فصلنامه علمی (مقاله علمی ـ پژوهشی)جامعه شناسی سیاسی ایران، سال دوم، شماره اول(پیاپی۵)،بهار ۱۳۹۸،صص۲۵۲-۲۳۲

بازدارندگی سایبری واینترنتی، راهبردی نوین در کسب اقتدار دفاعی وسیاسی کشور

سجاد فرهنگ[۱]

تاریخ دریافت: ۹۸/۱/۱۱

تاریخ پذیرش:۳۱ /۹۸/۲

چکیده:

بازدارندگی سایبری یکی از راهبردهای مقابله با تهدیدات سایبری و نیز تقویت اقتدار دفاعی کشورها در عرصه جنگ های نوپدید محسوب می گردد. بازدارندگی سایبری در برابرتهدیدات سایبری مستلزم شناخت دقیق مبانی و مفاهیم آن و نیز نحوه نحوه و جایگاه آن در شکل گیری اقتدار دفاعی می باشد. مقاله پیش رو به دنبال تبیین نقش بازدارندگی سایبری در اقتدار دفاعی ارتش جمهوری اسلامی ایران می باشد. مقاله از نظر هدف کاربردی بوده و شیوه انجام آن توصیفی- کتابخانه ای بوده است. جامعه آماری پژوهش شامل دیدگاه ها و نظرات فرماندهی معظم کل قوا در زمینه دفاع سایبری و نیز بازدارندگی سایبری در اسناد و مدارک بالادستی بوده است. به منظور تجزیه و تحلیل داده ها از روش های اماری کمی استفاده شده است. نتایج تحقیق بیانگر آن است که بازدارندگی سایبری در چهار بعد ارتباط، ثبات نظر، قابلیت و اعتبار بر اقتدار دفاعی کشور تاثیر گذار است. در پایان به منظور تقویت قدرت بازدارندگی راهبردهای پیشنهادی ارائه شده است.

واژگان کلیدی: الگو، اقتدار دفاعی، بازدارندگی سایبری، دفاع سایبری.

[۱] دکترای مدیریت رسانه دانشگاه آزاد اسلامی واحدعلوم تحقیقات تهران، ایران

مقدمه:

سازمان‌های نظامی برای دستیابی به اهداف راهبردی خود در تأمین امنیت و دفاع از کشور نیازمند ارتقای روزافزون دانش و فناوری در تمامی ابعاد ساختار و سازمان خود می‌باشند. به‌کارگیری فناوری‌های مدرن در تسلیحات نظامی امروز و آینده سبب شکل‌گیری راهبردهای جدید دفاعی و نظامی گردیده است. با توسعه علمی جوامع و گسترش آن‌ها مبتنی بر اقتصاد دانش‌بنیان به همان اندازه فناوری‌ها و ابزارهای جنگی بیشتری در اختیار نیروهای نظامی کشورها قرار می‌گیرد. بنابراین خصوصیت جنگ ، انعکاسی از وضعیت اجتماعی، اقتصادی و فنّاورانه جامعه‌ای است که جنگ در آن به وقوع می‌پیوندد. در سال‌های اخیر فناوری و راهبردهای به‌کارگیری آن در نیروهای نظامی به نحو چشمگیری تغییر کرده است. فناوری همچنین توانایی جنگ افروزی را تا حدی متحول ساخته است که باعث شده مفهوم تعیین مرکز جنگ بی‌معنی گردد. میدان‌های جنگی چند بعدی شده‌اند و سراسر کشورها، فضایی برای جنگ هستند. سازمان‌های نظامی همچون سایر سازمان‌های غیرنظامی در حال کاهش نیرو و منابع مالی و حذف فعالیت‌های غیرضروری خود هستند. ساختارهای سازمانی با ظهور فناوری‌های فرماندهی و کنترل پیشرفته به‌سوی عدم تمرکز پیش رفته‌اند. جنگ‌های شبکه محور سبب افزایش آگاهی از فضای جنگ گردیده و عملیات سریع‌تر و مؤثرتر را سبب شده است به‌نحوی‌که واحدهای فرماندهی در میدان درگیری قادر به اتخاذ تصمیم‌های درست در منطقه می‌باشند. از مؤلفه‌های اصلی جنگ-های امروزی وابستگی تسلیحات نظامی و سایر ملزومات جنگ به سامانه‌های فناوری اطلاعات و ارتباطات و فضای سایبر است که به‌عنوان شبکه عصبی و مغز سلسله‌مراتب فرماندهی عمل می‌نمایند. وابستگی سازمان‌های نظامی به ابزار فناوری اطلاعات و ارتباطات و فضای سایبر تا حدی است که هرگونه اخلال در عملکرد این سامانه‌ها سبب اخلال در عملیات خواهد شد.

همچنین وابستگی زیرساخت‌های حیاتی کشورها به فضای سایبر و آسیب‌پذیری‌های موجود در آن‌ها سبب شده است که دشمن یکی از اهداف نظامی خود در اعمال فشار و سلطه به کشور مقابل را تخریب و اخلال و نفوذ به سامانه‌های سایبری تعریف نماید. وقتی زیرساخت‌های انرژی، ارتباطات، سلامت و حمل‌ونقل در کشوری دچار اخلال در عملکرد و خدمات‌رسانی به مردم شوند زمینه نارضایتی عمومی و حتی اعتراضات و تظاهرات سازمان‌دهی شده فراهم گشته و کشور دچار وضعیت امنیتی می‌گردد که این

موضوع یعنی ایجاد خطر برای آن کشور در سطح امنیت ملی. درواقع می‌توان نتیجه‌گیری نمود که جنگ سایبر هم از منظر داخلی نیروهای مسلح و هم از منظر تهدید امنیت ملی بسیار حائز اهمیت هست. پیدایش جنگ سایبری، عملیات شبکه رایانه، دفاع سایبری و نظایر آن مبیین رویکرد جدید و گرایش روزافزون کشورهای مختلف به‌ویژه نیروهای دفاعی امنیتی به استفاده از این حوزه در کاهش آسیب‌پذیری سایبری است. امروزه بخش عظیمی از سرمایه‌های علمی اقتصادی و نظامی کشورها در فضای سایبر تولید ذخیره و مصرف می‌شوند. بنابراین تسلط بر این فضا برای حفاظت و صیانت از این سرمایه‌ها و دارایی‌های سایبری و نیز حمله به مواضع سایبری دشمنان در مواقع لزوم به یکی از بزرگ‌ترین دغدغه‌های نظامی کشورها تبدیل‌شده است. طی دهه آینده، حدود ۷۰ درصد تنازعات بین‌المللی در این فضا خواهد بود. در این شرایط، جهت‌گیری و رویکرد کلان نیروهای مسلح به ویژه ارتش جمهوری اسلامی ایران در خصوص نحوه بهره برداری از ظرفیت های موجود در فضای سایبری در راستای کسب اقتدار دفاعی از اهمیت بالایی برخوردار است.

مبانی نظری و پیشینه تحقیق:

تعریف فضای سایبری:

در جامعه‌ای که برای زندگی روزانه خود به فضای سایبری وابسته است و همه چیز از ماشین آلات، شبکه های برق و سدها گرفته تا سامانه‌های تسلیحاتی به یک شبکه متصل هستند، دغدغه‌های مربوط به اثرات احتمالی فعالیت‌های تهاجمی یا خرابکارانه در فضای سایبری تا حدودی موجه است.

فضای سایبری به عنوان محیط رقابت کنشگران دولتی و غیردولتی، هنوز نوپاست. هر چند هنوز کاملا معلوم نیست که چطورآسیب‌پذیری ذاتی فضای سایبری ممکن است امنیت و حتی حق حاکمیت را به مخاطره بیندازد، اما باز هم مبحث تهدیدهای سایبری و کج فهمی در سیاست های واکنش مناسب، با لغزش های تاسف باری همراه است. نگرانی ها از «پرل هاربر سایبری» آتی یا «آرماگدون سایبری» بارها اوج گرفته و اصطلاح «جنگ سایبری» هم بدون توجه به این امر به کار گرفته می شود که منظور از جنگ چیست و این جنگ در فضای سایبری چگونه خواهد بود.

آسیب پذیری های ذاتی فضای سایبری به حوزه های حیاتی کشیده شده و امنیت کشورهای پیشرفته و کلا روابط بین المللی را با چالش راهبردی مواجه کرده است. حفاظت اطلاعات، رفع نقاط ضعف زیرساخت ها و نوسازی روزافزون قابلیت های نظامی شبکه ای، از اولویت های اصلی سیاستمداران در دهه آینده محسوب می شود. بنابراین، توجه به ماهیت آشوب سایبری و چگونگی واکنش بهینه به آن، امری ضروری است.

بازدارندگی اغلب به عنوان سیاست و پاسخی بهینه به تهدید سایبری و راه‌حلی برای مقابله با تداوم جاسوسی سایبری مطرح می شود. با این حال، تهدید به مجازات، جلوی حملات سایبری یا سایر رفتارهای مخرب را نخواهد گرفت و بلکه به جای آن احتمالا باعث بی‌ثباتی بین المللی خواهد شد. در این زمینه، ضروری است که راهبردهای جایگزین فضای سایبری علاوه بر اعتمادسازی و کاهش خطر درگیری، از منافع ملی نیز حفاظت کند.

بازدارندگی سایبری:

در عصر کنونی، موضوعی جدید به ادبیات امنیت استراتژیک اضافه شده که بسیار پیچیده می نماید. سلاح مجازی [۱] افزوده ای جدید به زرادخانه دولت هاست. طراحان امنیتی باید معنای آن را برای استراتژی رمزگشایی کرده و سازوکارهای پیشین را بر مبنای مشخصات این عرصه بازتعریف کنند. یکی از این سازوکارها که در دوران جنگ سرد و برای سال ها، منطق استراتژیک جنگ سرد را به طرزی موفقیت آمیز شکل داده بود، بازدارندگی است. با وجود موفقیت این سازوکار در عرصه های سنتی، فهم بازدارندگی در فضای سایبر مشکل است؛ چراکه ذهن ما با ادبیات جنگ سرد، مبنی بر بازدارندگی به مثابه تهدید به تلافی یک حمله هسته ای با استفاده از ابزارهای هسته ای، شکل گرفته است. مقایسه وضعیت کنونی با بازدارندگی جنگ سرد اشتباه است. جلوگیری از آسیب در فضای سایبر، سازوکارهای پیچیده ای مانند تهدید به تلافی، انکار، گرفتار کردن [۲] و هنجارها [۳] را می طلبد. جرویس از سه مرحله نظریه پردازی بازدارندگی در دوران هسته ای صحبت کرده بود [۴] . نظریه پردازی در خصوص بازدارندگی در فضای سایبر، در اولین موج خود قرار دارد. فرمول بندی یک استراتژی مؤثر در عصر سایبر، نیازمند فهمی گسترده

تر و چندبُعدی از مفهوم بازدارندگی است و نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری بدهیم

بازدارندگی سایبری در اسناد و مدارک بالادستی

جمهوری اسلامی ایران در پیروی از آموزه های دینی جهت حفظ امنیت کشور و مردم، علاوه بر تدابیری که برای حفاظت سامانه های مختلف در مقابل حملات احتمالی سایبری اتخاذ کرده، در راستای بازدارندگی نیز تدابیری را اتخاذ کرده است که موارد ذیل از آن جمله اند.

بازدارندگی در کلام رهبری:

مقام معظم رهبری و فرماندهی معظم کل قوا 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 مصونیت ساز 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 جنگ افروزی، فروش سلاح و رونق بخشیدن به صنایع نظامی وابسته به سرمایه‌داران است، افزودند: تنها عاملی که موجب تضعیف انگیزه جنگ افروزی قدرت طلبان و یا از بین رفتن این انگیزه می شود، آمادگی عمومی ملت و آمادگی دفاعی نیروهای مسلح است. رهبر انقلاب اسلامی خاطرنشان کردند: احساس آمادگی عمومی در ملت ایران بویژه جوانان، امروز بیش از هر زمان دیگر است و نیروهای مسلح نیز بسیار آماده‌تر و تواناتر از گذشته هستند. حضرت آیت‌الله خامنه‌ای یاد خدا و معنویت را عامل اصلی افزایش توانایی و قدرت بازدارندگی نیروهای مسلح دانستند و تأکید کردند: پیروزی رزمندگان اسلام در ۸ سال دفاع مقدس و شکست ارتش به ظاهر قدرتمند و مجهز و مدعی رژیم صهیونیستی در جنگ های ۳۳ روزه لبنان و ۲۲ روزه غزه بهترین نمونه‌ها از تأثیر معنویت در افزایش قدرت و توان دفاعی هستند. ایشان افزودند: ملت ایران امروز بیش از هر زمان دیگر در مقابل دشمنان، احساس قدرت می کند و این احساس متکی بر واقعیات است. رهبر انقلاب اسلامی با تأکید بر لزوم حفظ و تقویت قدرت آمادگی ملت و نیروهای مسلح، خاطرنشان کردند: آمادگی و روحیه پای کار بودن ملت

ایران و نیروهای مسلح، آنچنان هیبتی بوجود آورده است که اجازه گمان و توهم تجاوز را نیز به دشمن نخواهد داد.(پایگاه اطلاع رسانی دفتر مقام معظم رهبری)

بازدارندگی در سیاست های کلی کشور:

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

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

در این ابلاغیه، سیاست های ناظر بر ایمن سازی و حفاظت، توسعه دانش و فناوری ها در حوزه سایبر، پیشگیری و بازدارندگی و تعامل های بین المللی و منطقه ای مورد توجه قرار گرفته است. متن این سیاست ها به شرح ذیل می باشد:

۱) ایجاد نظام جامع و فراگیر در سطح ملی و ساز وکار مناسب برای امن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات، و ارتقاء مداوم امنیت شبکه های الکترونیکی و سامانه های اطلاعاتی و ارتباطی در کشور به منظور:

- استمرار خدمات عمومی.

-پایداری زیرساخت های ملی.

-صیانت از اسرار کشور.

-حفظ فرهنگ و هویت اسلامی- ایرانی و ارزش‌های اخلاقی.

-حراست از حریم خصوصی و آزادی‌های مشروع و سرمایه‌های مادی و معنوی.

۲) توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی.

۳) ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (افتا)

۴) تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی در توسعه زیرساخت‌های علمی و فنی امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی.

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

بند ۵ بالا نشان می دهد: بازدارندگی امری مقطعی نبوده و ضمن اینکه باید قابلیت‌های بازدارندگی همواره حفظ گردند، با توجه به روزافزونگی تهدیدات و پیشرفت‌هایی که رقبا در حوزه سایبر دارند، باید نسبت به ارتقای مستمر بازدارندگی نیز اقدام شود.

سیاست های کلی پدافند غیرعامل:

در سیاست های کلی پدافند غیرعامل نیز بازدارندگی در مقابل تهدیدات و اقدامات نظامی دشمن، طبقه بندی مراکز و به کارگیری اصول و ضوابط پدافند غیرعامل در مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای نام برده شده که متن کامل این سیاست ها به شرح ذیل است:

۱) تأکید بر پدافند غیرعامل که عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می گردد.

۲) رعایت اصول و ضوابط پدافند غیرعامل از قبیل انتخاب عرصه ایمن، پراکنده سازی یا تجمیع حسب مورد، حساسیت زدایی، اختفاء، استتار، فریب دشمن و ایمن سازی نسبت به مراکز جمعیتی و حائز اهمیت بویژه در طرح‌های آمایش سرزمینی و طرح های توسعه آینده کشور.

۳) طبقه بندی مراکز، اماکن و تاسیسات حائز اهمیت به حیاتی، حساس و مهم و روزآمدکردن آن در صورت لزوم.

۴) تهیه و اجرای طرح های پدافند غیرعامل (با رعایت اصل هزینه – فایده) در مورد مراکز، اماکن و تاسیسات حائز اهمیت (نظامی و غیرنظامی) موجود و در دست اجراء بر اساس اولویت بندی و امکانات حداکثر تا پایان برنامه ششم و تامین اعتبار مورد نیاز.

الزامات نظریه بازدارندگی سایبری:

اجزای سازنده یک راهبرد بازدارندگی سایبر می تواند با بررسی مختصر چگونگی عملکرد بازدارندگی در طول جنگ سرد و وضعیت امروزی توضیح داده شود. تجربه جنگ سرد نمی تواند با واقعیت های متفاوت امروزی شامل قلمروی سایبری پیوند زده شود. برغم آن، فرآیندی که تئوری بازدارندگی در جنگ سرد براساس آن قرار گرفته بود، درس هایی را داده که می تواند برای ایجاد یک راهبرد معتبر بازدارندگی سایبر امروزی مورد استفاده قرار گیرد.

اشارات تئوری بازدارندگی هسته ای معاصر برای بازدارندگی حملات سایبر چیست؟ تئوری بازدارندگی امروز برای تمرکز بر نفوذ در انگیزه ها و الهامات بوسیله بازداشتن آنها از اینکه تهاجم نمی تواند موفق شود، بکار گرفته می شود. بدین ترتیب هدف اصلی راهبرد بازدارندگی ایالات متحده از اتحاد شوروی مرده تا کشورهای ورشکسته، تروریست ها و سایر رقبا به آنهایی که منافع ایالات متحده و متحدین اش را تهدید می کنند، تغییر داده است. در حالی که راهبرد هنوز هدفش حملات هسته ای و تهاجمات بزرگ متعارف است، همچنین بازداشتن تحریکاتی همچون تروریسم است. این تاکید بر رقبای چندگانه و تحریکات برای ظهور مفهوم "بازدارندگی مناسب" داده شده بود[۲]: بازدارندگی باید تمایلات ویژه هر رقیب انفرادی و هدایت آن را به حساب آورد. دکترین سه تایی هسته ای ایالات متحده اکنون مرکب از نیروهای آفندی، نیروهای دفاعی و زیرساخت هاست. امروز بمب افکن ها و موشک ها، کلاهک های متعارف (غیرهسته ای) دقیق در معادله بازدارندگی مهم شمرده می شوند. کل حالت نظامی متعارف ایالات متحده به عنوان یک سهیم عمده در بازدارندگی همچنین برای سایر فعالیت های کلیدی، توضیح داده شده در راهبرد دفاع ملی، شامل تضمین متحدین، بازداشتن دشمنان بالقوه از هدایت محرک رقابتی و شکست دادن رقبا در زمان جنگ نگریسته می شود.

در حالی که جنگ سرد در سال ۱۹۹۰ پایان یافت، بازدارندگی برای کاربردهای دیگر ادامه می یابد اما بنظر می رسد در برخی موارد شکست خورده است. آن در بازداشتن عراق از تهاجم به کویت در سال ۱۹۹۰، تهاجم صربستان به کوزوو در سال ۱۹۹۹ یا القاعده در استفاده از افغانستان برای راه اندازی حمله

---

[۲] - "بازدارندگی مناسب" یک مفهوم محوری راهبرد جاری بازدارندگی ایالات متحده است و در آیین نامه "عملیات های بازدارندگی، مفهوم عملیات مشترک" بحث شده است.

اش به ایالات متحده در سال ۲۰۰۱ شکست خورد. بازدارندگی، مانع از پیگیری تسلیحات هسته ای توسط کره شمالی نشد، حضور نیروهای زیاد نظامی ایالات متحده در عراق و افغانستان مانع از اجرای جنگ چریکی با هدف بی ثبات کردن دو کشور نشد.

چنین مسائلی برخی ناظرین را هدایت کرد به اینکه تئوری بازدارندگی در مقابل رقبای روز ایالات متحده که طیفی از کشورهای ورشکسته تا تروریستها را دربرمی گیرد، ناقص است. آیا مسئله این است که ایالات متحده یک تئوری بازدارندگی که بنحو صحیحی متقاعده کننده باشد، ندارد یا این است که رقبای امروزی اراده بیشتری برای ریسک پذیری دارند و قیمت های سنگینی از آنچه اتحاد شوروی در طول جنگ سرد می پرداخت، می پردازند؟ اگر موفقیت بازدارندگی برای اطمینان بخشی در طول جنگ سرد می توانست عمل کند، آن نمی تواند برای اطمینان بخشی امروزی عمل نماید. آن در تعادل راهبردی یک اعتبار است نه یک پایداری. برخی تهدیدات، سخت تر از سایرین برای بازداشتن هستند. شناخت این واقعیت ناراحت کننده هدف از طراحی یک راهبرد بازدارندگی سایبری موثر هم ضروری تر و هم مشکل تر را می سازد.»(Kramer, 2009: 324-325)

شیوه های اصلی بازدارندگی سایبری:

هدف یک راهبرد بازدارندگی سایبر نفوذ بسیار قاطعانه در محاسبات تصمیم سازی یک رقیب است تا آن حملات سایبری علیه منافع خودی راه نیاندازد. اقدامات هماهنگ شده شانس های موفقیت حمله کننده را کاهش می دهند بطوری که خطرات، هزینه ها، ریسک ها و ابهامات یک حمله سایبری، از سود یا پاداش مورد انتظار مشخص می شود. در مورد رقیبی که بدنبال استفاده از تهدیدات حملات سایبری یا حملات واقعی است تا کشور رقیب را وادار به اقدامی کند که در خدمت منافع یا اهداف بزرگترش باشد، یک راهبرد بازدارندگی سایبر کارآیی خواهد داشت چنانچه دشمن قضاوت کند که این تحمیل تلاش شده موفق نمی شود و اینکه حمله باعث مقابله به مثل کشور مقابل شده و یک عقب نشینی راهبردی خالص برای حمله کننده نتیجه آن خواهد بود.

چنین محاسبه راهبردی در استفاده چین از تهدیدات و حملات سایبری همچنین اقدامات سایر رقبای احتمالی در زمینه سایبر بکار می رود. واکنش های عملی بالقوه در چنین وضعیت هایی در سه شیوه اصلی بازدارندگی مورد نظر در مدل مفاهیم عملیات های مشترک خلاصه شده است: بازدارندگی بوسیله انکار سودهای آن، بازدارندگی بوسیله تحمیل هزینه ها و بازدارندگی بوسیله ارائه محرک هایی برای منع رقیب.

۱) **بازدارندگی بوسیله انکار سود**، مستلزم تهدید قابل باور در محروم کردن حمله کننده از منافع یا دستاوردهایی که در جستجوی آن است، می باشد: متقاعد کردن آن به اینکه یک حمله سایبری به اهدافش دست نخواهد یافت.

۲) **بازدارندگی بوسیله تحمیل هزینه** مستلزم تهدید قابل باور در تحمیل هزینه ها، ضایعات و ریسک هایی است که پذیرش آنها بسیار سخت است، بدین ترتیب متقاعد کردن رقیب به اینکه تنبیه بسیار سنگین تر از موفقیت های مورد انتظار خواهد بود.

۳) **بازدارندگی بوسیله ترغیب برای منع رقیب** به معنای متقاعد کردن رقیب به این است که هیچ حمله ای یک نتیجه قابل قبول و جذاب نخواهد داشت.

این سه مکانیسم بازدارندگی می توانند بصورت منفرد بکار گرفته شوند اما آنها احتمالا زمانی که به شیوه های تقویت متقابل ترکیب شوند، بهتر عمل می کنند. رقبای سایبری بالقوه ممکن نیست بازیگران یگانه ای باشند که بوسیله یک محاسبه راهبردی منفرد مورد تفوق قرار گرفته باشند، تصمیم سازان ممکن است بوسیله بازیگران چندگانه همچون بخش های مختلفی از یک حکومت خارجی یا شبکه تروریستی مورد نفوذ باشند که اولویت ها و تحول ریسک را متفاوت کرده است. این سه مکانیسم با همدیگر می توانند در بازیگران چندگانه به شیوه های مختلف و در درجات متفاوت نفوذ کنند و چشم اندازی را که مانع از تصمیم به انجام حملات سایبری شود، افزایش می دهند.

یک راهبرد بازدارندگی سایبر همچنین نیاز به هوشیاری در مورد آستانه ها دارد. حملات سایبری می توانند در اشکال و اندازه های مختلف انجام شوند و آنها همه شایستگی پاسخی همانند را نخواهند

داشت. برخی حملات ممکن است بقدری کوچک باشند که نباید در مورد آنها نگران شد. سایرین ممکن است شایسته یک پاسخ تلافی جویانه باشند اما درجه آن پاسخ بستگی به درجه تحریک دارد.

درباره ابزارها برای پیگیری بازدارندگی سایبر چه؟ یک راهبرد بازدارندگی سایبر در حمایت از تهدیدات چندگانه و وضعیت های مختلف هدفگذاری شده، نمی تواند اساسا بر هیچ ابزار منفردی متکی نباشد. این راهبرد باید قادر باشد تا ابزارهای چندگانه ای را بکار گیرد که یک دامنه گسترده ای از گزینه های پاسخ را پیشنهاد کند که بتواند دسته بندی شده و برای خدمت به اهداف ویژه ای که پیگیری می شوند، مجددا دسته بندی شده و اینکه اجازه تعامل با وضعیت های پیچیده متحول پویا را بدهد. ابزارهای چندگانه ممکن است بصورت انفرادی یا ترکیبی مورد استفاده قرار گیرند. ابزارهای منفرد ممکن است در مقابل رقبای ضعیف موثر باشند اما ابزارهای چندگانه احتمالا نیاز باشد تا علیه مخالفین جاه طلب مدعی بکار گرفته شوند. برای هر وضعیتی، ابزارهای تلافی باید کشور را قادر نمایند تا بطور قابل اعتماد و قدرتمندانه ای عمل نماید.

هم دفاع سایبر و هم آفند سایبری بخشی از راهبرد بازدارندگی هستند اما نه همه راه حل یا حتی مهمترین اجزای آن نیستند.

در برخی وضعیت ها، دفاع سایبری ممکن است بی تاثیر باشد بلکه یک کشور ممکن است پاسخ با یک ضدحمله سایبر را نگزیند. موثرترین پاسخ به برخی حملات سایبری ممکن است سیاسی و اقتصادی، شاید منزوی کردن حمله کننده در جامعه جهانی، بسیج کشورها برای برخورد با آن به عنوان یک منفور یا تحمیل تحریم های اقتصادی باشد. این می تواند تنبیهات رنج آورتر از هر ضدحمله سایبری را تحمیل نماید. حتی ضربات نظامی ممکن است در تلافی یک حمله واقعا ویرانگر به شبکه های اطلاعاتی ایالات متحده یا به عنوان بخشی از عملیات رزمی عمده علیه دشمنان اجرا شوند. بیش از هویت حمله کننده، طبیعت حملات بالقوه و طبیعت یک پاسخ مناسب بستگی دارد. کشور نیاز دارد تا قادر به پاسخ گویی منعطف برای برخورداری از سهم گزینه هایی که قابلیت سازگاری را فراهم نمایند، باشد و قابلیت بکارگیری ابزارهای چندگانه را داشته باشد. (Kramer,2009:327-329)

علاوه بر موارد سه گانه، در بازدارندگی اصول زیر نیز مورد توجه خواهد بود:

۱) آسیب ناپذیری:

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.

۲) پشیمان کنندگی:

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

۳) القای پیام اقتدار:

القا کردن در لغت به معنای رسانیدن سخن و آگاه کردن کسی به شیوه مستقیم یا غیرمستقیم آمده است. اقتدار با هدف بازدارندگی درصورتی مؤثر خواهد بود که پیام آن به دشمن برسد. تا زمانی که 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.

۴)برخورداری از فناوری بومی برتر:

برخورداری از فناوری در حوزه‌های زیرساخت‌ها اطلاعاتی و شبکه امکان نفوذ ناپذیری و کاهش آسیب پذیری آنها را فراهم می‌آورد به شرطی که این فناوری بومی باشد زیرا فناوری غیربومی و وابسته درصورت پیشرفته بودن هم برای دشمن قابل نفوذ خواهد بود لذا بازدارندگی ایجاد نخواهد کرد.

گام های بازدارندگی سایبری:

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

۱) تعیین اهداف بازدارندگی و مفهوم راهبردی

۲) برآورد محاسبه راهبردی تصمیم سازان رقیب

۳) شناسایی تاثیرات بازدارندگی مورد نظر در هدایت رقیب

۴) توسعه و برآورد راه کارهای طراحی شده برای دستیابی به تاثیرات مورد نظر

۵) توسعه طرح هایی برای اجرای راه کارها و برای پایش و برآورد پاسخ های رقیب

۶) توسعه ظرفیت ها برای پاسخ انعطاف پذیر و موثر همانطوری که وضعیت بازدارندگی تحول می یابد.

این شش گام انعکاس درخواست ها و چالش های دستیابی به بازدارندگی مناسب حملات سایبر هستند. بازدارندگی مناسب تایید می کند که اهداف ایالات متحده ممکن است بطور قابل ملاحظه ای بیش از یک وضعیت برای آینده باشند با نیاز به انواع مختلف پاسخ ها. بدین ترتیب، گام اول، نیات ایالات متحده برای وضعیت های سایبر را تعریف می کند. گام دوم بیان می کند که دلیل همه حریفان مشابه نیستند، ایالات متحده باید تعیین کند که چگونه با حریف برخورد شود، مفهوم راهبردی برخورد و محاسبه تصمیمی که بوسیله حریف بکار گرفته می شود. هر سه نوع رقبا – حریفان نزدیک، کشورهای ورشکسته اندازه متوسط و گروههای تروریستی – که احتمالا مورد رویارویی قرار می گیرند، وضعیت های روانی و انگیزه های مختلفی برای مواجهه با ایالات متحده دارند همچنین آنها رفتارهای مختلف در مسیر اهداف، اقدامات و ادراکات قدرت اراده و راه حل ایالات متحده، تمایلات ریسک پذیری و حمایت از ابهامات دارند.

گام های سوم و چهارم هر دو مهم و چالشی هستند. گام سوم شناسایی تاثیرات مورد نظر مستلزم بازدارندگی در هدایت حریف است؛ سپس در گام چهارم، راه های کار برای ایجاد این تاثیرات توسعه داده شده و ارزیابی می شوند. بطور کلی، وقتی که بازدارندگی در گذشته موفق شده است، ایالات متحده در شناسایی اینکه چگونه راه های کار ایجاد تاثیراتی کنند که بتوانند در انگیزه ها و رفتار دولت های رقیب به روش های مورد دلخواه نفوذ نمایند، دارای مهارت است. وقتی بازدارندگی شکست خورده، معمولا به این دلیل بوده که دولت امریکا در برخورداری از سیاست ها و اقدامات مثبتی که قویا در ادراکات و انگیزه های رقبا نفوذ نماید، شکست خورده است. در این موارد، مسئله این نبوده که در نیاز به ارسال علامت های قوی

بازدارندگی چشمانش بسته بوده اما اینکه آن علایم اشتباه ارسال کرده که در برخورداری از تاثیرات دلخواه شکست خورده بدلیل این بوده که آنها نشانه مطمئنی از اراده و قابلیت ایالات متحده نبوده اند.

بدلیل اینکه برخی وضعیت های حمله سایبری بخشی از رویارویی های ژئوپلیتیکی بزرگتری خواهند بود، تعیین اینکه چگونه علایم اطمینان بخش بازدارندگی سایبری ارسال شود، اقدامات چندگانه ای را ضروری خواهد ساخت که در مقابل، نیاز به فعالیت های گسترده تر ایالات متحده با هدف دستیابی به سایر منظورها خواهد داشت. وقتی ایالات متحده بطور ضعیفی در چشمان رقبا عمل می کند، آن ممکن است یک علامت بی هدفی باشد که حملات سایبری می توانند با مصونیت اجرا شوند یا با یک پاسخ قاطع مواجه نخواهند شد. بنابراین، وقتی ایالات متحده با قدرت در مدیریت یک بحران بزرگتر عمل می کند که ماورای قلمروی سایبر می رود، آن می تواند ریسک دفن علایم بازدارندگی سایبری آن در یک افراط در سایر فعالیت ها را داشته باشد، بدین ترتیب رقیب را به چشم پوشی یا سوء تفسیر آنها هدایت می کند. ماورای این، اقدامات ایالات متحده که نفوذ قوی در یک سری از رقبایی که ممکن است تاثیر اندکی در سایر رقبا داشته باشد، دارد که ممکن است بوسیله یک سری از اقدامات کاملا متفاوت مورد نفوذ قرار گیرند. برای برخی رقبا، یک هشدار ساده ممکن است بقدر کافی بازدارندگی داشته باشد، برای سایرین، یک پاسخ سایبری یا استفاده قدرتمندانه از سایر ابزارها و همچنین یک پاسخ سایبری ممکن است مناسب باشد. برای برخی، بدین ترتیب تنها پاسخ مناسب ممکن است استفاده از قدرت نظامی یا سایر ابزارهای غیرسایبری باشد. به چندین دلیل، بازدارندگی سایبر می طلبد که ایالات متحده مهارت هایش را در حل چگونگی نفوذ در هر رقیب و چگونگی اقدام بر طبق آن توسعه دهد.

گام پنجم، توسعه طرح ها، و گام ششم توسعه ظرفیت ها نیز مهم هستند. طرح ها، جزییات قاطعی را مشخص می کنند از اینکه چگونه ابزارهای چندگانه با همدیگر در یک بحران سایبری در هم می آمیزند؛ آنها همچنین ریسک های اشتباهات جدی در داوری را کاهش می دهند اگر لازم باشد اقدامات پیچیده با همدیگر در حرکت پیوند زده شوند. طرح های اجرایی نیاز به وضعیت های پیش بحران و گام های اولیه بحران های جاری و همچنین برای گام های متعدد در آنچه که یک بحران سایبری ممکن است افشا شود، همچنین یک وارسی حمله سایبری کوچک، بزرگتر اما هنوز حمله محدود شده، دارد. این ارتقای سایبر،

در مقابل، ممکن است بخشی از یک سلسله گام های سیاسی و نظامی با هدف فشار آوردن بر ایالات متحده باشد. بدین ترتیب یک راهبرد بازدارندگی سایبر نیاز به تسلط بر نردبان صعود همچنین سایر محتویات مدیریت بحران سایبر دارد.

بازدارندگی مناسب سایبر بیش از اینکه اجرای آنچه که رقبای بالقوه را از همدیگر متمایز می کند، ادراکات و انگیزه های مختلف را در بر خواهد گرفت و حملات سایبر را با دستورکارهای مختلف در ذهن بکار خواهد گرفت. آن همچنین تحقق این است که اهداف ایالات متحده از یک رقیب و وضعیت، به آینده نوسان خواهد کرد که پاسخ های متفاوتی را ممکن است به منظور داشتن انواع مختلف تاثیرات نیاز داشته باشد و اینکه طرح های پاسخ به بحران باید ظرفیتی را ایجاد کند که هم قوی و هم موثر باشند. برخی حملات سایبری در یک خلاء اتفاق نخواهند افتاد اما بجای آن در یک زمینه بزرگتری ظهور خواهند کرد که به پاسخ های چندگانه ایالات متحده به علاوه اینها در تضمین بازدارندگی سایبر هدفگذاری شده اند، نیازمند است. بدلیل اینکه هر وضعیت سایبری احتمالا منحصر به فرد است، بکاربردن بازدارندگی مناسب برای زمینه سایبر قول می دهد پیچیده و چالشی باشد.(Kramer, 2009: 329-331)

ضرورت‌های راهبردی برای بازدارندگی سایبری

بدلیل اینکه یک راهبرد بازدارندگی سایبر مناسب بایستی با تهدیدات مختلفی تعامل کند، موجودی ها و قابلیت های چندگانه مورد نیاز خواهد بود. این نیازمند یک تلاش پایدار با دامنه گسترده است. نیازها و اولویت های کلیدی برای دستیابی به یک قابلیت موثر برای اجرای یک راهبرد بازدارندگی سایبر عبارتند از[۳]:

- یک سیاست مثبت روشن و سخت که منظور ایالات متحده برای بازدارندگی حملات سایبر را توضیح دهد.
- هشدار وضعیتی بالای جهانی که طیف کاملی از تهدیدات و حالت های بالقوه سایبری را تعدیل نماید در جایی که آنها ممکن است ظاهر شوند.

---

3 -

- سامانه های خوب فرماندهی و کنترل که اجازه پاسخ های منطقه ای چندگانه و سرزمینی هماهنگ شده به تهدیدات سایبری را بدهد.
- دفاع سایبری موثر که هم از نیروهای مسلح و هم کشور با یک اولویت بالا برای دفاع از زیرساخت های کلیدی حفاظت نماید.
- یک طیف گسترده ای از قابلیت های آفندی ضدسایبر شامل حمله سایبری و سایر ابزارها برای تاکید بر قدرت ملی به منظور تقویت بازدارندگی قبل از بحران، در طول بحران و بعد از آن.
- همکاری و تشریک مساعی بین سازمانی خوب توسعه داده شده با متحدین و شرکا.
- روش شناسی ها، اقدامات و تجربیات بازدارندگی سایبری که بتواند به هدایت فرآیند طرح ریزی کمک نماید.

پیشینه تحقیق:

- رمضان زاده و همکاران(۱۳۹۹) در تحقیقی با عنوان ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تاکید بر بعد بازدارندگی به دنبال ارائه مدل در این زمینه بوده است. نتایج تحقیق وی نشان داد الگوی بازدارندگی سایبری ن. م دارای مولفه های پنج گانه پشیمان کنندگی، استمرار عملیات، پاسخ به تهدید، استحکام سازی و بازیابی است.
- محمد احدی (۱۳۹۶)در پژوهشی با عنوان طرح راهبردی دفاع سایبری جمهوری اسلام ی ایران در حوزه بازدارندگی در پاسخگویی به این سوال که « راهبردهای دفاع سایبری در حوزه بازدارندگی چیست؟ » انجام شد و در این راستا سوالات فرعی «اصول و ارزش ها و چشم انداز های دفاع سایبری در حوزه بازدارندگی چیست؟»، «ماموریت های طرح راهبردی دفاع سایبری در حوزه بازدارندگی چیست؟» و «عوامل داخلی و خارجی موثر در در حوزه بازدارندگی کدامند؟» مورد توجه قرار داده و با بهره گیری از روش تحلیل کمی و کیفی و روش دلفی و اکتشافی در مراجعه به اسناد و مدارک، به این نتیجه رسیدند که، بازدارندگی در حوزه سایبر متفاوت و پیچیده تر از حوزه نظامی است و با رعایت یک سری الزامات و بهره‌گیری از شیوه های مناسب می توان به آن دست یافت و بدین ترتیب هزینه دفاع را تا حد قابل توجهی کاهش داد.

• مؤلفه‌های بازدارندگی در دفاع سایبری: مدل بازدارندگی معطوف به جلوگیری از تحقق تهدیدات علیه خود است بنابراین، طراحی این بعد مستلزم به‌کارگیری پارامترهای مختلفی است که تحقق چنین موضوعی را سبب می‌شوند. در این راستا اولین جزء مدل، طراحی حوزه‌های راهبردی است که کشور در آن منافع متعددی داشته و تهدیدات علیه آن نیاز از چنین محیطی سرچشمه خواهد گرفت. دومین جزء این بعد معطوف به ایجاد شرایط مقدماتی و منطقی بازدارندگی است که شامل مؤلفه‌های ذیل خواهد بود:

• ارتباط: به معنای برقراری رابطه با حریف و آگاه ساختن وی از قصد و نیت و حدود اعمال ممنوعه است. در نظریه بازدارندگی، جلوگیری از برخورد میان طرفین، به تبادل‌نظر صریح و ضمنی طرفین بستگی دارد؛ بنابراین لازم است دولت‌ها از طریق انتشار اعلامیه رسمی، ارسال پیام و اعلام برنامه‌های خود، نیات واقعی خود را در این زمینه آشکار کنند بازدارندگی هنگامی مؤثر است که نیروی بازدارنده منظور خود را صریح و شفاف به اطلاع طرف مقابل برساند و معین کند در صورت موردحمله قرار گرفتن دقیقاً چه عواقبی در انتظار مهاجم خواهد بود. ارتباط می‌تواند به‌صورت صریح یا ضمنی باشد.

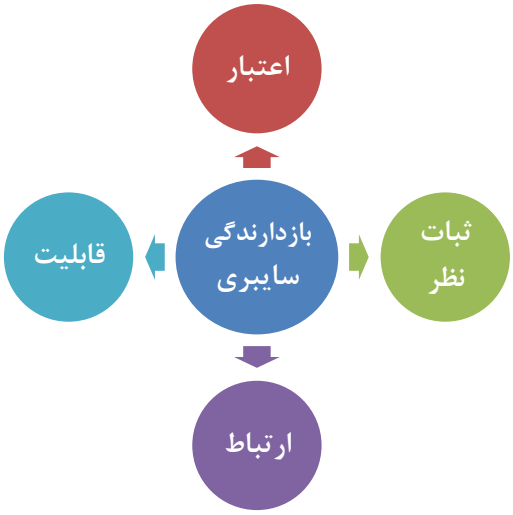
• توانایی یا قابلیت: علاوه بر عقلانیت، به معنای توانایی تحمیل خسارت غیرقابل‌تحمل بار دشمن و عقلانیت طرفین در محاسبه سود و هزینه احتمال رفتارهای خود است. این ویژگی به جنبه توانایی دولت‌ها در نظریه بازدارندگی مربوط می‌شود. این به معنای توانایی وارد آوردن ضربه به مهاجم احتمالی به‌وسیله تجهیزات متعارف و غیرمتعارف است. نیروی بازدارنده به‌جز مواردی که بلوف میزند، باید قادر باشد در صورت لزوم مجازات متناسب را برای طرف مهاجم به مرحله عمل درآورد.

• اعتبار: یعنی تهدید واقعی و باور حریف به اینکه طرف مقابل از چنین توانایی برخوردار است. به عبارتی عقلانی بودن تهدید شرط اعتبار تهدید به‌حساب می‌آید.

• ثبات نظر به معنای ثابت ماندن در دیدگاه‌ها و استحکام در مواضع است. اگر برخورد به‌اندازه 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، تحت تأثیر قرار دهند، یک نظام بازدارندگی مؤثر صرفاً به داشتن نیروی نظامی قدرتمند نیاز ندارد، بلکه یک قدرت بازدارنده مؤثر علاوه بر معتبر بودن، باید باثبات هم باشد.

مدل مفهومی پژوهش:

پس از بررسی ادبیات موضوع و نیز مصاحبه با صاحب نظران مدل مفهومی تحقیق به شرح زیر ارائه گردید.



شکل ۱: چارچوب مفهومی بازدارندگی سایبری

روش شناسی تحقیق

بر اساس نوع هدف تحقیق کاربردی می‌باشد، از نظر اجرا و گردآوری داده‌ها نیز این تحقیق با توجه به اهداف پژوهش، سوالات ویژه تحقیق، محدودیت‌های منابع اطلاعاتی، امکانات محیط آزمایشی و نیز محدودیت در زمان اجرا از روش توصیفی استفاده می‌کند. تحقیق توصیفی شامل مجموعه روش‌هایی است که هدف آن توصیف کردن شرایط یا پدیده‌های مورد بررسی می‌باشد (سرمد، بازرگان و حجازی، ۱۳۸۱).

نتیجه‌گیری و پیشنهادها:

فضای سایبری نقش مهمی در توانایی یک کشور در حفظ امنیت ملی و قابلیت نظامی‌اش ایفا می کند. اگرچه اعمال تهدید علیه رقبای بالقوه، آنها را از جاسوسی یا حمله سایبری منصرف نخواهد کرد، اما کنش ها و بیانیه ها در مورد فضای سایبری باید از تعهد یک کشور به انجام اقدامات سخت برای تامین منافع سایبری حکایت کند.

برای کارآمدی بازدارندگی در حوزه سایبر، باید از ترکیب سه مولفه کلیدی ، یعنی دفاع، شناسایی و تلافی بهره جست. بدون اقدامات دفاعی مناسب، نمی توان تعداد حملات موفق را کاهش داد و این حملات از کنترل خارج می شود. اگر چه بازدارندگی سایبری چالش برانگیز است اما با یک راهبرد سنجیده و واقع بینانه، بازدارندگی سایبری می تواند کارایی قابل توجهی در تقویت اقتدار دفاعی کشور داشته باشد.

راهبردهای بازدارندگی سایبری باید حاکی از موضع دفاع سایبری قدرتمند باشد و مسیرها و کنشگران اصلی تهدیدآمیز را شناسایی کند. این امر باعث حفظ اعتبار سیاست کلی بازدارندگی و موضع کشور خواهد شد. در زیر به برخی از پیشنهادات در این زمینه اشاره می شود:

باید از اعلام تهدیدهای بازدارندگی سایبری اجتناب شود؛ این تهدیدها بیهوده است، با خطر خسارت‌های ناخواسته همراه است و به خاطر پارادوکس اعتبار- ثبات، بی‌ثبات کننده هستند. در درون سیاست های اعلام شده، اظهاراتی مبنی بر تعهد کشور به دفاع از خود در فضای سایبری برای حمایت از موضع کلی بازدارندگی ضروری است، اما به تنهایی نمی تواند جلوی حملات سایبری یا جاسوسی سایبری را بگیرد.

باید به تشویق و ترغیب وضع قوانین بین المللی پرداخت که به شکل‌گیری این بحث کمک کند و افکار بین المللی را مطلع می سازد.

باید در فعالیت‌هایی مشارکت کرد که به دنبال ایجاد چهارچوبی برای جلوگیری از تشدید یا ظهور تنش ها در فضای سایبری هستند. گفتگوهای صریح دیپلماتیک درباره حوادث سایبری، عامل بالقوه ای برای کاهش درگیری ها یا تنش های سایبری احتمالی آتی محسوب می شود.

باید روی تجهیزاتی سرمایه گذاری شود که دفاع شبکه ای را تقویت می‌کند و ارزش درک شده تجاوز سایبری را کاهش می دهد. تاثیر بازدارندگی، رویکردی قوی، چابک و چند-لایه امنیت سایبری به تهدید به مجازات بیشتر است. شکست های پیاپی یا کاهش رسوخ در شبکه، کیفیت بازدارندگی راهبردی بازدارنده را اثبات می‌کند و به متخاصم عملا پیام می دهد که این شبکه هدفی سخت است و جسارت یک دشمن در طرح ریزی استفاده از ابزار دستکاری یا مخرب سایبری برای حمایت از اهداف نظامی یا ملی را از بین می برد.

تغییر برآورد هزینه و سود به نفع مدافع، غیر قابل نفوذ بودن یک شبکه را تضمین نمی کند، اما این شبکه را هدفی ناخوشایند برای متخاصمان ساخته و شبکه را از اختلال ناشی از متخاصمان غیرمصمم مصون می سازد و کشور باید تنها بر تهدیدهای خیلی مصمم، متمرکز شود.

باید در زیرساخت ها و شبکه های مقاوم سرمایه گذاری شود، زیرا در صورتی که متخاصمان از اقدامات خرابکارانه منصرف نشدند، سیستم ها به سرعت احیا می شوند و خسارت ناچیز خواهد بود.

بر همین منوال، **راهبرد بازدارنده برای سازمان های بخش خصوصی نیز موثر است** .سرمایه گذاری در قابلیت های امنیت سایبری باید بر اساس ارزیابی میزان حساسیت داده های نگهداری شده یا انتقال آن و نمایه ریسک سازمان، درجه بندی شود.

فصلنامه علمی (مقاله علمی - پژوهشی)جامعه شناسی سیاسی ایران، سال دوم، شماره اول (پیاپی ۵)، بهار ۱۳۹۸

منابع:

- رمضان زاده مجتبی " تدوین راهبردهای دفاع سایبری ارتش جمهوری اسلامی ایران" فصلنامه مدیریت نظامی دانشگاه امام علی (ع) شماره ۵۹ ، سال پانزدهم، پاییز ۱۳۹۴
- حسن بیگی، ابراهیم (۱۳۸۴)حقوق و امنیت در فضای سایبر،انتشارات موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر تهران
- حسینی، پرویز، و ظریف منش، حسین (۱۳۹۲)، «مطالعه تطبیقی ساختار دفاع سایبری کشورها»، فصلنامه پژوهش های حفاظتی و امنیتی، جلد ۲، شماره ۵. بازیابی از ۱۹.
- عبدالله‌خانی، علی(۱۳۸۵)، حفاظت از زیر ساخت‌های حیاتی اطلاعاتی(فصلنامه سیاست دفاعی، شماره ۵۴)، تهران، انتشارات دانشگاه امام حسین(علیه السلام)؛
- نامخواه، ناصر. (۱۳۹۰)، اینترنت و دفاع سایبری، تهران: دانشگاه آزاد اسلامی.
- Filipkwoski'Wojciech(2008)'cyber Laundering' an analysis of Typology and Technology
- Franklin D. Kramer, Cyberpower and National Security, U.S National Defense University, Washington D.C, 2009.
- Garvin, David A. "Building a Learning Organization". Harvard Business Review. July - August 1993. pp 78-91.
- Gunasekaran, A, McGaughey, R and Wolstencraft, V; Agile manufacturing: Concepts and framework, Agile Manufacturing: The 21st Century Competitive Strategy, Elsevier Science, 2001, 25-49
- http://iran1414.ir/index.php/content-a/yaddasht1035556214/39937-2012-10-20-15-02-29