نشریه علمی "پدافند الکترونیکی و سایبری "
سال هشتم، شماره ۴، زمستان ۱۳۹۹، ص ۱۷۳-۱۶۱

علمی– پژوهشی

توسعه مفهوم نظریه بازدارندگی در فضای سایبری کشور بر اساس اسناد بالادستی و رویکردهای موجود

غلامرضا جلالی فراهانی[1*]، محمدصادق بیک‌پوری[2]

۱- دانشیار علوم دفاعی راهبردی دانشگاه عالی دفاع ملی ۲- دانشجوی دکتری مدیریت راهبردی پدافند غیرعامل دانشگاه عالی دفاع ملی

(دریافت: ۱۳۹۹/۰۷/۱۲، پذیرش: ۱۳۹۹/۰۹/۱۵)

چکیده

جلوگیری از آسیب در فضای سایبری شامل فرآیندهای پیچیده‌ای از قبیل تهدید، مجازات، عدم پذیرش، گرفتاری و هنجارها است. هدف این مقاله، روشن کردن برخی از این ابعاد مفهومی و خط‌مشی استفاده از نظریه بازدارندگی در قلمروی سایبری جمهوری اسلامی ایران است. فرمول‌بندی راهبرد کارآمدی در عرصه سایبر، نیاز به شناخت عمیق‌تر ابعاد مختلف بازدارندگی و جلوگیری در دامنه سایبر دارد. تدوین نظریه پایه بازدارندگی در برابر تهدیدات سایبری دشمن در فضای سایبری کشور مستلزم شناخت دقیق حوزه آفندی و پدافندی و تدوین راهبردهایی بر اساس نظریه پایه بازدارندگی در فضای سایبری است که متأسفانه مورد غفلت واقع شده است. مسئله ما در این پژوهش فقدان نظریه مدون برای ایجاد بازدارندگی در فضای سایبری کشور، در رویارویی با تهدیدات سایبری و به‌تبع آن شناخت الزامات بازدارندگی در فضای مجازی کشور بر اساس اسناد بالادستی و رویکردهای موجود است به شکلی که در برابر تهدیدات دشمن مقاوم، مستحکم و باقابلیت تداوم کارکردها و درعین‌حال بتواند به تهدیدات دشمن پاسخ پشیمان کننده بدهد. ایجاد و استفاده از همه ظرفیت‌های سایبری (انسانی و فنی) به‌منظور آمادگی برای تطابق و تاب‌آوری (انعطاف‌پذیری) در شرایط متغیر و پویای سایبری یک ضرورت غیرقابل‌انکار است که ضمن پایداری و تسلط حاکمیتی موجب حفظ و افزایش منافع و اهداف ملی خواهد شد. این موضوع بایستی به‌عنوان یک ارزش اساسی و ملی در نظریه بازدارندگی موردتوجه باشد. در شرایط عدم قطعیت و همچنین پویایی فضای سایبری و تهدیدات آن، به‌منظور جلوگیری از شکست بازدارندگی با توجه به چالش شناخت منبع تهدید، به نظر می‌رسد که نظریه تکاملی برای به‌دست آوردن راهبردهای مطلوب، ارجح و پایدار، بروز رسانی و ترمیم مداوم آن است. در این پژوهش بر اساس نظر خبرگان ارتباطات و فناوری اطلاعات و پدافند غیرعامل در دانشگاه و دستگاه‌های اجرایی، مطلوبیت‌های راهبردی بازدارندگی سایبری (چشم‌انداز، اهداف کلان، ارزش‌های اساسی حاکم، اصول، الزامات در اسناد بالادستی) احصا و در جلسات خبرگی به تأیید آنان رسید.

کلیدواژه‌ها: فضای سایبر، بازدارندگی سایبری، تهدیدات سایبری

۱- مقدمه

فضای سایبری یکی از مؤلفه‌های امنیت ملی کشورها تلقی می‌شود، واکنش طبیعی کشورها در مقابل هرگونه تهدید یا تجاوز به قلمرو سایبری آن‌ها، استفاده از زور علیه متجاوز خواهد بود و ازآنجاکه این تجاوز از فضای سایبر آغاز شده است، طبیعتاً اولین پاسخ نیز در همین فضا داده خواهد شد، اگرچه به‌منظور تأمین بازدارندگی، معمولاً پاسخ کشورها به تجاوز سایبری تنها به پاسخ سایبری محدود نشده و از ابعاد همه‌جانبه اعم از سایبری، سیاسی، اقتصادی، اطلاعاتی و نظامی برخوردار خواهد بود. [۱]

فضای سایبر کشور، باید به‌صورت مداوم مورد رصد و پایش قرارگرفته و هرگونه تهدید، آسیب‌پذیری، مخاطره، تهاجم و حادثه سایبری و پیامد اعم از سایبری، فیزیکی و روانی، مورد شناسایی قرارگرفته و اقدام‌های مقابله‌ای برای کاهش و رفع آن‌ها انجام می‌گیرد. این اقدام‌های دفاعی باید در سطحی انجام گیرد که منجر به تأمین بازدارندگی دفاعی در فضای سایبر کشور شود و برای این منظور، لازم است قدرت سایبری به‌عنوان بخشی از قدرت نظامی کشور تحقّق یابد.

به‌طورمعمول شناخت بازدارندگی در فضای سایبری مشکل است زیرا بازدارندگی در اذهان ما توسط تصاویری از جنگ سرد به‌عنوان تهدید انتقام شدید توسط ابزارهای نظامی تسخیر شده است. بااین‌حال، مقایسه با بازدارندگی نظامی، گمراه‌کننده است. جلوگیری از آسیب در فضای سایبری شامل فرآیندهای پیچیده‌ای از قبیل تهدید، مجازات، عدم پذیرش، گرفتاری و هنجارها است. هدف این مقاله، روشن کردن برخی از این ابعاد

*رایانامه نویسنده مسئول: jalal826_s@yahoo.com

مفهومی و خط‌مشی استفاده از نظریه بازدارندگی در قلمروی سایبری جمهوری اسلامی ایران است. فرمول‌بندی راهبرد کارآمدی در عرصه سایبر، نیاز به شناخت عمیق‌تر ابعاد مختلف بازدارندگی و جلوگیری در دامنه سایبر دارد.

۲- بیان مسئله

گسترش منازعات به فضای سایبری و استفاده از ابزارهای فناوری اطلاعات و ارتباطات در قالب "تسلیحات سایبری" برای تهدید زیرساخت ملی کشورها توسط حریفان سیاسی به شکل جنگ سایبری یا توسط گروه‌های معارض با مفهوم تروریسم سایبری، لزوم توسعه و گسترش مفاهیم بازدارندگی سنتی به فضای سایبری را به‌عنوان راهبردی جهت جلوگیری از ایراد خسارت به منافع ملی کشورها، آشکار نموده است.

بازدارندگی سایبری، بر پایه اصول حاکم بر نظریه‌های بازدارندگی سنتی شکل‌گرفته است. برخی ویژگی‌های متمایز فضای سایبری به‌عنوان عرصه پنجم نبردها نظیر مشکل "عدم قطعیت در نسبت دادن حملات سایبری"، خصوصیاتی ویژه به بازدارندگی سایبری بخشیده است. اما با توجه به محدودیت تفکر بازدارندگی سنتی که در مورد دفاع سایبری استفاده می‌شود، آیا بازدارندگی سایبری می‌تواند به‌دست آید؟ امید قابل‌توجهی وجود دارد که بازدارندگی سایبری می‌تواند یک راهبرد مفید و مؤثر باشد، به‌ویژه زمانی که برای همه رهبران جامعه بیشتر از دیگران درک شود.

در حال حاضر آنچه قطعی است این است که بازدارندگی سایبری در حوزه غیرنظامی، علاوه بر پوشش کامل امنیت ایستا و دفاع فعال معطوف به توانمندی‌های پیش‌نگری و پیشگیری در حوزه‌های زیرساختی است و حوزه نظامی بر دفاع فعال و توانمندی‌های تهاجمی بازدارنده تمرکز بیشتری باید داشته باشند تدوین نظریه پایه بازدارندگی در برابر تهدیدات سایبری دشمن در فضای سایبری کشور مستلزم شناخت دقیق حوزه آفندی و پدافندی و تدوین یک چارچوب پیوست نگاری است که متأسفانه مورد غفلت واقع شده است.

تاکنون نظریه پایه و جامع و مدون بازدارندگی با اتکا به نقاط قوت و استفاده به‌موقع از فرصت‌ها، برای کاهش آسیب‌پذیری‌ها و دفع تهدیدات به‌منظور شناخت ابعاد و مؤلفه‌های اساسی تهدیدات سایبری دشمن علیه ج.ا.ا با نگاه به آینده تهیه نشده است؛ بنابراین مسئله ما فقدان نظریه مدون برای ایجاد بازدارندگی در فضای سایبری کشور، در رویارویی با تهدیدات سایبری و به‌تبع آن شناخت الزامات بازدارندگی در فضای مجازی کشور بر اساس اسناد بالادستی و رویکردهای موجود است به شکلی که در برابر تهدیدات دشمن مقاوم، مستحکم و باقابلیت تداوم کارکردها و در عین‌حال بتواند به تهدیدات دشمن پاسخ پشیمان کننده بدهد.

۳- اهمیت و ضرورت تحقیق

نظام مقدس جمهوری اسلامی ایران پس از پیروزی، در پی پیاده‌سازی اسلام ناب محمدی (صلی‌الله علیه و اله و سلم)، به‌عناوین‌مختلف مورد هجمه‌های گوناگون قرارگرفته است. پیشرفت فناوری در سال‌های اخیر به‌خصوص فناوری اطلاعات، فضای جدیدی را به نام فضای سایبر پیش روی انسان قرار داده است. شالوده اصلی و ویژگی‌های انحصاری فضای مجازی را می‌توان سرعت، دقت و کیفیت دانست که سبب گردیده اکثر فناوری‌ها به آن وابستگی پیدا کنند. سرمایه‌ها و دارایی‌ها چه اقتصادی، چه فرهنگی، چه انسانی، صنعتی و نظامی همه شکل‌دهنده شاکله وجودی نظام هستند و پاسداری از آن‌ها یعنی پاسداری از یک ملت. فضای سایبر کشور بزرگ جمهوری اسلامی ایران نیز یکی از سرمایه‌ها و دارایی‌های مهم، راهبردی و حیاتی این ملت غیور است که غفلت از پاسداری از آن خسارات و صدمات سنگینی را برای نظام اسلامی به همراه خواهد داشت.

آنچه امروز تحت عنوان تهدید در فضای سایبری مطرح است در واقع نوعی اعمال مخرب است که ممکن است لزوماً مغرضانه نباشند اما ماهیتی مخل و مخرب دارند. بدیهی است هنگامی‌که نتوانیم این تهدیدات چه از نوع مغرضانه و چه از نوع آگاهانه آن را به‌درستی شناسایی، دسته‌بندی و ارزش‌گذاری نماییم قطعاً نخواهیم توانست راهکارهای مقابله با آن‌ها را نیز به‌درستی تدبیر، طراحی و اجرا نماییم. از سوی دیگر آنچه مسلم است این است که شناسایی تهدیدات در حوزه‌ای به گستردگی و عمق فضای سایبر و بازدارندگی سایبری بدون پشتوانه پژوهشی، علمی و مطالعاتی موردنیاز هیچ‌گاه عملی نخواهد بود و نمی‌توان تضمین لازم را برای جامع‌ومانع بودن آن ارائه نمود.

۴- پیشینه

در رساله الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها، آقای علی ملائی (۱۳۹۸، دانشگاه عالی دفاع ملی) در پاسخ به این سؤال که الگو راهبردی بازدارندگی در دفاع سایبری بر اساس نظریه بازی‌ها چیست؟ به این نتیجه رسیده است که امروزه رشد هرچه بیشتر وابستگی‌های زندگی بشری به فضای سایبر، باعث شده است تا تهدیدات سایبری به زیرساخت‌های راهبردی موردتوجه دشمنان هر جامعه‌ای قرار بگیرد. حملات سایبری که در کشورهایی چون استونی، گرجستان و همچنین در ایران در گذشته رخ‌داده است به ما هشدار خواهد داد، آینده فضای سایبر عاری از حملات و تهدیدات دفاعی و امنیتی نخواهد

بود؛ بنابراین بازدارندگی یکی از موضوعات اساسی در حوزه دفاعی- امنیتی هر کشور است. در این پژوهش ارائه الگویی از بازدارندگی در تأمین امنیت دارایی‌های سایبری مسئله اصلی است [۲].

۲) آقایان محمدحسن فرخ و علی محمدی در مقاله مفهوم شناسی بازدارندگی سایبری به این جمع‌بندی رسیده‌اند که مفاهیم سنتی بازدارندگی، در فضای سایبری نیز توسعه و گسترش‌یافته‌اند و نظام جمهوری اسلامی ایران نیز به‌عنوان بازیگر مهم بین‌المللی، علیرغم دارا بودن توان بازدارندگی بالای سایبری، نیازمند آن است تا هرچه سریع‌تر الزامات این مهم را شناسایی و درصدد توفیق هرچه بیشتر بازدارندگی سایبری گام بردارد. در این تحقیق در این خصوص برخی الزامات پیشنهاد شده‌اند [۳].

۳) در مقاله بازدارندگی و محرومیت در فضای مجازی آقای جوزف نای با طرح این سؤال که آیا کشورها می‌توانند دیگران را از آسیب رساندن به فضای مجازی جلوگیری کنند یا مانع از آن شوند؟ این‌چنین پاسخ می‌دهد که، درک بازدارندگی در فضای مجازی اغلب دشوار است، زیرا ذهن ما توسط تصاویر جنگنده از بازدارندگی به‌عنوان تهدید انتقام عظیم به حمله هسته‌ای توسط وسایل هسته‌ای دستگیر شده است. بااین‌حال، مشابهت به بازدارندگی هسته‌ای گمراه‌کننده است جلوگیری از آسیب در فضای مجازی شامل فرآیندهای پیچیده‌ای مانند تهدید مجازات، انکار، پیچیدگی و هنجارها می‌شود. علاوه بر این، حتی زمانی که مجازات استفاده می‌شود، تهدیدهای بازدارنده نیازی به محدودیت پاسخ‌های سایبری نیست و ممکن است رفتار عمومی و همچنین اقدامات خاصی را موردتوجه قرار دهند [۴].

۴) در مقاله تئوری بازدارندگی در قرن سایبر، آنه گریت بندیک، توبیاس متزگر این سؤالات را مطرح می‌کنند که، چطور بازدارندگی سایبری از همتای حرکتی‌اش متمایز می‌شود؟ آیا توانایی‌های سایبری تهاجمی می‌توانند در بازدارندگی دشمنان مؤثر باشد؟ آیا گزینه تلافی باید «روی میز» باشد تا بازدارندگی موفق شود؟ چه تغییراتی برای پیاده‌سازی‌اش لازم است و جایی که چالش‌های کلیدی قرار می‌گیرند کجاست؟

آن‌ها معتقدند که ریشه اصطلاح بازدارندگی[1] به معنای «ترساندن از» و به شکل «تضعیف کردن و کنار گذاشتن یا محدود کردن با ترس» تعریف می‌شود. «بازدارندگی با مفهوم ترساندن دیگران از انجام کار به شیوه‌ای که برای خودشان مفید است و به شما آسیب می‌زند، مرتبط است». این تعریف دو مفهوم بازدارندگی را پررنگ می‌کند، نخست تضعیف مهاجم با دیگر مدافعان و دوم محدود کردن به سبب ترس انتقام‌گیری [۵].

۵) در تحقیقی با عنوان طرح راهبردی دفاع سایبری جمهوری اسلامی ایران در حوزه بازدارندگی (۱۳۹۶، دانشگاه عالی دفاع ملی) آقایان محمد احدی و محمدشاه محمدی این‌چنین نتیجه گرفته‌اند که، 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 ضرورت می‌یابد و در چنین طرحی بازدارندگی از اولویت بیشتری برخوردار خواهد بود هرچند بازدارندگی در حوزه سایبر پیچیده‌تر از بازدارندگی نظامی است اما با رعایت الزامات آن و بهره‌گیری از شیوه‌های مناسب می‌توان به آن دست‌یافت و بدین ترتیب هزینه دفاع در این حوزه تا حد قابل‌توجهی کاهش می‌یابد[۶] .

۶) آقای علی‌اصغر دهقانی، در تحقیقی با عنوان بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا که در مجله رهیافت‌های سیاسی و بین‌المللی (۱۳۹۶، شماره ۵۰) به چاپ رسیده عنوان می‌کنند که مقایسه وضعیت کنونی با بازدارندگی جنگ سرد اشتباه است. جلوگیری از آسیب در فضای سایبر، سازوکارهای پیچیده‌ای مانند تهدید به‌تلافی، انکار، گرفتار کردن و هنجارها را می‌طلبد. نظریه‌پردازی در خصوص بازدارندگی در فضای سایبر، در اولین موج خود قرار دارد. فرمول‌بندی یک راهبرد مؤثر در عصر سایبر، نیازمند فهمی گسترده‌تر و چندبعدی از مفهوم بازدارندگی است و نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری داد [۷] .

۷) در کتاب قدرت سایبری و امنیت ملی که توسط کرامر، فرانکلین و استار استوارت و لاری ونتز در سال ۲۰۱۰ به چاپ رسیده است در ۱۶ فصل به طرح مسائلی ازجمله مفاهیم و اجزای فضای سایبر، کاربردهای نظامی و بازدارندگی، امنیت اطلاعات، نفوذ سایبری و امنیت بین‌الملل، مشکلات راهبردی قدرت سایبری مانند جرائم سایبری و تروریسم سایبری و عوامل سازمانی ازجمله حاکمیت اینترنت و حقوق بین‌الملل و عملیات اطلاعاتی می‌پردازند. در این کتاب نقش قدرت سایبر در سطوح تاکتیکی، عملیاتی و راهبردی در سطوح ملی و امنیت بین‌الملل موردبررسی قرارگرفته است و چنین نتیجه‌گیری شده که، با توجه به پویایی و تحول فضای سایبر، استفاده از آن برای تقویت قدرت ملی، بدون طراحی راهبرد امکان‌پذیر نیست [۸].

۵- مبانی نظری

سرمایه‌ها و داراییهای هر ملتی چه اقتصادی، چه فرهنگی، چه انسانی، صنعتی و نظامی همه شکل دهنده شاکله وجودی آن

[1] deterrence

نظام هستند و پاسداری از آنها یعنی پاسداری از یک ملت.فضای سایبر کشور بزرگ جمهوری اسلامی ایران نیز یکی از سرمایه‌ها و داراییهای مهم، راهبردی و حیاتی این ملت غیور است که غفلت از پاسداری از آن خسارات و صدمات سنگینی را برای نظام اسلامی به همراه خواهد داشت. آنچه که امروز تحت عنوان تهدید در فضای سایبری مطرح است در واقع نوعی اعمال مخرب است که لزوما مغرضانه نیستند اما ماهیتی مخل و مخرب دارند.بدیهی است هنگامی که نتوانیم این تهدیدات چه از نوع مغرضانه و چه از نوع آگاهانه آن به درستی شناسایی، دسته بندی و ارزش گذاری نماییم قطعا نخواهیم توانست راهکارهای مقابله با آن‌ها را نیز به درستی تدبیر، طراحی و اجرا نماییم.

۵-۱- فضای سایبر

شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات می‌باشد. این فضا ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد [۹].

۵-۲- تهدیدات سایبری

هر رویداد یا واقعه باقابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر (پنداره) یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام (تخریب) افشاء، تغییر اطلاعات و یا ممانعت (ایجاد اختلال) از ارائه خدمت[۹].

۵-۳- بازدارندگی سایبری

یک فرآیند اعلام شده است که به معنای ممانعت از درگیری‌های اینترنتی یا فعالیت‌های تهدیدکننده در فضای مجازی است. فرآیندهای موجود برای بازدارندگی سایبری شامل سیاست، خط‌مشی، سلاح، توانایی یا اتحاد می‌شود [۱۰].

۵-۴- نظریه بازدارندگی سایبری کلی (عمومی)

برای پاسخ به این سؤال که آیا بازدارندگی سایبری امکان‌پذیر است، باید نظریه‌ها و مفاهیم پشت راهبرد بازدارنده موفق و نحوه اعمال آن در مورد سایبر موردبررسی قرار گیرد. هیچ تعریف واحدی از بازدارندگی یا فقدان نظریه‌ها برای کاربرد عملی آن وجود ندارد. دکترین (اصول) مشترک بازدارندگی به‌عنوان جلوگیری از عمل توسط «وجود یک تهدید معتبر از اقدامات متقابل غیرقابل‌قبول و یا اعتقاد به اینکه هزینه‌های عمل، مهم‌تر از مزایای درک شده است» تعریف می‌کنند. گزینه‌های بازدارنده می‌توانند به‌صورت فعال یا غیرفعال باشند. در کتابی تحت عنوان بازدارندگی سایبری و جنگ سایبری، مارتین لیبیکی این گزینه‌ها را این‌گونه توصیف می‌کند:

۱) بازدارندگی با انکار (توانایی خنثی کردن یک حمله) یا بازدارندگی غیرفعال

۲) بازدارندگی با مجازات (تهدید اقدامات تلافی‌جویانه) بازدارندگی فعال

از منظر سایبری، بازدارندگی غیرفعال شامل اقداماتی است که جهت حفاظت از شبکه‌ها از حملات یا ایجاد شبکه‌های انعطاف‌پذیر (مقاوم) که برای به حداقل رساندن و یا کاهش اثرات حمله، انجام می‌شود. این اقدامات مهمی از دکترین و مهندسی امنیت سیستم است اما نقش مهمی در بازدارندگی فعالانه حملات سایبری بازی نمی‌کنند. بااین‌وجود، آن‌ها می‌توانند تأثیر بازدارنده‌ای توسط انکار اعمال‌نفوذ دشمن از هرگونه اثرگذاری معناداری در سامانه‌ها شبکه‌ها، یا عملیات داشته باشند. به‌عنوان یک جایگزین، بازدارندگی فعال تلافی‌جویانه و یا نوعی از پاسخ‌های نامطلوب به یک حمله سایبری یا حادثه را تهدید می‌کند. ویژگی‌هایی که منجر به راهبرد بازدارندگی موفق می‌شوند چیست؟ برای اهداف این مطالعه هفت ویژگی متداول بازدارندگی ذکر شده که جهت ارزیابی برجسته شده است: منافع (علاقه‌ها)، اظهارات بازدارنده (بیانیه بازدارنده)، اعتبار، ترس، اقدامات انکار، اقدامات مجازات و محاسبه هزینه- سود (منفعت) .[۱۱]

بازدارندگی سایبری مانند همه بازدارندگی‌های دیگر، هنگامی موفق می‌شود که یک دشمن تصمیم بگیرد که با پرخاشگری و اقدامات تجاوزکارانه عمل نکند. این تصمیم دو ارزیابی جداگانه را دنبال می‌کند: آیا هزینه‌های تجاوز سایبری از مزایای آن فراتر رفته و آیا مزایای محدودیت در فضای سایبری از هزینه‌های آن فراتر رفته است. با غیرفعال کردن اهداف حمله سایبری، ایمن کردن آن‌ها به‌صورت غیرقابل نفوذ، یا انجام حملات غیرممکن و بیهوده، اقدامات انکار مزایای حمله سایبری احتمالی را کاهش می‌دهند. اما انکار به‌خودی‌خود برای جلوگیری از تجاوز در فضای سایبری کافی نیست. دشمنان را همچنان باید با تهدید به مجازات که هزینه‌های حمله سایبری را افزایش می‌دهد برای اجرا و تاثیرگذاشتن پیام‌های بازدارنده مواجه کنند. اگر دشمنان با مجازات روبرو نشوند، تا زمانی که یک رویکرد مؤثر پیدا کنند، به حملات سایبری ناموفق ادامه می‌دهند. درحالی‌که انکار

به‌طورقطع نمی‌تواند به‌تنهایی مقاومت کند، اقدامات انکار قدرتمند همراه با انتظار معقول مجازات، راهی طولانی به سمت پیشگیری از تجاوز سایبری خواهد داشت. علاوه بر اقدامات انکار قوی، نظریه بازدارندگی کلاسیک مستلزم آن است که اقدامات مجازات قطعی، شدید و فوری باشند. بااین‌حال، بازدارندگی سایبری بیش از شدت یا فوریت بر قطعیت تأکید دارد. به‌دلیل عواقب وخیم ناشی از آن، بازدارندگی هسته‌ای ایجاب می‌کند که کشورهای بازدارنده متقابل بتوانند به‌سرعت و به‌طور گسترده ضد حمله را انجام دهند. اما حملات سایبری به‌طورمعمول شامل عواقب کمتر جدی، مهاجمان باقابلیت شناسایی کمتر و ابزارهای وسیع‌تری برای ضد حمله هستند. با پیامدها و عواقب کمتر جدی، ضد حمله نیازی به مجازات بسیار شدید و نامتناسب ندارد. ضد حمله نباید فورا وارد عمل شود، برخلاف یک حمله هسته‌ای غافلگیرانه، در صورت وجود تعداد کم، حملات سایبری می‌توانند یک کشور قربانی (طعمه) را به‌طور کامل از پاسخ دادن ناتوان کنند. به همین دلیل درنهایت نه شدت عمل و خشونت و نه فوریت برای اقدامات مجازات بازدارندگی سایبری لازم است، فقط قطعیت و یقین [۱۲].

۵-۵- بازدارندگی سایبری جامع (گسترده)

یک راهبرد وسیع بازدارندگی سایبری شبیه چه چیزی خواهد بود؟ برخی از اسناد سیاست موجود این شواهد و الزامات را فراهم می‌کند. در راهبرد سایبری ایالات‌متحده از وزارت دفاع درخواست کمک جهت توسعه و پیاده‌سازی یک راهبرد بازدارندگی جامع برای جلوگیری از بازیگران اصلی دولتی و غیردولتی از انجام حملات سایبری علیه منافعشان شده است. این سیاست به طیف وسیعی از سیاست‌ها و قابلیت‌ها برای تأثیرگذاری بر رفتار بازیگران دولتی و غیردولتی اشاره می‌کند و نشان می‌دهد که بازدارندگی سایبری از طریق برجسته کردن کلیه اقدامات ازجمله سیاست رسمی و مثبت، نشانه‌ها و دلالت‌های قابل‌توجه قابلیت‌های هشدار، موقعیت دفاعی، رویه‌های پاسخگویی مؤثر انعطاف‌پذیری کلی شبکه‌ها و سامانه‌های حاصل خواهد شد [۱۳].

۵-۶- عناصر نظریه‌ی بازدارندگی

نظریه‌های بازدارندگی نظامی طی دوره رقابت‌های هسته‌ای بین بلوک شرق و غرب پس از جنگ جهانی دوم در خلال دوران جنگ سرد، رشد و توسعه یافته‌اند. با فراگیری شبکه جهانی اینترنت و شکل‌گیری فضای جدید سایبری که تمام ابعاد زندگی بشر را دگرگون ساخت، توجه دولت‌ها به بسط و گسترش قدرت در این فضای جدید معطوف شد. ازآن‌پس منازعات دنیای واقعی راه به‌سوی فضای سایبری یافتند. بازدارندگی نیز به‌عنوان عاملی مهم در راهبردهای اجتناب از نبرد کشورها، جایگاه خود را در این فضا به‌سرعت به‌دست آورد .ابعاد، مؤلفه‌ها و شاخص‌های فضای سایبری نیازمند آن است تا به‌منظور نیل به هدف نهایی «بازدارندگی سایبری «که همان »جلوگیری از وقوع جنگ سایبری» است، مفاهیم سنتی بازدارندگی در فضای سایبری بازتعریف گردند [۱۴] .

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

۱- شرایط عینی: فنّاوری 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 فنّاورانه 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 ازنظر راهبردی، بسیار بااهمیت است، به‌عبارت‌دیگر، ازنظر ذهنی کشور الف باید آمادگی عملی ساختن تهدید را داشته باشد و کشور ب نیز ازنظر ذهنی اقناع شود که در صورت در پیش نگرفتن سیاست‌های همگرا با کشور الف، موردحمله قرار خواهد گرفت [۱۵].

۳- مبادله‌ی اطلاعات: برای حصول بازدارندگی، اطلاعات مربوط به شرایط عینی و ذهنی طرفین باید مبادله شود تا سطح آگاهی آن‌ها افزایش یابد [۱۶].

۴- عقلانیت طرفین: مفهوم بازدارندگی بر این عقیده متمرکز می‌باشد که طرفین محاسبات خود را به‌صورت عقلانی انجام می‌دهند، بدیهی است که عقل در مقایسه با منافع به‌دست‌آمده، هزینه‌های گزاف را نمی‌پذیرد [۱۷] .

۵-۷- حملات سایبری و تئوری بازدارندگی

به گفته استراتژیست نظامی آمریکا، برنارد بردی (۱۹۴۶)، هدف ارتش‌ها از پیروزی در جنگ‌ها به جلوگیری از آن‌ها تغییریافته است. هیچ‌چیز باقدرت مخرب یک انفجار هسته‌ای مقایسه نمی‌شود. اما حملات سایبری در افق فکری به‌عنوان تهدیدی شناخته می‌شوند که به‌عنوان ابزارهای خارق‌العاده برای طیف گسترده‌ای از اهداف سیاسی و نظامی به بهترین صورت درک می‌شوند، بسیاری از این موارد می‌توانند دارای پیامدهای جدی

امنیت ملی باشند. تلاش‌های کنش گرایانه برای جلوگیری از حملات سایبری ممکن است به یک بخش اساسی در راهبردهای نظامی ملی تبدیل شود.

امروزه حملات سایبری می‌تواند رهبری سیاسی، سامانه‌های نظامی و شهروندان متوسط را در هر نقطه از جهان در طول زمان صلح یا جنگ، با سود اضافی ناشناس بودن مهاجم، هدف‌گیری کنند. طراحان راهبردهای سیاسی و نظامی اکنون برای دست‌یابی به اهداف خود از کامپیوترها، بانک‌های اطلاعاتی و شبکه‌هایی که آن‌ها را به هم وصل می‌کند استفاده و یا سوءاستفاده می‌کنند [۱۸].

۵-۸- مشکل بازدارندگی سایبری

چالش عصر دیجیتال برای تعریف کردن بازدارندگی نیست. بازدارندگی یک مفهوم به‌خوبی تعریف شده است که در طول تاریخ موردمطالعه و تمرین قرارگرفته است و بعد از ظهور سلاح‌های هسته‌ای، عمق بیشتری پیداکرده است. چالش فعلی درک کردن نقشی است که فناوری‌های دیجیتال در حوزه گسترده‌تر بازدارندگی بین دولتی بازی می‌کنند. بازدارندگی در یک حوزه به‌ندرت مستقل از سایر حوزه‌ها عمل می‌کند. بخش عمده‌ای از ادبیات بازدارندگی سایبری بر بازدارندگی دامنه تمرکز می‌کند. بااین‌حال، این‌یک محدودیت خطرناک است که ریسک‌ها را افزایش می‌دهد و احتمال موفقیت را به حداقل می‌رساند. کشف ادبیات مربوط به بازدارندگی و شناسایی کاربرد آن در حوزه تازه تعریف‌شده‌ای از اقدامات متقابل فضای سایبری یک ضرورت است. بازدارندگی کلاسیک بر روی محاسبه هزینه- سود (منفعت) دشمن بالقوه جهت متوقف کردن اقدامات خاص و متمایز کردن از (وادارندگی، عملیات وادارسازی[1]) با تمرکز بر دست‌کاری رفتار پیش‌بینی‌شده از طریق کاربردهای پیشین از نیرو و یا سایر ابزارهای قدرت دولتی متمرکز می‌شود. وادارندگی، توانایی یک دولت برای مجبور کردن دولت دیگر به عمل و یا به‌عنوان یک اقدام مستقیم است که دشمن را متقاعد می‌کند تا چیزی که موردنظر است رها کند که به‌منظور جلوگیری از دشمن از اقدام که توسط تهدید مجازات طراحی شده است. هم وادارسازی و هم بازدارندگی فرم‌های اجبار هستند.

اگر مجازات و انکار نتوانند مشکل بازدارندگی سایبری را به‌طور کامل برطرف کنند آیا هیچ راه‌حل معقولی وجود دارد؟. بازدارندگی هرگز ابزار واحدی در جعبه‌ابزار دولتی جهت انکار یا توقیف و یا شکل دادن رفتار دشمن نبوده است. بلکه همیشه با تلاش‌هایی که فراتر از مفاهیم بازدارندگی سنتی است و شامل شیوه‌های ژئوپلیتیک و فنی ترکیب شده است ازجمله توسعه نرمال، پیچیدگی، بازدارندگی تجمعی، تحقیق و توسعه، سیاست‌ها و قوانین، ساختار مسئولیت برای نرم‌افزار و سخت‌افزار، آموزش برای کاربران و توسعه سرمایه انسانی با فناوری اطلاعات و امنیت سایبری. بازدارندگی سایبری مؤثر و کارآمد باید سیاست‌های بین‌المللی را گسترش دهد و شامل زمینه‌های مانند جرم‌شناسی، ایمونولوژی (ایمن شناسی) و سلامت عمومی باشد. راه‌حل مشکل بازدارندگی رها کردن آن نیست بلکه گسترش طیف وسیعی از راهبردهای جایگزین است که در حال حاضر در نظر گرفته نشده است[۱۹].

۵-۹- فضای سایبر کشور، به‌مثابه زیرساخت حیاتی یا سرمایه ملی

سرمایه سایبری مؤلفه‌ای از فضای سایبر است که برای مالک آن فضا، دارای ارزش و نیازمند محافظت است. سرمایه سایبری در کنار انواع دیگر سرمایه، اعم از سرمایه فیزیکی، سرمایه انسانی، و سرمایه ذهنی یا شناختی دسته‌بندی می‌شود و ممکن است متعلق به اشخاص حقیقی، اشخاص حقوقی یا دولت‌ها باشد، لیکن برخی از این سرمایه‌های سایبری، از اهمیت و ویژگی‌های خاصی در سطح ملی برخوردار هستند که آن‌ها را از سایر سرمایه‌های سایبری متمایز می‌نماید. سرمایه ملی به‌دسته‌ای از سرمایه‌ها اطلاق می‌شود که نقش حیاتی در امنیت ملی، اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و نظایر آن‌ها در سطح ملی داشته باشد.

از سوی دیگر زیرساخت یا ستون فقرات به عوامل ساختاری به‌هم‌پیوسته‌ای اطلاق می‌گردد که به‌مثابه تکیه‌گاه برای یک سازه بوده و وارد شدن ضربه به این عوامل، موجب پاشیده شدن شیرازه‌ی سازه خواهد شد. بر این اساس زیرساخت حیاتی به زیرساخت‌هایی اطلاق می‌گردد که نقش حیاتی در توسعه‌ی اقتصادی و اجتماعی، افزایش سطح رفاه عمومی، ارتقاء توان دفاعی و امنیتی و تأمین نیازمندی‌های ضروری یک کشور داشته باشند، به‌نحوی‌که بُروز اختلال هرچند کوتاه‌مدت در عملکرد آن‌ها تأثیری فاجعه‌بار بر امنیت ملی، اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و اداره‌ی امور کشور داشته باشد.

سایر زیرساخت‌های حیاتی کشور نیز زیرساخت حیاتی وابسته به فضای سایبر یا سرمایه ملی وابسته به فضای سایبر می‌باشند که جمع‌آوری، پردازش، مبادله و ذخیره‌سازی هرگونه اطلاعات در خصوص آن‌ها و نهایتاً مدیریت و کنترل آن‌ها با بهره‌گیری از فضای سایبر انجام می‌شود. به‌این‌ترتیب بخش حیاتی فضای سایبر کشور، متشکل از زیرساخت ارتباطات و

[1] Compellence

فناوری اطلاعات کشور و زیرساخت سایبری سایر زیرساخت‌های حیاتی کشور است و هرگونه تهدید سایبری که منجر به تأثیر فاجعه‌بار بر این بخش از فضای سایبر کشور شود، باید موردتوجه جدی دفاع سایبری قرار گیرد.

بنابراین فضای سایبر کشور، زیرساخت حیاتی سایبری است که علاوه بر زیرساخت ارتباطات و فناوری اطلاعات کشور، زیرساخت سایبری سایر زیرساخت‌های حیاتی نیز می‌باشد. فضای سایبر کشور در این نوع کارکرد، زیرساخت حیاتی سایبری کشور است و از اهمیت حیاتی برخوردار است، لذا از منظر متولیان زیرساخت‌های حیاتی کشور، این فضا باید از بالاترین سطح امنیت (یعنی مصونیت) در برابر انواع تهدیدها و بالاترین سطح تاب‌آوری در مقابل انواع حملات سایبری برخوردار باشد.

هدف کارکردی امنیت فضای سایبر کشور به‌مثابه زیرساخت حیاتی و سرمایه ملی سایبری، تأمین مصونیت برای زیرساخت‌های حیاتی سایبری و وابسته به فضای سایبر در مقابل انواع تهدید سایبری و تاب‌آوری زیرساخت‌های حیاتی سایبری و وابسته به فضای سایبر در مقابل انواع حملات سایبری است[۲۰].

۵-۱۰- فضای سایبر کشور، به‌مثابه مؤلفه‌ی امنیت ملی

فضای سایبر کشور، علاوه بر این‌که یکی از مؤلفه‌های امنیت ملی محسوب می‌شود، نقش حیاتی در تأمین سایر مؤلفه‌های امنیت ملی، از قبیل اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و نظایر آن‌ها نیز دارد. در سال ۱۳۹۷ تأثیر بارز فضای سایبر ج.ا.ایران در ایجاد و تشدید بحران اقتصادی در سطح ملی را شاهد بودیم که ناشی از همین امر بود.

بر اساس این دیدگاه، فضای سایبر کشور، یکی از مؤلفه‌های کلیدی امنیت ملی و تأثیرگذار بر سایر مؤلفه‌ها از قبیل اقتصاد ملی، منافع ملی، روابط بین-المللی، اقتدار ملی، انسجام ملی، اعتماد عمومی و سلامت عمومی است. فضای سایبر کشور در این نوع کارکرد، باید به‌صورت مداوم مورد شناسایی و مراقبت قرار داشته باشد و سرویس‌های امنیتی کشور، اشراف اطلاعاتی کامل بر آن داشته باشند تا با هرگونه اقدام علیه امنیت ملی، اقتصاد ملی، منافع ملی، روابط بین‌المللی، اقتدار ملی، انسجام ملی، اعتماد عمومی و سلامت عمومی، برخورد و مقابله‌ی به‌موقع و مؤثر صورت گیرد.

هدف کارکردی امنیت فضای سایبر کشور به‌مثابه مؤلفه‌ی امنیت ملی تأمین اطمینان و آرامش برای کاربران و جامعه، از طریق اشراف اطلاعاتی بر مؤلفه‌ی امنیت ملی در مقابل هرگونه حضور و نفوذ دشمن است [۲۰].

۵-۱۱- تولید قدرت سایبری

اقدام‌های مقابله‌ای در فضای سایبر کشور در مقابل هرگونه تهدید، آسیب‌پذیری، مخاطره، تهاجم و حادثه سایبری و پیامد اعم از سایبری، فیزیکی و روانی، برای کاهش و رفع آن‌ها ضروری است. این اقدام‌های دفاعی باید در سطحی انجام گیرد که منجر به تأمین بازدارندگی دفاعی در فضای سایبر کشور شود و برای این منظور، لازم است قدرت سایبری به‌عنوان بخشی از قدرت نظامی کشور تحقّق یابد. در حقیقت هدف کارکردی امنیت فضای سایبر کشور به‌مثابه محیط عملیات نظامی تأمین بازدارندگی برای دفاع ملی در فضای سایبر کشور، از طریق تولید قدرت سایبری به‌عنوان یک مؤلفه از قدرت نظامی کشور می‌باشد.

همه اقدامات پدافندی چه در فضای بی‌طرف و چه در فضای دشمن از حالت پدافند غیرعامل خارج و به شکل پدافند عامل درمی‌آید. آفند اعم از پدافند فعال است. ما فقط آن جنبه از آفند را که صرفاً عوامل عینی و ذهنی حمله را می‌زند مدنظر داریم چراکه هر چیزی که عامل حمله و یا عامل جنگ سایبری را از کار بیندازد یک اقدام پیش‌کنش گرایانه است، این اقدامات باید تهدیدات را یا متوقف کند و بعد هم در زمان محدود، مجدد فعال شود. باید راهبرد اصلی توسعه قدرت سایبری باشد. ایجاد قدرت سایبری بازدارنده، راهبرد دیگر ارتقا قدرت است. اتکا به قدرت سیاست نکته کلیدی است. چون قوانین بین‌المللی قدرت پشتیبانی ندارند. [۱]

۵-۱۲- دفاع و بازدارندگی

دفاع در ۴ زمان قبل از جنگ، آستانه جنگ، حین جنگ و پس از جنگ انجام می‌شود ولی بازدارندگی بین آستانه و حین جنگ است. بحث مخاطره، بحث قدرت است اما در حد بازدارندگی. وقتی یک کشور به خطر می‌رسد اگر بازدارندگی نداشته باشد حمله می‌شود. راهبرد اصلی صیانت است که قبل از جنگ باید اتفاق بیافتد. در این مرحله بحث تاب‌آوری و انطباق‌پذیری مطرح می‌شود که یکپارچه‌سازی قدرت در همه ابعاد عملیات از اصول و اندیشه گرفته تا هنر رزم صورت پذیرد. بازدارندگی قبل از تاب‌آوری است. اشراف، آمادگی و مصونیت باید به وجود بیاید

یکی از راهبردهای کلیدی در بازدارندگی باید تمرکز بر روی یکسری از اولویت‌ها شامل پیش‌بینانه، پیشگیرانه، پیش‌کنش گرایانه، واکنش گرایانه و منفعلانه، باشد [۱].

۵-۱۳- نظریه بازدارندگی در فضای سایبری کشور چیست؟

در عرصه فضای سایبری قدرت می‌تواند به اشکال مختلفی بروز و ظهور پیدا کند ازجمله توسعه توانمندی‌ها در حوزه‌های سخت‌افزاری، نرم‌افزاری، ساختار افزاری و مغز افزاری اما آنچه واضح و مبرهن است حوزه مغز افزار پایه اصلی ایجاد توانمندی‌هاست. توانمندسازی سرمایه انسانی خلاق و کارآمد با ایجاد ذهنیت مسئولانه بازدارنده از طریق توسعه ابزارهای آموزشی و افزایش مستمر سطح آگاهی‌ها مهم‌ترین راهبرد بازدارندگی سایبری در مقابل تهدیدات می‌باشد هراندازه اشرافیت اطلاعاتی هوشمندانه در برابر تهدیدات فضای سایبری افزایش یابد به همان اندازه قدرت بازدارندگی را توسعه خواهد بخشید.

بازدارندگی سایبری می‌تواند پیشگیری از فعالیت دشمن با نمایش قدرت و به رخ کشیدن توانمندی‌ها از طریق ارتباطات باشد و او را به این باور ذهنی برساند که اقدام متقابل دارای هزینه‌ای بیش از فایده برای او خواهد بود.

همکاری‌های نهادی بخش دولتی و خصوصی، بهره‌مندی از قابلیت‌های بسیج و سازمان‌های مردم‌نهاد و ایجاد انسجام و وحدت رویه در حوزه دفاع سایبری از طریق اشتراک‌گذاری اطلاعات (پیام / اظهار بازدارنده) موجب ایجاد و افزایش ظرفیت ملی سایبری برای ارتقا توان بازدارندگی سایبری در مقابل تهدیدات خواهد شد .

برای اینکه بازدارندگی سایبری دارای اثر مثبت قطعی شود و شرایط عینی را تحقق بخشد نیاز به تاب‌آوری سایبری می‌باشد. ممانعت یکی از نتایج مهم تاب‌آوری است. در بازدارندگی مبتنی بر تاب‌آوری سایبری ضروری است ابتدا قدرت تحمل ضربه را افزایش داد و سپس اقدام متقابل (مجازات) نمود.

بدیهی است پیاده‌سازی و راهبری نظام بازدارندگی سایبری و همچنین پایش اثربخشی راهبردهای بازدارندگی در مقابل تهدیدات دشمن بر اساس تولید، توسعه و انتشار قدرت مبتنی بر چارچوب بازدارندگی فوق موجب مصون‌سازی سرمایه‌های سایبری ازجمله زیرساخت‌های حیاتی و حساس خواهد شد.

بازدارندگی جمهوری اسلامی ایران در سطح کل و خرد مطرح است. در سطح کل همان بازدارندگی نظامی و سطح خرد بازدارندگی غیرنظامی یا سایبری موردنظر است. رابطه بازدارندگی سطح کل با سطح خرد باید مشخص شود و نحوه کمک نیز بایستی مشخص شود. کشور در تولید قدرت و بازدارندگی باید یکپارچه باشد. مجموع قدرت فرهنگی، قدرت سیاسی، قدرت نظامی و قدرت اجتماعی، مؤلفه‌های قدرت نظام جمهوری اسلامی ایران را تشکیل می‌دهد. قدرت سایبری هم باید با این‌ها هماهنگ باشد چون در بحث سایبری موضوعات فرهنگی، سیاسی، اجتماعی و ... نیز جزئی از بازدارندگی کل است. برای پیاده‌سازی بازدارندگی سایبری باید مدل وجود داشته باشد و تصویری واضح و شفاف از یک قدرت برتر سایبری، یک قدرت دفاعی و یک قدرت زیرساختی و حتی یک قدرت آفندی ارائه شود [۲۱].

۶- مطلوبیت‌های راهبردی بازدارندگی سایبری

بر اساس نظر خبرگان ارتباطات و فناوری اطلاعات و پدافند غیرعامل در دانشگاه و دستگاه‌های اجرایی، مطلوبیت‌های راهبردی بازدارندگی سایبری (چشم‌انداز، اهداف کلان، ارزش‌های اساسی حاکم، اصول، الزامات در اسناد بالادستی) احصا و در جلسات خبرگی به تأیید آنان رسید که به شرح ذیل می‌باشد:

۶-۱- چشم‌انداز بازدارندگی سایبری

دفاع همه‌جانبه سایبری در قلمرو جمهوری اسلامی در افق ۱۴۰۴ در حوزه بازدارندگی، با بسیج منابع و سرمایه‌های ملی سایبری امن، بومی، پایدار، پاسخگو و پشیمان کننده در مقابل تهدیدات سایبری دشمن، برای دست‌یابی به قدرت سایبری پیشرو و برتر و برخوردار از:

۱. نظام جامعه بازدارندگی سایبری در جهت دفاع عمیق، لایه به لایه و مستحکم با توسعه عمق دفاعی
۲. نظام فرماندهی و کنترل هوشمند باقابلیت تشخیص و شناسایی تهاجم (فارنزیک قوی و همه‌جانبه)
۳. مصونیت در زیرساخت‌های حیاتی و حساس کشور در برابر تهدیدات و حملات سایبری
۴. سرمایه انسانی خلاق، کارآمد و جهادی با ذهنیت مسئولانه بازدارنده در حوزه دفاع سایبری
۵. نظام دیپلماسی سایبری فعال و ائتلافی در مسیر منافع ملی
۶. استقلال و خوداتکایی با صنعت بومی دفاع سایبری پیش‌کنش گرایانه
۷. طراحی، پیاده‌سازی و اجرای نظریه‌ها و الگوهای بازدارندگی سایبری بومی و دانش‌محور در جهت ممانعت از بروز تهدید
۸. آسیب‌ناپذیری زیرساخت‌های حیاتی و حساس
۹. تاب‌آوری با افزایش قابلیت‌ها و تطابق با شرایط در حال تغییر
۱۰. نظام نهادینه‌شده اشرافیت اطلاعات سایبری (فنی، شناختی، زیرساختی)
۱۱. مشارکت ظرفیت بخش‌های دولتی، غیردولتی، مردم‌نهاد و بسیج

۱۲. نظام تولید و توسعه قدرت درون‌زای سایبری
۱۳. اهداف کلان بازدارندگی سایبری:
۱۴. دست‌یابی به راهبردهای بازدارندگی سایبری برای توسعه دفاع ملی
۱۵. دست‌یابی به زیرساخت‌های مصون سایبری
۱۶. دست‌یابی به توان تاب‌آوری سایبری
۱۷. دست‌یابی به سرمایه‌های انسانی خلاق با ذهنیت مسئولانه بازدارنده
۱۸. دست‌یابی به قدرت درون‌زای بازدارندگی
۱۹. دست‌یابی به صنعت بومی خوداتکا و پیشرفته بازدارنده
۲۰. دست‌یابی به قدرت دیپلماسی سایبری بازدارنده
۲۱. دست‌یابی به مشارکت و ارتقا همکاری‌های نهادی
۲۲. دست‌یابی به قدرت آفندی تلافی‌جویانه، قاطع و پشیمان کننده

۶-۲- اهداف کلان بازدارندگی سایبری

۱. دست‌یابی به راهبردهای بازدارندگی سایبری برای توسعه دفاع ملی

۲. دست‌یابی به زیرساخت‌های مصون سایبری

۳. دست‌یابی به توان تاب‌آوری سایبری

۴. دست‌یابی به سرمایه‌های انسانی خلاق با ذهنیت مسئولانه بازدارنده

۵. دست‌یابی به قدرت درون‌زای بازدارندگی

۶. دست‌یابی به صنعت بومی خوداتکا و پیشرفته بازدارنده

۷. دست‌یابی به استانداردها و الگوهای بازدارندگی سایبری بومی و پویا

۸. دست‌یابی به قدرت دیپلماسی سایبری بازدارنده

۹. دست‌یابی به نظامات بازدارندگی سایبری

۱۰. دست‌یابی به مشارکت و ارتقا همکاری‌های نهادی

۱۱. دست‌یابی به قدرت آفندی تلافی‌جویانه، قاطع و پشیمان کننده

۱۲. دست‌یابی به سامانه‌های بومی و درون ساخت

۶-۳- ارزش‌های اساسی حاکم بر حوزه بازدارندگی سایبری

۱. خودباوری و خوداتکایی
۲. اعتمادسازی، اطمینان بخشی
۳. نوآوری و خلاقیت
۴. ارزش‌های والای انسانی – اسلامی
۵. نفی سلطه دشمن بر فضای سایبری
۶. مدیریت جهادی
۷. تفکر و عمل بسیجی
۸. استقلال درونی باقابلیت تعامل‌پذیری
۹. اصول حاکم بر بازدارندگی سایبری:
۱۰. وحدت فرماندهی دفاع سایبری کشور
۱۱. دفاع بومی، همه‌جانبه و بازدارنده (پاسخ به تهدیدات)
۱۲. هوشمندی در دفاع
۱۳. روزآمدی و آینده‌نگری
۱۴. آسیب‌ناپذیری
۱۵. تحمیل هزینه‌بر دشمن
۱۶. اشرافیت اطلاعاتی در فضای سایبری کشور
۱۷. نفوذناپذیری و اقتدار
۱۸. بی‌اعتمادی به محصولات خارجی
۱۹. استقلال و خودکفایی
۲۰. مبادله اطلاعات و ارسال پیام اقتدار

۶-۴- الزامات بازدارندگی سایبری در اسناد بالادستی

اسناد بالادستی نظام جمهوری اسلامی ایران دارای اشارات مستقیم یا غیرمستقیم به اصل بازدارندگی و الزامات آن در برابر تهدیدات دشمن هستند. به عبارتی، در این اسناد تحقق بازدارندگی مورد تأکید قرارگرفته و به مواردی اشاره شده است که با ارتقای قدرت و آسیب‌ناپذیری جمهوری اسلامی ایران به ترتیب از طریق ایجاد رعب و ناامید کردن دشمن، بازدارندگی ایجاد می‌کند. لازم به ذکر است که اشارات مربوطه در مواردی ناظر به بازدارندگی مطلق و در مواردی ناظر به بازدارندگی سایبری و الزامات آن‌ها هستند.

اسناد بالادستی که در این راستا موردبررسی و مبنای بیان الزامات قرارگرفته است، در لایه سیاست‌ها کلی نظام جمهوری اسلامی ایران در حوزه‌های مرتبط، سند چشم‌انداز بیست‌ساله، اسناد راهبردی پدافند سایبری و افتا و اسناد نظامات جامع شامل تبیین الزامات شبکه ملی اطلاعات، نظام جامع عملیات پدافند سایبری کشور و سند نظام ملی پیشگیری و مقابله با حوادث فضای مجازی هستند.

در ادامه، این الزامات که با استفاده از روش خبرگی انتخاب و اولویت‌بندی شده، ارائه می‌شود.

۶-۵- الزامات تحقق اصل بازدارندگی

۱. ایجاد سامان دفاعی باهدف بازدارندگی همه‌جانبه.
۲. ایران کشوری است امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه و پیوستگی مردم و حکومت.
۳. پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات.
۴. ارتقاء توان بازدارندگی کشور با: توسعه توان موشکی و فناوری‌ها و ظرفیت تولید سلاح‌ها و تجهیزات عمده دفاعی برتر ساز با توان بازدارندگی و متناسب با انواع تهدیدات.
۵. بهره‌گیری از کلیه امکانات غیرمسلحانه سایبری و غیر سایبری کشور، به‌منظور ایجاد بازدارندگی

۶-۶- الزامات تحقق بازدارندگی سایبری

این الزامات در چهار حوزه‌ی توسعه علم و فناوری، نیروی انسانی، ساختارهای نهادی و همکاری نظامات مختلف، بیان‌شده و درمجموع ناظر به ظرفیت‌سازی قدرت سایبری و آسیب‌ناپذیری برای ایجاد ممانعت از تهاجم دشمن یا ایجاد باور در دشمن نسبت به توان تقابل متوازن برای تنبیه تجاوز وی هستند.

۱. ایجاد، ساماندهی و تقویت نظام ملی اطلاع‌رسانی رایانه‌ای.
۲. اعمال تدابیر و نظارت‌های لازم به‌منظور صیانت از امنیت سیاسی، فرهنگی، اقتصادی، اجتماعی و جلوگیری از جنبه‌ها و پیامدهای منفی شبکه‌های اطلاع‌رسانی.
۳. ایجاد دسترسی به شبکه‌های اطلاع‌رسانی جهانی صرفاً از طریق نهادها و مؤسسات مجاز.
۴. ایجاد و تقویت نظام حقوقی و قضایی متناسب با توسعه شبکه‌های اطلاع‌رسانی به‌ویژه در جهت مقابله کارآمد با جرائم سازمان‌یافته الکترونیکی.
۵. توسعه فن‌آوری اطلاعات (به‌ویژه حفاظت از اطلاعات) و آینده‌نگری در خصوص آثار تحولات فن‌آوری اطلاعات در سطح ملی و جهانی.
۶. گسترش مطالعات و تحقیقات.
۷. تربیت نیروی انسانی متخصص در این زمینه.
۸. ساماندهی نظام ملی، قوانین و توسعه‌ی فناوری و نیروی انسانی متناسب تحولات جهانی و نیازهای کشور
۹. تحقق پدافند غیرعامل که عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد.
۱۰. تهیه و اجرای طرح‌های پدافند غیرعامل (با رعایت اصل هزینه – فایده) در مورد مراکز، اماکن و تأسیسات حائز اهمیت.
۱۱. فرهنگ‌سازی و آموزش عمومی درزمینهٔ به‌کارگیری اصول و ضوابط پدافند غیرعامل در بخش دولتی و غیردولتی، پیش‌بینی مواد درسی در سطوح مختلف آموزشی و توسعه تحقیقات درزمینه پدافند غیرعامل.
۱۲. 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.
۱۳. فرهنگ‌سازی، آموزش و افزایش آگاهی و مهارت‌های عمومی در حوزه افتا.
۱۴. برقراری ارتباط و همکاری با دیگر کشورها در زمینه‌های علمی، تولیدی و تجاری کالاها و خدمات دفاعی و امنیتی برای دست‌یابی به اهداف سیاست‌های کلی خودکفایی دفاعی و امنیتی.
۱۵. برون‌سپاری و جلب مشارکت سایر بخش‌ها اعم از دولتی و غیردولتی در تأمین نیازها
۱۶. گسترش هوشمندانه و مصون‌سازی با اجرای کامل پدافند غیرعامل در مراکز حیاتی و حساس کشور
۱۷. افزایش ظرفیت های قدرت نرم و دفاع سایبری و تأمین پدافند و امنیت سایبری برای زیرساخت های کشور در چارچوب سیاست‌های کلی مصوب.
۱۸. توسعه محتوی در فضای مجازی بر اساس نقشه مهندسی فرهنگی کشور تا حداقل پنج برابر وضعیت کنونی و بومی‌سازی شبکه‌های اجتماعی.
۱۹. ایجاد، تکمیل و توسعه شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمند آن و ساماندهی، احراز هویت و تحول در شاخص ترافیکی شبکه به‌طوری‌که ۵۰ درصد آن داخلی باشد.
۲۰. بهره‌گیری از موقعیت ممتاز کشور باهدف تبدیل ایران به مرکز تبادلات پستی و ترافیکی ارتباطات و اطلاعات منطقه و گسترش حضور در بازارهای بین‌المللی.
۲۱. حضور مؤثر و هدفمند در تعاملات بین‌المللی فضای مجازی.
۲۲. افزایش سهم سرمایه‌گذاری زیرساختی در حوزه فناوری اطلاعات و ارتباطات تا رسیدن به سطح کشورهای برتر منطقه.
۲۳. مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری

تحقق پدافند سایبری بازدارنده با رعایت اصول عملیاتی پدافند سایبری کشور شامل اصول عملیات پدافند سایبری عبارت

است از: صیانت، ممانعت، مانایی، یکپارچگی، مشارکت، دفاع جمعی، آمادگی، انطباق‌پذیری و تاب‌آوری برای دست‌یابی به برتری عملیاتی نیروهای پدافند سایبری خودی بر دشمن.

۷- روش تحقیق

این تحقیق با توجه به هدف آن کاربردی- توسعه‌ای است. هدف تحقیقات کاربردی توسعه دانش کاربردی در یک زمینه خاص است تا مسئله‌ای حل شود و نتایج تحقیق سریعاً به کار گرفته شود.

با توجه به اینکه این تحقیق منجر به بهبود و توسعه فرایندها شده و درصدد بهبود وضعیت به‌وسیله‌ی تحقیقات کاربردی است و به‌نوعی به دنبال عملیاتی سازی نتایج تحقیقات کاربردی در زیرساخت‌های کشور است، در زمره تحقیقات توسعه‌ای قرار می‌گیرد. تحقیقات توسعه‌ای به دنبال بسط و گسترش مفاهیم و رسیدن به راهبردهای جدید می‌باشند.

این پژوهش به روش توصیفی تحلیلی انجام پذیرفته و سپس با استفاده از رویکرد کمی و کیفی و روش‌های آمیخته و آینده‌پژوهی جمع‌آوری و تجزیه‌وتحلیل اطلاعات انجام شد سپس از روش‌های مصاحبه، نشست خبرگی و دلفی در جهت دست‌یابی به هدف پژوهش بهره‌گیری شده است. در این پژوهش، جامعه آماری از دو بخش تشکیل می‌شود:

کلیه اسناد و مدارک بالادستی و مرتبط با موضوع تحقیق و آثار مکتوب

جامعهٔ آماری شامل خبرگان آگاه و نخبگان صاحب‌نظر با ویژگی‌های زیر:

الف- شناخت کافی نسبت به مسائل راهبردی دفاعی و غیرنظامی.

ب- دارای مسئولیت در مشاغل راهبردی لشگری و کشوری.

ج- اساتید و دانش‌آموختگان علوم دفاعی و پدافند غیرعامل، سایبری و راهبردی کشور.

د- سابقه مسئولیت و مدیریت در حوزه‌های مرتبط با پدافند غیرعامل.

ه- دارا بودن تخصص میان‌رشته‌ای به‌خصوص در حوزه‌های پدافند غیرعامل و رشته‌های سایبری و دارای آگاهی به اصول و الزامات پدافند غیرعامل

به علت محدود بودن تعداد خبرگان و صاحب‌نظران در حوزه موردمطالعه، حجم نمونه بر حجم جامعه آماری منطبق و جامعه آماری به‌صورت تمام شمار موردپژوهش قرار گرفت.

در این تحقیق از هر دو روش گردآوری اطلاعات، یعنی روش‌های میدانی مصاحبه و مشاهده و روش کتابخانه‌ای (فیش‌برداری) استفاده شد.. هم‌چنین برای به‌دست آوردن بخشی از داده‌های کیفی، از روش انجام مصاحبه‌ی اکتشافی ساخت‌مند یا میزگرد خبرگی با متخصصان و خبرگان در این حوزه استفاده گردید. شیوه تجزیه‌وتحلیل داده در این تحقیق استفاده از رویکردهای کمی و کیفی است. در رویکرد کیفی پس از مطالعه اسناد و انجام مصاحبه با خبرگان با استفاده از روش تحلیل محتوا و تحلیل گفتمان، مطلوبیت‌های راهبردی بازدارندگی در حوزه سایبری احصا و مجدداً با تشکیل میزگرد خبرگی با استفاده از روش دلفی، نظر خبرگان در رابطه با موضوع ارائه‌شده توسط محقق بررسی گردید، آنگاه در رویکرد کمی با استفاده از پارامترهای آماری توصیفی و استنباطی جهت آزمودن الزامات بازدارندگی سایبری در اسناد بالادستی از قبیل آزمون‌های میانگین طراحی و اجرا شد.

۸- بحث و نتایج

بازدارندگی سایبری محدود به بازداشتن دشمن از به‌کارگیری تهدید سایبری علیه دارایی‌های سایبری نیست بلکه اعم از آن بوده و به معنای بازداشتن دشمن از هرگونه تهدید سایبری- غیرسایبری علیه هرگونه دارایی سایبری-غیرسایبری با استفاده از کلیه امکانات و اقتضائات فضای سایبری-غیرسایبری است. لازم به ذکر است که مقصود از غیر سایبری کلیه ابعاد فضای حقیقی تحت حاکمیت کشورها در حوزه‌های اقتصاد و تجارت، امنیت و حاکمیت، اعتماد عمومی، سلامت و ایمنی عمومی، قدرت علمی صنعتی و فناوری، قدرت فرهنگی- اجتماعی، دفاعی، روابط بین‌المللی، حقوق عمومی و حریم خصوصی است.

با مقدمه ذکرشده، امکان تطبیق و درواقع بسط نظریه بازدارندگی برای ارائه نظریه بازدارندگی سایبری در قلمرو جمهوری اسلامی ایران وجود دارد.

قدرت تسلط سایبری همچنان یکی از عناصر اصلی بازدارنده مؤثر، ازجمله بازدارندگی سایبری است. بازدارندگی سایبری چالش‌برانگیز است، اما با یک راهبرد سنجیده و واقع‌بینانه، بازدارندگی سایبری می‌تواند بیشتر کاره‌ای مؤثر مطلوب خود را انجام دهد. علیرغم پیش‌بینی نظریه‌پردازان بازدارندگی سایبری همچنان به جهان فیزیکی و سیاسی وابسته است و به نظر می‌رسد ازنظر تئوری سخت‌تر از آن است که در عمل اجرایی شود. عدم قطعیت درباره پیچیدگی سامانه‌ها و اثرات آن‌ها، ابعاد

مختلف بازدارندگی سایبری را تقویت می‌کند.

حوزه سایبری به یک راهبردی جامع و کامل نیاز دارد که شامل پاسخ‌های سایبری سریع و مستقیم که ناگهانی، پویا و متحرک، مخفیانه و تصادفی باشند تا دشمنان هم ازلحاظ روانی و هم ازلحاظ مجازی متحمل شکست شوند. بازدارندگی با تعامل و تعجب چنین راهبرد بازدارندگی است. این راهبرد از ویژگی‌های منحصربه‌فرد درگیری‌های سایبری بهره‌برداری می‌کند و یک منطقه بافر راهبردی را به وجود می‌آورد که به آن امکان می‌دهد به‌صورت پویا اقدامات متقابلی را بر اساس ساختارها و زمینه‌های خاص علاوه بر حمایت خود از مجموعه اطلاعات، عملیات اطلاعاتی و عملیات تعجب و غافلگیری انتخاب کند.

برای محدود کردن تهدیدات، نظریه‌ی بازدارندگی به‌صورت مفهومی ارزشمند در نظر گرفته شده است. اگر در نظر بگیریم که بازدارندگی ابزاری در سیاست امنیتی باقی بماند، باید هر برداشتی از نظریه بازدارندگی تصدیق کند که محدود به دفاع محض نخواهد بود. دریافت‌ها از مسئله‌ی تهدید، هم در ایجاد راهبرد مؤثر ملی و هم در هدف استفاده از نظریه‌ی بازدارندگی، نقشی محوری ایفا می‌کنند. ماهیت تهدید، عوامل تهدید، ابزار مورداستفاده و هدف بالقوه نیز مهم هستند.

۹- نتیجه‌گیری

۹-۱- بسط و توسعه نظریه پایه بازدارندگی

سرعت نوآوری در قلمروی سایبری بیشتر از سرعت آن در قلمروی هسته‌ای و... است. مزیت تهاجم نسبت به دفاع ممکن است در طول زمان تغییر کند. یادگیری سایبری نیز مهم است. همان‌طور که دولت‌ها و سازمان‌ها شناخت بهتری از محدودیت‌های حملات سایبری و اهمیت فزاینده اینترنت برای رفاه اقتصادی خود پیدا می‌کنند، محاسبات هزینه-سود سایبری ممکن است تغییر کند همه حملات سایبری دارای اهمیت مساوی نیستند؛ همه آن‌ها نمی‌توانند بازداشته شوند؛ و همه آن‌ها به سطح تهدیدهای مهم امنیت ملی نمی‌رسند. نکته کلیدی تمرکز روی مهم‌ترین حملات و شناخت دامنه کامل فرآیندها و زمینه‌ها برای جلوگیری از این حملات است.

با ایجاد توانمندی‌های آشکار و پنهان سایبری ضمن تداوم کارکردهای زیرساختی و پایداری دستگاه‌ها و سامانه‌ها، شرایط بنیادین قابلیت و ثبات بازدارندگی محقق خواهد شد و بدین ترتیب تضمین سامانه‌ای به وجود خواهد آمد.

حملات سایبری اجتناب‌ناپذیر هستند و به‌جای صرف زمان هنگفت برای اقدامات صرفاً پیشگیرانه امنیت سایبری که در خصوص حملات سایبری اجتناب‌ناپذیر کمکی نمی‌کنند، می‌توان بر انعطاف‌پذیری سایبری سرمایه‌گذاری کرد.

ایجاد و استفاده از همه ظرفیت‌های سایبری (انسانی و فنی) به‌منظور آمادگی برای تطابق و تاب‌آوری (انعطاف‌پذیری) در شرایط متغیر و پویای سایبری یک ضرورت غیرقابل‌انکار است که ضمن پایداری و تسلط حاکمیتی موجب حفظ و افزایش منافع و اهداف ملی خواهد شد. این موضوع بایستی به‌عنوان یک ارزش اساسی و ملی در نظریه بازدارندگی موردتوجه باشد. در این شرایط وجه دفاعی و پدافندی در مقوله بازدارندگی سایبری مطرح است ولیکن موضوع مکمل در نظریه بازدارندگی سایبری آفند و قدرت پاسخگویی است تا ضمن نجات سریع از اختلالات و آسیب‌پذیری‌ها، پاسخ قاطع و بلادرنگ (سایبری و غیر سایبری) به دشمن داده شود. مجازات یک عنصر مهم است که ضمن تحقق شرایط عینی بازدارندگی در مقابل تهدیدات دشمن، شرایط ذهنی برای ممانعت از اقدامات بعدی را نیز فراهم می‌کند به این صورت که هر اقدام ممکن است با پاسخ پشیمان کننده‌ای مواجه شود (تلافی مکرر)؛ بنابراین برای بازدارندگی به‌وسیله تلافی نمایش قدرت هم ضروری است.

برای اینکه بازدارندگی مؤثر و معتبر باشد، باید دشمن بالقوه (شاید پنهان) را قانع نمود که ما هم‌توان و هم قصد پاسخ تلافی‌جویانه و یا حتی آغاز نخستین حمله (پیش‌دستی) را برای خنثی کردن حملات دشمن‌داریم. قابلیت تلافی‌جویانه و واکنشی شامل توانایی شناسایی به‌موقع یک تهدید (پیش از ضد حمله) و تصمیم‌گیری سریع و به‌کارگیری یک حمله پیش‌دستانه (آغازگر) و تلافی‌جویانه برای واردکردن ضربه‌های پرهزینه و بازدارنده به مهاجم می‌باشد.

توسعه و ارتقاء در نظریه بازدارندگی سایبری با ایجاد و حفظ توانایی‌های پیشی جستن با اقدامات پیش‌دستانه و پیش‌کنش گرایانه از اقدامات خصمانه دشمن با جمع‌آوری و اشراف اطلاعات و طراحی و پیاده‌سازی عملیات‌های اطلاعاتی برای غافلگیری دشمن در سطوح مختلف خواهد بود. بازدارندگی جامع و کامل علاوه بر ایجاد و حفظ توانایی تحمل ضربه و تاب‌آوری، باقدرت و برتری سایبری و دفاع تهاجمی و پیش‌دستانه به وجود خواهد آمد.

اقدامات بازدارندگی شامل طیف وسیعی از سیاست‌های موجود است که دارای ارزش‌های بازدارنده ازجمله مجازات برای تهدیدات راهبردی سطح بالاتر و انکار برای فعالیت‌های سطح پایین‌تر است. بنابراین اهداف متنوع خواهند بود و درنتیجه استفاده از اقدامات بازدارنده نیز متفاوت خواهند بود.

بازدارندگی در دامنه سایبری با دیگر وجوه بازدارندگی کاملاً متفاوت است و پیچیده‌تر از حوزه‌های نظامی است (هوا، زمین، دریا و فضا). سلاح‌های سایبری و روش‌های سایبری تهاجمی گران هستند و به‌سادگی در دسترس نیستند. دشمنانی که قادرند

به شبکه‌های بزرگ حمله کنند، بسیار زیادند و به نظر می‌رسد جهت مقابله با هر گروهی یک راهبرد بازدارندگی چندلایه لازم باشد بنابراین باید از تمام ابزار و ظرفیت‌ها استفاده گردد. در شرایط عدم قطعیت و همچنین پویایی فضای سایبری و تهدیدات آن، به‌منظور جلوگیری از شکست بازدارندگی با توجه به چالش شناخت منبع تهدید، به نظر می‌رسد که نظریه تکاملی برای به‌دست آوردن راهبردهای مطلوب، ارجح و پایدار، بروز رسانی و ترمیم مداوم آن است.

بازدارندگی موفق به اراده بر انجام آن استوار است که می‌تواند همانند یک تهدید تأثیرگذار باشد. امروزه نیاز به فراتر رفتن از پاسخ‌های متعارف و معمول وجود دارد و انگیزه تازه‌ای برای ساختن یک وضعیت بازدارندگی واقعی باید ایجاد شود. راهبردهای بازدارندگی جدید و جامعی که مستلزم پاسخ‌های سریع و مستقیم سایبری هستند که ناگهانی، پویا، مخفی و تصادفی و سریع باشند تا دشمنان هم ازلحاظ ذهنی و هم عملی شکست بخورند.

راهبردهای بازدارندگی باید بتوانند به‌راحتی در امتداد نردبان نظریه بازدارندگی به سمت بالا یا پایین حرکت کنند، تا عمق راهبردی بازدارندگی ایجاد شود.

ارتباط بین متغیرها در بازدارندگی سایبری، ارتباطی پویا است که از هر دو موضوع فنّاوری و یادگیری تأثیر خواهد پذیرفت. دلایل مختلفی وجود دارند که چرا دولت‌ها خود- محدودسازی در قلمروی سایبری را اجرایی کرده‌اند، که بسیاری از آن‌ها ناشی از پیچیدگی محض و عدم قطعیت سامانه‌های سایبری هستند.نظریه بازدارندگی باید با اثرگذاری روی ادراکات مدیران راهبردی، منافع و مزایای اقدامات خاص راهبردهای بازدارنده و مکمل یکدیگر را به نمایش بگذارد.

بنابراین غنی‌سازی نظریه و ایجاد یک رویکرد جامع برای فرآیندهای بازدارندگی سایبری جدید با ایجاد، حفظ، تقویت و ترمیم مداوم بازدارندگی می‌تواند توسعه یابد.

۱۰- مراجع

[1] M. khaleghi, "Cyber Def Doctrine Study Report V0.66," Telecommunication Research Center (ITRC), 2019. (In Persian)

[2] A. Molaee and M. kargari, and M. R. khorashadizadeh, "Pattern of deterrence in cyberspace based on game theory," 2018. (In Persian)

[3] M. H. Farokh and A. Mohammadi, "Conceptology Cyber deterrenc," Supreme National Defense University, 2015. (In Persian)

[4] S. Joseph, "Deterrence and Dissuasion in Cyberspace," Nye Jr -2016.

[5] B. Annegret and M. Tobias, "Deterrence theory in the cyber-century," Working Paper RD EU/Europe, 2015.

[6] M. Ahadi and M. Shahmohammadi, "Strategic plan of cyber defense of the Islamic Republic of Iran in the field of deterrence," 2017. (In Persian)

[7] A. A. Dehghani, "Cyber deterrence in the new global security: Russia and China cyber threat against US critical infrastructure," Quarterly Journal of Political and International Approaches , Year 8, Issue 4, 2017. (In Persian)

[8] F. D. Kramer, S. H. Starr, and L. K. Wentz, "Cyber power and national security Translation of the Vice Chancellor for Research and Production of Science," Institute of Printing and Publishing, Faculty of Information, 2019. (In Persian)

[9] Strategic document of the country's cyber passive defense, 2015. (In Persian)

[10] Russia-U.S., "Bilateral on Cybersecurity Critical Terminology Foundations," 2014.

[11] T. M. McKenzie, "Is Cyber Deterrence Possible?," USAF, Colonel Air Force Research Institute Perspectives on Cyber Power Published by Air University in January, 2017.

[12] Cyber Deterrence Tougher in Theory than in Practice, Will Goodman Strategic Studies Quarterly, 2010.

[13] Cyber Deterrence: A Comprehensive Approach? Dr Joe Burton1 Visiting Researcher, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Senior Lecturer, New Zealand Institute for Security and Crime Science, University of Waikato, January 2018.

[14] M. H. Farokh and A. Mohammadi, "Conceptology Cyber deterrenc," Supreme National Defense University, 2015. (In Persian)

[15] S. Lotfiyan, "Deterrence of nuclear ransom and war," various theories of nuclear proliferation and use, Information newspaper, 1997. (In Persian)

[16] H. Ashrafirizi and Z. Kazempoor, "The concept of political geography of information, Tehran, 2009. (In Persian)

[17] A. M. Asgarkhani, "A look at theories of deterrence and control of nuclear weapons,Tehran," Journal of Defense Policy, no. 25, 1998. (In Persian)

[18] The Challenge of Cyber Attack Deterrence Kenneth Geers Naval Criminal Investigative Service (NCIS) Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010.

[19] F. Brantly, "The Cyber Deterrence Problem Aaron Assistant Professor," Department of Political Science Virginia Polytechnic and State University United States, 2018.

[20] Gh. R. jalali, "Studies of the comprehensive system of cyber defense operations," Telecommunication Research Center (ITRC), 2019. (In Persian)

[21] A. R. Ghaznavi, "Attached National Cyber Defense Information Network," Ministry of Information and Communications Technology of Iran(ICT),Tehran, 2019. (In Persian)

.

Journal of Electronical & Cyber Defence
Vol. 8, No. 4, 2021, Serial No. 32

Development of the Concept of Deterrence Theory in the Country's Cyberspace Based on Upstream Documents and Available Approaches

Gh. Jalali Farahani*, M. S. Beykpouri

*Supreme National Defense University

(Received: 03/10/2020, Accepted: 05/12/2020)

ABSTRACT

Preventing damage in cyberspace involves complex mechanisms such as threat, punishment, non-admission, plight and norms. The purpose of this article is to clarify some of these conceptual terms and the policy of using deterrence theory in the cyber territory of the Islamic Republic of Iran. Formulation of an effective strategy in the cyber arena, requires a deeper recognition of the various dimensions of deterrence and prevention in cyber domains. Developing the base theory of deterrence against enemy cyber threats in the country's cyberspace requires accurate knowledge of the domain of defense and formulation of strategies based on the base theory of deterrence in cyberspace which has unfortunately been neglected. Our problem in this research is the lack of a codified theory to create deterrence in the country's cyberspace in face of cyber threats and, consequently, the recognition of deterrence requirements based on upstream documents and existing approaches such that in the face of enemy threats, the country's cyberspace stands firm and resistant with the ability to continue the required functions and at the same time retaliate enemy threats. Creating and using all possible human and technical cyber capabilities in order to be ready for adaptation (resilience) in variable and dynamic cyber conditions is an undeniable necessity that while sustaining resistance and sovereignty, it will maintain and increase national interests and goals. This issue should be considered as a fundamental and national value in the theory of deterrence. Considering the uncertainty of the cyberspace in addition to its dynamics and threats, and given the challenge of identifying the source of the threat, in order to prevent the failure of deterrence, the evolutionary theory is proposed which seems capable of obtaining desirable, preferable and sustainable strategies, and their constant updating and restoration. In this research, the strategic benefits of cyber deterrence (vision, macro goals, dominant basic values, principles, requirements in upstream documents) have been enumerated, based on the opinion of communication, information technology and passive defense experts in the academic and executive bodies, and finally gained the necessary approvals in expert assemblies.

Keywords: Cyberspace, Cyber Deterrence, Cyber Threats

* Corresponding Author Email: jalal826_s@yahoo.com