فصلنامه مطالعات جنگ
سال دوم، شماره هفتم، زمستان ۱۳۹۹
مقالهٔ ششم از صفحه ۱۲۵ تا ۱۵٤

نقش جنگ سایبری و شناسایی مؤلفه‌های تأثیرگذار آن در بازدارندگی سایبری

عبداله وثوقی نیری*[۱]، داود غفوری[۲]، رسول کریمی طاهر[۳]

دریافت مقاله: ۹۹/۰۵/۲۰ پذیرش مقاله:۹۹/۰۹/۱۴

چکیده

با تغییر ماهیت آسیب به تهدید محیط صبغه و رنگ امنیتی به خود می‌گیرد و بازیگران را وامی‌دارد تا کنش‌ها و واکنش‌هایی را از خود ظاهر ساخته و به‌تناسب ابزارهای سخت‌افزاری و نرم‌افزاری را بکار گیرند.امروزه کشورهای در حال تخاصم بیش از آن‌که به حمله نظامی علیه یکدیگر دست بزنند، تلاش می‌کنند تا در ابعاد اقتصادی، اجتماعی و تروریسم به تهدید طرف مقابل بپردازند؛ چه آن‌که این حوزه‌ها دارای هزینه‌های مستقیم کمتری بوده و در بلندمدت تأثیر بیشتری می‌گذارد. بنابراین با عصری نوین مواجهیم که پررنگ شدن روزافزون تکنولوژی‌های سایبری در پارادایم برتری نظامی در آن مشهود است. نفوذ زیرساخت‌های سایبری در امور سیاسی، اقتصادی، اجتماعی و نظامی به حدی است که امروزه جنگ سایبری به علت توان درگیر کردن زیرساخت‌های حیاتی کشور، اهمیت دوچندانی یافته است. با توجه به مسائلی از قبیل عدم قطعیت در شناسایی مهاجم سایبری، حساسیت‌های ویژه‌ی نمایش توانایی‌های سایبری کشور و ابهام در شناسایی زمان دقیق و گستره تهاجم سایبری و لزوم پاسخ‌دهی سریع و آنی به حملات سایبری؛ بازدارندگی سایبری به یک چالش مهم برای کشور تبدیل‌شده است. بر این اساس، هدف از این تحقیق بررسی نقش جنگ سایبری و شناسایی مؤلفه‌های تأثیرگذار آن در بازدارندگی سایبری است. روش تحقیق در این پژوهش توصیفی- تحلیلی می‌باشد. مطالعه مبانی نظری تحقیق نشان داد مقابله‌به‌مثل، آسیب‌ناپذیری، انعطاف‌پذیری، نامریی شدن وابستگی متقابل راهبردهایی هستند که می‌توانند مولفه های تاثیر گذار جنگ سایبری باشند.

واژگان کلیدی: تهدید، جنگ، جنگ سایبری، بازدارندگی

۱ . هیئت علمی دانشگاه علوم و فنون هوایی شهید ستاری، a.vosoughi@yahoo.com
۲ . هیئت علمی دانشگاه علوم و فنون هوایی شهید ستاری
۳ . هیئت علمی دانشگاه علوم و فنون هوایی شهید ستاری

مقدمه

بافاصله گرفتن از رویارویی ابرقدرت‌ها، دولت‌ها شروع به مقابله با تهدیداتی کردند که در طول جنگ سرد وجود داشتند اما تصور می‌شد اهمیت کمتری دارند؛ که برخی نیز آن‌ها را تهدیدات کوچک می‌خواندند. یکی این تهدیدات جنگ سایبری است. هنوز تصور می‌شود که این تهدید به‌تنهایی پتانسیل سرنگونی دولت‌های پایدار و مستقر، به‌خصوص در جهان توسعه‌یافته، را ندارند. بااین‌حال، با توجه به ابعاد پیشرفت فناوری اطلاعات و گسترش استفاده از آن در اغلب ابعاد زندگی، فضای سایبری به‌صورت یک زیرساخت اساسی و حیاتی برای دولت‌ها درآمده است، طوری که هم‌اکنون حتی سلاح‌های نظامی هم از بستر سایبری استفاده می‌کنند. تهدیدهایی مانند ویروس استاکس نت و جریان سایبری به وجود آمده بین روسیه و گرجستان در سال ۲۰۰۸ نشان می‌دهد تهدیدات سایبری به‌مرورزمان از اهمیت استراتژیک بیشتری برخوردار می‌شوند.

ضروری و حیاتی است که همگام با تغییرات خصوصاً تغییر در تهدیدات، تحولات مثبتی در امر رویارویی و ارتقاء توان جنگ سایبری به وجود آید. زیـرا ارتش ارتش ج.ا.ا. با توجه به حساسیت در مأموریت‌های محوله، می‌بایست در هر مقطع زمانی همگام با تغییرات جهانی به‌روز باشد .

اطلاعات در این حوزه مسلماً نادر هستند که یکی از دلایل آن جدید بودن اندیشه راهبردی در جنگ سایبری است، دلیل دیگری هم ترکیبی از سازمان‌های نظامی به‌عنوان اندیشمندان راهبردی و پیوند نزدیک بین جنگ سایبری و دارایی‌های اطلاعاتی است، بدان معنی که اطلاعات محدودی در گستره غیر طبقه‌بندی‌شده وجود دارد. آنچه در پی آمده بدون شک تنها قسمت کوچکی از اندیشه راهبردی واقعی معاصر در جنگ سایبری است.

اندیشه راهبردی، درباره جنگ سایبری[1] در مراحل آغازین خود است (بیکر[2]، ۱۹۶۸)؛ مانند نیروی هوایی در سال‌های ۱۹۱۰، ایده‌ها، پایه‌ها و دکترین امروزی درباره‌ی بهترین روش استفاده از این جنگ‌افزار بالقوه در مراحل آغازینش است؛ و به همان شکل که سؤالات دیرین درباره‌ی سودمند

1 . Cyber War
2 . Gary S. Becker

بودن نیروی هوایی به‌عنوان ابزاری در جنگ با آزمون جنگ جهانی اول پاسخ داده شد، به همین شکل یک آزمون واقعی، این بار رویارویی روسیه – گرجستان در سال ۲۰۰۸ بر نقش حمله سایبری در جنگ، صحه نهاد. بحث‌های سال‌های ۱۹۹۰ درباره‌ی اینکه آیا تنها جنگ اطلاعات دفاعی یا تهاجمی قابل‌قبول است در دوره معاصر با تلاش آشکارا و روشن برای توسعه قابلیت‌های تهاجمی و دکترین همراه در جنگ سایبری جایگزین شده است.

یک گستره که در آن جنگ سایبری تفاوت قابل‌توجهی با نیروی هوایی، دریایی و زمینی دارد در داشتن مرزهای طبیعی است. خطوطی را که برای نیروی هوایی، دریایی یا هوایی مرز در نظر گرفته می‌شود به‌آسانی می‌توان جدا کرد، ولی منظور از جنگ سایبری دقیقاً چیست (بلنک[1]، ۲۰۰۱)؟ با استفاده از اصطلاح «جنگ اطلاعاتی» که تنها یک بخش از جنگ سایبری است این لغزش را به‌طور ضمنی مرتکب می‌شویم. اطلاعات نادر است که یکی از دلایل آن جدید بودن اندیشه راهبردی در جنگ سایبری است، دلیل دیگری هم ترکیبی از سازمان‌های نظامی به‌عنوان اندیشمندان راهبردی و پیوند نزدیک بین جنگ سایبری و دارایی‌های اطلاعاتی است، بدان معنی که اطلاعات محدودی در گستره غیر طبقه‌بندی‌شده وجود دارد. آنچه در پی آمده بدون شک تنها قسمت کوچکی از اندیشه راهبردی واقعی معاصر در جنگ سایبری است. جنگ سایبری طبقه یا مجموعه‌ای از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن یکی از طرفین درگیر بر دشمنان خود به مزیتی چشمگیر دست‌یافته و آن را حفظ می‌کند.

هفت شکل مختلف جنگ سایبری به شرح زیر است:

- جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.
- جنگ بر پایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم‌هایی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.

1 . Stephen Blank

- جنگ الکترونیک تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری.
- جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرز فکر دوستان، بی‌طرف‌ها، و دشمنان استفاده می‌شود.
- جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
- جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات باهدف کسب برتری اقتصادی.

در حقیقت جنگ سایبری امروزه ترکیبی از همه موارد فوق است که باعث برتری یکی از طرفین درگیر از جمیع جهات خواهد شد. از سوی دیگر برتری در تکنیک‌های جنگ سایبری موجب بازدارندگی نیز می‌شود. بازدارندگی سنگ بنای تعامل میان دولت‌ها بوده است. این امر به‌ویژه درزمانی که منافع کشورها درگیر شده و رهبران سیاسی به دنبال جلوگیری از درگیری نظامی مستقیم هستند مهم می‌گردد. در روابط سنتی بازدارندگی، محاسبات نظامی، اقتصادی و توان دیپلماسی درجه مؤثر بازدارندگی را تعیین می‌کند. با توجه به تغییر تهدیدات، به‌ویژه تهدیدات سایبری به‌واسطه ارتباطات و فن‌آوری ارتباطات جدیدی که در دسترس داشته قدرت گرفته‌اند، قطعاً رویکردهای بازدارندگی نیز بایستی تغییراتی داشته باشد و با توجه به اینکه تحقیقات معدودی در این حوزه وجود دارد این تحقیق می‌تواند دیدگاه‌ها و پارادایم‌های جدیدی در حوزه جنگ سایبری را نمایان سازد و با توجه به سیاست‌های دفاعی کشور در حوزه‌های مختلف به کار گرفته شود.

مبانی نظری تحقیق

جنگ سایبری

جنگ سایبری، در اینجا، به اقدامات خصمانه در فضای مجازی اشاره دارد؛ که حمله سایبری یا حمله به شبکه‌های کامپیوتری (**CNA**) هم نامیده می‌شود و می‌توان آن را به‌عنوان «استفاده از اقدامات عمدی، شاید برای یک دوره زمان طولانی، برای تغییر، مختل کردن، فریب، کاهش یا از بین بردن دستگاه‌های کامپیوتری دشمن یا شبکه‌ها و یا برنامه‌های مقیم و یا فعال بر روی این

سیستم و یا شبکه تعریف کرد» (بلنک، ۲۰۰۱). اگرچه ساده‌ترین شکل اجرای حمله به شبکه‌های کامپیوتری، از بین بردن کامپیوترهای دشمن است، توجه ما در اینجا بر استفاده از سلاح‌های دیجیتال است و نه حمله نظامی. جنگ سایبری یک عملیات تهاجمی سایبری است که مانند یک عملیات سایبری، هدفش بهره‌برداری از شبکه‌های کامپیوتری است (**CNE**). تمایز **CNE** از **CNA** در این است که کسانی که درگیر یک **CNE** هستند نمی‌خواهند مانع عملکرد طبیعی یک سیستم کامپیوتری شوند، ایده این است که به دست آوردن اطلاعات به‌احتمال‌زیاد یک دوره طولانی می‌طلبد. **CNE** یک فعالیت جاسوسی و یا جمع‌آوری اطلاعات است و در اینجا به‌عنوان بخشی از جنگ سایبری گنجانده نشده است (البته در عمل اینکه یک دولت تشخیص دهد که هدف **CNA** یا **CNE** واقع‌شده است سخت است، چراکه این دو از یک نظرگاه فنی از نزدیک به هم مرتبط‌اند.)

تعریف جنگ سایبری به شکلی که شامل پارامترهای محدود **CNA** باشد خود یک تحول در اندیشه راهبردی درباره‌ی جنگ سایبری است که در دوره پس از پایان جنگ سرد تابه‌حال معانی، عناوین، اشاره‌های جسته‌گریخته و زمینه متعددی داشته است. یکی از اولین تلاش‌ها برای تعریف جنگ سایبری توسط دو محقق رند، جان آرکیلا و دیوید رونفلدت، انجام‌شده است (بلنک، ۲۰۰۱). در یک مقاله از مجله معتبری در ۱۹۹۳ با عنوان «جنگ سایبری درراه است!» اظهار داشتند: جنگ سایبری به رویارویی وابسته به دانش در سطح نظامی اشاره دارد... انجام عملیات نظامی با توجه به پایه‌ها مربوط به اطلاعات... به معنی برهم زدن و از بین بردن دستگاه‌های اطلاعات و ارتباطات است ... این یعنی تلاش برای دانستن همه‌چیز درباره‌ی دشمن درحالی‌که دشمن را از دستیابی به اطلاعات درباره‌ی خود محروم کنیم.

دو نکته از اوایل این بحث مشخص شد. اول، برداشت آرکیلا و رونفلدت از جنگ سایبری تا حد زیادی با ایده‌هایی که پس‌ازآن در سال‌های ۱۹۹۰ به‌عنوان انقلاب در امور نظامی مطرح شد مرتبط است. این اصطلاح «جنگ سایبری» مدنظر آن‌ها، برای بحث درباره‌ی پیامدهای نظامی انقلاب اطلاعات برای جنگ، ازجمله تغییرات فنّاورانه، اعتقادی و سازمانی و همچنین به‌عنوان عبور از

توده به برتری اطلاعاتی استفاده شد. این ایده‌ها که در فصل ٤ با توجه به انقلاب در امور نظامی موردبحث قرار گرفت، موضوع این فصل نیست؛ بنابراین، اگرچه آرکیلا و رونفلدت آغازگر مفهوم جنگ سایبری و دلیل محبوبیت آن بودند، از آن‌ها در اینجا به‌عنوان اندیشمندان راهبردی جنگ سایبری نام‌برده نشده است. مهم‌ترین کمک آن‌ها به فکر راهبردی نظامی (و درواقع گستره اصلی تمرکز آن‌ها) در ایده دیگر آن‌ها یعنی «جنگ شبکه‌ای» است که بر یک حالت نوظهور رویارویی که بازیگران غیردولتی که در آن از فناوری اطلاعات و ارتباطات از فرم سازمان شبکه‌ای، با فعالیت در گروه‌های کوچک در مکان‌های پراکنده ولی به‌هم‌پیوسته استفاده می‌کنند. در یک کتاب بسیار معروف در ۱۹۹٦، شبکه‌ها و جنگ‌های شبکه‌ای، ظهور القاعده و شکل آن را به‌خوبی پیشگویی کردند.

نکته دوم این است که بحث آرکیلا و رونفلدت در رابطه با جنگ سایبری با شمول تخریب دستگاه‌های اطلاعات و ارتباطاتی به مفهوم گسترده‌تر «جنگ اطلاعات» اشاره می‌نماید. به‌عنوان یک عبارت هزار بیشه از سال‌های ۱۹۹۰، محتوای «جنگ اطلاعاتی» اولین بار توسط مارتین لیبیکی به شکلی سازمان‌یافته بررسی شد. در «جنگ اطلاعاتی چیست؟»، یک مطالعه در سال ۱۹۹۵ برای دانشگاه پدافند ملی، لیبیکی هفت شکل جنگ اطلاعات رایج در ادبیات در آن زمان را شناسایی کرد که با در نظر گرفتن همگی، با لیبیکی به این نتیجه می‌رسیم که موارد کمی وجود دارد که نتوان جنگ اطلاعاتی برشمرد. این اشکال شامل فرماندهی و کنترل جنگ در برابر سر و گردن دشمن، چه از طریق حمله نظامی یا **CNA** به اهداف نظامی؛ جنگ مبتنی بر اطلاعات. جنگ الکترونیک؛ جنگ روانی (عملیات روانی)، جنگ هکرها که **CNA** به اهداف غیرنظامی است (باربزا[1]، ۲۰۰۷)؛ جنگ اطلاعاتی اقتصادی؛ و جنگ سایبری که در آن زمان به‌عنوان «یک مجموعه از حالات مربوط به آینده است. همه این چیزها حالت‌های مختلف جنگ یا عملیات اطلاعاتی در نظر گرفته‌شده و عنصر مشترک آن‌ها این بود که اشکالی از جنگ بودند که به نحوی اطلاعات دشمن را تحت تأثیر قرار می‌داد.

1 . David Barboza

برخی بر این باورند حالت‌های جنگ اطلاعاتی شامل از بین بردن دستگاه‌های اطلاعات با استفاده از سلاح‌های اطلاعات خالص، مانند ویروس‌های کامپیوتری است. ولی بسیاری از قطعات «مجموعه» جنگ اطلاعاتی جدید بوده و ربطی به استفاده از بیت‌ها و بایت‌ها به‌عنوان ابزار جنگ نداشت. به‌عنوان‌مثال عملیات روانی و جنگ الکترونیک و فرماندهی و کنترل جنگ که هدف قرار دادن دقیق فیزیکی مراکز فرماندهی خوانده می‌شود که به‌عنوان «بریدن سر» در بحث نیروی هوایی توصیف می‌شود.

در نیمه دوم سال‌های ۱۹۹۰ پنتاگون اصطلاح جنگ اطلاعاتی را به خاطر چیزهایی مانند تبلیغات سیاسی در زمان صلح به نفع عملیات اطلاعات کنار گذاشت. درنتیجه امروزه جنگ سایبری را بیشتر می‌توان در یک طرح گسترده‌تر از «عملیات اطلاعات» یافت اگرچه محتوای آن با جنگ اطلاعات تفاوت کمی دارد. انتشارات مشترک عملیات اطلاعاتی ارتش ایالات‌متحده، چنین عملیاتی را به نام اشتغال یکپارچه جنگ الکترونیک، عملیات شبکه‌های کامپیوتری و عملیات روانی برای تأثیرگذاری، مختل کردن و تخریب اطلاعات و نظام‌های اطلاعات دشمن در حین پدافند در برابر امکانات خود تعریف می‌کند. بخش‌هایی از ارتش آمریکا هنوز حمله نظامی را در طرح کلی به‌حساب می‌آورند. برای مثال فرماندهی آموزش و دکترین ارتش ایالات‌متحده، حمله سایبری را شامل **CNA**، حمله الکترونیکی و حمله نظامی می‌پندارد. ارتش نیز اصطلاح «جنگ شبکه‌ای» را به استفاده از **CNA**، حمله الکترونیکی و حمله نظامی اختصاص می‌دهد.

باوجود اصل سازمان دهنده تحت تأثیر قرار دادن اطلاعات دشمن، اجزای مختلف عملیات اطلاعاتی مسلماً به‌ندرت به‌عنوان یک گروه واحد عملیاتی در نظر گرفته می‌شوند. بسیاری از جنبه‌های گوناگون آن خودبه‌خود می‌تواند به‌عنوان یک‌رشته جداگانه عمل کنند (بلنک، ۲۰۰۱). افزون بر آن این، همان‌طور که لیبیکی اشاره می‌کند، «پوشش، تعمیر کلی، هکرهای کامپیوتری و متخصصان الکترومغناطیس، عاملان رادار هوابرد، بروشورانداز‌ها، بمب‌افکن‌ها و تیراندازان یک چالش نظری خطیر است ". دراین‌بین هدف ما تغییر، اخلال، فریب، تخریب، یا از بین بردن دستگاه‌های کامپیوتری دشمن و یا شبکه‌های مورداستفاده توسط حمله دیجیتال خصمانه است.

پارامترهای شمول آنچه جنگ سایبری به‌حساب می‌آید لزوماً به **CNA** محدود است تا به نحوی منسجم گستره تحقیق ما نسبت به گستره‌های دیگر جنگی شناسایی شود.

جواز جنگ سایبری

اگرچه انواع متعددی عملیات تحت لوای گسترده‌تر جنگ اطلاعاتی / عملیات اطلاعاتی گنجانده می‌شود، در سال‌های ۱۹۹۰ حین بحث بر جواز جنگ اطلاعاتی، به‌طور ضمنی و همواره منظور یک نوع خاص از عملیات بود (بلنک، ۲۰۰۱): حملات کامپیوتری در برابر دستگاه‌های کامپیوتری. تا اواخر ۱۹۹۸ جنگ اطلاعاتی تهاجمی، به معنی **CNA**، در بحث‌های عمومی تابو شمرده می‌شد. در سال ۱۹۹۸ پنتاگون نیروی مأموریت مشترک برای پدافند در برابر شبکه کامپیوتری را تأسیس کرد (کارترایت۱، ۲۰۰۷) و دستور آن حفاظت از شبکه‌های کامپیوتری پنتاگون بود و در سال ۲۰۰۰ به این نیرو یک مأموریت تهاجمی نیز اختصاص داده شد. چند سال بعد، این سازمان به دو قسمت تقسیم شد که تمرکز بخش‌هایش تهاجمی و دفاعی بود. بنا به گزارش بخشنامه امنیت ملی دولت آمریکا در سال ۲۰۰۲ ریاست جمهوری دستور به توسعه دستورالعمل حملات سایبری علیه دستگاه‌های کامپیوتری دشمن داده است.

بااین‌حال در اواخر این دهه و شاید با حملات سایبری علیه استونی در سال ۲۰۰۷ و گرجستان در سال ۲۰۰۸ ، تمام بهانه‌ها برای یک گرایش عمدتاً دفاعی صرف از بین رفته بود. در سال ۲۰۱۰ فرماندهی سایبر آمریکا به‌عنوان یک زیر فرماندهی تحت فرماندهی راهبردی ایالات‌متحده تشکیل شد. فرماندهی دوباره مأموریت‌های سایبری دفاعی و تهاجمی را متحد کرد و به‌صراحت نه‌تنها به پدافند بلکه، با دستور رئیس‌جمهور، اجازه حمله به دشمنان را دارا بود. گزینه جنگ سایبری تهاجمی آمریکا می‌تواند شامل نفوذ سایبری "با شدت کم " مانند شنود محدوده «ارتباطات دشمن» تا حمله "با شدت بالا " برای فلج کردن سیستم پدافند هوایی دشمن برای باز کردن راه برای یک بمباران است.

1 . James E. Cartwright

در همین حال ناتو به‌عنوان یک سازمان خود را، حداقل رسماً، بر پدافند در برابر شبکه‌های رایانه‌ای تمرکز کرده است. مفهوم راهبردی ۲۰۱۰ آن می‌گوید؛ بعد سایبر از منازعات مدرن در دکترین ناتو قرار دارد ولی در قالب بهبود قابلیت‌های تشخیص، ارزیابی، جلوگیری از انجام آن و بازیابی در صورت یک حمله سایبری خواهد بود. در سال ۲۰۱۱ رهبری تحول فرماندهی متحدین ناتو رویکرد دفاعی ناتو را تأیید کرد.

در مقابل تغییر تدریجی در تأکید امریکا و ناتو بر موضعشان، به نظر می‌رسد چین در اواخر سال‌های ۱۹۹۰ تصمیم خود را برای توسعه قابلیت جنگ اطلاعاتی تهاجمی گرفته باشد. جنگ ۱۹۹۱ خلیج فارس نشان داد که برای یک دولت مقابله مستقیم در میدان نبرد متعارف با ایالات‌متحده ممکن نیست، درحالی‌که در بحران سال ۱۹۹٦ تایوان به چین نشان داد که نیاز بالقوه‌ای برای مقابله با ایالات‌متحده در آینده خواهد داشت. برای رسیدن به چنین توانی، چین بر رویکردهای "نامتقارن " تمرکز کرد که نقاط ضعف و آسیب‌پذیری آمریکا را هدف قرار داد. (سی. اس. آی. اس[1]، ۲۰۰۸). اقدام نسبی چین در این گستره، در تضاد با روسیه است؛ که جنگ سایبری را بدون اقرار به اندیشه راهبردی در این گستره تمرین می‌کند (به‌ویژه در گرجستان).

تفاوت جنگ سایبر با سایر گستره‌های جنگ

شاید قابل‌توجه‌ترین مشخصه بین ابعاد سایبری و دیگر گستره‌های جنگ (دریا، زمین، هوا و فضا) این است که یک گستره برای فتح کردن وجود ندارد. فضای مجازی یک ساختار تکراری است و تکراری بودن آن، باعث شده هم‌زمان در مکان‌های مختلف وجود داشته باشد. هر سیستم و هر شبکه می‌تواند تعداد نامحدودی فضا دربر داشته باشد. افزون بر آن این، فضای مجازی در مقایسه با گستره‌های دیگر یک‌چشم‌انداز بسیار متغیر است. بخش‌هایی از فضای مجازی به‌طور مستمر با نوآوری در فن‌آوری و افزون بر آن این، حذف، جایگزینی و یا پیکربندی مجدد شبکه تغییر، تحول و گسترش می‌یابد. حتی اگر تنها به یک فضای مجازی مفهومی بنگریم، بازمی‌بینیم که حتی از این دید هم طبیعتان منحصربه‌فرد است (کارترایت، ۲۰۰۷)، زیرا با فقدان کامل مرزها مشخص می‌شود.

1. Commission on Cybersecurity

برخلاف جنگ‌افزار فیزیکی، حمله به شبکه کامپیوتری می‌تواند در سراسر جهان و با سرعت نور انجام شود، نامرئی از بسیاری مرزهای بین‌المللی گذشته تا به هدف خود برسد. ماهیت لحظه‌ای جنگ سایبری و توانایی حمله به‌کل دامنه به‌طور هم‌زمان از ویژگی‌هایی است که باعث شده ابعاد سایبری جنگ به‌خصوص بالقوه خطرناک باشند. ویژگی جنگ سایبری با توجه به این واقعیت که، برخلاف انواع دیگر فیزیکی آن، استفاده از یک حمله از جنگ‌افزار سایبری پتانسیل یک تخریب گسترده، با آسیب گسترده را دارد (کافمن[1]، ۱۹۹۸). در مقیاس بزرگ حمله سایبری می‌تواند عملکرد جامعه را مختل کرده و منجر به تلفات غیرمستقیم شود. درنتیجه جنگ‌افزار سایبری، یک‌گونه کاملاً جدید در نوع خود است.

هدف از جنگ سایبری

این واقعیت که فضای مجازی یک ساختار قابل تکرار است بدان معنی است که هدف عملیاتی جنگ سایبری از بین بردن توانمندی‌های سایبری نیست که مانند یک نیروی زمینی به دنبال نابود کردن نیروهای زمینی دشمن باشد. "درحالی‌که مفهومی همانند به فتح را می‌تواند برای فضای مجازی تعریف کرد، خود فضای مجازی را نمی‌توان در معنای متعارف فتح کرد" (فاینارو و گریمالدی[2]، ۲۰۰۱). آسیب رساندن دائمی به یک سیستم از طریق **CNA** یک گزینه نیست. جنگجوی سایبری به دنبال اهداف دیگری است. هدف آنی ممکن است کور کردن حریف با ایجاد سروصدای بالا در اطراف سیگنال اطلاعات سودمند برای از دست رفتن آن؛ مختل کردن دسترسی به داده‌ها؛ تخریب اطلاعات با اضافه کردن بیت نادرست به آن، درنتیجه فریب حریف و، یا به‌اشتباه انداختن و یا گمراهی حریف با تضعیف اعتبار اطلاعات؛ به سرقت بردن اطلاعات؛ و دست‌کاری در دستگاه‌های حریف با تغیر آن‌ها برای انجام چیزی غیر ازآنچه موردنظر طراحان آن باشد. یک تم غالب در ادبیات ایالات‌متحده آمریکا ممانعت از آزادی عمل دشمن است (کول[3]، ۲۰۰۹). اصل اثر صحبت از جنگ سایبر ممانعت از آزادی عمل دشمن در فضای مجازی است.

1 . William Kaufmann
2 . Steve Fainaru and James V. Grimaldi
3 . Dan Kuehl

درنهایت، هدف راهبردی جنگ سایبری تهاجمی ممکن است وادار کردن حریف، نشان دادن توان و یا "درس دادن به کشورهای دیگر،" غیرفعال کردن قابلیت دشمن و یا حمایت از عناصر سرویس دیگری برای برتری در رویارویی باشد (سی. اس. آی. اس، ۲۰۰۸). جنگ سایبری در اصل یک‌شکل پشتیبانی از جنگ است. پیام ضمنی در این بحث از ویژگی‌های جنگ سایبری این است که تنها در جنگ علیه عناصری با شبکه‌های کامپیوتری نسبتاً گسترده سودمند است (سی. اس. آی. اس، ۲۰۰۸). به همین دلیل جنگ سایبری به‌ویژه به جنگ یک دولت با دولت دیگر مربوط است. حملات سایبری درباره‌ی فریب هستند و جوهر فریب در آنچه شما انتظار دارید و آنچه واقعی است تجلی می یابد: غافلگیری، جنگ سایبری برای حمله غافلگیرانه ساخته‌شده، برای یک حمله غیرمنتظره.

مقایسه سه کشور چین، روسیه و آمریکا

فکر راهبردی در جنگ سایبری مدتی است در بین ارتش آزادی‌بخش خلق (PLA) جریان دارد. ازلحاظ تاریخی، رویکرد جنگی چین "پدافند فعال " است که به معنی این است کشور یک حمله را آغاز نمی‌کند ولی آماده به پاسخ به هر حمله خواهد بود (فاینارو و گریمالدی، ۲۰۰۱). در عصر اطلاعات این به جنگ با رویکرد تهاجم فعال تغییر کرده است. دیدگاه این است که کلید عملیات مؤثر سایبری در دست گرفتن ابتکار عمل، شروع تهاجم سایبری و حتی عمل پیشگیرانه است.

نیروی نظامی چین یک استراتژی به نام شبکه یکپارچه جنگ الکترونیک برای هدایت اشتغال ترکیبی ابزار جنگ شبکه‌ای (بیت) و سلاح‌های جنگ الکترونیک (امواج) را در برابر دستگاه‌های اطلاعات دشمن توسعه داده است. این استراتژی به چند امتیاز در پایه‌های جنگ سایبری اشاره دارد. استدلال شده که حمله سایبری، باید در مراحل اولیه و یا آغاز یک رویارویی استفاده شود. ایده این است که از کوری موقت دشمن بهره برد تا یک سری از حملات متعارف انجام داد، یعنی حملات فیزیکی، بر روی پلتفرم و کارکنان. هدف رویکرد سایبری، در این روش یکپارچه جنگی به‌طور خاص C4ISR دشمن (فرمان، کنترل، ارتباطات، کامپیوتر، هوش، نظارت و شناسایی) و

دستگاه‌های تدارکات شبکه به‌عنوان بالاترین اولویت برای جنگ اطلاعاتی شناسایی می‌شود (کارترایت، ۲۰۰۷). حمله به دستگاه‌های اطلاعات دشمن، برای سرکوب کامل شبکه‌های انتقال و حس‌گرها نیست ... [بلکه] تنها آن دسته از گره‌هایی که برنامه ریزان PLA های جنگ اطلاعاتی به‌عنوان چیزهایی که تصمیم‌گیری، عملیات و روحیه دشمن را به بهترین شکل هدف قرار می‌دهند ارزیابی کرده‌اند. درنتیجه روش PLA ذاتاً کیفی و مبتنی براثرات است. در جهت ممانعت از داشتن آزادی عمل حریف در فضای مجازی، چین به دنبال سلطه اطلاعاتی یا برتری با حمله به زیرساخت‌های C4ISR دشمن برای جلوگیری و یا اخلال در اکتساب، پردازش و یا انتقال اطلاعات در پشتیبانی عملیات رزم است (دنینگ[1]، ۲۰۰۱). درنهایت، PLA موارد نیاز برای حملات هماهنگ و یا هم‌زمان به شبکه‌ها و دستگاه‌ها دشمن را شناسایی کرده و به عملیات خاموش و یا غیرقابل تشخیص برای سرقت و یا دست‌کاری اطلاعات ارزش می‌نهد.

جامعه نظامی ایالات‌متحده. ادبیات علمی آمریکا در جنگ سایبری نشان می‌دهد که حداقل ۱۳ سند دکترین مختلف در سطح معاونت پدافند، وزارت پدافند، نیروی دریایی، ارتش، نیروی هوایی و فرماندهی راهبردی (STRATCOM) چگونگی مبارزه امریکا در یک جنگ سایبری را نشان خواهد داد. باوجوداین، این اطلاعات درباره‌ی رفتار امریکا در جنگ در گستره سایبری نسبتاً محدود است. کیفیت یک CNA از توانایی فریب، غلبه و یا دور زدن پدافند مشتق شده است، درحالی‌که کیفیت دفاعی در توانایی پیش‌بینی روش تهاجم دشمن است. هنگامی فن‌های تهاجمی یا دفاعی شناخته شد، در مدت‌زمان نسبتاً کوتاهی روش‌های تهاجمی و دفاعی مربوطه دشمن می تواند مهندسی شود. شناسایی اندیشه راهبردی ایالات‌متحده با توجه به اداره جنگ در بعد سایبری ممکن است. موضوع اصلی در ادبیات نظامی آمریکا لزوم تهاجم است. برخلاف گستره‌های دیگر که در آن در طول تاریخ پرسش‌هایی درباره تهاجم یا پدافند غالب شود ایجاد می‌شود، در گستره سایبری پرسش به پاسخ مبنی بر حمایت از تهاجم انجامید (فاینارو و گریمالدی، ۲۰۰۱). متحدان آمریکا اشاره‌کرده‌اند که جنگ سایبری بیشتر به نفع مهاجم است تا مدافع. اگرچه تم تهاجمی تم

1 . Dorothy Denning

غالب در ادبیات آمریکا است، این بدان معنا نیست که پدافند در اندیشه راهبردی درباره‌ی این دامنه جنگ تأثیر ندارد. مفهوم پدافند شایع است، ولی در یک ساختار عامل و نه غیرعامل ارائه‌شده است (دنینگ، ۲۰۰۱). در امتداد این خطوط، تحلیلگران دفاعی ایالات‌متحده تأکید کرده‌اند که پدافند در برابر شبکه‌های رایانه‌ای چیزی بیش از تر از ساختن دیوار آتش و نرم‌افزار آنتی‌ویروس است. همچنین این شامل یافتن تهدیدات قبل از انجام آن‌ها است و شاید این امکان را می‌دهد که ارتش ایالات‌متحده از دستگاه‌های سایبری **CNA** برای رسیدن به دشمن و پاسخ سایبری استفاده کند. شورای تحقیقات ملی آمریکا موافق است که پدافند غیرعامل برای اطمینان از امنیت کافی نیست و اجازه دادن به دشمن به انجام حمله و عدم مجازات آن تا موفق شدنش یا توقف خودخواسته عقلانی نیست. رهبران نظامی ایالات‌متحده بر نیاز به سرعت در انجام جنگ سایبری تأکید دارند. در جنگ، سرعت عملیاتی یک منبع قدرت مبارزه است. بخشی از این سرعت شامل استفاده از جریان اطلاعات برای به دست آوردن و حفظ ابتکار عمل و عمل درون چرخه تصمیم دشمن است. فراتر از این، جنگ سایبری یک مانور جنگی است که در آن سرعت و چابکی مهم‌ترین اصل است، درحالی‌که متحدان آمریکا توجه خود را به‌سرعت، غافل‌گیری و صرفه‌جویی نیرو به‌عنوان ویژگی‌های مربوط به جنگ سایبری معطوف کرده‌اند (اسپینر[1]، ۲۰۰۸). ناظران هشدار داده‌اند که سرعتی که با حملات الکترونیکی را می‌توان انجام داد " زمان کمی برای برخورد با خونسردی" باقی می‌گذارد و حمله پیشگیرانه را ترجیح می‌دهد. تم غالب یک رویکرد ساکت و پنهانی است. یک موسسه امنیت سایبری استدلال کرده است: " هک کردن پرسروصدا است. در حال حاضر، هدف مسکوت ماندن است ". برخی استدلال می‌کنند بهترین رویکرد برای جنگ سایبری نفوذ به کامپیوتر و شبکه دشمن، جاسوسی از آن‌ها و تغییر مخفیانه ارتباطات آن‌ها بدون آگاهی‌شان است. دکترین فعلی ایالات‌متحده درباره‌ی پیامدها یک حمله سایبری به آن‌که یک حمله مسلحانه تلقی شود مشخص نیست. برخی پیشنهاد کرده‌اند با استفاده از نیروهای مسلح متعارف به

1 . Tom Espiner

آن پاسخ داد. برخی هم بر این باورند باید از طریق ابزارهای سایبری به آن پاسخ داد (هریس[1]، ۲۰۰۸).

روسیه. کسی نمی‌تواند بدنه اندیشه راهبردی روسیه در جنگ سایبری را مشخص کند. بااین‌حال، بیرون کشیدن عناصر چشم‌انداز آن‌ها درباره‌ی جنگ را می‌توان به با نگاه به جنگ کوتاه روسیه با گرجستان در اوت ۲۰۰۸ که گفته می‌شد طی آن حملات سایبری علیه گرجستان بوده مشاهده کرد (هاندلی و اندرسن[2]، ۲۰۰۹). تحلیلگران اشاره می‌کنند که یک جنگ تاریخی و بی‌سابقه بود، زیرا برای اولین بار یک حمله در دامنه فضای مجازی هماهنگ با جنگ متعارف انجام شد. که توجه ما را به چند پایه بالقوه برای رفتار در جنگ سایبری آینده، ازجمله مفهوم حملات موازی و یا هم‌زمان توسط نیروهای فیزیکی و سایبری جلب می‌کند. در سطح عملیاتی و تاکتیکی جنگ، نیروهای گفته‌شده مجازی روسیه از نزدیک با گستره‌های زمین، دریا و هوا هماهنگ بوده تا به نتیجه موردنظر برسند. روسیه همچنین اقدام به شناسایی مرکز گرانش سایبری دولت گرجستان کرد، در این مورد توانایی‌ها برای برقراری ارتباط با جهان خارج بسیار دشوار شد. هکرهای وطن‌پرست روسیه در هفته‌های منتهی به جنگ واقعی به دستگاه‌های گرجستان نفوذ کرده و با تأکید بر ارزش عملیات آماده‌سازی – ازجمله فعالیت‌های شناسایی و کاوش – در پشتیبانی واقعی از یک عملیات نظامی سنتی پیش از هر حمله به شبکه انجام دادند. این واقعیت است که هکرها گرجستان را هدف قرار گرفتند یک عنصر مهم در رفتار جنگ سایبری است یعنی ایده مختل کردن، کاهش و حتی حذف قابلیت تلافی‌جویانه را تقویت می‌کند. بر اساس جنگ گرجستان روسیه – به‌عنوان‌مثال، تحلیلگران استدلال می‌کنند که هکرهای وطن‌پرست در آینده از همسنگ فضای مجازی آتش و مانور در حمایت مستقیم از جنگ در گستره‌های دیگر استفاده خواهند کرد.

1 . Shane Harris
2 . Richard O. Hundley and Robert H. Anderson

پارادوکس‌های جنگ سایبری

آستانه‌ها: ظهور جنگ در گستره سایبری تعدادی سؤال مرتبط با جنگ مطرح کرده است. اول و اساسی‌ترین سؤال این است که آیا جنگ سایبری را می‌توان یک جنگ در نظر گرفت؟ تعریف جنگ به‌عنوان یک رویارویی به‌زور اسلحه بین ملت‌ها و یا بین طرفین در یک کشور برای جنگ سایبری مشکل‌ساز است (فاینارو و گریمالدی، ۲۰۰۱). این سؤال که چه زمانی فعالیت تهاجمی در فضای مجازی به یک اقدام جنگی تبدیل می‌شود یک سؤال بسیار مهم است (هلمز[1]، ۲۰۰۹)؛ زیرا، طبق قوانین بین‌المللی، ماده ۵۱ منشور سازمان ملل متحد،" اگر یک حمله مسلحانه رخ دهد " استفاده از زور در پدافند در برابر خود (سایبری و یا فیزیکی) مجاز هست. افزون بر آن این، اگر حمله مسلحانه قریب‌الوقوع بوده ولی هنوز رخ نداده باشد فعالیت پیشگیرانه نظامی، پدافند در برابر خود پیش‌بینی‌شده و مجاز است. دانشمندان آمریکایی تأکید می‌کنند که در ارزیابی پاسخ به یک تهدید سایبری، ایالات‌متحده نباید تمایزی بین روش‌های حمله سایبری و ابزار فیزیکی قائل گردد، بلکه تمرکز باید براثرات آن باشد. با نگاهی به اثرات، بسیاری ازآنچه است که یک حمله سایبری یا جنگ سایبری نامیده می‌شود در گستره‌های دیگر یک حمله به‌حساب نمی‌آید. رخنه‌ها ذاتاً هک، جاسوسی، یا مجرمانه‌اند و بیشتر یک محرک به‌حساب می‌آیند تا اقدام جنگی (هارت[2]، ۲۰۰۸). دانشمندان حقوق استدلال کرده‌اند تمایز بین یک عمل مجرمانه و یک اقدام جنگی در فضای مجازی با در نظر گرفتن اثرات همسنگ در فضای مجازی به یک حمله مسلحانه قابل‌تعریف است. از این منظر، آستانه برای جنگ و یا حمله نباید خیلی با جنگ در یک محیط فیزیکی متفاوت باشد. قریب‌الوقوع بودن: این چارچوب به‌ظاهر ساده با عوامل اضافی مانند قریب‌الوقوع بودن که تعیین آن در هر جنگ غیرمتعارف دشوار است پیچیده شده و در جنگ سایبری چالش بزرگ‌تری هم هست (هاساوی[3]، ۲۰۰۸). چگونه تعیین می‌کنید که یک حمله قریب‌الوقوع است؟ درجه قطعیت لازم قبل از اجازه پاسخ چقدر است؟ (اسپینر، ۲۰۰۸).

1 . Erik Holmes
2 . Kim Hart
3 . Melissa E. Hathaway

نسبت دادن: حتی اگر تلقی شود که یک حمله مسلحانه صورت گرفته است یا به‌زودی انجام خواهد شد، پاسخ توسط نسبت دادن آن در جهان سایبری پیچیده می‌شود. تاکنون درباره حملات روسیه در استونی ادعاهایی مطرح کردیم زیرا هویت مهاجمان همچنان نامشخص است. نسبت دادن حمله در مفهوم بازدارندگی برای جنگ سایبری یک مشکل اساسی است (اسپینر، ۲۰۰۸).

سودمندی: سؤالاتی نیز درباره‌ی ابزار حمله سایبری به‌عنوان یک ابزار جنگی مطرح‌شده است. پیامدهای حمله سایبری بیشتر همانند ویرانگری به دست چریک‌ها یا نیروهای عملیات ویژه است تا جنگ در گستره دریا، زمین، یا هوا. افزون بر آن، افزونگی دستگاه‌هایی که زیرساخت‌های اساسی را کنترل می‌کنند به این معنی است که درجه‌ای که آن‌ها در معرض خطر هستند ممکن است اغراق‌آمیز توصیف‌شده باشد (گوناراتنا[1]، ۲۰۰۲). قضاوت در این زمینه بر عهده زمان خواهد بود که مشخص کند درجه واقعی یک تهدید سایبری چقدر است. بدیهی است استفاده از حمله سایبری در جنگ روسیه – گرجستان ویروس استاکس نت، نشان می‌دهد جنگ سایبری، یک جنگ‌افزار تهاجمی بالقوه در آینده است.

غیرقابل‌پیش‌بینی بودن: درنهایت، حتی اگر سودمندی جنگ سایبری به‌عنوان یک ابزار مؤثر در جنگ ثابت شود، برنامه ریزان ممکن است به دلیل ماهیت غیرقابل‌پیش‌بینی شونده آن تمایلی به راه انداختن جنگ سایبری نداشته باشند. در حمله یک موشک کروز به مرکز کنترل دشمن می‌توان با اطمینان گفت که امکانات دیگر در گوشه و یا کنار جهان ناشی از آن موشک منفجر نخواهد شد. ولی پیش‌بینی اثرات یک **CNA** بر مجموعه‌ای از دستگاه‌های کامپیوتری می‌تواند به‌مراتب بیشتر باشد (گیتس[2]، ۲۰۰۸). اثرات سلاح‌های سایبری ذاتاً جهانی است و نمی‌توان لزوماً به یک محدوده جغرافیایی مشخص محدود کرد. پتانسیل آسیب و اثرات ناخواسته به غیرنظامیان داشته، پس استفاده از حمله سایبری خطرناک است. یک نظامی ارشد آمریکا اشاره می‌کند که در استفاده از سلاح‌های نظامی، باید زمان و مکان تأثیر قابل پیش‌بینی باشد (اسپینر، ۲۰۰۸).

1 . Rohan Gunaratna
2 . Robert Gates

بازدارندگی سایبری

انجام عملیات سایبر توسط بازیگران دولتی و بازیگران غیردولتی به‌شدت افزایش‌یافته است. توانایی ملت‌ها در اعمال اصول بازدارندگی به فعالیت‌های سایبری در تلاش برای دفاع از شبکه و زیرساخت‌های خود اهمیت بالایی دارد. بازدارندگی سایبری انعطاف‌پذیری و گزینه‌های بسیار بیشتری از روش‌های بازدارندگی سنتی توسعه‌یافته در عصر جنگ سرد هسته‌ای را دربرمی‌گیرد (فاینارو و گریمالدی، ۲۰۰۱). علاوه بر انتقام نظامی، بازدارندگی سایبری گزینه‌هایی مانند مجهز کردن، ایجاد شبکه‌های ارتباطی غیر قابل ردگیری، اطلاعات قابل بازیابی در کوتاه ترین زمان و حتی در زمان حمله بدافزارها و مجموعه های وابسته را شامل می‌شود. در میان نگران‌کننده‌ترین انواع هک، حوادث متمرکز بر زیرساخت‌های ملی قرار دارد (اسپینر، ۲۰۰۸). به رسمیت شناختن نقش و اهمیت بازدارندگی عملیات سایبری مخرب، مفاهیم سنتی بازدارندگی را با این خطر مدرن برای امنیت ملی تلفیق می‌کند. بازدارندگی از یونان باستان بخشی از رهنامه امنیتی سیاسی بوده است و در جهان هسته‌ای پس از جنگ جهانی دوم نقش بسیار کلیدی ایفا کرده است (هرزاگ[1]، ۱۹۸۲). درواقع، درعین‌حال که عملیات سایبری به‌عنوان ابزاری برای دستیابی به اهداف ملی قابلیت‌های منحصربه‌فردی دارند، جنبه‌های متمایزی از بازدارندگی کنونی را که نیازمند به‌کارگیری هردوی مفاهیم سنتی بازدارندگی و نیز برخی از روش‌های نوآورانه و مترقی بازدارندگی را در برمی‌گیرد. با توسعه عملیات سایبری مدرن، دولت‌ها و همچنین دانشگاهیان و متخصصان، توجه خود را بر بازدارندگی سایبری متمرکز کرده‌اند (شولسکی[2]، ۲۰۰۹). ماهیت عملیات سایبری باعث شده است که نقش بالقوه بازدارندگی تا حدی کاهش یابد. گمنامی، دسترسی جهانی، ماهیت پراکنده و پیوستگی شبکه‌های اطلاعات تا حد زیادی اثر بازدارندگی سایبری را کاهش داده و حتی می‌تواند آن را کاملاً بی‌فایده کند. باوجوداین، بازدارندگی سایبری همچنان اهمیت خود را با آسیب‌پذیری کشورها و دستگاه‌های سایبری بخش خصوصی حفظ کرده است.

1 . Chaim Herzog
2 . Abram N. Shulsky

یک طیف کامل از بازدارندگی نیاز است؛ حداقل در دوسطح: فرض اولیه این است که بازدارندگی سایبری در طیف بسیار وسیع‌تری از سلاح‌ها و بازیگران دیگر و قطعاً از بحث بازدارندگی هسته‌ای پس از جنگ جهانی دوم موردنیاز است، عملیات سایبری ذاتاً با بسیاری از سلاح‌های دیگر که از خشونت در سطح دولتی بهره می‌برند متفاوت‌اند، زیرا آن‌ها در دسترس طیف گسترده‌ای از بازیگران هستند. برای مثال، فقط چند کشور قابلیت هسته‌ای دارند (لیک[1]، ۲۰۰۸). از سوی دیگر، گزارش‌شده بیش از ۱۴۰ کشور درحال‌توسعه سلاح‌های سایبری بوده و بیش از سی کشور در حال ایجاد واحد سایبری در ارتش خود هستند. (لمونیک[2]، ۱۹۸۹). کارشناسان روسی بر این باورند که در حال حاضر جنایتکاران و تروریست‌ها بزرگ‌ترین تهدید برای امنیت فضای مجازی فراملی است (سی. اس. آی. اس، ۲۰۰۸). علاوه بر این، عملیات سایبری اجازه می‌دهد دشمن به یک طیف گسترده‌ای از اثرات دست یابد. این به این معنی است که نظریه بازدارندگی سایبری باید یک طیف بسیار بزرگ‌تر از دشمنان بالقوه را در نظر گرفته و از انواع بسیار متنوع‌تری از بازیگران با روش‌های تازه جلوگیری کند.

این طیف از حملات احتمالی و مهاجمان باعث می‌شود بازدارندگی حداقل در دو سطح در نظر گرفته شود: عام و خاص (ترینر[3]، ۲۰۰۸). بازدارندگی عمومی برای اعمال گسترده و پیش از هرگونه حمله بالقوه طراحی می‌شود. به‌عنوان‌مثال، داشتن یک زرادخانه هسته‌ای است که می‌تواند در پاسخ به انواع حملات مختلف استفاده شود یک عامل بازدارنده با ابعاد کلی است. در قلمرو سایبری، اقدامات خاصی، مانند نصب یک فایروال، مانند یک عامل بازدارنده عمومی برای همه بازیگران است. بازدارندگی با هدف و دشمن مشخص و یا آنچه در حال حاضر به نام «بازدارندگی در سطوح بالا» شناخته‌شده، برای جلوگیری از یک نوع خاص عملیات سایبری، یک بازیگر خاص و یا هر دو مؤثر است. در قلمرو سایبری، این شاید شامل مسدود کردن ترافیک اینترنتی کامل از یک سرور خاص و یا حامل یک نوع فایل خاص است. ازآنجاکه یک ملت باید شبکه‌های خود را

1 . Eli Lake
2 . Michael D. Lemonick
3 . Ian Traynor

در برابر همه دشمنان بالقوه با تمام قابلیت‌های بالقوه امن کند، بازدارندگی برای اینکه واقعاً مؤثر باشد باید در هر دو سطح به کار رود. درنتیجه بازدارندگی باید انواع ذی نفعان و عاملان حملات، انواع ساده حمله سایبری و یا سازماندهی شده در سطوح جاسوسی، ترور و امنیت ملی و ابعاد حمله را پوشش دهد.

ناکارآمدی تضمین‌شده: فرض دیگر در مورد بازدارندگی سایبری این است که فارغ از تلاش‌ها، بازدارندگی هرگز به‌طور کامل مؤثر نخواهد بود (اسپینر، ۲۰۰۸). این امر نه‌تنها ازنظر فنی، بلکه از دیدگاه جامعه‌شناختی است. برخی از گزینه‌های که برخی از دشمنان بالقوه را بازمی‌دارد، به برخی انگیزه می‌دهد و برخی از بازیگران هم قابل منصرف شدن نیستند. در حوزه سایبری، نه‌تنها بسیار دشوار است که تعیین کرد حادثه سایبر کجا آغازشده، بلکه «کلاه‌برداری» در فعالیت سایبری وانمود می‌کند که رویداد کار شخص دیگری بوده است. این جنبه ذاتی عملیات سایبری اجازه می‌دهد یک‌نهاد یک عملیات سایبری بزرگ بر روی یک هدف انجام دهد و سپس آن را به شکل عملیات توسط یک‌نهاد سوم نشان دهد. ملت هدف، در تلاش برای پاسخ و جلوگیری، شاید یک حمله سایبری یا فیزیکی ویرانگر به نهاد سوم انجام دهد. یکی از جنبه‌های نهایی در فرض ناکارآمدی بازدارندگی سایبری این است که برخی دارندگان قابلیت‌های سایبری هرگز قابل منصرف شدن نیستند (فرناندز[1]، ۲۰۰۸). کشورهای سرکش، تروریست‌ها یک مثال آشکارند.

توانایی تشخیص هویت مهاجمان و رهبران احتمالی حملات: یکی از آزاردهنده‌ترین مشکلات مرتبط با عملیات سایبری این روند نسبت‌دهی است. این مشکل در گزارش‌ها و نوشته‌های متعدد مشخص‌شده است؛ که درباره توانایی یک قربانی برای شناسایی «مهاجم است. با توجه به ماهیت اینترنت، همراه با پیچیدگی بسیاری از مهاجمان، بسیاری از حوادث سایبری مهم هنوز به کسی نسبت داده نشده‌اند. درنهایت، حتی با شناسایی رایانه‌ای تولیدکننده عملیات سایبری سندی برای تعیین مجرم نداریم مگر اینکه راهی برای شناسایی کاربر آن بیابیم. پس ناتوانی در نسبت سریع

1 . Manny Fernandez

عملیات سایبری موانع قانونی قابل‌توجهی سر راه بازدارندگی مؤثر ایجاد می‌کند. تا زمانی که قربانی نداند که چه کسی به دستگاه‌های رایانه‌ای حمله کرده، بازداری او سخت خواهد بود.

با توجه به این مشکلات، دو عامل مهم دیگر در مورد بازدارندگی باید در نظر گرفته شود. اول، باوجوداین واقعیت که بسیاری از حملات نسبت داده نشده باقی می‌مانند، باگذشت زمان و منابع کافی، بسیاری از حملات را می‌توان با درجه‌ای از اطمینان به یک بازیگر نسبت داد. درواقع، بسیاری اکنون استدلال می‌کنند که موضوع واقعی نسبت‌دهی نیست، بلکه نسبت‌دهی «فوری» است. دوم، نسبت دادن به شکل «یا این/ یا آن» نیست. درواقع، بیشتر شبیه به یک طیف است که در آن باگذشت زمان یک قربانی از هویت مهاجم مطمئن‌تر می‌شود. تصمیم سیاسی برای ملت قربانی این‌گونه است که چقدر اسناد برای انجام عملی انتقام‌جویانه موردنیاز است.

تقویت ساز و برگ سایبری و ایجاد رعب در متجاوزان احتمالی: در طول تاریخ بازدارندگی، توانایی علامت‌دهی به دشمنان، یکی از اصول اساسی در هر دو زمان جنگ و زمان صلح بوده است (بتس[1]، ۱۹۸۲). اول، به دلیل دشواری انتساب و استتار عملیات اعلام آشکار توانمندی‌های سایبری به‌ندرت سودمند دیده می‌شود. ازآنجاکه بی‌نشان بودن در اینترنت حتی پس از یک عملیات سایبری زیاد است، انگیزه‌ها برای اعلام قابلیت یا نیت کم هستند (کمپبل[2]، ۱۹۹۸). استفاده از سلاح‌ها باعث شناسایی دولت استفاده‌کننده آن است؛ بااین‌حال، دولت‌ها می‌توانند توانمندی‌های سایبری خود را بدون نسبت داده شدن به آن توسعه و استفاده کنند، درنتیجه از مزایای اعلام رسمی توانمندی های سایبری کاسته شده است. دوم، برخلاف بسیاری از سلاح‌های فیزیکی، سلاح سایبری «دارای نیمه عمر کاربردی کوتاه» هستند. سوم، علامت‌دهی به یک هدف به همان اندازه بی‌فایده است. اگرچه معمولاً در عملیات سایبری حمله‌بر دفاع ترجیح دارد، اطلاع دادن از قصد حمله به شبکه یا دستگاه‌های رایانه‌ای به هدف به تضعیف اثرات حمله می‌انجامد. این کار به

1 . Richard Betts
2 . Matthew Campbell

دشمن اجازه می‌دهد از اطلاعات حفاظت کند و یا برخی از وسایل دیگر را برای خنثی کردن حمله به سیستم و یا شبکه هدف بکار گیرد

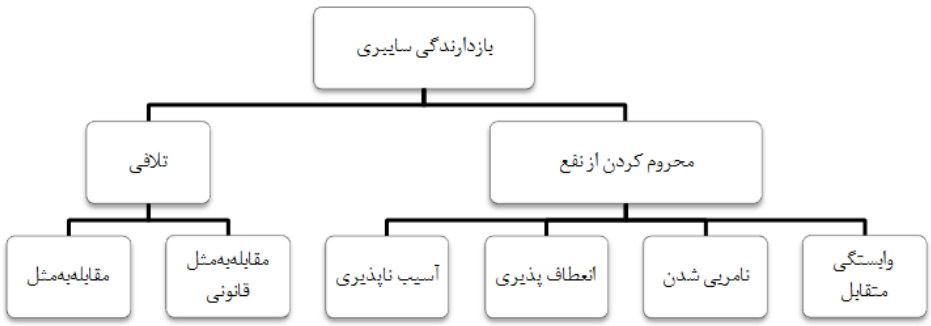
مقیاس و زمان: زمان و مقیاس عملیات بالقوه سایبری مخرب نیز مسائل اساسی هستند که بر بازدارندگی سایبری تأثیر می‌گذارد (رید[1]، ۲۰۰۵). اغلب گفته می‌شود که خطرناک‌ترین حمله سایبری آن است که هنوز کشف نشده است. این واقعیت که دشمن به یک شبکه نفوذ کرده به‌اندازه کافی نگران‌کننده است؛ ولی دریافتن اینکه برای چندین سال بدون اطلاع کسی نفوذ داشته است بسیار مشکل‌ساز است. یکی از جنبه‌های منحصربه‌فرد اینترنت است که عمل تهاجمی آسان‌تر از دفاع است. بدیهی است که پیدا کردن یک نقطه‌ضعف در یک شبکه و یا سیستم از دفاع از کل شبکه یا سیستم آسان‌تر است. مانند زمان، مقیاس یک عملیات سایبری مخرب باید از عملیات فیزیکی معمولی متفاوت درک شود. چند میلی‌ثانیه طول می‌کشد تا یک حمله انجام شود، اما مقیاس این آسیب می‌تواند بسیار زیاد باشد.

ضرورت: درنهایت، مهم است به نظریه ضرورت اشاره کرد. بر اساس این قانون برای شروع جنگ، رهنامه ضرورت یک نیاز برای دفاع از خود در پاسخ به هر حمله مسلحانه‌ای است. اگرچه چندین نظریه برای تعیین عامل یک حمله به شبکه مطرح است، برجسته‌ترین این نظریه‌ها مستلزم نگاه به نتایج حاصل از این حمله است. به‌طورکلی، با وقوع حمله نظریه بازدارندگی که در زیر بحث شده می‌تواند توانایی یک دولت قربانی را برای توجیه پاسخ به چالش می‌کشد اگر هیچ‌چیز از این حمله به دست نیاید ملت قربانی نمی‌تواند یک واکنش را توجیه کند. حتی اگر بازدارندگی تنها قادر به کاهش اثر حمله باشد، رهنامه ضرورت و تناسب، پاسخ قانونی موجود قربانی را محدود می‌سازد. این قطعاً یک توجیه برای چشم‌پوشی از بازدارندگی نیست، اما یک موضوع مهمی است که یک ملت باید در روش‌های مختلف جلوگیری از دشمنان بکار برد. باوجوداین مسائل مهم، استفاده از بازدارندگی از طریق و علیه عملیات سایبری برای امنیت ملی حیاتی است.

1 . Thomas C. Reed

الگوی بازدارندگی سایبری

بازدارندگی سایبری باید نقشی فعالی در راهبرد امنیت ملی داشته باشد. به دلیل ماهیت منحصربه‌فرد آن، عملیات سایبری یک دیدگاه گسترده در بازدارندگی سایبری ایجاد کرده که شامل بسیاری از مفاهیم تاریخی بازدارندگی است اما شباهت کمی با بازدارندگی در جنگ سرد دارد. بازدارندگی سایبری در این بخش به دودسته گسترده تقسیم‌شده است: الف) تلافی و ب) محروم کردن از کسب منافع. در این دودسته، شش روش برای بازدارندگی سایبری می‌شود.



نمودار ۱: طیف بازدارندگی سایبری

روش شناسی پژوهش

روش تحقیق در این پژوهش توصیفی- تحلیلی می‌باشد. با مطالعه مبانی نظری و ادبیات تحقیق عوامل اثر گذار بر بازدارندگی سایبری شناسایی و یافته های بر اساس آن تبیین گردید.

یافته‌های تحقیق

تلافی

تهدید به‌تلافی، هنگام داشتن قابلیت و اراده، می‌تواند برای بسیاری از بازیگران بالقوه عامل بازدارنده خوبی باشد (لیبیکی[1]، ۲۰۰۷). همه دشمنان بالقوه قابل منصرف کردن نخواهند بود اما چون بسیاری منصرف می‌شوند پس یک جنبه حیاتی از بازدارندگی است. این امر در بازدارندگی سایبری هم درست است. دو جنبه خاص از اقدامات تلافی‌جویانه درخور مطالعه است. نخست، اقدامات تلافی‌جویانه به یک حادثه سایبری ممکن است به شکل حمله متقابل به مجرم باشد.

1 . Martin C. Libicki

چنین پاسخی در بسیاری از موارد قانونی است، هرچند مسائل قانونی هم وجود دارد. دوم، اقدامات تلافی‌جویانه نیز می‌تواند در چهارچوب یک الگوی اجرای قانون انجام شود، مانند جریمه کیفری یا مدنی و مجازات است.

- حمله متقابل: در پاسخ به یک حمله سایبری، یک دولت می‌تواند طیف کاملی از پاسخ را در نظر گرفته، طرح و علامت کند (زاگار و کولگور[1]، ۱۹۹۸). پاسخ نظامی، می‌تواند یک گزینه بازدارنده‌ای برای جنگ سایبری باشد. پتانسیل پاسخ براثر سوءتفاهم باعث شده آمریکا با روسیه و چین در مورد تأسیس یک نسخه سایبری از خط ویژه پیام‌رسانی مذاکره کند. ایده استفاده از یک واکنش فیزیکی به یک حمله سایبری جدید نیست و در ادبیات بحث شده است. واضح است که درحالی‌که بسیاری از مفسران بر اصل آن توافق دارند، اما اذعان دارند که پاسخ نظامی به یک حمله سایبری به نگرانی‌های منطقی می‌انجامد (گورمن[2]، ۲۰۰۸). صرف‌نظر از مشکلات نسبت دادن موردبحث در بالا و توانایی برای جعل هویت مهاجم، پاسخ فیزیکی خطراتی دارد. این محدودیت‌ها درباره حمله متقابل به‌عنوان‌مثال عامل بازدارنده، منکر سودمندی آن نیست اما کشورها را تشویق می‌کند فقط بر یک نظریه واحد بازدارندگی تکیه نکنند. پاسخ سایبری به یک حمله سایبری ممکن است در برخی شرایط مؤثر باشد. نکته کلیدی این است که به‌عنوان‌مثال ماده اعلام توانمندی های تهاجم سایبری در بازدارندگی، حمله متقابل به عملیات سایبری محدود نمی‌شود و می‌تواند طیف کاملی از پاسخ نظامی و سخت و خشن را در برگیرد. توانایی یک دولت به‌مثابه علامت قانونی، «حمله متقابل» بازدارنده برای حمله سایبری منوط خواهد بود به تعیین عامل و اینکه یک حمله مجازی معادل استفاده از زور یا مسلحانه بوده است (ناکاشیما[3]، ۲۰۱۰).
- تناسب: هرچند که قانون بین‌المللی الزامی در پاسخ به نوع یک حمله ندارد، دفاع از خود با اصل تناسب محدودشده است. هر پاسخ برنامه‌ریزی‌شده و یا در نظر گرفته‌شده به‌عنوان‌مثال

1 . Frank C. Zagare and D. Marc Kolgour
2 . Siobhan Gorman
3 . Ellen Nakashima

عامل بازدارنده باید با تهدید یا استفاده از زور پیش‌بینی‌شده متناسب باشد. استفاده از اصطلاح «متناسب» به این معنا نیست که پاسخ باید همانند آن حمله و یا به همان روش باشد. بلکه به این معنی که پاسخ باید با حمله اولیه معادل بوده و به تشدید نینجامد. البته برخی استدلال کرده‌اند که تعیین یک پاسخ متناسب با یک عملیات سایبری ممکن است دشوار باشد.

حمله متقابل قانونی: حمله متقابل به‌احتمال‌زیاد اثر مخربی دارد، اینجا به بازدارندگی از طریق پارادایم سنتی اجرای قانون می‌پردازیم. به‌عبارت‌دیگر، این نوع از بازدارندگی یعنی «پس از حمله تو را پیداکرده و مجبور به پرداخت تاوان می‌کنم».

پیگرد قانونی: اعمال دولت در پاسخ به یک حادثه سایبری در تمام جهان روی پارادایم حقوق کیفری متکی است. این حتی در حالتی که عملیات سایبری علیه رایانه‌های دولت انجام شد درست است (متیو[1]،۲۰۰۹). به‌عنوان‌مثال، حمله سایبر در سال ۲۰۰٦ علیه دستگاه‌های دولتی و رایانه غیرنظامی در استونی که در ابتدا تصور می‌شد توسط دولت روسیه انجام شد، درنهایت با استفاده از پارادایم حقوق کیفری پیگیری شد. حمله متقابل قانونی در قالب پیگرد قانونی بدون شک می‌تواند نقش مهمی در هر دو بازدارندگی عام و خاص بازی کند. تعقیب موارد گذشته به استفاده از مجازات و به اعتبار روش بازدارندگی می‌افزاید. بسیاری از کشورها در حال تقویت قابلیت‌های اقدامات قانونی رایانه‌ای خود و تصویب قوانین داخلی برای پوشش و مجازات این جرائم است. اما مسائل حقوقی در حمله متقابل قانونی بازدارندگی شامل مسائل فراملی و بین‌المللی رویه‌ای، مانند استرداد و صلاحیت و همچنین ناتوانی قانون برای رسیدگی به بازیگران خاصی که از مهار نشدنی هستند برمی‌گردد (بون[2]، ۲۰۰۷). علاوه بر این، کمبود توافقنامه‌های بین‌المللی مؤثر برای حل این مشکلات توانایی یک ملت در علامت حمله متقابل قانونی را به‌عنوان‌مثال عامل بازدارنده واقعی محدود می‌کند.

محروم کردن از نفع حمله

1 . William Matthews
2 . M. Elaine Bunn

موفقیت این دو روش قبلی برای بازدارندگی متکی بر ترس از برخی از اقدامات تلافی‌جویانه، یا به دلیل یک توان و تمایل بالقوه قربانی در مقابله‌به‌مثل است. بااین‌حال، این تنها راه برای مشاهده اثرات بازدارندگی نیست. بازدارندگی همچنین می‌توانید با حذف منافع ناشی از حمله دشمن انجام می‌شود. درک درست از بازدارندگی سایبری از دیگر راهبُردهای بازدارندگی فیزیکی متفاوت است زیرا در آن‌ها تکیه‌بر شدت در مقابله‌به‌مثل کردن است. هرچند همه پارادایم‌های بازدارندگی تا حدی بر ایده محروم کردن دشمن از دیدن حمله تکیه می‌کنند! عملیات سایبری اجازه می‌دهد این جنبه بازدارندگی به رویکرد اولیه تبدیل شود. از طریق ساخت دستگاه‌های سایبری مقاوم به حمله سایبری، ساختمان انعطاف‌پذیر دستگاه‌های سایبری، ساخت دستگاه‌های خاص نامرئی در برابر مهاجمان و شبکه‌های وابسته به‌طوری‌که حتی مهاجمان احتمالی خود نیز در یک حمله صدمه ببینند منافع پیش‌بینی‌شده را انکار می‌شود. یک نکته در نظریه بازدارندگی سایبری؛ ایجاد یک توازن بین هزینه‌های حمله و درک احتمال موفقیت است (لانگ[1]، ۲۰۰۸). به‌عبارت‌دیگر بازدارندگی کامل وقتی است که مهاجم هیچ شانسی برای موفقیت نبیند.

آسیب‌ناپذیری

درکلی‌ترین شرایط، این روش بازدارنده ممکن است به شکل «حتی اگر سعی کنید، نمی‌توانید به من آسیب بزنید. این فرم پیشنهادی در امنیت شبکه سایبری و دارایی‌ها به‌طور قابل از توجهی حمله جلوگیری خواهد کرد. حفاظت از دستگاه‌ها؛ حضور دستگاه‌های سایبری در همه‌جا باعث می‌شود که حفاظت از آن‌ها بسیار دشوار شود. دستگاه‌های حمله دشمنان به‌طور مداوم تغییر کرده و تقریباً هرگز نمی‌توان بلافاصله تشخیص داد که آن حمله کجا سرچشمه گرفته و هدف نهایی چیست. حمله به دستگاه‌های سایبری اغلب غیرقابل‌کشف هستند و حمله خطرناک‌تر آن است که اغلب نمی‌دانیم در حال وقوع است. علاوه بر مسائل مربوط به فناوری، توانایی تأمین امنیت رایانه و شبکه‌های رایانه‌ای همچنین نگرانی حقوقی قابل‌توجهی به همراه دارد. این نگرانی‌ها در موردتعامل هرگونه اقدامات امنیتی با نهادهای مدنی خصوصی و با دوستان، متحدان و شرکایی

1. Austin Long

است که ممکن است از طریق این اقدامات امنیتی متأثر شده و مسائل بالقوه انتقال فنّاوری لازم برای تسهیل تعامل را شامل شود. بیشتر ترافیک اینترنت دولت از زیرساخت اینترنت غیرنظامی می‌گذرد. اجرای هر اقدام امنیتی برای محافظت در برابر عملیات سایبری مخرب، لزوماً ارائه‌دهندگان اینترنت خصوصی را متأثر می‌کند.

انعطاف‌پذیری

ایده انعطاف‌پذیری یعنی دستگاه‌های سایبری یک ملت تا حدی بادوام است که درواقع حمله به قربانی صدمه نخواهد زد. این نوع از بازدارندگی در مقابله با دشمنانی که به دنبال اطلاعات خاصی است و یا فقط می‌خواهند به یک رایانه خاص ضربه بزنند کارا نیست. بااین‌حال، انعطاف‌پذیری قربانی ممکن است انگیزه برای حمله مهاجم را اگر هدف تخریب گسترده سیستم است از میان ببرد. انعطاف‌پذیری به دودسته عمده تقسیم می‌شود: افزونگی و بازسازی. توانایی ادامه به کار حتی پس از یک حمله موفق (افزونگی) و یا بازسازی سیستم سریع تا اثرات حمله موفق را حداقل کند (بازسازی). افزونگی در یک سیستم یک عامل بازدارنده است چون مهاجمان احتمالی را به این دلیل که توانایی اثر حمله به عملکرد سیستم را ندارند منصرف می‌کند. علاوه بر افزونگی، یک ملت می‌تواند با افزایش توانایی خود در بازسازی بعد از یک حمله از آن جلوگیری کند (شولسکی، ۲۰۰۹). این مورد کمی با انعطاف‌پذیری متفاوت است، درواقع به این معنی نیست که این حمله اثر موردنظر خود را نخواهد داشت بلکه به این معنی است که یک ملت می‌تواند به‌سرعت اثرات این حمله را حداقل کرده و مجدد، شروع به کار کند.

نامرئی بودن

یکی از راه‌های محافظت از خود از حمله این است که برای دشمنان نامرئی بود. اگر دشمن نتواند سیستم و یا رایانه را برای حمله پیدا کنید، پس بازداشته شده است. در این صورت، مهم نیست که سلاح دشمن چقدر قوی است؛ اگر مهاجم نتوانید هدف را پیدا کند، سلاح‌هایش بی‌اثر است. نامرئی بودن به شکل یک عامل بازدارنده کار می‌کند زیرا اگر دشمن نتواند هدف خود را پیدا کنید، بر جای دیگری تمرکز می‌کند. حتی اگر مهاجم بداند که سیستم وجود دارد، مجبور به تعیین

تخصیص زمان و منابع خود برای یافتن آن کند. در یک محیط با اهداف بسیار، دستگاه‌هایی که سخت‌تر پیدا خواهد شد احتمال کمتری دارد موردحمله قرار گیرد. گمراه کردن مهاجم؛ و نمایش اغراق‌آمیز تأثیر نفوذ گر به او تصویری غلط از توانایی‌های فیزیکی خود می‌دهد.

وابستگی متقابل

روش نهایی بازدارندگی سایبری موردبحث در این مقاله وابستگی متقابل است؛ مانند بقیه، این روش دارای ویژگی‌های منحصربه‌فردی در پارادایم اینترنتی است. توانایی هم‌پیوستگی وابستگی دیجیتالی با دیگر کشورها، ازجمله دشمنان، با ظهور اینترنت به‌صورت تصاعدی افزایش‌یافته است. توسعه قابلیت آگاهی و هشدار مشترک بین‌المللی به بازدارندگی جمعی می‌انجامد (متیو،۲۰۰۹). اینترنت به ارتباط متقابل در امور مالی، علم، هنر و زمینه‌های دیگر می‌انجامد که حکومت با آن به ارائه یک تجربه زندگی غنی‌تر در شهروندان را تسهیل کرده است. این وابستگی به بازدارنده ذاتی برای کشور و بازیگران غیردولتی در انجام حمله سایبر منجر می‌شود.

سهیم شدن در اثرات؛ افزایش سطح وابستگی متقابل اجازه می‌دهد تا یک ملت هدف، به مهاجم استدلال کند که صدمه زدن به آن دولت هدف، به همان اندازه به مهاجم لطمه می‌زند. این‌چنین استدلال‌هایی مسلماً بسیار بیشتر بر دولت‌ها تأثیر دارند تا بازیگران غیردولتی، اما حتی برخی از بازیگران غیردولتی ممکن است متقاعد شوند که حمله به جنبه‌های خاصی از یک حوزه متقابل، ازجمله قدرت اقتصادی دولت موردنظر، می‌تواند تأثیرات قابل‌توجهی بر توانایی بازیگر غیردولتی و اهداف کلی آن داشته باشد. بارزترین نامزدهای این روش بازدارندگی کشورهایی با ارز مشترک (مانند یورو) و یا درگیر در توافق‌نامه تجاری، ازجمله اعضای اتحادیه اروپا و یا قرارداد تجارت آزاد آمریکای شمالی هستند. بااین‌حال، این می‌تواند میان دشمنان سایبری بالقوه مانند آمریکا و چین یا آمریکا و روسیه باشد. هر چند در بحث فناوریهای حساس منجر به اخذ تعهد از کشور دریافت کننده شود؛ به‌طور مثال، هنگامی‌که آمریکا اجازه فروش فن‌آوری حساس می‌دهد، معمولاً از ملت دریافت‌کننده تعهداتی می‌خواهد که فنّاوری را نشر ندهند (لانگ، ۲۰۰۸).

نتیجه‌گیری

هدف این مقاله نقش جنگ سایبری و شناسایی مؤلفه‌های تأثیرگذار آن در بازدارندگی سایبری بود که بر این اساس اندیشه راهبردی پس از جنگ سرد درباره‌ی جنگ سایبری نشان می‌دهد یک نظریه برای جنگ سایبری را با پایه‌ها آتی ارائه کرد که عبارت‌اند از: جنگ سایبری در اصل برای استراتژی تهاجمی مناسب است و روش‌های دفاعی هم باید، فعالانه یا تا حدی در شیوه‌ای تهاجمی دنبال شود. حملات سایبری، به‌جای اینکه ذاتاً گسترده باشند، باید برای هدف قرار دادن تعیین گره‌های باارزش بالا و مهم طراحی شود؛ سرعت، مانور و چابکی از عوامل مهم در جنگ سایبری است که در صورت انجام در مراحل آغازین رویارویی که بهترین نتیجه را دارد و یا حتی پیشگیرانه؛ با آغاز رویارویی، حملات سایبری باید به‌صورت موازی یا هم‌زمان با حملات متعارف، برای به حداکثر رساندن اثر اجرا شوند. جنگ سایبری ذاتاً غیر افزایشی است. منحنی یادگیری نیز در طرف هدف نشان می‌دهد که بسیار برای غافلگیری مناسب است؛ همان زمان یک رویکرد ساکت و آرام، پنهانی، یواشکی و باحوصله به جنگ سایبری می‌تواند در دست‌کاری اطلاعات و دستیابی به اثرات روانی مؤثر باشد. بازدارندگی سایبری باید نقشی فعالی در راهبرد امنیت ملی کشورداشته باشد. به دلیل ماهیت منحصربه‌فرد آن، عملیات سایبری یک دیدگاه گسترده در بازدارندگی سایبری ایجاد کرده که شامل بسیاری از مفاهیم تاریخی بازدارندگی است اما شباهت کمی با بازدارندگی در جنگ سرد دارد. برابر نتایج بازدارندگی سایبری به دودسته گسترده تقسیم‌شده است: الف) تلافی و ب) محروم کردن از کسب منافع؛ که تلافی شامل: حمله متقابل قانونی و مقابله مثل و محروم کردن از کسب منافع شامل: آسیب‌ناپذیری، انعطاف‌پذیری، نامرئی بودن شدن، وابستگی متقابل می باشد. امید است که با اقدام موثر در این زمینه و بسط و گسترش ارتش سایبری امکان بازدارندگی سایبری و محافظت از سامانه‌ها در مقابل حملات سایبری با توجه به دشمنی قدرت‌های فرامنطقه‌ای و بعضی دول و گسترش روزافزون فضاهای مجازی محقق گردد.

فهرست منابع:

- Becker, Gary S. (1968), “Crime and Punishment: An Economic Approach”, Journal of Political Economy, Vol. 76, No. 2, p. 210.
- Blank, Stephen. (2001), “Can Information Warfare Be Deterred?” Defense Analysis, Vol. 17, No. 2, p. 130.
- Cartwright, James E. (2007), "Statement on the United States Strategic Command Before the House Armed Services Committee".
- CSIS Commission on Cybersecurity for the 44th Presidency. (2008), "Securing Cyberspace for the 44th Presidency", Washington, D.C.: Center for Strategic and International Studies.
- Kaufmann, William. (1998), “The Evolution of Deterrence 1945–1958”, unpublished RAND research
- Fainaru, Steve., and Grimaldi, James V. (2001), “FBI Knew Terrorists Were Using Flight Schools”, Washington Post, p. A24.
- Kuehl, Dan. (2009), “From Cyberspace to Cyberpower: Defining the Problem", in Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., "Cyberpower and National Security", Washington D.C.: National Defense University Press, p. 30.
- Cartwright, James E. (2007), "Statement on the United States Strategic Command Before the House Armed Services Committee".
- Denning, Dorothy. (2001), “Obstacles and Options for Cyber Arms Control", presented at Arms Control in Cyberspace, Heinrich Boll Foundation, Berlin, Germany.
- Espiner, Tom. (2008), “US Reveals Plans to Hit Back at Cyber Threats", ZDNet News.
- Hundley, Richard O., and Anderson, Robert H. (2009), “Emerging Challenge: Security and Safety in Cyberspace", IEEE Technology and Society Magazine, Vol. 14, No. 4, p. 25.
- Holmes, Erik. (2009), “Donley Sets out Structure for Cyber Command", Air Force Times.
- Hart, Kim. (2008), “Longtime Battle Lines Are Recast in Russia and Georgia’s Cyberwar", Washington Post, p. D01.
- Harris, Shane. (2008), “China’s Cyber Militia", National Journal Magazine.
- Hathaway, Melissa E. (2008), “Cyber Security: An Economic and National Security Crisis", The Intelligencer: Journal of U.S. Intelligence Studies, Vol. 16, No. 2, p. 35.
- Gunaratna, Rohan. (2002), "Inside Al Qaeda’s Global Network of Terror", New York: Columbia University Press.
- Gates, Robert. (2008), “Nuclear Weapons and Deterrence in the 21st Century", address to the Carnegie Endowment for International Peace.
- Herzog, Chaim. (1982), "The Arab-Israel Wars: War and Peace in the Middle East from the War of Independence Through Lebanon", New York: Random House.
- Shulsky, Abram N. (2009), "Deterrence Theory and Chinese Behavior", Santa Monica, Calif.: RAND Corporation, MR-1161
- Lake, Eli. (2008), “McCain Backs Tougher Line Against Russia”, The Sun (New York).
- Lemonick, Michael D. (1989), “The Chernobyl Cover-Up", Time.

- Traynor, Ian. (2008), “Russia Accused of Unleashing Cyberwar to Disable Estonia” The Guardian.
- Fernandez, Manny. (2008), “Terrible Rumble, Then Chaos as Crane Fell”, New York Times.
- Betts, Richard. (1982), "Surprise Attack", Washington D.C.: Brookings Institution.
- Campbell, Matthew. (1998), "‘Logic Bomb’ Arms Race Panics Russians", The Sunday Times.
- Reed, Thomas C. (2005), "At the Abyss: An Insider’s History of the Cold War", San Francisco: Presidio Press
- Libicki, Martin C. (2007), "Conquest in Cyberspace", Cambridge, U.K.: Cambridge University Press.
- Zagare, Frank C., and Kolgour, D. Marc. (1998), “Deterrence Theory and the Spiral Model Revisited”, Journal of Theoretical Politics, Vol. 10, No. 1, p. 70.
- Gorman, Siobhan. (2008), "Bush Looks to Beef Up Protection Against Cyberattacks", WALL ST.J.
- Nakashima, Ellen. (2010), "Large Worldwide Cyber Attack Uncovered", WASH. POST, at A3.
- George, Alexander L. & Smoke, Richard. (1974), "Deterrence In American Foreign Policy: Theory And Practice 12".
- Matthews, William. (2009), "Cyber War’s ‘Front Lines’ May Be in Private Hands", DEF. NEWS.
- Bunn, M. Elaine. (2007), "Can Deterrence Be Tailored?", STRATEGIC FORUM, p. 4.
- Long, Austin. (2008), "Deterrence: From Cold War To Long War", World Politics 143, P. 3.