نخستین همایش ملی واکاوی تهدیدهای نوپدید دفاعی- نظامی
دانشگاه فرماندهی و ستاد آجا

نقش جنگ سایبری و شناسایی مؤلفه‌های تأثیرگذار آن در بازدارندگی سایبری

عبداله وثوقی نیری، داود غفوری ، رسول کریمی طاهر
نویسنده مسئول، هیئت علمی دانشگاه علوم و فنون هوایی شهید ستاری، a.vosoughi@yahoo.com
هیئت علمی دانشگاه علوم و فنون هوایی شهید ستاری
هیئت علمی دانشگاه علوم و فنون هوایی شهید ستاری

چکیده
امروزه جنگ سایبری به علت توان درگیر کردن زیرساخت‌های حیاتی کشور، اهمیت دوچندانی یافته 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.
کلید واژه: تهدید، جنگ، جنگ سایبری، بازدارندگی

مقدمه و بیان مساله
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 .
اندیشه راهبردی، درباره جنگ سایبری در مراحل آغازین خود است (بیکر، ۱۹۶۸). جنگ سایبری تفاوت قابل‌توجهی با نیروی هوایی، دریایی و زمینی دارد و آن 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، ۲۰۰۱)؟ 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 است؛ جنگ فرماندهی و کنترل، جنگ بر پایه، جنگ الکترونیک، جنگ روانی، جنگ هکرها وجنگ اطلاعاتی 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). 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.
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. (بلنک، ۲۰۰۱).

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 (کارترایت، ۲۰۰۷) و دستور آن حفاظت از شبکه‌های کامپیوتری پنتاگون بود و در سال ۲۰۰۰ به این نیرو یک مأموریت تهاجمی نیز اختصاص داده شد. 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.
چین در اواخر سال‌های ۱۹۹۰ تصمیم خود را برای توسعه قابلیت جنگ اطلاعاتی تهاجمی گرفته است. چین بر رویکردهای "نامتقارن " تمرکز کرد که نقاط ضعف و آسیب‌پذیری آمریکا را هدف قرار داد. (سی. اس. آی. اس، 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. 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. ماهیت لحظه‌ای جنگ سایبری و توانایی حمله به‌کل دامنه به‌طور هم‌زمان از ویژگی‌هایی است که باعث شده ابعاد سایبری جنگ به‌خصوص بالقوه خطرناک باشند. (کافمن، ۱۹۹۸).

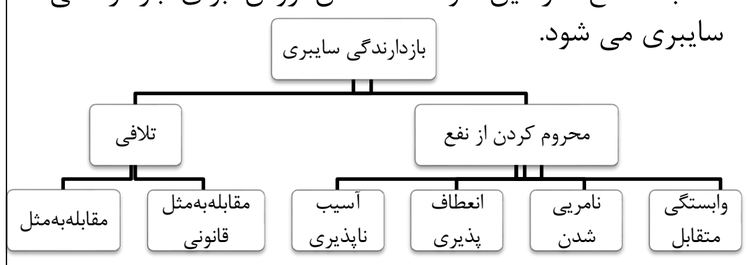
هدف جنگ سایبری
هدف عملیاتی جنگ سایبری از بین بردن توانمندی‌های سایبری نیست که مانند یک نیروی زمینی به دنبال نابود کردن نیروهای زمینی دشمن باشد. "درحالی‌که مفهومی همانند به فتح را می‌توان برای فضای مجازی تعریف کرد، خود فضای مجازی را نمی‌توان در معنای متعارف فتح کرد" (فاینارو و گریمالدی، ۲۰۰۱). هدف جنگجوی سایبری 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، ۲۰۰۹). 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). 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 چین جریان دارد(فاینارو و گریمالدی، ۲۰۰۱). 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. 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، ۲۰۰۱). درنهایت، 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.
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. موضوع اصلی در ادبیات نظامی آمریکا لزوم تهاجم است(فاینارو و گریمالدی، ۲۰۰۱). پدافند در اندیشه راهبردی در یک ساختار عامل و نه غیرعامل ارائه‌شده است (دنینگ، ۲۰۰۱). جنگ سایبری یک مانور جنگی است که در آن سرعت و چابکی مهم‌ترین اصل است (اسپینر، 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، ۲۰۰۹).

روش تحقیق
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.

یافته های تحقیق
الف پارادوکس‌های جنگ سایبری
آستانه ها: اولین و اساسی‌ترین سؤال این است که آیا جنگ سایبری را می‌توان یک جنگ در نظر گرفت؟ (هلمز ، ۲۰۰۹)؛ رخنه‌ها ذاتاً هک، جاسوسی، یا مجرمانه‌اند و بیشتر یک محرک به‌حساب می‌آیند تا اقدام جنگی (هارت ، ۲۰۰۸).
قریب‌الوقوع بودن: این چارچوب به‌ظاهر ساده در جنگ سایبری چالش بزرگ‌تری هم هست (هاساوی ، ۲۰۰۸).
نسبت دادن: نسبت دادن حمله در مفهوم بازدارندگی برای جنگ سایبری یک مشکل اساسی است (اسپینر، ۲۰۰۸).
سودمندی: پیامدهای حمله سایبری بیشتر همانند ویرانگری به دست چریک‌ها یا نیروهای عملیات ویژه است تا جنگ در گستره دریا، زمین، یا هوا. (گوناراتنا ، ۲۰۰۲). جنگ سایبری، یک جنگ‌افزار تهاجمی بالقوه در آینده است.
غیرقابل‌پیش‌بینی بودن: اثرات سلاح‌های سایبری ذاتاً جهانی است و نمی‌توان لزوماً به یک محدوده جغرافیایی مشخص محدود کرد(گیتس ، ۲۰۰۸).

ب الگوی بازدارندگی سایبری
بازدارندگی سایبری باید نقشی فعال در راهبرد امنیت ملی داشته باشد. 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 می شود.



نمودار شماره ۱الگوی بازدارندگی سایبری

نتیجه گیری
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 و همچنین با ایفای نقش دفاع عامل و اقدام برای تلافی و محروم کردن از منافع متناسب با قوانین بین المللی از حمله های مشابهی چون استاکس نت جلوگیری نمود.