رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی
دوفصل‌نامهٔ علمی ـ پژوهشی، سال هشتم، شمارهٔ اول، بهار و تابستان ۱۳۹۷، ۶۱-۸۸

قدرت بازدارندگی در فضای سایبر

اردشیر زابلی‌زاده*

پیمان وهاب‌پور**

چکیده

وضعیت «آنارشیک»گونهٔ فضای سایبرْ تأثیرات عمیقی در 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؛ استراتژی بازدارندگی می‌تواند در این زمینه به‌کار آید. مقالهٔ حاضر به بررسی این موضوع می‌پردازد که آیا استراتژی بازدارندگی در فضای سایبر کارآمدی دارد یا نه و شرایط این کارآمدی چیست. یافته‌های این پژوهش نشان می‌دهد که هرچند استراتژی بازدارندگی نمی‌تواند همانند دوران جنگ سرد در فضای مجازی نیز کارآیی داشته باشد، پتانسیل زیادی برای محافظت از منافع و امنیت ملی کشورها دارد. سه مؤلفهٔ اساسی برای کارآمدی این استراتژی نیز شناسایی شد که عبارت‌اند از قدرت دفاعی زیاد، قابلیت شناسایی مهاجم و توان‌مندی انجام اقدامات تلافی‌جویانهٔ سخت. «شناسایی» مؤلفهٔ کلیدی و اساسی نظریهٔ بازدارندگی در حوزهٔ سایبری است؛ چراکه شناسایی موفقْ متضمن مؤثر و مفید بودن اقدامات تلافی‌جویانه است و باعث می‌شود که تهدیدات واقعی از بین برود. هم‌چنین یافته‌های این مقاله نشان می‌دهد که استراتژی بازدارندگی، بدون اقدامات تلافی‌جویانه، موفق نخواهد بود. در نبود اقدامات تلافی‌جویانه، مهاجمان بالقوه هم انگیزه‌ای برای خودداری از حمله ندارند.

کلیدواژه‌ها: بازدارندگی، فضای سایبری، شناسایی، دفاع، اقدامات تلافی‌جویانه.

---

* استادیار و رئیس دانشکدهٔ ارتباطات صداوسیما (نویسندهٔ مسئول)، azmmf9432@gmail.com
** دکترای روابط بین‌الملل از دانشگاه علامه طباطبایی، pvahabpoor@gmail.com
تاریخ دریافت: ۱۳۹۶/۱۱/۱۸، تاریخ پذیرش: ۱۳۹۷/۰۲/۱۵

۱. مقدمه

قدرت سایبری امروزه بُعد مهمی از زیست‌وارهٔ جهانی را شکل می‌دهد. اطلاعات و فناوری‌های اطلاعاتی در سپهر سیاسی، اقتصادی، و نظامیْ نقشی حیاتی ایفا می‌کنند و مقدمات فعالیت‌های عملیاتی را فراهم می‌آورند. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این باره ایجاد می‌شود؛ این گسترش درکنار آثار مثبت در بهبود زیست جهانی برخی ابعاد منفی نیز دارد که حتی ممکن است آثار آن مخرب‌تر از جنگ‌های نظامی باشد و امنیت ملی و حیات مردم را به چالش بکشاند. با توسعهٔ فناوری‌های اطلاعاتی، خطرات دیگری هم‌چون حملهٔ مجازی یا جاسوسی سایبری در کمین تصمیم‌سازان و سیاست‌گذاران کشورهاست. ولی باتوجه‌به هزاران حملهٔ سایبری که درطی روز اتفاق می‌افتد، کار تمیز حملات جدی و مهم از حملات ناکارآمد و جزئی بسیار سخت شده است.

آن‌چه در زمینهٔ کنترل فضای مجازی چالش برانگیز است تفاوت ماهوی آن با دنیای واقعی است و همین امر هم کار را بر دولت‌مردان سخت می‌کند. بخش مهمی از ظرفیت‌های دولت‌های ملی در عصر کنونی معطوف به افزایش توانمندی برای برقراری امنیت و افزایش قدرت است. قدرت، به‌طور سنتی، بر افزایش توانمندی‌های نظامی، اقتصادی، و سیاسی و تحکیم پایه‌های حکومت ازطریق حکومت خوب و ایجاد هم‌بستگی ملی صورت می‌گیرد. تهدیدها نیز ازطریق افزایش و تقویت چنین ظرفیت‌هایی دفع یا تعلیق می‌شود.

در فضای سایبر ما با وضعیتی متفاوت مواجه هستیم. دولت‌ها، افراد، سازمان‌های بین‌المللی، دانشگاه‌ها و غیره، به‌رغم استفاده و بهره‌گیری از این فضا، روزبه‌روز دچار آسیب‌پذیری بیش‌تری دربرابر تهدیدات جدید می‌شوند. فضای سایبرْ حاکمیت و قدرت را تنها به‌دست دولت نسپرده است؛ لویاتان حاکمی بر این فضای هزارسر وجود ندارد.

شاید بتوان گفت فضای سایبر هنوز دوران «وضع طبیعی» خود را می‌گذراند. دردیدگاه توماس هابز، استقرار دولت قدرت‌مند (لویاتان) برای پایان دادن به وضع طبیعی ضروری است. لویاتان نیز ازطریق قرارداد اجتماعی، که افراد با یک‌دیگر منعقد می‌کنند، به‌وجود می‌آید. ازنظر هابز، زمانی حاکمیت مستقر می‌شود که تعداد کثیری از افراد با یک‌دیگر توافق کنند که حق نمایندگی را به آن اعطا کنند. بدین‌سان هابز به پاسخی برای پرسش قدرت می‌رسد که خود آن نیز قدرت‌محور است. لویاتان فراقدرتی است که، ضمن نفی قدرت

فردی، درخدمت تضمین بقای فرد در حیات جمعی قرار می‌گیرد. به‌عقیدهٔ هابز، غلبهٔ خصلت قدرت‌جویی ازیک‌سو و میل به بقا ازسوی‌دیگر انسان‌ها را به ضرورت پذیرش این فراقدرت سوق می‌دهد (منوچهری ۱۳۷۶: ۳۳).

اما در فضای سایبر هیچ‌گونه حاکمیتی وجود ندارد که افراد بتوانند ازطریق قرارداد اجتماعی یا از هر مسیر دیگری بر حرص و ترس خود فائق آیند. جهان امروز و آیندهٔ ما به نظام بین‌المللی جدیدی وارد شده است و آن‌گونه‌که باید و شاید از امکانات تهدیدآمیز و حتی همکاری‌جویانهٔ فضای سایبر اطلاع ندارد. فضای آنارشیک سایبرْ راه را برای خشونت و اعمال قدرت سخت باز می‌کند.

راه‌های متعددی برای اعمال این نوع از قدرت وجود دارد. درادامه سعی می‌شود به این سؤال پاسخ داده شود که آیا استراتژی بازدارندگی در فضای سایبر کارآمد است یا نه و، درصورت کارآمدی، شرایط آن چیست.

این مقاله از چند بخش تشکیل شده است؛ ابتدا مروری بر پیشینهٔ پژوهش صورت می‌گیرد و آثار مرتبط با این حوزه، که به زبان‌های فارسی و انگلیسی نگاشته شده‌اند، بررسی می‌شود. در بخش دوم، چیستی فضای سایبر موردمداقه قرار می‌گیرد و سپس در بخش سوم، مفهوم «قدرت» در فضای سایبر و تحول معنایی آن را بررسی خواهیم کرد. بعد از بحث دربارهٔ تحول معنایی این مفهوم، شناخت جنگ‌های سایبری اهمیت وافری می‌یابد؛ بخش چهارم به این موضوع اختصاص دارد. در بخش پنجم، به استراتژی بازدارندگی در فضای سایبری می‌پردازیم و آثار و پی‌آمدهای آن را بررسی می‌کنیم. در بخش نهایی نیز به نتیجه‌گیری و ارائهٔ راه‌کارها پرداخته می‌شود.

۲. پیشینهٔ پژوهش

آثار مربوط به فضای سایبر در چند سال اخیر رشدی باورنکردنی داشته است. مؤسسات و نهادهای بسیاری تأثیرات این عرصه در زندگی اجتماعی، سیاسی، و فرهنگی انسان هزارهٔ سوم را بررسی می‌کنند. به همین میزان نیز محتوا تولید شده است، به‌گونه‌ای‌که فضای سایبر برای ما دیگر فضایی گنگ و مبهم نیست. در ایران نیز برخی آثار ترجمه شده و برخی نیز به رشتهٔ تحریر درآمده است. درادامه، برخی از این کتاب‌ها و مقالات را بررسی می‌کنیم. باتوجه‌به گستردگی پژوهش‌های این حوزه، صرفاً به آن دسته از آثاری خواهیم پرداخت که به متغیر مستقل ما، یعنی «فضای سایبر»، مربوط باشد.

۱. به‌عنوان اولین نمونه می‌توان به کتاب پرفروش نای (Nye 2011) با عنوان *آیندهٔ قدرت* اشاره کرد. نای در این کتاب تاریخی تحول قدرت در زندگی سیاسی بشر را بررسی می‌کند. وی قدرت سایبر را «احراز نتایج ترجیحی ازطریق استفاده از منابع اطلاعاتی به‌هم‌پیوستهٔ الکترونیکی در حوزهٔ سایبر» تعریف می‌کند. نای در این کتاب دو بُعد از قدرت سایبری را برمی‌شمرد: وجه فیزیکی و وجه مجازی. بر همین اساس، اهداف و مرجع نهایی قدرت سایبر را نیز در دو حوزه دسته‌بندی می‌کند: دستهٔ اول در درون فضای سایبر اتفاق می‌افتد که وجه سخت و نرم دارد، مانند «حملات سایبری» که در وجه سخت جای می‌گیرد. تأثیرگذاری بر ارزش‌ها و معیارهای زندگی دیگران در وجه نرم صورت‌بندی می‌شود. اما دستهٔ دوم خارج از فضای سایبر روی می‌دهد که آن هم به وجه سخت و نرم تقسیم می‌شود. نای کنترل بر سیستم‌های تبادل اطلاعات و جریان آزاد اطلاعات را وجه سخت و استفاده از فضای سایبر برای دیپلماسی عمومی در عرصهٔ روابط خارجی و بین‌المللی کشور را وجه نرم می‌خواند.

اثر نای بی‌شک مهم‌ترین بستری است که سایر محققان و پژوهش‌گران می‌توانند از آن بهره‌برداری کنند. اما نای در بررسی رویکردهای تئوریک به فضای سایبر و این‌که جریان اصلی روابط بین‌الملل و سایر نظریه‌های اجتماعی به آن چه دیدگاهی دارند مطلب زیادی به ما نمی‌گوید. ازسوی‌دیگر، وی به تمام وجوه قدرت، به‌ویژه مقایسهٔ قدرت در فضای سایبر با آن‌چه نظریه‌های اجتماعی و پست‌مدرنْ وجه نامرئی قدرت می‌خوانند، اشاره‌ای نمی‌کند.

۲. محقق دیگری که به موضوع فضای سایبر به‌منزلهٔ متغیر تأثیرگذار در عرصهٔ سیاسی می‌پردازد کرامپتون (Crampton) است. وی در کتاب خود با عنوان *صورت‌بندی سیاسی فضای سایبر* (2004) به این سؤالات پاسخ می‌دهد: ۱. «بودن» در فضای سایبر به چه معناست؟ ۲. فضای سایبر چگونه نظم پیدا می‌کند و روابط قدرت چگونه بر تنظیم فضای سایبر اثر می‌گذارند؟ وی با استفاده از رهیافت فوکویی به این سؤالات پاسخ می‌دهد. کرامپتون با پیش‌کشیدن بحث «فناوری‌های خود» (technologies of the self) به تحلیل فضای سایبر روی می‌آورد. وی توضیح می‌دهد که چگونه هویت افراد در فضای سایبر تغییر می‌کند. کرامپتون فضای سایبر را مجموعهٔ دقیقی از روابط قلمداد می‌کند که در آن ما خود را پیدا می‌کنیم. به‌رغم‌این‌که مباحث کرامپتون در حوزهٔ اندیشه‌ای قابل‌تأمل و جالب است، به‌صورت عملیاتی چیز زیادی دربارهٔ چگونگی اثر این فضا بر قدرت به‌ویژه در عرصهٔ بین‌المللی به ما نمی‌گوید.

۳. مورد بعدی *ظهور سیاست شبکه‌ای: چگونه اینترنت سیاست و دیپلماسی بین‌المللی را تغییر می‌دهد* است که بویلر (Bollier 2003) آن را تدوین کرده است. فصل اول این کتاب به چگونگی تأثیر شبکه‌های الکترونیکی در ماهیت قدرت و فرهنگ می‌پردازد. بخش دوم بر بحث اینترنت و ظهور قدرت نرم متمرکز است و در فصل سوم به رقابت روایت‌ها در سیاست بین‌الملل در عصر سایبر اشاره می‌شود. این کتاب، به‌رغم توضیح و تبیین مفصل درخصوص نقش فضای سایبر در قدرت نرم و سخت در روابط بین‌الملل، متغیر «قدرت» را به‌صورت کامل توضیح نداده است. هم‌چنین این اثر فاقد نگاه تئوریک به موضوع است.

۴. پژوهش دیگری که بدان اشاره می‌شود مقالهٔ اریکسون و گیاکوملو (Eriksson and Giacomello 2006) با عنوان «انقلاب اطلاعاتی، امنیت، و روابط بین‌الملل» است. آنان به‌دنبال پاسخ به این سؤال هستند که تئوری‌های روابط بین‌الملل درمورد اثر فضای سایبر و انقلاب ارتباطات و اطلاعات بر روابط بین‌الملل چه می‌گویند. نویسندگان چنین نتیجه‌گیری می‌کنند که بسیاری از نظریه‌های روابط بین‌الملل درمورد این موضوع سکوت کرده‌اند؛ به‌جز نظریه‌هایی که محوریت سیاست‌گذارانه دارند و به مسائل امنیتی مرتبط با تکنولوژی اطلاعاتی پرداخته‌اند، نظریه‌های روابط بین‌الملل در این مورد حرفی برای گفتن ندارند. لذا نویسندگان، در بخش دوم مقاله، بار دیگر نظریه‌های رئالیسم، لیبرالیسم، و سازه‌انگاری را موردبازبینی قرار می‌دهند تا شاید عناصر مرتبط با امنیت (و نه قدرت) در عصر دیجیتال را در آن‌ها بیابند. در این مقاله، به‌رغم مطرح‌شدن نکات ویژه، مبحث امنیت بیش از قدرت محوریت دارد و نویسندگان اشاره‌ای به تأثیر فضای سایبر در قدرت بازیگران بین‌المللی نمی‌کنند.

۵. پژوهش دیگری که می‌توان دربارهٔ فضای سایبر به آن اشاره کرد کتاب *انقلاب اطلاعات، امنیت، و فناوری‌های جدید* اثر روزنا و دیگران (۱۳۹۰) است. این کتاب در سیزده فصل به اثر انقلاب اطلاعات بر امنیت در روابط بین‌الملل پرداخته است. چند فصل از کتاب به اثر فناوری‌های اطلاعات بر محیط پیرامونی به‌ویژه دولت، حاکمیت، و توسعهٔ انسانی تمرکز دارد. نویسندگان به این موضوع اشاره می‌کنند که بسیاری از نظریه‌های جریان اصلی روابط بین‌الملل درخصوص موضوع امنیت در فضای سایبر سکوت پیشه کرده‌اند؛ بنابراین، پیش‌نهاد می‌کنند که برای فائق‌آمدن بر این مشکل با استفاده از ره‌یافتی «عمل‌باورانه»تر به فضای سایبر و امنیت نگریسته شود. نای و کیئن، در فصل یازدهم، موضوع انقلاب اطلاعات، وابستگی متقابل، و قدرت را بررسی کرده‌اند. در این فصل، که به موضوع این نوشتار ارتباط مستقیم پیدا می‌کند، بحث قدرت قدری به محاق رفته است

و عملاً موضوع وابستگی متقابل موردتأکید قرار گرفته است که آن هم به دیدگاه نای در کتاب *فضای سایبر و قدرت* نزدیک می‌شود. نویسندگان معتقدند این پیش‌بینی عامه‌پسند که انقلاب‌های اطلاعات و ارتباطات موجب می‌شود توزیع قدرت در میان دولت‌ها به برابرشدن نزدیک‌تر گردد خطاست. درحقیقت در تناقض با فرضیهٔ مقالهٔ حاضر نیز قرار می‌گیرد.

۶. اثر دیگری که می‌توان به آن اشاره کرد نوشتهٔ آلبرتس و پاپ (۱۳۸۵) با عنوان *گزیده‌ای از عصر اطلاعات: الزامات امنیت ملی در عصر اطلاعات* است. نویسندگان در فصل اول کتاب به موضوع امنیت ملی در عصر اطلاعات می‌پردازند. فصل دوم با عنوان «بایت‌ها و دیپلماسی» موضوعاتی چون دهکدهٔ جهانی، سرچشمهٔ جدید ثروت، سلطهٔ اطلاعاتی و رهبری واقعی در عصر اطلاعات را موردبررسی قرار می‌دهد. کتاب، در فصل سوم، هفت نوع جنگ اطلاعاتی را بررسی می‌کند: جنگ فرماندهی و کنترل، جنگ اطلاعات‌محور، جنگ روانی، جنگ الکترونیکی، جنگ رخنه‌گری (هک)، جنگ اطلاعاتی، و درنهایت جنگ اینترنتی که هم به‌لحاظ ماهیت و هم ازحیث آثار توضیح داده می‌شوند. در فصل بعدی کتاب، آثار اینترنت بر امنیت ملی به‌طور مبسوط توضیح داده شده است؛ به‌ویژه به امنیت ملی آمریکا و اقداماتی که باید این کشور انجام دهد پرداخته شده است. نویسندگان توضیح می‌دهند که رشد اینترنتْ نگرانی‌هایی جدی در پی دارد؛ اما چون ایالات متحده و دنیا می‌توانند منافعی عظیم از دست‌رسی به یک شبکهٔ جهانی مقاوم در بسیاری از عرصه‌ها (تجارت، فرهنگ، آموزش و در قلمرو امنیت ملی، هدف حیاتی ترویج آزادی) به‌دست آورد، ایالات متحده باید به‌طور حتم یاد بگیرد که با خطرهای امنیت ملی کنار بیاید؛ دولت آمریکا باید بیاموزد که به‌گونه‌ای عمل کند که ارزش‌های اساسی آن (مانند آزادی بیان و حکومت آزاد)، که جامعه براساس آن‌ها شکل گرفته است، تهدید نشود.

این کتاب، گرچه ازحیث ارائهٔ اطلاعات دربارهٔ نقش فناوری‌های اطلاعات بسیار مفید است، درخصوص موضوع مقالهٔ حاضر جز ازطریق اشاره به تهدیدهای منبعث از فضای سایبر مطلبی ارائه نمی‌کند. این کتاب بیش‌تر بر موضوع نقش فناوری اطلاعات در جاسوسی و سرقت اطلاعات تمرکز دارد و اطلاعاتی دربارهٔ تأثیر فضای سایبر بر قدرت و بازدارندگی در سطح روابط بین‌المللی ارائه نمی‌کند. ازسوی‌دیگر، مباحث این کتاب بیش‌تر بر سیاست داخلی ایالات متحده متمرکز است و نگاه کلان به موضوع کم‌تر دیده می‌شود.

۷. آخرین پژوهشی که به آن اشاره می‌کنیم کتاب کاستلز (۱۳۸۰) است با عنوان *عصر اطلاعات: اقتصاد، جامعه، و فرهنگ*. این اثر یکی از منابع ارزش‌مندی است که دربارهٔ جامعهٔ اطلاعاتی و تبعات اقتصادی و فرهنگی و اجتماعی آن نوشته شده است. هدف کاستلز آن بوده است که با بررسی تحلیلی مهم‌ترین رویدادها و پدیدارهایی که در زمانهٔ حاضر درحال شکل‌دادن به جوامع بشری و رقم‌زدن سرنوشت آدمی برروی کرهٔ خاکی هستند، امکان فهم عقلانی تحولات حیرت‌انگیزی را فراهم آورد که اثر آن بر همهٔ ابعاد حیات انسان‌ها مشهود است. کاستلز کتاب پرحجم خود را به بحث دربارهٔ جامعهٔ شبکه‌ای، که آن را یکی از ویژگی‌های سرمایه‌داری متکی به اطلاعات به‌شمار می‌آورد، اختصاص داده است. این کتاب، باوجود مباحث بسیاری که مطرح می‌کند، درخصوص قدرت در روابط بین‌الملل به‌صورت خاص هیچ بحثی را ارائه نکرده است؛ چراکه بیش از آن‌که کتابی در حوزهٔ روابط بین‌الملل باشد، کتابی است که در حوزهٔ علوم اجتماعی و اقتصاد نوشته شده است.

این مقاله در نظر دارد با نگاهی جامع به مقولهٔ «فضای سایبر» اثر آن را بر قدرت بازدارندگی دولت‌ها بررسی و مؤلفه‌های اساسی آن را برآورد کند، کاری که تاکنون در آثار و منابع در دست‌رس برای نگارندگان صورت نپذیرفته است.

۳. چیستی فضای سایبر

«فضای سایبر» جدیدترین و درعین‌حال پیچیده‌ترین حوزه‌ای است که زندگی بشر در قرن ۲۱ را به خود مشغول کرده است. زمانی‌که کامپیوترهای اولیه در ایالات متحده اختراع شد، کم‌تر کسی تصور می‌کرد انقلاب اطلاعاتی و داده‌ای ناشی از این امکان جدید می‌تواند تبعات پیچیده‌ای برای بشر داشته باشد. رایانه‌ها، قبل از ورود به حوزهٔ شبکه، دستگاه‌های پردازش‌گری بودند که دورنمای سرعت و دقت را برای شرکت‌ها و نهادهای دولتی و غیردولتی فراهم کرده بودند. اما زمانی‌که این پردازش‌گرها برای اولین‌بار به‌صورت شبکه‌ای در یکی از اتاق‌های وزارت دفاع آمریکا درآمدند، اولین نطفه‌های فضای سایبر را نیز بنا نهادند.

برای اولین بار مفهوم فضای سایبر را گیبسون (Gibson 1984) نویسندهٔ داستان‌های علمی ـ تخیلی در سال ۱۹۸۴ ارائه کرد. کرامپتون آن را حوزه‌ای از جغرافیای دانش می‌داند که میان جامعه و تکنولوژی قرار گرفته است (Crampton 2004: 6).

بندیکت این فضا را چنین تعریف می‌کند:

> یک جهان جدید و موازی با دنیای روزمرهٔ بشر، که با کامپیوتر و خطوط ارتباطی جهانی ایجاد شده است؛ جهانی با ویژگی‌هایی نظیر عبورومرور فراگیر دانش، اسرار، سنجش‌ها، شاخص‌ها و سرگرمی‌ها که ازطریق کارگزاری انسان به صداها، جلوه‌ها و حضوری جهانی که تا پیش از این وجود نداشته شکل می‌دهد (Benedikt 1992: 1-3).

وی تعریف دیگری نیز از این فضا ارائه می‌کند:

> دست‌رسی ازطریق هر کامپیوتری که به سیستم ارتباط جهانی متصل است، مکانی بدون محدودیت که هم‌زمان افرادی از زیرزمین خود در ونکوور 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 هنگ‌کنگ، از یک کافه در کیوتو، از یک ورزشگاه در کینشازا، و از یک لابراتوار در ایستگاه فضایی بین‌المللی در آن حضور دارند (Benedikt 1992: 3).

«عدم محدودیت» در فضای اینترنت آثار و پی‌آمدهای ویژه‌ای دارد. آن‌چه به‌مثابهٔ انقلاب اطلاعاتی، که نقش دولت‌ها را بسیار کاهش داده، مطرح است ازطریق این ویژگی فضای سایبر متمایز می‌شود. این فضا، برخلاف محیط روزمرهٔ زندگی انسان که سرشار از واقعیت‌هاست، به‌صورت مجازی تبادل را امکان‌پذیر می‌سازد. درحقیقت، «هرجا» (everywhere) بودن و «هیچ‌جا» (nowhere) بودن با فضای مجازی تحقق پیدا می‌کند (.ibid).

محدودیت‌های فضای فیزیکی در فضای جدید وجود ندارد. ارتباطات در فضای فیزیکی ازطریق نامه‌ها، کتاب‌ها، و مانند این‌ها صورت می‌گرفت. اشیای فیزیکی فقط در فضای فیزیکی وجود داشت؛ اما این اشیا به‌صورت سایبری در فضای سایبر 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 مرحلهٔ اول، در کجا بودن را به ذهن متبادر می‌سازد. این‌که منبع انتشار و کنش سایبری کجاست و آدرس و مقصد این کنش کجا را نشانه گرفته است همه ازطریق سؤال دربارهٔ مکان پاسخ داده می‌شود. ارسال ایمیل یا پیام یا هرگونه کنش سایبری‌ای در فضای مورداشاره، چه ازطریق ارسال‌کنندهٔ پیام چه درمورد گیرندهٔ پیام، باز، «مکان» را به‌منزلهٔ عنصری حیاتی مطرح می‌کند. فاصله نشان می‌دهد که به چه‌تعداد کامپیوتر مختلف برای رساندن اطلاعات به مقصد موردنظر نیاز هست. اندازه بر مقدار اطلاعاتی که با بسیاری از لینک‌ها و پیوندها و وب‌سایت‌ها ردوبدل

می‌شود دلالت می‌کند. و، درنهایت، ریشه به منبع ارسال و دریافت خبر اشاره دارد (Bryant 2001: 140). اگر ازمنظر کلان به فضای سایبر بنگریم، ارسال و دریافت خبر ازطریق شبکهٔ جهانی وب صورت می‌گیرد، اما خود این مسئله یکی از وجوه مشکل برای زندگی روزمرهٔ ما در فضای سایبر است.

ازسوی‌دیگر، فضای سایبر پی‌آمدهایی را نیز برای زندگی روزمرهٔ ما داشته است، به‌گونه‌ای‌که بسیاری از کارشناسان از وضعیت خطرناک آینده سخن می‌گویند. دیوید تاون، استاد دانشگاه هاروارد، فضای سایبر را با وضع طبیعی که توماس هابز ترسیم کرده است مقایسه می‌کند. او معتقد است عبارات جنایت سایبر، تروریسم سایبر، و جنگ‌افزارهای سایبر نشان‌دهندهٔ وضعیتی وحشت‌ناک، طغیان‌گر، و لجام‌گسیخته است (Daniel 2009: 17).

باوجود این اوصاف، به این نتیجه می‌رسیم که فضای سایبر ترکیب جدیدی از الگوی زندگی در یک فضای ناشناخته را به بشر ارائه می‌دهد. این فضا برای تمام بشر امکان بازیگری را فراهم می‌کند، از کودکان خردسال گرفته تا سازمان‌ها و شرکت‌های چندملیتی و نیز دولت‌های قدرت‌مند. فضای سایبر امکانات جدیدی در اختیار بشر قرار می‌دهد: جغرافیا را از بین می‌برد، انسان را از فاعل‌بودن در محیط اجتماعی به سوژگی در محیط مجازی سوق می‌دهد، ایده‌ها را گسترش می‌دهد، کنترل‌پذیری را بی‌معنا می‌سازد و دولت را به‌عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی، و غیره خلع سلاح می‌کند.

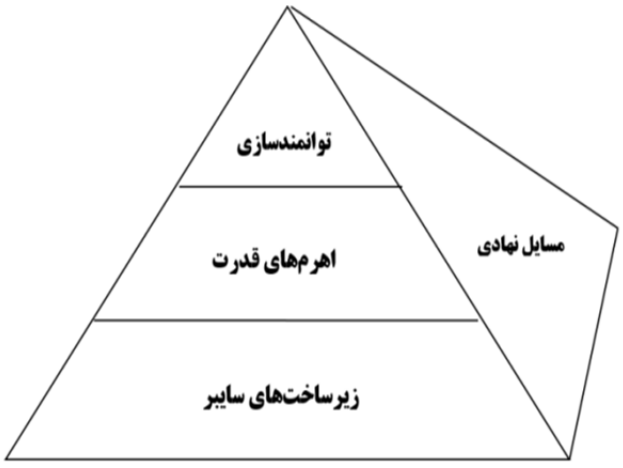
وجود پیوند میان فضای سایبر و قدرت در روابط بین‌الملل، درحال‌حاضر، امری بدیهی محسوب می‌شود. وجوه قدرت در فضای فیزیکی متنوع است. این تعدد وجهٔ خود را در فضای سایبر نیز نشان می‌دهد. می‌توان از چند وجه قدرت در روابط بین‌الملل و جهان سیاست صحبت کرد: وجه سخت‌افزاری و وجه‌نرم‌افزاری، و غیره. در فضای سایبر نیز می‌توان نشانه‌های چنین وجوهی را جست‌وجو کرد.

۴. «قدرت» و تحول معنایی آن در فضای سایبر

مفهوم «قدرت سایبر» را می‌توان دربرابر مفاهیمی چون «قدرت دریایی» (sea power)، «قدرت هوایی» (air power)، «قدرت زمینی» (land power)، و حتی «قدرت فضایی» (outer space power) بررسی کرد (Kramer 2009: 4-5). تعاریف از قدرت دریایی و زمینی

و غیره، هرچند بسیار مبهم است، به‌نوعی به ظرفیت‌های بالای دولت در استفاده از آن به‌عنوان مزیتی نسبی اشاره دارد. درحقیقت، هرقدر دولتی بتواند با استفاده از این ظرفیت‌ها به اهداف خود در سریع‌ترین و کم‌هزینه‌ترین راه دست پیدا کند آن را می‌توان قدرتی هوایی یا دریایی در نظر گرفت.

استار (Starr)، با ارائهٔ چهارچوبی نظری، قدرت سایبر را در حوزه‌های متعددی بررسی می‌کند. وی، با ترسیم نموداری، قدرت‌گیری بازیگران بین‌المللی را در عرصهٔ سایبر مبتنی بر اهرم‌های قدرتی می‌داند که این عرصه ارائه می‌کند. ازنظر او، اهرم‌های قدرت در قالب سیاسی، اقتصادی، نظامی، و اطلاعاتی تعریف می‌شوند. سطح زیرین هرم شامل زیرساخت‌هایی است که به فضای سایبر شکل می‌دهد. خروجی این زیرساخت‌ها سطوح سنتی قدرت (سیاسی، اطلاعاتی، نظامی، و اقتصادی) را تقویت می‌کند. این سطوح قدرتْ خود پایه‌هایی را برای توان‌مندسازی بازیگران در رأس هرم فراهم می‌کند. این بازیگران عبارت‌اند از افراد، تروریست‌ها، جنایت‌کاران فراملی، شرکت‌ها، دولت ـ ملت‌ها و سازمان‌های بین‌المللی. ذکر این نکته لازم است که، برخلاف دولت‌ها، احتمال دارد سایر بازیگران به همهٔ وجوه و زیرساخت‌های فضای سایبر دست‌رسی نداشته باشند. اما بازیگران غیردولتی با محدودیت‌های ساختاری‌ای چون موافقت‌نامه‌های بین‌المللی که امکان توان‌مندسازی را محدود می‌کند مواجه نیستند.



شکل ۱. چهارچوب مفهومی قدرت سایبر (Starr 2008: 47)

این هرم و چهارچوب مفهومی سویهٔ دیگری نیـز دارد و آن «مسـائل نهـادی» اسـت. ایـن مسـائل شـامل عـواملی چـون حکومـت، ملاحظـات حقـوقی و قـانونی، نظـم‌دهـی، به‌اشتراک‌گذاری اطلاعات، و ملاحظاتی درخصوص آزادی‌های مدنی است.

۱.۴ قدرت اطلاعات

عنصر اساسی‌ای که به قدرت سایبر ارتباط بسیار نزدیکـی دارد «اطلاعـات» (information) اسـت. فضـای سـایبر و قـدرت سـایبر بـه‌وضـوح ابعـادی از «ابـزار اطلاعـاتی قـدرت» (informational instrument of power) هستند که در قالب مدل سیاسی، اطلاعاتی، نظامی، و اقتصادی قرار می‌گیرند.[۱] بر این اساس، مجموعه‌ای از اطلاعات که در فضای سایبر تولیـد، منتشر، و ذخیره‌سازی می‌شود برای همهٔ بازیگران اجتماعی و نیز بازیگران دولتـی بـه‌منزلـهٔ عنصر اساسی قدرت محسوب می‌شود و این اطلاعات ایجاد می‌شود و استفاده از ابزارهای دیگر را ممکن می‌سازد.

۲.۴ قدرت اقتصادی

قدرت سایبر به‌طور روزافزونی در توانایی اقتصادی نقش حیاتی ایفا می‌کنـد. حتـی دولـت ریگان (Unite States and Ronald Reagan 1988: 34) در دهـهٔ ۱۹۸۰ مـیلادی در *اسـتراتژی امنیت ملی* با اشاره به نقش اطلاعات و تکنولوژی‌های جدید اطلاعاتی در قدرت اقتصادی آمریکا به این موضوع پرداخت. در اقتصاد جهانی قـرن ۲۱، کـه اقتصـادی جهـان‌شـمول و به‌هم‌پیوسته شده است، فضای سایبر را می‌توان تنها عامل مهم به‌هم‌پیوسـتگی بـازیگران بـا یک‌دیگر دانست که تولید را تقویت مـی‌کنـد، بازارهـای جدیـدی مـی‌گشـاید و مـدیریت ساختارهایی را که ثروت‌های کلانی ایجاد می‌کند ممکن می‌سازد.

۳.۴ قدرت سیاسی و دیپلماتیک

تأثیر قدرت سایبر در امور سیاسی و دیپلماتیک کم‌تر تبیین شده اسـت. قـدرت‌منـدترین و بانفوذترین رسانه‌هایی که ازطریق تلویزیون ماهواره‌ای به اشاعهٔ دیدگاه‌ها و نظرهای سیاسی خود می‌پردازند با سیستم‌ها و شبکه‌های فضای سایبر به یک‌دیگر متصل هستند. هم دولت آمریکا و هم ترویست‌های القاعده هردو از امکانات فضای سـایبر بـرای اشـاعهٔ پیـام‌هـا و ایده‌های خود استفاده می‌کنند.

۴.۴ قدرت نظامی

به‌لحاظ نظامی، قدرت سایبر شاید مهم‌ترین ابزار نوظهور چند دههٔ گذشته باشد. درحال‌حاضر اغلب کشورها برای ایمن‌سازی مرزهای سایبر و فراسایبری خود دربرابر چنین تحول جدیدی آماده می‌شوند. دکترین‌های جدید نظامی براساس فضای سایبر تدوین می‌شود. در تمام سطوح منازعه، از شورش‌های داخلی گرفته تا جنگ‌های متعارف، قدرت سایبرْ عامل حتمی و گریزناپذیر توان‌مندی‌های نظامی است و این توان‌مندی برپایهٔ تکنولوژی‌های مدرن شکل گرفته است. قدرت سایبر روزبه‌روز خود را به‌عنوان عاملی اثرگذار بر سیاست‌گذاری‌های ملی در تمام حوزه‌های اشاره‌شده توسعه می‌دهد. در زمینه‌های متعددی، از اقدامات ضدتروریستی گرفته تا سامان‌دادن سیاست، اقتصاد، و حتی روابط با سایر کشورها، ردپای 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 می‌کنند که حتی تا یک دهه پیش وجود نداشت موضوعیت پیدا می‌کند. میزان تسهیل در دست‌رسی به این فضای تکنولوژیکْ میزان موفقیت شهروندان و به‌تبع آن دولت را رقم می‌زند. قدرت سایبر میان سایر عناصر و ابزارهای قدرت پیوند برقرار می‌سازد و آن‌ها را برای تغییر وضعیت به بهترین وضعیت یاری می‌رساند؛ به‌عبارت‌دیگر، فضای سایبر همانند مادهٔ خامی است که سوخت اقتصاد و جامعه را فراهم می‌کند.

باتوجه‌به توضیحاتی که داده شد، می‌توان قدرت سایبر را چنین تعریف کرد: «توانایی استفاده از فضای سایبر برای ایجاد مزیت‌ها و اثرگذاری بر رویدادها در تمام محیط‌های عملیاتی و ازطریق ابزارهای قدرت» (Betz and Stevens 2011: 34). در این تعریف، چنان‌که مشاهده می‌شود، فضای سایبر از ویژگی گستردگی برخوردار است، چراکه فضای سایبر برخلاف سایر حوزه‌های فیزیکی محدود نیست. ابزارهای قدرت در این فضا با عوامل متعددی شکل گرفته است. تازمانی‌که فضای سایبر به‌عنوان یک محیط زیست مطرح است، قدرت سایبر نیز سنجه‌ای برای توانایی استفاده از آن محیط قلمداد می‌شود. تکنولوژیْ عامل اصلی محسوب می‌شود و امکان بهره‌برداری از این فضای جدید بدون استفاده از آن عامل وجود ندارد. اما نکتهٔ اساسی در این است که، برخلاف سایر حوزه‌های قدرت که صرفاً در انحصار بازیگران دولتی قرار داشت، فضای سایبر محدود به بازیگران دولتی نیست. این تکنولوژی اساساً امکان بهره‌گیری را برای افراد، سازمان‌ها

(غیردولتی)، جوامع، دانشگاه‌ها، و غیره فراهم آورده است تا از مزیت‌های بسیار منحصربه‌فردی برخوردار شوند. ازاین‌رو، بررسی تبعات ظهور چنین فضایی برای امنیت ملی کشورها حائز اهمیت می‌نماید. جنگ سایبری یکی از مؤلفه‌هایی است که امنیت ملی کشورها را به‌شدت متأثر از خود می‌سازد.

۵. جنگ سایبری

همانند عرصه‌های هوایی، زمینی، دریایی، و حتی فضایی، عرصهٔ سایبر نیز ابزارهای جنگی دارد. حملات سایبر امروزه امری واقعی و تعین‌یافته است که در حیات بشری دیده می‌شود. حملات سایبری قدرت نسبی دولت‌ها را و، به‌تبع آن، بقای آنان را در نظام بین‌الملل متأثر می‌سازد. «جنگ سایبری» (cyberwarfare) محدوده‌ای جدید از نزاع، قدرت، و امنیت است که پیش از این برخلاف نظر واقع‌گرایان به‌هیچ‌وجه در دایرهٔ عناصر قدرت تعریف نمی‌شد. اما شاید بتوان تعریف مورگنتا از قدرت را در این خصوص مستثنی کرد؛ ازنظر مورگنتا قدرت «ممکن است شامل هر چیزی که کنترل بر انسان را ایجاد و حفظ کند» بشود. «قدرتْ همهٔ روابط اجتماعی‌ای را که در اختیار این هدف باشد، از خشونت فیزیکی گرفته تا پیوندهای لطیف روان‌شناختی که ذهن فرد را کنترل می‌کند، شامل می‌شود» (مورگنتا ۱۳۸۹: ۴۰-۵۴). تکنیک‌های جنگ در فضای سایبر به محدودسازی خودمختاری و کنترل دولت‌ها تمایل دارد. برای دست‌یابی به این هدف در جنگ سایبر ابزارهای متعددی مورداستفاده قرار می‌گیرد.

براساس تعریف، «حملات سایبریْ کنش‌های تعمدی برای جای‌گزینی، درهم‌گسیختن، فریفتن، منحط‌کردن یا تخریب سیستم‌ها یا شبکه‌های کامپیوتری و یا اطلاعات و برنامه‌های این سیستم‌ها هستند» (Lin 2011: 63).

دولت‌ها نیازمند نگه‌داری و محافظت از انسجام شبکه‌ها و سیستم‌های کامپیوتری خود هستند. این محافظت نه با دفاع فیزیکی (در شکل سنتی)، بلکه با کاهش آسیب‌پذیری سیستم‌ها دربرابر جنگ‌افزارهای جدید سایبری‌ای است که اطلاعات را هدف قرار می‌دهند. برخی از نویسندگانْ جاسوسی سایبری را از حملات سایبری تفکیک کرده‌اند (Bajaj 2010: 2)، چراکه آسیب‌های جاسوسی سایبری مستقیماً متوجه زیرساخت‌های آنان نمی‌شود. اما، نمی‌توان چنین تفکیکی را قائل شد، چون آسیب در فضای سایبر صرفاً به‌معنی تخریب زیرساخت‌ها نیست، بلکه هرگونه اطلاعاتی که به

سرقت برود ممکن است نتایج فاجعه‌باری داشته باشد. در این مورد می‌توان به اطلاعاتی که از شرکت Sony Pictures در اواخر سال ۲۰۱۴ در آستانهٔ اکران فیلمی ضد هیئت حاکمهٔ کرهٔ شمالی به سرقت رفت اشاره کرد که دو کشور آمریکا و کرهٔ شمالی را به‌شدت دربرابر هم قرار داد و رئیس‌جمهور 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 شده‌اند، این امکان را به بازیگران دولتی و غیردولتی می‌دهد که میلیون‌ها یا شاید ده‌ها میلیون ماشین دیجیتال را تسخیر و کنترل کنند (Libicki 2009: 4).

اما در جهان دیجیتال، به‌سبب ارزانی و دسترسی گسترده به فناوری اطلاعاتی، توان‌مندی قابل‌ملاحظه‌ای حتی برای فقیرترین دولت‌ها و کنش‌گران منطقه‌ای و جهانی فراهم می‌شود که ممکن است برای به‌چالش‌کشیدن و تهدید دیگران استفاده شود. این مسئله برخلاف فناوری‌های نظامی مهم عصر صنعتی است. در عصر اطلاعات، سخت‌افزارها و نرم‌افزارها به‌صورت گسترده در دست‌رس و به‌سادگی قابل‌استفاده است، درحالی‌که در سلاح‌های عصر صنعتی، مانند سلاح‌های هسته‌ای، موشک‌های قاره‌پیما، ناوهای جنگی هواپیمابر و تانک‌ها، این‌گونه نیست. بنابراین، در عصر اطلاعات، دولت‌ها تنها کنش‌گران بین‌المللی‌ای 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: ۴۵). به همین سبب، سطوح و انواع حملات سایبری روزبه‌روز درحال گسترش است. این حملات ممکن است از به‌سرقت‌رفتن رمز عبور حساب بانکی یک فرد تا حملات ویران‌گری چون استاکس نت به تأسیسات غنی‌سازی هسته‌ای ایران متفاوت باشد.

این سنخ از حملات هم تهدید و هم فرصت تلقی می‌شود. تهدید برای کشورها و بازیگرانی که روزبه‌روز زندگی خود را بیش‌تروبیش‌تر با فضای جدید پیوند می‌زنند و فرصت برای بازیگرانی که از امکان ضربه‌زدن یا برآورده‌سازی خواست‌ها و منافع خود در شکل سنتی عاجز هستند یا تمایل ندارند هزینه‌های تهدید سنتی یک بازیگر دیگر را به جان بخرند. باراک اوباما، رئیس‌جمهور آمریکا، در سال ۲۰۱۳ درخصوص ویژگی منحصربه‌فرد

خطرهایی که حملات سایبری به زندگی بشر تحمیل می‌کند هشدار داد (Obama 2013). وی با اشاره به خطرهایی که این فضا در اختیار مهاجمان قرار می‌دهد نوشت:

> در منازعهٔ آینده، دشمن قادر به چالش‌کشیدن برتری نظامی ما نخواهد بود، بلکه به‌دنبال بهره‌برداری از آسیب‌پذیری‌های سیستم‌های کامپیوتری ما در سرزمینمان خواهد بود. ازکارانداختن سیستم‌های بانک‌داری حیاتی می‌تواند به یک بحران مالی وحشتناک منجر شود. فقدان آب تمیز و گوارا و یا ازکارانداختن کارکرد بیمارستان‌ها می‌تواند سلامت عمومی ما را به خطر اندازد. و هم‌چنان‌که در گذشته شاهد بوده‌ایم، فقدان برق می‌تواند تجارت، شهرها، و مناطق منحصربه‌فرد ما را دچار وقفه کند (ibid.).

۱.۵ جنگ سایبری

جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به‌مفهوم استفادهٔ دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی با هدف به‌مخاطره‌انداختن عناصر اطلاعاتی دشمن (اطلاعات، پروسه‌های مبتنی بر اطلاعات، سیستم‌های اطلاعاتی، و شبکه‌های رایانه‌ای) در فضای سایبری است. چنین عملیاتی به‌طور مشخص با اهداف نظامی، تجاری، سیاسی، فرهنگی، و غیره انجام می‌پذیرد؛ بنابراین، باید ارزش افزوده و به‌اصطلاح بهره‌برداری از عناصر دشمن داشته باشد، همان‌طوری‌که هرنوع جنگ دیگر نیز درنهایت به سوءاستفاده از منابع دشمن ختم خواهد شد. جنگ سایبری برای مراکز نظامی، سرویس‌های جاسوسی و اطلاعاتی، و دنیای تجارت اهمیت روزافزون دارد. ولی درمجموع هر دو دیدگاه نظامی و غیرنظامی را باید در نظر داشت (غروی و محمدی ۱۳۹۰: ۷۷).

جنگ در فضای سایبر درحال تبدیل‌شدن به یک مفهوم اساسی است. برای این جنگْ سلاح‌هایی نیز اختراع شده است. این سلاح‌ها ممکن است قدرت دولت را کاهش دهد و کنترل آن‌ها در اختیار بازیگر دیگری قرار گیرد. مشکل اساسی این است که آغاز و پایان کنترل هیچ‌گاه مشخص نمی‌شود. در این عرصه، قدرتْ دولت‌محور و حتی واقعیت‌محور نیست، بلکه ممکن است خود را در تکنولوژی نمایان سازد که بر پایهٔ کدهای «دودویی» (binary code) بنا شده است. قدرت، به‌ویژه باتوجه‌به جنگ سایبری، همیشه باید، به‌طورکلی، به‌عنوان بخش جدایی‌ناپذیر امنیت ملی و انسانی مفهوم‌سازی شود. وزارت

دفاع ایالات متحده این عرصهٔ جدید را بخش جدایی‌ناپذیر امنیت ملی خود قلمداد می‌کند. این وزارت‌خانه بخش فرماندهی سایبر را با نام «فرماندهی سایبری ارتش آمریکا» (US Army Cyber Command/ USCYBERCOM) ایجاد کرده است که وظایفی چون «برنامه‌ریزی، هماهنگی، انسجام، زمان‌بندی و هدایت فعالیت‌ها برای رهبری عملیات و دفاع از شبکه‌های اطلاعاتی خاص وزارت دفاع و آمادگی برای ادارهٔ طیف کاملی از عملیات نظامی فضای سایبر به‌منظور بالفعل‌سازی اقدامات در تمام حوزه‌ها، تضمین آزادی عمل متحدان ایالات متحده در فضای سایبر و گرفتن این آزادی عمل از دشمنان را برعهده دارد» (Clarke and Knake 2012: 20-44).

۲.۵ محدودهٔ عملیاتی

برای فضای سایبر نمی‌توان محدودهٔ جغرافیایی تصور کرد؛ بنابراین، جنگ سایبر نیز مرز ندارد. محدودهٔ عملیات سایبر بسیار گسترده است، از تولید پارازیت مخابراتی گرفته تا عملیات روانی، از تغییر صفحات یک وب‌سایت گرفته تا بمباران ایمیلی. ولی، نهایتاً هدف اصلی تهدیداتْ منابع اطلاعاتی هستند، به‌نحوی‌که امنیت ملی دشمنْ موردمخاطره قرار گیرد. بدین ترتیب، بستر عملیات سایبری همانا زیرساخت‌های اطلاعاتی است. محدودهٔ عملیات سایبری به‌طور مشخص در حدود منابع دشمن است، ولی ممکن است دربرگیرندهٔ اشیای خود حمله‌کننده نیز باشد یا در محدودهٔ سایبری دیگر عوامل وابسته یا غیروابسته باشد. برای تفهیم بهتر به این سناریو دقت کنید: حمله‌کننده‌ای قصد دارد اقدام به دزدیدن اطلاعات دشمن و فروش آن‌ها به شخص ثالث کند. وی ازطریق یک کانال واسطه به دشمن نفوذ می‌کند و نهایتاً اطلاعات نیز از همان کانال منتقل می‌شود. این سناریو دقیقاً نظیر نمونه‌ای واقعی است که برای منابع اطلاعات ایالات متحدهٔ آمریکا محقق گردید و، در آن، حمله‌کنندهٔ برزیلیْ اطلاعات را، به‌طور غیرمستقیم، با واسطه به جمهوری شوروی سابق فروخت.

درمورد محدودهٔ عملیاتی باید این نکته را مدنظر داشته باشیم که، با انتخاب نادرست محدودهٔ عملیات، بروز مشکل در محدودهٔ سایبری خود حمله‌کننده نیز محتمل است. این مسئله به‌علت نزدیکی و تداخل مرزهای سایبری است. تصور کنید که حمله‌کنندهٔ سایبری مبادرت به تهاجم به یک سایت اینترنتی می‌کند و نهایتاً موجب پایین‌آمدن کارآیی آن سایت می‌گردد، ولی هدف از پایین‌آمدن کارآیی سایت انهدام سرور اصلی بوده است و یکی از

سرورهای محدودهٔ جغرافیایی حمله‌کننده به‌طور ناخواسته در محدودهٔ عملیاتی بوده است. این مشکل به‌ویژه با انتشار و نامتمرکز بودن خدمات ثبت دامنه، میزبانی فضای وب، ثبت آدرس اینترنتی، و ارائهٔ پهنای باند بسیار محتمل و رایج است.

به‌عنوان نمونه‌هایی از محدوده‌های عملیات سایبری می‌توان از موارد ذیل نام برد:

- اشیای بسترساز شبکه (روترها، سوئیچ‌ها، و ماهواره‌ها)؛
- عناصر وب (سایت‌های وب، پایگاه اطلاعاتی مبتنی بر وب)؛
- ایمیل به‌عنوان رایج‌ترین عنصر گذشته و حال در فضای سایبر.

ازسوی‌دیگر، برای جنگ و عملیات تخریبی در فضای سایبر نمی‌توان محدودیتی تصور کرد. درحقیقت، جنگ سایبری مرز ندارد. ولی باید در نظر داشت که تجسم جنگ به‌سبب مقایسهٔ مستقیم فضای سایبر با دنیای حقیقی و براساس دانسته‌ها و قراردادهای فیزیکی است. درعمل فضای سایبری نیز مرز دارد. مرزها درعین هم‌بستگی کاملاً گسیخته هستند و این تصور نیز به‌سبب تجسم فیزیکی حاصل می‌گردد.

۳.۵ گونه‌شناسی ابزارهای جنگی در فضای سایبر

ابزارها و جنگ‌افزارهای سایبر برای خشونت سایبری بسیار متفاوت است. موارد فراوانی را که ممکن است زیرساخت‌های زندگی را تهدید کنند می‌توان برای آن در نظر گرفت. روزبه‌روز نیز این ابزارها رو به تزاید می‌گذارد. قبل از پرداختن به ابزارهای مورداستفاده در جنگ سایبر لازم است الگوی کلی جنگ سایبری را تشریح کنیم. این کار برای توضیح و تبیین چگونگی کاربرد ابزارها در حوزه‌های متعدد ضروری است.

در چهارچوب مدل واقع‌گرایانه، باتوجه‌به محدودهٔ عملیات، جنگ سایبری از سه بخش عمدهٔ جنگ شبکه‌ای، جنگ رایانه‌ای، و جنگ فرماندهی و کنترل تشکیل شده است. حوزه‌های اصلی جنگ شبکه‌ای عبارت‌اند از «جنگ‌های چندرسانه‌ای، فرهنگی، دیپلماتیک، اقتصادی، روانی، و ...» (غروی و محمدی ۱۳۹۰: ۷۵). جنگ رایانه‌ای معمولاً در محیط اطلاعاتی محلی یا جهانی رخ می‌دهد و هدف آن تسلط (آگاهی یا تخریب) بر اطلاعات است. در این مدل، مهم‌ترین بخشْ جنگ فرماندهی و کنترل است که جنگ الکترونیک یا جنگ‌های فیزیکی مرسوم فقط زیربخش‌هایی از آن محسوب می‌شوند. اجزای این بخش بدین قرار است: جنگ الکترونیک، فریب نظامی، عملیات روانی، امنیت اطلاعات، تخریب فیزیکی، تخریب، و غیرفیزیکی.

در این مدل نحوهٔ عملکردْ همان حمله و دفاع رایج است و مؤلفه‌های زیر را دارد:

ـ انگیزه: بدون شک، حمله‌کننده باید انگیزهٔ مشخص مستقیم یا غیرمستقیم داشته باشد. درغیراین‌صورت، مراحل بعدی بستر و پایهٔ منطقی نخواهد داشت.

ـ هدف: باتوجه‌به انگیزه، محدودهٔ عملیات مشخص می‌گردد. این همان چیزی است که آن را هدف می‌نامیم. هدف ممکن است به‌بزرگی و گسترهٔ شبکهٔ توزیع نیرو در یک کشور یا به‌کوچکی سیستمی در شبکه‌ای محلی باشد. در این‌جا، بزرگی و کوچکی هدف مهم نیست، بلکه ارزش هدف تعیین‌کننده است. در عملیات سایبری، یک هدف خاص که در شکل فیزیکی بسیار کوچک است ممکن است ارزشی بزرگ‌تر و بیش‌تر از کیلومترها خاک داشته باشد.

ـ جمع‌آوری اطلاعات: هر عملیاتی، چه فیزیکی و چه سایبری، باید با آگاهی صورت پذیرد. بدون اطلاعات فقط نیرو و منابع از دست می‌رود، ضمن آن‌که احتمال ردیابی و شناسایی برای دشمن افزایش می‌یابد. کسب اطلاعات از عناصر سایبری دشمنْ مهم‌ترین بخش از عملیات سایبری محسوب می‌شود. ازدید کارشناسان، جمع‌آوری اطلاعات از اهداف سایبری به‌مفهوم انجام پنجاه درصد از کل عملیات است. در این‌جا، اطلاعات به‌مفهوم هر جنبه از هدف است که به‌نحوی با ایمنی سایبری آن در ارتباط باشد: بلوک‌ها و آدرس‌های اینترنتی/ اینترانتی، اسامی دامنه‌های عمومی و خصوصی، سرویس‌های مبتنی‌بر پروتکل اینترنت (TCP/ IP)، معماری سیستم‌ها و شبکه‌ها، مکانیسم‌های تصدیق، و ... مصداق جمع‌آوری اطلاعات می‌شوند. جمع‌آوری اطلاعات سه مرحله دارد که شامل شناسایی، وارسی، و کنکاش می‌شود.

ـ نقاط ضعف: وقتی اطلاعات حمله‌کننده دربارهٔ ماهیت سایبری هدف کامل شد، این مرحله آغاز می‌شود. این بخشْ ساده‌ترین قسمت عملیات است. با دانستن مشخصات هدف، تعیین عیوب سخت‌افزاری و نرم‌افزاری چندان دشوار نیست و فقط زمان لازم است. اگر دشمن به چنین مرحله‌ای برسد، انجام حمله قطعی است.

ـ نفوذ: پس از تعیین نقاط ضعف یا درنظرگرفتن اطلاعات به‌دست‌آمده و با آگاهی از مکانیسم‌های ردیابی، عملیات سایبری درجهت نفوذ به هدف آغاز می‌شود. این مرحله، اگرچه بخش پایانی عملیات است، زمان بیش‌تری را به خود اختصاص می‌دهد، زیرا قسمت‌های متعددی دارد. در جدول ۱، این ابزارهای نفوذ دسته‌بندی شده است:

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

نوع ابزار سایبر	مصداق
سرقت (theft)	دست‌یافتن به رمزهای عبور و اطلاعات حساس ازطریق تخمین و حدس، سرقت یا به‌خطرافتادن سیستم‌های کامپیوتری
باگ‌ها[۲]/ بک‌دورها[۳]	کدگذاری غلط، سختی در یافتن نتایج یک برنامه در سیستم قربانی
شکست احراز هویت (authentication failure)	شکست در ورود به سایت به‌سبب مداخله‌گری یا به‌خطرافتادن سرور
شکست پروتکل (protocol failures)	رد دست‌رسی به نرم‌افزارها با پروتکل معیوب
درزکردن اطلاعات (information leakage)	جاسوسی از کامپیوتر
حملات نمایان (exponential attacks)	استفاده از ویروس‌ها و کرم‌هایی که به‌سرعت گسترش می‌یابند و به خسارت به سیستم‌های کامپیوتری منجر می‌شوند
حملات ویران‌گر خدمات (denial of service attacks)	استفادهٔ بیش از حد از یک درگاه اینترنتی و ایجاد ترافیک مصنوعی و فشار بر سخت‌افزارها برای تعطیلی یا کاهش خدمات
بات‌نت‌ها[۴]	جاسوسی، اسب‌های تروا و کرم‌ها
حملات فعال	مزاحمی که اطلاعات را حذف می‌کند، تغییر می‌دهد، و به‌جای آن اطلاعات خود را ارسال می‌کند

۶. بازدارندگی در عرصهٔ سایبر

درهم‌تنیدگی دنیای کنونی در عصر ارتباطات و فناوری اطلاعات، درکنار فرصت‌های بی‌نظیری که به‌وجود آورده، نگرانی‌هایی را نیز در پی داشته است. یکی از این نگرانی‌های مهمْ مسائل مربوط به امنیت ملی است که فعالیت‌های سایبری‌ای نظیر حملات سایبری یا جاسوسیْ آن را به‌شدت موردتهدید قرار می‌دهند. روزانه هزاران حملهٔ سایبری در جهان رخ می‌دهد و این میزان از حمله مانع از آن می‌شود که بتوان بین حملات جدی و نه‌چندان جدی تمایزی قائل شد (Kramer 2009: 15). با گسترش فناوری‌های اطلاعاتی و نفوذ هرچه بیش‌تر این فناوری‌ها در حیات شخصی و ملی افراد، دامنه و شدت این تهدیدات نیز گسترده‌تر می‌شود، مخصوصاً در جوامعی که افرادْ آزادی بیش‌تری در استفاده از فناوری‌ها دارند. ازاین‌رو لازم است که کشورها تدابیری را برای مقابله با این تهدیدات اتخاذ کنند.

استراتژی بازدارندگی یکی از نظریه‌های امنیتی سنتی است که می‌تواند در عرصهٔ سایبری نیز کارآیی خاص خود را داشته باشد.

از عصر یونان باستان، بازدارندگی بخشی از دکترین امنیتی ـ سیاسی کشورهای غربی بوده است (George and smoke 1974: 12). این استراتژیْ نقشی بسیار کلیدی در رویارویی دو ابرقدرت درطول جنگ سرد و عصر سلاح‌های هسته‌ای ایفا کرد و هم‌چنان نقش مهمی در سیاست جهانی دارد و حتی می‌توان آن را در جهان سایبر نیز به‌کار گرفت، چنان‌که درحال‌حاضر نیز عنصر اساسی در استراتژی امنیت ملی دولت آمریکا به‌شمار می‌رود (Bunn 2007). درواقع، درعین‌حال‌که عملیات سایبری توان‌مندی‌های مناسبی را در اختیار دولت‌ها قرار می‌دهد تا درجهت اهداف ملی خود گام بردارند، ابعاد جدیدی از مفهوم بازدارندگی را مطرح می‌سازد که برخی از این ابعاد منطبق با مفهوم سنتی بازدارندگی است و برخی دیگر نیز تازگی دارد. این ابعاد ازحیث حقوق بین‌الملل و مسائل سیاسی بحث‌های بسیاری را به خود اختصاص داده‌اند. ولی، ما در این مقاله به ابعاد عملیاتی و سیاسی آن می‌پردازیم تا کارآمدی آن در سیاست‌های امنیت ملی کشورها را موردمداقه 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 است که نوعی توان‌مندی در فضای سایبر برای خود ایجاد کند تا در مقابل تهدیدات دیگران از این توان‌مندی استفاده و دربرابر آن تهدیدات مقابله‌به‌مثل کند. کشورهای دیگری هم‌چون چین و هند نیز درصدد ایجاد سیستم تهاجمی تلافی‌جویانه‌ای برای مقابله با تهدیدات جدی یا بازداشتن دیگر بازیگران از تهدید سایبری علیه منافع ملی خودشان هستند (Bagchi 2008). به همین دلیل، تعجب‌آور نیست جوامعی که توان‌مندی حملات سایبری خود را تقویت می‌کنند منافعشان ایجاب کند که قدرت بازدارندگی خود در عرصهٔ سایبر را تقویت کنند. اما درمقابل جوامعی که توان‌مندی تلافی‌جویانهٔ آن‌ها بر ابزارهای متعارف تکیه دارد احساس نیاز اساسی به تقویت قدرت بازدارندگی سایبری نمی‌کنند.

هدف از بازدارندگی در عرصهٔ سایبری ایجاد تمایز بین آغاز و انجام اقدامات خصومت‌آمیز است. کشوری که قابلیت بازدارندگی در عرصهٔ سایبری را دارد تهدید می‌کند که رفتارهای نامناسب در این عرصه را مجازات خواهد کرد، اما درعین‌حال این موضوع را تلویحاً اعلام می‌کند که اگر رفتار نامناسبی شکل نگیرد یا خطوط قرمز آن نادیده گرفته نشود، تنبیهی هم در کار نخواهد بود.

کاگلر (Kugler)، که کارشناس صاحب‌نامی در زمینهٔ سیاست‌گذاری امنیت ملی است، به‌دلیل محدودیت‌های اقدامات دفاعی، به‌شدت از استراتژی بازدارندگی دفاع می‌کند (Kugler 2009: 309). پاتریک مورگان، رئیس گروه صلح و منازعه و علوم سیاسی در دانشگاه کالیفرنیا، نیز بر آن است که تحلیل‌گران سنتی نظریهٔ بازدارندگی به‌راستی متحیرند که چرا آمریکا تلاش زیادی نمی‌کند تا این استراتژی ارزش‌مند را به‌شکلی کارآمد در حوزهٔ سایبری به‌کار بندد. سؤالی که این‌جا مطرح می‌شود این است که استراتژی بازدارندگی کارآمد باید واجد چه ویژگی‌هایی باشد؟

۱.۶ بازدارندگی کارآمد در عرصهٔ سایبری

هدف از استراتژی بازدارندگیْ کاهش یا ازبین‌بردن خطر حمله با افزایش هزینه‌هاست تا مهاجم را به این نتیجه برساند که هزینه‌های حمله بیش از منافع آن است. برای کاربست این استراتژیْ داشتن دو نوع توان‌مندی بسیار حیاتی و کلیدی است. اولین توان‌مندی داشتن قابلیت دفاعی قوی و مستحکمی است که باعث شود مهاجم برای شروع حملهٔ خود احتیاط بیش‌تری به خرج داده تأمل بیش‌تری کند. در عرصهٔ سایبری، داشتن این توان‌مندی برای مقابله با اکثر حملات بسیار عملیاتی و مفید است. مورد دومْ توان‌مندی قابل‌ملاحظه برای اقدامات تلافی‌جویانه است. اگر تعدادی از مهاجمان با اقدامات تلافی‌جویانهٔ شدیدی روبه‌رو شوند، به‌احتمال زیاد مهاجمان دیگر از روی‌آوردن به حملهٔ سایبری نیز خودداری خواهند کرد.

چیزی که بازدارندگی در عرصهٔ سایبری را از مفهوم سنتی آن متمایز می‌کند مشکل شناسایی منبع حمله است. در جهان سایبری، این امر مانع بسیار عمده‌ای برای اتخاذ اقدامات تلافی‌جویانه است؛ چراکه قلمرو دیجیتالْ عرصهٔ گم‌نامی است. بنابراین، این چالش بُعد مهم سومی را به استراتژی بازدارندگی در عرصهٔ سایبری اضافه می‌کند و آن چالش شناسایی (attribution) است. ازاین‌رو، استراتژی بازدارندگی سایبری سه بعد مهم به شرح زیر دارد:

۱. دفاع: سیستم دفاعی مستحکمْ اولین گام در راه محافظت از منابع و زیرساخت‌های کشورها دربرابر اکثر مهاجمان است و اغلب آن‌ها را از انجام حمله منصرف می‌سازد.

۲. شناسایی: توان‌مندی مرتبط‌ساختن حمله‌ای به بازیگر یا منبعی خاصْ عنصر کلیدی دیگری در عرصهٔ سایبری است که اعتبار و مشروعیت بازیگر را در عرصهٔ داخلی و خارجی حفظ می‌کند.

۳. تلافی‌کردن: تمایل به تلافی هر حمله‌ای از هر منبعی و تحت هر شرایطی و توان‌مندی در آن باید ایجاد شود.

۱.۱.۶ دفاع

برای دست‌یابی به قدرت دفاعی مطلوب و کارآمد در عرصهٔ سایبر باید به‌خوبی بر ویژگی‌های این حوزه تسلط داشت. کرامر، معاون سابق وزیر دفاع و یکی از ویراستاران 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 ناشناس‌ماندن و مخفی‌شدن نیز فراهم است (Kramer 2009: 12). اما برخلاف زمین، فاصلهٔ جغرافیایی زیادی بین مهاجم و هدف او در عرصهٔ سایبری وجود دارد. این عامل هم‌راه با عنصر گم‌نامی ممکن است ترس از تلافی را کاهش دهد؛ برای مثال، دانشجویی که در مسکو در کافی‌نتی درحال قهوه‌خوردن و نفوذ به شبکهٔ زیرساختی یکی از نهادهای دولتی آمریکاست نگرانی کم‌تری از اقدامات تلافی‌جویانهٔ آمریکا دارد تا بازیگری که می‌خواهد به‌صورت مستقیم علیه آن نهاد حملهٔ نظامی انجام دهد.

تقریباً هیچ کشوری در دنیا نیست که بتواند روزانه درمقابل هزاران حملهٔ سایبری اقدامات تلافی‌جویانه انجام دهد یا عاملان آن‌ها را شناسایی کند (Morgan 2010: 59). بنابراین، اولین عنصر نظریهٔ بازدارندگی در عرصهٔ سایبری باید قدرت دفاعی قوی باشد، بدان معنا که سخت‌افزارها و نرم‌افزارها به‌شکل مستحکمی با یک‌دیگر امتزاج یافته باشند و بتوانند هرنوع دست‌رسی غیرمجازی را تقریباً غیرممکن سازند. این امر دو هدف عمده را برآورده می‌سازد: نخست این‌که باعث می‌شود اغلب افراد غیرمجاز نتوانند وارد سیستم شوند؛ دوم این‌که افراد غیرمجاز را از تلاش برای نفوذ در سیستم باز می‌دارد، چراکه احتمال موفقیت خود را کم می‌بینند (Kugler 2009: 334). هدف اصلی مؤلفهٔ دفاعی آن است که مهاجمان علاقه‌مند به حمله را از انجام حمله منصرف سازد یا مسیر آن‌ها را مسدود کند. ازاین‌رو، با کاهش میزان مهاجمان، بقیهٔ مهاجمان را می‌توان با مؤلفهٔ اقدامات تلافی‌جویانه از حملات بعدی منصرف ساخت.

۲.۱.۶ شناسایی

مسئلهٔ شناسایی مشکل شناخته‌شدهٔ جهانی در عرصهٔ سایبری است. حضور گسترده و بی‌شمار کاربران و ماهیت نسبتاً ناشناس آن‌ها در حوزهٔ سایبری باعث می‌شود که مسئلهٔ

شناسایی مهاجم و نسبت‌دادن حملهٔ سایبری به فرد یا گروهی خاص دشوارتر از دوران بازدارندگی هسته‌ای باشد (Kramer 2009: 12). دولت‌ها می‌توانند، برای پنهان‌ماندن از شناسایی‌شدن، اقدامات خود را توسط افراد یا گروهی از کاربران انجام دهند و هر اتهامی را به‌راحتی منکر شوند. افراد و گروه‌ها نیز می‌توانند بدون پشتوانهٔ مالی قابل‌توجه به تأسیسات دولتی یا شرکت‌های خصوصی حمله کنند.

اما همهٔ این موارد بدان معنا نیست که شناسایی مهاجم غیرممکن است؛ زیرا نمونه‌های موفق زیادی در این خصوص وجود دارد. عاملان حملهٔ سایبری به شبکه‌های اطلاعاتی در استونی در سال ۲۰۰۷ و گرجستان در سال ۲۰۰۸ به‌سرعت شناسایی شدند؛ این عاملان ماهیت روسی داشتند. اخیراً هم روزنامهٔ *NEW York Times* با بهره‌گیری از کارشناسان سایبری توانست هکرهایی را شناسایی کند که اسم کاربری و رمز عبور آن را ربوده بودند و دست به اقدامات غیرقانونی در فضای سایبر می‌زدند. آنان تبعهٔ چین بودند (Goodman 2010: 105). این نمونه‌ها نشان می‌دهد که مسئلهٔ شناسایی غیرقابل‌حل نیست و می‌توان به‌طور نسبی بر این مشکل نیز فائق آمد. درعمل، بسیاری از حملات سایبری تا حد مکان اعمال آن‌ها شناسایی شده‌اند، هرچند که برخی هکرها از مجازات گریخته‌اند. با سرمایه‌گذاری در نیروی انسانی و بخش تکنولوژی می‌توان بر این مشکل نیز چیره گشت.

باوجود این چالش‌ها در حوزهٔ شناسایی، باید اشاره کرد که این مؤلفه هم‌چنان بخش کلیدی و اساسی نظریهٔ بازدارندگی در حوزهٔ سایبری است؛ چراکه شناسایی موفقْ ضامن مؤثر و مفیدبودن اقدامات تلافی‌جویانه است و باعث می‌شود که تهدیدات واقعی از بین برود. شناسایی موفق عاملان حمله اعتبار و مشروعیت دولت‌ها را در داخل و در جامعهٔ بین‌المللی افزایش می‌دهد.

۳.۱.۶ اقدامات تلافی‌جویانه

استراتژی بازدارندگی بدون اقدامات تلافی‌جویانه موفق نخواهد بود. در نبود اقدامات تلافی‌جویانه، مهاجمان بالقوه هم انگیزه‌ای برای خودداری از حمله ندارند. مورگان بر این اعتقاد است که کارآمدی اقدامات تلافی‌جویانه دربرگیرندهٔ سه شاخص عمده است: غیرقابل‌قبول‌بودن آن برای دشمن، عملیاتی‌بودن آن، و قابل‌قبول‌بودن آن برای طرف تلافی‌کننده و هم‌چنین پذیرش جامعهٔ جهانی (Morgan 2010: 56).

برای مقابله با بازیگران غیردولتی، اتخاذ اقدامات تلافی‌جویانهٔ متناسب با جرم رخ‌داده چالش‌هایی را برای دولت‌ها به‌وجود می‌آورد؛ زیرا هنوز قوانینی در حقوق بین‌الملل برای

این موضوع تصویب نشده است. به همین منظور، کشورها باید به‌شدت در این زمینه فعال باشند و دقیقاً اقدامات غیرقانونی را تعریف کنند. این امر می‌تواند در فرایند قضایی و دادخواهی بسیار مؤثر واقع شود.

باوجود این مشکل حقوقی، مقابله با تهدید بازیگران غیردولتی بسیار حائز اهمیت است. بسیاری از حملات سایبری روزانه به‌علت عدم ترس مهاجمان از تلافی است. اگر دولت‌ها درپی کاستن از میزان این حملات مخرب هستند، باید در عمل نشان دهند که مهاجمان از تلافی آن‌ها در امان نخواهند بود. لازم نیست که اقدامات تلافی‌جویانه شبیه اقدام مهاجم باشد. زمانی‌که رفتارهای سایبری غیرقانونی دقیقاً مشخص و تعریف شدند، دستگیری و بازداشت عاملان آن‌ها نیز گزینهٔ مناسبی خواهد بود.

مسئلهٔ تلافی در روابط بین کشورها متفاوت با افراد و بازیگران غیردولتی است و مسئلهٔ دیگری را پیش می‌کشد؛ زیرا ممکن است آثار پیچیده‌ای بر روابط بین دو کشور داشته باشد. اما، برای انجام اقدامات تلافی‌جویانه علیه کشور مهاجم، بازیگران دولتی نباید اقدامات خود را محدود به حوزهٔ سایبری کنند، بلکه برای بیشینه‌سازی کارآمدی بازدارندگی در حوزهٔ سایبری، دولت‌ها باید آمادگی خود را برای اتخاذ انواع اقدامات تلافی‌جویانه در حوزه‌های مختلف از تحریم‌های اقتصادی و ضبط اموال کشور مهاجم گرفته تا انواع اقدامات دیپلماتیک و سیاسی و حتی نظامی نشان دهند.

اقدامات تلافی‌جویانه علیه کشورها ضرورتاً لازم نیست با اقدام طرف مقابل متناسب باشد؛ یعنی کیفر حتماً نباید متناسب با جرم باشد؛ اما باید واقعیت‌های ژئوپلتیکی را هم در نظر داشت. رهبران باید همواره این محاسبه را انجام دهند که چه‌نوع اقدامی بهتر می‌تواند مانع از اقدامات مشابه در آینده شود. ولی، اقدام اتخاذشده باید به‌قدری شدید باشد که هر مهاجم بالقوهٔ دیگری را از انجام حمله در آینده منصرف سازد. هم‌چنین این اقدام باید بتواند مشروعیت لازم داشته باشد و حمایت دیگر بازیگران را از اقدامات تلافی‌جویانهٔ آتی درپی داشته باشد.

پرچالش‌ترین اتفاقات سایبری زمانی است که نتوان عاملان حمله‌ای را شناسایی کرد. مورگان بر این باور است که در نظریهٔ بازدارندگی کلاسیکْ شناسایی غیرضروری است و هر کشوری را می‌توان درقبال حمله‌ای که از خاک آن کشور به کشور دیگر انجام می‌شود مسئول قلمداد کرد (Morgan 2010: 70). اما این قاعده را در حوزهٔ سایبری فقط در ارتباط با حملات بسیار شدید می‌توان پذیرفت. گودمن نیز از این نظریه دفاع می‌کند که اگر رفتاری

غیرقانونی قابل‌انتساب به کشوری باشد، آن‌گاه مسئلهٔ شناسایی دقیق مهاجمان ضروری نخواهد بود (Goodman 2010: 79). علی‌رغم آرای ذکرشده، عملی‌کردن آن‌ها در دنیای واقعی دشوار است و ره‌یافت مناسبی برای برخورد با حملات سایبری نیست؛ چراکه تنبیه یک کشور به‌دلیل حملات سایبری افراد گم‌نام تاحدود زیادی به شرایط ژئوپلتیکی، اقتصادی، و دیپلماتیک ارتباط پیدا می‌کند (Kugler 2009: 328). هم‌چنین کشورها نمی‌توانند این هنجار را ایجاد کنند که، به‌دلیل حملهٔ سایبری افرادی از خاک یک کشور علیه آن‌ها، خود آن کشور را متهم بدانند؛ زیرا این هنجار ممکن است در آینده علیه خود آن‌ها نیز به‌کار رود.

۷. نتیجه‌گیری

ماهیت حوزهٔ سایبری متفاوت با دنیای واقعی است و نظریهٔ بازدارندگی سایبری نمی‌تواند کارآیی دوران جنگ سرد و عصر هسته‌ای را داشته باشد. این استراتژی راه‌حل نهایی برای جرائم سایبری، جاسوسی، و حملات سایبری نیست؛ هم‌چنین، فارغ از کارآمدی آن، نمی‌تواند جرائم سایبری را کاملاً ریشه‌کن سازد. اما این استراتژی نقشی کلیدی در کاهش حملات سایبری تاحد تعدادی قابل‌مدیریت دارد؛ این موارد باقی‌مانده را هم می‌توان با اقدامات تلافی‌جویانه و هزینهٔ کم‌تر کاهش داد.

برای کارآمدی بازدارندگی در حوزهٔ سایبر، باید از ترکیب سه مؤلفهٔ کلیدی، یعنی دفاع، شناسایی، و تلافی، بهره جست. بدون اقدامات دفاعی مناسب، نمی‌توان تعداد حملات موفق را (که باید شناسایی شوند) کاهش داد و این حملات از کنترل خارج می‌شود. فناوری‌های شناسایی باید بتوانند منابع حمله را شناسایی کنند تا مانع از اقدامات مهاجمان بالقوه در آینده، به‌سبب ترس از شناسایی‌شدن، شوند. تلافی از آن رو حائز اهمیت است که نشان می‌دهد اقدام سایبری علیه دولت و نهادهای آن یا مردم حتماً با مجازاتی روبه‌رو خواهد شد.

پی‌نوشت‌ها

۱. این مدل با عنوان PIME مخفف political، informational، military، و economic است و یکی از مدل‌های مشهور برای بررسی عناصر قدرت محسوب می‌شود.

۲. باگ‌ها (bugs) را در اصطلاحات علوم کامپیوتر «اشکال» یک برنامه یا هر سیستم عامل معنی می‌کنند. اگر نرم‌افزار یا حتی سیستم عاملی اشکالی داشته باشد، اصطلاحاً باگ دارد.

۳. بک‌دورها (back doors)، که در فارسی به «در پشتی» نیز ترجمه شده است، به‌معنای آسیب‌پذیری خاصی در رایانه‌هاست که به هکرها و حمله‌کنندگان فرصت می‌دهد تا مکانیزم‌های امنیتی معمول را دور زده به‌صورت غیرمجاز به منابع و اطلاعات سیستم دست‌رسی داشته باشند. ازآن‌جاکه این تهدید در پس‌زمینه فعال است و خود را از کاربر پنهان می‌سازد، شناسایی و حذف آن کاری تقریباً مشکل است.

۴. بات‌نت‌ها (botnets) شبکه‌هایی هستند که با دراختیارگرفتن مجموعه‌ای از کامپیوترها که بات (bot) نامیده می‌شوند به‌وجود می‌آیند. این شبکه‌ها را یک یا چند مهاجم که botmaster نامیده می‌شوند با هدف انجام فعالیت‌های مخرب کنترل می‌کنند. بات‌ها کدهای مخربی هستند که روی کامپیوترهای میزبان اجرا می‌شوند تا امکان کنترل آن‌ها را از راه دور برای botmaster فراهم کنند و او بتواند این مجموعه را وادار به انجام فعالیت‌های مختلف کند.

کتاب‌نامه

آلبرتس، دیوید س. و دانیل س. پاپ (۱۳۸۵)، *گزیده‌ای از عصر اطلاعات: الزامات امنیت ملی در عصر اطلاعات*، ترجمهٔ علی علی‌آبادی و رضا نخجوانی، تهران: پژوهشکدهٔ مطالعات راهبردی.

روزنا، جیمز و دیگران (۱۳۹۰)، *انقلاب اطلاعات، امنیت و فناوری‌های جدید*، ترجمهٔ علیرضا طیب، تهران: پژوهشکدهٔ مطالعات راهبردی.

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

غروی، حسین و علی محمدی (۱۳۹۰)، «معرفی رویکردها و متدولوژی‌های طراحی و اجرای سناریوهای مقابله با تهدیدات سایبری»، در: *مجموعه‌مقالات همایش ملی دفاع سایبری*، تهران: دانشگاه دفاع ملی.

منوچهری، عباس (۱۳۷۶)، *قدرت، مدرنیسم، و پست‌مدرنیسم*، مجلهٔ *اطلاعات سیاسی ــ اقتصادی*، ش ۱۲۱–۱۲۲.

مورگنتا، هانس جی. (۱۳۸۹)، *سیاست میان ملت‌ها: تلاش در راه قدرت و صلح*، تجدیدنظر کنت دبلیو. تامپسون، ترجمهٔ حمیرا مشیرزاده، تهران: وزارت امور خارجه.

Bagchi, Indrani (2008), "China Mounts Cyber Attacks on Indian Sites", *The Times of India*: <https://timesofindia.indiatimes.com/india/China-mounts-cyber-attacks-on-Indian-sites/articleshow/3010288.cms>.

Bajaj, Kamlesh. (2010), "The Cybersecurity Agenda: Mobilizing for International Action", The EastWest Institute: < https://www.eastwest.ngo/sites/default/files/ideas-files/Bajaj_Web.pdf>

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

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

Bollier, David (2003), *The Rise of Netpolitik: How the Internet Is Changing International Politics and Diplomacy; A Report of the Eleventh Annual Aspen Institute Roundtable on Information Technology*, Washington: The Aspen Institute.

Bryant, Rebecca (2001), "What Kind Of Space Is Cyberspace?," *Minerva*, no. 5.

Bunn, M. Elaine (2007), "Can Deterrence Be Tailored?," *Strategic Forum*, no. 225.

Cheswick, William R., Steven M. Bellovin, and Aviel D. Rubin (2003), *Firewalls and Internet Security: Repelling the Wily Hacker* (2nd ed.), Boston: Addison-Wesley.

Clarke, Richard A. and Robert K. Knake (2012), *Cyber War: The Next Threat to National Security and What to Do About It*, New York: Harper Collins.

Crampton, Jeremy W. (2004), *The Political Mapping of Cyberspace*, Chicago: University of Chicago.

Eriksson, Johan and Giampiero Giacomello (2006), "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?," *International Political Science Review*, vol. 27, no. 3.

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

Gibson, William (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. (2009), "Cyberpower and National Security: Policy Recommendations for a Strategic Framework", in: *Cyberpower and National Security*, Franklin D. Kramer, Stuart H. Star, and Larry K. Wentz (eds.), Dulles: National Defense University Press and Potomac Books.

Kugler, Richard L. (2009), "Deterrence of Cyber Attacks", in: *Cyberpower and National Security*, Franklin D. Kramer, Stuart H. Star, and Larry K. Wentz (eds.), Dulles: National Defense University Press and Potomac Books.

Libicki, Martin C. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica: Rand.

Lin, Herbert. (2011), "Responding to Sub-Threshold Cyber Intrusions: A Fertile Topic for Research and Discussion", *Georgetown Journal of International Affairs*, Special vol., International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity.

Morgan, Patrick M. (2010), "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm", in: National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, DC: National Academies.

Nye, Joseph S. (2011), *The Future of Power*, New York: Public Affairs.

Obama, Barack (2013), "Executive Order 13636-Improving Critical Infrastructure Cybersecurity", *Federal Register*:

<https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>.

United States and Ronald Reagan (1988), *National Security Strategy of the United States*, Washington: the White House.

Starr, Stuart H. (2009), "Developing a Theory of Cyber Power", in: F. D. Kramer, S. Starr, and L. K. Wentz (ed.), *Georgetown Journal of International Affairs*, Special Issue, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity.