۳۳	/۴۶۶۶۶۷	۰/۰۳۵۴۳۶	۰	۰	۴	۲۶	۳۰	/۴۳۳۳۳۳		/۱۵۷۰۹۸ ۰
T2	۰	۰	۶	۲۳	۳۱	/۴۱۶۶۶۷	۰/۰۳۵۰۳۹	۰	۰	۴	۲۴	۳۲	/۴۶۶۶۶۷		/۱۵۶۵۰۸ ۰
T3	۰	۰	۲	۳۱	۲۷	/۴۱۶۶۶۷	۰/۰۳۵۰۳۹	۰	۲	۳	۲۲	۳۳	/۴۳۳۳۳۳		۰/۱۵۵۳۴
T4	۰	۰	۱۰	۲۱	۲۹	/۳۱۶۶۶۷	۰/۰۳۴۲۴۶	۰	۱	۵	۲۲	۳۲	/۴۱۶۶۶۷		/۱۵۱۲۵۲ ۰
T5	۰	۰	۴	۲۳	۳۳	/۴۸۳۳۳۳	۰/۰۳۵۵۶۸	۰	۲	۴	۱۳	۴۱	۴/۵۵۰۰۰		/۱۶۱۸۳۴ ۰
T6	۰	۰	۳	۲۳	۳۴	/۵۱۶۶۶۷	۰/۰۳۵۸۳۲	۰	۰	۲	۱۸	۴۰	/۶۳۳۳۳۳		/۱۶۶۰۲۳ ۰
T7	۰	۰	۴	۲۱	۳۵	/۵۱۶۶۶۷	۰/۰۳۵۸۳۲	۰	۲	۳	۱۱	۴۴	/۶۱۶۶۶۷		/۱۶۵۴۲۶ ۰
T8	۰	۰	۴	۲۴	۳۲	/۴۶۶۶۶۷	۰/۰۳۵۴۳۶	۰	۰	۲	۱۵	۴۳	/۶۸۳۳۳۳		/۱۶۵۹۵۷ ۰
T9	۰	۰	۴	۲۷	۲۹	/۴۱۶۶۶۷	۰/۰۳۵۰۳۹	۰	۰	۲	۱۶	۴۲	/۶۶۶۶۶۷		/۱۶۳۵۱۵ ۰
T10	۰	۰	۲	۲۴	۳۴	/۵۳۳۳۳۳	۰/۰۳۵۹۶۵	۰	۰	۳	۲۳	۳۴	/۵۱۶۶۶۷		۰/۱۶۲۴۴
T11	۰	۰	۱	۲۰	۳۹	/۶۳۳۳۳۳	۰/۰۳۶۷۵۸	۰	۰	۳	۲۶	۳۱	/۴۶۶۶۶۷		/۱۶۴۱۸۵ ۰
T12	۰	۰	۸	۲۱	۳۱	/۳۸۳۳۳۳	۰/۰۳۴۷۷۵	۰	۰	۱	۱۸	۴۱	/۶۶۶۶۶۷		/۱۶۲۲۸۱ ۰
T13	۰	0	۱	20	39	/۶۳۳۳۳۳	۰/۰۳۶۷۵۸	۰	0	۲	12	46	/۷۳۳۳۳۳		/۱۷۳۹۸۷ ۰

T14	۰	۰	۷	۲۰	۳۳	/۴۳۳۳۳۳	۰/۰۳۵۱۷۱	۰	۰	۲	۲۵	۳۳	/۵۱۶۶۶۷ ۴	/۱۵۸۵۷ ۰
T15	۰	۰	۷	۲۴	۲۹	/۳۶۶۶۶۷ ۴	۰/۰۳۴۶۴۲	۰	۰	۱	۱۷	۴۲	/۶۸۳۳۳۳ ۴	/۱۶۲۲۴۲ ۰
جمع					۶۷		۰/۵۳۱۵۳۵						۶۸/۴۸۳۳۳	/۴۲۶۹۴۵ ۲
جمع کل					۱۲۶/۰۵		۱						۱۱۱/۱۸۳۳	/۸۵۶۱۳۵ ۳

جدول(۱۰) خلاصه ماتریس عوامل خارجی(EFE)

عوامل محیط داخلی	میانگین موافقت	وزن عامل	میانگین وضع موجود(ضریب اهمیت)	نمره موزون
فرصت	۵۹/۰۵	۰/۴۶۸۴۶۵	۴۲/۷	۱/۴۲۹۱۹
تهدید	67	۰/۵۳۱۵۳۵	۶۸/۴۸۳۳۳	۲/۴۲۶۹۴۵
جمع کل	۱۲۶/۰۵	۱	۱۱۱/۱۸۳۳۳	۳/۸۵۶۱۳۵

براساس نتایج حاصله، چون عدد تهدیدات بیش از عدد فرصت‌ها می‌باشد بنابراین دفاع سایبری در محیط خارجی با تهدید روبرو است.

تجزیه وتحلیل داده‌ها

جدول(۱۱) تقسیم‌بندی و تخصیص منابع دفاع سایبری

عوامل/ درصد منابع تخصیص یافته	مقادیر	درصد تخصیص منابع مورد نیاز
قــوت‌ها	۱/۱۹۸۵۸۷	۱۵/54893
ضعف‌ها	۲/۶۵۳۷۶۳	۳۴/42652
فــرصت‌ها	۱/42919	۱۸/54048
تهــدیدها	۲/۴۲۶۹۴۵	۳۱/48407
مجموع قوت‌ها و ضعف‌ها	۳/۸۵۲۳۵	۴۹/97545
مجموع فرصت‌ها و تهدیدها	۳/۸۵۶۱۳۵	۵۰/02455

ماتریس ارزیابی موقعیت و اقدام راهبردی[1] دفاع سایبری کشور

در تعیین موقعیت راهبردی و تحلیل شکاف از ماتریس IFE & EFE بدین صورت استفاده می‌شود:

[1]. Strategic Position And Action Evaluation Matrix (SPACE)

مختصات وضع موجود= (A, B)	
A = نمره موزون ضعف‌ها - نمره موزون قوت‌ها	- ۱/۴۵۵۱۸
B = نمره موزون تهدیدات- نمره موزون فرصت‌ها	-۰/99775
C = Arctg A/B	55/56°
D = زاویه نقطه مطلوب(ایده‌آل) با محور X ها	۴۵°
C+D= مقدار زاویه چرخش راهبردی از وضع موجود به وضع مطلوب =55/56° +۹۰° +۴۵° =**190/56°**	

شکل (۹) نمودار تحلیل شکاف و ارزیابی موقعیت

مقدار زاویه چرخش از وضع موجود به وضع مطلوب $190/56^{\circ}$درجه می‌باشد. بنابراین وضع موجود دفاع سایبری کشور در ناحیه تدافعی یا انفعالی قرار داشته و تهدید محور و در وضعیت ناپایداری قرار دارد و در مواجهه با تهدیدها آسیب‌پذیر می‌باشد و از نظر منابع و امکانات تخصصی با مشکل مواجه است و تاکید بر دستیابی به سامانه‌های نوین دفاع سایبری با رویکرد راه‌کارهای ناهمتراز، میانبر و خلاقانه مدنظر می‌باشد. بنابراین برای رسیدن به وضع مطلوب باید به رویکرد مقتدرانه آموزش، تحقیق، توسعه و تولید سامانه‌های نوین دفاع سایبری هوشمند و بومی به رویکرد تهاجمی یا فعال برسیم، به فرصت‌ها توجه بیشتری از قوت‌ها و به نقاط ضعف و قوت داخلی توجه بیشتری شود در این صورت دفاع سایبری به وضعیت پایدار و مطلوبی خواهد رسید.

نتیجه‌گیری و پیشنهادها

با اولویت‌بندی و تعیین مطلوبیت‌های راهبردی با استفاده از نظر ۱۵ نفر خبره و نرم افزارTOPSIS، یافته‌های تحقیق به عنوان مناسب‌ترین راهبردهای دفاع سایبری کشور در برابر تهدیدات آتی دشمن در افق چشم‌انداز ۱۴۰۵ از بین ۲۰ راهبرد در نهایت ۱۲راهبرد، به ترتیب اولویت زیر احصاء گردید:

جدول(۱۲) اولویت‌بندی و مطلوبیت راهبردهای احصاءشده

اولویت	راهبردها	مطلوبیت راهبردها	راهبردها
۱	راهبرد۳	۰/۷۳۲۳۴۵	بومی سازی و هو شمند سازی سامانه‌های نرم‌افزاری و سخت‌افزاری سایبری کشور از منظر فرآیندها، نظامات، ا ستانداردها، پروتکل‌ها، رویه‌ها و روال‌ها با ا ستفاده از توان و ظرفیت‌های علمی دانشگاه‌ها و مراکز تحقیقاتی کشور با هدف مصون‌سازی و افزایش بازدارندگی سایبری در برابر تهدیدها و حمله‌های سایبری دشمن
۲	راهبرد۱۵	۰/۶۵۲۴۳۵	تشکیل سامانه فرماندهی و کنترل هوشمند بومی سایبری با هم‌افزایی و یکپارچگی کلیه زیر ساخت‌های سایبری کشور با هدف تشخیص، هشدار، کنترل، ارزیابی و پایش تهدیدهای سایبری در سطوح عملیاتی، راه‌کنشی و راهبردی.
۳	راهبرد۷	۰/۶۴۳۲۳۹	تقویت قرارگاه دفاع سایبری کشور از طریق هم‌افزایی و توسعه مراکز رصد، پایش و اقدام تهدیدهای سایبری کشور با هدف افزایش بازدارندگی سایبری کشور.
۴	راهبرد۲	۰/۶۱۲۳۴۵	دور زدن و بی‌اثرسازی تحریم‌های سایبری کشور با استفاده از تکمیل و گسترش زیرساخت‌های بومی سایبری کشور از جمله شبکه ملی اطلاعات کشور با هدف ارتقاء قدرت سایبری کشور.
۵	راهبرد۹	۰/۵۸۵۴۳۲	نهادینه‌سازی اصول، راهبردها، ملاحظات و الزامات پدافندغیرعامل و پدافند سایبری از طریق بکارگیری در زیرساخت‌های حیاتی، حساس و مهم کشور با هدف مصون‌سازی در برابر تهدیدات.
۶	راهبرد۶	۰/۵۲۳۴۹۸	فلج‌سازی راه‌کنشی، عملیاتی و راهبردی دشمن با طرح‌ریزی و اجرای حمله، شنود و فریب سایبری سامانه‌های سایبری دشمن با هدف کسب برتری قدرت سایبری.
۷	راهبرد۸	۰/۵۱۹۸۶۵	ایمن‌سازی زیرساخت‌های سایبری کشور از طریق طراحی، ساخت و بکارگیری سامانه‌های نرم افزاری و سخت افزاری ضدشنود و ضدرهگیری هوشمند بومی با هدف تامین امنیت پایدار.
۸	راهبرد۱	۰/۴۷۷۶۵۴	طراحی، ساخت و بکارگیری سامانه‌های نرم‌افزاری و سخت‌افزاری بومی دفاع سایبری کشور با استفاده از توانمندی‌های علمی مراکز دانشگاهی و پژوهشی کشور با هدف قطع وابستگی و رسیدن به خودکفایی و خوداتکایی سایبری.
۹	راهبرد۱۱	۰/۴۵۸۹۲۳	طراحی، پیاده‌سازی و اجرای مدل‌ها و الگوهای دفاع سایبری بومی، دانش محور و پاسخگو به تهدیدهای سایبری از طریق اجرای رزمایش‌های سایبری با هدف بازدارندگی و ارتقاء پایداری ملی.

اولویت	راهبردها	مطلوبیت راهبردها	راهبردها
۱۰	راهبرد۱۴	۰/۴۳۸۷۵۴	طراحی، پیاده‌سازی و اجرای نظام حقوق بین‌الملل دفاع سایبری کشور از طریق تعامل و مشارکت بین المللی با کشورهای دوست با هدف ارتقاء منافع ملی.
۱۱	راهبرد۱۰	۰/۳۹۴۵۸۹	آموزش و فرهنگ‌سازی علوم و دانش دفاع سایبری از طریق بکارگیری در نظام آموزشی کشور در کلیه سطوح متوسطه و دانشگاهی با هدف نهادینه‌سازی دفاع جامع سایبری کشور.
۱۲	راهبرد۵	۰/۳۰۳۲۴۵	هم‌افزایی و همگرایی جنگ سایبری، جنگ الکترونیک و اطلاعات سیگنالی از طریق ساختاردهی و توسعه زیرساخت‌های میدان نبرد دیجیتالی و الکترونیکی باهدف ارتقاء اشرافیت اطلاعاتی و قدرت پاسخگویی بالا.

با توجه به عوامل احصاء شده و راهبردهای تدوین‌شده در این پژوهش، پیشنهادات اجرایی دفاع سایبری ذیل ارائه می‌گردد:

۱. اصلاح ساختار سازمانی دفاع سایبری کشور در کلیه سطوح عملیاتی، راه‌کنشی و راهبردی.
۲. آموزش و نهادینه‌سازی اصول و الزامات دفاع سایبری کشور.
۳. هم‌افزایی کلیه زیرساخت‌های سایبری کشوری و لشکری در طرح‌های آمایش دفاع سایبری کشور.
۴. بومی‌سازی و هوشمندسازی کلیه زیرساخت‌های نرم افزاری و سخت‌افزاری سایبری کشور.
۵. مصون‌سازی زیرساخت‌های حیاتی، حساس و مهم کشور با بکارگیری الزامات دفاع سایبری و پدافند غیرعامل.
۶. بکارگیری فرماندهی و کنترل سایبری هوشمند بومی در کلیه زیرساخت‌های کشور.
۷. ایمن‌سازی و مقاوم‌سازی سامانه‌های سایبری با اجرای اصول و الزامات پدافند غیرعامل.
۸. بکارگیری فناوری‌های پیشرفته دفاع سایبری در سامانه‌های ارتباطی کشور.

قدردانی

از کلیه کارشناسان و متخصصان حوزه سایبری کشور، که در تهیه و تدوین این مقاله با اینجانب همکاری نمودند کمال تشکر و امتنان را دارم. امیدوارم این مقاله مورد استفاده پژوهشگران و علاقمند این حوزه در کلیه سطوح قرار گیرد.

منابع

- احمدوند، علی محمد. رضازاده، اکبر.(۱۳۹۵).تدوین الگوی طرح دفاع سایبری در برابر تهدیدات سایبری حوزه اقتصاد. فصلنامه امنیت ملی دانشگاه عالی دفاع ملی.۶(۲۱):۶۵-۸۴.
- پورابراهیمی، ابراهیمی.کیان‌خواه، احسان.(۱۳۹۴). امنیت قلب در فضای سایبر، مبانی و ارکان. فصلنامه امنیت ملی،۵(۱۷) :۱۰۷-۱۲۶
- پورابراهیمی، علیرضا. صفرنژاد، داریوش.کاشف، حمیدرضا.(۱۳۹۵). دفاع سایبری جمهوری اسلامی ایران در برابر تهدیدات جنگ روانی. فصلنامه امنیت ملی دانشگاه عالی دفاع ملی.۶(۲۲):۱۱۹-۱۴۶ .
- پورابراهیمی، علیرضا.(۱۳۹۲). پدافند ملی سایبری، دانشگاه عالی دفاع ملی.
- تقی‌پور،رضا. اسماعیلی، علی.(۱۳۹۷).طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران .فصلنامه امنیت ملی،۸(۳۰):۱۸۱-۲۰۲.
- ریاضی، عبدالمجید.(۱۳۸۶).نظام‌جامع فناوری اطلاعات کشور. تهران. وزارت ارتباطات و فناوری اطلاعات.
- ریاضی،عبدالمجید.(۱۳۸۶). نظام جامع فناوری اطلاعات کشور(سند راهبردی) تهران.
- سندراهبردی پدافند سایبری کشور.(۱۳۹۴).سازمان پدافند غیرعامل کشور و مرکز پدافندسایبری کشور.
- عبدالله‌خانی، علی. حسینی، پرویز.(۱۳۹۴). سنجش تهدیدات سایبری سنجش تهدیدات سایبری، فصلنامه امنیت ملی دانشگاه عالی دفاع ملی.۴(۱۶):۴۵-۸۰.
- فرحبخت، احمدرضا. دهقانی، مهدی.(۱۳۹۸).الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح. فصلنامه امنیت ملی،۹(۳۱):۱۹۹-۲۱۹.
- محمودزاده،ابراهیم، اسماعیلی، کیوان.(۱۳۹۷). الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح، دانشگاه عالی دفاع ملی، فصلنامه امنیت ملی، ۸ (۳۰):۲۰۳-۲۳۷.
- ملائی، علی. کارگری، مهرداد. خراشادی زاده، محمدرضا.(۱۳۹۷). الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها.فصلنامه امنیت ملی دانشگاه عالی دفاع ملی،۸(۲۹):۱۴۱-۱۷۱.
- هلیلی، خداداد. ولوی، محمدرضا، موحدی‌صفت، محمدرضا. باقری، مسعود. (۱۳۹۷). قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر. فصلنامه امنیت ملی دانشگاه عالی دفاع ملی، ۸(۲۹):۱۷۳-۲۰۰.
- یزادنیان، حمید.جلال، غلامرضا.(۱۳۹۶). متغیرهای کلیدی منابع انسانی در تقویت دفاع سایبری جمهوری اسلامی ایران. فصلنامه علمی پژوهشی امنیت ملی،۷(۲۶):۱۲۷-۱۴۲.
- WWW.Khamenei.Ir- ۸۹/۱۱/۳۰

- Joint Publicatioon 3-13-1. (2007).Electronic Warfare. , U.S.Army, 25 Juanery.
- JP 3-12. (2018). Cyberspace Operations, U.S. Army, 8 june,
- FM 3-12.(2021). Cyberspace Operation and Electronicmagnetic Warfare Operations, U.S. Army.
- Zsolt, Haig. (2015). Electronic Warfare in Cyberspace, Faculty of Military Sciences and Officer Training National University of Public Service, Budapest, Hungary.p6.