آینده‌پژوهی دفاعی، سال ششم، شماره ۲۰، بهار ۱۴۰۰

تاریخ دریافت: ۱۳۹۹/۱۱/۰۸ تاریخ پذیرش: ۱۴۰۰/۰۳/۲۶

از صفحه ۵۹ تا صفحه ۸۱

بررسی قدرت پدافند سایبری نیروهای مسلح با روش برنامه‌ریزی مبتنی بر سناریو

مجتبی رمضان‌زاده*[۱]
مجید غیوری ثالث[۲]
علی‌محمد احمدوند[۳]
محسن آقایی[۴]
ابراهیم نظری فرخی[۵]

نوع مقاله: پژوهشی

چکیده

شناخت صحیح و ورود به‌موقع در عرصه‌های نوین دفاعی، همواره یکی از دغدغه‌های طراحان و بازیگران حوزه جنگ‌های سایبری است. ارزیابی قدرت سایبری و شناخت نقاط ضعف و آسیب‌پذیری‌ها به‌منظور پیشگیری از غافلگیری در عرصه جنگ‌های آینده از اهمیت بسزایی برخوردار است. در پژوهش حاضر، با نگاهی جامع و آینده‌نگرانه، ابعاد و مؤلفه‌های قدرت سایبری در بُعد پدافند سایبری نیروهای مسلح مطالعه و سناریوهایی برای ارزیابی قدرت سایبری نیروهای مسلح، ارائه گردید. هدف از انجام این پژوهش، ارزیابی قدرت سایبری نیروهای مسلح در بُعد پدافند سایبری است. جامعه آماری شامل ۲۰ نفر از خبرگان حوزه سایبر نیروهای مسلح است. نوع پژوهش، کاربردی است. روش پژوهش با استفاده از رویکرد آینده‌پژوهی و مبتنی بر روش سناریو، انجام‌شده است. نتیجه آنکه رویکرد پدافند سایبری دارای مؤلفه‌های چهارگانه شامل: بستر پدافندی، دیپلماسی سایبری، عامل انسانی و افزارها است. همچنین، مؤلفه عامل انسانی، از اولویت بالاتری نسبت به سایر مؤلفه‌ها برخوردار است. پیشنهاد می‌شود، معاونت فاوای نیروهای مسلح، نسبت به ارزیابی قدرت سایبری با تأکید بر بعد آفند سایبری و در قالب پژوهشی مجزا، اقدام نماید.

واژه‌های کلیدی:

قدرت سایبری، پدافند سایبری، جنگ آینده، آینده‌پژوهی، سناریو، نیروهای مسلح.

---

[۱]. دانشجوی دکتری امنیت سایبر، دانشگاه عالی دفاع ملی و تحقیقات راهبردی

[۲]. استادیار دانشگاه امام حسین علیه‌السلام(ع)

[۳]. استادیار دانشگاه امام حسین علیه‌السلام(ع)

[۴]. استادیار دانشگاه عالی دفاع ملی و تحقیقات راهبردی

[۵]. استادیار دانشگاه افسری امام علی علیه‌السلام(ع)

* نویسنده مسئول: Email: Bmr.98@yahoo.com

مقدمه

سازمان‌ها به زیرساخت‌های فناوری اطلاعات و محیط سایبری وابستگی شدیدی دارند و نفوذ، خرابکاری و افشای اطلاعات سازمان‌ها هزینه‌های زیادی در پی خواهد داشت، درنتیجه امن سازی این محیط بسیار ضروری است. یکی از مسائل در شناسایی نقاط آسیب‌پذیر مشکلات اجرایی آزمون نفوذ مانند هزینه‌بر بودن، احتمال ایجاد اختلال در سرویس‌دهی و عدم اعتماد کامل به شرکت‌های اجراکننده آزمون نفوذ است (نصرت‌آبادی، ۱۳۹۷). آنچه در زمینه کنترل فضای سایبر، چالش‌برانگیز است تفاوت ماهوی آن با دنیای واقعی است و همین امر هم کار را بر دولتمردان سخت می‌کند. بخش مهمی از ظرفیت‌های دولت‌های ملی در عصر کنونی معطوف به افزایش توانمندی‌ها برای برقراری امنیت و افزایش قدرت است. قدرت به‌طور سنتی، بر افزایش توانمندی‌های نظامی، اقتصادی، سیاسی و تحکیم پایه‌های حکومت از طریق حکومت خوب و ایجاد همبستگی ملی صورت می‌گیرد. تهدیدها نیز از طریق افزایش و تقویت چنین ظرفیت‌هایی دفع یا تعلیق می‌شود (زابلی زاده و وهاب پور، ۱۳۹۷).

مقابله با تهدیدات جنگ‌های آتی، نیازمند شناخت فضای نبرد آینده و استفاده از تمام ظرفیت‌ها و مؤلفه‌های قدرت ملی می‌باشد (شهلایی و همکاران، ۱۳۹۶). قدرت به مفهوم تأثیرگذاری بر رفتار دیگران است، به‌نحوی‌که آنچه می‌خواهیم اتفاق بیفتد (گلشن پژوه، ۱۳۸۷). برخی از سازمان‌ها، انبوهی از تجهیزات الکترونیکی را صرف‌نظر از کاربردهای نظامی و غیرنظامی آن در مقیاس‌های کوچک و بزرگ استفاده می‌کنند. این قطعات الکترونیک به اشکال مختلف و در مقیاس‌های مختلف در قالب کامپیوترهای بزرگ و کوچک، ثابت و سیار و یا قطعات کوچک داخل مدارهای پیچیده در ادوات جنگی، جنگنده‌ها، پهپادها، انواع ناوها و ناوچه‌ها، سامانه‌های پدافندی و حتی ماهواره‌ها در کشور استفاده می‌کنند. به علت محدودیت‌های مالی و فناورانه، عموم این تجهیزات از کشورهایی تأمین می‌گردند که خود مخرب‌ترین حملات سایبری را در سال‌های اخیر انجام داده‌اند (اکرمی نسب، ۱۳۹۶).

ارتقاء قدرت سایبری مستلزم اتخاذ راهبردهای مناسب، استفاده بهینه از توانمندی‌های بالقوه و بالفعل سایبری و داشتن سناریو برای مواجهه با رویدادهای شگفتی‌ساز آینده است. (هلیلی، ۱۳۹۷: ۱۲).

پرداختن به مسئله قدرت سایبری ازجمله دغدغه‌های انجام پژوهش حاضر به شمار می‌رود. همچنین تهدیدات ازنظر تنوع و پیچیدگی به‌طور مستمر در حال گسترش هستند که این خود

نیازمند بررسی عوامل محیطی و مطالعه و رصد دائم تهدیدات و به‌تبع آن، ارائه طرح بومی ارتقاء قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران است.

عدم وجود یک الگوی راهبردی برای ارتقاء قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران به‌منظور غلبه بر بحران‌ها و چالش‌های سایبری و ایجاد قابلیت بازدارندگی دغدغه اصلی محقق است. در این تحقیق مسئله اصلی این است که: ارزیابی قدرت پدافند سایبری نیروهای مسلح چگونه است؟

اهمیت موضوع سایبر، امنیت سایبر و دفاع سایبر از بیانات مقام معظم رهبری به‌وضوح قابل مشاهده است: اگر من امروز رهبر انقلاب نبودم حتما رئیس فضای مجازی کشور می‌شدم (۱۳۹۷/۱۰/۲۰ در دیدار معلمان و اساتید استان خراسان شمالی). با توجه به تأکید مقام معظم رهبری(حفظه‌الله تعالی) و وجود اسناد بالادستی و رویکرد فعلی کشورهای متخاصم در استفاده ابزاری از حملات سایبری علیه جمهوری اسلامی ایران در بخش‌های مختلف نظامی، اقتصادی، علمی و فرهنگی، داشتن مدل ارزیابی و سنجش قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران امری دارای اهمیت و اولویت بالا می‌باشد. از طرفی در گام نخست برای تدوین مدل ارزیابی قدرت سایبری، داشتن مدلی مفهومی با تأکید بر بعد پدافند قدرت سایبری، ضرورتی اجتناب‌ناپذیر است؛ یکی از دلایل اصلی این است که قدرت سایبری مفهومی وسیع است که گستره بزرگی را در بردارد. برخی از مزایای ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد پدافند سایبری در راستای پاسخگویی به تهدیدات سایبری در افق ۱۴۰۴، شامل موارد زیر می‌شود:

- بهره‌مندی از الگویی جامع برای بررسی وضعیت توان سایبری نیروهای مسلح در هر زمان.
- کشف توانمندی‌های بالقوه سایبری نیروهای مسلح جمهوری اسلامی ایران.

از این رو ضرورت دارد نیروهای مسلح جمهوری اسلامی ایران متناسب با رویکرد کشورهای فرا منطقه‌ای، خود را با یک ساختار منطقی مجهز به علوم دفاع و حتی حمله در حوزه سایبر نمایند و در این زمینه بایستی از کلیه ظرفیت‌های نیروهای مسلح و بخش دولتی و خصوصی کشور با رعایت ملاحظات امنیتی در این زمینه استفاده نموده تا به قدرت پدافند در حوزه سایبری برسیم.

بنا به بررسی جامع به‌عمل‌آمده تعداد شانزده مدل مطرح شاخص‌گذاری امنیت سایبری جهت محاسبه قدرت و یا میزان امنیت سایبری در سطح جهانی وجود که دقیقا منطبق بر ارتقاء قدرت سایبری نیست و برای ایران و یا نیروهای مسلح بومی نیست. از طرفی مدل‌های

موجود به برر سی امنیت سایبری پرداخته‌اند و مو ضوع قدرت سایبری در آن‌ها مطرح نی ست. امنیت سایبر به مجموعه اقداماتی اطلاق می شود که در درون ف ضای سایبر هر سازمان برای جلوگیری از دســـترســـی افراد غیرمجاز صـــورت می‌گیرد تا از بهره‌برداری یا تخریب رایانه‌ها، ســـامانه‌های ارتباطات الکترونیکی و دیگر فناوری‌های اطلاعات شـــامل فناوری اطلاعات ســـکو، همین‌طور اطلا عات درون آن و از دســـترس پذیری، درســـتی، احراز هو یت، محر مانگی و انکارناپذیری اطمینان حاصل شود (کارگروه خبرگی تدوین سند جامع فضای سایبری، ۱۳۹۹). قدرت ســـایبری، مجموعه منابعی مرتبط با پایداری، کنترل و پیوند میان اطلاعاتی الکترونیک و رایانه‌بنیاد، زیرســـاخت، شـــبکه‌ها، نرم‌افزار مهارت‌های انســـانی تعریف نمود که نه‌فقط اینترنت رایانه‌های شبکه‌ای شده، بلکه اینترانت‌های، فناوری‌های سلولار و ارتباط فضابنیاد را دربردارند. از قدرت سایبری می‌توان برای دستیابی به نتایج دلخواه در درون فضای سایبری استفاده نمود. این قدرت درعین‌حال می‌تواند از اهرم‌های ســـایبری برای کســـب نتیجه دلخواه بیرون از فضـــای ســـایبری نیز اســـتفاده نماید (هلیلی، ۱۳۹۷). در تحقیقات انجام شـــده چارچوبی برای ارزیابی قدرت ســـایبری با روش برنامه‌ریزی مبتنی بر ســـناریو ارائه ننموده‌اند؛ بلکه هدف آن‌ها پرداختن به مباحث کمی در زمینه‌ی قدرت سایبری و فضای سایبری است.

هدف اصلی ارزیابی قدرت پدافند سایبری نیروهای مسلح می‌باشد. سؤال اصلی تحقیق این است که: مهم‌ترین سناریوهای پیش روی ارزیابی قدرت سایبری نیروهای مسلح در بعد پدافند سایبری کدام‌اند؟

مبانی نظری و پیشینه‌های پژوهش

در اینجا نخست به ارائه تعاریفی از مفهوم قدرت از منظر صاحب‌نظران مختلفی پرداخته شده است:

در نگرش اسلامی، قدرت هم‌افق با حکومت تعریف‌شده و مبتنی بر آیات قرآن کریم و روایات معصومان، منشأ قدرت از آن خداوند تبارک‌وتعالی بوده که برای ایجاد حکومت الهی برای دستیابی به اهداف برتر هست (جعفری‌پناه و پوراحمدی،۱۳۹۲).

«قدرت»، هسته و مرکز ثقل سیاست را به وجود می‌آورد و همه کشاکش‌ها در زندگی سیاسی به قدرت مربوط می‌شود (عالم، ۱۳۸۳). هانس مورگنتا، قدرت را چیزی می‌داند که موجبات اعمال سلطه انسانی بر انسان دیگر را فراهم می‌کند و آن را تداوم می‌بخشد. اختیار تحمیل اراده به دیگران به‌صورت قهری (اجباری) و یا اختیاری (رضایت). قدرت بیانگر رابطه طرفیتی، بین انسانها است که یک طرف تأثیرگذار و طرف دیگر تأثیرپذیر است (رفیع و قربی، ۱۳۹۰).

فضای سایبر مجموعه‌ای متشکل از زیرساخت‌ها، شبکه‌ها، نرم‌افزارها، سخت‌افزارها، پروتکل‌ها، محتوی و سیاست‌های حاکم بر این حوزه است (حسینی و ظریف‌منش، ۱۳۹۲).
قدرت سایبری: مجموعه منابعی مرتبط با پایداری، کنترل و پیوند میان اطلاعاتی الکترونیک و رایانه‌بنیاد، زیرساخت، شبکه‌ها، نرم‌افزار مهارت‌های انسانی تعریف نمود که نه‌فقط اینترنت رایانه‌های شبکه‌ای شده، بلکه اینترانت‌های، فناوری‌های سلولار و ارتباط فضا بنیاد را دربردارند. از قدرت سایبری می‌توان برای دستیابی به نتایج دلخواه در درون فضای سایبری استفاده نمود. این قدرت درعین‌حال می‌تواند از اهرم‌های سایبری برای کسب نتیجه دلخواه بیرون از فضای سایبری نیز استفاده نماید.

سناریوها برای آن نوشته میشوند تا سیاست‌گذاران و تصمیم‌گیران بتوانند به گزینه‌های بدیل برای تصمیم‌گیری بیندیشند(نبوی و همکاران، ۱۳۹۹). دستیابی‌به آینده، بدون داشتن سناریو و تصویر مطلوب اگر غیرممکن نباشد، امری دشوار است (سلیمانی و همکاران، ۱۳۹۹). به ارزیابی قدرت سایبری: عبارت است از وسیله‌ای برای شناخت و دانش شاخص‌های قدرت سایبری و درنتیجه حذف، تغییر، اصلاح و یا تجدیدنظر فرآیندهای منجر به بهبود وضعیت قدرت سایبری (هلیلی، ۱۳۹۷). انقلاب فنّاوری در برهه‌های مختلف تاریخ بشر رخداده و اندیشمندان هر عصر تلاش کرده‌اند واقعیت‌های جدید را وارد استراتژی کرده و آن را تئوریزه کنند. بنا به نظر جوزف نای[۱]، در مقایسه با سال‌های اولیه انقلاب تکنولوژیکی هسته‌ای، مطالعات استراتژیک فضای سایبر، از نظر مفاهیم مربوطه معادل دهه‌های گذشته است. ریچارد کلارک و رابرت ناک دو تن از اولین اندیشمندان حوزه امنیت سایبری، اعتقاد دارند که: «از بین تمام مفاهیم استراتژی هسته‌ای، بازدارندگی کمترین امکان را برای انتقال به نبرد سایبر دارد» فرمول‌بندی یک استراتژی مؤثر در عصر سایبر، نیازمند فهمی گسترده‌تر و چندبعدی از مفهوم بازدارندگی بوده و اشتباه است حوزه سایبر را تنها ببینیم. نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری ارائه دهیم. بازدارندگی سایبری به این معناست که در پاسخ به یک حمله سایبری می‌توانیم از طریق تمامی عرصه‌ها پاسخ دهیم (دهقانی، ۱۳۹۷). 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 در زمینه بومی‌سازی تجهیزات ساخت افزاری و نرم افزاری به ویژه در بخش دفاع و ایجاد زنجیره تأمین امن صورت پذیرد (تقی‌پور و اسماعیلی، ۱۳۹۷). هوشمندی یکی دیگر از نیازمندی‌های قدرت سایبری است که

---

۱. Nye

شامل: مدل سازی رفتار مهاجمین، پیش‌بینی صحیح و به موقع حملات، شناسایی مراکز حمله، اتخاذ روش و مکانیزم مناسب برای قدرت دفاع سایبری، اجرا ضدحمله‌های مؤثر بصورت بلادرنگ و یا غیر بلادرنگ، همگی رفتارهای هوشمندانه و دانشی هستند که باید مورد توجه قرار گیرند. (اکرمی نسب، ۱۳۹۶)

جهت بررسی پیشینه تحقیق و مطالعات گذشته، در بانک اطلاعات رساله‌ها و مطالعات گروهی دانشگاه عالی دفاع ملی، سامانه پژوهشگاه علوم و فناوری اطلاعات ایران، بانک اطلاعات پژوهشی نیروهای مسلح سایر پایگاه‌های علمی داخلی و خارجی اقدام به جستجو در موضوعات مرتبط با عنوان پژوهش انجام گردید:

جدول (۱) پیشینه پژوهش‌های انجام‌شده

عنوان پژوهش انجام‌شده	سال انجام	روش و نتایج
امنیت ملی در فضای سایبر	واحدی،صنیعی -۱۳۹۲	تأثیر فضای سایبر بر امنیت ملی چیست؟ نتیجه به شرح زیر است: 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. بهره‌برداری از فضای سایبر در این حوزه انتخابی نیست بلکه اجباری است.
سند راهبردی پدافند سایبری کشور	۱۳۹۴	اهمیت داشتن طرح چشم‌انداز در عرصه‌ی سایبری چیست؟ مفاهیم مهم و مرتبط در عرصه‌ی سایبری کدامند؟ چگونه می‌توان اصول پدافند در فضای سایبری را تبیین نمود؟ نتایج تحقیق به شرح زیر است: تعریف چشم‌انداز پدافند سایبری در افق ۱۴۰۴ 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.
تأثیر قدرت سایبری بر سیاست خارجی ایالات‌متحده آمریکا	جاوید-۱۳۹۴	قدرت سایبری ایالات‌متحده امریکا چگونه بر جایگاه این کشور در نظام بین‌الملل در سال‌های ۲۰۱۵-۲۰۰۱ تأثیر گذاشته است؟ نتایج رساله: قدرت سایبری برای آمریکا به‌عنوان پیش تاز این عرصه، با دارا بودن غول‌های عظیم خصوصی مانند گوگل و ... با حجم گردش مالی بسیار بیشتر از تعداد قابل‌توجهی از کشورهای دنیا و استقرار اغلب شرکت‌ها و سازمان‌های غیردولتی ارائه‌دهنده و مدیریت کننده خدمات اینترنتی در آن امتیازی

عنوان پژوهش انجام‌شده	سال انجام	روش و نتایج
		تقریباً انحصاری داده است. محتمل‌ترین فرضیه موجود برای پرسش‌های مطرح‌شده این است که: قدرت سایبری با حفظ امکان برتری‌جویی در سیاست خارجی، به تداوم هژمونی ایالات‌متحده امریکا در نظام بین‌الملل در سال‌های ۲۰۱۵-۲۰۱۱ انجامیده است.
ارتش سایبری و پیش‌بینی بعد از حمله‌ی سایبری	درویشی-۱۳۹۴	تروریسم سایبری چیست؟ در صورت بروز حملات سایبری وظیفه‌ی ما چیست؟ نتایج رساله: ارتش ضد سایبری با شعار پیشگیری قبل از درمان عنوان می‌شود و ما با قبول حرکت سیل‌آسا و فزاینده فنّاوری و وابستگی بیش‌ازپیش به اینترنت یک اصل در امنیت اطلاعات و محافظت از کشور و زیرساخت‌ها بیان می‌شود. ابتدا باید تعریف جامعی از تروریسم سایبری داشته و راه‌های مختلف را بررسی نماییم. گام بعدی ما می‌تواند یک‌قدم به جلوتر و دید بدبینانه‌ای باشد و آن اینکه، یک حمله سایبری اتفاق افتاده باشد و بدانیم وظیفه‌ی ما چیست؟
بررسی نقش قدرت سایبری در هندسه قدرت جمهوری اسلامی ایران	شهبا-۱۳۹۶	در این پژوهش به بررسی این سؤالات پرداخته شده است: قدرت سایبری و تأثیرگذاری آن بر جامعه‌ی ایران به چه میزان است؟ آیا هندسه‌ی قدرت سایبری حکومت جمهوری اسلامی ایران مؤثرتر بوده است یا سایر گروه‌ها؟
حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری	قوچانی خراسانی و حسینی-۱۳۹۶	چگونه می‌توان با استفاده از مفاهیم حاکمیت و حاکمیت شبکه‌ای مدلی برای حاکمیت در فضای سایبری ارائه نمود؟ نتایج رساله: عدم درک اهمیت فرهنگ پژوهشی در حوزه‌ی سایبری در بدنه‌ی حاکمیتی کشور، نبود یک نقشه راه مدون برای امنیت سایبری کشور، تدوین نظام‌های قراردادی صحیح میان نهادهای حاکمیتی و خصوصی با حفظ حقوق مالکیت معنوی یکی از نیازهای مهم در زمینه‌ی حاکمیت در حوزه‌ی سایبری است.
شناسایی عوامل قدرت هوشمند در فضای سایبری	آریان-۱۳۹۷	قدرت سایبری چیست؟ چگونه می‌توان قدرت را به‌مثابه پدیده نوظهوری در راستای هم‌اندیشی امنیتی در بازه‌های زمانی مختلف دانست؟ نتایج به‌دست‌آمده حاکی از آن است که عوامل فضای سایبری به‌صورت معنی‌دار در تمامی عوامل قدرت هوشمند اوّل بر عامل کنترل دوّم بر نوآوری، سوّم بر مدیریت زمان هوشمند، چهارم بر مشارکت و پنجم بر استراتژی دارد.
ارائه الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی	هلیلی و ولوی -۱۳۹۷	الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی چگونه است؟ ابعاد، مؤلفه‌ها و شاخص‌های مؤثر در ارتقاء قدرت سایبری کدام‌اند؟ شاخص‌های کلان سنجش قدرت سایبری در تراز جهانی کدام‌اند؟ نتایج رساله: پس از مروری بر مفاهیم قدرت و قدرت سایبری، ارکان جهت ساز قدرت سایبری احصاء و ابعاد قدرت سایبری تدوین و الگوی راهبردی ارائه گردید.
بازدارندگی سایبری در امنیت نوین جهانی:	دهقانی-۱۳۹۷	آیا کشورها می‌توانند در فضای سایبر دیگران را از آسیب رساندن به امنیت خود بازداشته و منصرف کنند؟ چگونه می‌توان مهاجمان سایبری را از

عنوان پژوهش انجام‌شده	سال انجام	روش و نتایج
تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا		اقدامات مغایر امنیت ملی و بین‌المللی بازداشت؟ نتایج رساله: مطابق نظریه‌ی رئالیسم ساختاری، کشورها تمایل به افزایش قدرت تهاجمی خود در عرصه‌ی سایبری دارند. به همین دلیل، ویژگی بازدارندگی در فضای سایبری، نسبت به دیگر فضاها متفاوت است و در این فضا باید مباحثی مانند هنجار سازی، انکار، تلافی و گرفتار سازی را در زمینه‌ی بازدارندگی در نظر گرفت.
از فضای سایبر تا قدرت سایبر	کوئل[۱]-۲۰۰۹	ابعاد قدرت سایبری کدام‌اند؟ نتایج مقاله: قدرت سایبری را می‌توان بنا به دسته‌بندی نوعی فضای سایبری به سه بعد تقسیم نمود: بعد فضای سایبری نزدیک که شامل شبکه‌ها و زیرساخت‌هایی است که مستقیماً متعلق و زیر نظر دولت است؛ بعد فضای میانه که شمال قلمروی سایبری شرکت‌ها و سازمان‌های خارجی است و فضای دور سایبری که قلمرو و زیرساخت‌های دشمنان احتمالی را شامل می‌شود.
آناتومی قدرت سایبر	رولاند[۲] و همکاران- ۲۰۱۴	ویژگی‌های مهم قدرت سایبری و کشورهای قدرتمند در زمینه‌ی سایبری چیست؟ نیازمندی حفظ قدرت سایبری چیست؟ نتایج مقاله: یک کشور و یا ماهیت به‌عنوان یک قدرت سایبری دارای سه مؤلفه‌ی ایدئولوژی، بدنه‌ی سیاسی [۳] و زیرساخت مناسب برای فعالیت در فضای سایبری باشد. علاوه بر این‌ها باید دارای خصائص زیر نیز باشد: سازگاری با تغییر در محیط پویای سایبری، مشروعیت برای فعالیت در فضای سایبری، تاب‌آوری در فضای سایبری، رابطه و مشارکت با دیگر قدرت‌ها.
تحلیل تئوری دفاع- حمله توان سایبری روسیه	مونتری[۴] و همکاران- ۲۰۱۵	آیا قابلیت‌های سایبری فدراسیون روسیه ناشی از سلاح‌های سایبری آفندی و پدافندی هست؟ چهره‌ی روسیه از جنبه‌ی آفندی و پدافندی در عرصه‌ی بین‌المللی چگونه است؟ چگونه می‌توان با استفاده از نظریه‌ی آفند-پدافند رابرت جرویس [۵] یک ارزیابی از قدرت سایبری روسیه ارائه نمود. نتایج رساله به این شرح است که: قابلیت روسیه در فضای سایبری بر مبنای نظریه‌ی جرویس آفندی است ولی نمای بیرونی و ظاهری آن‌هم آفندی و هم پدافندی است.

۱. Kuehl

۲. Rowland

۳. Body politic

۴. Mountery

۵. Robert jerois

عنوان پژوهش انجام‌شده	سال انجام	روش و نتایج
قدرت سایبری و سیستم بین‌المللی	شاون[۱]-۲۰۱۷	برخورد بین کشورها در عرصه‌ی سایبری چگونه صورت می‌گیرد؟ روش‌های بازدارندگی و قبولاندن نظر خود در فضای سایبری چگونه است؟ نتایج رساله: باوجوداینکه بازدارندگی در فضای سایبری مانند فضاهای دیگر معنی ندارد ولی به دلایلی مانند مسئله‌ی نسبت‌دهی (مشخص نمودن منبع حملات و نسبت دادن) 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. معمولاً پاسخگویی در همین فضا صورت نمی‌گیرد بلکه پاسخگویی به حملات سایبری در یک زمینه‌ی چند فضایی صورت می‌پذیرد.
قدرت سایبر و اثربخشی سایبری	ببر[۲]-۲۰۱۷	چگونه می‌توان یک چارچوب تحلیلی برای اندازه‌گیری قدرت سایبری بالقوه‌ی یک حکومت ارائه نمود؟ ابعاد موردبحث درزمینه‌ی قدرت سایبری بالقوه کدام‌اند؟ نتایج مقاله: در این مقاله یک چارچوب نظری برای بررسی متغیرهای قدرت سایبری یک حکومت و همین‌طور اثربخشی آن ارائه‌شده است.
مدل بلوغ اکوسیستم سایبر	چنگ و شوو[۳]-۲۰۱۸	چگونه می‌توان بر مبنای ویژگی‌های محیط سایبری، مدلی برای بلوغ سنجی آن ارائه نمود؟ در این پژوهش مدل بلوغ اکوسیستم سایبر ارائه گردیده است.
طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن	مطالعه گروهی پژوهشگران مدیریت راهبردی امنیت فضای سایبری- داعا	نظام دفاع سایبری کشور چگونه است و الزامات تحقق آن کدامند؟ نتایج مقاله: برای شکل‌گیری دفاع سایبری منسجم و یکپارچه در کشور ضرورت دارد دستگاه‌ها و سازمان‌های مختلفی در سطح کشور با مدیریت واحد تعامل و همکاری نزدیک داشته باشند. ساختار برخی از این نهادها که در دفاع سایبری نقش دارند از قبل ایجادشده است (مانند سازمان صداوسیما). سطوح نظام دفاع سایبری عبارت‌اند از: سیاست‌گذاری، فرهنگ‌سازی، پشتیبانی، عملیاتی، دفاع و بازاریابی.

پس از جمع‌بندی پیشینه پژوهش مواردی در قالب نقاط اشتراک، نقاط افتراق و نقاط مغفول-مانده در زیر آمده است.

الف- نقاط اشتراک:

- یکی از موضوعات مهم کاربردی در اغلب این منابع پرداختن به بحثِ بازدارندگی است.
- تعدادی از منابع برای بیان قدرت سایبری به مفهوم امنیت سایبری پرداختند.

---

۱. Shawn

۲. Bebber

۳. Cheng

- در اکثر منابع به موضوع قدرت و یا امنیت سایبری با رویکرد زیرساخت سایبری پرداخته شده است.

ب- نقاط افتراق:

- برخی از این منابع، امنیت سایبر را قدرت سایبری تلقی کردند.
- به علت تفاوت در منافع ملی کشورها، نگاه متفاوت به قدرت سایبری وجود دارد.

پ- نقاط مغفول مانده:

- به قدرت سایبری به مفهوم خاص قدرت در داخل کشور پرداخته نشده است.
- ارزیابی قدرت پدافند سایبری برای نیروهای مسلح کشورها، ارائه نشده است.

روش‌شناسی پژوهش

نوع پژوهش، کاربردی است. روش پژوهش با استفاده از رویکرد آینده‌پژوهی و تأکید بر روش سناریو انجام‌شده است.

۲۰ نفر از خبرگان حوزه سایبری نیروهای مسلح که دارای سابقه مدیریتی، اجرایی و تحصیلات مرتبط با حوزه سایبر را دارا بودند، تعیین‌شده‌اند. تنوع محل خدمتی، تعداد نفرات، سنوات خدمتی و سطح تحصیلات به‌صورت جدول زیر در نظر گرفته‌شده است.

جدول (۲) توزیع نمونه آماری از نظر محل خدمت

ردیف	محل خدمتی	تعداد	سنوات خدمتی	سطح تحصیلات
۱	ستاد کل نیروهای مسلح (معاونت فاوا)	۳	بالای ۲۵ سال	دکتری/کارشناسی ارشد
۲	اداره فناوری ستاد آجا	۵	بالای ۲۵ سال	دکتری/کارشناسی ارشد
۳	معاونت فاوا نیروی زمینی	۳	بین ۲۰ تا ۲۵ سال	دکتری/کارشناسی ارشد
۴	اداره فاوا ق.پدافند هوایی خاتم‌الانبیاء(ص)	۲	بین ۲۰ تا ۲۵ سال	دکتری/کارشناسی ارشد
۵	معاونت فاوا نیروی هوایی	۲	بین ۲۰ تا ۲۵ سال	دکتری/کارشناسی ارشد
۶	معاونت فاوا نیروی دریایی راهبردی	۲	بین ۲۰ تا ۲۵ سال	دکتری/کارشناسی ارشد
۷	فرماندهی جنگال راهبردی آجا	۳	بین ۲۰ تا ۲۵ سال	دکتری/کارشناسی ارشد
جمع		۲۰		

ازآنجاکه تک‌تک سؤالات مصاحبه مبتنی بر ادبیات پژوهش، مصاحبه با خبرگان و با اقتباس از پژوهش‌های مرتبط انجام‌شده در داخل کشور و سایر کشورها می‌باشد، این مصاحبه دارای روایی است. علاوه برآن به‌منظور حصول اطمینان بیشتر از روایی مصاحبه، نقطه نظرات خبرگان و تأیید آنان در قالب جلسات طوفان مغزی نیز اخذشده است.

در این پژوهش، برای جمع‌آوری اطلاعات از روش کتابخانه‌ای مبتنی بر بررسی سایت‌های اینترنتی و فیش‌برداری و بررسی اسناد و مدارک مرتبط با موضوع استفاده شد. همچنین با استفاده از ابزار مصاحبه، داده‌های موردنیاز جهت روش سناریو استفاده گردید.

تجزیه‌وتحلیل و یافته‌های پژوهش

در این پژوهش، مؤلفه‌ها و شاخص‌های موردمطالعه از طریق مطالعه ادبیات مرتبط و مصاحبه با صاحب‌نظران حوزه سایبر به‌دست‌آمده است، نتایج به‌دست‌آمده در قالب جدول (۳)، ارائه گردیده است.

جدول (۳) توصیفی مؤلفه‌ها و شاخص‌ها

بعد	مؤلفه‌ها	شاخص	منابع
قدرت پدافند سایبری	افزارها (سخت و نرم)	بومی بودن	طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران
		به‌روز بودن	
		هوشمندی	اکرمی نسب، ۱۳۹۶
		توان جلوگیری از حمله	مصاحبه با خبرگان
		توان بررسی حملات سایبری(شناسایی، ره‌گیری و اقدام)	مصاحبه با خبرگان
		توان تشخیص حمله	اکرمی نسب، ۱۳۹۶
		استفاده از هوش مصنوعی	
	تقویت عامل انسانی	فرماندهی و مدیریت	
		هویت	کارگروه خبرگی تدوین سند جامع فضای سایبری، ۱۳۹۹
		هوش	مصاحبه با خبرگان
		تخصص سایبری	مصاحبه با خبرگان
		خلاقیت	مصاحبه با خبرگان
		تعداد (کمی)	مصاحبه با خبرگان
	دیپلماسی سایبری	تبادل اطلاعات	مصاحبه با خبرگان
		تعامل پدافندی	مصاحبه با خبرگان
		دفاع سایبری جمعی	مصاحبه با خبرگان
		همکاری و مشارکت‌های بین‌المللی	مطالعه گروهی پژوهشگران مدیریت راهبردی امنیت فضای سایبری- داعا
	بستر پدافندی	عایق نمودن مراکز داده	مصاحبه با خبرگان
		مستحکم سازی زیرساخت‌های سایبری	درویشی، ۱۳۹۴
		پراکندگی در زیرساخت‌ها	مصاحبه با خبرگان

بعد	مؤلفه‌ها	شاخص	منابع
		بانک اطلاعاتی از شگردهای سایبری مهاجمان (کشف الگوهای حملات)	مصاحبه با خبرگان

در ادامه، پژوهش حاضر بر مبنای روش سناریو، انجام‌شده است که مراحل انجام آن به شرح زیر می‌باشد:

مرحله اول: مشخص نمودن وضعیت فعلی قدرت سایبری نیروهای مسلح

در این مرحله ابتدا مؤلفه‌ها و شاخص‌های احصاء شده بعد پدافند سایبری قدرت سایبری از طریق مصاحبه با خبرگان حوزه سایبری نیروهای مسلح و برگزاری جلسات طوفان مغزی به شرح جدول شماره ۲، تعیین‌شده‌اند.

مرحله دوم: ترسیم وضعیت مطلوب قدرت سایبری نیروهای مسلح

فضای سایبری، همواره روند پیشرفت و تکامل را پیش‌رو داشته است. یکی از سازمان‌های درگیر پیش‌بینی ظهور و بلوغ قدرت پدافند سایبری، نیروهای مسلح است. تاکنون برآوردهای متفاوتی از آینده سایبر، ارائه‌شده است که هر یک بر اساس مأموریت و اهداف مختلف و متنوعی دنبال شده است.

مرحله سوم: ارائه سناریوهای پیشنهادی ارزیابی قدرت سایبری نیروهای مسلح

به‌طورکلی برای ساخت سناریو مراحل زیر اجرا می‌گردند:

- ≠ مشخص کردن موضوع اصلی سناریو
- ≠ مشخص کردن عامل‌های کلیدی
- ≠ مشخص کردن نیروهای پیشران
- ≠ مشخص کردن میزان عدم قطعیت عامل‌های کلیدی
- ≠ شناسایی و تعیین منطق سناریو
- ≠ داستان‌سرایی
- ≠ بررسی اولویت‌بندی سناریوها (خوش دهقان، ۱۳۸۸)

مرحله اول:

در این مرحله، تبیین وضع موجود با طرح سئوال‌های مناسب و با توجه به دو متغیر اهمیت و عدم قطعیت انجام گردیده است.

مرحله دوم:

در ادامه و با اجماع نظر خبرگان، وضع مطلوب برای دستیابی آجا به این جایگاه، ترسیم‌شده است.

مرحله سوم:

گام اول-مشخص کردن موضوع اصلی سناریو

تعیین موضوع اصلی سناریو و به‌تبع آن تبیین چهار طرح سناریو به شرح زیر ازجمله گام‌های انجام‌شده در این پژوهش به شمار می‌رود:

موضوع اصلی: ارزیابی قدرت سایبری نیروهای مسلح مبتنی بر روش سناریو: رویکرد پدافند سایبری

نتایج حاصل از ادبیات موضوع و اجماع خبرگان بر این قرار گرفت تا چهار مؤلفه اصلی حوزه پدافند سایبری، به‌عنوان سناریوهای اصلی در این پژوهش موردمطالعه قرار گیرند:

سناریو اول: تقویت عامل انسانی

سناریو دوم: افزارها (سخت و نرم)

سناریو سوم: دیپلماسی سایبری با تأکید بر تعامل پدافندی

سناریو چهارم: بستر پدافندی

گام-دوم مشخص کردن عوامل کلیدی

در این گام طی جلسات متعدد اقدام به جمع‌آوری اطلاعات و تبادل‌نظر درباره عامل‌های کلیدی و سپس جدول ارتباط کمی عامل‌های کلیدی تأثیرگذار بر هر سناریو مطابق با جدول زیر ترسیم می‌گردند (میزان نفوذ و مداخله سازمانی از طریق اخذ نظر خبرگان در پنج وضعیت بسیار قوی، قوی، متوسط، ضعیف و بی‌اثر، تقسیم‌بندی و کمی می‌شوند).

جدول (۴) عامل‌های کلیدی تأثیرگذار بر سناریو اول

طرح سناریو اول: تقویت عامل انسانی			
ردیف	**عامل‌های کلیدی**	**نسبت تأثیر**	**میزان نفوذ و مداخله سازمانی**
۱	فرماندهی و مدیریت	۲۰٪	قوی
۲	هویت	۱۰٪	متوسط
۳	هوش	۲۰٪	قوی
۴	تخصص سایبری	۲۰٪	قوی
۵	خلاقیت	۱۵٪	متوسط
۶	تعداد (کمی)	۱۵٪	متوسط
جمع		۱۰۰٪	

جدول(۵) عامل‌های کلیدی تأثیرگذار بر سناریو دوم

طرح سناریو دوم: افزارها (سخت و نرم)			
ردیف	عامل‌های کلیدی	نسبت تأثیر	میزان نفوذ و مداخله سازمانی
۱	بومی بودن	۲۰٪	قوی
۲	به‌روز بودن	۱۵٪	متوسط
۳	هوشمندی	۱۵٪	متوسط
۴	توان جلوگیری از حمله	۱۰٪	متوسط
۵	توان بررسی حملات سایبری (شناسایی، ره‌گیری و اقدام)	۲۰٪	قوی
۶	توان تشخیص حمله	۱۰٪	متوسط
۷	استفاده از هوش مصنوعی	۱۰٪	متوسط
جمع		۱۰۰٪	

جدول (۶) ارتباط کمی عامل‌های کلیدی تأثیرگذار بر سناریو سوم

طرح سناریو سوم : دیپلماسی سایبری با تأکید بر تعامل پدافندی			
ردیف	عامل‌های کلیدی	نسبت تأثیر	میزان نفوذ و مداخله سازمانی
۱	تبادل اطلاعات	۳۰٪	قوی
۲	تعامل پدافندی	۲۵٪	قوی
۳	دفاع سایبری جمعی	۲۰٪	قوی
۴	همکاری و مشارکت‌های بین‌المللی	۲۵٪	قوی
جمع		۱۰۰٪	

جدول (۷) ارتباط کمی عامل‌های کلیدی تأثیرگذار بر سناریو چهارم

طرح سناریو چهارم : بستر پدافندی			
ردیف	عامل‌های کلیدی	نسبت تأثیر	میزان نفوذ و مداخله سازمانی
۱	عایق نمودن مراکز داده	۲۵٪	قوی
۲	مستحکم‌سازی زیرساخت‌های سایبری	۴۰٪	قوی
۳	پراکندگی در زیرساخت‌ها	۲۰٪	متوسط
۴	بانک اطلاعاتی از شگردهای سایبری مهاجمان(کشف الگوهای حملات)	۱۵٪	متوسط
جمع		۱۰۰٪	

گام سوم- مشخص کردن نیروهای پیشران

نیروهای پیشران، موتورهای تغییر عامل‌های کلیدی هستند موضوعی که همواره می‌تواند، عامل-های کلیدی را تحت تأثیر قرار داده و تغییرات موردنیاز را درباره آن‌ها به وجود آورد، واقعه و یا رویدادی را سریع‌تر از زمان خود و یا کندتر از زمان واقعی، با شدت و قدرت متفاوت، ایجاد کند همان نیروهای پیشران هستند (عطاری، ۱۳۹۳). در این مرحله از طریق مصاحبه انجام شده با خبرگان، پیشران‌های مؤثر بر این پژوهش در حوزه‌های مختلف اقتصادی، سیاسی، جامعه، دانش و فناوری احصاء گردیده است.

جدول (۸) نیروهای پیشران تأثیرگذار بر عامل‌های کلیدی

نیروی پیشران
پیشران‌های اقتصادی
تخصیص بودجه مستقل دفاع سایبری سازمان‌ها
تأمین اعتبارات عمومی زیرساخت‌های سایبری
توسعه از طریق بخش خصوصی قابل‌اعتماد
پیشران‌های سیاسی
انتخاب مدیر آگاه
ایجاد جامعه اطلاعاتی
عضویت در پیمان‌های امنیتی
تشکیل سازمان مستقل دفاع سایبری
پیشران‌های مربوطه به جامعه (مسائل فرهنگی، مذهبی، اجتماعی، زیست‌محیطی، آموزش، رشد جمعیت، رفاه عمومی و ..)
آموزشی عمومی و تخصصی نیروی انسانی
شبکه‌های اجتماعی بومی
ارتقاء سطح فرهنگی و سایبری ملی
مرجعیت دینی
پیشران‌های دانش و فناوری
سیستم بومی
رشته‌های کاربردی
سخت‌افزار و نرم‌افزار بومی
تحقیقات علمی و صنعتی

پس از این مرحله، ماتریس میزان ارتباط و تأثیر نیروهای پیشران بر عامل‌های کلیدی ترسیم می‌شود.

جدول (۹) ماتریس ارتباط کمی نیروهای پیشران با عامل‌های کلیدی

طرح سناریو اول: تقویت عامل انسانی								
ردیف	عامل‌های کلیدی / نیروهای پیشران	فرماندهی و مدیریت	هویت	هوش	تخصص سایبری	خلاقیت	تعداد	جمع
۱	پیشران‌های اقتصادی	۵	۳	۵	۵	۳	۳	۲۱
۲	پیشران‌های سیاسی	۷	۵	۳	۵	۵	۷	۲۷
۳	پیشران‌های جامعه	۹	۳	۷	۵	۵	۵	۳۱
۴	پیشران‌های دانش و فناوری	۳	۳	۵	۳	۵	۵	۲۱
امتیاز		۲۴	۱۶	۲۰	۱۸	۱۸	۲۰	۱۰۰

جدول (۱۰) ماتریس ارتباط کمی نیروهای پیشران با عامل‌های کلیدی

طرح سناریو دوم: افزارها (سخت و نرم)								
ردیف	عامل‌های کلیدی / نیروهای پیشران	بومی بودن	به روز بودن	هوشمندی	توان جلوگیری از حمله	توان بررسی حملات سایبری (شناسایی، ردگیری و اقدام)	توان تشخیص حمله	استفاده از هوش مصنوعی	جمع
۱	پیشران‌های اقتصادی	۵	۳	۵	۳	۳	۵	۷	۲۸
۲	پیشران‌های سیاسی	۵	۳	۵	۳	۵	۳	۳	۲۴
۳	پیشران‌های جامعه	۵	۳	۵	۳	۳	۳	۵	۲۴
۴	پیشران‌های دانش و فناوری	۵	۵	۳	۳	۳	۵	۳	۲۴
امتیاز		۲۰	۱۴	۱۸	۱۲	۱۴	۱۶	۱۸	۱۰۰

جدول (۱۱) ماتریس ارتباط کمی نیروهای پیشران با عامل‌های کلیدی

طرح سناریو سوم: دیپلماسی سایبری با تأکید بر تعامل پدافندی						
ردیف	عامل‌های کلیدی / نیروهای پیشران	تبادل اطلاعات	تعامل پدافندی	دفاع سایبری جمعی	همکاری و مشارکت‌های بین‌المللی	جمع
۱	پیشران‌های اقتصادی	۱۳	۹	۷	۱۱	۳۱
۲	پیشران‌های سیاسی	۱۱	۵	۷	۹	۲۷
۳	پیشران‌های جامعه	۹	۳	۵	۷	۲۱
۴	پیشران‌های دانش و فناوری	۵	۷	۹	۷	۲۱
امتیاز		۳۸	۲۴	۲۸	۳۴	۱۰۰

جدول (۱۲) ماتریس ارتباط کمی نیروهای پیشران با عامل‌های کلیدی

طرح سناریو چهارم: بستر پدافندی						
ردیف	عامل‌های کلیدی / نیروهای پیشران	شیلد بودن مراکز داده	مستحکم سازی زیرساخت‌های سایبری	پراکندگی در زیرساخت‌ها	بانک اطلاعاتی از شگردهای سایبری مهاجمان(کشف الگوهای حملات)	جمع
۱	پیشران‌های اقتصادی	۷	۷	۵	۳	۱۹
۲	پیشران‌های سیاسی	۹	۱۱	۷	۵	۲۷
۳	پیشران‌های جامعه	۷	۱۳	۹	۹	۲۹
۴	پیشران‌های دانش و فناوری	۵	۱۱	۹	۷	۲۵
امتیاز		۲۸	۴۲	۳۰	۲۴	۱۰۰

گام چهارم-مشخص کردن میزان عدم قطعیت عامل‌های کلیدی اصلی سناریو

در چهارمین قدم، اولویت‌بندی عامل‌های کلیدی بر اساس میزان عدم قطعیت انجام می‌شود. هدف این است که عامل‌های کلیدی بااهمیت‌تر مشخص گردد. درواقع این عامل‌های کلیدی

معیارهای متفاوت سناریوها هستند. اولویت‌بندی، باعث جلوگیری از تعدد بیش‌ازحد سناریوها می‌شود.

جدول (۱۳) عامل‌های کلیدی و مهم بر اساس درجه اهمیت و عدم قطعیت

عامل‌های کلیدی و مهم بر اساس درجه اهمیت و عدم قطعیت	
ردیف	عامل‌های کلیدی
۱	فرماندهی و مدیریت
۲	بومی بودن
۳	تبادل اطلاعات
۴	مستحکم‌سازی زیرساخت‌های سایبری

گام پنجم- شناسایی و تعیین منطق سناریو

در این گام، جهت شناسایی منطق سناریو، پس از کسب اطلاع از زمان، چگونگی و میزان تأثیر نیروهای پیشران بر یکدیگر با استفاده از طرح و پاسخگویی به سؤالات مناسب برای هریک از عامل‌های کلیدی اولویت‌بندی شده یک ماتریس اثرگذاری و اثرپذیری نیروهای پیشران به وجود آمده و درنتیجه برای هر سناریو به تعداد عامل‌های کلیدی، ماتریس اثرگذاری و اثرپذیری نیروهای پیشران تهیه می‌گردد.

گام ششم – داستان‌سرایی

در این گام، منطقی کلی و اسکلتی که تا مرحله قبل به‌عنوان استخوان‌بندی اصلی سناریو مشخص‌شده بود و به‌صورت داستانی برای هر سناریو مطرح می‌شود. این موضوع به‌منزله درک عمیق‌تر و شفاف‌تر شدن بهتر ارتباطات و تعاملات در محتوای سناریو به شمار می‌رود. جهت داستان‌سرایی از جلسات ذهن انگیزی استفاده‌شده است که در ادامه داستان اصلی هر سناریو به شرح زیر مطرح می‌شود:

سناریو اول : تقویت عامل انسانی

در این سناریو، توجه به ارتقاء دانش فرماندهی و مدیریت عامل انسانی در سیر مراحل مدیریتی عرصه پدافند سایبری، قابل‌توجه می‌باشد. هویت‌بخشی به عوامل انسانی با تأکید بر ارتقاء تخصص سایبری از سایر مقوله‌های مدنظر در این سناریو است. جذب کمی عامل‌های انسانی هوش محور و دارای قدرت خلاقیت و نوآوری به‌منظور تقویت بعد پدافند سایبری در راستای ارتقاء قدرت سایبری نیز از دیگر ابعاد قابل‌توجه در این سناریو به شمار می‌رود.

سناریو دوم: افزارها (سخت و نرم)

در این سناریو، متناسب با نیاز و ویژگی‌های سایبری در هر بخش، محصولات سایبری به‌طور مستمر بومی و به‌روز می‌شوند. به‌کارگیری دانش روز حوزه هوش مصنوعی در دسترس نهادهای

مختلف سایبری قرارگرفته و از آن در تولید محصولات بومی مختلف و متنوع استفاده می‌شود. با انجام تحقیقات مرتبط، توان جلوگیری از حمله و توان بررسی حملات در این راستا در محصولات بومی سایبری، نهادینه‌شده است. همچنین تأکید بر توان تشخیص حمله‌های سایبری در تولید و به‌کارگیری محصولات بومی سایبری، ضروری است.

سناریو سوم: دیپلماسی سایبری با تأکید بر تعامل پدافندی

در این سناریو، بر ایجاد تعامل پدافندی به‌منظور تبادل اطلاعات به‌گونه‌ای پایدار و مطابق با شرایط روزبه نحوی که تضمین‌کننده اهداف، منافع ملی و سازمانی باشد، تأکید می‌شود. هم‌چنین به‌کارگیری دفاع سایبری جمعی در برابر تهدیدات و حملات، قدرت پیشگیری و بازدارندگی یا قدرت اصلاح و یا واکنش مناسب و لازم، مدنظر است. از طرفی زمینه همکاری و مشارکت‌های بین‌المللی موردنیاز را ایجاد خواهد نمود.

سناریو چهارم: بستر پدافندی

در این سناریو شیلدنمودن مراکز داده‌ی موردنیاز، مطابق با پیشرفت‌ها و تغییرات کاربردهای فناوری اطلاعات و ارتباطات کشور، تعریف و عملیاتی می‌گردند. هم‌چنین سازوکار مناسب برای بهبود و مستحکم‌سازی بیش‌ازپیش زیرساخت‌های سایبریِ موجود، پیش‌بینی می‌شود. در این سناریو از طریق پراکندگی در زیرساخت‌ها، کلیه نیازمندی‌های حاکمیتی و مدیریتی حوزه قدرت سایبری کشور را پوشش داده و سازوکارهای بهبودپذیر و اثربخش برای انجام ارتقاء قدرت سایبری، ایجاد می‌گردند. برای ارتقاء قدرت سایبری و افزایش توان بعد پدافند سایبری، بانک اطلاعاتی حاوی از شگردهای سایبری مهاجمان به‌منظور کشف الگوی حمله مهاجمان تشکیل خواهد شد.

گام هفتم- بررسی و اولویت‌بندی سناریوها

در این مرحله، به بررسی پیامدها و نتایج هر یک از سناریوها پرداخته می‌شود. تعیین جایگاه موضوع اصلی در سناریوها، اهمیت فراوانی دارد و سناریوهایی که فصل مشترک بیشتر و مؤثرتری داشته و به موضوع اصلی نزدیک‌تر باشند، به‌عنوان سناریوهای برتر انتخاب می‌شوند.

نتیجه‌گیری و پیشنهادها

ارزیابی و سنجش وضعیت موجود قدرت سایبری با بهره‌گیری ازنظر خبرگان حوزه قدرت سایبری نیروهای مسلح از نتایج این پژوهش است که نشان داد، برای ارزیابی قدرت پدافند سایبری نیاز است تا چهار مؤلفه: تقویت عامل انسانی، افزارها، دیپلماسی سایبری و بستر پدافندی موردسنجش

قرار گیرند. همچنین مطالعه ادبیات موضوع نشان داد که ۲۱ شاخص در قالب چهار مؤلفه بالا نیازمند مطالعه است تا قدرت سایبری نیروهای مسلح، مورد ارزیابی قرار گیرد.

ترسیم وضعیت مطلوب توسعه قدرت سایبری در افق ده‌ساله آینده در بعد پدافند سایبری با استفاده از پیشران‌ها و روندهای موجود و ارائه چهار سناریو راهبردی برای دستیابی به وضعیت مطلوب بر طبق روش هفت مرحله‌ای سناریونویسی شده که از نتایج عمده این پژوهش، می‌باشد. در ادامه پیشنهادهایی به شرح زیر ارائه می‌شود:

۱. فراهم ساختن شرایط و حمایت مالی، مدیریتی و حاکمیتی لازم، جهت عملیاتی نمودن سناریوهای ارائه‌شده از سوی مسئولین امر و احصای چالش‌های امنیتی سناریوهای فوق از پیشنهادهایی اجرایی محققین برای انجام پژوهش‌های آتی می‌باشد.

۲. معاونت فاوای نیروهای مسلح، نسبت به شناسایی و اولویت‌بندی سرمایه‌های سایبری نیروهای مسلح، اقدام نماید.

۳. معاونت فاوای نیروهای مسلح با استفاده از ظرفیت انجام تحقیق و توسعه در مراکز پژوهشی، مطالعاتی و آزمایشگاهی خود و با تأکید بر رعایت ملاحظات امنیتی، نسبت به تولید، تأمین و تجهیز یگان‌های سایبری به افزارهای سخت‌افزاری و نرم‌افزاری بومی امن به‌منظور تقویت پدافند سایبری اقدام نمایند. نیروهای مسلح با استفاده از ظرفیت دیپلماسی سایبری در حوزه داخل نیروهای مسلح و خارج از نیروهای مسلح و حتی با انعقاد قرارداد با کشورهای هم‌پیمان و متحد به‌منظور تقویت پدافند سایبری اقدام نمایند.

۴. معاونت تربیت و آموزش نیروهای مسلح، از طریق انجام مطالعه آینده‌پژوهی، سرفصل-های آموزشی مرتبط با مؤلفه‌های بعد پدافند سایبری را به‌روزرسانی و تقویت و به سازمان‌های تابعه ابلاغ نماید.

۵. این پژوهش بر موضوع پدافند سایبری نیروهای مسلح ج.ا.ا تمرکز داشته و سایر جوانب از قبیل موضوعات نرم و فرهنگی می‌تواند در مطالعه آینده‌پژوهی دیگری مطرح گردد.

۶. با توجه به پرحجم و وسیع بودن دامنه اعمال ارزیابی قدرت سایبری، پیشنهاد می‌گردد این عنوان در سایر ابعاد و در قالب پژوهشی مجزا، انجام گردد.

۷. از طریق انجام پژوهشی، الزامات و اقدامات اساسی برای پیاده‌سازی ارزیابی مؤلفه و شاخص‌های احصاء شده در این مطالعه، آینده‌نگاری گردد.

قدردانی:

بدین‌وسیله از زحمات استادان محترم راهنما و مشاور، داوران محترم فصلنامه و کلیه صاحب‌نظران و عزیزانی که در طی فرآیند انجام این تحقیق، به هر نحوی، تیم مطالعه را یاری نمودند، کمال تشکر و قدردانی اعلام می‌گردد.

منابع:

≠ اکرمی، نسب معصومه. (۱۳۹۶). امنیت و دفاع سایبری (قسمت سوم)، *مجله علم و فناوری ایرانیان*.

≠ آریان، حامد. (۱۳۹۷). *شناسایی عوامل قدرت هوشمند در فضای سایبری*، پایان‌نامه کارشناسی ارشد، دانشگاه پیام نور استان تهران، دانشکده فنی و مهندسی، مرکز پیام نور تهران غرب.

≠ آسایش جاوید، مهدی. (۱۳۹۴). *تأثیر قدرت سایبری ایالات‌متحده آمریکا بر سیاست خارجی این کشور (۲۰۱۵-۲۰۰۱)*، پایان‌نامه کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه خوارزمی.

≠ تقی‌پور، رضا، اسماعیلی، علی. (۱۳۹۷). *طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، رساله دکتری*، دانشکده امنیت سایبری، دانشگاه عالی دفاع ملی.

≠ جعفری پناه، مهدی.، پور احمدی، حسین. (۱۳۹۲). قدرت نرم از دیدگاه اسلام و کاربرد مؤلفه‌های آن در جمهوری اسلامی ایران، *دو فصلنامه مطالعات قدرت نرم*، ۳(۸): ۹۷–۱۱۲.

≠ حسینی، پرویز.، ظریف منش، حسین. (۱۳۹۲). مطالعه تطبیقی ساختار دفاع سایبری کشورها، پژوهش‌های حفاظتی و امنیتی، ۲(۵): ۶۸-۴۱.

≠ خوش دهقان.، علی. (۱۳۸۸). *آینده‌پژوهی با تکنیک سناریوسازی*، چاپ اول، تهران: مرکز آموزش تحقیقات صنعتی ایران.

≠ درویشی، عزیز اله. (۱۳۹۴). ارتش سایبری و پیش‌بینی بعد از حمله‌ی سایبری، *نخستین کنفرانس بین المللی فناوری اطلاعات*.

≠ دهقانی فیروزآبادی، سید جلال. (۱۳۹۰). فناوری‌های قدرت در جنگ نرم، *فصلنامه مطالعات راهبردی*، ۱۴(۵۱)، ۳۰-۵.

≠ دهقانی، علی‌اصغر. (۱۳۹۷). بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا، *فصلنامه رهیافت‌های سیاسی و بین‌المللی*، ۸ (۴): ۱۴۷-۱۲۱.

≠ رفیع، حسین.، قربی، سید جواد. (۱۳۹۰). بازخوانی قدرت نرم؛ مطالعه موردی عملیات روانی، *فصلنامه مطالعات سیاسی*، ۳(۱۲): ۱۷۳-۱۳۹.

≠ زابلی زاده، اردشیر.، وهاب پور، پیمان. (۱۳۹۷). قدرت بازدارندگی در فضای سایبر، *دو فصلنامه علمی-پژوهشی رسانه و فرهنگ*، ۸(۱): ۸۸-۶۱.

≠ سخنرانی مقام معظم رهبری، ۱۳۹۷/۱۰/۲۰ در دیدار معلمان و اساتید استان خراسان شمالی.

≠ سلیمانی، عباس.، پورعزت، علی‌اصغر. و اسماعیلی گیوی، محمدرضا. (۱۳۹۹). تصویربرداری از آینده سازمان تامین اجتماعی ایران از طریق سناریوپردازی. *فصلنامه علمی پژوهشی آینده‌پژوهی دفاعی*، ۵ (۱۷): ۱۱۷-۹۳.

≠ سند راهبردی پدافند سایبری کشور. (۱۳۹۴). *سازمان پدافند غیرعامل کشور*، مرکز پدافند سایبری کشور، تهران.

≠ شهبا، حجت. (۱۳۹۶). *بررسی نقش قدرت سایبری در هندسه قدرت جمهوری اسلامی ایران*، پایان‌نامه کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه شهید باهنر کرمان.

≠ شهلایی، ناصر.، نادری، علیرضا.، قیم، جمال.، اکبرپور، فریدون.، ذوالفقاری، علی‌صفر. و قادری، سیامک. (۱۳۹۶). مدل مناسب آماد و پشتیبانی در فرماندهی مشترک منطقه‌ای در فضای نبرد آینده. *فصلنامه علمی پژوهشی آینده‌پژوهی دفاعی*، ۱(۳): ۳۴-۷.

≠ عالم، عبدالرحمن. (۱۳۸۳). *بنیاد علم سیاست*، چاپ اول، تهران: نشر نی.

≠ عطاری، مازیار و دیگران. (۱۳۹۳). *روش‌های آینده‌نگاری*، چاپ اول، تهران: بنیاد تدبیر گران توسعه فردا.

≠ قوچانی خراسانی، محمدمهدی.، حسین‌پور، داود. (۱۳۹۶). حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری. *فرایند مدیریت و توسعه*، ۳۰ (۱) :۸۰-۵۱.

≠ کارگروه خبرگی تدوین سند جامع فضای سایبری. (۱۳۹۹). *قرارگاه سایبری حضرت خاتم‌الانبیا (ص)* ستاد کل نیروهای مسلح.

≠ گلشن‌پژوه، محمود رضا. (۱۳۸۷). *جمهوری اسلامی ایران و قدرت نرم (نگاهی به قدرت نرم‌افزاری جمهوری اسلامی)*، چاپ اول، معاونت پژوهشی دانشگاه آزاد اسلامی، دفتر گسترش تولید علم.

≠ مطالعه گروهی. (۱۳۹۵). *طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن*، پژوهشگران مدیریت راهبردی امنیت فضای سایبری، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی.

≠ نبوی، مهدی.، صفوی، سیدحمزه. و کوشکی، محمدصادق، کوشکی. (۱۳۹۹). تدوین سناریوهای روابط ایران و ترکیه در افق ۱۴۰۸. *فصلنامه آینده‌پژوهی دفاعی*، ۵(۱۸): ۳۶-۷.

≠ نصرت‌آبادی، جمشید. (۱۳۹۷). ارائه الگوی ارزیابی قدرت سایبری ارتش جمهوری اسلامی ایران، *فصلنامه علمی پژوهشی امنیت ملی*، دانشکده مدیریت دفاعی، دانشگاه عالی دفاع ملی.

≠ واحدی، مرتضی.، صنیعی، محمدحسین. (۱۳۹۲). *امنیت ملی در فضای سایبر*، رساله دکتری، دانشکده مدیریت دفاعی، دانشگاه عالی دفاع ملی.

≠ هلیلی، خداداد.، ولوی، علی. (۱۳۹۷). *ارائه الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی*، رساله دکتری، دانشکده مدیریت دفاعی، دانشگاه عالی دفاع ملی.

≠ Bebber, Robert. (2017). *Cyber Power and Cyber Effectiveness: An Analytic Framework*, Doctoral Dissertation, Comparative Strategy 36(5):426.

≠ Kuehl, D.T. (2009). *From Cyberspace to Cyber power: Defining the problem*.

≠ Medvedev, Sergei-Monterey. (2015*). Offense-defense theory analysis of Russian cyber capability و California: Naval Postgraduate School*.

≠ Rowland, Jill, Rice, Mason and Shenoi, Sujeet. (2014). The Anatomy of Cyber Power, *International Journal of Critical Infrastructure Protection*.

≠ Shawn, William Lonergan. (2017). *Cyber Power and the International System*, Doctoral Dissertation, Columbia University.

≠ Tong, Gong Cheng, Xi, Dian, Yu, Shu, Zi, Ji. (2018). Maturity Model of Cyber Ecosystem, *Systems Engineering and Electronics Journal*, 40(10).