دریافت مقاله: ۱۳۹۸/۰۶/۰۴ فصلنامهٔ مدیریت نظامی
پذیرش مقاله: ۱۳۹۹/۰۶/۰۲ سال بیستم، شمارهٔ ۲، تابستان ۱۳۹۹
مقاله پژوهشی ص‌ص ۶۱-۹۲

ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بُعد بازدارندگی سایبری

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

چکیده

از جمله روش‌های مقابله با تهدیدات سایبری، فراهم نمودن زمینه ایجاد بازدارندگی سایبری است. در پژوهش حاضر، ابعاد و مؤلفه‌های قدرت سایبری در حوزه بعد بازدارندگی سایبری نیروهای مسلح مطالعه گردید. هدف از این پژوهش، ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی سایبری است. جامعه آماری، متخصصان حوزه سایبر بوده که با رعایت ملاحظات امنیتی متشکل از ۲۰۰ نفر و حجم نمونه شامل ۱۳۲ نفر است. نوع پژوهش، کاربردی است. روش پژوهش، در مرحله اول به علت شناخت ابعاد و مؤلفه‌های مدل مفهومی، اکتشافی است و در مرحله دوم به علت انجام تحلیل‌های آماری، تحلیلی است. روش گردآوری داده‌ها، میدانی و ابزار گردآوری داده‌ها، پرسشنامه است. از روش تحلیل آماری، تی- تک نمونه‌ای استفاده شده است. نتیجه آنکه مدل مفهومی دارای مؤلفه‌های پنج‌گانه: پشیمان‌کنندگی دشمن، استمرار عملیات، پاسخ به تهاجم، استحکام‌سازی و بازیابی است. همچنین، مؤلفه استمرار عملیات، از اولویت بالاتری نسبت به سایر مؤلفه‌ها برخوردار است. استفاده از نتیجه این تحقیق به وسیلهٔ معاونت فاوا می‌تواند برای شناسایی و اولویت‌بندی سرمایه‌های سایبری نیروهای مسلح به منظور ایجاد زمینه بازدارندگی سایبری در مقابل تهدیدات، مفید باشد.

واژه‌های کلیدی: بازدارندگی سایبری، مدل مفهومی، قدرت سایبری و نیروهای مسلح.

---

۱. دانشجوی دکترای مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، تهران، ایران، (* نویسنده مسئول)؛ bmr.۱۳۹۸@yahoo.com
۲. دکترای مهندسی نرم‌افزار، استادیار و عضو هیات علمی دانشگاه امام حسین(ع)، تهران، ایران
۳. دکترای مدیریت سیستم، عضو هیات علمی دانشگاه جامع امام حسین(ع) تهران، ایران
۴. دکترای مدیریت سیستم، عضو هیات علمی و استادیار دانشگاه عالی دفاع ملی، تهران، ایران
۵. دکترای مدیریت فناوری اطلاعات، استادیار دانشگاه افسری امام علی(ع)، تهران، ایران

مقدمه

قدرت به مفهوم تأثیرگذاری بر رفتار دیگران است؛ به نحوی که آنچه می‌خواهیم اتفاق بیفتد (گلشن پژوه، ۱۳۸۷). فضای سایبر مجموعه‌ای متشکل از زیرساخت‌ها، شبکه‌ها، نرم‌افزارها، سخت‌افزارها، پروتکل‌ها، محتوی و سیاست‌های حاکم بر این حوزه است (حسینی و ظریف منش، ۱۳۹۲).

آنچه که در زمینهٔ کنترل فضای سایبر، چالش‌برانگیز است، تفاوت ماهوی آن با دنیای واقعی است و همین امر هم کار را برای دولتمردان سخت می‌کند .بخش مهمی از ظرفیت‌های دولت‌های ملی در عصر کنونی معطوف به افزایش توانمندی‌ها برای برقراری امنیت و افزایش قدرت است. قدرت به طور 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 (زابلی‌زاده و وهاب‌پور، ۱۳۹۷).

سازمان‌ها به زیرساخت‌های فناوری اطلاعات و محیط سایبری وابستگی شدیدی دارند و نفوذ، خرابکاری و افشای اطلاعات سازمان‌ها هزینه‌های زیادی در پی خواهد داشت، در نتیجه امن‌سازی 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 اجراکنندهٔ آزمون نفوذ است (نصرت‌آبادی، ۱۳۹۷).

استفاده از فناوری‌های فضای سایبر با توجه به رویکردهای جدید در دنیای کنونی امری اجتناب‌ناپذیر می‌باشد. با نگرش به در اینکه قواعد و ابزار فضای سایبر در اختیار دیگران می‌باشد، بازیگر یا کشوری که می‌خواهد وارد این عرصه شود باید تلاش کند که از همه ظرفیت‌ها، نقاط مثبت و فرصت‌های آن استفاده کند و با تهدیدات موجود در فضای مذکور مبارزه نموده و حداکثر بهره‌برداری لازم را از این فضا داشته باشد و این مهم بدون داشتن ساختار مناسب جهت مقابله با تهدیدات این حوزه امکان‌پذیر نمی‌باشد (حسینی و ظریف‌منش، ۱۳۹۲).

سرمایه ملی سایبری، به بخشی از دارایی‌های کشور اعم از زیرساخت‌ها، سامانه‌ها، تجهیزات، نرم‌افزارها، اطلاعات و حتی افراد اطلاق می‌شود که در فرآیند تولید، پردازش، ذخیره‌سازی،

مبادله، بازیابی و بهره‌برداری از داده‌های دارای اهمیت حیاتی، حساس و مهم در فضای سایبری کشور، نقش مستقیم و تعیین‌کننده داشته باشند (اساسنامه شورای عالی پدافند غیرعامل، ۱۳۹۴).

قدرت سایبری، توانایی کسب نتایج مطلوب با استفاده از منابع اطلاعاتی الکترونیکی در حوزه سایبری است. قدرت سایبری می‌تواند برای حصول به نتایج مطلوب در داخل فضای سایبر استفاده شود یا می‌تواند از ابزارهای سایبری برای کسب نتیجه مطلوب در سایر حوزه‌ها از آن استفاده کند (نای[۱]، ۲۰۱۰).

قدرت سایبری امروزه بعد مهمی از زیست‌واره جهانی را شکل می‌دهد. اطلاعات و فناوری‌های اطلاعاتی در سپهر سیاسی، اقتصادی و نظامی نقش حیاتی ایفا کرده و مقدمات فعالیت‌های عملیاتی را فراهم می‌آورد. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود و در کنار آثار مثبتی که در بهبود زیست جهانی دارد، برخی ابعاد منفی و قابل‌توجه دیگری نیز دارد که حتی ممکن است آثار آن مخرب ترانسفورماتور از جنگ‌های نظامی بوده و امنیت و حیات ملی مردمی را به چالش بکشاند .با توسعه فناوری‌های اطلاعاتی، خطرات دیگری همچون حمله مجازی یا جاسوسی سایبری در کمین تصمیم‌سازان و سیاست‌گذاران کشورهاست. ولی با توجه به هزاران حمله سایبری که در طی روز اتفاق می‌افتد، کار تمیز حملات جدی و مهم از حملات ناکارآمد و جزئی بسیار سخت شده است (همان منبع).

در عرصه سایبر، دفاع بسیار مشکل است و این مسئله ما را به سمت بازدارندگی سوق می‌دهد. پنج مانع در مسیر دفاع سایبری وجود دارد. اولین مانع، غیرقابل‌پیش‌بینی و غیرقابل‌کشف بودن حمله است. چون حمله از طریق حفره‌های امنیتی انجام می‌شود که هنوز به وسیلهٔ شرکت‌های امنیت سایبری و ویروس‌یاب‌ها کشف نشده‌اند. قربانی از وجود آن خبری ندارد تا بتواند پیش‌بینی یا کشف حمله کند. به‌عنوان مثال، گفته می‌شود عامل‌های استاکس‌نت به مدت سه سال در سیستم‌های ایران مقیم بوده و کارشناسان ایران از وجود آن‌ها اطلاعی نداشته‌اند. دومین مانع در مسیر دفاع سایبر، انکار نتایج دفاع است. همان‌گونه که در بخش‌های قبلی مورد اشاره قرار گرفت، نتیجه دفاع در فضای سایبر بسیار محدود است. سومین مانع، وجود

---

۱. Nye

سطوح پیچیده دفاع است. همان‌گونه که اشاره شد، پیچیده شدن روزافزون سیستم‌ها، به‌معنای ازدیاد راه‌های نفوذ نیز هست. با افزایش حجم نرم‌افزارها در دنیای اپلیکیشن‌ها، در کنار قابلیت‌های بیشتر و ظاهر زیباتر، در واقع دفاع نیز سخت‌تر و پیچیده‌تر می‌شود. چهارمین مانع، چندتکه شدن دفاع است. در حال حاضر بخش اعظم شبکه‌های حساس کشورها از طریق بخش خصوصی اداره می‌شوند و این بدین معنی است که در هنگام دفاع می‌بایست بین بخش‌های مختلف دولتی و خصوصی هماهنگی به وجود بیاید و این بر مشکلات خواهد افزود. مانع پنجم، ریسک‌های زنجیره تأمین است. در دنیای کنونی هیچ کشوری زنجیره تأمین اقلام سایبری خود را به صورت کامل در دست نداشته و ضروری است تا بخشی از این تجهیزات از خارج از کشور تأمین شوند. در هر مرحله‌ای از این زنجیره تأمین، سازمان‌های اطلاعاتی خارجی می‌توانند بخشی از سیستم‌ها را بدون اطلاع کشور هدف آلوده کرده و در نتیجه بدافزارهای مورد نظر را وارد شبکه آن کنند (دهقانی، ۱۳۹۷).

قدرت بازدارندگی یکی از موضوعات روابط بین‌الملل می‌باشد که در هر دو حوزهٔ راهبردی و دیپلماسی کاربرد دارد. در حقیقت، نظریه بازدارندگی آخرین سازوکاری است که با مشخص کردن هزینهٔ جنگ، عملاً از وقوع آن جلوگیری می‌کند. بازدارندگی عبارت است از اقدام یا مجموعه‌ای از اقدامات که برای پیشی جستن از اقدامات خصمانه‌ی دشمن صورت می‌گیرد. نظریهٔ بازدارندگی یعنی کوشش یکی برای اعمال‌نفوذ در دیگری تا او را از اقدام به عملی، که متضمن خسارت یا هزینه‌ای برای اولی است، بازدارد (راوش، ۱۳۹۵).

اهمیت موضوع سایبر، امنیت سایبر و دفاع سایبر از بیانات مقام معظم رهبری به وضوح قابل مشاهده است: «فضای مجازی به‌اندازه انقلاب اسلامی اهمیت دارد.»

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 یکی از ابعاد قدرت سایبری، ضرورتی اجتناب‌ناپذیر است؛ یکی از دلایل اصلی این است که قدرت سایبری مفهومی وسیع است که گستره بزرگی را دربر دارد. برخی از مزایای ارائه مدل

مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی در راستای پاسخگویی به تهدیدات سایبری در افق ۱۴۰۴، شامل موارد زیر می‌شود:

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

ضرورت دارد نیروهای مسلح جمهوری اسلامی ایران متناسب با رویکرد کشورهای فرامنطقه‌ای، خود را با یک ساختار منطقی مجهز به علوم دفاع و حمله در حوزه سایبر نمایند و در این زمینه بایستی از کلیه ظرفیت‌های کشور در این زمینه استفاده نموده تا به قدرت بازدارندگی سایبری نائل گردیم (حسینی و ظریف‌منش، ۱۳۹۲).

پیشینهٔ پژوهش

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:

- سندی با عنوان سند راهبردی پدافند سایبری کشور در سال ۱۳۹۴ در تهران انجام شده است. سؤالات تحقیق شامل موارد زیر است: اهمیت داشتن طرح چشم‌انداز در عرصهٔ سایبری چیست؟ مفاهیم مهم و مرتبط در عرصه‌ی سایبری کدمند؟ 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 کشو حیاتی هست را افزایش داده است.

- پژوهشی با عنوان امنیت ملی در فضای سایبر با طرح این سؤال اصلی که تأثیر فضای سایبر بر امنیت ملی چیست؟ توسط واحدی و صنیعی در سال ۱۳۹۲ در دانشگاه عالی دفاع

ملی انجام شده است. نتیجه این پژوهش به شرح زیر است: با توجه به اینکه بنیان‌های اقتصادی و حتی سیاسی، فرهنگی و نظامی به‌گونه‌ای بر بستر فضای سایبر قرار گرفته و یا در حال قرار گرفتن است. ازاین‌رو ایجاد هر گونه اشکال در این فضا می‌تواند چالش‌های پیچیده و فلج‌کننده‌ای برای نظام پدید آورد. این چالش‌ها می‌تواند امنیت ملی را مخدوش کند. برای تأمین امنیت ملی باید از حوزه شناخت خودی صیانت نمود و بر حوزه شناخت دشمن اثر گذاشت. این کار با بهره‌گیری از فضای سایبر انجام می‌شود. بهره‌برداری از فضای سایبر در این حوزه انتخابی نیست بلکه اجباری است. در این طرح پژوهشی مؤلفه‌های حفظ و تحکیم امنیت ملی در فضای سایبر طبقه‌بندی و موردبررسی قرارگرفته است.

- آریان در سال ۱۳۹۷ در پایان‌نامه‌ای با عنوان: «شناسایی عوامل قدرت هوشمند در فضای سایبری» به بررسی این سؤالات زیر پرداخته است: 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 به صورت معنی‌دار در تمامی عوامل قدرت هوشمند اوّل بر عامل کنترل دوّم بر نوآوری، سوّم بر مدیریت زمان هوشمند، چهارم بر مشارکت و پنجم بر راهبرد(استراتژی) دارد. آزمون فریدمن نشان می‌دهد که با توجه به نتایج به‌دست‌آمده اولویت‌بندی عوامل فضای سایبری و قدرت هوشمند ارتباط معنی‌داری با یکدیگر دارند.

- آسایش جاوید در سال ۱۳۹۴ در پایان‌نامه‌ای با عنوان: «تأثیر قدرت سایبری ایالات‌متحده آمریکا بر سیاست خارجی این کشور (۲۰۱۵-۲۰۰۱)» به دو سؤال پاسخ داده است: چگونه ایالات‌متحده بعد از واقعهٔ یازده سپتامبر، سیاست تسلط خود را در عرصهٔ سایبری پیش برده است؟ قدرت سایبری ایالات‌متحده امریکا چگونه بر جایگاه این کشور در نظام بین‌الملل در سال‌های ۲۰۱۵-۲۰۰۱ تأثیر گذاشته است؟ نتایج رساله: قدرت سایبری که دامنه تعریف آن همه ابزارهای ارتباطی و رسانه‌ای نوین را دربرمی‌گیرد، برای آمریکا به عنوان پیشتاز صنعت ارتباطات و اینترنت 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 تقریباً انحصاری داده است. اولین و 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.

- شهبا در سال ۱۳۹۶ در پژوهشی با عنوان: «بررسی نقش قدرت سایبری در هندسه قدرت جمهوری اسلامی ایران»، به بررسی این سؤالات پرداخته است: قدرت سایبری و تأثیرگذاری آن بر جامعه‌ی ایران به چه میزان است؟ آیا هندسهٔ قدرت سایبری حکومت جمهوری اسلامی ایران مؤثرتر بوده است یا سایر گروه‌ها؟

مونتری و همکاران در سال ۲۰۱۵ در پژوهشی با عنوان: «تحلیل تئوری دفاع-حمله توان سایبری روسیه»، به این سؤالات پاسخ داده است: آیا قابلیت‌های سایبری فدراسیون روسیه ناشی از صلاح‌های سایبری آفندی و پدافندی هست؟ چهرهٔ روسیه از جنبهٔ آفندی و پدافندی در عرصهٔ بین‌المللی چگونه است؟ چگونه می‌توان با استفاده از نظریهٔ آفند-پدافند رابرت جرویس (defensive realism) یک ارزیابی از قدرت سایبری روسیه ارائه نمود. نتایج رساله به این شرح است که قابلیت روسیه در فضای سایبری بر مبنای نظریهٔ جرویس آفندی است، ولی نمای بیرونی و ظاهری آن‌هم آفندی و هم پدافندی است.

- شاون در سال ۲۰۱۷ در رساله دکتری با عنوان قدرت سایبری و سیستم بین‌المللی، به این سؤالات پاسخ داده است: ویژگی منحصربه‌فرد دامنهٔ سایبری چیست؟ برخورد بین کشورها در عرصهٔ سایبری چگونه صورت می‌گیرد؟ روش‌های بازدارندگی و قبولاندن نظر خود در فضای سایبری چگونه است؟ نتایج رساله: با وجود این‌که بازدارندگی در فضای سایبری مانند فضاهای دیگر معنی ندارد، ولی به دلایلی مانند مسئلهٔ نسبت‌دهی (به سختی می‌توان منبع حملات را مشخص نمود و به کشور نسبت داد) در آن مورد توجه کشورها در زمینهٔ بازدارندگی قرار گرفته است. عملیات سایبری معمولاً به صورت مخفیانه و غیرعلنی انجام می‌گیرند؛ یعنی تا حد ممکن بازیگران قدرت در این عرصه سعی می‌کنند، از رویارویی مستقیم پرهیز کنند. فضای سایبری ماهیتاً به‌دلیل مسئلهٔ نسبت‌دهی کمتر در معرض خطر رویارویی دولت‌هاست، ولی معمولاً پاسخگویی در همین فضا صورت نمی‌گیرد، بلکه پاسخگویی به حملات سایبری در یک زمینهٔ چند فضایی صورت می‌پذیرد.

- هلیلی و ولوی در سال ۱۳۹۷ پژوهشی با عنوان: «ارائه الگوی راهبردی ارتقای قدرت سایبری جمهوری اسلامی ایران در تراز جهانی»، انجام داده و به بررسی این سؤالات پرداخته-

اند: الگوی راهبردی ارتقاءی قدرت سایبری جمهوری اسلامی ایران در تراز جهانی چگونه است؟ ماهیت، اجزا، منابع، ویژگی‌ها، پیامدها و دستاوردهای قدرت سایبری چیست؟ ابعاد، مؤلفه‌ها و شاخص‌های مؤثر در ارتقای قدرت سایبری کدام‌اند؟ شاخص‌های کلان سنجش قدرت سایبری در تراز جهانی کدامند؟ نتایج رساله: پس از مروری بر مفاهیم قدرت و قدرت سایبری، ارکان جهت‌ساز قدرت سایبری احصا و ابعاد قدرت سایبری تدوین و الگوی راهبردی ارائه گردید.

- درویشی در سال ۱۳۹۴ در پژوهشی با عنوان: «ارتش سایبری و پیش‌بینی بعد از حملهٔ سایبری»، به بررسی این سؤالات پرداخته است: تروریسم سایبری چیست؟ در صورت بروز حملات سایبری وظیفهٔ ما چیست؟ نتایج رساله: ارتش ضد سایبری با شعار پیشگیری قبل از درمان عنوان می‌شود و ما با قبول حرکت سیل‌آسا و فزاینده فناوری 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 و حملات سایبری داشته باشیم 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 وظیفهٔ ما چیست؟

- دهقانی در سال ۱۳۹۷ در پژوهشی با عنوان: «بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا»، به بررسی این سؤالات پرداخته است: آیا کشورها می‌توانند در فضای سایبر دیگران را از آسیب رساندن به امنیت خود بازداشته و منصرف کنند؟ چگونه می‌توان مهاجمان سایبری را از اقدامات مغایر امنیت ملی و بین‌المللی بازداشت؟ نتایج رساله: مطابق نظریهٔ رئالیسم ساختاری، کشورها تمایل به افزایش قدرت تهاجمی خود در عرصهٔ سایبری دارند؛ به همین دلیل بسیار از اندیشمندان بر این باورند که ویژگی بازدارندگی در فضای سایبری نسبت به دیگر فضاها متفاوت است و در این فضا باید مباحثی مانند هنجارسازی، انکار، تلافی و گرفتارسازی را در زمینهٔ بازدارندگی در نظر گرفت.

- قوچانی خراسانی و حسینی در سال ۱۳۹۶ در پژوهشی با عنوان: حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری، به بررسی این سؤال پرداخته است: 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 بدنهٔ 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 زمینهٔ حاکمیت در حوزهٔ سایبری است.

- زابلی‌زاده و وهاب‌پور در سال ۱۳۹۷ در پژوهشی با عنوان: قدرت و بازدارندگی در فضای سایبری به بررسی این سؤالات پرداخته است: آیا کشورها می‌توانند در فضای سایبر دیگران را از آسیب رساندن به امنیت خود بازداشته و منصرف کنند؟ چگونه می‌توان مهاجمان سایبری را از اقدامات مغایر امنیت ملی و بین‌المللی بازداشت؟ نتایج مقاله: سه مؤلفه‌ی اساسی در زمینهٔ بازدارندگی در فضای سایبری به دست آمد. همچنین نتیجهٔ دیگر این است که بدون عملیات تلافی‌جویانه، بازدارندگی در فضای سایبری چندان مؤثر نیست.

- بیبر در سال ۲۰۱۷ در پژوهشی با عنوان: «قدرت سایبر و اثربخش سایبری: یک چارچوب تحلیلی» به بررسی این سؤالات پرداخته است: چگونه می‌توان یک چارچوب تحلیلی برای اندازه‌گیری قدرت سایبری بالقوهٔ یک حکومت ارائه نمود؟ ابعاد مورد بحث در زمینهٔ قدرت سایبری بالقوه کدامند؟ نتایج مقاله: در این مقاله یک چارچوب نظری برای بررسی متغیرهای قدرت سایبری یک حکومت و همین طور اثربخشی آن ارائه شده است.

- رولاند و همکاران در سال ۲۰۱۴ در پژوهشی با عنوان: آناتومی قدرت سایبر به بررسی این سؤالات پرداخته است: ویژگی‌های مهم قدرت سایبری و کشورهای قدرتمند در زمینهٔ سایبری چیست؟ نیازمندی حفظ قدرت سایبری چیست؟ نتایج مقاله: یک کشور و یا ماهیت به عنوان یک قدرت سایبری دارای سه مؤلفهٔ ایدئولوژی، بدنهٔ سیاسی (body politic) 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.

- چِنگ و شوو در سال ۲۰۱۸ در پژوهشی با عنوان: «مدل بلوغ اکوسیستم سایبر» به بررسی این سؤال پرداخته است: چگونه می‌توان بر مبنای ویژگی‌های محیط سایبری مدلی

برای بلوغ‌سنجی آن ارائه نمود؟

- کوئل در سال ۲۰۰۹ در پژوهشی با عنوان: «از فضای سایبر تا قدرت سایبر: تعریف مسئله»، به‌بررسی سؤال زیر پرداخته است: ابعاد قدرت سایبری کدامند؟ 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.

- پژوهشگران مدیریت راهبردی امنیت فضای سایبری، دانشگاه عالی دفاع ملی در سال ۱۳۹۵ در مطالعه گروهی با عنوان: طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن، به بررسی این سؤال پرداخته است: 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 ایجاد شده است (مانند سازمان صداوسیما). برخی سازمان‌ها نیز اگرچه به صورت مستقل در کشور وجود ندارد، ولی وظایف آن‌ها در سازمان‌ها و وزارتخانه‌های مختلف انجام می‌پذیرد (مانند تحقیقات، آموزش، استانداردسازی، بومی‌سازی تجهیزات سایبری با همکاری وزارتخانه‌های علوم، تحقیقات و فناوری، صنعت، معدن و تجارت قابل‌دستیابی خواهد بود. بخش سوم نقش‌های جدیدی هستند که نهادی در کشور برای آن پیش‌بینی نشده است (مانند متولی هماهنگی امنیت سایبری در قوای سه‌گانه). بنابراین لازم است برای فرآیندهای مشابه نهادهایی ایجاد گردد. سطوح نظام دفاع سایبری عبارت‌اند از: سیاست‌گذاری، فرهنگ‌سازی، پشتیبانی، عملیاتی، دفاع و بازاریابی.

جمع‌بندی پیشینه‌های مرتبط با تحقیق

نقاط اشتراک:

- سعی در تبیین ابعاد و مؤلفه‌های فضای سایبری و قدرت سایبری در اغلب موارد.
- تعدادی از این منابع درزمینه‌ی حوزه‌ی سایبری و قدرت سایبری به یک سری شاخص

و مؤلفه‌ی کیفی رجوع می‌کنند که حاصل مقایسهٔ بررسی پایین به بالا و میدانی از موضوع قدرت سایبری است.

- در اغلب این منابع به این اشاره شده است که یکی از موضوعات مهم کاربردی در حوزه‌ی سایبری بحث بازدارندگی است.
- محققین به موضوع قدرت و یا امنیت سایبری با رویکرد زیرساخت سایبری پرداختند.

نقاط افتراق:

- در این منابع، بحث‌های حوزهٔ سایبری و قدرت سایبری بسیار متنوع است؛ چنان که موضوعاتی مانند حاکمیت فناوری اطلاعات در زمینهٔ سایبری، بازدارندگی، اندازه‌گیری قدرت سایبری و شاخص‌های تأثیرگذار در این زمینه را شامل می‌شود.
- تعدادی از محققان امنیت سایبر را قدرت سایبری تلقی کردند.
- به علت تفاوت در منافع ملی کشورها، نگاه متفاوت به قدرت سایبری وجود دارد.

نقاط مغفول مانده:

در تحقیق‌های صورت گرفته چندین نکتهٔ مغفول مانده است:

- به قدرت سایبری به مفهوم خاص قدرت در داخل کشور پرداخته نشده است.
- طرح راهبردی برای ارزیابی قدرت سایبری برای نیروهای مسلح وجود ندارد.
- ابعاد، مؤلفه و شاخص و وزن هرکدام در محاسبه قدرت سایبری احصا نشده است.
- تلفیق قدرت سایبری با قدرت رزم انجام نشده است.
- هیچ کدام از این تحقیقات به دنبال ارائه یک چارچوب برای ارزیابی و کمی‌سازی قدرت سایبری نیستند، بلکه بیشتر هدف آن‌ها بررسی موضوعات کلی و یا پرداختن به مباحث کیفی در زمینهٔ قدرت سایبری و فضای سایبری است.
- یک بحث نسبتاً دور ازنظر در اینجا این است که ترکیب دو موضوع تهدیدات سایبری و ارزیابی قدرت سایبری بسته به رویکرد مورد استفاده ممکن است متفاوت باشد، چنان که معمولاً بررسی تهدیدات یک موضوع وابسته به مواردی مانند هدف تهدید، روش تهدید و منبع تهدید است که می‌توان در آن بسیار جزئی نگاه کرد. در حالی که مقولهٔ ارزیابی قدرت سایبری

مفهومی به مراتب کلان‌تر و سطح بالاتری است.

نوآوری تحقیق فعلی

- ارائه مدل مفهومی ارزیابی قدرت سایبری با تأکید بر بعد بازدارندگی سایبری در سطح یک سازمان نظامی، که خود فراتر از تحقیقات موجود در این زمینه هست. بیشتر تحقیقات در این حوزه به بررسی کیفی قدرت سایبری و عوامل تأثیرگذار آن در سطح یک کشور می‌پردازند.

هدف اصلی تحقیق

هدف اصلی این پژوهش، ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بُعد بازدارندگی سایبری است.

اهداف فرعی تحقیق:

۱. شناخت مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح؛

۲. تبیین مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح؛

۳. تبیین شاخص‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح؛

۴. تبیین ارتباط مؤلفه‌های بُعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح با یکدیگر؛

۵. تعیین اولویت مؤلفه‌های بُعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح.

سؤال‌ها و فرضیه‌ها

سؤال اصلی تحقیق:

مدل مفهومی برای ارزیابی بعد بازدارندگی قدرت سایبری نیروهای مسلح چگونه است؟

سؤالات فرعی تحقیق:

۱. مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح کدامند؟

۲. شاخص‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح کدامند؟

۳. ارتباط مؤلفه‌های بعد بازدارندگی در ارزیابی قدرت سایبری نیروهای مسلح با یکدیگر چگونه است؟

۴. اولویت‌بندی مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح چگونه است؟

فرضیه‌های تحقیق

فرضیه‌های فرعی:

۱. مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح، تدوین‌پذیر است.

۲. شاخص‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح، تدوین‌پذیر است.

۳. ارتباط مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح، با یکدیگر تبیین‌پذیر است.

۴. اولویت‌بندی مؤلفه‌های بعد بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح، امکان‌پذیر است.

مفاهیم و مبانی نظری

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

«قدرت»، هسته و مرکز ثقل سیاست را به‌وجود 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 ظرفیتی، بین انسان‌ها است که یک‌طرف تأثیرگذار و طرف دیگر تأثیرپذیر است (رفیع و قربی، ۱۳۹۰).

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 دربردارنده. 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. 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).

ویژگی‌های نظریه‌ی بازدارندگی:

الف) قابلیت: این ویژگی به جنبه توانایی دولت‌ها در نظریه‌ی بازدارندگی مربوط می‌شود؛ یعنی توانایی وارد آوردن ضربه به مهاجم احتمالی به‌وسیله‌ی تجهیزات متعارف و غیرمتعارف. نیروی بازدارنده به‌جز مواردی که بلوف می‌زند، باید قادر باشد در صورت لزوم مجازات متناسب را برای طرف مهاجم به‌مرحلهٔ عمل درآورد.

ب) اعتبار: یعنی قبول واقعیت داشتن توانمندی و اراده‌ی لازم برای کاربرد آن، جهت بازداشتن مهاجم از تهاجم؛ به عبارتی بازدارندگی زمانی مؤثر است که توانایی کافی برای پاسخ به تهدید، وجود داشته باشد.

ج) ثبات: اگر برخورد به‌اندازه‌ی کافی شدید باشد، طرف‌های منازعه نه‌تنها باید بتوانند تصمیم به‌اجرای تهدید را به یکدیگر بفهمانند، بلکه باید رهبران دشمن را در مورد نیت خود، تحت تأثیر قرار دهند؛ یک نظام بازدارندگی مؤثر صرفاً به‌داشتن نیروی نظامی قدرتمند نیاز ندارد، بلکه یک قدرت بازدارنده‌ی مؤثر علاوه بر معتبر بودن، باید باثبات هم باشد.

د) ارتباط: در نظریه‌ی بازدارندگی، جلوگیری از برخورد میان طرفین، به تبادل‌نظر صریح و ضمنی طرفین بستگی دارد.

بنابراین لازم است دولت‌ها از طریق انتشار اعلامیه‌ی رسمی، ارسال پیام و اعلام برنامه‌های خود، نیات واقعی خود را در این زمینه آشکار کنند .بازدارندگی هنگامی مؤثر است که نیروی بازدارنده منظور خود را صریح و شفاف به اطلاع طرف مقابل ، برساند و معین کند در صورت موردحمله قرار گرفتن دقیقاً چه عواقبی در انتظار مهاجم خواهد بود(راوش، ۱۳۹۵).

عناصر نظریه‌ی بازدارندگی

نظریه‌پردازان مختلف برای بازدارندگی عناصری را طرح کرده‌اند که با دیدگاه‌های مختلف در خصوص بازدارندگی، در اینجا به عناصر مشترک در میان این نظریه‌ها اشاره می‌شود:

۱. شرایط عینی: فناوری تسلیحاتی نوین دائماً دست‌خوش تحولی پویاست، این امر از مسئله‌ی فنی میزان آسیب‌پذیری، یا آسیب‌ناپذیری سلاح‌های هسته‌ای حکایت می‌کند .برای تأمین توان بازدارندگی، داشتن میزانی از توانایی‌های نظامی و تکنولوژیک لازم است و بدون آن، رسیدن به مرحله‌ی بعدی، که اثرگذاری در ذهن و باور طرف مقابل است، میسر نخواهد بود.

۲. شرایط ذهنی: مقصود این است که محیط روانی طرفین بازدارندگی از نظر راهبردی، بسیار بااهمیت است، به‌عبارت‌دیگر، از نظر ذهنی کشور «الف» باید آمادگی عملی ساختن تهدید را داشته باشد و کشور «ب» نیز از نظر ذهنی اقناع شود که در صورت در پیش نگرفتن سیاست‌های هم‌گرا با کشور «الف» موردِ حمله قرار خواهد گرفت.

۳. شرایط خاص: شرایط خاص ناظر بر ویژگی‌های خاص هر کشور است، به‌طوری‌که هر تهدیدی علیه هر کشور، نتیجه‌ی مشخصی را به بار نخواهد آورد، یعنی این‌که ممکن است کشوری در مقابل تهدیدهای سطح پایین‌تر نیز تسلیم شود درحالی‌که کشوری دیگر، در مقابل تهدیدات بسیار شدیدتر نیز سر تسلیم فرود نیاورد.

۴. مبادله‌ی اطلاعات: برای حصول بازدارندگی، اطلاعات مربوط به شرایط عینی و ذهنی طرفین باید مبادله شود تا سطح آگاهی آن‌ها افزایش یابد.

۵. عدم توسل به زور: بر اساس محاسبهٔ عقلانی، حتی باوجود تهدید به اعمال زور، جنگی بین طرفین صورت نخواهد گرفت و صرفاً انجام تهدید، برای تأمین هدف کارساز خواهد بود.

۶. عقلانیت طرفین: مفهوم بازدارندگی بر این عقیده متمرکز می‌باشد که طرفین محاسبات خود را به صورت عقلانی انجام می‌دهند. بدیهی است که عقل در مقایسه با منافع به‌دست‌آمده، هزینه‌های گزاف را نمی‌پذیرد (همان). درواقع ما در فضای سایبر با پدیده‌ای مواجه هستیم که واجد ویژگی‌هایی است که در هیچ یک از عرصه‌های سنتی موجود نبوده و کاملاً جدید است. این پدیده در درون رشته روابط بین‌الملل و بین نویسندگان مختلف، مباحثی در خصوص سطح راهبردی تهدیدات سایبری و مسئله بازدارندگی به‌وجود آورده است(دهقانی،

۱۳۹۷). بازدارندگی کلاسیک دو سازوکار اصلی دارد:

الف- تهدید مؤثر تلافی؛ ب- انکار نتایج اقدام.

انکار به این معنی است که اقداماتی انجام دهیم تا مهاجم به این درک برسد که در صورت اقدام به حمله، نمی‌تواند تأثیر آن‌چنانی بر جای گذاشته و نتیجه‌ای برای او دربر ندارد (همان).

بازدارندگی سایبری

فضای سایبر علاوه بر فراهم‌سازی مزایای بی‌نظیر برای حکومت‌ها و مردم، تهدیدهای فراوانی را نیز برای جرائم عادی و سازمان‌یافته نظیر فعالیت‌های جاسوسی، تروریستی و نظامی فراهم آورده است. امروزه تهدیدات روزافزون فضای سایبر یکی از دغدغه‌های مشترک کلیه کشورها محسوب می‌گردد و علی‌رغم این‌که راه‌کارهای فراوانی جهت مقابله با آن‌ها پیش‌بینی و به مورد اجرا گذارده شده، کماکان به‌عنوان یک مسئله و مشکل جهانی باقی‌مانده است؛ لذا تمامی کشورها حتی کشورهای پیشرفته در برابر حملات سایبری آسیب‌پذیر هستند، حملات 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 ارتش سایبری، مراکز دفاع سایبری، ... از جمله اقدامات عمده کشورها می‌باشد تا بتوانند با گسترش توان سایبری ، جایگاه خود را در سلسله‌مراتب توان جهانی ارتقاء بخشند. (سیادت،۱۳۹۴).

انقلاب فناوری در برهه‌های مختلف تاریخ بشر رخ داده و اندیشمندان هر عصر تلاش کرده‌اند واقعیت‌های جدید را وارد راهبرد کلان کرده و آن را سامان‌مند(تئوریزه)کنند. بنا به نظر جوزف نای، در مقایسه با سال‌های اولیه انقلاب فناورانهٔ هسته‌ای، مطالعات راهبردی فضای سایبر، از نظر مفاهیم مربوطه معادل دهه ۵۰ است. ریچارد کلارک و رابرت ناک دو تن از اولین اندیشمندان حوزه امنیت سایبری، اعتقاد دارند که: «از بین تمام مفاهیم راهبردی هسته‌ای، بازدارندگی کمترین امکان را برای انتقال به نبرد سایبر دارد»، فرمول‌بندی یک راهبرد مؤثر در عصر سایبر، نیازمند فهمی گسترده‌تر و چندبعدی از مفهوم بازدارندگی بوده و اشتباه است حوزهٔ 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).

ارتش جمهوری اسلامی ایران در حوزه سایبری، اقدامات ارزشمندی را در جهت ارتقای سطح امنیت فناوری اطلاعات و ایجاد ظرفیت پاسخ‌گویی و مقابله با تهدیدات سایبری انجام داده است، ولی اقدامات مذکور با توجه به گستردگی حوزه سایبر در حد جامع نبوده و لازم است که فعالیت‌های فراوان دیگری در جهت تکمیل حلقه محافظت از زیرساخت‌های فاوا پایه و ایجاد قابلیت و اجرای عملیات آفند و پدافند سایبری، تأمین نیازمندی‌های اطلاعاتی،عملیاتی واحدهای عملیاتی در ارتش جمهوری اسلامی ایران صورت پذیرد. (پوردستان، ۱۳۹۶).

در عرصه سایبر، دفاع بسیار مشکل است و این مسئله ما را به سمت بازدارندگی سوق می‌دهد. در فضای سایبر، باتوجه به تفاوت‌هایی که با فضای واقعی وجود دارد، موضوع متفاوت است. در ابتدای تفکر در مورد راهبرد بازدارندگی سایبری و به دلیل مشکل انتساب که در آن امکان شناسایی حمله‌کننده محدود است، امکان تلافی بسیار ضعیف می‌شود؛ زیرا تنبیه زمانی اتفاق می‌افتد که بتوان حمله‌کننده را شناسایی کرد. ولی با توجه به عدم امکان شناخت مهاجم، مکانیزم تلافی، کارایی خود را از دست داده و بنابراین بر اهمیت انکار افزوده خواهد شد. در سال ۲۰۱۰، ویلیام لین معاون وزیر دفاع اعلام کرد که: « بازدارندگی ضرورتاً بر مبنای سلب امکان کسب هرگونه مزیت از حمله‌کنندگان خواهد بود تا تحمیل هزینه از طریق تلافی» و راهبرد سایبری وزارت دفاع در سال ۲۰۱۱ بیشتر تأکید را به جای تلافی و تنبیه، بر دفاع قرارداد (دهقانی، ۱۳۹۷).

حملات سایبری از هر مکان و در هر زمان به وسیلهٔ هر فرد و یا سازمانی با استفاده از هر نوع سامانه رایانه‌ای (کامپیوتری) و ارتباطی ثابت و یا سیار ممکن است انجام شود. دامنه و میزان خسارت احتمالی حمله می‌تواند بسیار گسترده و مؤثر باشد و ده‌ها هزار سامانه رایانه‌ای و مراکز داده را از کار انداخته و انبوهی از خدمات رایانه‌ای را مختل نماید. این ادعا که می‌توان با سازمان‌دهی عملیات سایبری، نفوذ سایبری دشمن را به صفر رساند، کاملاً ادعای اشتباهی است. اغلب حملات ناموفق با درصدی از نفوذ همراه هستند. متولیان عملیات سایبری و توان دفاع سایبری این اصل را پذیرفته‌اند که نفوذ سایبری را نمی‌توان به صفر رساند، لذا باید توانمندی درک درست موقعیت و حساس بودن به وقایع، کنش پیش‌دستانه، مدیریت ریسک و بازدارندگی را مورد توجه قرارداد (اکرمی نسب، ۱۳۹۶).

ارزیابی سازوکارهای چهارگانه بازدارندگی در فضای سایبری

۱) تلافی: به دلیل عدم قطعیت امکان شناسایی حمله‌کننده، تهدید به‌تلافی کارایی زیادی ندارد. با این وجود، این سازوکار هم چنان به عنوان یکی از مهمترین بخش‌های معادله بازدارندگی در فضای سایبر باقی خواهد ماند. نردبان پاسخ‌های تلافی‌جویانه بر اساس شدت حمله شامل: اقدامات دیپلماتیک، اقتصادی، سایبری، قدرت فیزیکی و نیروی هسته‌ای خواهد بود. پیشرفت‌های اخیر در حوزه سیستم‌های فارنزیک نیز کارایی این مکانیزم را افزایش داده است. استفاده آمریکا از کلیه روش‌های در دسترس در پاسخ به حمله سایبری، راهبرد ترکیبی پنتاگون نام دارد.

۲) انکار: مسئله عدم امکان شناسایی می‌تواند مشکلاتی را برای مکانیزم‌های تلافی و هنجار ایجاد کند. ولی مکانیزم‌های انکار و گرفتارسازی نیازی به شناسایی ندارند. یک دفاع سایبری خوب باید شامل چند مؤلفه باشد. یکی از این مؤلفه‌ها، نگه‌داری یک نمونه از کلیه اطلاعات موجود در یک مکان امن است تا در صورت بروز حمله سایبری و از دست رفتن اطلاعات، بتوان از اطلاعات پشتیبان استفاده نمود. مؤلفه دیگر، برگشت‌پذیری است. به این معنا که در صورت هرگونه حمله سایبری و بروز خرابی، بتوانیم کل سیستم را به حالت اولیه برگردانیم. استفاده از مکانیزم انکار بیشتر می‌تواند گروه‌ها و دولت‌های ضعیف را از حمله منصرف کند و دولت‌های قوی دارای آن‌چنان قدرت بالایی هستند که این روش‌ها قادر به بازداشتن آن‌ها نیستند.

۳) گرفتارسازی: استفاده از این سازوکار مستلزم درک مشترک همگان مبنی بر سودمندی استفاده از اینترنت و فضای مجازی برای ایشان است. در صورت رسیدن به چنین درکی، قطعاً به دنبال استفاده غیر صلح‌آمیز از این فضا نخواهند بود. بارزترین نمونه استفاده از این سازوکار در بازدارندگی، موضوع اختلافات سایبری آمریکا و چین است. می‌دانیم که ادامه قدرت چین به اینترنت بستگی تام دارد. درواقع این سازوکار بر اساس وابستگی متقابل کار می‌کند. برخی از وابستگی‌ها دو یا چند طرفه هستند، ولی برخی دیگر سیستمی بوده و بر اثر اخلال در سیستم، منافع از دست خواهند داد. در این حالت کشورها به دنبال ثبات سیستمی خواهند رفت. چین به دلیل وابستگی سیستمی به اینترنت، اقدامات بی‌ثبات‌ساز در اینترنت را پایان بخشید. این سازوکار برای همه کشورها کارایی ندارد؛ به عنوان مثال کشوری مانند کره شمالی را نمی‌توان با این مکانیزم بازداشت.

۴) هنجار: چهارمین سازوکار، هنجارها و تابوها هستند. مسئله شناسایی در عملکرد این سازوکار نیز اهمیت پیدا می‌کند. در صورتی که بتوان با تصویب قوانین بین‌المللی، عملیات سایبری را به‌صورت تابو درآورد، آنگاه شکستن تابو برای کشورها هزینه خواهد داشت. بازدارندگی از این طریق، قدرت نرم کشورها را هدف قرار می‌دهد. هنجارها با گذشت زمان شکل می‌گیرند و هنجارسازی مراحلی دارد که در زمینهٔ سایبر، در مراحل اولیه آن قرار داریم (دهقانی، ۱۳۹۷).

روش اجرای پژوهش

نوع پژوهش، کاربردی است. روش پژوهش، در مرحله اول به علت شناخت ابعاد و مؤلفه‌های مدل مفهومی، اکتشافی است و در مرحله دوم به علت انجام تحلیل‌های آماری، تحلیلی است.

در این تحقیق جامعه آماری مورد مطالعه، متشکل از کلیه خبرگانی که در معاونت پژوهشی فناوری اطلاعات و اداره‌های تابعه معاونت فاوای نیروهای مسلح و کلیه متخصصان حوزه که در امر آموزشی و پژوهشی مشغول انجام وظیفه هستند، می‌باشند. جامعه آماری با رعایت ملاحظات امنیتی متشکل از ۲۰۰ نفر می‌باشد.

حجم نمونه با ضریب اطمینان ۹۵٪ و سطح خطای ۰/۰۵ درصد با استفاده از فرمول کوکران، به شرح زیر محاسبه می‌گردد:

با توجه به تنوع محل خدمتی جامعه آماری، حجم نمونه بر اساس فرمول کوکران به تعداد ۱۳۲ نفر و از طریق روش طبقاتی و به‌صورت زیر تعیین می‌گردد. ضمناً برای اطمینان از تکمیل پرسشنامه‌ها تعداد نمونه‌ها را ۱۴۰ نفر در نظر می‌گیریم.

جدول شمارهٔ ۱: توزیع جامعه آماری و نمونه از نظر محل خدمت

ردیف	محل خدمتی جامعه آماری	حجم جامعهٔ آماری	حجم نمونه
۱	ستاد کل نیروهای مسلح (معاونت فاوا)	۳۵	۲۳
۲	اداره فناوری ستاد آجا	۴۰	۲۶
۳	معاونت فاوا نیروی زمینی	۳۰	۲۰
۴	اداره فاوا قرارگاه پدافند هوایی خاتم‌الانبیاء (ص)	۲۵	۱۷
۵	معاونت فاوا نیروی هوایی	۲۵	۱۷

۶	معاونت فاوا نیروی دریایی راهبردی	۲۵	۱۷
۷	فرماندهی جنگال راهبردی آجا	۲۰	۱۲
جمع		۲۰۰	۱۳۲

جهت بررسی پایایی پرسشنامه، از روش محاسبه ضریب آلفای کرونباخ استفاده شده است، هر چه این ضریب به عدد یک نزدیک‌تر باشد؛ نشان‌دهنده پایایی مناسب ابزار می‌باشد. میزان پایایی در پژوهش حاضر با استفاده از نرم‌افزار SPSS برابر با ۰/۷۸۱ شده است که نشان می‌دهد آزمون از پایایی قابل قبولی برخوردار است.

تعداد سؤالات	آلفای کرونباخ
۳۶	۰,۷۸

از آنجا که تک‌تک سؤالات پرسشنامه مبتنی بر ادبیات پژوهش و با اقتباس از پژوهش‌های مرتبط انجام شده در داخل کشور و سایر کشورها می‌باشد، این پرسشنامه دارای روایی لازم است. علاوه بر آن به منظور حصول اطمینان بیشتر از روایی پرسشنامه، نقطه نظرات خبرگان و تأییدآنان نیز أخذ شده است.

روش و ابزار گردآوری داده‌ها

در این پژوهش، تجزیه و تحلیل داده‌های حاصل از توزیع پرسشنامه انجام گرفته است. هدف از این تحلیل، تجزیه‌وتحلیل داده‌های به‌دست‌آمده و انجام آزمون فرضیات در چارچوب فرآیند و روش تحقیق تعریف شده است. به همین منظور داده‌های اختصاصی که از طریق مصاحبه و گویه‌های پرسشنامه به دست آمده است، بررسی و نتایج به‌دست‌آمده در قالب سه بخش تحلیل‌های کیفی و تحلیل‌های توصیفی و استنباطی ارائه گردیده است.

یافته‌های توصیفی

قبل از تحلیل‌های استنباطی سؤالات پرسشنامه، ابتدا به کمک آمار توصیفی به بررسی توزیع فراوانی پاسخ‌های داده‌شده به هرکدام از سؤالات پرسشنامه پرداخته شد و فراوانی پاسخ‌ها به هر سؤال مورد تحلیل قرار گرفت تا از این طریق، مرتبط بودن/نبودن هر یک از شاخص‌ها با بعد بازدارندگی سایبری مطالعه شود که نتایج به شرح جدول زیر می‌باشد:

جدول شمارهٔ ۲: بررسی توصیفی سؤالات پرسشنامه

	شاخص
بعد	دستورالعمل‌های سایبر در رزم
	انجام رزمایش سایبری
	دفاع در نقطه شروع تهاجم
	پدافند در عمق
	احراز و تصدیق هویت
	نظارت بر حسن اجرای سیاست‌های ابلاغی
	تلافی
	حقوقی و قراردادها
	کاهش زمان واکنش
	استفاده از ظرفیت بسیج
	توان حمایت از پاسخ
	پیشگیری از خسارت
	تحمیل هزینه به دشمن
	امنیت تبادل داده‌ها
	عدم وابستگی زیرساخت‌ها
	آگاهی‌بخشی سایبری
	تجهیزات بومی امن
	بازیابی داده‌ها
	مدیریت حوادث
	واکنش مناسب به حملات
	پشتیبان از اطلاعات
	تعامل با حوزه‌های هم‌تراز سایر سازمان‌های کشوری و لشگری

	مدیریت استمرار عملیات
	توسعه شبکه متخصصین

مطابق خروجی جدول و با توجه به فراوانی‌های مشاهده‌شده مشخص گردید که بیشترین فراوانی پاسخ‌های پاسخ‌دهندگان بر روی گزینه‌های زیاد و خیلی زیاد بوده است این بدان معناست که کلیه سؤال شوندگان معتقدند که شاخص‌های استخراج‌شده با بعد قابلیت بازدارندگی سایبری، در ارزیابی قدرت سایبری نیروهای مسلح مرتبط هستند.

یافته‌های استنباطی

در تحلیلی جداگانه علاوه بر تحلیل توصیفی جدول بالا، مؤلفه‌های مربوطه نیز به کمک فنون آمار استنباطی، مورد تجزیه‌وتحلیل قرار گرفت تا ارتباط هر یک از شاخص‌ها با مؤلفه‌ها استخراج و احصاء گردد. پس از گردآوری و تحلیل داده‌ها، نتایج به شرح زیر حاصل گردیده است. برای این منظور فرضیاتی مطرح و سپس به کمک آزمون مقایسه میانگین با عدد ثابت مورد تحلیل واقع گردید:

فرضیه الف:

H۰: مؤلفه استحکام‌سازی با بعد قابلیت بازدارندگی سایبری مرتبط نیست.

H۱: مؤلفه استحکام‌سازی با بعد قابلیت بازدارندگی سایبری مرتبط است.

جدول شمارهٔ ۳: آزمون ارتباط مؤلفه استحکام‌سازی

		استحکام	بازدارندگی
استحکام	Pearson Correlation	۱	.۶۹۳**
	Sig. (۲-tailed)		.۰۰۰
	N	۳۸	۳۸
بازدارندگی	Pearson Correlation	.۶۹۳**	۱
	Sig. (۲-tailed)	.۰۰۰	
	N	۳۸	۳۸

**. Correlation is significant at the ۰,۰۱ level (۲-tailed).

با توجه به خروجی جدول بالا چون سطح معناداری کمتر از میزان خطای ۰۵/ به‌دست‌آمده است، فرض ادعای محقق یعنی فرضیه H۱ مورد تأیید واقع می‌گردد. این بدان معنا است که از نظر جامعه پاسخ‌دهنده، مؤلفه استحکام‌سازی با بعد قابلیت بازدارندگی سایبری، مرتبط بوده است.

فرضیه ب:

H۰: مؤلفه پاسخ به تهاجم با بعد قابلیت بازدارندگی سایبری مرتبط نیست.

H۱: مؤلفه پاسخ به تهاجم با بعد قابلیت بازدارندگی سایبری مرتبط است.

جدول شمارهٔ ۴: آزمون ارتباط مؤلفه پاسخ به تهاجم

		بازدارندگی	پاسخ
بازدارندگی	Pearson Correlation	۱	.۶۵۳**
	Sig. (۲-tailed)		.۰۰۰
	N	۳۸	۳۸
پاسخ	Pearson Correlation	.۶۵۳**	۱
	Sig. (۲-tailed)	.۰۰۰	
	N	۳۸	۳۸

**. Correlation is significant at the ۰،۰۱ level (۲-tailed).

با توجه به خروجی جدول شمارهٔ ۴ چون سطح معناداری کمتر از میزان خطای ۰/۰۵ به‌دست‌آمده، فرض ادعای محقق یعنی فرضیه H۱ مورد تأیید واقع می‌گردد. این بدان معنا است که از نظر جامعه پاسخ‌دهنده، مؤلفه پاسخ به تهاجم با بعد قابلیت بازدارندگی سایبری مرتبط بوده است.

فرضیه ج:

H۰: مؤلفه پشیمان‌کنندگی بر بعد قابلیت بازدارندگی سایبری مرتبط نیست.

H۱: مؤلفه پشیمان‌کنندگی بر بعد قابلیت بازدارندگی سایبری مرتبط است.

جدول شمارهٔ ۵: آزمون ارتباط مؤلفه پشیمان‌کنندگی

		بازدارندگی	پشیمان‌کنندگی
بازدارندگی	Pearson Correlation	۱	.۸۲۴**
	Sig. (۲-tailed)		.۰۰۰
	N	۳۸	۳۸
پشیمان‌کنندگی	Pearson Correlation	.۸۲۴**	۱
	Sig. (۲-tailed)	.۰۰۰	
	N	۳۸	۳۸

**. Correlation is significant at the ۰،۰۱ level (۲-tailed).

با توجه به خروجی جدول شمارهٔ ۵ چون سطح معناداری کمتر از میزان خطای ۰/۰۵ به‌دست‌آمده، فرض ادعای محقق یعنی فرضیه H۱ مورد تأیید واقع می‌گردد. این بدان معنا است که از نظر جامعه پاسخ‌دهنده، مؤلفه پشیمان‌کنندگی با بعد قابلیت بازدارندگی سایبری، مرتبط بوده است.

فرضیه د:

H۰: مؤلفه بازیابی با بعد قابلیت بازدارندگی سایبری مرتبط نیست.

H۱: مؤلفه بازیابی با بعد قابلیت بازدارندگی سایبری مرتبط است.

جدول شمارهٔ ۶: آزمون ارتباط مؤلفه بازیابی

		بازدارندگی	بازیابی
بازدارندگی	Pearson Correlation	۱	.۹۰۸**
	Sig. (۲-tailed)		.۰۰۰
	N	۳۸	۳۸
بازیابی	Pearson Correlation	.۹۰۸**	۱
	Sig. (۲-tailed)	.۰۰۰	
	N	۳۸	۳۸

**. Correlation is significant at the ۰،۰۱ level (۲-tailed).

با توجه به خروجی جدول شمارهٔ ۶ چون سطح معناداری کمتر از میزان خطای ۰/۰۵ به‌دست‌آمده است، فرض ادعای محقق یعنی فرضیه H۱ مورد تأیید واقع می‌گردد. این بدان معنا است که از نظر جامعه پاسخ‌دهنده، بازیابی با بُعد قابلیت بازدارندگی سایبری مرتبط بوده است.

فرضیه ه:

H۰: مؤلفه استمرار عملیات با بعد قابلیت بازدارندگی سایبری مرتبط نیست.

H۱: مؤلفه استمرار عملیات با بعد قابلیت بازدارندگی سایبری مرتبط است.

جدول شمارهٔ ۷: آزمون ارتباط مؤلفه استمرار عملیات

		بازدارندگی	استمرار
بازدارندگی	Pearson Correlation	۱	.۸۵۶**
	Sig. (۲-tailed)		.۰۰۰
	N	۳۸	۳۸
استمرار	Pearson Correlation	.۸۵۶**	۱
	Sig. (۲-tailed)	.۰۰۰	
	N	۳۸	۳۸

**. Correlation is significant at the ۰،۰۱ level (۲-tailed).

با توجه به خروجی جدول شمارهٔ ۷ چون سطح معناداری کمتر از میزان خطای ۰/۰۵ به‌دست‌آمده است، فرض ادعای محقق یعنی فرضیه **H۱** مورد تأیید واقع می‌گردد. این بدان معنا است که از نظر جامعه پاسخ‌دهنده، مؤلفه استمرار عملیات با بُعد قابلیت بازدارندگی سایبری مرتبط بوده است.

جدول شمارهٔ ۸: همبستگی (پیرسون) بین متغیرها

متغیرهای کنترل			استحکام	پاسخ	پشیمان‌کنندگی	بازیابی	استمرار	بازدارندگی
-none-[a]	استحکام	Correlation	۱،۰۰۰	.۴۴۰	.۴۸۹	.۵۲۸	.۴۲۵	.۶۹۳
		Significance (۲-tailed)	.	.۰۰۶	.۰۰۲	.۰۰۱	.۰۰۸	.۰۰۰
		df	۰	۳۶	۳۶	۳۶	۳۶	۳۶
	پاسخ	Correlation	.۴۴۰	۱،۰۰۰	.۴۸۳	.۴۰۲	.۲۶۳	.۶۵۳
		Significance (۲-tailed)	.۰۰۶	.	.۰۰۲	.۰۱۲	.۱۱۱	.۰۰۰
		df	۳۶	۰	۳۶	۳۶	۳۶	۳۶

	پشیمان کنندگی	Correlation	.۴۸۹	.۴۸۳	۱,۰۰۰	.۶۴۴	.۶۶۹	.۸۲۴
		Significance (۲-tailed)	.۰۰۲	.۰۰۲	.	.۰۰۰	.۰۰۰	.۰۰۰
		df	۳۶	۳۶	۰	۳۶	۳۶	۳۶
	بازیابی	Correlation	.۵۲۸	.۴۰۲	.۶۴۴	۱,۰۰۰	.۹۳۱	.۹۰۸
		Significance (۲-tailed)	.۰۰۱	.۰۱۲	.۰۰۰	.	.۰۰۰	.۰۰۰
		df	۳۶	۳۶	۳۶	۰	۳۶	۳۶
	استمرار	Correlation	.۴۲۵	.۲۶۳	.۶۶۹	.۹۳۱	۱,۰۰۰	.۸۵۶
		Significance (۲-tailed)	.۰۰۸	.۱۱۱	.۰۰۰	.۰۰۰	.	.۰۰۰
		df	۳۶	۳۶	۳۶	۳۶	۰	۳۶
	بازدارندگی	Correlation	.۶۹۳	.۶۵۳	.۸۲۴	.۹۰۸	.۸۵۶	۱,۰۰۰
		Significance (۲-tailed)	.۰۰۰	.۰۰۰	.۰۰۰	.۰۰۰	.۰۰۰	.
		df	۳۶	۳۶	۳۶	۳۶	۳۶	۰
بازدارندگی	استحکام	Correlation	۱,۰۰۰	-.۰۲۴	-.۲۰۳	-.۳۳۶	-.۴۵۴	
		Significance (۲-tailed)	.	.۸۸۸	.۲۲۷	.۰۴۲	.۰۰۵	
		df	۰	۳۵	۳۵	۳۵	۳۵	
	پاسخ	Correlation	-.۰۲۴	۱,۰۰۰	-.۱۲۹	-.۶۰۲	-.۷۵۹	
		Significance (۲-tailed)	.۸۸۸	.	.۴۴۷	.۰۰۰	.۰۰۰	
		df	۳۵	۰	۳۵	۳۵	۳۵	
	پشیمان کنندگی	Correlation	-.۲۰۳	-.۱۲۹	۱,۰۰۰	-.۴۳۹	-.۱۲۴	
		Significance (۲-tailed)	.۲۲۷	.۴۴۷	.	.۰۰۷	.۴۶۳	
		df	۳۵	۳۵	۰	۳۵	۳۵	
	بازیابی	Correlation	-.۳۳۶	-.۶۰۲	-.۴۳۹	۱,۰۰۰	.۷۰۸	
		Significance (۲-tailed)	.۰۴۲	.۰۰۰	.۰۰۷	.	.۰۰۰	
		df	۳۵	۳۵	۳۵	۰	۳۵	
	استمرار	Correlation	-.۴۵۴	-.۷۵۹	-.۱۲۴	.۷۰۸	۱,۰۰۰	
		Significance (۲-tailed)	.۰۰۵	.۰۰۰	.۴۶۳	.۰۰۰	.	
		df	۳۵	۳۵	۳۵	۳۵	۰	

نتایج حاصل از جدول بالا نشان می‌دهد همبستگی دو متغیر اول (استحکام و پاسخ)، بدون در نظر گرفتنِ اثر متغیر بازدارندگی، معادل ۴۴۰. و در سطح ۵ درصد معنی‌دار است. با در نظر گرفتن اثر متغیر بازدارندگی، همبستگی دو متغیر استحکام و پاسخ، معادل ۰۲۴.- خواهد بود که در سطح خطای ۵ درصد معنی‌دار است.

رتبه‌بندی مؤلفه‌های بعد بازدارندگی سایبری الگوی ارزیابی قدرت دفاع سایبری

در ادامه به اولویت‌بندی هرکدام از مؤلفه‌ها و شاخص‌های الگوی ارزیابی قدرت دفاع سایبری پرداخته شده است. برای این منظور فرضیه‌های تدوین و سپس به کمک آزمون فریدمن مورد تحلیل قرار گرفت که رتبه میانگین هر یک از مؤلفه‌ها مشخص گردید. نتایج به شرح زیر می‌باشد:

اولویت‌بندی مؤلفه‌های بعد بازدارندگی سایبری

H۰: اولویت مؤلفه‌های بعد بازدارندگی سایبری یکسان است.

H۱: حداقل اولویت دو مؤلفه از مؤلفه‌های بعد بازدارندگی سایبری باهم تفاوت معنادار دارد.

مطابق خروجی جدول زیر، چون سطح معناداری کمتر از میزان خطای ۰/۰۵ به‌دست‌آمده است، فرض H۱ مورد تأیید واقع می‌گردد؛ این بدان معنا است که رتبه اهمیت میانگین مؤلفه‌های بعد بازدارندگی سایبری یکسان نیست و با هم تفاوت معنادار دارند.

جدول شمارهٔ ۹: آزمون رتبه‌بندی مؤلفه‌های بعد بازدارندگی سایبری

آزمون	ابعاد	رتبه میانگین
فریدمن	استحکام	۳,۱۶
	پاسخ به تهاجم	۲,۴۵
	پشیمان کنندگی دشمن	۲,۸۹
	بازیابی	۳,۰۴
	استمرار عملیات	۳,۴۶
N =۳۸ و ۸,۶۱۸= ۲ᵡ و ۴ =df و ۰۶۱/= sig		

بحث و نتیجه‌گیری:

در تحقیق حاضر سؤال اصلی عبارت بود از «مؤلفه‌ها و شاخص‌های بازدارندگی سایبری در ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران، چگونه است؟»، برای پاسخ به این سؤال چند سؤال فرعی به شرح ذیل طرح گردید:

به منظور احصای مؤلفه‌ها و شاخص‌های بعد بازدارندگی قدرت دفاع سایبری نیروهای مسلح ج.ا.ا، ویژگی‌ها و شاخص‌های اصلی سایر مطالعه‌ها موردِ بررسی قرار گرفت و در احصای شاخص‌ها در تعیین مدل مفهومی مورد استفاده قرار گرفتند.

نتایج این مطالعه با پژوهش مونتری و همکاران در سال ۲۰۱۵ که به دنبال ارزیابی قدرت سایبری روسیه بوده است، هم‌راستا است. همچنین این مطالعه با پژوهش شاون در سال ۲۰۱۷ که به بازدارندگی از طریق پاسخ‌گویی به جملات سایبری معتقد است، هم‌راستا می‌باشد. روش انجام این پژوهش با پژوهش هلیلی و ولوی در سال ۱۳۹۷ هم‌راستا است.

مؤلفه‌ها و شاخص‌های بعد بازدارندگی سایبری

در این پژوهش، پس از مطالعه در حوزه بازدارندگی سایبری از طریق پایگاه‌های اطلاعاتی، مقاله، رساله و کتب مرتبط با موضوع و با کسب نظر خبرگان حوزه فضای سایبر از طریق پرسشنامه، مؤلفه‌ها و شاخص‌های بعد بازدارندگی سایبری مرتبط با ارزیابی قدرت سایبری به شرح ذیل احصا گردید:

جدول شمارهٔ ۱۰: بُعد بازدارندگی سایبری

بعد	مؤلفه	شاخص
بازدارندگی سایبری	استحکام‌سازی	دستورالعمل‌های سایبر در رزم
		انجام رزمایش سایبری
		دفاع در نقطه شروع تهاجم
		پدافند در عمق
		احراز و تصدیق هویت
	پاسخ به تهاجم سایبری	نظارت بر حسن اجرای سیاست‌های ابلاغی
		تلافی

		حقوقی و قراردادها
		کاهش زمان واکنش
		استفاده از ظرفیت بسیج
	پشیمان‌کنندگی دشمن (اقدام متقابل)	توان حمایت از پاسخ
		پیشگیری از خسارت
		تحمیل هزینه به دشمن
		امنیت تبادل داده‌ها
		عدم وابستگی زیرساخت‌ها
		آگاهی‌بخشی سایبری
		تجهیزات بومی امن
	بازیابی	بازیابی داده‌ها
		مدیریت حوادث
		واکنش مناسب به حملات
	استمرار عملیات (افزونگی)	پشتیبان از اطلاعات
		تعامل با حوزه‌های هم‌تراز سایر سازمان‌های کشوری و لشگری
		مدیریت استمرار عملیات
		توسعه شبکه متخصصان

۱. بُعد قابلیت بازدارندگی سایبری با ارزیابی قدرت سایبری مرتبط بوده است.

۲. مؤلفه استحکام‌سازی با بعد قابلیت بازدارندگی سایبری، مرتبط بوده است.

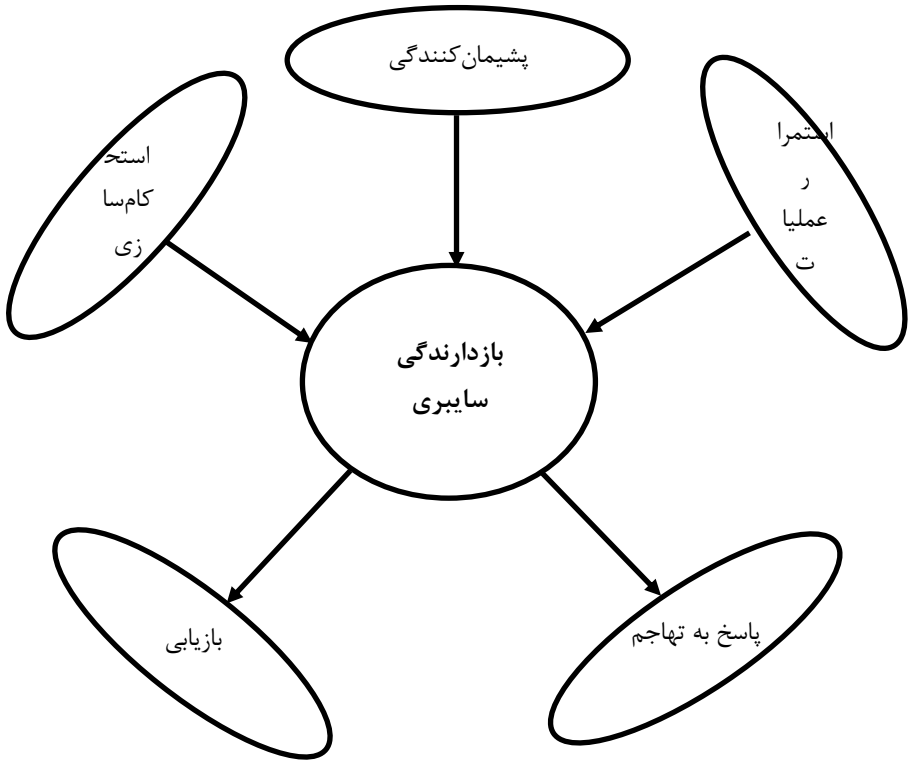
۳. مؤلفه پاسخ به تهاجم با بعد قابلیت بازدارندگی سایبری مرتبط بوده است.

۴. مؤلفه پشیمان کنندگی با بعد قابلیت بازدارندگی سایبری مرتبط بوده است.

۵. مؤلفه بازیابی با بعد قابلیت بازدارندگی سایبری مرتبط بوده است.

۶. مؤلفه استمرار عملیات با بعد قابلیت بازدارندگی سایبری مرتبط بوده است.

در پاسخ به سؤال اصلی «مدل مفهومی برای ارزیابی بُعد بازدارندگی قدرت سایبری نیروهای مسلح، چگونه است؟» مدل مفهومی بازدارندگی سایبری به شکل زیر احصا گردید.



شکل شمارهٔ ۱: مدل مفهومی بازدارندگی سایبری

پیشنهادها:

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

۲) معاونت تربیت و آموزش نیروهای مسلح، سرفصل‌های آموزشی مرتبط با مؤلفه‌های بُعد بازدارندگی سایبری را به‌روزرسانی و تقویت و به سازمان‌های تابعه ابلاغ نماید.

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

۴) 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.

الزامات و اقدامات اساسی برای پیاده‌سازی ارزیابی مؤلفه و شاخص‌های احصا شده در این مطالعه، انجام گردد.

محدودیت‌های پژوهش:

۱) در دسترس نبودن خبرگان حوزه فضای سایبری کشور به دلیل مشغله‌های زیاد.

۲) اشتغال به کار صاحب‌نظران حوزه دفاع سایبری و دشواری هماهنگی جلسات حضوری.

عدم استفاده از سامانه پست الکترونیک با توجه به موضوعات امنیتی به منظور تشکیل جلسات خبرگی به صورت مجازی.

فهرست منابع:

اساسنامه شورای عالی پدافند غیرعامل کشور، ۱۳۹۴/۰۲/۲۹.

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، مرکز پیام نور تهران غرب.

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

پوردستان، احمدرضا(۱۳۹۶)، مراسم تجلیل از برگزیدگان حوزه ارتباطات، مخابرات و فناوری اطلاعات ارتش جمهوری اسلامی ایران.

حسینی، پرویز، ظریف‌منش، حسین (۱۳۹۲). «مطالعه تطبیقی ساختار دفاع سایبری کشورها»، فصلنامه پژوهش‌های حفاظتی-امنیتی دانشگاه جامع امام حسین(ع)، سال دوم، شماره ۵، صص ۶۸-۴۱.

واحدی، مرتضی، صنیعی، محمدحسین (۱۳۹۲). امنیت ملی در فضای سایبر، دانشگاه عالی دفاع ملی.

خراسانی، حمدمهدی، حسینی، داوود (۱۳۹۶). حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری، فصلنامه فرآیند مدیریت و توسعه، دوره ۳۰، شماره ۱.

درویشی، عزیزالله، (۱۳۹۴). «ارتش سایبری و پیش‌بینی بعد از حملهٔ سایبری»، نخستین کنفرانس بین‌المللی فناوری اطلاعات.

دهقانی، علی اصغر (۱۳۹۷). «بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا»، فصلنامه رهیافت‌های سیاسی و بین‌المللی، سال هشتم، شماره ۴، پیاپی ۵۰.

راوش، حمید (۱۳۹۵). قدرت بازدارندگی پدافند غیرعامل ایران در برابر تهدیدات دشمن، پنجمین کنفرانس الگوی اسلامی ایرانی پیشرفت؛ الگوی پیشرفت پایه.

رفیع، حسین، قربی، سیدجواد (۱۳۹۰). «بازخوانی قدرت نرم؛ مطالعه موردی عملیات روانی»،

فصلنامه مطالعات سیاسی، سال سوم، شماره ۱۲، صص ۱۷۳-۱۳۹.

زابلی‌زاده، اردشیر و وهاب‌پور، پیمان (۱۳۹۷). «قدرت بازدارندگی در فضای سایبر»، دو فصلنامه علمی-پژوهشی رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی، ۷۴-۴۷.

سیادت مهدی(۱۳۹۴)، بررسی فضای سایبری ایران در منطقه و جهان.

سند راهبردی پدافند سایبری کشور، سازمان پدافند غیرعامل کشور، مرکز پدافند سایبری کشور، تهران، ۱۳۹۴.

شهبا، حجت (۱۳۹۶). بررسی نقش قدرت سایبری در هندسه قدرت جمهوری اسلامی ایران، پایان‌نامه کارشناسی ارشد، دانشگاه شهید باهنر کرمان.

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

عالم، عبدالرحمن (۱۳۸۳). بنیاد علم سیاست، تهران: نشر نی.

گلشن‌پژوه، محمودرضا (۱۳۸۷). جمهوری اسلامی ایران و قدرت نرم (نگاهی به قدرت نرم‌افزاری جمهوری اسلامی)، معاونت پژوهشی دانشگاه آزاد اسلامی، دفتر گسترش تولید علم، چاپ اول، تهران: دانشگاه آزاد اسلامی.

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

هلیلی، خداداد و ولوی، علی (۱۳۹۷). ارائه الگوی راهبردی ارتقای قدرت سایبری جمهوری اسلامی ایران در تراز جهانی، دانشگاه عالی دفاع ملی.

Bebber, Robert (۲۰۱۷). Cyber Power and Cyber Effectiveness: An Analytic Framework, Comparative Strategy ۳٦(٥):٤۲٦.

Joseph S. Nye. (۲۰۱۰). Cyber Power (The future of power in the ۲۱th century). MIT-Harvard Minerva Project, Harvard Kennedy School.

Kuehl, D.T (۲۰۰۹). From Cyberspace to Cyber power: Defining the problem.

Medvedev, Sergei-Monterey (۲۰۱٥). Offense-defense theory analysis of Russian cyber capability و California: Naval Postgraduate School.

Rowland, Jill, Rice, Mason and Shenoi, Sujeet (۲۰۱٤). The Anatomy of Cyber Power, International Journal of Critical Infrastructure Protection.

Shawn William Lonergan (۲۰۱۷). Cyber Power and the International System, Columbia University, Doctoral Dissertation.

Tong Gong Cheng, Xi, Dian, Yu, Shu, Zi, Ji (۲۰۱۸). Maturity Model of Cyber Ecosystem, Systems Engineering and Electronics ٤۰(۱۰).

Venables, Adrian, Siraj Shaikh, James Shuttle (۲۰۱٥). A Model for Characterizing Cyber power, worth Infrastructure Protection (ICCIP), Mar ۲۰۱٥, Arlington, VA, United States. IFIP Advances in Information and Communication Technology, AICT-٤٦٦, pp.۳-۱٦, Critical Infrastructure Protection IX.