*رسانه و فرهنگ*، پژوهشگاه علوم انسانی و مطالعات فرهنگی
دوفصل‌نامهٔ علمی ـ پژوهشی، سال هشتم، شمارهٔ اول، بهار و تابستان ۱۳۹۷، ۴۷–۷۴

# قدرت بازدارندگی در فضای سایبر

**اردشیر زابلی‌زاده***

**پیمان وهاب‌پور****

## چکیده

وضعیت «آنارشیک»گونه فضای سایبر، تأثیرات عمیقی روی منافع و امنیت ملی کشورها می‌گذارد. بازیگران ناشناس متعددی روزانه منافع و زیرساخت‌های حیاتی دیگر بازیگران را تهدید می‌کنند. دولت‌ها باید راهی برای کاستن از آسیب‌های این فضا بیابند و استراتژی بازدارندگی می‌تواند در این زمینه به کار آید. مقاله حاضر به بررسی این موضوع می‌پردازد که آیا استراتژی بازدارندگی در فضای سایبر کارآمدی دارد؟ و شرایط این کارآمدی کدام‌ها هستند؟ یافته‌های این پژوهش نشان می دهد که هرچند استراتژی بازدارندگی نمی‌تواند همانند دوران جنگ سرد در فضای مجازی نیز کارآیی داشته باشد اما پتانسیل زیادی برای محافظت از منافع و امنیت ملی کشورها دارد. سه مولفه اساسی برای کارآمدی این استراتژی نیز شناسایی شدند که عبارتند از قدرت دفاعی زیاد، قابلیت شناسایی مهاجم و توانمندی انجام اقدامات تلافی‌جویانه سخت. «شناسایی» مولفه کلیدی و اساسی نظریه بازدارندگی در حوزه سایبری هست. چرا که شناسایی موفق، متضمن موثر و مفید بودن اقدامات تلافی جویانه است و باعث می‌شود که تهدیدات واقعی از بین بروند. همچنین یافته‌های این مقاله نشان می‌دهند که استراتژی بازدارندگی بدون اقدامات تلافی جویانه، موفق نخواهد بود. در نبود اقدامات تلافی جویانه، مهاجمان بالقوه هم انگیزه ای برای خودداری از حمله ندارند.

**کلیدواژه‌ها:** بازدارندگی، فضای سایبری، شناسایی، دفاع، اقدامات تلافی جویانه.

---

* استادیار و رئیس دانشکده ارتباطات صداوسیما، azmmf9432@gmail.com
** دکتری روابط بین‌الملل از دانشگاه علامه طباطبایی، pvahabpoor@gmail.com
تاریخ دریافت: ۱۳۹۶/۱۱/۱۸ تاریخ پذیرش: ۱۳۹۷/۰۲/۱۵

## ۱. مقدمه

قدرت سایبری امروزه بعد مهمی از زیست‌واره جهانی را شکل می دهد. اطلاعات و فناوری‌های اطلاعاتی در سپهر سیاسی، اقتصادی و نظامی نقش حیاتی ایفا کرده و مقدمات فعالیت‌های عملیاتی را فراهم می‌آورد. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود و در کنار آثار مثبتی که در بهبود زیست جهانی دارد برخی ابعاد منفی و قابل توجه دیگری نیز دارد که حتی ممکن است آثار آن مخرب تر از جنگ‌های نظامی بوده و امنیت و حیات ملی مردمی را به چالش بکشاند. با توسعه فناوری‌های اطلاعاتی، خطرات دیگری همچون حمله مجازی یا جاسوسی سایبری در کمین تصمیم‌سازان و سیاست‌گذاران کشورهاست. ولی با توجه به هزاران حمله سایبری که در طی روز اتفاق می‌افتد، کار تمیز حملات جدی و مهم از حملات ناکارآمد و جزئی بسیار سخت شده است.

آنچه که در زمینه کنترل فضای مجازی چالش برانگیز است تفاوت ماهوی آن با دنیای واقعی است و همین امر هم کار را بر دولتمردان سخت می کند. بخش مهمی از ظرفیت‌های دولت‌های ملی در عصر کنونی معطوف به افزایش توانمندی‌ها برای برقراری امنیت و افزایش قدرت است. قدرت به طور سنتی ، بر افزایش توانمندی‌های نظامی، اقتصادی، سیاسی و تحکیم پایه‌های حکومت از طریق حکومت خوب و ایجاد همبستگی ملی صورت می‌گیرد.تهدیدها نیز از طریق افزایش و تقویت چنین ظرفیت هایی دفع یا تعلیق می شود.

در فضای سایبر ما با یک وضعیت متفاوت مواجه هستیم. به رغم استفاده و بهره گیری دولت ها، افراد، سازمان های بین المللی، دانشگاه ها و ... از این فضا، روز به روز از آسیب پذیری بیشتری در قبال تهدیدات جدید برخوردار می شوند. فضای سایبر حاکمیت و قدرت را تنها به دست دولت نسپرده است، لویاتان حاکمی بر این فضای هزار سر وجود ندارد.

شاید بتوان گفت اینجا هنوز دوران «وضع طبیعی» خود را می گذارند. در دیدگاه توماس هابز،استقرار دولت قدرتمند (لویاتان) برای پایان دادن به وضع طبیعی، ضروری است. لویاتان نیز از طریق قرارداد اجتماعی که افراد با یکدیگر منعقد می کنند، به وجود می آید. طبق نظر هابز، زمانی که یک حاکمیت مستقر می شود که تعداد کثیری از افراد با یکدیگر توافق می کنند که حق نمایندگی را به آن اعطا کنند. بدین سان هابز به پاسخی

برای پرسش قدرت می رسد که خود آن نیز قدرت محور است. لویاتان فراقـدرتی کـه در عین نفی قدرت فردی، در خدمت تضمین بقای فرد در حیات جمعی قـرار مـی گیـرد. بـه عقیده هابز، غلبه خصلت قدرت جویی از یک سو و میل به بقا از سوی دیگر، انسان هـا را به ضرورت پذیرش این فراقدرت سوق می دهد. (منوچهری،۱۳۷٦: ۳۳)

اما در فضای سایبر هیچ گونه حاکمیتی که افراد بتوانند چه از طریق قرارداد اجتمـاعی و یا هر مسیر دیگری بر حرص و ترس خود فائق آیند وجود ندارد. جهان امروز و آینده مـا به یک نظام بین المللی جدیدی وارد شده است که آنگونه که باید و شاید، از ظرفیت هـای تهدید آمیز و حتی همکاری جویانه فضای سایبر اطلاع ندارد. فضای آنارشیک سایبر، راه را برای خشونت و اعمال قدرت سخت باز می کند.

راه های متعددی برای اعمال این نوع از قدرت وجود دارد. در ادامه سعی می شـود بـه این سوال پاسخ داده شود که آیا استراتژی بازدارندگی در فضای سایبر قابلیت کاربرد دارد و شرایط کارآمدی آن کدام ها هستند؟

این مقاله از چند بخش تشکیل شده است. ابتدا مروری بر ادبیات پژوهش داشته و آثـار مرتبط با این حوزه که به زبان های فارسی و انگلیسی نگاشته شده اند مـورد بررسـی قـرار می‌گیرند. در بخش دوم، چیستی فضای سایبر مورد مداقه قرار خواهد گرفـت و سـپس در بخش سوم به بررسی مفهوم قدرت در فضای سایبر و تحول معنایی آن خواهیم پرداخـت. بعد از تحول معنایی قدرت، شناخت جنگ های سایبری اهمیت وافری می‌یابد کـه بخـش چهارم را به خود اختصاص می دهد. در بخش پنجم به اسـتراتژی بازدارنـدگی در فضـای سایبری پرداختـه و آثـار و پیامـدهای آن را بررسـی خـواهیم کـرد. بخـش نهـایی نیـز بـه نتیجه‌گیری و ارائه راهکارها اختصاص دارد.

## ۲. پیشینهٔ پژوهش

ادبیات و نوشته های مربوط به فضای سایبر در چند سال اخیر رشـد بـاور نکردنـی داشـته است. موسسات و نهادهای بسیاری به بررسی پیامدهای این عرصه بـر زنـدگی اجتمـاعی، سیاسی و فرهنگی انسان هزاره سوم، می پردازند. به همین میزان نیز محتوا تولید شده است. به گونه ای که فضای سایبر برای ما دیگر فضای گنگ و مبهمی نیست.

در داخل کشور نیز برخی از این آثار ترجمه شده و برخی نیز به رشته تحریـر در آمـده است. در ادامه به بررسی برخی از این کتابها و مقالات می پردازیم. با توجه بـه گسـتردگی

ادبیات این حوزه، صرفاً به آن دسته از نوشته ها خواهیم پرداخت که بـه متغیـر مسـتقل مـا یعنی فضای سایبر مربوط می شود.

**۱.۲** به عنوان اولین نمونه می توان به کتاب پرفروش جوزف نای با عنوان «آینده قدرت در قرن ۲۱»اشاره کرد(Nye,2011). نای در این کتاب به بررسی تـاریخی تحـول قـدرت در زندگی سیاسی بشر می پردازد. وی قدرت سایبر را «احراز نتایج ترجیحی از طریق اسـتفاده از منابع اطلاعاتی به هم پیوسته الکترونیکی در حوزه سایبر» تعریف می کند. «نای» در ایـن کتاب دو بعد از قدرت سایبری را برمی شمرد: وجه فیزیکی قدرت سایبر و وجـه مجـازی قدرت سایبر. بر همین اساس اهداف و مرجـع نهـایی قـدرت سـایبر را نیـز در دو حـوزه دسته‌بندی می کند. دسته اول در درون فضای سایبر اتفاق می افتد که وجـه سـخت و نـرم دارد. مانند «حملات سایبری» که در وجه سخت جای می گیرد تأثیرگذاری بر ارزش هـا و معیارهای زندگی دیگران که در وجه نرم صورت بندی می شود.

اما دسته دوم خارج از فضای سایبر روی می دهد که آن هـم بـه وجـه سـخت و نـرم تقسیم می شود. نای از کنترل بر سیستم های تبادل اطلاعـات و جریـان آزاد اطلاعـات بـه عنوان وجه سخت و استفاده از فضای سـایبر بـرای دیپلماسـی عمـومی در عرصـه روابـط خارجی و بین المللی کشور به عنوان وجه نرم یاد می کند.

آنچه که نای انجام داده است، بی شک مهمتـرین بسـتری اسـت کـه سـایر محققـین و پژوهشگران می توانند از آن بهره برداری کنند. اما نـای بـه بررسـی رویکردهـای تئوریـک نسبت به فضای سایبر و این که جریان اصلی روابط بین الملل و سایر نظریه های اجتماعی نسبت به آن چه دیدگاهی دارند، مطلب زیادی به ما نمی گوید. از سوی دیگر وی، به تمام وجوه قدرت به ویژه مقایسه قدرت در فضای سایبر با آنچه کـه نظریـه هـای اجتمـاعی و پست مدرن از آن به عنوان وجه نامرئی قدرت یاد می کنند، اشاره ای نمی کند.

**۲.۲** فرد دیگری که به موضوع فضای سایبر به عنوان متغیر تأثیرگذار بر عرصه سیاسـی می پردازد، جرمی کرامپتون است. وی در کتاب خود با عنوان «صورت بندی سیاسی فضای سایبر»(Crampton, 2004) به این سؤالات پاسخ می دهد که «بودن» در فضای سایبر بـه چـه معناست؟ فضای سایبر چگونه نظم پیدا می کندو روابط قدرت چگونـه بـر تنظـیم فضـای سایبر تأثیر می گذارد؟. وی با استفاده از رهیافت فوکویی به سؤالات بالا پاسخ مـی دهـد. کرامپتون با پیش کشیدن بحث «فناوریهای خود(Technologies of the Self) به تحلیل فضای سایبر روی می آورد. وی توضیح می دهد که چگونه هویت افراد در فضای سایبر تغییر پیدا

می کند. کرامپتون فضای سایبر را به عنوان مجموعه دقیقی از روابط قلمداد می کند کـه در آن ما خود را پیدا می کنیم. به رغم اینکه مباحث کرامپتون در حوزه اندیشه ای قابل تأمل و جالب است، اما به صورت عملیاتی چیز زیادی در مورد چگونگی تأثیر این فضا بر قـدرت به ویژه در عرصه بین المللی اشاره نمی کند.

**۳.۲** «ظهور سیاست شبکه ای؛ چگونه اینترنت سیاست و دیپلماسی بین المللی را تغییـر می دهد»مورد بعدی است که توسط دیوید بویلر تدوین شده اسـت(Bollier, 2003). فصـل اول این کتاب به چگونگی تأثیر شبکه های الکترونیکی بر ماهیت قدرت و فرهنـگ اشـاره دارد. بخش دوم به بحث اینترنت و ظهور قدرت نرم متمرکـز اسـت و در فصـل سـوم بـه رقابت روایت ها در سیاست بین الملل در عصر سایبر اشاره می شود. بـه رغـم توضـیح و تبیین مفصل در خصوص نقش فضای سایبر در قدرت نرم و سخت در روابط بـین الملـل، متغیر قدرت به صورت کامل توضیح داده نشده اسـت. همچنـین فاقـد نگـاه تئوریـک بـه موضوع می باشد.

**٤.۲** منبع دیگری که بدان اشاره می شود، مقاله جان اریکسون و جیامپیورگ یاکوملو بـا عنوان «انقلاب اطلاعاتی، امنیت و روابط بین الملل» است(Eriksson and Iacomello, 2006) . آنان به دنبال پاسخ به این سؤال هستند که تئوری های روابـط بـین الملـل در مـورد تـأثیر فضای سایبر و انقلاب ارتباطات و اطلاعات بر روابط بین الملل چه می گویند. نویسندگان چنین نتیجه گیری می کنند که بسیاری از نظریه های روابط بین الملل در مورد این موضوع سکوت کرده اند. به جز نظریه هایی که محوریت سیاستگذارانه دارند و بـه مسـایل امنیتـی مرتبط با تکنولوژی اطلاعاتی پرداخته اند، سایر نظریه های روابط بین الملل در ایـن مـورد حرفی برای گفتن ندارند. لذا نویسندگان در بخش دوم مقاله، بار دیگر نظریه های رئالیسم، لیبرالیسم و سازه انگاری را مورد بازبینی قرار می دهند تا شاید عناصر مرتبط با امنیت (و نه قدرت) در عصر دیجیتال را در آنها بیابند. به رغم مطرح کردن نکات ویـژه در ایـن مقالـه، مبحث امنیت بیش از قدرت در این مقاله محویـت دارد و نویسـندگان اشـاره ای بـه تـأثیر فضای سایبر بر قدرت بازیگران بین المللی نمی کنند.

**۵.۲** پژوهش دیگری که می توان در خصوص فضای سایبر بـه آن اشـاره کـرد، کتـاب «انقلاب اطلاعات، امنیت و فناوری های جدید» می باشد، که توسط جیمز روزنا و دیگران به رشته تحریر در آمده است (روزنا، ۱۳۹۰). این کتاب در سیزده فصل بـه موضـوع تـأثیر انقلاب اطلاعات بر موضوع امنیت در روابط بین الملل پرداخته است. چند فصل از کتـاب

به تأثیر فناوری های اطلاعات بر محیط پیرامونی به ویژه دولت، حاکمیت و توسعه انسانی تمرکز دارد. نویسندگان به این موضوع اشاره می کنند که بسیاری از نظریه های جریان اصلی روابط بین الملل، در خصوص موضوع امنیت در فضای سایبر سکوت پیشه کرده اند. لذا پیشنهاد می کنند که برای فائق آمدن بر این مشکلات با استفاده از رهیافتی «عمل باورانه» تر به موضوع فضای سایبر و امنیت نگریسته شود. جوزف نای و رابرت کیئن در فصل یازدهم موضوع انقلاب اطلاعات، وابستگی متقابل و قدرت را بررسی کرده اند. در این فصل که عملاً به موضوع نوشتار و رساله نگارنده ارتباط مستقیم پیدا می کند، بحث قدرت قدری به محاق رفته است و عملاً موضوع وابستگی متقابل مورد تأکید قرار گرفته که آن هم به نوشتار جوزف نای در کتاب «فضای سایبر و قدرت» که در بالا نیز بدان اشاره شد، نزدیک می شود. نویسندگان معتقدند، این پیش بینی عامه پسند که انقلاب های اطلاعات و ارتباطات موجب خواهد شد توزیع قدرت در میان دولت ها برابر تر شود، خطاست. در حقیقت به نوعی در تناقض با فرضیه مقاله حاضر نیز قرار می گیرد.

**٦.٢** کتاب دیگر که قابل اشاره است توسط دیوید آلبرتس و دانیل پاپ تحت عنوان «گزیده ای از عصر اطلاعات؛ الزامات امنیت ملی در عصر اطلاعات»نوشته شده است (آلبرتس و پاپ، ۱۳۸۵). نویسندگان در فصل اول کتاب به موضوع امنیت ملی در عصر اطلاعات می پردازند. فصل دوم با عنوان «بایت ها و دیپلماسی» موضوعاتی چون دهکده جهانی، سرچشمه جدید ثروت، سلطه اطلاعاتی و رهبری واقعی در عصر اطلاعات را مورد بررسی قرار می دهد. کتاب در فصل سوم هفت نوع جنگ اطلاعاتی را بررسی می کند: جنگ فرماندهی و کنترل، جنگ اطلاعات ـ محور، جنگ روانی، جنگ الکترونیکی، جنگ رخنه گری (هک)، جنگ اطلاعاتی، و در نهایت جنگ اینترنتی که هم به لحاظ ماهیت و هم از حیث آثار توضیح داده می شوند. در فصل بعدی کتاب آثار اینترنت بر امنیت ملی به طور مبسوط توضیح داده شده است. به ویژه امنیت ملی آمریکا و اقداماتی که باید این کشور انجام دهد. نویسندگان توضیح می دهند که رشد اینترنت، نگرانی های جدی ای در پی دارد. اما چون ایالات متحده و دنیا می تواند منافعی عظیم از دسترسی به یک شبکه جهانی مقاوم در بسیاری از عرصه ها ـ تجارت، فرهنگ، آموزش و در قلمرو امنیت ملی هدف حیاتی ترویج آزادی ـ به دست آورد، ایالات متحده باید به طور حتم یاد بگیرد که با خطرهای امنیت ملی کنار بیاید. دولت آمریکا باید بیاموزد که به گونه ای عمل کند که

ارزش های اساسی آن ـ مانند آزادی بیان و حکومت آزاد ـ که جامعه بر اساس آنها شکل گرفته است، مورد تهدید قرار نگیرد.

کتاب حاضر گرچه از حیث ارائه اطلاعات در خصوص نقش فناوری های اطلاعات، بسیار مفید می باشد، اما در خصوص موضوع مقاله حاضر جز از طریق اشاره به تهدیدهای منبعث از فضای سایبر مطلبی ارائه نمی کند. کتاب بیشتر بر موضوع نقش فناوری اطلاعات در جاسوسی و سرقت اطلاعات تمرکز دارد و اطلاعاتی را در خصوص تأثیر فضای سایبر بر قدرت و بازدارندگی در سطح روابط بین المللی ارائه نمی کند. از سویی دیگر مباحث بیشتر بر روی سیاست داخلی ایالات متحده متمرکز است و نگاه کلان به موضوع کمتر دیده می شود.

**۷.۲** به عنوان نمونه آخر، به کتاب مانوئل کاستلز اشاره می کنیم، که با عنوان «عصراطلاعات : اقتصاد،جامعهوفرهنگ» به رشته تحریر درآمده و یکی از منابع ارزشمندی است که در خصوص جامعه اطلاعاتی و تبعات اقتصادی و فرهنگی و اجتماعی آن نوشته شده است(کاستلز، ۱۳۸۰).

هدف کاستلز آن بوده که با بررسی تحلیلی مهمترین رویدادها و پدیدارهایی که در زمانه حاضر در حال شکل دادن به جوامع بشری و رقم زدن سرنوشت آدمی بر روی کره خاکی هستند، امکان فهم عقلانی تحولات حیرت انگیزی را که تأثیر آن بر همه ابعاد حیات انسان‌ها مشهود است فراهم آورد. کاستلز کتاب پر حجم خود را به بحث درباره جامعه شبکه‌ای، که آنرا یکی از ویژگی‌های سرمایه‌داری متکی به اطلاعات به شمار می‌آورد، اختصاص داده است. این کتاب با تمام مباحثی که مطرح می کند، اما در خصوص قدرت در روابط بین الملل به صورت خاص هیچ بحثی را ارائه نکرده است. چرا که بیش از آن که یک کتاب در حوزه روابط بین الملل باشد، کتابی است که درحوزه علوم اجتماعی و اقتصاد نوشته شده است.

این مقاله در نظر دارد با نگاهی جامع به مقوله ای به نام فضای سایبر، تأثیر آن را بر قدرت بازدارندگی دولتها بررسی نماید و مولفه‌های اساسی آن را برآورد نماید. کاری که تاکنون در آثار و منابع قابل دسترس برای نگارنده صورت نپذیرفته است.

## ۳. چیستی فضای سایبر

«فضای سایبر» جدیدترین و در عین حال پیچیده ترین حوزه ای است که زندگی بشر در قرن ۲۱ را به خود مشغول کرده است. زمانی که کامپیوترهای اولیه در ایالات متحده اختراع شدند، کمتر کسی فکر می کرد، انقلاب اطلاعاتی و داده ای ناشی از این امکان جدید، می‌تواند تبعات و آثار پیچیده‌تری نیز در اختیار بشر قرار دهد. رایانه ها، قبل از ورود به حوزه شبکه، دستگاه های پردازشگری بودند که دورنمای سرعت و دقت را برای شرکت‌ها و نهادهای دولتی و غیردولتی فراهم کرده بودند. اما زمانی که این پردازشگرها برای اولین بار به صورت شبکه ای در یکی از اتاق های وزارت دفاع آمریکا درآمدند، اولین نطفه های فضای سایبر را نیز بنا نهادند.

برای اولین بار مفهوم فضای سایبر توسط «ویلیام گیبسون» نویسنده داستانهای علمی–تخیلیدر سال ۱۹۸٤ ارائه شد(Gibson, 1984). جرمی کرامپتون آن را به عنوان حوزه ای از جغرافیای دانش توضیح می دهد که میان جامعه و تکنولوژی قرار گرفته است( Crampton, 2004: 6).

بندیکت این فضا را چنین تعریف می کند: «یک جهان جدید و موازی با دنیای روزمره بشر، که بوسیله کامپیوتر و خطوط ارتباطی جهانی ایجاد شده است»(Benedikt, 1992: 1-3). جهانی با ویژگیهایی نظیر عبور و مرور فراگیر دانش، اسرار، سنجش ها، شاخص ها، سرگرمی ها که از طریق کارگزاری بدیل انسان به صداها، جلوه ها و حضوری جهانی که تا پیش از این وجود نداشته شکل می دهد». وی تعریف دیگری نیز از این فضا ارائه می کند:

> دسترسی از طریق هر کامپیوتری که به سیستم ارتباط جهانی متصل است. مکانی بدون محدودیت که همزمان افرادی از زیرزمین خود در ونکوو کانادا، از یک قایق در پرتوپرنس، از یک تاکسی در نیویورک، از یک گاراژ در تگزاس، از یک آپارتمان در رم، از یک اداره در هنگ کنگ از یک کافه در کیوتو از یک ورزشگاه در کینشازا و از یک لابراتوار در ایستگاه فضایی بین المللی در آن حضور دارند (Benedikt, 1992: 3).

«عدم محدودیت» در فضای اینترنت دارای آثار و پیامدهای ویژه ای است. در حقیقت آنچه که به عنوان انقلاب اطلاعاتی که نقش دولت ها را بسیار کاهش داده مطرح است، از طریق این ویژگی فضای سایبر متمایز می شود. این فضا، برخلاف محیط روزمره زندگی انسان که سرشار از واقعیت هاست، به صورت مجازی تبادل را امکان پذیر می سازد. در

حقیقت «هرجا»(Everywhere ) بودن و «هیچ جا» (Nowhere)بودن با فضای مجازی تحقق پیدا می کند.(Benedikt,1992: 3)

محدودیت های فضای فیزیکی در فضای جدید وجود ندارد. ارتباطات در فضای فیزیکی از طریق نامه ها، کتابها و از این قبیل صورت می گرفت. در حالی که اشیای فیزیکی تنها در فضای فیزیکی وجود داشت، این اشیاء به صورت سایبری در فضای سایبر نیز وجود دارد.فضای سایبر همانند فضای فیزیکی حداقل چهار مفهوم فرعی را به یدک می‌کشد: مکان، فاصله، اندازه و مسیر.

صحبت از فضای سایبر در حقیقت در مرحله اول، در کجا بودن را به ذهن متبادر می‌سازد. این که منبع انتشار و کنش سایبری کجاست و آدرس و مقصد این کنش کجا را نشانه گرفته است. همه، از طریق سؤال درباره مکان پاسخ داده می شود. در حقیقت ارسال ایمیل یا پیام یا هر گونه کنش سایبری در فضای مورد اشاره چه از طریق ارسال کننده پیام و چه در مورد گیرنده پیام باز «مکان» را به عنوان یک عنصر حیاتی مطرح می کند.فاصلهدر حقیقت نمایانگر این است که چه تعداد کامپیوتر مختلف برای رساندن اطلاعات به مقصد مورد نظر مورد نیاز است. اندازه در مورد مقدار اطلاعاتی که توسط بسیاری از لینک ها و پیوندها و وبسایت ها رد و بدل می شود، صحبت می کند. و در نهایت ریشه، به منبع ارسال و دریافت خبر اشاره دارد (Bryant, 2011: 140). اگر نگاه کلان به فضای سایبر داشته باشیم، منبع ارسال و دریافت خبر از طریق شبکه جهانی وب صورت می گیرد، اما در حقیقت خود این مسئله یکی از وجوه مشکل برای زندگی روزمره ما در فضای سایبر است.

از سویی دیگر، فضای سایبر پیامدهای را نیز برای زندگی روزمره ما داشته است. به گونه ای که بسیاری از کارشناسان از وضعیت خطرناک آینده صحبت به میان می آورند. دیوید تاون استاد دانشگاه هاروارد، فضای سایبر را با وضع طبیعی که توماس هابز ترسیم کرده مقایسه می کند. او معتقد است؛ عبارات جنایت سایبر، تروریسم سایبر و جنگ افزارهای سایبرنشان دهنده وضعیت وحشتناک، طغیان گر و لجام گسیخته است (Daniel, 2009: 17).

با تمام این اوصاف به این نتیجه می رسیم که فضای سایبر ترکیب جدیدی از الگوی زندگی در یک فضای ناشناخته را به بشر ارائه می دهد. این فضا برای تمام بشریت امکان بازیگری را فراهم می کند. از کودکان خردسال گرفته تا سازمان های و شرکت های چند ملیتی و نیز دولت ها قدرتمند.

فضای سایبر امکانات جدیدی در اختیار بشر قرار می دهد. جغرافیا را از بین مـی بـرد؛ انسان را از فاعل بودن در محیط اجتماعی، به سوژگی در محیط مجـازی سـوق مـی دهـد؛ ایدها را گسترش می دهد؛ کنترل پذیری را بی معنا می سازد؛ و دولت را به عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و ... خلع سلاح می کند.

وجود پیوند میان فضای سایبر و قدرت در روابط بین الملل، در حال حاضر امر بـدیهی محسوب می شود. وجوه قدرت در فضای فیزیکی متنوع است. این تعدد وجه، خود را در فضای سایبر نیز نشان می دهد. می توان از چند وجه قدرت در روابط بین الملـل و جهـان سیاست صحبت کرد. وجه سخت افزاری، و وجه نرم افزاری قدرت و .... در فضای سـایبر نیز می توان نشانه های چنین وجوهی را جستجو کرد.

## ۴. قدرت و تحول معنایی آن در فضای سایبر

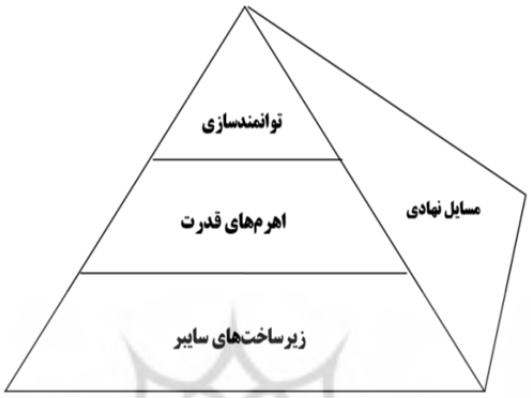
مفهوم قدرت سایبر را می توان در برابر مفاهیمی چون قدرت دریایی(Sea Power)، قـدرت هـوایی(Air Power)، قـدرت زمینـی(Land Power) و حتـی قـدرت فضـایی( Outer Space Power) بررسی کرد(Kramer, 2009: 4-5).

تعاریف از قدرت دریایی و زمینی و ... هر چند بسـیار مـبهم اسـت، امـا بـه نـوعی بـه ظرفیت‌های بالای یک دولت در استفاده از آن به عنوان یـک مزیـت نسـبی اشـاره دارد. در حقیقت هرقدر دولتی بتواند با استفاده از این ظرفیت‌ها به اهداف خود در سریعترین و کـم هزینه‌ترین راه دست پیدا کند او را می توان به عنـوان یـک قـدرت هـوایی یـا دریـایی در نظر گرفت.

«استوارت اچ استار»Stuart H. Starr ) با ارائه یک چارچوب نظـری، قـدرت سـایبر را در حوزه های متعددی بررسی مـی کنـد. وی بـا ترسـیم نمـوداری قـدرت گیـری بـازیگران بین‌المللی را در عرصه سایبر مبتنی بر اهرم های قدرتی می داند که این عرصه ارائه می‌کنند. از نظر او اهرم های قدرت در قالب سیاسی، اقتصادی، نظامی، اطلاعاتی تعریف می‌شوند.

سطح زیرین هرم، شامل زیرساختهایی است که به فضای سایبر شکل می دهد. خروجی این زیرساخت ها، سطوح سنتی قدرت (سیاسی، اطلاعاتی، نظامی و اقتصـادی) را تقویـت می کنند. این سطوح قدرت به نوبه خود، پایه هایی را برای توانمندسازی بازیگران در رأس هرم فراهم می‌کند. این بـازیگران عبارتنـد از : افـراد، تروریسـت‌هـا، جنایتکـاران فراملـی، شرکت‌ها، دولت ـ ملت ها و سازمان های بین المللـی. لازم بـه ذکـر اسـت کـه بـرخلاف

دولت‌ها، احتمال دارد سایر بازیگران به همه وجوه و زیرساخت‌های فضای سایبر دسترسی نداشته باشند. اما بر عکس بازیگران غیردولتی با محدودیتهای ساختاری چون موافقتنامه‌های بین‌المللی که امکان توانمندسازی را محدود می کند، مواجه نیستند.




**شکل ۱: چارچوب مفهومی قدرت سایبر (Starr, 2008: 47)**

این هرم و چارچوب مفهومی سویه‌ی دیگری نیز دارد و آن «مسایل نهادی» است. این مسایل شامل عواملی چون حکومت، ملاحظات حقوقی و قانونی، نظم دهی، به اشتراک گذاری اطلاعات و ملاحظاتی در خصوص آزادی های مدنی است.

## ۱.٤ قدرت اطلاعات

عنصر اساسی که به قدرت سایبر ارتباط بسیار نزدیکی دارد، «اطلاعات»(information ) است. فضای سایبر و قدرت سایبر به وضوح ابعادی از «ابزار اطلاعاتی قدرت»(informational instrument of power) هستند که در قالب مدل سیاسی، اطلاعاتی، نظامی، اقتصادی قرار می‌گیرند[۱]. مدل رهیافت‌های متعددی که اخیر به عناصر قدرت پرداخته‌اند و ما می‌توانیم هزاران روشی را که قدرت سایبر پیوند می‌خورد، حمایت می‌کند و ایجاد و استفاده از ابزارهای دیگر را ممکن می سازد را مشاهده کنیم.

### ۲.٤ قدرت اقتصادی

قدرت سایبر به طور روزافزونی در توانایی اقتصادی نقش حیاتی ایفا می‌کند. حتی دولت ریگان در دهه ۱۹۸۰ میلادی در «استراتژی امنیت ملی» با اشاره به نقش اطلاعات و تکنولوژی های جدید اطلاعاتی در قدرت اقتصادی اقتصاد آمریکا به این موضوع پرداخت. (Reagan, 1988: 34) در اقتصاد جهانی قرن ۲۱ که اقتصادی جهان شمول و به هم پیوسته شده، فضای سایبر را می توان تنها عامل مهم به هم پیوستگی بازیگران با یکدیگر دانست که تولید را تقویت می کند، بازارهای جدیدی می گشاید و مدیریت ساختارهایی که ثروت‌های کلانی ایجاد می کند را ممکن می سازد.

### ۳.٤ قدرت سیاسی و دیپلماتیک

تأثیر قدرت سایبر بر امور سیاسی و دیپلماتیک به سختی کمتر گسترده شده است.قدرتمندترین و با نفوذترین رسانه‌هایی که از طریق تلویزیون ماهواره‌ای به اشاعه دیدگاه‌های و نظرات سیاسی خود می پردازند، از طریق سیستم‌ها و شبکه‌های فضای سایبر به همدیگر متصل هستند. هم دولت آمریکا و هم ترویست‌های القاعده هر دو از امکانات فضای سایبر برای اشاعه پیام‌ها و ایده‌های خود استفاده می کنند.

### ٤.٤ قدرت نظامی

به لحاظ نظامی، قدرت سایبر، شاید مهمترین ابزار نوظهور چند دهه گذشته باشد. در حال حاضر اغلب کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود در برابر چنین تحول جدیدی آماده می‌شوند. دکترین‌های جدید نظامی بر اساس فضای سایبر تدوین می‌شود. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ متعارف، قدرت سایبر، عامل حتمی و گریزناپذیر توانمندیهای نظامی است و این توانمندی بر پایه تکنولوژی‌های مدرن شکل گرفته است. قدرت سایبر روز به روز خود را به عنوان یک عامل تأثیرگذار در سیاست‌گذاری‌های ملی در تمام حوزه‌های مورد اشاره توسعه می‌دهد. از اقدامات ضدتروریستی گرفته تا سامان دادن سیاست، اقتصاد و حتی روابط با سایر کشورها، رد پای این قدرت سایبر را مشاهده می‌کنیم. در امور دولتی و حتی محلی، قدرت سایبر در شکل‌دهی به این موضوع که حکومت‌ها چگونه به شهروندان خود خدمات عمومی ارائه

کنند که حتی تا یک دهه پیش وجود نداشت، موضوعیت پیدا مـی‌کنـد. میـزان تسـهیل در دسترسی به این فضای تکنولوژیک، میزان موفقیت شهروندان و بـه تبـع آن دولـت را رقـم می‌زند. قدرت سایبر میان دیگر عناصر و ابزارهای قدرت پیوند برقرار می‌سـازد و آن‌هـا را برای بهترین شدن وضعیت یاری می‌رساند. به عبارتی دیگـر، فضـای سـایبر هماننـد مـواد خامی است که سوخت اقتصاد و جامعه را فراهم می کند.

با توجه به توضیحاتی که داده شد، می‌توان قدرت سایبر را چنین تعریف کرد: «توانـایی استفاده از فضای سایبر برای ایجاد مزیت‌ها و تأثیرگذاری بر رویدادها در تمام محـیط‌هـای عملیاتی و از طریق ابزارهای قدرت»(Betz,2011: 34)

این تعریف همچنانکه مشاهده می‌شود، از ویژگی گستردگی برخوردار است، چـرا کـه فضای سایبر برخلاف سایر حوزه‌های فیزیکی، محدود نیست. ابزارهای قدرت در این فضا بوسیله عوامل متعددی شکل گرفته است. تا زمانی که فضای سایبر به عنـوان یـک محـیط زیست مطرح است، قدرت سایبر نیز سنجه‌ای برای توانـایی اسـتفاده از آن محـیط قلمـداد می‌شود. تکنولوژی عامل اصلی محسوب می‌شود که بدون استفاده از آن، امکان بهره‌برداری از این فضای جدید وجود ندارد، اما نکته اساسی در این است که برخلاف سایر حوزه‌های قدرت که صرفاً در انحصار بازیگران دولتی قرار داشت، فضای سایبر محدود بـه بـازیگران دولتی نیست. این تکنولوژی اساساً امکان بهره‌گیری بـرای افـراد، سـازمان‌هـا (غیردولتـی)، جوامع، دانشگاه‌ها و ... را فراهم آورده است تا از مزیت‌های بسیار منحصرانه‌ای برخـوردار شوند. از این رو، بررسی تبعات ظهور چنین فضایی بر امنیت ملی کشـورها حـائز اهمیـت می‌نماید. جنگ سایبری یکی از مولفه‌هایی است که امنیت ملی کشورها را به شدت متأثر از خود می سازد.

## ۵. جنگ سایبری

همانند عرصه‌های هوایی، زمینی، دریایی و حتی فضایی، عرصه سایبر نیـز دارای ابزارهـای جنگی است. حملات سایبر امروزه امری واقعی و تعین یافته اسـت کـه در حیـات بشـری دیده می‌شود. حملات سایبری قدرت نسبی دولت‌ها را و به تبع آن، بقـاء آنـان را در نظـام بین‌الملل متأثر می‌سازد. «جنگ سایبری»(cyberwarfare) محدوده‌ای جدید از نزاع، قدرت و امنیت است که پیش از این برخلاف نظرات واقع‌گرایان به هیچ وجه در دایره عناصر قدرت تعریف نمی‌شد. اما شاید بتوان تعریف مورگنتا از قدرت را در این خصوص مستثنی کـرد:

برای مورگنتا قدرت «... ممکن است شامل هر چیزی که کنترل بر انسان را ایجـاد و حفـظ کند» معنی می شود.«قدرت همه روابـط اجتمـاعی را کـه در اختیـار ایـن هـدف باشـد، از خشونت فیزیکی گرفته تا پیوندهای لطیف روانشناختی که ذهن فرد را کنترل می‌کند، شامل می‌شود».(مورگنتا، ۱۳۸۹: ٤٠-٥٤) تکنیک‌های جنـگ در فضـای سـایبر بـه محدودسـازی خودمختاری و کنترل دولت ها تمایل دارد. برای دست یابی به این هدف در جنـگ سـایبر ابزارهای متعددی مورد استفاده قرار می گیرد.

بر اساس تعریف؛ «حمـلات سـایبری، کـنش هـای تعمـدی بـرای جـایگزینی، درهـم گسیختن، فریفتن، منحط کردن یا تخریب سیستم‌ها یا شبکه‌های کامپیوتری و یا اطلاعات و برنامه‌های این سیستم ها هستند.» (Lin, 2011: 63)

دولت‌ها نیازمند نگهداری و محافظت از انسجام شبکه‌ها و سیستم‌های کامپیوتری خـود هستند. این محافظت نه به وسیله دفاع فیزیکی (در شـکل سـنتی)، بلکـه بوسـیله کـاهش آسیب‌پذیری سیستم‌ها در برابر جنگ‌افزارهای جدید سایبری است که اطلاعـات را هـدف قرار می دهند. برخی از نویسـندگان، جاسوسـی سـایبری را از حمـلات سـایبری تفکیـک کـرده‌انـد، (Bajaj, 2010: 2) چـرا کـه آسـیب‌هـای جاسوسـی سـایبری مسـتقیما متوجـه زیرساخت‌های آنان نمی‌شود، اما نمی‌توان چنین، تفکیکیرا قائـل شـد. چـرا کـه آسـیب در فضای سایبر صرفاً به معنی تخریب زیرساخت‌ها معنی نمی‌شود، بلکه هر گونه اطلاعاتی که به سرقت رود می‌تواند نتایج فاجعه باری داشته باشد. در این مورد می‌توان به اطلاعاتی کـه از شرکت سونی پیکچرز در اواخر سال ۲۰۱٤ در آستانه اکران فیلمی ضد هیئت حاکمه کره شمالی، به سرقت رفت، اشاره کرد که دو کشور آمریکا و کره شمالی را به شـدت در برابـر هم قرار داد و رئیس جمهور آمریکا را وادار به واکنش تند علیه این کشور کرد.

رشد جمعیت کاربران در جهان دیجیتالی بدون مرز، در عصری که ماشینهای دیجیتال و کاربرانش تبدیل به جنگاوران سایبر شده اند،این امکان را به بـازیگران دولتـی و غیردولتـی می‌دهد که میلیون‌ها و یا شـاید دهها میلیـون ماشـین دیجیتـال را تسـخیر و کنتـرل کننـد. (Libicki, 2009: 4)

اما در جهان دیجیتال به دلیل ارزانی و دسترسی گسترده به فناوری اطلاعاتی، توانمندی قابل ملاحظه‌ای حتی برای فقیرترین دولت‌ها و کنشگران منطقه‌ای و جهانی فراهم خواهـد کرد که ممکن است برای به چالش کشیدن و تهدیـد دیگـران اسـتفاده شـود. ایـن مسـأله برخلاف فناوری های نظامی مهم عصر صنعتی است. در عصر اطلاعات، سـخت‌افزارهـا و

نرم‌افزارها به صورت گسترده در دسترس و به سادگی قابل استفاده است، در حالی که در سلاح‌های عصر صنعتی، مانند سلاح‌های هسته‌ای، موشک‌های قاره پیما، ناوهای جنگی هواپیمابر و تانک‌ها این‌گونه نیستند. بنابراین در عصر اطلاعات، دولت‌ها تنها کنشگران بین‌المللی نیستند که ممکن است توانمندی‌های فنی را توسعه دهند، تا برای آسیب‌رسانی استفاده کنند. شرکت‌های چندملیتی، سازمان‌های غیردولتی، گروه‌های جنایی و تروریستی و حتی افراد ممکن است دست به عملکردهای جنگی بزنند. (آلبرتس و پاپ، ۱۳۸۵: ٤٥)

به همین خاطر سطوح و انواع حملات سایبری روز به روز در حال گسترش است. این حملات ممکن است از به سرقت رفتن یک پسورد یا رمز عبور به حساب بانکی یک فرد تا حملات ویرانگری چون استاکس نت به تأسیسات غنی سازی هسته ای ایران متفاوت باشد.

این سنخ از حملات هم تهدید و هم فرصت تلقی می شود. تهدید برای کشورها و بازیگرانی که روز به روز زندگی خود را بیشتر و بیشتر با فضای جدید پیوند می زنند. و فرصت برای بازیگرانی که از امکان ضربه زدن و یا برآورده سازی خواست ها و منافع خود در شکل سنتی عاجز هستند و یا تمایل ندارند هزینه های تهدید سنتی به یک بازیگر دیگر را به جان بخرند.

باراک اوباما رئیس جمهور آمریکا در سال 2013 در خصوص ویژگی منحصر به فرد خطراتی که توسط حملات سایبری به زندگی بشر تحمیل می شود هشدار داد. ( Obama, 2013)وی با اشاره به خطراتی که این فضا در اختیار مهاجمان قرار می دهد نوشت: «در منازعه آینده، دشمن قادر به چالش کشیدن برتری نظامی ما نخواهد بود، بلکه به دنبال بهره‌برداری از آسیب پذیری‌های سیستم‌های کامپیوتری ما در سرزمینمان خواهد بود. از کار انداختن سیستم‌های بانکداری حیاتی می‌تواند به یک بحران مالی وحشتناک منجر شود. فقدان آب تمییز و گوارا و یا از کارانداختن کارکرد بیمارستان‌ها می‌تواند سلامت عمومی ما را به خطر اندازد. و همچنانکه در گذشته شاهد بوده‌ایم، فقدان برق می‌تواند تجارت، شهرها و مناطق منحصر به فرد ما را دچار وقفه کند. (Ibid)

## ۱.۵ جنگ سایبری

جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم های اطلاعاتی با هدف به مخاطره انداختن

عناصر اطلاعاتی دشمن (اطلاعات، پروسه های مبتنی بر اطلاعات، سیستم های اطلاعاتی و شبکه های رایانه ای) در یک فضای سایبری است. چنین عملیاتی به طور مشخص با اهداف نظامی، تجاری، سیاسی، فرهنگی و غیره انجام می پذیرد. بنابراین باید دارای ارزش افزوده و به اصطلاح بهره برداری از عناصر دشمن باشد. همان طوریکه هر نوع جنگ دیگر نیز در نهایت به سوء استفاده از منابع دشمن ختم خواهد شد. جنگ سایبری دارای اهمیت روزافزون برای مراکز نظامی، سرویس های جاسوسی، اطلاعاتی و دنیای تجارت است. ولی در مجموع هر دو دیدگاه نظامی و غیرنظامی را باید مد نظرداشت. (غروی و محمدی، ۱۳۹۰: ۷۷)

جنگ در فضای سایبر در حال تبدیل شدن به یک مفهوم اساسی است. برای این جنگ سلاح هایی نیز اختراع شده است. این سلاح‌ها می تواند قدرت یک دولت را کاهش دهد و کنترل آن را در اختیار بازیگر دیگری قرار دهد. مشکل اساسی این است که آغاز و پایان کنترل هیچ گاه مشخص نمی‌شود. در این عرصه، قدرت، دولت محور و حتی واقعیت محور نیست، بلکه می‌تواند خود را در تکنولوژی نمایان سازد که بر پایه کدهای باینری(Binary Code) یا «دو دویی» بنا شده است. قدرت، به ویژه با توجه به جنگ سایبری، همیشه باید به طور کلی و در نتیجه، بخش جدایی ناپذیر امنیت ملی و انسانی مفهوم‌سازی شود. وزارت دفاع ایالات متحده این عرصه جدید را به عنوان بخش جدایی ناپذیر امنیت ملی خود قلمداد می کند. این وزارتخانه بخش فرماندهی سایبر را تحت نام «فرماندهی سایبری ارتش آمریکا»(US Army Cyber Command (USCYBERCOM) ) ایجاد کرده که وظایفی چون : «برنامه‌ریزی، هماهنگی، انسجام، زمان بندی و هدایت فعالیت ها برای : رهبری عملیات و دفاع از شبکه‌های اطلاعاتی خاص وزارت دفاع و آمادگی برای اداره طیف کاملی از عملیات نظامی فضای سایبر به منظور بالفعل سازی اقدمات در تمام حوزه‌ها، تضمین آزادی عمل متحدان ایالات متحده در فضای سایبر و گرفتن این آزادی عمل از دشمنان» برعهده دارد. ( Clarke and Knake, 2012: 20-44)

## ۲.۵ محدودهٔ عملیاتی

برای فضای سایبر نمی توان محدوده جغرافیایی تصور نمود. بنابراین جنگ سایبر نیز دارای مرز نیست. محدوده عملیات سایبر بسیار گسترده است، از تولید پارازیت مخابراتی گرفته تا عملیات روانی، از تغییر صفحات یک وب سایت گرفته تا بمباران ایمیلی. ولی نهایتاً هدف

اصلی تهدیدات، منابع اطلاعاتی هستند، به نحوی که امنیت ملی دشمن، مورد مخاطره قرار گیرد. بنابراین بستر عملیات سایبری همانا زیرساخت های اطلاعاتی مـی باشـند. محـدوده عملیات سایبری به طور مشخص در حدود منابع دشمن است، ولی می توانـد دربرگیرنـده اشیاء خود حمله کننده نیز باشد و یا در محدوده سایبری دیگر عوامل وابسته یا غیروابسـته باشد و یا در محدوده سایبری دیگر عوامل وابسته یا غیروابسته باشد. برای تفهیم بهتر به این سناریو دقت کنید: حمله کننده ای قصد دارد، اقدام به دزدیدن اطلاعات دشـمن و فـروش آنها به شخص ثالث نماید. وی از طریق یک کانال واسطه به دشمن نفوذ می کنـد و نهایتـاً اطلاعات نیز از همان کانال منتقل می شود. سناریوی فوق دقیقا نظیر نمونه حقیقی است که برای منابع اطلاعات ایالات متحده آمریکـا محقـق گردیـد و در آن حملـه کننـده برزیلـی، اطلاعات را به طور غیر مستقیم با واسطه به جمهوری شوروی سابق فروخت.

در مورد محدوده عملیاتی باید این نکته را مدنظر داشته باشیم که بـا انتخـاب نادرسـت محدوده عملیات، بروز مشکل در محدوده سایبری خود حمله کننده نیز محتمل است. ایـن به علت نزدیکی و تداخل مرزهای سایبری است. تصـور کنیـد کـه حملـه کننـده سـایبری مبادرت به تهاجم به یک سایت اینترنتی می نماید و نهایتاً موجب پـایین آمـدن کـارآیی آن سایت می گردد، ولی هدف از پایین آمدن سایت، انهدام سرور اصلی بوده است و یکـی از سرورهای محدوده جغرافیایی حمله کننده به طور ناخواسته در محدوده عملیاتی بوده است. این مشکل به ویژه با انتشار و نامتمرکز بودن خدمات ثبت دامنه، میزبانی فضای وب، ثبـت آدرس اینترنتی و ارائه پهنای باند بسیار محتمل و رایج است.

بعنوان نمونه هایی از محدوده های عملیات سایبری، می توان از موارد ذیل نام برد:

- اشیاء بسترساز شبکه (روترها، سوئیچ ها، ماهواره ها)
- عناصر وب (سایت های وب، پایگاه اطلاعاتی مبتنی بر وب)
- ایمیل بعنوان رایج ترین عنصر گذشته و حال در فضای سایبر.

از سویی دیگر برای جنگ و عملیات تخریبی در فضای سـایبر نمـی‌تـوان محـدودیتی تصور کرد. در حقیقت جنگ سایبری دارای مرز نیست. ولی باید در نظر داشت که تجسـم به علت مقایسه مستقیم فضای سایبر با دنیای حقیقی و بر اساس دانسـته‌هـا و قراردادهـای فیزیکی می‌باشد. در عمل فضای سایبری نیز دارای مرز است. در حقیقـت مرزهـا در عـین همبستگی کاملاً گسیخته هستند و این تصور نیز به سبب تجسم فیزیکی حاصل می‌گردد.

## ۳.۵ گونه‌شناسی ابزارهای جنگی در فضای سایبر

ابزارها و جنگ افزارهای سایبر برای خشونت سایبری بسیار متفاوت است. مصداق‌های فراوانی را می توان برای آن در نظر گرفت که می تواند منجر به تهدید زیرساخت های زندگی شود. روز به روز نیز این ابزارها رو به تزاید می گذارد. قبل از پرداختن به ابزارهای مورد استفاده در جنگ سایبر لازم است الگوی کلی جنگ سایبری را تشریح کنیم. این کار برای توضیح و تبیین چگونگی کاربرد ابزارها در حوزه های متعدد ضروری است.

در یک مدل واقع گرایانه با توجه به محدوده عملیات، جنگ سایبری از سه بخش عمده؛ جنگ شبکه ای، جنگ رایانه ای و جنگ فرماندهی و کنترل تشکیل شده است.

حوزه های اصلی جنگ شبکه ای عبارتند از : «جنگ های چندرسانه ای، فرهنگی، دیپلماتیک، اقتصادی، روانی و ...» (غروی، محمدی، ۱۳۹۰ : ۷۵)

جنگ رایانه ای معمولاً در محیط اطلاعاتی محلی یا جهانی رخ می دهد و هدف آن تسلط (آگاهی یا تخریب) بر اطلاعات است. در این مدل مهمترین بخش، جنگ فرماندهی و کنترل است که جنگ الکترونیک یا جنگهای فیزیکی مرسوم، تنها زیربخش هایی از آن محسوب می شوند. این بخش از اجزای زیر تشکیل شده است: جنگ الکترونیک، فریب نظامی، عملیات روانی، امنیت اطلاعات، تخریب فیزیکی، تخریب غیرفیزیکی.

در این مدل نحوه عملکرد همان حمله و دفاع رایج است و دارای مولفه های زیر است:

انگیزه: بدون شک، حمله کننده باید دارای انگیزه مشخص مستقیم یا غیر مستقیم باشد. در غیر این صورت، مراحل بعدی دارای بستر و پایه منطقی نخواهند بود.

هدف: باتوجه به انگیزه، محدوده عملیات مشخص می گردد. این همان چیزی است که آن را هدف می نامیم. هدف ممکن است به بزرگی و گستره شبکه توزیع نیرو، در یک کشور باشد و یا به کوچکی یک سیستم در یک شبکه محلی باشد. در اینجا بزرگی و کوچکی هدف مهم نیست، بلکه ارزش هدف تعیین کننده است. در عملیات سایبری، یک هدف که در شکل فیزیکی بسیار کوچک است، می تواند دارای ارزشی بزرگتر و بیشتر از کیلومترها خاک داشته باشد.

جمع‌آوری اطلاعات: هر عملیاتی چه فیزیکی و چه سایبری باید با آگاهی صورت پذیرد. بدون اطلاعات فقط نیرو و منابع از دست می رود، ضمن آنکه احتمال ردیابی و شناسایی برای دشمن افزایش می یابد. کسب اطلاعات از عناصر سایبری دشمن به عنوان

مهمترین بخش از عملیات سایبری مورد توجه است. از دید کارشناسان جمع آوری اطلاعات از اهداف سایبری به مفهوم انجام پنجاه درصد از کل عملیات است. در اینجا، اطلاعات به مفهوم هر جنبه از هدف است که به نحوی با ایمنی سایبری آن در ارتباط باشد: بلوک ها و آدرس های اینترنتی/اینترانتی، اسامی دامنه های عمومی و خصوصی، سرویس‌های مبتنی بر پروتکل اینترنت (TCP/IP)، معماری سیستم ها و شبکه ها، مکانیسم‌های تصدیق و ... جمع آوری اطلاعات شامل شناسایی، وارسی و کنکاش می شود.

نقاط ضعف: وقتی اطلاعات حمله کننده درباره ماهیت سایبری هدف کامل شد، این مرحله آغاز می شود. این بخش ساده ترین قسمت عملیات است. با دانستن مشخصات هدف، تعیین عیوب سخت افزاری و نرم افزاری چندان دشوار نبوده و فقط زمان لازم است. اگر دشمن به چنین مرحله ای برسد، انجام حمله قطعی است.

نفوذ: پس از تعیین نقاط ضعف و یا در نظر گرفتن اطلاعات به دست آمده و با آگاهی از مکانیسم های ردیابی، عملیات سایبری در جهت نفوذ به هدف آغاز می شود.این مرحله اگرچه بخش پایانی عملیات است، ولی زمان بیشتری را به خود اختصاص می دهد، زیرا دارای قسمت های متعدد است. در جدول ذیل این ابزارها دسته بندی شده است:

**جدول شماره ۱. (Cheswick et al., 2003: 95-118)**

| نوع ابزار سایبر | مصداق |
|---|---|
| سرقت(Theft) | رمزعبورها، اطلاعات حساس از طریق تخمین و حدس، سرقت یا به خطر افتادن سیستم های کامپیوتری |
| باگ ها[۲]/ بک دورها[۳] | کدگذاری غلط، سختی در یافتن نتایج یک برنامه در سیستم قربانی |
| شکست احراز هویت (Authentication failure) | شکست در ورود به سایت بواسطه مداخله‌گری یا به خطرافتادن سرور |
| شکست پروتکل( Protocol failures ) | رد دسترسی به نرم افزارها به واسطه پروتکل معیوب |
| تراوش اطلاعات (Information leakage) | جاسوسی از کامپیوتر |
| حملات نمایان (Exponential attacks ) | استفاده از ویروس ها و کرم هایی که به سرعت گسترش می یابند و منجر به خسارت به سیستم های کامپیوتری می شوند |
| حملات ویرانگر خدمات( Denial of service attacks ) | استفاده بیش ازحد و فشار برسخت افزارها برای تعطیلی و یا کاهش خدمات |

| | |
|---|---|
| بات‌نت‌ها[۴] | جاسوسی، اسب های تروا و کرم ها |
| حملات فعال | مزاحمی که اطلاعات را حذف می کند، تغییر می دهد و به جای آن اطلاعات خود را ارسال می کند. |

## ۶. بازدارندگی در عرصهٔ سایبر

درهم تنیدگی دنیای کنونی در عصر ارتباطات و فناوری اطلاعات، در کنار فرصت های بی‌نظیری که بوجود آورده، نگرانی‌هایی را نیز در پی داشته است. یکی از این نگرانی‌های حائز اهمیت، مسائل مربوط به امنیت ملی است که فعالیت‌های سایبری نظیر حملات سایبری یا جاسوسی آن را به شدت مورد تهدید قرار می دهند. روزانه هزاران حمله سایبری در جهان رخ می دهد و مانع از آن می شود که بتوان بین حملات جدی و نه چندان جدی تمایزی قائل شد(Kramer, 2009: 15) . با گسترش فناوری‌های اطلاعاتی و نفوذ هرچه بیشتر این فناوری‌های در حیات شخصی و ملی افراد، دامنه و شدت این تهدیدات نیز گسترده‌تر می شود، مخصوصاً در جوامعی که افراد آزادی بیشتری در استفاده از فناوری‌ها دارند. از این رو لازم هست که کشورها، تدابیری را برای مقابله با این تهدیدات اتخاذ کنند. استراتژی بازدارندگی یکی از نظریه های امنیتی سنتی هست که می‌تواند در عرصه سایبری نیز کارایی خاص خود را داشته باشد.

از عصر یونان باستان، بازدارندگی بخشی از دکترین امنیتی- سیاسی کشورهای غربی بوده است(George and smoke,1974:12). این استراتژی نقش بسیار کلیدی در رویارویی دو ابرقدرت در طول جنگ سرد و عصر سلاح های هسته‌ای ایفا کرد و همچنان نقش مهمی در سیاست جهانی داشته و حتی می‌تواند در جهان سایبر نیز به کار گرفته شود. همچنان که در حال حاضر نیز عنصر اساسی در استراتژی امنیت ملی دولت آمریکا به شمار میرود(Bunn, 2007). در واقع، در عین حال که عملیات سایبری توانمندی‌های مناسبی را در اختیار دولت ها قرار می دهد که در راستای اهداف ملی خود گام بردارند، همزمان ابعاد جدیدی از مفهوم بازدارندگی را مطرح می سازد که برخی از این ابعاد در راستای مفهوم سنتی بازدارندگی هست و برخی دیگر نیز تازگیدارند. این ابعاد، از حیث مباحث حقوق بین الملل و مسائل سیاسی بحث‌های زیادی را به خود اختصاص داده‌اند. اما ما در این مقاله به ابعاد عملیاتی و سیاسی آن می‌پردازیم تا کارآمدی آن در سیاست‌های امنیت ملی کشورها را مورد مداقه قرار دهیم.

آمریکا از مدت‌ها پیش به اهمیت فضای سایبر و تهدیدات و فرصت‌های آن آگاه بوده و پیشگام پژوهش‌های مختلف در این زمینه بوده است. ژنرال کارترایت(General Cartwright) در این زمینه معتقد است که آمریکا نیازمند آن هست کـه نوعیتوانمنـدی در فضـای سـایبر برای خود ایجاد کند تا در مقابل تهدیدات دیگران از این توانمندی استفاده کرده و بـا آنهـا مقابله به مثل کند. کشورهای دیگری همچون چین و هند نیز درصدد ایجـاد یـک سیسـتم تهاجمی تلافی‌جویانه برای مقابله با تهدیدات جدی و یا بازداشتن دیگر بازیگران از تهدیـد سایبری علیه منافع ملی خودشان هستند(Bagchi, 2008). تعجـب برانگیـز هـم نیسـت کـه جوامعی که توانمندی حملات سایبری خود را تقویت می‌کنند، منافعشان ایجاب می کند که قدرت بازدارندگی خود در عصر سایبر را تقویت کنند تـا جـوامعی کـه توانمنـدی تلافـی جویانه آنها بر ابزارهای متعارف تکیه دارد.

هدف از بازدارندگی در عرصه سایبری، ایجاد تمایز بین آغاز و انجام اقدامات خصومت آمیز است. کشوری که دارای قابلیت بازدارندگی در عرصه سایبری است تهدید می کند که رفتارهای نامناسب در این عرصه را مجازات خواهد کرد، اما در عین حال ایـن موضـوع را تلویحاً اعلام می کند که اگر رفتار نامناسبی شکل نگیرد و یا خطوط قرمز آن نادیده گرفتـه نشوند، تنبیهی هم در کار نخواهد بود.

ریچارد کاگلر(Richard L. Kugler) که کارشناس صـاحب نـامی در زمینـه سیاسـتگذاری امنیت ملی هست، بـه دلیـل محـدودیت هـای اقـدامات دفـاعی، بـه شـدت از اسـتراتژی بازدارندگی دفاع می کند (Kugler, 2009: 309). پاتریک مورگان، رئیس گروه صلح و منازعه و علوم سیاسی در دانشگاه کالیفرنیا نیز بر آن است که تحلیل‌گران سنتی نظریه بازدارنـدگی واقعاً گیج شده اند که چرا آمریکا تلاش زیادی نمی کند تا ایـن اسـتراتژی ارزشـمند را بـه شکل کارآمدی در حوزه سایبری به کار بندد. سوالی که اینجا مطرح می شود این است کـه یک استراتژی بازدارندگی کارآمد باید واجد چه ویژگی‌هایی باشد؟

## ۱.٦ بازدارندگی کارآمد در عرصهٔ سایبری

هدف از استراتژی بازدارندگی، کاهش یا از بین بردن خطر حمله با افزایش هزینه‌هـا اسـت تا مهاجم را به این نتیجه برساند که هزینه های حمله بیش از منافع آن است. برای کاربست این استراتژی داشتن دو نوع توانمندی بسیار حیـاتی و کلیـدی هسـت. اولـین توانمنـدی، داشتن قابلیت دفاعی مستحکم و قوی است که باعث شود مهاجم برای شروع حمله خـود

احتیاط بیشتری به خرج داده و تأمل بیشتری کند. در عرصه سایبری، داشتن این توانمندی برای مقابله با اکثر حملات بسیار عملیاتی و مفید خواهد بود.

مورد دوم، توانمندی قابل ملاحظه اقدامات تلافی جویانه است. اگر تعدادی از مهاجمان با اقدامات تلافی جویانه شدیدی روبرو شوند، به احتمال زیاد مهاجمان دیگر از روی آوردن به حمله سایبری نیز خودداری خواهند کرد.

آن‌چیزی که بازدارندگی در عرصه سایبری را از مفهوم سنتی آن متمایز می‌کند، مشکل شناسایی منبع حمله است. در جهان سایبری، این امر مانع بسیار عمده‌ای برای اتخاذ اقدامات تلافی جویانه است. چرا که قلمرو دیجیتال، عرصه گم‌نامی است. بنابراین، این چالش بعد مهم سومی را به استراتژی بازدارندگی در عرصه سایبری اضافه می کند و آن چالش شناسایی(attribution) است. از این رو، استراتژی بازدارندگی سایبری دارای سه بعد مهم به شرح زیر است:

۱- دفاع:یک سیستم دفاعی مستحکم اولین گام در راه محافظت از منابع و زیرساخت‌های کشورها در برابر اکثر مهاجمان بوده و اغلب آنها را از انجام حمله منصرف می سازد.

۲- شناسایی: توانمندی مرتبط ساختن حمله ای به یک بازیگر یا منبع خاص، عنصر کلیدی دیگری در عرصه سایبری است که اعتبار و مشروعیت بازیگر را در عرصه داخلی و خارجی حفظ می کند.

۳- تلافی کردن: تمایل و توانمندی تلافی بر علیه هر حمله ای از هر منبعی و تحت هر شرایطی باید ایجاد شود.

### ۱.۱.۶ دفاع

برای دست یابی به قدرت دفاعی مطلوب و کارآمد در عرصه سایبر باید به خوبی بر ویژگی‌های این حوزه تسلط داشت. فرانکلین کرامر، معاون سابق وزیر دفاع و نویسنده کتاب قدرت سایبری و امنیت ملی بر این اعتقاد است که سایبر از سه منظر شبیه زمین است: بازیگران متعدد هستند، موانع ورود بازیگران به این عرصه محدود است و بستر مناسبی برای ناشناس ماندن و مخفی شدن نیز فراهم است(Kramer, 2009: 12).اما بر خلاف زمین، فاصله جغرافیایی زیادی بین مهاجم و هدف آنها در عرصه سایبری وجود دارد. این عامل همراه با عنصر گم نامی می‌تواند ترس از تلافی را کاهش دهد. به عنوان مثال،

دانشجویی که در مسکو در کافی‌نتی در حال قهوه خوردن و نفوذ به شبکه زیرساختی یکی از نهادهای دولتی آمریکاست نگرانی کمتری از اقدامات تلافی جویانه آمریکا دارد تا بازیگری که بخواهد به صورت مستقیم علیه آن نهاد حمله نظامی انجام دهد.

تقریباً هیچ کشوری در دنیا نیست که بتواند روزانه در مقابل هزاران حمله سایبری اقدامات تلافی جویانه انجام دهد و یا عاملان آنها را شناسایی کند(Morgan,2010:59). بنابراین، اولین عنصر نظریه بازدارندگی در عرصه سایبری، قدرت دفاعی قوی باید باشد. بدان معنا که سخت افزارها و نرم افزارها به شکل مستحکمی با یکدیگر امتزاج یافته و بتواند هر نوع دسترسی غیرمجازی را تقریباً غیرممکن سازد. این امر دو هدف عمده را برآورده می سازد: اولاً که باعث می‌شود اغلب افراد غیرمجاز نتوانند وارد سیستم شوند. دوم اینکه افراد غیرمجاز را از تلاش برای نفوذ در سیستم باز می دارد چرا که احتمال موفقیت خود را کم می بینند(Kugler,2009:334). هدف اصلی مولفه دفاعی آن است که مهاجمان علاقمند را از انجام حمله منصرف سازد یا آنها را بلوکه کند. بدین طریق، با کاهش میزان مهاجمان، بقیه موارد حمله را می توان با مولفه اقدامات تلافی جویانه از حملات بعدی منصرف ساخت.

### ۲.۱.۶ شناسایی

مسأله شناسایی یک مشکل شناخته شده جهانی در عرصه سایبری هست. حضور گسترده و بی‌شمار کاربران و ماهیت نسبتاً ناشناس آنها در حوزه سایبری باعث می شود که مسأله شناسایی مهاجم و نسبت دادن حمله سایبری به فرد یا گروه خاصی مشکل‌تر از دوران بازدارندگی هسته‌ای باشد(Kramer,2009:12). دولت‌ها می‌توانند برای پنهان ماندن از شناسایی شدن، اقدامات خود را توسط افراد یا گروهی از کاربران انجام دهند و هر اتهامی را به راحتی منکر شوند. افراد و گروه ها نیز می‌توانند بدون پشتوانه مالی قابل توجه، به تأسیسات دولتی یا شرکت های خصوصی حمله کنند.

اما همه این موارد بدان معنا نیستند که شناسایی مهاجم کاملاً غیرممکن است. چرا که نمونه های موفق زیادی در این خصوص وجود دارند. عاملان حمله سایبری به شبکه‌های اطلاعاتی در استونی در سال ۲۰۰۷ و گرجستان در سال ۲۰۰۸ به سرعت شناسایی شدند که ماهیت روسی داشتند. اخیراً هم روزنامه نیویورک تایمز با بهره‌گیری از کارشناسان سایبری توانست هکرهایی راشناسایی کند که اسم کاربری و رمز عبور آن را ربوده و دست

به اقدامات غیرقانونی در فضای سایبر می‌زدند. آنان هم تبعه چینی بودند(Goodman,2010:105). این نمونه‌ها نشان می‌دهند مسأله شناسایی آن چنان هم غیرقابل حل نیست و می‌توان به طور نسبی بر این چالش نیز فائق آمد. در عمل، بسیاری از حملات سایبری تا مکان اعمال آن شناسایی شدند هر چند که برخی هکرها از مجازات گریخته اند. با سرمایه گذاری در نیروی انسانی و بخش تکنولوژی می‌توان بر این چالش نیز چیره گشت.

علیرغم وجود این چالش‌ها در حوزه شناسایی، باید به این امر اشاره داشت که این مولفه همچنان بخش کلیدی و اساسی نظریه بازدارندگی در حوزه سایبری هست. چرا که شناسایی موفق، متضمن موثر و مفید بودن اقدامات تلافی جویانه است و باعث می‌شود که تهدیدات واقعی از بین بروند. شناسایی موفق عاملان حمله، اعتبار و مشروعیت دولت‌ها را در داخل و جامعه بین المللی افزایش می دهد.

### ۳.۲.۶ اقدامات تلافی‌جویانه

استراتژی بازدارندگی بدون اقدامات تلافی جویانه موفق نخواهد بود. در نبود اقدامات تلافی جویانه، مهاجمان بالقوه هم انگیزه ای برای خودداری از حمله ندارند. مورگان بر این اعتقاد است که کارآمدی اقدامات تلافی جویانه متضمن دربرگرفتن سه شاخص عمده است: غیرقابل قبول بودن آن برای دشمن؛ عملیاتی بودن آن و قابل قبول بودن آن برای طرف تلافی کننده و همچنین پذیرش جامعه جهانی(Morgan, 2010:56).

برای مقابله با بازیگران غیردولتی، اتخاذ اقدامات تلافی جویانه متناسبجرم رخ داده، چالش‌هایی را برای دولتها بوجود می‌آورد چرا که هنوز قوانینی در حقوق بین الملل برای این موضوع تصویب نشده است. به همین منظور، کشورها باید به شدت در این زمینه فعال بوده و دقیقاً اقدامات غیرقانونی را تعریف کنند. این امر می‌تواند در فرآیند قضایی و دادخواهی خیلی موثر واقع شود.

علیرغم چالش حقوقی، مقابله با تهدید بازیگران غیردولتی بسیار حائز اهمیت هست. بسیاری از حملات سایبری روزانه به دلیل عدم ترس مهاجمان از تلافی است. دولتها اگر در پی کاستن از میزان این حملات مخرب هستند باید در عمل نشان دهند که مهاجمان از تیغ تلافی آنها در امان نخواهند بود. لازم نیست که اقدامات تلافی جویانه، شبیه اقدام

مهاجم باشد. زمانیکه رفتارهای سایبری غیرقانونی دقیقاً مشخص و تعریف شدند، آن‌گاه دستگیری و بازداشت آنها نیز گزینه های مناسبی خواهند بود.

مسأله تلافی در روابط بین کشورها متفاوت از افراد و بازیگران غیردولتی است و چالش دیگری را پیش می کشد. چرا که می تواند تبعات و آثار پیچیده ای بر روابط بین دو کشور داشته باشد. اما برای انجام اقدامات تلافی جویانه علیه کشور مهاجم، بازیگران دولتی نباید اقدامات خود را محدود به حوزه سایبری کنند. بلکه برای بیشینه سازی کارآمدی بازدارندگی در حوزه سایبری، دولت ها باید آمادگی خود را برای اتخاذ انواع اقدامات تلافی جویانه در حوزه های مختلف از تحریم‌های اقتصادی و ضبط اموال کشور مهاجم گرفته تا انواع اقدامات دیپلماتیک و سیاسی و حتی اقدام نظامی نشان دهند.

اقدامات تلافی جویانه بر علیه کشورها ضرورتاً لازم نیست با اقدام طرف مقابل متناسب باشد. یعنی کیفر حتما نباید متناسب با جرم باشد. اما باید واقعیت‌های ژئوپلتیکی را هم مدنظر داشت. رهبران باید همواره این محاسبه را انجام دهند که چه نوع اقدامی بهتر می‌تواند مانع از اقدامات مشابه در آینده شود. اما اقدام اتخاذ شده باید به قدری شدید باشد که هر مهاجم بالقوه دیگری را از انجام حمله در آینده منصرف سازد. همچنین این اقدام باید بتواند مشروعیت لازم را داشته و حمایت دیگر بازیگران از اقدامات تلافی جویانه آتی را در پی داشته باشد.

پرچالش ترین اتفاقات سایبری زمانی است که نتوان عاملان حمله ای را شناسایی کرد. مورگان بر این باور است که در نظریه بازدارندگی کلاسیک، شناسایی غیرضروری است و هر کشوری می تواند در قبال حمله ای که از خاک آن کشور به کشور دیگر انجام می شود مسئول قلمداد شود(Morgan,2010:70). اما پذیرش این قاعده در حوزه سایبری می تواند تنها در ارتباط با حملات خیلی شدید اتفاق افتد. گودمن نیز از این نظریه دفاع می کند که اگر رفتاری غیرقانونی قابل تفویض به کشوری باشد آنگاه مسأله شناسایی دقیق مهاجمان ضروری نخواهد بود(Goodman, 2010:79). علیرغم نظرات فوق، عملی کردن آنها در دنیای واقعی پرچالش خواهد بود و رهیافت مناسبی برای برخورد با حملات سایبری نخواهد بود. چرا که تنبیه یک کشور به دلیل حملات سایبری توسط افراد گمنام تا حدود زیادی به شرایط ژئوپلتیکی، اقتصادی و دیپلماتیک ارتباط پیدا می کند(Kugler,200: 328). همچنین کشورها نمی تواند این هنجار و رویه را ایجاد کنند که به دلیل حمله سایبری افرادی از

خاک یک کشور علیه آنها، خود آن کشور را متهم بدانند، چرا که این هنجار مـی توانـد در آینده علیه خود آنها نیز به کار رود.

## ۷. نتیجه‌گیری

ماهیت حوزه سایبری متفاوت از دنیای واقعی است و نظریه بازدارندگی سایبری نمی‌توانـد کارآیی دوران جنگ سرد و عصر هسته‌ای را داشته باشد. این استراتژی نمی تواند راه حـل نهایی برای جرائم سایبری، جاسوسی و حملات سایبری باشد. همچنین فـارغ از کارآمـدی آن، نمی تواند جرائم سایبری را کاملاً ریشه کن سازد. اما نقش کلیدی در کاهش حمـلات سایبری به تعداد قابل مدیریتی دارد که آنها را هم می توان با اقدامات تلافی جویانه و هزینه کمتر کاهش داد.

برای کارآمدی بازدارندگی در حوزه سایبر، باید از ترکیب سه مولفه کلیدی یعنی دفـاع، شناسایی و تلافی بهره جست. بدون اقدامات دفاعی مناسب، نمی توان تعداد حملات موفق را برای شناسایی کردن کاهش داد و این حملات از کنترل خارج می شـوند. فنـاوری‌هـای شناسایی باید منابع حمله را بتوانند شناسایی کنند تا مـانع از اقـدامات مهاجمـان بـالقوه در آینده از ترس شناسایی شدن شوند. تلافی از آن رو حائز اهمیت است که نشـان مـی دهـد اقدام سایبری علیه دولتی یا مردم و نهادهای آن، حتماً با مجازاتی روبرو خواهد شد.

## پی‌نوشت‌ها

۱. این مدل تحت عنوان (PIME) مخفف عبـارات، Political، Informational، Military و Economic قرار می گیرد و به عنوان یکی از مدل های مطرح برای بررسی عناصر قدرت محسوب می شود.

۲. باگ ها ( Bugs) در اصطلاحات کامپیوتر آن را «اشکال» یک برنامه یا هر سیسـتم عامـل و یـا ... معنی می‌کنند. در واقع اگر نرم‌افـزار یـا حتـی سیسـتم عـاملی اشـکالی داشـته باشـد اصـطلاحاً باگ دارد..

۳. بک دورها (back doors) که در فارسی به در پشتی نیز ترجمه شده است، آسیب‌پـذیری خاصـی در رایانه‌ها وجود دارد که به هکرها و حمله‌کنندگان فرصت می‌دهد تا مکانیزم‌های امنیتی معمول را دور زده و به صورت غیرمجاز به منابع و اطلاعات سیستم دسترسی داشته باشند. از آنجـا کـه این تهدید در پس‌زمینه فعال بوده و خود را از کاربر پنهان می‌سازد، شناسایی و حذف آن کـاری تقریباً مشکل است.

٤. بات‌نت‌ها (Botnet ) شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از کامپیوترها که بات (bot) نامیده می‌شوند، تشکیل می‌شوند. این شبکه‌ها توسط یک و یا چند مهاجم که botmasters نامیده می‌شوند، با هدف انجام فعالیت‌های مخرب کنترل می‌گردند. به عبارت بهتر بات‌ها کدهای مخربی هستند که بر روی کامپیوترهای میزبان اجرا می‌شوند تا امکان کنترل نمودن آن‌ها از راه دور را برای botmasterها فراهم نمایند و آن‌ها بتوانند این مجموعه را وادار به انجام فعالیت‌های مختلف نمایند.

## کتاب‌نامه


آلبرتس، دیوید س و دانیل س پاپ (۱۳۸۵)، گزیده ای از عصر اطلاعات؛ الزامات امنیت ملی در عصر اطلاعات، ترجمه علی علی آبادی و رضا نخجوانی، تهران: پژوهشکده مطالعات راهبردی.

روزنا، جیمز و دیگران (۱۳۹۰)، انقلاب اطلاعات، امنیت و فناوری های جدید، ترجمه؛ علیرضا طیب، تهران: پژوهشکده مطالعات راهبردی.

کاستلز، مانوئل(۱۳۸۰)، عصر اطلاعات: اقتصاد، جامعه و فرهنگ، مترجمان؛ احمد علیقلیان، افشین خاکباز، تهران: طرح نو.

غروی حسین، محمدی علی (۱۳۹۰) معرفی رویکردها و متدولوژیهای طراحی واجرای سناریوهای مقابله با تهدیدات سایبری، تهران: انتشارات دانشگاه دفاع ملی، مجموعه مقالات همایش ملی دفاع سایبری.

منوچهری، عباس (۱۳۷٦)، قدرت، مدرنیسم و پست‌مدرنیسم،اطلاعات سیاسی اقتصادی، شماره ۱۲۲-۱۲۱.

هانس جو اکیم مور گنتا (۱۳۸۹)،سیاست میان ملتها: تلاش در راه قدرت و صلح، مترجم: حمیرا مشیرزاده، تهران: وزارت امور خارجه.

Bagchi, Indrani (2008), "China Mounts CyberAttacks on Indian Sites," The Times of India, May 5, 2008.

Bajaj, Kamlesh. (2010), The Cybersecurity Agenda. Mobilizing for International Action. available via The EastWest institute.http://ewi.info/system/files/Bajaj_web.pdf.

Benedikt Michael. (1992) Cyberspace: First Steps, Cambridge, MIT Press.

Betz J. David andStevens Tim (2011),Cyberspace and The State: Toward a Strategy For Cyber - Power, The International Institute for Strategic Studies (IISS)

Bollier, David (2003), The Rise of Netpolik; How the Internet Is ChangingInternational Politics and Diplomacy,A Report of the Eleventh Annual Aspen InstituteRoundtable on Information Technology.

Bryant, Rebecca (2001), What Kind Of Space Is Cyberspace?, Minerva, 5:138-155.

Bunn, M. Elaine (2011), Can Deterrence Be Tailored? Strategic Forum, No. 225.

Cheswick William R. andBellovin Steven M. (2003), Firewalls and Internet Security: Repelling the Wily Hacker (2nd Edition).

Clarke Richard A. and Knake Robert. (2012), Cyber War: The Next Threat to National Security and What to Do About It, Paperback press.

Crampton, JeremyW. (2004), The Political Mapping of Cyberspace,Chicago: University of Chicago Press.

Eriksson, John and Giocomello(2006), "The Information Revolution, Security, and International Relations: (IR) relevant Theory?" International Political Science Review (2006), Vol. 27, No. 3, 221-244.

George, Alexander L. and Richard Smoke (1974), Deterrence in American Foreign Policy: Theory and Practice, New York: Columbia University Press.

Gibson, W. (1984) Neuromancer. New York, Ace Books.

Goodman, Will (2010), "Cyber Deterrence: Tougher in Theory than in Practice," Strategic Studies Quarterly, Vol.4, No.3.

Kramer, Franklin D .et al (2009), Cyberpower and National Security, Dulles: National Defense University Press and Potomac Books.

Kuehl T. Daniel (2009) From Cyberspace to Cyberpower: Defining the Problem," in FD Kramer, S. Starr, L.K. Wentz (ed. ) (2008), Cyberpower and National Security, National Defense University Press, Washington (DC)

Kugler, Richard L. (2009), "Deterrence of Cyber Attacks," in Franklin D. Kramer et al (2009), Cyberpower and National Security, Dulles: National Defense University Press and Potomac Books, Inc.

Libicki, Martin C. (2009)Cyber deterrence and cyberwar, USA, Rand Corporation.

Lin, Herbert. (2011) 'Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion', inGeorgetown Journal of International Affairs, Special Issue, International Engagement on Cyber:Establishing International Norms and Improved Cybersecurity, pp. 127–135.

Morgan, Patrick M. (2010), "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," paper presented at a workshop on deterring cyberattacks, Washington DC.

Nye, J (2011), The Future of Power in the 21st Century, New York: Public Affairs Press.

Obama, Barack. (2013), Improving Critical Infrastructure Cybersecurity, available via: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

President Ronald Reagan, (1988) National Security Strategy of the United States, available at :http://history.defense.gov/HistoricalSources/NationalSecurityStrategy.aspx

Starr ,Stuart H. (2008), Developing a theory of cyber power, in FD Kramer, S. Starr, L.K. Wentz (ed. )Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber:Establishing International Norms and Improved Cybersecurity, pp. 127–135.