فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش‌راهبردی
سال هشتم، شماره ۳۱، تابستان ۱۳۹۷، صفحات ۲۵۲-۲۲۵

طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی

محمد احدی[۱]؛ محمد شاه‌محمدی[۲]

تاریخ دریافت: ۱۳۹۶/۰۶/۲۵ تاریخ پذیرش: ۱۳۹۶/۰۹/۲۵

چکیده

با گسترش فضای سایبر و وابستگی روزافزون زیرساخت‌های کشورها به این فضا و آسیب‌پذیری که آن‌ها در مقابل حملات سایبری دارند، برخورداری از یک طرح راهبردی دفاعی در این حوزه ضرورت می‌یابد و در چنین طرحی، بازدارندگی از اولویت بیشتری برخوردار خواهد بود. پژوهشی حاضر که از نوع کاربردی – توسعه‌ای است، با استفاده از روش‌های کمی و کیفی و روش دلفی جهت جمع‌آوری اطلاعات از نخبگان در حوزه سایبری و روش اکتشافی در مراجعه به اسناد و مدارک بهره‌برداری شده است. حجم نمونه معادل حجم جامعه آماری یعنی ٤٠ نفر از نخبگان و خبرگان بوده و برای تعیین پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شده است. بر اساس نتایج این پژوهش می‌توان گفت هرچند بازدارندگی در حوزه سایبر متفاوت و پیچیده‌تر از بازدارندگی نظامی است اما با رعایت الزامات آن و بهره‌گیری از شیوه‌های مناسب می‌توان به آن دست یافت و بدین‌ترتیب هزینه دفاع در این حوزه تا حد قابل توجهی کاهش می‌یابد.

واژه‌های کلیدی: فضای سایبر، راهبرد، بازدارندگی.

۱- عضو هیئت علمی دانشکده فارابی و نویسنده مسئول (رایانامه: ahadimohammad@yahoo.com)
۲- دانش‌آموخته دکترای علوم سیاسی گرایش جامعه شناسی سیاسی

مقدمه

واژه بازدارندگی هرچند اولین‌بار در چارچوب رقابت هسته‌ای قدرت‌های بزرگ وارد فرهنگ دفاعی شد، اما به مرور و در خلال دهه اخیر در سایر حوزه‌ها و اخیراً در حوزه سایبر نیز وارد شده و با توجه به اولویت بازدارندگی در دکترین دفاعی جمهوری اسلامی ایران، در فضای سایبر نیز این اولویت قابل اعمال خواهد بود و می‌تواند جایگاه مناسبی در الگوی طرح راهبردی دفاع سایبری کشور کسب نماید.

با توجه به گستردگی و پیچیده شدن و اهمیت فضای سایبری در جهان، ضرورت دارد قدرت بُرد راهبردی و بُرد تاکتیکی نظام جمهوری اسلامی ایران در یک جنگ اطلاعاتی و سایبری بیش‌ازپیش افزایش یابد. بنابراین لازم است تا نظام جمهوری اسلامی به کمک نخبگان بتواند دکترین امنیتی خود را به‌طور جامع‌تر و با قبول حضور گسترده‌تر در فضای سایبر و جامعه اطلاعاتی پی‌ریزی نماید. بدون‌تردید پیشرفت و شکوفایی کشور در عرصه علم و فناوری، موجب تثبیت قدرت ملی در این عرصه خواهد شد، چرا که افزایش سطح کیفی نیازهای دستگاه‌های مختلف از یک‌سو و تقویت قدرت پدافندی در فضای سایبر از سوی دیگر، موجب قدرت‌بخشی و قدرت‌افکنی خواهد شد. از آنجا که عرصه سایبری نسبت به سایر عرصه‌های نبرد از قدمت و سابقه کمتری برخوردار است و به‌ویژه بازدارندگی در این عرصه هنوز جایگاه واقعی خود را نیافته، تاکنون طرح راهبردی در این زمینه تدوین نگردیده است. از این‌رو تحقیق حاضر درصدد پاسخ به این سوال است که الگوی بازدارندگی سایبری در جهت تأمین منافع و امنیت‌ملی با عنایت به اصول و ارزش‌های حاکم، چشم‌انداز، ماموریت، عوامل داخلی و خارجی مؤثر بر طرح راهبردی دفاع سایبری چیست؟

اهمیت تحقیق در این است که حساسیت لازم دستگاه‌های مختلف کشوری و لشکری را نسبت به ادبیات بازدارندگی سایبری برانگیخته و به اتخاذ تدابیر راهبردی در این جهت هدایت کرده و نحوه بازدارندگی در فضای سایبر را به‌طور یکنواخت و هماهنگ با منافع و امنیت ملی تبیین خواهد نمود.

ضرورت اجرای این تحقیق نیز در این است که نبود طرح راهبردی مناسب بازدارندگی سایبری مبتنی‌بر دانش بومی و نیازمندی ملی، در سنوات پیشین سبب آسیب‌پذیری در حوزه‌های مختلف گردیده و تهاجم سایبری را به اشکال گوناگون از سوی بیگانگان به دنبال داشته و نبود راهبرد در بازدارندگی سایبری، هزینه‌ها را در دفاع سایبری افزایش خواهد داد.

هدف اصلی تحقیق حاضر ارائه راهبردهای بازدارندگی سایبری کشور در برابر تهدیدهای سایبری است و این تحقیق در پی پاسخ به این سوال اصلی است که راهبردهای بازدارندگی سایبری کشور در برابر تهدیدهای سایبری چیست؟

سوال‌های فرعی نیز عبارتند از:

۱) اصول، ارزش‌ها و چشم‌انداز بازدارندگی سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی کدامند؟

۲) ماموریت‌های بازدارندگی سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی کدام است؟

۳) عوامل داخلی و خارجی مؤثر در بازدارندگی سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی کدامند؟

مبانی نظری و پیشینه‌شناسی پژهش

فضای سایبر

اصطلاح فضای سایبر از ترکیب دو واژه «سایبر» و «فضا» تشکیل شده است که برای درک بهتر این اصطلاح، هریک از واژه‌ها جداگانه بررسی می‌شود. سایبر از لغت یونانی(Kybernetes) سایبرنتیک به‌معنای سکاندار یا راهنما مشتق شده است.

فضای سایبر، فضایی تخیلی است که از اتصال رایانه‌هایی پدید آمده که تمام انسان‌ها، ماشین‌ها و منابع اطلاعاتی در جهان را به‌هم متصل کرده است. این معنا به‌طور تقریبی مشابه معنایی است که امروزه از کاربرد لفظ فضای مجازی وجود دارد. در این پژوهش، فضای مجازی برای توصیف تمام انواع منابع اطلاعاتی ایجاد شده از طریق شبکه‌های رایانه‌ای به‌کار برده می‌شود.

بازدارندگی

بازدارندگی یکی از موضوعات روابط بین‌الملل می‌باشد که در هر دو حوزه‌ی راهبرد و دیپلماسی کاربرد دارد. بازدارندگی عبارت است از اقدام یا مجموعه‌ای از اقدامات که برای پیشی‌جستن از اقدامات خصمانه‌ی دشمن صورت می‌گیرد. تئوری بازدارندگی یعنی کوشش یکی برای اعمال نفوذ در دیگری تا او را از اقدام به عملی که متضمن خسارت یا هزینه‌ای برای اولی است، باز دارد (الیوت،۱۳۷۸: ۳۷۰).

بازدارندگی متقارن[1] بر اساس توازن قدرت یا موازنه فیزیکی قدرت صورت می‌پذیرد، در صورتی‌که در بازدارندگی نامتقارن[2] موازنه وحشت اساس توازن خواهد بود (افشردی و همکاران،۱۳۹۳:۲۲).

در این پژوهش، بازدارندگی به مفهوم هرگونه تدبیر یا فعالیتی است که دشمن را از تصمیم‌گیری برای حمله (سایبری) بازدارد و به او تفهیم کند که زیان ناشی از اقدام او بیش از سود آن برای او خواهد بود.

راهبرد

راهبرد راهی برای رسیدن به آینده مطلوب است، یا به مجموعه‌ای از انتخاب‌های بنیادی و یا حیاتی درباره نتایج یک فعالیت و ابزار انجام آن فعالیت را راهبرد گویند (حسن‌بیگی،۱۳۹۰:۴۳).

طرح راهبردی

طرح راهبردی فرآیندی است که راهبردهای مناسب را برای رسیدن به اهداف خاص تولید می‌کند. طرح راهبردی فرآیندی است که طی آن سوال‌ها، بحث‌ها و مشکلات طرح و سپس رفع شده و اغلب کیفیت تصمیمات راهبردی را نیز تعیین می‌کند (Stanley,2012: 4)

طرح راهبردی مسیر آینده سازمان را پیش‌بینی می‌کند (اینکه آیا سازمان در مسیر خود ادامه می‌دهد یا مسیر دیگری را برمی‌گزیند) پیش‌بینی این که چگونه بازار، مشتری و خط تولید تغییر یا واکنش نشان می‌دهد و تاب‌آوری سازمان در برابر ریسک محاسبه می‌شود (Barksdole and Lound,2006: 7).

طرح راهبردی سندی است که در آن سازوکارها، اولویت‌ها، چگونگی تمرکز منابع، خروجی‌ها و نتایج مورد نظر با در نظر گرفتن متغیرهای محیطی برای یک افق مشخص تدوین می شود.

الزامات نظریه بازدارندگی سایبری

ریچارد ال.کوگلر[3] در مقاله خود تحت‌عنوان "بازدارندگی حملات سایبری" درخصوص الزامات تئوری بازدارندگی می‌نویسد:

«نیازمندی‌های یک تئوری بازدارندگی موثر چیست؟ یک پاسخ ساده این است: دفاع قوی که بتواند حملات سایبر را دفع کند و آفندهای سایبری را تقویت نماید که بتوانند خسارات تلافی‌جویانه انبوه را تحمیل نماید. بدین‌ترتیب در چنین رویکرد قابلیت پایه‌ای فرض می‌شود جنگ‌های سایبری در حالت ایزوله از سایر وقایع بزرگتر پیرامون آن، اتفاق بیافتد و بتوان با آن

1 Symmetrical Deterrence
2 Asymmetrical Deterrence
3 - Richard L. Kugler

به‌عنوان خودحاکم، تابع منطق و نیازهای خود رفتار شود. بدین‌ترتیب، احتمال بیشتر این است که برخی حملات سایبری عمده احتمالاً به‌عنوان یک ابزار در دستیابی به اهداف سیاسی و راهبردی، نه‌فقط تحمیل خسارت به طرف مقابل می‌نماید بلکه به‌عنوان ابزارهای چانه‌زنی و اجبار مورد استفاده قرار می‌گیرند تا کشور هدف را وادار به تسلیم در مقابل خواسته‌های سیاسی – راهبردی مهاجمین نماید. تعامل با حملات سایبری از این نوع، نه‌فقط نیازمند قابلیت‌های آفندی و پدافندی برای بازدارندگی آن‌ها در برخی صحنه‌های مکانیکی است، بلکه نیازمند ظرفیت برای نفوذ در انگیزه‌ها و روان مهاجمین و همچنین یک ظرفیت برای پاسخ‌های سایبری – آفندی و پدافندی – با سایر ابزارهای قدرت ملی و پاسخ به بحران است. به این دلایل، مسئله راهبرد بازدارندگی سایبری نمی‌تواند از بقیه سیاست‌های امنیتی ملی تفکیک شود.

بنابراین، بازدارندگی به‌معنی صحیح آن، یعنی برای هر نوع از تهدیدات ظرفیت‌هایی را باید فراهم نمود که اعمال تهدید یا متوقف و ناممکن شود و یا با تحمیل هزینه زیاد مانع از اعمال آن گردد، همان راهبردی که جمهوری اسلامی ایران در قبال تهدیدات سخت دشمن به‌کار بست و نه‌تنها به مسابقه تسلیحاتی روی نیاورد و از حوضه‌های دیگر غافل نشد و هزینه‌های گزاف تسلیحاتی و نظامی بر خود تحمیل نکرد، بلکه با حداقل هزینه‌ها و بهره‌گیری از فرصت‌ها و شناخت صحیح و کامل تهدیدات سخت متصور، با خلق قابلیت‌های مهار تهدید، جمهوری اسلامی ایران را از شر تهدیدات سختِ نظام سلطه مصون نمود و توانست امنیتی پایدار را به ارمغان آورد.

ویژگی‌های تهدیدهای سایبری

تهدیدهای سایبری که امروزه در حال توسعه است، دارای ویژگی‌هایی است که شناخت آن‌ها در بازدارندگی موثر خواهد بود. اهم این ویژگی‌ها به شرح ذیل می‌باشد:

الف) تعدد بازیگران تهدیدکننده

یک مسئله مهم در بازدارندگی سایبر تعدد بازیگرانی است که احتمالاً تهدیدهای سایبر به‌ویژه تهدید به حملات مخرب در سال‌های آینده را اعمال خواهند کرد. توانایی استفاده از فضای سایبر برای ایجاد برتری و نفوذ در رویدادها در سایر محیط‌های عملیاتی و میان مولفه‌های چندگانه قدرت توسعه می‌یابد. امروز برخی مهاجمین سایبری به‌عنوان هکرهای فردی با نیت کاملاً سوء یا شاید گروه‌های جنایی که هدفشان استفاده از شبکه‌های اطلاعاتی در راستای منافع خود می‌باشد، شناخته می‌شوند. علاوه‌بر این، بازیگران با دستورکارهای سیاسی یا ایدئولوژیک –

شامل گروه‌های تروریستی، کشورهای ورشکسته و حتی قدرت‌های بزرگ هم‌چون آمریکا، چین و روسیه – نیز به دنبال قدرت سایبری هستند و نقش‌هایی با اهمیت فزاینده بازی خواهند کرد.

ب) تنوع اهداف تهدید

بازیگران سایبری ممکن است به دنبال استفاده از تهدیدهای یا حملات سایبری برای پیگیری اهداف راهبردی و سیاسی در رقابت ژئوپلیتیکی با قدرت‌های دیگر باشند. چنین حملات سایبری، بیشتر ابزارهای اقناع و اکراه هستند که در چارچوب دستورکارهایی عمل می‌کنند که ماورای فضای سایبر را نیز دربرمی‌گیرند. این بازیگران و فعالیت‌های آن‌ها ممکن است تهدیدهای سایبری بزرگتری از آنچه قبلاً صورت گرفته بود را باعث شوند و بدین‌ترتیب توجه به یک راهبرد بازدارندگی سایبری را ضروری می‌سازند.

ج) سرعت تحولات

ظهور روندهایی در امور امنیت جهانی، مرحله‌ای را ایجاد خواهد کرد که تهدیدهای جدید و بزرگ‌تر ممکن است در سال‌های آینده اشاعه یابند. در مقایسه با جنگ سرد، جهان امروز بسیار پیچیده‌تر است. نظام دوقطبی به پایان رسیده و هیچ ساختار دائمی جای آن را نگرفته است. در عوض، دنیا به سرعت در پاسخ به جهانی شدن و سایر دینامیک‌های حوزه اطلاعات تغییر می‌کند. نقش‌های متغیر دولت – ملت‌ها و سایر بازیگران، ایدئولوژی‌های سیاسی جدید، شرایط امنیتی متغیر، اقتصاد جهانی شدیداً رقابتی، ظهور فناوری‌های جدید و نیروهای نظامی متحرک، همگی به محیط جهانی با تغییرات سریع اضافه می‌شوند. غافلگیری‌ها مدام اتفاق می‌افتند، جهش‌های ناگهانی در روندها اتفاق می‌افتد و حتی کارشناسان قادر به پیش‌بینی آینده نیستند.

د) مبهم بودن

ساختار نظام امنیت بین‌الملل امروز دارای سه بخش مهم است: بخش اول جامعه مرفه دمکراتیک است مرکب از ایالات‌متحده، اروپا، و بخش‌هایی از آسیا به اضافه تعدادی از کشورهای آمریکای لاتین که البته دمکراتیک هستند نه مرفه. از نظر اکثر بخش‌ها، این جامعه دمکراتیک شکوفا، امن و باثبات است. بخش دوم مرکب از چالش‌گران راهبردی است شامل قدرت‌های بزرگی هم‌چون چین، روسیه و هند (البته از نظر آمریکایی‌ها). این سه قدرت بزرگ، با دارا بودن نزدیک به نیمی از جمعیت جهان و یک رشد رفاه اقتصادی، هویت‌شان را در جهان باز تعریف می‌کنند و خود را به‌عنوان یک بازیگر امور امنیت جهانی ثبت می‌کنند. بخش سوم ساختار جهانی "طاق جنوبی

بی‌ثباتی"[1] از خاورمیانه بزرگ تا جنوب آسیاست. این منطقه عظیم یک دیگ جوشان از آشفتگی‌ها و هرج‌ومرج، رژیم‌های استبدادی، جوامع بی‌ثبات، فقر، غوغا، بنیادگرایی اسلامی رنجیده و خشونت است. آینده تهدیدهای امروزین تروریسم، اشاعه تسلیحات کشتارجمعی و کشورهای ورشکسته برخاسته از این منطقه یک علامت سوال بزرگ است. جنگ‌های سخت در عراق و افغانستان ، منازعه اسراییل – فلسطین و جستجوی یک دیپلماسی موثر در منطقه از سوی ایالات متحده به ابهامات افزوده است (Kramer,2009: 314-316).

ویژگی تهدیدها در فضای سایبری

خودکارسازی زیرساخت‌های ملی از طریق فناوری اطلاعات و اتصال روزافزون شبکه‌های رایانه‌ای به شبکه جهانی، تهدیدهای ناشی از کشورها و سازمان‌های خارجی در فضای سایبری را افزایش داده و توسعه این تهدیدها، بخشی از تلاش‌های گسترده برای اثرگذاری بر امنیت ملی کشورها در عصر اطلاعات است (حسن‌بیگی،۱۳۸۸: ۱۰۲).

تهدیدهای سایبری تمایزات اساسی با تهدیدهای سنتی دارد. بخشی از ویژگی‌های این تهدیدها به شرح زیر است:

الف) غیرسرزمینی بودن: برخی تهدیدها نظیر تروریسم، بیماری‌های مسری، حملات سایبری در دنیای پس از جنگ سرد فراسرزمینی‌اند و در کوتاه‌ترین زمان ممکن می‌توانند از کشوری به کشور دیگر منتقل شوند و وجود مرزهای دولتی مانعی در برابر انتقال تهدیدها نیست.

ب) این تهدیدها را نمی‌توان تنها با اتکا به سیاست‌های دفاعی سنتی مدیریت کرد. سازمان‌های نظامی، دفاعی امکان دارد به‌ویژه در کشمکش‌های خشونت‌آمیز نقش داشته باشند ولی باید در نظر داشت که مدیریت موثر، مستلزم طیفی از رهیافت‌های غیرنظامی است (حسن بیگی،۱۳۸۸: ۹۸).

ج) نامشخص بودن: در شرایط حاضر دولت‌ها و ملت‌ها با زنجیره‌ای از تهدیدهای نامشخص در محیط‌های مجازی مواجهند که امنیت آن‌ها را به چالش کشیده و ابزارهای سنتی تامین امنیت ملی نیز توان مقابله با آن‌ها را ندارد (حسن بیگی،۱۳۸۸:۲۸۸).

د) عدم‌انتساب: یکی از ویژگی‌های حملات و تهدیدهای سایبری، عدم‌امکان انتساب حمله به حمله‌کنندگان است، به واسطه نامشخص بودن منشا تهدید یا حمله فرایند انتساب دچار چالش می‌گردد.

[1] - Southern Arc of Instability.

ویژگی‌های نظریهٔ بازدارندگی

ویژگی‌های نظریه‌ی بازدارندگی شامل قابلیت، اعتبار، ثبات و ارتباط به شرح ذیل است:

۱) قابلیت: این ویژگی به جنبه‌ی توانایی دولت‌ها در نظریه‌ی بازدارندگی مربوط می‌شود. یعنی توانایی واردآوردن ضربه به مهاجم احتمالی به وسیله‌ی تجهیزات متعارف و غیرمتعارف. نیروی بازدارنده به‌جز مواردی که بلوف می‌زند، باید قادر باشد در صورت لزوم مجازات متناسب را برای طرف مهاجم به مرحله‌ی عمل درآورد (امیدوارنیا،۱۳۸۱:٤٤).

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

۳) ثبات: اگر برخورد به اندازه‌ی کافی شدید باشد، طرف‌های منازعه نه‌تنها باید بتوانند تصمیم به اجرای تهدید را به یکدیگر بفهمانند، بلکه باید رهبران دشمن را در مورد نیت خود، تحت‌تاثیر قرار دهند؛ یک نظام بازدارندگی موثر صرفاً به داشتن نیروی نظامی قدرتمند نیاز ندارد، بلکه یک قدرت بازدارنده‌ی موثر علاوه‌بر معتبربودن، باید با ثبات هم باشد (همان: ٤٥).

٤) ارتباط: در نظریه‌ی بازدارندگی، جلوگیری از برخورد میان طرفین، به تبادل نظر 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 مورد حمله قرار گرفتن دقیقا چه عواقبی در انتظار مهاجم خواهد بود (ازغندی،۱۳۷٤:۲۳۱).

عناصر نظریه‌ی بازدارندگی

نویسندگان و نظریه‌پردازان مختلف برای بازدارندگی عناصری را بیان کرده‌اند که با جمع‌بندی دیدگاه‌های مختلف در خصوص بازدارندگی، در اینجا به شش عنصر مشترک در میان این نظریات اشاره می‌شود:

۱) شرایط عینی؛ ۲) شرایط ذهنی؛ ۳) شرایط خاص؛ ٤) مبادله‌ی اطلاعات؛ ٥) عدم‌توسل به زور؛ ٦) عقلانیت طرفین.

شیوه‌های اصلی بازدارندگی

بازدارندگی به وسیله انکار سود، مستلزم تهدید قابل باور در محروم کردن حمله‌کننده از منافع یا دستاوردهایی است که در جستجوی آن است.

بازدارندگی به‌وسیلهٔ تحمیل هزینه مستلزم تهدید قابل باور در تحمیل هزینه‌ها، ضایعات و مخاطره‌هایی است که پذیرش آن‌ها بسیار سخت است، بدین‌ترتیب متقاعد کردن رقیب به اینکه تنبیه بسیار سنگین‌تر از موفقیت‌های مورد انتظار خواهد بود.

بازدارندگی به‌وسیلهٔ ترغیب برای منع رقیب به‌معنای متقاعد کردن رقیب به این است که هیچ حمله‌ای یک نتیجه قابل قبول و جذاب نخواهد داشت (Kramer,2009:327-329).

گام‌های بازدارندگی

مدل عمومی بازدارندگی شش گام تحلیلی را برای پیگیری هر مورد بازدارندگی سایبر در زمان صلح، جنگ و بحران ارائه می‌کند:

۱) تعیین اهداف بازدارندگی و تدبیر راهبردی؛
۲) برآورد محاسبه راهبردی تصمیم‌سازان رقیب؛
۳) شناسایی تاثیرات بازدارندگی موردنظر در هدایت رقیب؛
٤) توسعه و برآورد راه‌کارهای طراحی شده برای دستیابی به تاثیرات مورد نظر؛
٥) توسعه طرح‌هایی برای اجرای راه‌کارها و برای پایش و برآورد پاسخ‌های رقیب؛
٦) توسعه ظرفیت‌ها برای پاسخ انعطاف‌پذیر و موثر (Kramer, 2009: 329-331).

دیدگاه اسلام

«وَأَعِدُّواْ لَهُم مَّا اسْتَطَعْتُم مِّن قُوَّةٍ وَمِن رِّبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدْوَّ اللّهِ وَعَدُوَّكُمْ وَآخَرِينَ مِن دُونِهِمْ لاَ تَعْلَمُونَهُمُ اللّهُ يَعْلَمُهُمْ» (سوره انفال- آیه ٦٠).

یکی از ویژگی‌های جامعه اسلامی، اقتدار این جامعه است؛ لذا ترس انداختن در دل دشمن یکی از توصیه‌های جدی قرآن کریم است که در آیه مذکور بدان اشاره شده و اساساً ترساندن با هدف بازدارندگی صورت می‌گیرد.

در آیات قرآن به‌ویژه آیه مذکور به اصول کلی توجه شده و تنها برای بیان نمونه، برخی از مصادیق نام برده شده است. اصل کلی که قرآن به‌صورت آموزه‌ای دستوری به مسلمانان آموزش می‌دهد فراهم‌آوری توان و نیرو است. توان شامل هرگونه ابزار و آلات بازدارنده و یا هجومی و یا دفاعی

است. از این رو تنها به سلاح اشاره نشده است. تهیه هر چیزی که قدرت امت و دولت اسلامی را افزایش دهد، امری لازم و ضروری است و با توجه به شرایط مکانی و زمانی تغییر می‌کند. ممکن است چیزی در زمانی ابزار جنگی مناسبی باشد ولی در عصر دیگری نه‌تنها مفید نباشد بلکه زیان‌بار به قدرت اسلام و مومنان باشد. در عصر حاضر رسانه‌ها به‌عنوان یکی از ابزارهای جنگی قوی مطرح هستند بنابراین بر امت است که از این توان نیز برخوردار گردند. چنان‌که فراهم‌آوری نفرات و نیروی انسانی زبده و کارآمد امری است که هرگز نباید آن را دست کم گرفت. در زمانی نیروی زبده کسی است که سوار بر اسب تیراندازی می‌کند و در زمانی دیگر کسی است که در شبکه جهانی اینترنت و یا حوزه خبری و رسانه‌ها به جنگ روانی می‌پردازد. فراهم‌آوری و آموزش نیرو زبده به معنای آن است که در همه زمینه‌ها (توان و نیرو) از آمادگی لازم و بازدارنده برخوردار باشیم. در همه این ابزارها و نیروها آن چه مهم و اساسی است اصل هراس انگیزی و ایجاد بازدارندگی است (ترجمه تفسیر مجمع البیان(ج ۳)، ۱۳۷۹ : ۱۱۲).

سیاست‌ها و تدابیر جمهوری اسلامی ایران

جمهوری اسلامی ایران در پیروی از آموزه‌های دینی جهت حفظ امنیت کشور و مردم، علاوه‌بر تدابیری که برای حفاظت سامانه‌های مختلف در مقابل حملات احتمالی سایبری اتخاذ کرده، در راستای بازدارندگی نیز تدابیری را اتخاذ کرده است که موارد ذیل از آن جمله‌اند:

الف) رویکرد تهدید در مقابل تهدید

مقام معظم رهبری و فرماندهی معظم کل قوا حضرت آیت‌الله العظمی امام خامنه‌ای (مدظله‌العالی) با ابلاغ تدبیر «تهدید در مقابل تهدید»، ایده جدیدی را در عرصه دفاعی مطرح کردند که در واقع همان رویکرد بازدارندگی است. ایشان نیروهای مسلح را مایه امنیت خاطر ملت و مصونیت‌ساز در مقابل توهمات تجاوزکارانه بیگانگان دانستند و تأکید کردند: ملت ایران به پیروی از تعالیم اسلام اهل تجاوز و تعرض نیست اما در مقابل هیچ تجاوزی نیز کوتاه نخواهد آمد. ایشان با تأکید بر اینکه انگیزه سلطه‌گران برای جنگ‌افروزی، فروش سلاح و رونق بخشیدن به صنایع نظامی وابسته به سرمایه‌داران است، افزودند: تنها عاملی که موجب تضعیف انگیزه جنگ‌افروزی قدرت‌طلبان و یا از بین رفتن این انگیزه می‌شود، آمادگی عمومی ملت و آمادگی دفاعی نیروهای مسلح است. رهبر انقلاب اسلامی خاطر نشان کردند: احساس آمادگی عمومی در ملت ایران به‌ویژه جوانان، امروز بیش از هر زمان دیگر است و نیروهای مسلح نیز بسیار آماده‌تر و تواناتر از گذشته هستند.

ب) بازدارندگی در سیاست‌های کلی کشور

سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا) و سیاست‌های کلی پدافند غیرعامل در بهمن ماه سال ۱۳۸۹ از سوی مقام معظم رهبری ابلاغ شد.

۱) سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)

در این ابلاغیه، سیاست‌های ناظر بر ایمن‌سازی و حفاظت، توسعه دانش و فناوری‌ها در حوزه سایبر، پیشگیری و بازدارندگی و تعامل‌های بین‌المللی و منطقه‌ای مورد توجه قرار گرفته است. در بند پنجم این سیاست‌ها تصریح شده است:

پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات.

۲) سیاست‌های کلی پدافند غیرعامل

در سیاست‌های کلی پدافند غیرعامل نیز بازدارندگی در مقابل تهدیدهای و اقدامات نظامی دشمن، طبقه‌بندی مراکز و به‌کارگیری اصول و ضوابط پدافند غیرعامل در مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به‌منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای نام برده شده است.

پیشینه تحقیق

پیشینه‌های تحقیقاتی مرتبط با این پژوهش در دو حوزه سایبر و بازدارندگی هستند که هر دو جزء موضوعاتی هستند که سابقه توجه به آنها در حوزه پژوهشی به سال‌های اخیر برمی‌گردد:

پروژه‌های تحقیقاتی و مقاله‌های متعددی در حوزه سایبر انجام و بخشی از آن‌ها منتشر شده‌اند، لیکن بخشی از پروژه‌های تحقیقاتی دارای طبقه‌بندی می باشند. پروژه تحقیقاتی «طرح تدوین طرح جامع فناوری اطلاعات کشور» از آن جمله است که منجر به ارائه و تصویب سند "نظام جامع فناوری اطلاعات کشور" شده و طی آن ۷ حوزه راهبردی تدوین و به بررسی قلمروهای اساسی پرداخته است.

"الزامات جنگ مجازی و تمهیدات پدافندی برای آن" دیگر پروژه تحقیقاتی است که با هدف بررسی ارتباط بین تهدیدجنگ شبیه‌سازی شده دشمن و تمهیدات پدافندی رایانه‌ای اجرا شده و چنین نتیجه‌گیری شده که تأثیرآنتی‌ویروس‌ها برتمهیدات پدافندی در جنگ مجازی دشمن با

میانگین ٤/٦ بیشترین اثر و به میزان خیلی‌زیاد مؤثر است و میزان تعیین کلمه عبور در سطح شبکه بر تمهیدات پدافندی در جنگ مجازی دشمن با میانگین ۲/۳ پایین است.

همچنین در زمینه بازدارندگی پروژه‌های تحقیقاتی، رساله‌های دکتری و مقاله‌های علمی – پژوهشی متعددی منتشر شده‌اند که نمونه‌های زیر از آن جمله‌اند:

قنبرای (۱۳۹٤) در پروژه‌ای تحت‌عنوان «فرایند طراحی رهنامهٔ بازدارندگی همه‌جانبهٔ ج.ا. ایران در چشم‌انداز بیست‌سالهٔ کشور»، اجرا و رهنامهٔ بازدارندگی، رهنامهٔ دفاعی و رهنامهٔ امنیتی را تبیین می‌کند و رویکرد کلی رهنامهٔ بازدارندگی همه‌جانبهٔ ج.ا.ایران را دفاع مبتنی‌بر بازدارندگی همه‌جانبه بیان می‌کند.

کریمی (۱۳۹۱) در رساله دکتری با عنوان «تبیین الگوی بازدارندگی همه‌جانبه دفاعی ج.ا.ا در مقابل تهدید ناهمتراز» چنین نتیجه‌گیری کرده است که بین مولفه‌های «توان مدیریتی سطوح راهبردی»، «توان بسیج مردمی»، «توان نظامی بومی»، «عمق راهبردی مبتنی‌بر ظرفیت‌های ژئوپلیتیکی ج.ا.ا» و «الگوی بازدارندگی همه‌جانبه دفاعی ج.ا.ا در مقابل تهدید ناهمتراز» رابطه معناداری وجود دارد.

در پژوهش‌های مذکور در حوزه سایبری عمدتاً به امنیت سایبری پرداخته شده و در موضوع بازدارندگی نیز تکیه بر بازدارندگی نظامی به‌ویژه بازدارندگی متعارف بوده است و در آن‌ها بازدارندگی سایبری مورد توجه نبوده امری که در این پژوهش به دنبال دستیابی به آن هستیم.

روش تحقیق

این تحقیق به لحاظ بهره‌برداری در حوزه بازدارندگی، کاربردی و در راستای راهبردی بودن در سطح ملی و قابلیت تعمیم‌پذیری، توسعه‌ای می‌باشد.

همچنین در این تحقیق از روش ترکیبی (سه بعدی) با استفاده از روش‌های کمی و کیفی و ترکیب آن و روش دلفی جهت جمع‌آوری اطلاعات از نخبگان در حوزه سایبری و روش اکتشافی در مراجعه به اسناد و مدارک بهره‌برداری شده است.

جامعه آماری موردنظر این پژوهش، خبرگانی دارای مدرک دکتری یا کارشناسی‌ارشد مستقر در شهر تهران هستند که در مقوله موضوع مورد پژوهش، از اطلاعات و تجارب کافی برخوردار می‌باشند. این افراد کسانی هستند که سال‌ها در زمینه موضوع تحقیق در دانشگاه‌ها، مؤسسات آموزش عالی، پژوهشکده‌ها و مؤسسات علمی کشور تدریس کرده و یا در مسئولیت‌های اجرایی

کشور دارای تجارب عملی بوده و یا در مراکز تصمیم‌گیری کلان کشور قرار داشته و در این زمینه مسئولیت داشته‌اند. این افراد با توجه به جدید بودن موضوع سایبر به‌خصوص بازدارندگی در این حوزه، بسیار محدود بوده و محقق موفق به شناسایی ٤٠ نفر شد؛ بدین‌ترتیب حجم نمونه معادل حجم جامعه آماری یعنی ٤٠ نفر در نظر گرفته شد.

روایی و پایایی

در این پژوهش برای تعیین روایی پرسشنامه از روش خبرگی بهره گرفته شده است. بدین‌ترتیب که نگاشت اول در جمع خبرگی متشکل از اعضای مطالعه گروهی شهید صیاد شیرازی دانشگاه عالی دفاع ملی و اساتید این مطالعه گروهی ارائه و با نظر آن‌ها اصلاحات لازم در پرسشنامه اعمال گردید.

برای تعیین پایایی پرسشنامه از ضریب آلفای کرونباخ[1] استفاده شده است که مشهورترین ضریب اعتبار از طریق یکبار اجرای آزمون می‌باشد. با توجه به واریانس هریک از متغیرها، ضریب آلفای کرونباخ با استفاده از نرم‌افزارSPSS محاسبه گردید، با توجه به اینکه در پژوهش‌های علوم انسانی، ضریب آلفای بالاتر از ۰/۷۰ قابل‌قبول است، پایایی سوالات پرسشنامه تائید گردیدند.

جدول ۱. پایایی پرسشنامه

متغیرهای پژوهش	ضریب آلفای کرونباخ
اصول و ارزش های حاکم	۰/۸۷
چالش های اساسی	۰/۸۱
تهدید	۰/۸۰
فرصت	۰/۷۹
ضعف	۰/۸۳
قوت	۰/۸۵
راهبردهای دفاع سایبری	۰/۸٤

تجزیه‌وتحلیل داده‌ها و یافته‌های پژوهش

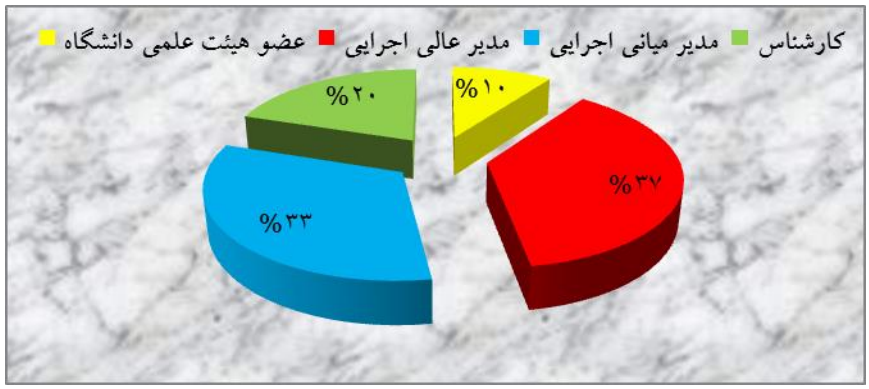
یافته‌های تحقیق با استفاده از شاخص‌های مرکزی که مهم‌ترین آن میانگین است و همچنین با بهره‌گیری از نرم‌افزار Excel و SPSS تجزیه‌وتحلیل شده است.

[1]. Cronbach Alpha

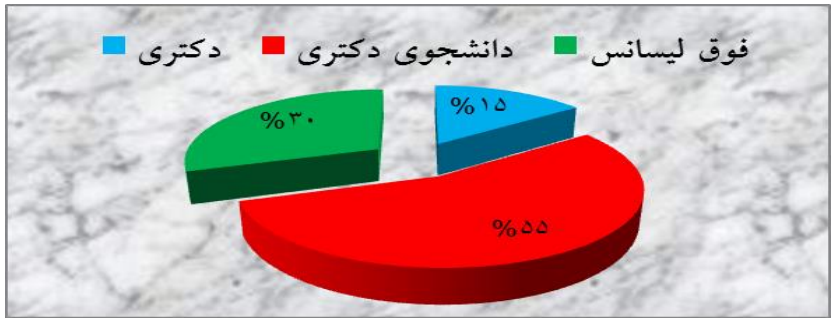
ابتدا داده‌های جمع‌آوری شده به وسیله پرسشنامه، مورد تجزیه‌وتحلیل قرار گرفت، به‌طوری‌که ابتدا فراوانی‌های مربوط به سوالات عمومی پرسشنامه (شامل: سمت، تحصیلات و سنوات خدمتی) مورد تجزیه‌وتحلیل و بررسی قرار گرفت و سپس با در نظر گرفتن درصد نظرات پاسخ‌دهندگان به هریک از گویه‌های پرسشنامه، به شناسایی بیشترین و کمترین عامل تاثیرگذار در هریک از متغیرهای پژوهش پرداخته شد.

الف) تحلیل ویژگی‌های جمعیت‌شناختی

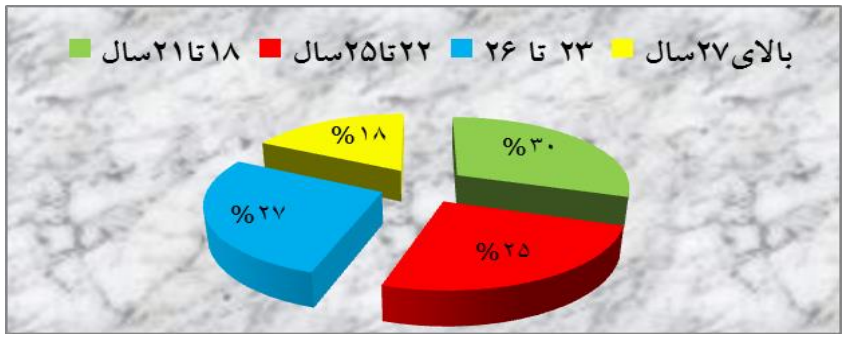
ویژگی‌های جمعیت‌شناختی در نمودارهای شماره ۱، ۲ و ۳ ارائه می‌گردند.



شکل ۱. فراوانی شرکت‌کنندگان در نظرسنجی به تفکیک سمت



شکل ۲. فراوانی شرکت‌کنندگان در نظرسنجی به تفکیک تحصیلات

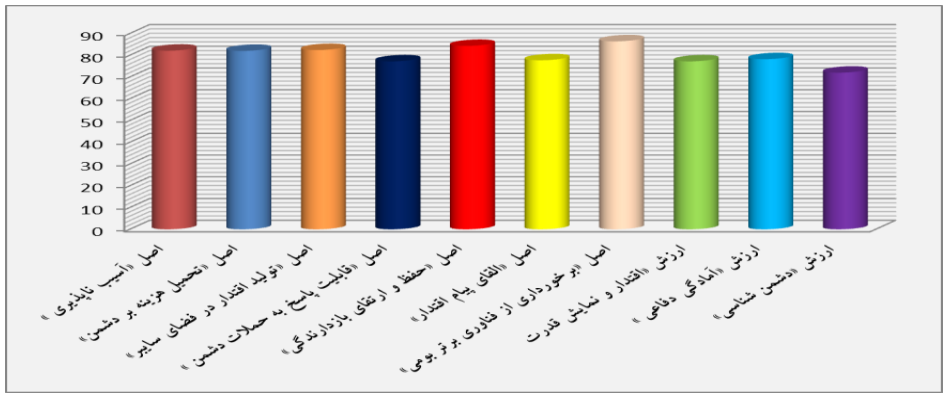


شکل ۳. فراوانی شرکت‌کنندگان در نظرسنجی به تفکیک سنوات خدمتی

ب) آمار استنباطی

در این پژوهش ابتدا درصد پاسخ‌های مربوط به هر یک از طیف ۹ درجه‌ای پرسشنامه از طریق نرم‌افزار SPSS محاسبه شده و سپس میانگین مربوط به هرکدام از سوالات پژوهش محاسبه و در نهایت میانگین کل سوالات مربوط به آن سوال برآورد تا درصد پاسخ‌های مربوط به آن حوزه مشخص شود و در مرحله بعد، اهمیت آن حوزه را محاسبه گردد. هریک از این حوزه‌ها به تفکیک در ذیل بررسی شده‌اند:

۱) اصول و ارزش‌های اساسی در حوزه بازدارندگی

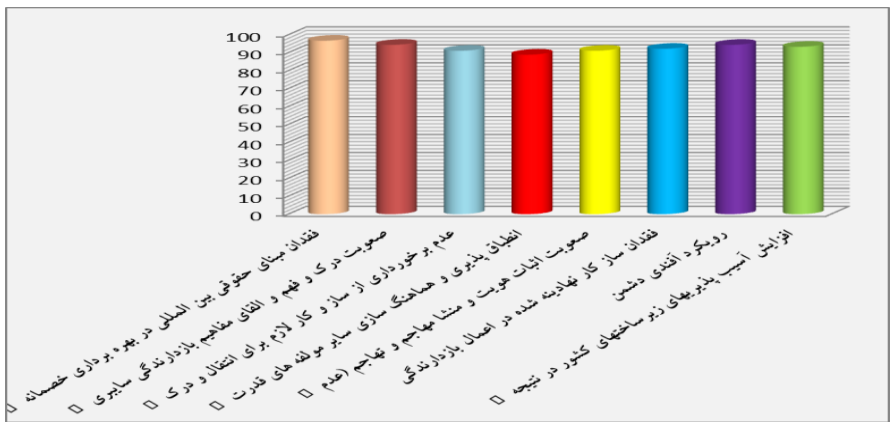


شکل ٤. اهمیت اصول و ارزشهای حاکم در حوزه بازدارندگی

در این بخش از سؤالاتِ ابعاد پروژهٔ تحقیقاتی، از مجموعِ میانگین (۷۹/۹٪)، حدّاقلِ تعداد پاسخ‌گویان (۷۲٪)، شاخصِ دشمن‌شناسی را به‌عنوان اصول و ارزش‌های اساسی در حوزهٔ بازدارندگی سایبر دانسته و در نقطهٔ مقابل، بیشترین مخاطبان (۸٦/٤٪)، «برخورداری از فناوری

برتر بومی» را نسبت به سایر شاخص‌ها بالاتر دانسته و به‌عنوان اصول و ارزش‌هـای اساسـی در حوزۀ مورد نظر معرفی نموده‌اند.

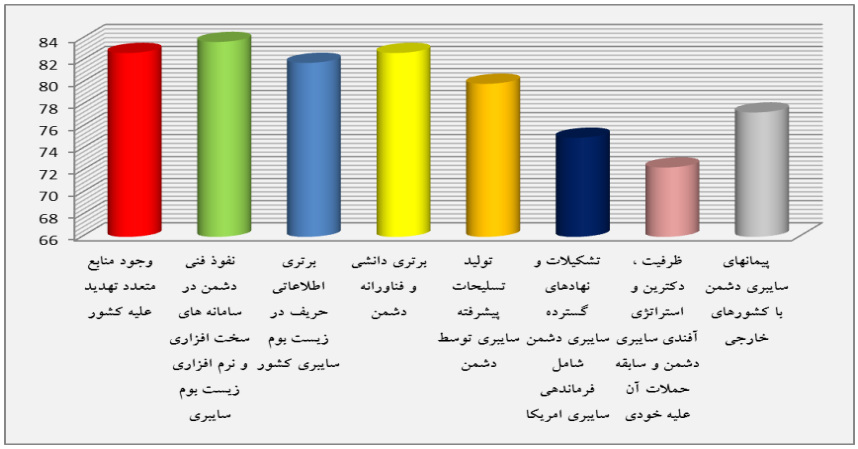
۲) چالش‌های اساسی در حوزه بازدارندگی



شکل ۵. چالش‌های اساسی در حوزه بازدارندگی

در این قسمت از سؤالاتِ ابعاد پروژۀ تحقیقاتی، از مجمـوعِ میـانگین (۹۲/۸٪)، کمتـرین تعـداد مخاطبان(۸۸/۹٪)، شاخصِ «انطباق‌پذیری و هماهنگ‌سازی سایر مولفه‌های قـدرت بـرای ایجـاد بازدارندگی سایبری» را از چالش‌های اساسی در حوزۀ بازدارندگی سایبر دانسته و از سوی دیگر بیشترین مخاطبان (۹۶/۷٪)، شاخصِ «فقدان مبنای حقوقی بین‌المللی در بهره‌برداری خصمانه از زیست‌بوم سایبری» را نسبت به مجموعِ شاخص‌ها موثرتر دیـده و آن را بـه‌عنـوان چـالش‌هـای اساسی در حوزۀ مزبور ارزیابی کرده‌اند.

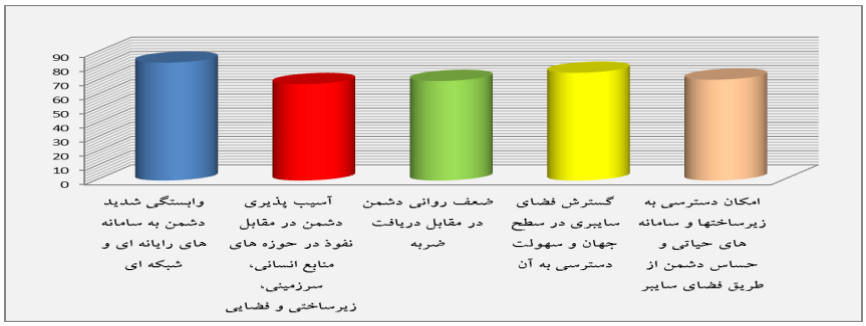
۳) تهدیدها در حوزه بازدارندگی



شکل ٦. تهدیدها در حوزه بازدارندگی

در ارتباط با این بُعد از پروژهٔ تحقیقاتی، از مجموعِ میانگین (۷۹/٤٪)، حدّاقل تعداد نخبگان (۷۲/۳٪)، شاخصِ «ظرفیت ، دکترین و استراتژی آفندی سایبری دشمن و سابقه حملات آن علیه خودی» را مهم‌ترین تهدید در حوزه بازدارندگی سایبر تشخیص داده و در نقطهٔ مقابل، بیشترین نخبگان (۸۳/۷٪)، در تشخیص خود، «نفوذ فنی دشمن در سامانه‌های سخت‌افزاری و نرم‌افزاری زیست‌بوم سایبری» را مهم‌ترین تهدید در حوزهٔ مزبور اعلام کرده‌اند.

٤) فرصت‌ها در حوزه بازدارندگی

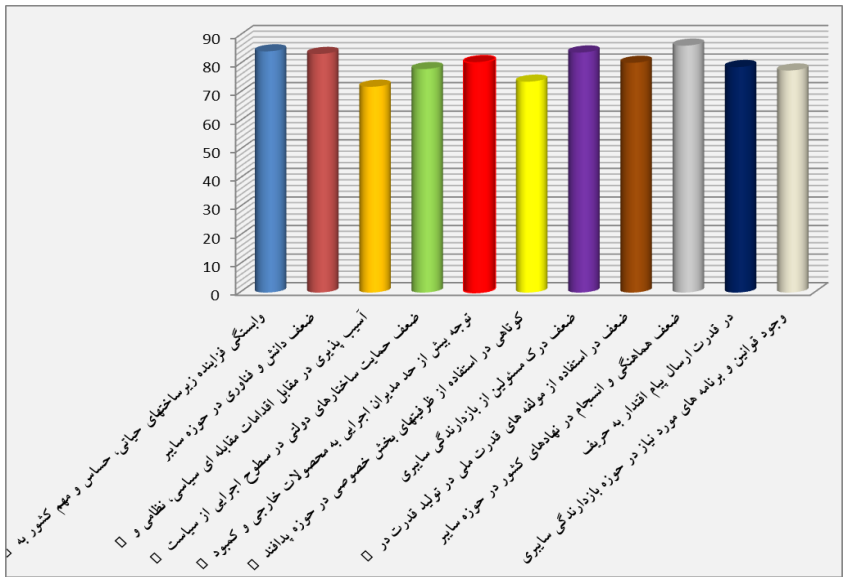


شکل ۷. فرصت‌ها در حوزه بازدارندگی

در خصوص این بُعد از پروژهٔ تحقیقاتی، از مجموعِ میانگین (۷۳/٦۸٪)، کمترین تعداد پاسخگویان (٦۸٪)، شاخصِ «آسیب‌پذیری دشمن در مقابل نفوذ در حوزه‌های منابع انسانی،

سرزمینی، زیرساختی و فضایی» اعلام کرده‌انـد و از سـوی دیگـر، بیشـترین تعـداد پاسـخگویان (۸۳/۱٪)، در اعلام نظر خود شاخصِ «وابستگی شدید دشمن به سامانه‌های رایانه‌ای و شبکه‌ای» را به‌عنوان یک فرصت در در حوزه بازدارندگی سایبرکشور ارزیابی کرده‌اند.

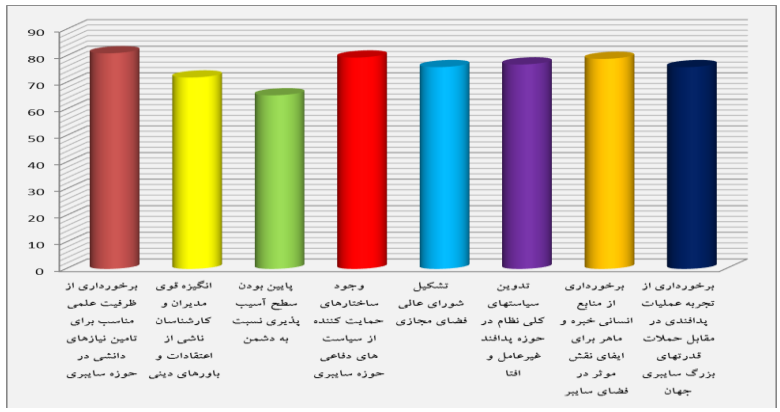
۵) ضعف‌ها در حوزه بازدارندگی



شکل ۸. ضعف‌ها در حوزه بازدارندگی

در این بخش از سؤالاتِ ابعاد پروژهٔ تحقیقاتی، از مجموعِ میانگین (۸۰٪)، حدّاقل تعداد نخبگان (۷۲٪)، در تشخیص خود شاخصِ «آسیب‌پذیری در مقابل اقدامات مقابلـه‌ای سیاسـی، نظـامی و اقتصادی دشمن» را به‌عنوان ضعف در حوزهٔ موردنظر اعلام کـرده‌انـد؛ لـیکن در نقطـهٔ مقابـل، بیشترین نخبگان (۸۴/٤٪)، در ارزیابی خویش «وابستگی فزاینده زیرساخت‌های حیاتی، حسـاس و مهم کشور به فضای سایبر که قابل‌نفوذ و آسـیب‌پـذیر اسـت» را بـه‌عنـوان ضـعف در حـوزه بازدارندگی سایبری کشور دانسته‌اند.

٦) قوت‌ها در حوزه بازدارندگی



شکل ۹. قوت‌ها در حوزه بازدارندگی

در خصوص این بُعد از پروژهٔ تحقیقاتی، از مجموعِ میانگین (۷۵/۷ ٪)، کمترین تعداد مخاطبان (٦٥/٣٪)، «پایین بودن سطح آسیب‌پذیری نسبت به دشمن» را یک قوت در حوزهٔ مربوطه می‌دانند اما از طرف دیگر، بیشترین تعداد مخاطبان (۸۱/۱٪)، در اعلام‌نظر خود شاخصِ «برخورداری از ظرفیت علمی مناسب برای تامین نیازهای دانشی در حوزه سایبری» را به‌عنوان قدرت در این حوزه اعلام کرده‌اند.

۷) راهبردهای بازدارندگی سایبر

شکل ۱۰. راهبردهای بازدارندگی سایبر

در این قسمت از سؤالاتِ ابعاد پروژهٔ تحقیقاتی، از مجموعِ میانگین (۸۱/٤٪)، حدّاقل تعداد نخبگان (۷۲/۷٪) در تشخیص خود شاخصِ «تعریف، تبیین و اعمال منافع ملی سایبری کشور با

درجه‌بندی حیاتی و مهم» را به‌عنوان راهبردهای بازدارندگی سایبر دانسته‌اند و در نقطهٔ مقابل نیز بیشترین تعداد نخبگان (۸۵/۷٪)، در نظرات خویش راهبردهای «تولید ظرفیت و قدرت پاسخگویی قاطع به تهدیدهای سایبری» و «نمایش قدرت و اقتدار سایبری از طریق رزمایش و تولید پیام اقتدار طی فرآیند متمرکز و انتقال پیام» را به‌عنوان راهبردهای حوزه بازدارندگی سایبری ارزیابی کرده‌اند.

نتیجه‌گیری و پیشنهاد

هدف اصلی تحقیق حاضر ارائه راهبردهای دفاع سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی بوده است.

در اجرای این تحقیق و در درجه نخست با انجام مطالعات اکتشافی و انجام مطالعات نظری و با استفاده از اسناد و مدارک معتبر مبادرت به شناخت کلیاتی از وضعیت سایبری در حوزه بازدارندگی نموده و سپس با مراجعه به جامعه خبرگی و جامعه آماری در صدد پاسخ‌گویی به سؤالات پژوهشی به شرح زیر برآمده است:

- ***پاسخ به سوال فرعی اول*** مبنی‌بر "اصول، ارزش‌ها و چشم‌انداز دفاع سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی کدامند؟"

۱) اصول: اصول حاکم در برابر تهدیدهای سایبری در حوزه بازدارندگی عبارتند از: آسیب‌ناپذیری؛ تحمیل هزینه بر دشمن؛ پاسخ به حملات دشمن؛ حفظ و ارتقای بازدارندگی؛ پشیمان‌کنندگی؛ القای پیام اقتدار و برخورداری از فناوری بومی برتر که به‌ترتیب تشریح می‌گردند:

۱-۱) آسیب‌ناپذیری

اگر رقبا به این نتیجه برسند که حملات سایبری نمی‌توانند به اهداف‌شان در آسیب وارد کردن بر شبکه‌های اطلاعاتی خودی دست یابند، تمایل کم‌تری به تحمل هزینه‌ها و ریسک‌های راه‌اندازی آن‌ها خواهند داشت. هرچه آسیب‌پذیری شبکه‌های خودی بیشتر باشد، امید برای بازدارندگی موثر را تضعیف می‌کند.

۱-۲) تحمیل هزینه بر دشمن

هدف یک راهبرد بازدارندگی سایبر نفوذ بسیار قاطعانه در محاسبات تصمیم‌سازی یک رقیب است تا حملات سایبری علیه منافع خودی راه نیاندازد. اقدامات هماهنگ‌شده، شانس‌های موفقیت حمله‌کننده را کاهش می‌دهند به‌طوری‌که خطرات، هزینه‌ها، ریسک‌ها و ابهامات یک

حمله سایبری، از سود یا پاداش مورد انتظار مشخص می‌شود. دشمن باید بداند که در صورت اقدام به حمله، با هزینه سنگینی مواجه خواهد شد.

۳-۱) پاسخ به حملات دشمن

آنچه مسلم است ضرورت آمادگی برای پاسخ به حملات جدی دشمن است تا با درک او از چنین آمادگی و اراده‌ای، تصمیم به حمله سایبری نگیرد.

٤-۱) حفظ و ارتقای بازدارندگی

توان بازدارندگی نمی‌تواند در یک مقطع زمانی تامین و کنار گذاشته شود؛ بلکه این توان علاوه‌بر اینکه حفظ می‌شود باید تدابیری برای ارتقای مستمر آن اتخاذ شود تا بتواند مفهوم بازدارندگی را حفظ کند.

۵-۱) پشیمان کنندگی

پاسخ به حمله دشمن باید به قدری شدید، سریع، قاطع و ... باشد که مهاجم از حمله خود پشیمان شود. این امر به‌معنای تحمیل هزینه‌ای بر دشمن است که بیش از سودی باشد که او از حمله برده است. زمانی‌که دشمن به این قابلیت پی‌ببرد، تصمیم به حمله نخواهد گرفت و این قدرت بازدارنده خواهد بود.

٦-۱) القای پیام اقتدار

القا کردن در لغت به‌معنای رسانیدن سخن و آگاه کردن کسی به شیوه مستقیم یا غیرمستقیم آمده است. اقتدار با هدف بازدارندگی در صورتی مؤثر خواهد بود که پیام آن به دشمن برسد. تا زمانی‌که این پیام به طرف مقابل القا نشده، وجود اقتدار کارکرد لازم را نخواهد داشت. القای پیام با استفاده از شیوه‌ها و ابزارهای مختلف رسانه‌ای صورت می‌گیرد.

۷-۱) برخورداری از فناوری بومی برتر

برخورداری از فناوری در حوزه‌های زیرساخت‌ها اطلاعاتی و شبکه امکان نفوذناپذیری و کاهش آسیب‌پذیری آن‌ها را فراهم می‌آورد به شرطی‌که این فناوری بومی باشد زیرا فناوری غیربومی و وابسته در صورت پیشرفته بودن هم برای دشمن قابل نفوذ خواهد بود، لذا بازدارندگی ایجاد نخواهد کرد.

۲) ارزش‌ها: ارزش‌های حاکم در برابر تهدیدهای سایبری در حوزه بازدارندگی عبارتند از: اقتدار و نمایش قدرت؛ آمادگی دفاعی و ارعاب دشمن که به‌ترتیب تشریح می‌گردند:

۲-۱) اقتدار و نمایش قدرت

اقتدار به معنای برخورداری از شرایطی است که طرف مقابل را بدون استفاده از زور وادار کند تا کاری را که نمی‌خواهیم انجام ندهد و یا کاری را انجام دهد که موردنظر ماست. هرچند قدرت یکی از ابزارها و عوامل اقتدار است اما اقتدار صرفاً با قدرت به‌دست نمی‌آید. یکی از راه‌های کسب اقتدار از طریق قدرت نمایش آن است و از این طریق می‌توان قدرت را به اقتدار تبدیل کرد. یکی از ابزارهای ترساندن دشمن که در آیه ٦٠ سوره انفال مورد تاکید قرار گرفته، قدرت و نمایش آن است.

۲-۲) آمادگی دفاعی

اصل کلی که قرآن در آیه ٦٠ سوره انفال به‌صورت آموزه‌ای دستوری به مسلمانان آموزش می‌دهد فراهم‌آوری توان و نیرو است. توان شامل هرگونه ابزار و آلات بازدارنده و یا هجومی و یا دفاعی است. از این‌رو تنها به سلاح اشاره نشده است. تهیه هر چیزی که قدرت امت و دولت اسلامی را افزایش می‌دهد، امری لازم و ضروری است و با توجه به شرایط مکانی و زمانی تغییر می‌کند.

۲-۳) ارعاب دشمن

تنها برخورداری از قدرت و آمادگی دفاعی، تامین‌کننده نیاز دفاع به‌خصوص در حوزه بازدارندگی نخواهد بود و خداوند در آیه ٦٠ سوره انفال، به صراحت به این اصل تاکید می‌کند و پس از ضرورت آمادگی، ارعاب دشمن را نیز خواستار است.

۳) چشم‌انداز: چشم‌انداز جمهوری اسلامی ایران در برابر تهدیدهای سایبری در حوزه بازدارندگی به شرح ذیل بیان می‌گردند.

۳-۱) بیانیه چشم‌انداز

جمهوری اسلامی ایران در افق ۱۰ ساله کشوری است با قدرت ممتاز سایبری در حوزه بازدارندگی، پاسخ‌گویی به تهدید و پشیمان‌کنندگی است به‌طوری‌که بتواند در مقابل تهدیدهای سایبری، ایجاد بازدارندگی مطلوب نماید. معاونت حوزه بازدارندگی قرارگاه پدافند سایبری کشور دارای رتبه یکم در چارچوب افق ۱۰ ساله دارای چشم‌انداز زیر است:

- برخوردار از ساختار دفاعی آسیب‌ناپذیر و نفوذناپذیر در حوزه‌های حیاتی و حداقل آسیب‌پذیری در مقابل تهدیدهای و حملات سایبری با ویژگی‌های: تاب‌آوری؛ قابلیت کاهش خسارت و زمان ترمیم؛ انعطاف در گزینش و ترجیح شیوه دفاع لایه‌ای.

– برخوردار از ظرفیت و توان دفاعی و آفندی پاسخ‌گویی سایبری به تهدیدهای سایبری دشمن با ویژگی‌های قابلیت کشف سریع حملات و نفوذها و منشاء آن‌ها؛ قابلیت پاسخ مناسب قاطعانه و هماهنگ؛ دارای طرح‌های مناسب، منعطف و مطمئن تهاجمی علیه تهدیدها؛ دارای قدرت تهاجمی قابل رقابت با متخاصمین.

– دارای ظرفیت و توان تحمیل خسارات غیرمنتظره و غیرقابل باور به دشمن با هدف پشیمان کردن و انصراف از تهدید علیه سامانه‌های سایبری کشور با ویژگی‌های شدید، قاطع، مقتدر، سریع و مهلک.

– برخوردار از اقتدار دفاعی و صلابت و القای پیام اقتدار به دشمن با ویژگی‌های دارای رسانه‌های کارآمد در انتقال پیام؛ دارای قدرت پذیرفته شده به‌وسیلهٔ رقبا؛ باثبات و خودباور.

– دارای نظام پایش، به‌روز شونده و بازتولیدکننده بازدارندگی سایبری برای دشمن و ارتقای بازدارندگی با ویژگی‌های دارای قدرت اطلاعاتی سایبری برتر؛ چابک؛ پویا و اطمینان‌بخش.

– برخوردار از نظام پدافند سایبری توسعه‌یافته با قابلیت مقاومت و پایداری زیرساخت‌ها در برابر تهدیدها با ویژگی‌های برخوردار از نیروهای ماهر و کارآمد در حوزه سایبری؛ دارای عزم بکارگیری قدرت سایبری؛ بهره‌مند از قابلیت هم‌افزایی سایر مولفه‌های قدرت در پاسخ‌گویی به حملات سایبری دشمن؛ برخوردار از فرماندهی و کنترل موثر، شبکه‌ای، امن، سریع، هماهنگ و ملی.

– دستیافته به زیرساخت‌های حیاتی پایدار و آسیب‌ناپذیر و زیرساخت‌های حساس با حداقل آسیب‌پذیری در زیرساخت‌های مهم با ایمنی لازم در مقابل دشمن با ویژگی‌های برخوردار از فناوری بومی و تمرکز در هدایت.

– برخوردار از نظام دفاعی جمعی (پروتکل‌ها و پیمان‌های دفاعی) سایبری کشورهای مسلمان، قدرت‌های منطقه‌ای همکار و هم‌پیمان در حوزه نظامات دفاع سایبری با ویژگی‌های مبادله اطلاعات، آموزش و رزمایش مشترک، اعتماد متقابل، همکار در مجمع بین‌المللی.

– ***پاسخ به سوال فرعی دوم*** مبنی‌بر "مأموریت‌های طرح راهبردی دفاع سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی کدام است؟"

۱) رسالت: تامین بازدارندگی در مقابل حملات سایبری علیه زیست‌بوم ملی سایبری.

۲) مأموریت: معاونت حوزه بازدارندگی قرارگاه پدافند سایبری کشور مأموریت دارد با آسیب‌ناپذیرسازی زیرساخت‌های اساسی کشور در مقابل تهدیدهای و پاسخ به تهدیدها و حملات سایبری دشمن و برخورداری از قدرت پشیمان‌کنندگی دشمن در جهت تأمین بازدارندگی اقدام کند.

۳) وظایف: وظایف عمده معاونت حوزه بازدارندگی این قرارگاه به شرح زیر خواهد بود:

- طراحی ساختار دفاعی آسیب‌ناپذیر و نفوذناپذیر در زیرساخت‌های حیاتی و دفاع اطمینان‌بخش و لایه‌ای در مقابل حملات سایبری.
- طراحی و اقدام جهت حداکثر کاهش خسارات وارده به تاسیسات کشور در نتیجه حملات سایبری و کاهش زمان ترمیم آن‌ها.
- تامین ظرفیت و توان آفندی پاسخ‌گویی سایبری به تهدیدهای سایبری دشمن.
- تهیه طرح‌های مناسب، منعطف و مطمئن تهاجمی علیه تهدیدها.
- تامین قابلیت تولید پیام اقتدار سایبری و رسانه‌های انتقال‌دهنده پیام به رقبا.
- رصد، پایش، کنترل و برآورد اطلاعاتی تهدیدهای سایبری دشمن.
- ترمیم و به‌روز شوندگی بازدارندگی چابک، پویا و اطمینان‌بخش.
- آموزش، تمرین، رزمایش و نمایش قدرت و آماده‌سازی نیروهای ماهر و کارآمد در حوزه سایبری.

- ***پاسخ به سوال فرعی سوم*** مبنی‌بر "عوامل خارجی و داخلی مؤثر در دفاع سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی کدامند؟"

۱) تهدیدها

- نفوذ فنی دشمن در سامانه‌های سخت‌افزاری و نرم‌افزاری زیست‌بوم سایبری.
- وجود منابع متعدد تهدید علیه کشور.
- برتری دانشی و فناورانه دشمن.
- برتری اطلاعاتی حریف در زیست‌بوم سایبری کشور.
- تولید تسلیحات پیشرفته سایبری توسط دشمن.
- پیمان‌های سایبری دشمن با کشورهای خارجی.

۲) فرصت‌ها

- وابستگی شدید دشمن به سامانه‌های رایانه‌ای و شبکه‌ای.

– گسترش فضای سایبری در سطح جهان و سهولت دسترسی به آن.
– امکان دسترسی به زیرساخت‌ها و سامانه‌های حیاتی و حساس دشمن از طریق فضای سایبر ضعف روانی دشمن در مقابل دریافت ضربه.

۳) ضعف‌ها

– ضعف هماهنگی و انسجام در نهادهای کشور در حوزه سایبر.
– وابستگی فزاینده زیرساخت‌های حیاتی، حساس و مهم کشور به فضای سایبر که قابل نفوذ و آسیب‌پذیر است.
– ضعف درک مسئولین از بازدارندگی سایبری.
– کوتاهی در استفاده از ظرفیت‌های بخش خصوصی در حوزه پدافند سایبری.
– ضعف دانش و فناوری در حوزه سایبر.

٤) قوت‌ها

– برخورداری از ظرفیت علمی مناسب برای تامین نیازهای دانشی در حوزه سایبری.
– وجود ساختارهای حمایت‌کننده از سیاست‌های دفاعی حوزه سایبری.
– برخورداری از منابع انسانی خبره و ماهر برای ایفای نقش موثر در فضای سایبر.
– تدوین سیاست‌های کلی نظام در حوزه پدافند غیرعامل و افتا.
– تشکیل شورای عالی فضای مجازی.

– ***پاسخ به سؤال اصلی*** مبنی‌بر "راهبردهای دفاع سایبری کشور در برابر تهدیدهای سایبری در حوزه بازدارندگی چیست؟"

بازدارندگی هرچند مفهومی است که در دوره جنگ سرد و در حوزه هسته‌ای بکار گرفته شد اما به مرور در حوزه‌های دیگر نیز کاربرد یافت و از جمله در حوزه سایبر اتخاذ تدابیری برای اینکه حریف از دست‌زدن به حمله باز داشته شود و در واقع طوری به او القاء شود که هزینه هرگونه حمله‌ای برای او بیش از منافع آن خواهد بود. هرچند بازدارندگی در حوزه سایبر متفاوت و پیچیده‌تر از بازدارندگی نظامی است اما با رعایت الزامات آن و بهره‌گیری از شیوه‌های مناسب به آن دست یافت تا هزینه دفاع را نیز کاهش دهد.

برای دستیابی به راهبردهای در دفاع سایبری، منابع دینی، اسناد بالادستی، مبانی نظری، مطالعات تطبیقی و سایر مطالعات در حوزه بازدارندگی انجام و اصول و ارزش‌های حاکم بر طرح، عوامل

خارجی و داخلی مؤثر بر آن و چشم‌انداز و رسالت و مأموریت قرارگاه دفاع سایبری احصاء و راهبردهای دفاع سایبری مورد مطالعه قرار گرفت و تجزیه‌وتحلیل داده‌ها براساس آن‌ها و با استفاده از نرم‌افزار EXCEL و نرم‌افزار SPSS صورت گرفت.

مهم‌ترین و موثرترین راهبردهای پیشنهادی در بازدارندگی سایبری به شرح زیر می‌باشند:

- تولید ظرفیت و قدرت پاسخ‌گویی قاطع به تهدیدهای سایبری.
- نمایش قدرت و اقتدار سایبری از طریق رزمایش و تولید پیام اقتدار طی فرآیند متمرکز و انتقال پیام.

منابع و مآخذ

الف) منابع فارسی

- بیانات و سخنرانی‌های حضرت آیت‌الله العظمی امام خامنه‌ای، قابل دسترسی در سایت: www.khamenei.ir
- ازغندی، علی‌رضا؛ روشندل، جلیل (۱۳۷٤). مسائل نظامی و استراتژی معاصر، تهران: انتشارات سمت.
- اشرفی‌ریزی، حسن؛ کاظم‌پور، زهرا (۱۳٦۸). مفهوم جغرافیای سیاسی اطلاعات، تهران: نشر چاپار.
- افشردی محمدحسین؛ نوروزانی، شهرام؛ نوشادی رضا (۱۳۹۳). «کارکرد الگوی بازدارندگی طالبان در جنگ پیشگیرانه امریکا علیه افغانستان در سال ۲۰۰۱ (با تأکید بر عوامل داخلی افغانستان)»، فصلنامه دفاعی استراتژیک، سال دوازدهم، شماره ٥٦.
- امیدوارنیا، محمدجواد (۱۳۸۱). امنیت در قرن بیست و یکم، تهران: نشر دفتر مطالعات سیاسی و بین‌المللی.
- ام.الیوت، جفری؛ رجینالد، رابرت (۱۳۷۸). فرهنگ اصطلاحات سیاسی و استراتژیک، ترجمه میرحسین رئیس‌زاده، تهران: دفتر مطالعات سیاسی و بین‌المللی.
- جان‌پرور، محسن؛ حیدری موصلو، طهمورث (۱۳۹۰). «آسیب‌شناسی فضای سایبر بر امنیت اجتماعی»، فصلنامه نظم و امنیت اجتماعی، دوره چهارم، شماره سوم.
- حسن‌بیگی، ابراهیم (۱۳۸۸). حقوق و امنیت در فضای سایبر، تهران: دانشگاه عالی دفاع ملی.
- حسن‌بیگی، ابراهیم (۱۳۹۰). مدیریت راهبردی، تهران: انتشارات سمت.
- خلیلی‌پور رکن‌آبادی، علی؛ نورعلی‌وند، یاسر (۱۳۹۱). «تهدیدات سایبری و تاثیر آن بر امنیت ملی»، فصلنامه مطالعات راهبردی، شماره دوم، سال پانزدهم.
- دوئرتی، جیمز (۱۳۷۲). نظریه‌های متعارض در روابط بین‌الملل، ترجمه علی‌رضا طیب و وحید بزرگی، جلد دوم، تهران: انتشارات قومس.
- صلاحی، سهراب؛ کشفی، سیدمهدی (۱۳۹۵). «جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تامین»، دوفصلنامه مطالعات نرم، دوره ششم، شماره چهاردهم.
- عباسی، مجید؛ مرادی، حسین (۱۳۹٤). «جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه»، فصلنامه مجلس و راهبرد، دوره بیست و دوم، شماره ۸۱.

– عسگرخانی، ابومحمد (۱۳۷۷). «سیری در نظریه‌های بازدارندگی خلع سلاح و کنترل تسلیحات هسته‌ای»، مجله‌ی سیاست دفاعی، شماره ۲۵.

– طبرسی، امین‌الاسلام (۱۳۷۹). ترجمه تفسیر مجمع‌البیان (جلد ۳)، ترجمه علی کرمی، تهران: موسسه انتشارات فراهانی.

– قاسمی، فرهاد (۱۳۹۱). «بازسازی مفهومی نظریهٔ بازدارندگی منطقه‌ای و طراحی الگوهای آن بر اساس نظریه‌های چرخهٔ قدرت و شبکه»، فصلنامهٔ راهبرد دفاعی، سال دهم، شماره ۳۸.

– قنبری‌جهرمی، محمدحسین (۱۳۹٤). فرایند طراحی رهنامهٔ بازدارندگی همه‌جانبهٔ ج.ا. ایران در چشم‌انداز بیست‌سالهٔ کشور، تهران: مرکز تحقیقات راهبردی دفاعی.

– کریمی، حمید (۱۳۹۱). تبیین الگوی بازدارندگی همه‌جانبه دفاعی ج.ا.ا در مقابل تهدید ناهمتراز، رساله دکتری، تهران: دانشگاه و پژوهشگاه عالی دفاعی ملی و تحقیقات راهبردی.

– مکارم شیرازی، ناصر (۱۳۵۳). تفسیر نمونه (جلد ۸)، تهران: انتشارات دارالکتب الاسلامیه.

– نورمحمدی، مرتضی (۱۳۹۰). «جنگ نرم، فضای سایبر و امنیت جمهوری اسلامی ایران»، فصلنامه راهبرد و فرهنگ، شماره شانزدهم.

ب) منابع انگلیسی

- Abraham, Stanley, (2012). strategic planning a practical guide for competitive success, US, Harwad house.

- Barksdole, susan and Lound teri (2006). 10 steps to success strategic planning, Virginia alexanderia.

- Franklin D. (2009). Kramer, Cyberpower and National Security, U.S National Defense University, Washington D.C.