بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا

علی‌اصغر دهقانی*

تاریخ دریافت: ۱۳۹۶/۱۱/۲
تاریخ تأیید: ۱۳۹۷/۳/۳

چکیده

در عصر کنونی، موضوعی جدید به ادبیات امنیت استراتژیک اضافه شده که بسیار پیچیده می‌نماید. سلاح مجازی[1] افزوده‌ای جدید به زرادخانه دولت‌هاست. 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 سال‌ها، منطق استراتژیک جنگ سرد را به طرزی موفقیت‌آمیز شکل داده بود، بازدارندگی است. با وجود موفقیت این سازوکار در عرصه‌های سنتی، فهم بازدارندگی در فضای سایبر مشکل است؛ چراکه ذهن ما با ادبیات جنگ سرد، مبنی بر بازدارندگی به‌مثابه تهدید به تلافی یک حمله هسته‌ای با استفاده از ابزارهای هسته‌ای، شکل گرفته است. مقایسه وضعیت کنونی با بازدارندگی جنگ سرد اشتباه است. جلوگیری از آسیب در فضای سایبر، سازوکارهای پیچیده‌ای مانند تهدید به تلافی، انکار، گرفتار کردن[2] و هنجارها[3] را می‌طلبد. جرویس از سه مرحله نظریه‌پردازی بازدارندگی در دوران هسته‌ای صحبت کرده بود[4]. نظریه‌پردازی در خصوص بازدارندگی در فضای سایبر، در اولین موج خود قرار دارد. فرمول‌بندی یک استراتژی مؤثر در عصر سایبر، نیازمند فهمی گسترده‌تر و چندبعدی از مفهوم بازدارندگی است و نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری بدهیم.

واژگان کلیدی: بازدارندگی سایبری، امنیت سایبری، فضای سایبر، حمله سایبری، بازدارندگی.

* دانشجوی دکتری روابط بین‌الملل، دانشکده علوم اقتصادی و سیاسی، دانشگاه شهید بهشتی، تهران.
dehghan.com@gmail.com

1 Virtual Weapon
2 Entanglement
3 Norms
4 Robert Jervis, «Deterrence Theory Revisited», World Politics, 1979

مقدمه

آیا کشورها می‌توانند در فضای سایبر دیگران را از آسیب رساندن به امنیت خود بازداشته و منصرف کنند؟ این یکی از مهم‌ترین پرسش‌هایی است که اخیراً پیش روی متفکران حوزه امنیت بین‌الملل و مطالعات استراتژیک قرارگرفته است. مزیت‌های بدیعی که فضای سایبر در اختیار قرار داده، موجب گسترش روزافزون استفاده افراد، گروه‌ها و سازمان‌های ملی و بین‌المللی شده و ضمن ارائه خدمات بی‌شمار، عرصه امنیت ملی و بین‌المللی را آبستن مخاطرات جدیدی نموده است: حملات سایبری.

ویژگی‌های منحصربه‌فرد این عرصه جدید امکانات مناسبی در اختیار مهاجمانی قرار داده که می‌توانند زیرساخت‌های ملی را مورد تهدید قرار دهند. ما در این مقاله، به دنبال بررسی این موضوع هستیم که چگونه می‌توان این مهاجمان را از اقدامات مغایر امنیت ملی و بین‌المللی بازداشت؟ آیا استراتژی بازدارندگی که منطق استراتژیک دوران جنگ سرد را تشکیل می‌داد، در عصر سایبر قابلیت عملکرد دارد؟ می‌خواهیم ببینیم که مشخصات عرصه جدید چه تفاوت‌هایی با عرصه‌های نبرد سنتی داشته و سایبر قابلیت تغییر کدام‌یک از مؤلفه‌های منطق استراتژیک را داراست. درواقع، سؤال اصلی مقاله این است که کارکرد عناصر مختلف نظریه بازدارندگی سنتی در فضای سایبر چگونه خواهد بود؟ و آیا نظریه بازدارندگی در این عرصه جدید، قابلیت کاربست دارد یا خیر؟ فرضیه اصلی مقاله این است که بازدارندگی به آن شکلی که متناسب با فضای جنگ سرد و سلاح‌های مخرب[5] طراحی شده بود، در فضای سایبر تناسب ندارد و ضروری است تغییراتی در آن لحاظ گردد تا برای نبرد دیجیتال کارایی داشته باشد.

این مقاله، ابتدا تلاش خواهد کرد تا به ارزیابی تئوریک نظریه بازدارندگی پرداخته و پس از ارزیابی عناصر نظریه بازدارندگی هسته‌ای، نسبت به ایضاح شرایط عرصه سایبر و تغییرات ایجادشده (به نسبت عرصه‌های سنتی) اقدام کند. پس‌ازآن، به بازدارندگی سایبری پرداخته خواهد شد. مقاله با ارزیابی یک مورد تهدید سایبری در دنیای واقع ادامه می‌یابد و تلاش خواهد شد تا نظریه بازدارندگی در مورد آن به کار بسته شود.

۱. پیشینه و ادبیات پژوهش

جدید بودن عرصه سایبر در کنار بدیع و تخصصی بودن اصطلاحات و مفاهیم[6] آن، ازجمله دلایلی هستند که باعث شده تا اندیش‌مندان حوزه امنیت بین‌الملل، تاکنون اقبال مناسبی به

5 Kinetic

6 Concepts

آن نشان ندهند. استفان والت در این خصوص می‌گوید: «کل موضوع رمزگونه است. شما نیازمند این هستید که اطلاعات زیادی در خصوص شبکه‌های کامپیوتری، نرم‌افزار، رمزنگاری و ... داشته باشید تا بتوانید میزان خطر واقعی را درک کنید». با وجود این، یکی از مهم‌ترین نظریه‌پردازانی که ورود مناسبی به موضوع داشته، جوزف نای است که تلاش دارد مسائل حوزه امنیت سایبری را مورد بررسی قرار دهد. او در کتابی با عنوان آینده قدرت[7]، به بررسی تحول مفهوم قدرت در دوران جدید پرداخته و بخش بزرگی از آن را صرفاً به موضوع سایبر اختصاص داده است. نای مهم‌ترین تحول ایجادشده در رابطه با قدرت را پراکندگی آن می‌داند؛ به این معنا که قدرت به نحو روزافزونی از دست منابع پیشین خارج‌شده و به شکلی پراکنده و متفرق در دست بازیگرانی جدید قرار می‌گیرد که فاقد مشخصات و محذوریت‌های دولت‌های ملی بوده و امکان ایجاد بازدارندگی در برابر آن‌ها کاهش می‌یابد.

او در این کتاب بیان می‌دارد که در قرن حاضر دو گونه جابه‌جایی قدرت را پیش رو داریم: گذار از قدرت[8] و پراکندگی قدرت[9]. گذار از قدرت از کشوری غالب به کشوری دیگر، پدیده‌ای آشنا در پهنه تاریخ است. اما پراکندگی آن تحولی است تازه. ما امروزه با مخاطرات، تهدیدات و چالش‌هایی مواجهیم که با وجود تأثیر آن بر کشوری واحد، عمدتاً یا تماماً ریشه در کشوری دیگر دارند. بحران‌های مالی، جرائم سازمان‌یافته، مهاجرت انبوه، گرمایش جهانی، بیماری‌های عالم‌گیر و تروریسم جهانی از این جمله‌اند. یکی از دلایل این مشکل، پراکندگی قدرت است. انقلاب اطلاعاتی دست‌اندرکار تغییر ماهیت قدرت و پراکنده‌تر ساختن آن است. این بدین معناست که سیاست جهانی دیگر تیول اختصاصی دولت‌ها نیست. هم افراد و هم سازمان‌های خصوصی و تروریست‌ها، توان نقش‌آفرینی مستقیم در سیاست جهانی را یافته‌اند. فضای سایبر درعین‌حال که جایگزین فضای جغرافیایی نشده و خدشه‌ای بر مرزهای حاکمیتی کشورها وارد نساخته، عرصه‌ای برای هم‌زیستی است و تا حد زیادی آنچه را که مفهوم کشوری قدرت‌مند و برخوردار از حاکمیت و استقلال القا می‌کند، پیچیده می‌سازد. قدرت سایبری عبارت است از توانایی اخذ نتایج سخت و نرم دل‌خواه در درون و برون فضای سایبر. اکثریت کشورها درعرصه‌های هوایی و دریایی هنوز هم امکان ورود ندارند، ولی فضای سایبر این‌گونه نیست و بازیگران گوناگون‌اند. نمود پراکندگی قدرت در فضای سایبر، فراوانی بازیگران (افراد، شرکت و دولت) و کاهش نسبی اختلاف حد و دامنه قدرت آن‌هاست. مدیریت جنگ سایبری به‌منزله چشمگیرترین تهدید بالقوه

7 Nye, J.S. Jr. «The Future of Power» (2011)
8 Transition
9 Diffusion

در شرایط حاضر، از طریق نوعی بازدارندگی میان‌کشوری (گرچه متفاوت با بازدارندگی کلاسیک هسته‌ای)، ایجاد ظرفیت‌های هجومی و تمهیداتی برای پایایی شبکه و زیرساخت، در صورت ناکامی بازدارندگی، امکان‌پذیر است[۱۰].

درواقع ما در فضای سایبر با پدیده‌ای مواجه هستیم که واجد ویژگی‌هایی است که در هیچ‌یک از عرصه‌های سنتی موجود نبوده و کاملاً جدید است. این پدیده در درون رشته روابط بین‌الملل و بین نویسندگان مختلف، مباحثی در خصوص سطح استراتژیک بودن تهدیدات سایبری و مسئله بازدارندگی به وجود آورده است. برخی از نویسندگان، اهمیت موضوع را در حد تاکتیک قلم‌داد کرده و معتقدند که نیازی به ورود نظریه‌پردازان به این عرصه نبوده و مسائل این حوزه در قالب نظریات و مسائل استراتژیک موجود قابل بررسی هستند. به نظر این افراد، سایبر تنها یکی از ابزارهای نبرد بوده و نیاز نیست برای تک‌تک ابزارهای نبرد استراتژی تدوین شود. به‌عنوان مثال، اریک گارتزکه[۱۱] در مقاله‌ای در مجله «International Security» معتقد است به دلیل این‌که فضای سایبر سه ویژگی ضروری موردنظر کلازویتس، فیلسوف جنگ پروسی، را نداشته و فاقد این عناصر است (خشونت‌بار/ ابزاری/سیاسی)، نمی‌توان به آن به‌عنوان موضوعی جنگی نگریست. وی می‌گوید: «سایبر یک ضمیمه به جنگ‌های جدید است، نه یک جایگزین و تا زمانی که جنگ به صحنه زمین نیاید، معلوم می‌شود که مسئله زیاد مهم نیست» (Gartzke 2013). و در جای دیگری از مقاله می‌گوید: «در صورت عدم برخورداری از قدرت در سایر حوزه‌ها، سایبر امکان پیروزی و ایجاد بی‌ثباتی را ندارد» و در نهایت، معتقد است که «نظر به موارد فوق، نبرد سایبری شایستگی بررسی ذیل موضوعات استراتژیک امنیت بین‌الملل را ندارد». در طرف دیگر این مباحثه نیز گروه دیگری از اندیش‌مندان قرار دارند. به‌عنوان مثال، لوکاس در مقاله‌ای در «International Security» می‌گوید: «برخی از جنبه‌های سایبر قادر به تطابق با چارچوب‌های امنیت سنتی است و برخی دیگر برای آن چالش ایجاد می‌کنند؛ از جمله: گسترش تهدید غیرفیزیکی بر امنیت ملی، توان‌مندی بازیگران غیردولتی در ایجاد بحران دیپلماتیک، از بین رفتن تمایز میان جنگ محلی و جنگ از راه دور، نفوذ دشمنان ناشناس و غیره. شکاکان این ویژگی‌های امنیت در عصر حاضر را در نظر نمی‌گیرند و فقط می‌خواهند موضوع را با استفاده از منطق سابق توضیح دهند. آنها به دنبال این هستند تا تأثیر سلاح

10 Nye, J.S. Jr. «The Future of Power» (2011), Ch.5
11 Erick Gartzke

مجازی را تا سطح مسائل متعارف کشورداری پایین بیاورند؛ چراکه فکر می‌کنند با این کار به‌عنوان خدمت‌کاران راستین رشته روابط بین‌الملل معرفی خواهند شد. کارل فون کلازویتس از اهمیت تکنولوژی در عصر خود غفلت کرده است. این اشتباه است که فکر کنیم مفاهیم او قادر به رمزگشایی از تکنولوژی جدید عصر ما هستند» (Lucas, 2013).

در مقاله‌ای دیگر، تیموتی جونیو در مجله Strategic Studies، در موافقت با استحقاق این عرصه و در جهت بذل توجه و ایجاد مکتب سایبر در مطالعات امنیت بین‌الملل استدلال می‌کنند[۱۲]. تأکید وی بر اشتباه بودن این نظر شکاکان است که «جنگ سایبری رخ نخواهد داد» [۱۳]. سایبر بیشتر از سایر تکنولوژی‌ها شانس شرکت در عملیات تهاجمی را دارد. تامس رید[۱۴] و آدام لیف[۱۵] (نویسنده مقاله Cyber war: a new Absolute Weapon) ابراز نموده‌اند که نبرد سایبری نداریم. ولی بدون اتکا به نظریه، این نتیجه‌گیری را ارائه داده‌اند. در صورت استفاده از نظریه، نتیجه متفاوتی به دست خواهد آمد. سلاح‌های سایبری بسیاری از سازوکارهای تشدید خشونت را دارند. در سازوکارهای سنتی شروع عملیات بسیار مشکل و پرهزینه بود، ولی در این‌جا آسان و کم‌هزینه است. لذا می‌بایست به سایبر توجه بیش‌تری شود. نظریه Principal-agent توضیح می‌دهد که چگونه اختلاف انگیزه‌ها و ترجیحات افراد و سازمان‌ها می‌تواند به بروز جنگ در راستای منافعی خاص دامن بزند و با توجه به طبیعت مسائل سایبری، شروع نبرد سایبری بسیار محتمل و آسان‌تر است (و این در حالی است که شروع عملیات نظامی متعارف به دلیل هزینه بالا به‌راحتی قابل انتخاب نیست). پس «جنگ سایبری رخ خواهد داد». رید و لیف دولت‌ها را بازیگرانی منطقی و یک‌پارچه تصور کرده‌اند و به پیچیدگی‌های فرآیندهای داخلی جهت انتخاب سیاست خارجی توجه نمی‌کنند. ایشان به مقایسه تکنولوژی‌های هسته‌ای و سایبری پرداخته و اعلام می‌کند که در مقایسه با سلاح‌های هسته‌ای، شروع تهاجم سایبری بسیار سهل‌الوصول است. به دلیل ماهیت تهاجمی سایبر، سازمان‌های سایبری نظامی بسیار تهاجمی‌تر از سایر بروکراسی‌ها رفتار می‌کنند.

باوجود این اختلافات، اخیراً اندیش‌مندان مسائل استراتژیک با پذیرش اهمیت فضای سایبر، در حال حرکت به سمت نظریه‌پردازی مسایل سایبر بوده و مطالعات سایبر ذیل رشته امنیت بین‌الملل در حال تئوریزه کردن جنبه‌های مختلف موضوع است (Lucas, 2013).

12 Timothy Junio, «How Probable is Cyber War: Bringing IR theory Back In to the Cyber Conflict Debate», The Journal of Strategic Studies, March 2013

۱۳ عنوان مقاله‌ای از توماس رید که استدلال می‌کند سایبر در حد تاکتیک است (Cyber War will not Take Place).

14 Thomas Rid

15 Adam Liff

۲. چارچوب نظری

رئالیسم تهاجمی[16] به زیرشاخه‌ای از نظریه نئورئالیسم[17] در روابط بین‌الملل اشاره دارد که از نظریات کنت والتز[18] در رئالیسم ساختاری[19] منشعب شده است. رئالیسم کلاسیکِ متفکرانی مانند هانس مورگنتا بر طبیعت انسانی متمرکز بود. والتز تمرکز رئالیسم را بر نظام بین‌الملل منتقل کرد که در آن ساختار آنارشیک نظام بین‌الملل، کشورها را وامی‌دارد تا در جهت بقای خود اقدام به افزایش قدرت نمایند. قدرت که با توزیع نسبی توانمندی‌های نظامی و اقتصادی در سطح نظام اندازه‌گیری می‌شود، تنها تضمین‌کننده امنیت کشورها محسوب می‌شود. به همین ترتیب، نظریات رئالیسم تهاجمی و تدافعی نیز زیرشاخه‌هایی از نظریه والتز هستند.

این مقاله به دنبال کاربست نظریه رئالیسم تهاجمی جان مرشایمر بر نبرد سایبری و بازدارندگی آن است. دلیل این انتخاب، طبیعت تعارض‌آمیز این عرصه است. رئالیسم تهاجمی اشعار می‌دارد که قدرت‌های بزرگ در جهت تضمین امنیت خود، همواره به دنبال بیشینه‌سازی درصد سهم خود از قدرت جهانی‌اند. قدرت فائقه بودن، بهترین راه تضمین بقاست. بنابراین دولت‌ها در جهت تهاجم از یکدیگر سبقت می‌گیرند[20]. مرشایمر پنج مفروضه را در خصوص نظام بین‌الملل برمی‌شمرد که باعث می‌شوند دولت‌ها سیاست‌های تهاجمی در پیش گیرند: ۱. آنارشی اصل نظم‌دهنده نظام بین‌الملل است؛ ۲. قدرت‌ها به دنبال کسب قابلیت‌های نظامی هستند؛ ۳. کشورها هیچ‌گاه نمی‌توانند در مورد نیات دیگران اطمینان یابند؛ ۴. بقا مهم‌ترین هدف کشورهاست و ۵. کشورها بازیگران خردمند هستند (Mearsheimer, 2001). در شرایط عدم امکان اطمینان به دیگران و لزوم زندگی در شرایط خودیاری، کشورها کسب قدرت بیشتر را به‌عنوان بهترین راه تضمین بقای خود خواهند یافت. پس به دنبال بیشینه‌سازی قدرت خود و تغییر موازنه قدرت (حتی به قیمت افزایش سوء ظن و خصومت دیگران) خواهند بود.

رئالیسم تهاجمی چهارچوبی مفید جهت بررسی تعدادی از مسائل مرتبط با امنیت ملی در فضای سایبر مهیا می‌کند. با وجود این، امکان ایضاح کلیه مسائل این حوزه را نداشته و برخی از مفروضه‌های پنج‌گانه مرشایمر در این فضا جاری نیستند؛ لذا نیازمند چارچوب‌های دیگری نیز هستیم. این نظریه بیشتر در جهت توضیح نظام بین‌المللی، شامل قدرت‌های بزرگ و کشورها (دولت-ملت‌ها) بوده و در صورت نیاز به تحلیل روابط سایبری واحدهای

16 Offensive Realism
17 NeoRealism
18 Kenneth Waltz
19 Structural Realism
20 John J. Mearsheimer, The Tragedy of Great Power Politics

ملی در نظام بین‌الملل، می‌تواند تا حدود زیادی مفید واقع گردد. درحالی‌که در موضوعات سایبری، همان‌گونه که خواهیم دید، بازیگران ضعیف‌تر و حتی افراد و گروه‌های غیردولتی نیز قادر به ایجاد اخلال در بازدارندگی هستند. به همین دلیل، از جمله مسائل غیرقابل کاربست این نظریه، موضوعات پراکندگی قدرت و حضور بازیگران زیر-ملی، هنجارها و همکاری‌های بین‌المللی در عرصه سایبر است که برای تحلیل آن‌ها می‌توان از سایر نظریه‌ها بهره جست. به‌عنوان نمونه، می‌توان از نظریه نئولیبرالیسم و نهادگرایی جدید نام برد. یکی از مهم‌ترین گزینه‌های پیش رو در زمینه مهار مخاطرات فضای سایبر، همکاری بین‌المللی در قالب موافقت‌نامه‌ها و نهادهای بین‌المللی است که مجموعه رئالیسم ابزار مناسبی جهت تحلیل دقیق این‌گونه مسائل در اختیار قرار نداده و لذا می‌توانیم از نهادگرایی جهت ایضاح آن استفاده کنیم. یکی دیگر از نارسایی‌های تحلیلی مجموعه رئالیسم، نگاه به دولت به‌عنوان تنها بازیگر حاضر در عرصه معادلات بین‌المللی و عدم شناسایی دقیق نقش گروه‌های زیر-ملی و غیردولتی است. درحالی‌که در موضوع سایبر- همان‌گونه که در این مقاله خواهیم دید- یکی از مهم‌ترین نیروهای تهدیدکننده نظم بین‌الملل، گروه‌های غیردولتی فروملی یا فراملی هستند. بارزترین عنصر شکل‌دهنده به این گروه‌ها، هویت است. این هویت می‌تواند در اشکال مختلف (دینی، ملی، زبانی و ...) موجد همکاری افراد در قالب یک نیروی هماهنگ شده و با بر هم زدن منطق آنارشی، موجب ایجاد بی‌نظمی بین‌المللی گردد که جهت بررسی این موضوع، می‌توان از نظریه سازه‌انگاری استفاده کرد. لذا، در مجموع می‌توان گفت که فهم موضوعات حوزه سایبر نیازمند رویکرد تلفیقی به نظریه‌های روابط بین‌الملل است.

۱-۲. روش پژوهش

این مقاله از روش توصیفی-تحلیلی برای پاسخ به سؤال پژوهش بهره می‌برد. در این روش، محقق در ابتدا تلاش می‌کند تا با استخراج اطلاعات از منابع گوناگون و ارائه آن‌ها، صرفاً به توصیف شرایط بپردازد. در بخش بعد، با استفاده از استدلال و با توجه به توصیفات ارائه‌شده، به توضیح و تشریح این مقوله می‌پردازیم و به این ترتیب در جهت تبیین فرضیه خود اقدام می‌کنیم. به همین ترتیب، در این پژوهش نیز تلاش شده تا در ابتدا نظریه بازدارندگی هسته‌ای و عناصر و سازوکارهای آن مورد اشاره قرار گیرد و سپس با استفاده از تبیین و استدلال، امکان کاربرد نظریه بازدارندگی هسته‌ای در فضای سایبر بررسی شود. جمع‌آوری داده‌ها از طریق مطالعات کتابخانه‌ای و اسنادی است و تحلیل فرآیند به‌صورت نظری انجام خواهد شد.

۳. نظریه بازدارندگی هسته‌ای و عناصر و سازوکارهای آن

بازدارندگی در تاریخ سیاست بین‌الملل اصطلاحی عمومی است و تا قبل از جنگ جهانی دوم به‌عنوان اصلی بدیهی مورد استفاده بود. به‌محض آغاز جنگ سرد تحلیل‌گران و سیاست‌مداران این اصطلاح را گرفتند و از آن در جهت بنای مفهومی برای جلوگیری از جنگی دیگر بهره برده و در پی آن، چارچوب‌های نظری بازدارندگی در سیاست بین‌الملل و استراتژی‌های ملی بازدارندگی پدید آمدند (Morgan, 2010). پاتریک مورگان، استاد دانشگاه ایالتی واشنگتن و متخصص امنیت ملی، در کتاب «بازدارندگی» می‌نویسد: «بازدارندگی مستلزم تحت تأثیر قرار دادن رفتار انسانی از طریق تهدید وی است. بازدارندگی مستلزم تهدید به استفاده از زور برای جلوگیری از کاربرد نیروی قهریه توسط شخص دیگری است».

بازدارندگی به‌عنوان یک استراتژی، در پی آن است که متخاصمان را به نحوی تشویق و ترغیب کند تا در پیگیری منافع خویش از انجام برخی اقدامات پرهیز کنند، و در چارچوب سلاح‌های استراتژیک نشان می‌دهد که هزینه‌ها و مخاطراتی که ملازم با یک تجاوز نظامی است، فراتر از دستاوردهایی است که معمولاً انتظار می‌رود از آن حاصل شود. بازدارندگی هم‌چنین واجد جنبه‌های روانی است. ژنرال بوفر[۲۱]، استراتژیست معروف فرانسوی، می‌گوید: «استراتژی بازدارندگی یک فرآیند روانی است که در آن زور جای مهمی دارد، ولی دارای اهمیت انحصاری نیست. به عبارت دیگر، بازدارندگی دشمن را از نظر فیزیکی دفع نمی‌کند، بلکه به لحاظ روانی از تجاوز او جلوگیری می‌کند» (Beaufre, 1964). هنری کسینجر[۲۲] در زمینه مفهوم بازدارندگی و بعد روانی آن می‌گوید: «همان‌طور که قدرت به طرز وحشتناکی رشد کرده، به‌صورت انتزاعی نامحسوس و اغفال‌کننده نیز درآمده است. بازدارندگی یک سیاست مسلط نظامی است، لیکن بیش از هر چیز وابسته به ملاک‌های روانی است. در این استراتژی سعی می‌شود تا با تجلی خطرات غیرقابل تحمل، طرف مخالف را از ارتکاب به عمل بازداشت. پیروزی این سیاست، بستگی به آگاهی کامل از محاسبات طرف مخالف دارد. بلوفی که جدی گرفته می‌شود، به‌مراتب مؤثرتر از تهدیدی است که به‌عنوان یک بلوف تلقی می‌شود. برای مقاصد سیاسی ،میزان قدرت مؤثر نظامی یک کشور، همان ارزیابی یک کشور دیگر از آن قدرت است. پس ملاک‌های روانی کم‌اهمیت‌تر از نیروهای واقعی نیستند» (Kissinger, 1957).

در بازدارندگی، معمولاً عمل متقابل یا تلافی‌جویانه نقش اساسی دارد. پیام بازدارندگی

21 Deterrence and Strategy (London: Faber, 1965 [Dissuasion et stratégie Paris, Armand Colin, 1964])

22 **Nuclear Weapons and Foreign Policy** (1957)

باید به‌گونه‌ای باشد که چنان‌چه دشمن جنگ را آغاز کند، بهای بسیار سنگینی را بپردازد. پس بازدارندگی بین دو دولت الف و ب، عبارت است از قدرت تهدید از ناحیه الف علیه ب به‌منظور پیش‌گیری از آغاز جنگ از ناحیه ب، به‌نحوی‌که در فقدان این قبیل تهدیدات، ب بتواند به جنگ مبادرت ورزد. البته باید متوجه بود که بین بازدارندگی از طریق انکار[۲۳] و بازدارندگی از طریق عمل متقابل و تلافی[۲۴] تفاوت‌هایی وجود دارد. «انکار» یعنی هرگونه پیش‌گیری از حمله؛ مانند استفاده از فناوری و توانایی فنی برای ساقط کردن کلاهک‌های هسته‌ای در هنگام حمله، ولی «تلافی» یعنی تهدید به عمل متقابل (عسگر خانی ۱۳۷۷).

در سیاست بین‌الملل، بازدارندگی به تلاش‌هایی اطلاق می‌شود که طی آن یک کشور از طریق تهدید به وارد آوردن ضربه قوی متقابل، به دنبال این است که از حمله دیگر کشورها جلوگیری کند. تهدید ذکرشده می‌تواند از طریق دو سازوکار عمل نماید: در سازوکار اول، این تهدید از طریق دفاع قدرت‌مندی که می‌تواند عملیات طرف مقابل را خنثی یا بسیار پرهزینه نموده و یا برد پرهزینه‌ای را نصیب او نماید، عملیاتی می‌شود که به آن انکار[۲۵] گفته می‌شود. در سازوکار دوم، این تهدید می‌تواند از طریق تلافی[۲۶] اعمال شود (Morgan, 2010). در دوران جنگ سرد با توجه به ماهیت سلاح‌های هسته‌ای و دفاع‌ناپذیر بودن این تسلیحات، عمدتاً سازوکار تلافی مورداستفاده قرار می‌گرفت، ولی با این حال در برخی موارد نیز از انکار استفاده می‌شد. هم‌چنین در شرایطی هر دوی این سازوکارها در دستور کار قرارگرفته و مفید واقع می‌شدند. در خصوص نحوه عملکرد این سازوکار، در ادامه مقاله توضیحات مفصل‌تری ارائه خواهد شد.

۴. مشخصات فضای سایبر

از ابتدای قرن حاضر، شبکه اینترنت رشد روزافزونی کرده، به‌نحوی‌که در سال ۲۰۱۶ در حدود ۴ تریلیون دلار از اقتصاد جهانی به این بستر وابسته بوده و این شبکه نیمی از جمعیت جهان را به هم متصل نموده است. در مقام مقایسه، باید گفت که ۲۰ سال پیش در جهان تنها ۱۶ میلیون کاربر اینترنت (کمتر از نیم در صد جمعیت جهان) وجود داشت. ترافیک داده (data) در یک دهه گذشته ۴۵ برابر رشد داشته و وابستگی متقابل ایجادشده، ظرفیت جدیدی در جهت ناامنی جهانی مهیا کرده است. پیش‌بینی می‌شود که در ۵ سال آینده، ۲۰ میلیارد دستگاه در قالب اینترنت اشیا[۲۷] (IOT) به شبکه افزوده شده و محدوده اهداف بالقوه

23 Deterrence by Denial
24 Deterrent by Punishment
25 Denial
26 Punishment
۲۷ Internet of Things: روند موجود به گونه‌ای است که با هدف بهبود کنترل، درآینده کلیه لوازم خانگی و

جهت حملات سایبری به‌شدت افزایش یابد (Naughton, 2016). در این میان، وابستگی روزافزون کشورها به فضای سایبر باعث آسیب‌پذیری هر چه بیشتر آن‌ها در این عرصه جدید خواهد شد. تهدیدات سایبری در سال ۲۰۰۷ در لیست تهدیدات بزرگ امنیت ملی جایی نداشت. این در حالی است که در سال ۲۰۱۵ اولین رتبه را در لیست مزبور به خود اختصاص داده است (Clapper, 2016)

از سوی دیگر، فضای سایبر محل مناسبی جهت نشو و نمای آشوب سیاسی و بی‌ثباتی استراتژیک است. این فضا ویژگی‌هایی دارد که آن را از عرصه‌های سنتی متمایز کرده و امکانات مناسبی جهت ایجاد هرج‌ومرج در اختیار قرار می‌دهد. عمده ویژگی‌های آن به شرح زیر قابل دسته‌بندی است:

- غلبه حمله بر دفاع: بر اساس نظریه رئالیسم تهاجمی، دولت‌ها میل دارند تا در جهت تضمین امنیت خود، در تهاجم از یکدیگر سبقت بگیرند. عرصه سایبر نیز فضایی است که در آن حمله بر دفاع غلبه دارد (Libicki 2012). در واقع شرایط به‌گونه‌ای است که امکانات موجود برای حمله به‌مراتب بیشتر از دفاع است. در عرصه‌های سنتی، شروع یک حمله (زمینی، هوایی یا دریایی) نیاز به زمینه‌چینی و اخذ مجوز از بوروکراسی داشته و عواقب بین‌المللی زیادی بر حمله مترتب است. درحالی‌که در فضای سایبر، شروع حمله بدون نیاز به اقدامات اولیه آن‌چنانی و با هزینه ملی و بین‌المللی پایین صورت می‌گیرد. از طرفی، افزایش حجم و پیچیدگی‌های روزافزون نرم‌افزارها، در واقع حفره‌های امنیتی آن‌ها را افزایش داده و به مهاجمان اجازه می‌دهد که از طریق این حفره‌ها (در اصطلاح فنی به این حفره‌ها Vulnerability Zero-Day گفته می‌شود) نفوذ کنند. این در حالی است که سیستم‌های قربانی هیچ‌گونه اطلاعی از این موضوع ندارند.بنابراین، در وضعیت بی‌اطلاعی مدافعین، امکان دفاع از بین می‌رود. در واقع ذات مسئله به‌گونه‌ای است که امکان دفاع برای قربانی بسیار محدود است.

موضوع غلبه حمله بر دفاع، معمای امنیت[۲۸] را به سه روش تشدید می‌کند (Lucas, ۲۰۱۳). در اولین وجه، فهم غلبه حمله بر دفاع، مسابقه تسلیحات سایبری بین دولت‌هایی را که بر اساس نظریه رئالیسم تهاجمی به دنبال کسب برتری در این فضای استراتژیک هستند، افزایش می‌دهد. هیچ‌گونه کنترلی بر تولید و انتقال سلاح‌های سایبری وجود ندارد. دومین وجه تشدید معمای امنیت این است که دارندگان این سلاح‌ها قطعاً از آن‌ها بهره‌برداری

دستگاه‌ها و خودروها به اینترنت وصل خواهند شد.

28 Security Dilemma

خواهند نمود. برخلاف سلاح‌های هسته‌ای، در شرایط کنونی این‌ها سلاح‌هایی برای استفاده کردن هستند. سومین وجه مسئله این است که در عرصه سایبر، نظم دفاع-حمله بر هم می‌خورد. در عرصه سنتی، عبور هر کشور از مرزهای طرف مقابل، حمله تلقی می‌شد، ولی در فضای سایبر این‌گونه نیست و حساسیت‌ها پایین‌تر است. هم‌چنین، موضوعی به‌نام دفاع فعال وجود دارد که طی آن شما می‌توانید در جهت دفاع و جلوگیری از حمله سایبری، اقدام به ورود به سیستم طرف مقابل کرده و آن را مختل نمایید. لذا در این‌جا هرکسی که وارد شبکه طرف مقابل می‌شود، می‌تواند مدعی اقدام پیش‌گیرانه شود.

- مشکل انتساب[۲۹]: یافتن منبع حمله معمولاً مشکل است. چهار ویژگی درگیری سایبری، موجد این مسئله هستند. اول، تکثیر بیش‌ازحد سلاح‌های سایبری به معنی این است که تعداد حمله‌کنندگان ممکن بسیار زیاد است. دوم، یافتن مکان یا هویت حمله‌کننده چالش بزرگی است، زیرا فضای سایبر امکانات زیادی جهت مخفی کردن مکان و هویت افراد در اختیار قرار می‌دهد. سوم، به دلیل امکان عبور مهاجم از شبکه کشورهای مختلف، یافتن او مستلزم همکاری مؤثر بین‌المللی است که کار را مشکل می‌کند و چهارم، با فرض امکان‌پذیری همه موارد فوق، یافتن مهاجم آن‌قدر زمان‌بر است که ممکن است ماه‌ها طول بکشد و یا سال‌ها به طول انجامند. مشکل عدم امکان انتساب، بازدارندگی را به‌شدت کاهش می‌دهد، چراکه زمانی که امکان شناسایی حمله‌کننده کم باشد، مهاجمان بدون ترس از عواقب آن، اقدام به حمله می‌کنند (Morgan, 2010).

- مشکل سرعت پیشرفت تکنولوژی: سلاح‌های سایبری و نرم‌افزارها با آن‌چنان سرعتی رشد می‌کنند که صرف زمان جهت شناسایی آن‌ها بیهوده است، زیرا به‌سرعت از دور خارج‌شده و سلاح‌های جدیدی جای آن‌ها را می‌گیرد. در برخی مواقع، عمر حفره‌های امنیتی[۳۰] در حد چند روز است و به‌محض کشف، توسط شرکت‌های تولیدکننده نرم‌افزار شناسایی و وصله[۳۱] می‌شوند. این در حالی است که در فضای سنتی، عمر تسلیحات به ده‌ها سال نیز می‌رسد.

- عمق استراتژیک کم: چهارمین فاکتور بی‌ثبات‌کننده در فضای سایبر، زمان کمی است که یک مدافع از لحظه کشف احتمالی حمله تا زمان اتمام آن زمان دارد. سرعت سلاح‌های سایبری، امکان دفاع را سلب می‌کند. این ویژگی جدید، حد نهایی سرعت سیستم‌های تسلیحاتی را از ۲۰ ماخ (سرعت موشک‌های بالستیک بین‌قاره‌ای) به شتاب الکترون‌ها

29 Attribution
30 Zero-Day Vulnerability
31 Patch

کاهش داده است. بنابراین، دایره زمانی عملکرد تسلیحات سایبری در حد میلی‌ثانیه است (Mallery, 2011). در این مهلت محدود، زمانی برای تصمیم‌گیری انسانی و بروکراسی سازمانی و دفاع وجود ندارد.

- مشکل پراکندگی قدرت: سهولت ورود به حوزه سایبر، به این معنی است که در این عرصه بازیگران فراوانی شامل دولت‌ها، گروه‌های غیردولتی و افراد حضور دارند (Nye, 2015). این مسئله می‌تواند ثبات استراتژیک را از سه طریق مختل کند. اولین عامل، مشکل بودن همکاری دولت‌هاست. در صورت افزایش تعداد دولت‌های دارای قابلیت سایبری، هماهنگی بین این دولت‌ها در طول زمان مشکلات عدیده‌ای ایجاد خواهد کرد. قابل ذکر است که در عرصه سنتی، تعداد کشورهای درگیر در یک جنگ مسلحانه شامل چند کشور همسایه درگیر و برخی از ابرقدرت‌ها می‌شد و در کل بسیار محدود بود، لیکن به دلیل عدم وجود مرز در درگیری‌های سایبری، کشورهایی از قاره‌های مختلف می‌توانند با عبور از مرزهای سایر کشورها مبادرت به حمله سایبری کنند. در این‌جا، حل مسائل مستلزم همکاری همه این کشورها بوده و افزایش تعداد کشورها مشکلاتی را ایجاد خواهد کرد. دومین عامل، افزایش تعداد بازیگران دولتی در درون کشورهاست (در درون یک کشور نیروهای مختلف دولتی و حاکمیتی می‌توانند در حملات سایبری مشارکت کنند). ایجاد هماهنگی بین تمامی این نیروهای داخلی به‌نحوی‌که به‌عنوان یک بدنه منسجم عمل کنند، مشکل است. به‌عنوان مثال، هرچند آمریکا نیروی سایبری خود را در سال ۲۰۰۹ ایجاد کرد، ولی قدم‌های اولیه برای استانداردسازی عملیات سایبری بین واحدهای عملیاتی، از سال ۲۰۱۲ شروع شد (Zachary, 2012). سومین عامل تشدید بی‌ثباتی، پراکندگی قدرت در خارج از دولت است. باوجود این‌که دولت قوی‌ترین بازیگر عرصه سایبری است، بااین‌حال تنها بازیگر نیست. تکنولوژی جدید بازیگران مختلفی ازجمله گروه‌های تندروی مذهبی، فعالین سیاسی، گروه‌های خلاف‌کار و اشخاص را قدرت‌مند کرده است. حملات سایبری علیه استونی و گرجستان، سهولت امکان استفاده شهروندان از سلاح سایبر جهت تحمیل صدمات اقتصادی و تاکتیکی در خارج از مرزهاشان را نشان داد. ویروسی که در سال ۲۰۰۰ توسط یک نوجوان فیلیپینی ساخته شد، از هر ۱۰ کامپیوتر کره زمین، به یک کامپیوتر آسیب رسانده و صدمات زیادی به پنتاگون وارد کرد.

۵. بازدارندگی سایبری[۳۲]

انقلاب تکنولوژی در برهه‌های مختلف تاریخ بشر رخ داده و اندیش‌مندان هر عصر تلاش کرده‌اند واقعیت‌های جدید را وارد استراتژی کرده و آن را تئوریزه کنند. بنا به نظر جوزف نای، در مقایسه با سال‌های اولیه انقلاب تکنولوژیکی هسته‌ای، مطالعات استراتژیک فضای سایبر، از نظر مفاهیم مربوطه معادل دهه ۵۰ است[۳۳]. ریچارد کلارک و رابرت ناک دو تن از اولین اندیش‌مندان حوزه امنیت سایبری، اعتقاد دارند که «از بین تمام مفاهیم استراتژی هسته‌ای، بازدارندگی کمترین امکان را برای انتقال به نبرد سایبر دارد»(Clarke, 2010). فرمول‌بندی یک استراتژی مؤثر در عصر سایبر، نیازمند فهمی گسترده‌تر و چندبعدی از مفهوم بازدارندگی بوده و اشتباه است حوزه سایبر را تنها ببینیم. نیاز نیست که پاسخ یک حمله سایبری را تنها با ابزار سایبری ارائه دهیم. بازدارندگی سایبری به این معناست که در پاسخ به یک حمله سایبری می‌توانیم از طریق تمامی عرصه‌ها پاسخ دهیم. در استراتژی سایبری آمریکا در ۲۰۱۱ تصریح شده است که آمریکا حق استفاده از کلیه ابزارهای دیپلماتیک، اطلاعاتی، نظامی و اقتصادی را برای خود محفوظ می‌داند[۳۴].

در عرصه سایبر، دفاع بسیار مشکل است و این مسئله ما را به سمت بازدارندگی سوق می‌دهد. پنج مانع در مسیر دفاع سایبری وجود دارد (Lucas, 2013): اولین مانع، غیرقابل‌پیش‌بینی و غیرقابل‌کشف بودن حمله است. چون حمله از طریق حفره‌های امنیتی[۳۵] انجام می‌شود که هنوز توسط شرکت‌های امنیت سایبری و ویروس‌یاب‌ها کشف نشده‌اند. قربانی از وجود آن خبری ندارد تا بتواند پیش‌بینی یا کشف حمله کند. به‌عنوان مثال، گفته می‌شود عامل‌های استاکس نت به مدت سه سال در سیستم‌های ایران مقیم بوده و کارشناسان ایران از وجود آن‌ها اطلاعی نداشته‌اند (Lucas, 2013). دومین مانع در مسیر دفاع سایبر، انکار نتایج دفاع است. همان‌گونه که در بخش‌های قبلی مورد اشاره قرار گرفت، نتیجه دفاع در فضای سایبر بسیار محدود است. سومین مشکل، وجود سطوح پیچیده دفاع است. همان‌گونه که اشاره شد، پیچیده شدن روزافزون سیستم‌ها، به معنای ازدیاد راه‌های نفوذ نیز هست. با افزایش حجم نرم‌افزارها در دنیای اپلیکیشن‌ها، در کنار قابلیت‌های بیشتر و ظاهر زیباتر، در واقع دفاع نیز سخت‌تر و پیچیده‌تر می‌شود. چهارمین مانع، چندتکه شدن

32 Cyber Deterrence
33 Nye, J.S. Jr. «The Future of Power»(2011), Ch.5
34 Strategy for Cyberspace: Prosperity, Security and Openness in a networked world», (Washington, D.C.: White House, May 2011) White House, «International
35 Zero-Day vulnerability

دفاع است. در حال حاضر بخش اعظم شبکه‌های حساس کشورها توسط بخش خصوصی اداره می‌شوند و این بدین معنی است که در هنگام دفاع می‌بایست بین بخش‌های مختلف دولتی و خصوصی هماهنگی به وجود بیاید و این بر مشکلات خواهد افزود. مشکل پنجم، ریسک‌های زنجیره تأمین است. در دنیای کنونی هیچ کشوری زنجیره تأمین اقلام سایبری خود را به‌صورت کامل در دست نداشته و ضروری است تا بخشی از این تجهیزات از خارج از کشور تأمین شوند. در هر مرحله‌ای از این زنجیره تأمین، سازمان‌های اطلاعاتی خارجی می‌توانند بخشی از سیستم‌ها را بدون اطلاع کشور هدف آلوده کرده و درنتیجه بدافزارهای موردنظر را وارد شبکه آن کنند. پنج عامل برشمرده‌شده فوق‌الذکر، دفاع را در فضای سایبر به‌شدت پیچیده و در اکثر مواقع غیرممکن می‌نمایند.

مایک مولن رئیس ستاد مشترک ارتش آمریکا می‌گوید: «ما در حال ورود به وقایع فاجعه‌باری هستیم. برخی از این سلاح‌ها (سایبری) ساخته شده و در حال رسیدن در دست گروه‌هایی است که به دنبال تغییر نظم جهانی هستند»[۳۶]. همه می‌دانیم که سیاست بین‌الملل در غیاب یک اقتدار محدودکننده ظهور می‌یابد. این عدم وجود قدرت مرکزی موجد رقابتی دائمی و خشونت موردی بین بازیگرانی می‌شود که برای امنیت رقابت می‌کنند. ویژگی مهم آنارشی وجود درگیری نیست، بلکه وجود نظم است. در جهان سنتی، منطق آنارشی موجد ثبات می‌شد. تغییر تکنولوژی این چارچوب سیاسی جامعه بین‌الملل را بر هم می‌زند. گروه‌هایی قدرت می‌یابند که دغدغه دولت‌ها مبنی بر حفظ نظم باهدف بقا را نداشته و مکانیزم موجود را متزلزل می‌کنند. در واقع فضای سایبر یک محیط ماقبل آنارشیک ایجاد کرده است. این محیط جدید فاقد خطوط راهنمایی است که در فضای سنتی وجود داشت و رفتارهای بازیگران را قاعده‌مند و محدود می‌کرد (Kello, 2014).

نظریه بازدارندگی در بخش‌های قبلی توضیح داده شد و نیازمند توضیح مجدد نیست، اما به جهت لزوم ورود به مبحث بازدارندگی سایبری و برجسته نمودن برخی عناصر این نظریه که در فضای سایبر می‌توانند به کار بسته شوند، مورد اشاره محدود و گذرا قرار می‌گیرد. توماس شلینگ هنگامی‌که در کتاب خود، *The Strategy of Conflict*، در سال ۱۹۶۰ از بازدارندگی صحبت می‌کند، بر نقش تهدید تأکید دارد، اما در سال ۱۹۶۶ در کتاب دیگری تعریف گسترده‌تری از آن ارائه می‌دهد: «جلوگیری کردن از کاری با ترس از عواقب آن». گلن اسنایدر یکی دیگر

36 Alexander Fitzpatrick, «Cybersecurity experts need to meet growing demand,» Washington Post, May 29, 2012

ازنظریه‌پردازان کلاسیک، بازدارندگی را گسترده‌تر از منصرف کردن دیگران با تهدید تلافی یا قول جایزه تعریف می‌کند. او می‌گوید معنای بازدارندگی بسیار گسترده‌تر از آن است که مردم می‌پندارند و صرفاً بر نیروی نظامی تکیه ندارد. بنابراین، می‌توان گفت که ترس از طرد شدن نیز در معنای بازدارندگی مستتر است. پس، در بازدارندگی عنصر روانشناسی نیز بسیار اهمیت دارد و در صورت عدم امکان فهم یکسان طرفین، شکست خواهد خورد. مفهوم بازدارندگی از زمان‌های قبل از بمب هسته‌ای هم وجود داشته و اکنون نیز در صورت تغییر درک ما و گسترش مفهوم، می‌توان آن را به فضای سایبر اطلاق کرد (Nye, 2017).

همان‌گونه که قبلاً ذکر شد، بازدارندگی کلاسیک دو سازوکار اصلی داشت: تهدید مؤثر تلافی و انکار نتایج اقدام. انکار به این معنی است که اقداماتی انجام دهیم تا مهاجم به این درک برسد که در صورت اقدام به حمله، نمی‌تواند تأثیر آن‌چنانی بر جای گذاشته و نتیجه‌ای برای او در بر ندارد. همان‌گونه که گفته شد، در دوران سلاح‌های هسته‌ای و در قالب نظریه بازدارندگی هسته‌ای، به دلیل قدرت بالا و تخریب گسترده سلاح‌های هسته‌ای، انکار کم‌اثر بود و نمی‌توانست در بازدارندگی نقش‌آفرینی کند. درنتیجه، بازیگران به اجبار به سمت تلافی سوق داده شدند. به این معنا که بر مبنای MAD[۳۷] (نابودسازی تضمینی دوجانبه)، هر یک از ابرقدرت‌ها به‌قدری سلاح داشته و آن را در جغرافیای وسیعی پخش کرده بودند که در صورت دریافت ضربه اول[۳۸]، قابلیت پاسخ به آن و اعمال ضربه دوم[۳۹] را دارا بودند. ترس از تلافی و نابودی تضمینی، باعث خودداری طرفین از حمله می‌شد. در حادثه خلیج خوک‌ها در سال ۱۹۶۳، این سازوکار کارایی خود را به‌خوبی نشان داده و از بروز جنگ هسته‌ای جلوگیری کرد.

در فضای سایبر، با توجه به تفاوت‌هایی که در بخش‌های قبلی مقاله مورد اشاره قرار گرفت، موضوع اندکی متفاوت است. در ابتدای تفکر در مورد استراتژی بازدارندگی سایبری و به دلیل مشکل انتساب[۴۰] که در آن امکان شناسایی حمله‌کننده محدود است، امکان تلافی بسیار ضعیف می‌شود، چراکه تنبیه زمانی اتفاق می‌افتد که بتوان حمله‌کننده را شناسایی کرد. ولی با توجه به عدم امکان شناخت مهاجم، مکانیزم تلافی کارایی خود را از دست داده و بنابراین بر اهمیت انکار افزوده خواهد شد. در سال ۲۰۱۰، ویلیام لین معاون وزیر دفاع اعلام کرد[۴۱] که «بازدارندگی ضرورتاً بر مبنای سلب امکان کسب هرگونه مزیت از حمله‌کنندگان

37 Mutual Assured Destruction
38 First Strike
39 Second Strike
40 Attribution
41 William J. Lynn III, «Defending a New Domain: The Pentagon's Cyberstrategy,» Foreign Affairs,

خواهد بود تا تحمیل هزینه از طریق تلافی»[۴۲] و استراتژی سایبری وزارت دفاع در سال ۲۰۱۱ بیشتر تأکید را به‌جای تلافی و تنبیه، بر دفاع قرار داد. دلیل این کار، وجود مشکلات در شناسایی منبع حمله بود. در نتیجه، دولت اوباما متهم شد که نتوانسته استراتژی بازدارندگی سایبری مؤثری را در پیش گیرد. این انتقادها نگاه مضیقی به بازدارندگی داشتند. پاسخ دولت این بود که نیاز نیست بازدارندگی سایبری به فضای سایبر محدود شود و استراتژی سایبری سال ۲۰۱۵ تأکید بیشتر را بر تلافی (بیشتر در خارج از فضای سایبر) قرار داد. در این بخش از مقاله، به ارزیابی تک‌تک سازوکارهای چهارگانه بازدارندگی در فضای سایبر می‌پردازیم:

۱. تلافی: همان‌گونه که ذکر آن رفت، به دلیل عدم قطعیت امکان شناسایی حمله‌کننده، تهدید به تلافی کارایی زیادی ندارد. با وجود این، این سازوکار هم‌چنان به‌عنوان یکی از مهم‌ترین بخش‌های معادله بازدارندگی در فضای سایبر باقی خواهد ماند. نردبان پاسخ‌های تلافی‌جویانِ بر اساس شدت حمله شامل اقدامات دیپلماتیک، اقتصادی، سایبری، قدرت فیزیکی و نیروی هسته‌ای خواهد بود (Libicki, 2012). پیشرفت‌های اخیر در حوزه سیستم‌های فارنزیک[۴۳] نیز کارایی این مکانیزم را افزایش داده است. استفاده آمریکا از کلیه روش‌های در دسترس در پاسخ به حمله سایبری، استراتژی ترکیبی[۴۴] پنتاگون نام دارد.

۲. انکار: مسئله عدم امکان شناسایی می‌تواند مشکلاتی را برای مکانیزم‌های تلافی و هنجار ایجاد کند. ولی مکانیزم‌های انکار و گرفتارسازی[۴۵] نیازی به شناسایی ندارند. یک دفاع سایبری خوب باید شامل چند مؤلفه باشد. یکی از این مؤلفه‌ها، نگهداری[۴۶] یک نمونه از کلیه اطلاعات موجود در یک مکان امن است تا در صورت بروز حمله سایبری و از دست رفتن اطلاعات، بتوان از اطلاعات پشتیبان استفاده نمود. مؤلفه دیگر، برگشت‌پذیری[۴۷] است. به این معنا که در صورت هرگونه حمله سایبری و بروز خرابی، بتوانیم کل سیستم را به حالت اولیه برگردانیم. استفاده از مکانیزم انکار بیشتر می‌تواند گروه‌ها و دولت‌های ضعیف را از حمله منصرف کند و دولت‌های قوی دارای آن‌چنان قدرت بالایی هستند که این روش‌ها قادر به بازداشتن آن‌ها نیستند.

۳. گرفتارسازی: استفاده از این سازوکار مستلزم درک مشترک همگان مبنی بر سودمندی

Vol. 89, No. 5 (September/October 2010), p. 99.

42 William J. Lynn, «Defending a new domain: the pentagon's cyberstrategy,» Foreign Affairs, 2010

۴۳ Forensic: سیستم‌هایی هستند که عمدتاً در اختیار پلیس بوده و جهت شناسایی مجرمان سایبری استفاده می‌شود.

44 MIX Strategy

45 Entanglement

46 Backup

47 Resilience

استفاده از اینترنت و فضای مجازی برای ایشان است. در صورت رسیدن به چنین درکی، قطعاً به دنبال استفاده غیرصلح‌آمیز از این فضا نخواهند بود. بارزترین نمونه استفاده از این سازوکار در بازدارندگی، موضوع اختلافات سایبری آمریکا و چین است. می‌دانیم که ادامه قدرت چین به اینترنت بستگی تام دارد (Nye, 2017). در واقع این سازوکار بر اساس وابستگی متقابل کار می‌کند. برخی از وابستگی‌ها دو یا چند طرفه هستند، ولی برخی دیگر سیستمی بوده و در اثر اخلال در سیستم، منافع از دست خواهند داد. در این حالت کشورها به دنبال ثبات سیستمی خواهند رفت. چین به دلیل وابستگی سیستمی به اینترنت، اقدامات بی‌ثبات‌ساز در اینترنت را پایان بخشید. این سازوکار برای همه کشورها کارایی ندارد. به‌عنوان مثال کشوری مانند کره شمالی را نمی‌توان با این مکانیزم بازداشت.

۴. هنجار: چهارمین سازوکار، هنجارها و تابوها هستند. مسئله شناسایی در عملکرد این سازوکار نیز اهمیت پیدا می‌کند. در صورتی که بتوان با تصویب قوانین بین‌المللی، عملیات سایبری را به‌صورت تابو درآورد، آنگاه شکستن تابو برای کشورها هزینه خواهد داشت. بازدارندگی از این طریق، قدرت نرم[۴۸] کشورها را هدف قرار می‌دهد. هنجارها با گذشت زمان شکل می‌گیرند و هنجارسازی مراحلی دارد که در زمینه سایبر، در مراحل اولیه آن قرار داریم.

آمریکا و قدرت‌های بزرگ اعلام نموده‌اند که از نظر آنان فضای سایبر نیز مشمول قوانین درگیری مسلحانه (LOAC)[۴۹] خواهد شد. بر اساس این قوانین، تمایز بین اهداف نظامی و غیرنظامی و تناسب در پاسخ می‌بایست رعایت گردد (Nye, 2017). در همین زمینه، مایکل هایدن از رؤسای پیشین سازمان اطلاعات مرکزی می‌نویسد: «در جعبه ابزار ما حجم وسیعی از سلاح‌های سایبری انبار شده است، اما استفاده از همگی آن‌ها زیبا نیست. این تسلیحات باید شاهد اعمال یک سری تغییرات باشند تا بتوانند نیازهای کاربردی و حقوقی را پوشش دهند. چیزی که ما نیاز داریم این است که این تسلیحات بتوانند استانداردها و قوانین جنگ مسلحانه را بپذیرند»[۵۰]. بسیاری معتقدند که آمریکا با توجه به این مسائل، در سال ۲۰۰۳ و قبل از حمله به عراق، از به‌کار بردن قابلیت‌های سایبری جهت ضربه به زیرساخت‌های مالی عراق خودداری کرده و یا در سال ۲۰۱۱ در جریان کمپین براندازی قذافی، سیستم‌های ضدهوایی لیبی را غیرفعال نکرده است.

در ارزیابی کلی، می‌توان گفت که هیچ‌یک از این سازوکارها کامل نیستند، ولی جمعاً در

48 Soft Power
49 Lows of Arms Conflict
50 Hayden CSM 2016

کنار هم می‌توانند حملات سایبری را کاهش داده و محیطی امن‌تر ایجاد کنند. همان‌گونه که قبلاً ذکر شد، جرویس از سه دوره نظریه‌پردازی بازدارندگی در زمان جنگ سرد صحبت به میان می‌آورد. نظریه‌پردازی در بازدارندگی در عصر سایبر هنوز در مرحله اول‌اش قرار دارد (Nye, 2017). بنابراین، با پیشرفت تکنولوژی و فعالیت نظریه‌پردازان، ممکن است بخش‌هایی از مطالب گفته‌شده تغییر یافته و نظریات کامل‌تری ارائه شود. موضوع مهم قابل‌ذکر این است که بازدارندگی سایبری در خصوص دولت‌ها بهتر کار خواهد کرد، چراکه دولت‌ها خود را ملزم به حفظ نظم بین‌المللی دانسته و بر اساس وابستگی متقابل، قابل بازداری هستند. سایر بازیگران عرصه سایبر، مانند افراد یا گروه‌های مختلف با انگیزه‌های مختلف که اساساً به دنبال بر هم زدن نظم موجود بوده و منافع جمعی برای آنان فاقد اهمیت است، به‌سختی قابل بازداری هستند.

در همین راستا، فهرستی از مهم‌ترین حملات سایبری که درجاتی از اختلال با انهدام پراهمیت را ایجاد نموده‌اند به شرح زیر قابل احصاست: در سال ۲۰۰۷ پس از یک سری اختلافات در خصوص جابه‌جایی یک مجسمه یادبود جنگ جهانی دوم با روسیه، کشور استونی متحمل مجموعه‌ای از حملات انکار سرویس (DOS)[۵۱] شد که دسترسی کشور به اینترنت را به مدت چند هفته با اخلال مواجه کرد. حملات مشابهی در ۲۰۰۸ و متعاقب درگیری‌های روسیه و گرجستان، ارتباطات دفاعی گرجستان را مختل نمود. در ۲۰۱۰ ویروس استاکس نت موجب تخریب بیش از ۱۰۰۰ سانتریفیوژ و تعویق برنامه هسته‌ای ایران شد که به آمریکا و اسرائیل نسبت داده شد. برخی معتقدند حملات انکار سرویس سال‌های ۲۰۱۲ و ۲۰۱۳ که سیستم مالی آمریکا را هدف قرار داده بود، از سوی ایران در تلافی استاکس نت انجام شده است. همچنین بسیاری از صاحب‌نظران در سال ۲۰۱۲ ایران را متهم به ایجاد ویروس Shamoon کردند که حدود ۳۰ هزار از کامپیوترهای شرکت نفتی آرامکو سعودی را هدف قرار داد. کره شمالی به‌کرات در شبکه‌های کره جنوبی نفوذ کرده و خرابی‌هایی به‌بار آورده است. در سال ۲۰۱۴، کره شمالی در نتیجه عصبانیت از تولید فیلمی در خصوص رهبری کشورش، به کمپانی Sony حمله کرده و خساراتی به‌بار آورد. در سال ۲۰۱۵ و اختلافات روسیه- اوکراین، ویروسی باعث اختلال چندساعته در ۲۲۵ هزار مشترک شبکه برق اوکراین شد. پیش از آن، گزارش‌هایی در خصوص اختلال در شبکه‌های سایبری اوکراین در خلال جنگ هایبرید روسیه منتشر شده

۵۱ Denial OF Service: حملاتی هستند که طی آن مهاجمان حجم زیادی از ترافیک را بر روی سرویس‌دهنده وب ارسال کرده و فعالیت آن را متوقف می‌کنند.

بود. در ۲۰۱۶، سایت ویکی لیکس فاش کرد که سرویس‌های اطلاعاتی روسیه باعث اخلال در کمپین ریاست جمهوری دمکرات‌های آمریکا شده‌اند (Nye, 2017).

همه حملات سایبری مهم که تاکنون رخ داده‌اند، می‌توانند به‌عنوان شکست بازدارندگی تلقی شوند اما تمام آن‌ها از نظر تأثیر بر امنیت ملی در حد متوسط قرار داشتند و در دوگانه سنتی جنگ و صلح، در منطقه خاکستری قرار می‌گیرند (Nye, 2017). بااین‌حال، این حملات با دیدگاه‌های نظری رئالیسم تهاجمی هم‌راستا هستند؛ چراکه در این نظریه، تهاجم بر سایر سناریوها برتری دارد. واقعیت این است که جنگ سایبری تمام‌عیار تاکنون رخ نداده است و کشورها تمایلی به فاش کردن توان‌مندی نهایی خود ندارند. لذا واقعیت‌های نهایی نبرد سایبری، در زمان بروز یک نبرد سایبری تمام‌عیار رخ خواهد داد. در این‌جا ضروری است تا گفته جرویس را یک‌بار دیگر به یاد آوریم که از سه دوره استراتژی بازدارندگی در جنگ سرد نام برده بود[۵۲] و جوزف نای نیز این مسئله را در خصوص سایبر تأیید کرده بود؛ بدین معنی که با گذشت زمان و پیشرفت‌های تکنولوژیکی آینده و بروز احتمالی جنگ‌های سایبری جدی‌تر، مسائل مطرح در خصوص بازدارندگی سایبری نیز ممکن است دست‌خوش تغییر و تحولاتی شود. در ادامه مقاله، به بررسی موردی نمونه‌ای عملیاتی از تهدیدات سایبری که حدس زده می‌شود بازدارندگی سایبری در آن موفق عمل نموده، می‌پردازیم.

۶. تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا – شبکه برق

در این بخش به بررسی موضوع تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا پرداخته و عملکرد سازوکارهای ذکرشده را در این خصوص مورد ارزیابی قرار خواهیم داد. مدعای اصلی این است که روسیه و چین توانسته‌اند با جایگذاری عامل‌های حمله سایبری در درون سیستم‌های شبکه برق آمریکا، در مقابل این کشور نوعی بازدارندگی ایجاد نمایند. بدین معنی که ایالات متحده از ترس امکان فعال کردن و استفاده از این عوامل و تخریب سیستم‌های شبکه و در نتیجه قطعی گسترده برق در بخش‌های وسیعی از کشور که می‌تواند مشکلات امنیت ملی ایجاد نماید، به‌راحتی به این کشورها حمله نخواهد کرد.

حرکت زیرساخت‌های برق آمریکا و سایر کشورها به سمت تکنولوژی شبکه دیجیتال[۵۳]

52 Robert Jervis, «Deterrence Theory Revisited», World Politics, 1979

۵۳ Digital Grid: شبکه نوین برق که در آن امکانات مختلفی از جمله دستگاه‌های کنترل نیروی الکترونیکی و کنترل تولید و توزیع نیروی برق خدمات را مطمئن‌تر از قبل ارائه می‌کند.

باعث آسیب‌پذیری این سیستم‌ها در مقابل نقاط ضعف ذاتی کامپیوترها شده و تهدیدهای مؤثر از ناحیه فعالیت‌های مخرب سایبری را در آمریکای شمالی بیشتر و حرفه‌ای‌تر کرده است (Will, 2015). وجود پتانسیل بازیگران متخاصم جهت اعمال تأثیر مخرب فیزیکی بر سیستم‌های کامپیوتری تولید، توزیع و انتقال برق ایالات متحده، به منبع اصلی نگرانی برای مسئولین تبدیل شده است[۵۴].

با گذشت زمان، شبکه‌های الکتریسیته مدرن‌تر شده و به تکنولوژی روز مجهز شده‌اند؛ چراکه اولویت اول دست اندرکاران، تحویل امن و مطمئن برق به مصرف‌کنندگان نهایی است. از اوایل قرن بیستم و هم‌زمان با افزایش تقاضا برای برق در بین مردم، شرکت‌های متولی امر به سمت توسعه سیستم‌های اتوماسیون و کاهش نیاز به نیروی انسانی گرایش داشته‌اند. این سیستم‌ها در جهت افزایش قابلیت اطمینان، دائماً به سمت افزایش حفاظت، اتوماسیون و قابلیت‌های کنترلی خود حرکت کرده‌اند. افزایش سطوح قابلیت اطمینان، نیاز به سیستم‌های برخط [۵۵] را افزایش داده با ورود سیستم‌های سایبری کلیه قابلیت‌های کنترلی و اطمینان در همه سطوح ارتقای چشم‌گیری را تجربه کرده‌اند. از طرف دیگر، وابستگی روزافزون به سیستم‌های کامپیوتری باعث افزایش سطوح تهدید شده و آسیب‌پذیری گسترده‌ای را در برابر شبکه‌های برق آمریکا قرار داده است.

احتمال حمله سایبری علیه شبکه‌های برق‌رسانی از نظر تعداد و شدت افزایش‌یافته است. گزارش وضعیت تهدید سایبری ۲۰۱۵ نشان داده است که تعداد حملات انجام‌شده به شرکت‌های برق به نسبت سال ۲۰۱۴ به میزان ۶ برابر افزایش داشته است[۵۶]. بر اساس گزارش ICS[۵۷] که مهم‌ترین منبع در زمینه گزارش حملات سایبری است، در سال ۲۰۱۴ از ۲۴۵ حمله پرقدرت APT[۵۸] انجام‌شده به آمریکا، ۷۹ حمله علیه شرکت‌های برق انجام‌شده است.

این مشکل نه‌تنها در شبکه برق، بلکه در سایر زیرساخت‌های حیاتی آن کشور موجود است و به حدی نگران‌کننده است که لئون پانتاوزیر دفاع اسبق ایالات متحده می‌گوید:»آمریکا با احتمال مواجهه با پرل هاربر سایبری روبرو بوده و به‌طور روزافزونی در مقابل هکرهای خارجی آسیب‌پذیر است که می‌توانند شبکه برق، سیستم حمل‌ونقل، شبکه بانکی و دولت را ازهم بگسلند»[۵۹].

54 Cyber threat and vulnerability analysis of the U.S. electric Sector Idaho National Institute 2016

۵۵ Real time: سیستم‌هایی که اطلاعات را بصورت آنی منتقل می‌کنند.

56 2015 Global State of Information Security Survey

57 ICS Cert Monitor 2014 Report

58 Advanced Persistent Threats

59 http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

لئون پانتا در این سخنرانی جنبه‌هایی از تأثیرات حملات احتمالی سایبری به زیرساخت‌های حیاتی آمریکا را برشمرده است. او معتقد است که در مقابل پیشرفت‌های تکنولوژیکی کشورهای بالقوه متخاصم (از دید وی شامل چین، روسیه، ایران، کره شمالی و گروه‌های شبه‌نظامی) می‌بایست سیاست جدی اتخاذ شود. وی ادامه می‌دهد: «یک کشور متجاوز یا گروه بنیادگرا می‌تواند با استفاده از ابزار سایبری کنترل سیستم‌ها را در دست گرفته و پس‌ازآن قطارهای مسافری یا حتی خطرناک‌تر از این، قطارهای حامل محموله‌های سمی کشنده را از خط خارج، منابع آب آشامیدنی در شهرهای بزرگ را مسموم، و یا شبکه‌های برق را در بخش‌های وسیعی از کشور خاموش کند»[۶۰].

مقامات دفاعی آمریکا پس‌ازآن ابراز نمودند که سخنان وزیر دفاع اغراق نبوده و به‌عنوان شاهدی بر این مخاطرات، به حملات گسترده سایبری به مؤسسات بزرگ آمریکایی اشاره کردند. علاوه بر این مورد، حمله گسترده سایبری به شرکت نفت عربستان (آرامکو) که موجب ازکارافتادگی ۳۰ هزار کامپیوتر شد نیز مورد اشاره قرار گرفت. این مقامات همچنین فاش کردند که وزارت دفاع در حال اعمال فشار بر مجلس نمایندگان است تا قوانین و استانداردهای جدید جهت حفاظت از زیرساخت‌های حیاتی کشور (که عمدتاً توسط بخش غیردولتی اداره می‌شوند)، مانند نیروگاه‌های برق، امکانات توزیع آب و لوله‌های گاز- که یک حفره کوچک امنیتی می‌تواند آسیب‌های شدید اقتصادی و اجتماعی بر جای گذارد- را تصویب کنند.

به عقیده پانتا، بدترین حالت ممکن، ترکیب یک حمله فیزیکی (غیرسایبری) با حمله هم‌زمان سایبری چند گروه مختلف به بخش‌های گوناگونی از زیرساخت‌های حیاتی کشور است که می‌تواند به‌عنوان یک پرل هاربر سایبری، باعث خرابی‌ها و مرگ‌ومیر گسترده شده و با شوک دادن و فلج کردن ملت، باعث ایجاد احساس عمیقی از آسیب‌پذیری ملی شود[۶۱].

پانتا در بخش دیگری از سخنان‌اش اظهار می‌دارد: «ایالات‌متحده تنها با دفاع سایبری قادر به جلوگیری از حملات سایبری نخواهد شد» و ادامه می‌دهد «چنان‌چه می‌خواهیم وقوع حمله‌ای قریب‌الوقوع را که می‌تواند خسارات فیزیکی گسترده به‌بار آورده و جان افراد زیادی را تهدید کند، تشخیص دهیم، می‌بایست گزینه‌هایی جهت اقدام علیه آنان که قصد دارند به کشور حمله کنند در دست داشته باشیم». او در ادامه می‌افزاید «برای این نوع از سناریوها، وزارت دفاع اقدام به توسعه قابلیت‌های تهاجمی علیه کسانی که منافع ملی ما در فضای سایبر

60 http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

61 Nicole Perlroth,» Infrastructure Armageddon», New York Times, Oct 23 2015

را تهدید می‌کنند نموده»[۶۲].

پنهان بودن یکی از مهم‌ترین ویژگی‌های این‌گونه عملیات است. به‌عنوان مثال، در خصوص استاکس نت که برنامه هسته‌ای ایران را هدف قرار داد، گفته می‌شود که عامل‌های مربوطه به مدت سه سال در محیط منطقی سیستم‌های کنترل صنعتی (PLC) و بدون اطلاع اپراتورها مستقر بوده‌اند (Kello, 2014). علاوه بر این، استاکس نت قادر بود فعالیت‌های مخرب خودش را حتی بعد از شروع عملیات از دید کنترل‌کننده‌ها مخفی نگه دارد؛ به‌گونه‌ای که چند ماه پس از شروع حمله قادر به تشخیص عامل عملکرد نامطلوب سانتریفیوژها شدند.

یک عامل خفته[۶۳] از این نوع، می‌تواند در مسیر رسیدن به هدف در بحران‌های دیپلماتیک یا نظامی از راه دور اجرا و کنترل شود (Lucas, 2013). یکی از مهم‌ترین روش‌های ارتقای بازدارندگی سایبری خصوصاً میان قدرت‌های بزرگ سایبری، ایجاد و ارسال و جاسازی[۶۴] این عوامل سایبری در درون زیرساخت‌های حیاتی کشور هدف است. با این اقدام، کشورها به دلیل نگرانی از احتمال بهره‌برداری طرف مقابل از این نرم‌افزارهای جاداده‌شده و تخریب زیرساخت‌ها و ایجاد بحران امنیت ملی، از اقدام تهاجمی در خصوص کشور مقابل بازداشته می‌شوند. در همین راستا، منابع آگاه در سازمان اطلاعات مرکزی آمریکا اعلام کرده‌اند که روسیه و چین اقدام به جاسازی قابلیت‌های سایبری درون شبکه برق آمریکا نموده‌اند که آن‌ها را قادر می‌سازد در مواقع مورد نیاز، کل شبکه یا بخش‌هایی از آن را خاموش کنند[۶۵].

در سال ۲۰۱۳، کمیته اطلاعات مجلس نمایندگان آمریکا در بیانیه‌ای اخطار داد که تجهیزات الکترونیکی شرکت هواوی (شرکتی چینی که به‌وسیله یکی از مقامات ارشد ارتش آزادی‌بخش خلق ایجاد شده است) می‌تواند برای اهداف تهدیدکننده امنیت ملی مورداستفاده قرار گیرد[۶۶].

در خصوص آمریکا، حقیقت آن است که گرچه این کشور در توسعه تکنولوژی سایبر و اینترنت پیشرو بوده، اما به همان نسبت نیز در مقابل ابزار مخرب سایبری آسیب‌پذیر شده است (Nye, 2017). بسیاری معتقدند که اتصال گسترده زیرساخت‌های حیاتی آمریکا و وابستگی شدید به شبکه اینترنت، کلیه زیرساخت‌ها را در مقابل حملات سایبری آسیب‌پذیر کرده است. اتصال هر چه بیشتر سیستم‌های بنیادی به اینترنت، در واقع به معنی بیشتر شدن

62 http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html
63 Sleeper
64 Embed
65 Ted Koppel, «Where is Americas cyber defense plan?», Washington Post, December 7, 2015
66 Subcommittee on Europe, Eurasia and emerging threats, 2013

راه نفوذ هم هست. لذا با توجه به این استدلال، اندیش‌مندان معتقدند که در این‌گونه موارد بازدارندگی به‌درستی عمل می‌کند. بر این مبنا، به دلیل عملکرد بازدارندگی سایبری، آمریکا در خصوص روسیه و چین هیچ‌گاه به حملات پرحجم سایبری متوسل نخواهد شد.

بر مبنای نظریه رئالیسم تهاجمی، تمامی اقدامات تهاجمی آمریکا در این عرصه و همچنین اقدامات روسیه و چین در خصوص کارگذاری عامل خفته در درون شبکه حیاتی برق آمریکا، در راستای بیشینه‌سازی قدرت و افزایش توان‌مندی در جهت افزایش امنیت و تضمین بقاست.

برای بررسی بیشتر موضوع، عملکرد سازوکارهای چهارگانه را در این مورد بررسی قرار خواهیم کرد. شاید بتوان گفت که سازوکار تلافی بیشترین نقش را در این بازدارندگی داراست. در واقع، آمریکا به دلیل وحشت ناشی از تلافی این کشورها و بروز بحران‌های سیاسی، اجتماعی، اقتصادی و امنیتی مرتبط با این موضوع، به‌راحتی اقدام تحریک‌کننده‌ای انجام نخواهد داد. عنوان یکی از مقالات چاپ‌شده در نیویورک‌تایمز که در آن به بررسی مخاطرات حمله سایبری برای زیرساخت‌های حیاتی آمریکا پرداخته شده، آرماگدون زیرساختی[۶۷] است. عنوان این مقاله به اندازه کافی گویاست. نویسنده معتقد است در صورت وقوع حمله سایبری روسیه و چین به زیرساخت‌های حیاتی آمریکا، آخرالزمان فرا خواهد رسید. در این راستا، ریچارد کلارک به‌عنوان یکی از اساتید پیشرو در این زمینه می‌گوید: «در دنیای واقعی آمریکا باید به دلیل ترس از اثرات نامتقارنی که مجازات تلافی‌جویانِ می‌تواند بر شبکه‌های کشور داشته باشد، از حملات بزرگ سایبری بازداشته شود» (Clarke 2010).

در خصوص سازوکار انکار می‌توان گفت که چین و روسیه از سال‌های پیش، اقدامات گسترده‌ای جهت پایداری و برگشت‌پذیری شبکه‌های خود انجام داده‌اند. در این حالت آمریکا از کارایی حملات خود اطمینان چندانی ندارد (هرچند که اهمیت این سازوکار هم‌سنگ تلافی نیست). در نتیجه، سازوکار انکار نیز واجد کارایی است. این سازوکار در خصوص کشورهای کمتر توسعه‌یافته بازدارندگی چندانی ایجاد نخواهد کرد، زیرا این کشورها صرفاً مصرف‌کننده تکنولوژی بوده و توانایی اجرای سناریوهای قوی و پیشرفته امنیتی در شبکه‌های خود را ندارند. لذا امکان نفوذ و برداشت اطلاعات یا تخریب سیستم‌ها به‌راحتی میسر است.

در خصوص سازوکار هنجار، باید گفت که هنوز هنجارهای مؤثر بین‌المللی در این خصوص ایجاد نشده‌اند. هیچ سازمان بین‌المللی‌ای مسئولیتی در این خصوص نپذیرفته و در صورت بروز هرگونه حمله سایبری، اقدامات بین‌المللی هماهنگی صورت نخواهد پذیرفت. در این

67 Infrastructure Armageddon

مورد، کشورها به‌صورت انفرادی عمل می‌کنند. تنها نهاد بین‌المللی که اقدامات اولیه در این خصوص به انجام رسانده ناتو است. پس از حمله سایبری به استونی و با توجه به این‌که این کشور عضو ناتو است، کشورهای عضو اقدام به ایجاد نهاد سایبری ناتو تحت نام CCDCOE [۶۸] در پایتخت استونی[۶۹] نموده و سندی مشتمل بر قوانین حقوقی تهیه و منتشر کردند[۷۰]. در حال حاضر، تنها سند بین‌المللی که در زمینه‌ی مسائل استراتژیک حوزه سایبر اقدام به بررسی اولیه مسائل حقوقی و قانونی کرده، این سند است که در آن تنها به تطبیق تک‌تک قوانین و حقوق نبرد مسلحانه به حوزه سایبر اکتفا شده است. لذا ضروری است تا نهادهای فراگیر بین‌المللی (خصوصاً سازمان ملل متحد)، گام‌های عملی در خصوص تدوین هنجارها و قوانین بین‌المللی جهت مواجهه با این پدیده جدید بردارند.

آخرین مکانیزم موردبررسی، گرفتارسازی است. حداقل می‌توان گفت با توجه به یکپارچگی اقتصاد آمریکا با اقتصاد جهانی و نقش بارز اینترنت و سایر شبکه‌های ارتباطی در این زمینه، این کشور به‌راحتی اقدام به هنجارشکنی و اقدام به حمله سایبری نخواهد کرد. ایالات‌متحده به‌عنوان قدرت هژمون تاکنون سردم‌دار جهانی‌سازی بوده و منافع بی‌شماری کسب کرده است؛ به‌طوری که شاید بتوان گفت ادامه برتری آمریکا، به تسهیل روند حاکمیت اینترنت[۷۱] وابسته است.

68 NATO Cooperative Cyber Defense Center Of Excellence
69 Tallinn
70 NATIONAL CYBER SECURITY FRAMEWORK MANUAL
71 Internet Governance

نتیجه‌گیری

بر اساس نظریه رئالیسم ساختاری، کشورها در حوزه‌های مختلف از جمله سایبر، به تقویت قدرت تهاجمی خود ادامه خواهند داد تا بتوانند امنیت خود را ارتقا بخشند. بر این اساس، فضای سایبر به سمت ناامنی روزافزون حرکت خواهد کرد. در این میان، برخی از اندیش‌مندان حوزه امنیت اظهار داشته‌اند که نظریه بازدارندگی قابلیت انتقال به حوزه سایبر را ندارد. این تفکر از آن‌جا نشأت می‌گیرد که ذهنیت ایشان بر مبنای مفروضات بازدارندگی هسته‌ای شکل گرفته و نمی‌خواهند یا نمی‌توانند آن را تغییر دهند. در واقع با لحاظ مفروضات پیشین، کاربست نظریه بازدارندگی هسته‌ای بر نبرد سایبری نتیجه‌ای در بر نخواهد داشت و ضروری است به شکل متفاوتی با موضوع برخورد شود. مشخصات فضای سایبر تفاوت زیادی با فضای سنتی دارد و ضروری است تغییراتی متناسب با این موضوع در بازدارندگی اعمال شود تا بتواند در محیط جدید قابلیت کاربرد پیدا کند. از مهم‌ترین تغییرات مورد نیاز، می‌توان به لزوم استفاده از چهار سازوکار تلافی، انکار، گرفتارسازی و هنجار استفاده نمود. در خصوص سازوکار تلافی، می‌توان به لزوم پاسخ به حمله سایبری با استفاده از تمامی ظرفیت‌ها (ظرفیت‌های اقتصادی، دیپلماتیک و نظامی) اشاره کرد. از طرفی، سرعت پیشرفت تکنولوژی سایبر بسیار بیشتر از تکنولوژی هسته‌ای بوده است. توسعه روزافزون فناوری نیازمند اعمال تغییراتی در استراتژی است و این به معنی ورود موج‌های مختلف نظریه‌پردازی در حوزه بازدارندگی سایبری در آینده خواهد بود که در هر موج نسبت به موج پیشین، نظریات جامع‌تری ارائه خواهد شد. با توجه به جدید بودن کل موضوع نبرد سایبری، تاکنون درصحنه عملیاتی نیز جنگ تمام‌عیار سایبری وقوع نیافته است. در صورت وقوع جنگی همه‌جانبه بین کشورهای مسلط این حوزه، می‌توان ابعاد مخاطرات واقعی این موضوع را بهتر درک و تئوریزه کرد. این مقاله عمدتاً در خصوص زمان صلح است و از زمان جنگ اطلاع زیادی نداریم، ولی قطعاً تعدادی از عناصر زمان صلح با جنگ تفاوت دارند. هم‌اکنون دانشگاه‌های بزرگ جهان، با راه‌اندازی رشته‌های مختلف در تلاش‌اند تا خلأهای موجود در زمینه نظریه‌پردازی حوزه علم و تکنولوژی –عموماً- و امنیت سایبری –خصوصاً- را در درون رشته روابط بین‌الملل پوشش دهند. در این رابطه، مطالعات علوم و تکنولوژی[۷۲] به دنبال مفهوم‌سازی فناوری در روابط بین‌الملل بوده و مطالعات سایبر در تلاش است تا بتواند ابعاد مختلف موضوع نبرد سایبری را تا حد ممکن بررسی و تئوریزه کند. با این اقدامات، به نظر می‌رسد آینده مطالعات عرصه سایبر و خصوصاً بازدارندگی سایبری قدرت‌مندتر از گذشته به مسیر خود ادامه خواهد داد.

72 Science and Technology Studies (STS)

منابع

الف) منابع فارسی

عسگر خانی، ابومحمد. (۱۳۸۳). **رژیم‌های بین‌المللی**، تهران: ابرار معاصر.

فریدمن، لاورنس. (۱۳۸۶). **بازدارندگی**، ترجمه عسکر قهرمانپور، تهران: پژوهشکده مطالعات راهبردی.

ب) منابع انگلیسی

Clarke, Richard. (2010). **Cyber War: The Next Threat to National Security and What to Do About It**, Harper Collins Publications.

DoD. (2015). **The DOD Cyber Strategy**, The Department of Defense.

Gartzke, Erick. (2013). *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*, **International Security**.

Junio, Thimoty. (2013). *How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate*, **Journal of Strategic Studies**.

Kello, Lucas. (2013). *The Meaning of the Cyber Revolution: perils to theory and statecraft*, **International Security**, vol ۳۸

Kello, Lucas. (2015). *The Virtual Weapon: Dilemmas and Future Scenarios*, **IFRI**.

Koppel, Ted. (2015). **Lights Out a Cyberattack Nation Unprepared**, Crown New York.

Libicki, Martin. (2012). **Cyber Deterrence and Cyber War**, RAND.

Lynn, William. (2010). *Defending a New Domain: The Pentagons Cyber Strategy*, **Foreign affairs**.

Mission Support Center. (2016). **Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector**, Idaho National Laboratory.

Morgan, Patrick. (2010). **Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm**, University of California.

Naughton, John. (2016). *The evolution of the internet: from military experiment to general purpose technology*, **Journal of Cyber Policy**.

Nye, Joseph S. (2017). *Deterrence and Dissuasion in cyberspace*, **International Security**

Nye, Joseph. (2011). *Nuclear Lessons for Cyber Security*, **Strategic Studies Quarterly**.

Rid, Thomas. (2013). *Cyber war Will Not Take Place*, **Journal of Strategic Studies**.