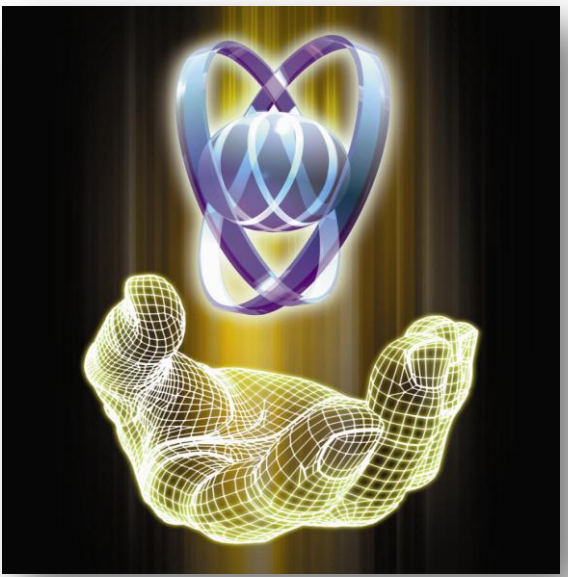
فضای سایبر

بعنوان یک حوزه جدید و مهم از قدرت



فهرست

مقدمه

جوزف اس.نای (Joseph S. Nye) "استاد برجسته دانشگاه هاروارد و نظریه پرداز جنگ نرم در سایت "مرکز علوم و امور بین‌المللی بلفر – دانشکده کندی هاروارد" مقاله ای را در رابطه با اینکه فضای سایبر یک حوزه جدید و مهم از قدرت است، به چاپ رسانده است که اهمیت این فضا در آن تا حدود زیادی بیان شده است.

این نظریه پرداز آمریکایی جنگ نرم در تعریف قدرت سایبری می‌نویسد: قدرت در بستر معنا می‌یابد، و رشد سریع فضای سایبر بستری جدید و مهم در سیاست جهان است، فضای سایبر یک حوزه جدید و مهم از قدرت است و حتی کشورهایی مانند آمریکا، که منابع عظیمی از قدرت سخت و نرم در اختیار دارند، خود را در حال تقسیم عرصه با بازیگران جدید و مواجه شدن با مشکلات بیشتر در کنترل مرزهایشان در حوزه سایبر می‌یابند.

چکیده

قدرت در بستر معنا می‌یابد، و رشد سریع فضای سایبر بستری جدید و مهم در سیاست جهان است .هزینه پایین ورود، گمنامی، و نامتقارن بودن در آسیب‌پذیری، بدین معناست که بازیگران کوچکتر در فضای سایبر نسبت به حوزه‌های سنتی‌تر سیاست جهانی ظرفیت بیشتری برای اعمال قدرت سخت و نرم دارند. تغییرات به وجود آمده در اطلاعات همیشه تاثیر مهمی بر قدرت داشته‌اند، اما حوزه سایبر یک محیط مصنوعی جدید و غیرقابل پیش‌بینی است. ویژگی‌های فضای سایبر برخی از اختلافات قدرت بین بازیگران را کاهش داده و بدین ترتیب مثال خوبی از پراکندگی قدرت را که ویژگی سیاست جهانی در قرن حاضر است، به نمایش می‌گذارد. قدرت‌های بزرگ نخواهند توانست به اندازه حوزه‌هایی چون دریا و خشکی بر این حوزه مسلط شوند. نکته دیگری که فضای سایبر بر آن تاکید می‌کند این است که پراکندگی قدرت به معنای برابری قدرت یا جایگزینی دولت‌ها به عنوان قدرتمندترین بازیگران سیاست جهانی نیست.

اطلاعات و پراکندگی قدرت

انتقال قدرت از یک کشور برتر به کشور دیگر یک رویداد تاریخی آشناست، اما پراکندگی قدرت روندی جدید است. مشکل کشورها در عصر اطلاعات امروز این است که چیزهای بیشتری خارج از کنترل قدرتمندترین کشورها حادث می‌شوند.

انقلاب اطلاعاتی جدید در حال تغییر ماهیت قدرت و افزایش پراکندگی آن است. دولت‌ها بازیگران غالب در عرصه جهانی باقی خواهند ماند، اما این عرصه را خیلی شلوغ‌تر، و کنترل آن را مشکل‌تر خواهند یافت .اکنون بخش خیلی بیشتری از جمعیت هم در داخل و هم خارج از کشورها به قدرتی دسترسی دارند که از اطلاعات نشئت می‌گیرد . حکومت‌ها همیشه در مورد جریان و کنترل اطلاعات نگران بوده‌اند، و دوره کنونی اولین دوره‌ای نیست که از تغییرات چشمگیر در فن‌آوری اطلاعات شدیدا متاثر می‌شود. به عنوان مثال، گفته می‌شود که اختراع دستگاه چاپ به دست یوهان گوتنبرگ در قرن پانزدهم که منجر به چاپ انجیل و قرار گرفتن آن در دسترس بخش بزرگی از اروپا شد، نقش عمده‌ای در شروع اصلاحات داشته است.

انقلاب اطلاعاتی کنونی، که گاها "انقلاب صنعتی سوم" نیز خوانده می‌شود، ریشه در پیشرفت‌های تکنولوژیکی سریع در زمینه رایانه، ارتباطات و نرم‌افزار دارد که متعاقبا منجر به کاهش اساسی هزینه ایجاد، پردازش و انتقال اطلاعات شده است. طی۳۰ سال، سرعت محاسباتی در هر ۱۸ ماه دو برابر می‌شد، در حالیکه در آغاز قرن بیست‌ویکم هزینه آن هزار برابر نسبت به اوایل دهه ۱۹۷۰ کاهش یافته بود. در سال ۱۹۹۳ حدود ۵۰ وب‌سایت در جهان وجود داشت حال آنکه تا انتهای دهه این رقم از ۵ میلیون فراتر رفته بود. تا سال ۲۰۱۰ چین به تنهایی نزدیک به ۴۰۰ میلیون کاربر داشت.

پهنای باندهای مخابرات به سرعت افزایش می‌یابد، و هزینه‌های مخابراتی حتی از هزینه‌های قدرت محاسباتی نیز سریعتر کاهش می‌یابند. تا همین اواخر در سال ۱۹۸۰، تماس‌های تلفنی روی سیم‌های مسی در هر ثانیه تنها یک صفحه اطلاعات را می‌توانستند منتقل کنند، در حالیکه امروز، یک رشته باریک فیبر نوری می‌تواند نود هزار جلد کتاب را در یک ثانیه منتقل کند! در سال ۱۹۸۰ یک گیگابایت حافظه فضایی به اندازه یک اتاق را اشغال می‌کرد و امروز ۲۰۰ گیگابایت حافظه در جیب پیراهن شما جای می‌گیرد!

مقدار اطلاعات دیجیتال هر پنج سال ده برابر می‌شود. این موضوع برای قدرت و حاکمیت در قرن بیست‌ویکم چه معنایی می‌تواند داشته باشد؟

فضای سایبر یک حوزه جدید و مهم از قدرت است

"قدرت"، به عنوان مضمونی که به طور وسیع مورد استفاده قرار می‌گیرد، به طور شگفت‌انگیزی نامحسوس بوده و اندازه‌گیری‌اش مشکل است .همانند بسیاری از ایده‌های پایه، قدرت یک مفهوم مورد بحث است. هیچ تعریف واحدی وجود ندارد که مورد قبول تمام کسانی که از این واژه استفاده می‌کنند قرار داشته باشد، و تعریفی که افراد برای آن انتخاب می‌کنند منعکس کننده منافع و ارزش‌هایشان است. فرهنگ لغت به ما می‌گوید که قدرت ظرفیت انجام کارها است، اما اگر به طور ویژه به مسائل سیاسی علاقمند باشید، قدرت عبارت است از توانایی تاثیر بر افراد دیگر به منظور نیل به نتایج مورد نظر. برخی افراد این را نفوذ می‌نامند، و قدرت را از نفوذ متمایز می‌سازند، اما علت اینکه در این تعریف سردرگمی وجود دارد این است که فرهنگ لغت این دو واژه را طوری تعریف کرده است که به جای یکدیگر به کار می‌روند.

از دیدگاه "ماکس وبر"، می‌خواهیم بدانیم امکان اینکه یک بازیگر در یک رابطه اجتماعی بتواند خواسته خود را پیش ببرد، چقدر است. حتی هنگامی که بر روی عوامل یا بازیگران به خصوصی تمرکز می‌کنیم، بدون مشخص کردن قدرت برای "انجام چه چیز"، نمی‌توانیم بگوییم که یک بازیگر "قدرت دارد". باید مشخص شود که چه کسانی در رابطه قدرت درگیر هستند، به علاوه اینکه چه موضوعاتی مورد بحث هستند. اظهارنظر در مورد قدرت همیشه به زمینه بستگی دارد و فضای سایبر یک زمینه جدید و مهم از قدرت است.

تعاریف علوم اجتماعی نوین از قدرت رفتاری، گاها تحت عنوان "سه روی قدرت" خلاصه می‌شوند. اولین جنبه قدرت وادار ساختن افراد برای انجام کاری که در شرایط دیگر آن را انجام نمی‌دهند است، "روی دوم قدرت" بعد تعیین برنامه، یا تنظیم مسائل به نحوی است که هرگز مسئله تحمیل و اجبار مطرح نشود. و در دهه ۱۹۷۰، عنوان شد که عقاید و باورها نیز در شکل دادن به سلایق دیگران موثر هستند و فرد با تعیین خواسته‌های دیگران نیز می‌تواند اعمال قدرت کند. در سال ۱۹۹۰، من قدرت سخت و نرم را همراه با دامنه‌ای از

رفتار اجباری تا انتخابی، از یکدیگر متمایز کردم. رفتار قدرت سخت بر پایه اجبار و پرداخت قرار دارد. اما رفتار قدرت نرم بر اساس تدوین دستورکار، جذب یا ترغیب استوار است.

حتی کشورهای بزرگ که منابع عظیمی از قدرت سخت و نرم در اختیار دارند، خود را در حال تقسیم عرصه با بازیگران جدید و مواجه شدن با مشکلات بیشتر در کنترل مرزهایشان در حوزه سایبر می‌یابند .فضای سایبر جای فضای جغرافیایی را نخواهد گرفت و حاکمیت دولت را منسوخ نخواهد ساخت، اما پراکندگی قدرت در فضای سایبر وجود خواهد داشت و اعمال قدرت در هر یک از این ابعاد را به شدت پیچیده خواهد ساخت.

قدرت سایبری

قدرت سایبری برخلاف قدرت بر اساس منابع اطلاعاتی موضوع جدیدی است؛ تعاریف متعددی برای فضای سایبر وجود دارد اما عموما "سایبر" پسوندی است که معنای فعالیت‌های مرتبط با رایانه و الکترونیک را می‌رساند. بر اساس یکی از تعاریف، فضای سایبر یک حوزه عملیاتی است که به منظور بهره‌برداری از اطلاعات از طریق سامانه های به هم پیوسته و زیرساخت یکپارچه آن‌ها، با استفاده از علم الکترونیک شکل گرفته است. بعضی وقت‌ها فراموش می‌کنیم که فضای سایبر تا چه حد تازگی دارد. در سال ۱۹۶۹، وزارت دفاع آمریکا تحت پروژه ARPANET شروع به اتصال محدود چند رایانه کرد و در سال ۱۹۷۲ کدهای تبادل داده (TCP/IP) ایجاد شدند تا یک اینترنت اولیه را که قادر به مبادله بسته‌های اطلاعات دیجیتال باشد، تشکیل دهند .سامانه نام دامنه آدرس‌های اینترنتی در سال ۱۹۸۳ راه اندازی شد و اولین ویروس‌های رایانه ای در حدود همان زمان به وجود آمدند. شبکه جهانی (World Wide Web) در سال ۱۹۸۹ آغاز به کار کرد. معروفترین موتور جستجو، یعنی گوگل، در سال ۱۹۹۸تاسیس شد. در اوخر دهه ۱۹۹۰ شرکت‌های تجاری استفاده از فناوری جدید را آغاز کردند تا تولید و فروش را در زنجیره‌های پیچیده تامین جهانی تغییر دهند. دایرةالمعارف منبع باز ویکیپدیا در سال ۲۰۰۱ آغاز به کار کرد و "پردازش ابری"، که طی آن شرکت‌ها و افراد می‌توانند داده‌ها و نرم‌افزارهایشان را در وب ذخیره کنند، تنها همین اواخر به وجود آمده‌اند. شرکت اختصاص اسامی و شماره‌ها در اینترنت (ICANN) در سال ۱۹۹۸ به وجود آمد و دولت آمریکا تنها از ده سال پیش توسعه طرح‌های ملی جدی برای امنیت سایبری را آغاز کرده است. در سال

۱۹۹۲، تنها یک میلیون کاربر اینترنت وجود داشت و طی ۱۵ سال این رقم به یک میلیارد رسید.

فضای سایبر را می‌توان به صورت لایه‌های زیادی از فعالیت‌ها تصور کرد، اما برداشت ساده و اولیه آن را به صورت یک رژیم مرکب منحصر به فرد از خصوصیات فیزیکی و مجازی به تصویر می‌کشد. لایه زیرساخت فیزیکی از قوانین اقتصادی منابع رقیب و افزایش هزینه‌های جانبی و قوانین سیاسی قدرت عالیه و کنترل پیروی می‌کند. لایه مجازی یا اطلاعاتی، از ویژگی اقتصادی "بازده فزاینده نسبت به مقیاس" برخوردار بوده و رسوم سیاسی آن به گونه‌ای است که کنترل قانونی را مشکل می‌سازد. از حوزه اطلاعاتی، که هزینه‌ها در آن پایین است، می‌توان حملاتی را علیه حوزه فیزیکی، که منابع آن کمیاب و گران هستند، انجام داد. اما برعکس، کنترل لایه فیزیکی می‌تواند آثار سرزمینی و برون‌مرزی بر لایه اطلاعاتی داشته باشد.

رفتار قدرت سایبری بر مجموعه‌ای از منابع استوار است که به ایجاد، کنترل و انتقال اطلاعات بر اساس الکترونیک و رایانه مربوط می‌شوند – یعنی زیرساخت، شبکه‌ها، نرم‌افزار و مهارت انسانی– این قدرت یک شبکه سراسری از رایانه های به هم پیوسته (اینترنت)، همچنین شبکه‌های داخلی (اینترانت)، فناوری‌های تلفن همراه و ارتباطات ماهواره‌ای را شامل می‌شود. اگر بخواهیم از بعد رفتاری تعریف کنیم، قدرت سایبری عبارت است از توانایی کسب نتایج مطلوب با استفاده از منابع اطلاعاتی الکترونیکی در حوزه سایبری. طبق یکی از تعاریف جامع، قدرت سایبری یعنی توانایی استفاده از فضای سایبر برای خلق مزیت‌ها و تاثیر بر رویدادهای محیط‌های عملیاتی دیگر و ابزارهای قدرت. قدرت سایبری می‌تواند برای حصول نتایج مطلوب در داخل فضای سایبر استفاده شود، یا می‌تواند از ابزارهای سایبری برای کسب نتایج مطلوب در حوزه‌های دیگر خارج از فضای سایبر استفاده کند. به همین سیاق، قدرت دریایی به استفاده از منابع در حوزه دریا برای پیروزی در نبردهای دریایی، کنترل نقاط بازرسی کشتیرانی نظیر تنگه‌ها و نمایش حضور در دریاها اتلاق می‌شود، اما همچنین توانایی استفاده از دریاها برای تاثیر گذاشتن بر نبردها، تجارت و افکار در خشکی را نیز شامل می‌شود.

در سال ۱۸۹۰، "آلفرد تایر ماهان [Alfred Thayer Mahan] "اهمیت قدرت دریایی را در زمینه فن‌آوری‌های جدید موتور بخار، زره و توپ‌های دوربرد برجسته ساخت. در سال

" ۱۹۰۷تئودور روزولت" نیروی دریایی آب‌های آزاد خود را به شکل قابل‌توجهی گسترش داده و آن را به سراسر جهان گسیل نمود. پس از معرفی هواپیما در جنگ جهانی اول، نظامیان شروع به نظریه پردازی در مورد حوزه قدرت هوایی و قابلیت آن برای حمله مستقیم به مرکز ثقل شهری دشمن بدون نیاز به عبور ارتش از مرزها کردند. سرمایه‌گذاری‌های فرانکلین روزولت در قدرت هوایی در جنگ جهانی دوم حیاتی بود. پس از ساخت موشک‌های قاره‌پیما و ماهواره‌های شناسایی و مخابراتی در دهه ۱۹۶۰، نویسندگان شروع به نظریه‌پردازی در مورد حوزه مخصوص قدرت فضایی نمودند. "جان اف کندی" برنامه‌ای را آغاز کرد تا از پیشگامی آمریکا در فضا مطمئن شده و یک انسان را به ماه بفرستد. در سال ۲۰۰۹، "باراک اوباما" خواستار یک پیشقدمی بزرگ و جدید در زمینه قدرت سایبری شد و کشورهای دیگر نیز این رویه را پیش گرفته‌اند. این نشان می دهد به محض اینکه تغییرات فناورانه، حوزه‌های قدرت را تغییر می‌دهند، رهبران سیاسی نیز با آن همراهی می‌کنند.

حوزه سایبر از این نظر منحصر به فرد است که مجازی و نوین بوده و به مراتب سریع‌تر از محیط‌های دیگر در معرض تغییرات فناورانه است . "جغرافیای فضای سایبر بسیار ناپایدارتر از محیط‌های دیگر است. جابجا کردن کوه‌ها و دریاها مشکل است، اما با فشردن یک کلید می‌توان بخش‌هایی از فضای سایبر را خاموش و روشن کرد!" گسیل کردن الکترون‌ها به سراسر جهان ارزان‌تر و سریع‌تر از جابجایی کشتی‌های بزرگ در فواصل طولانی آن هم با اصطکاک آب شور است. هزینه‌های ساخت هواپیمابرها و ناوگان‌های زیردریایی، موانع عظیمی را برای ورود کشورها به این حوزه ایجاد می‌کنند و ما را قادر می‌سازد تا از تسلط دریایی دم بزنیم. با اینکه دزدی دریایی یک گزینه محلی برای بازیگران غیردولتی در مناطقی چون تنگه‌های سومالی و مالاکا است، کنترل دریایی از دست بازیگران غیردولتی خارج است. در مقابل، به طوریکه قبلا ذکر شد، موانع ورود به حوزه سایبر آن‌قدر کم هستند که بازیگران غیردولتی و دولت‌های کوچک نیز می‌توانند با هزینه‌ای پایین نقش برجسته‌ای ایفا نمایند. بر خلاف دریا، هوا و فضا، "حوزه سایبر" در سه ویژگی با جنگ زمینی مشترک است. این ویژگی‌ها عبارتند از تعداد بازیکنان، آسان بودن ورود، و شانس اختفا .با اینکه کشورهای معدودی بر روی زمین استعداد بیشتری نسبت به دیگران دارند اما تسلط، معیاری نیست که در این حوزه به سادگی بتوان اندازه گرفت. صحبت از تسلط در فضای سایبر نیز

به طوریکه در مورد قدرت‌های دریایی و هوایی رایج است، بی‌معناست. حتی اگر چنین چیزی وجود هم داشته باشد، وابستگی به سامانه های سایبری پیچیده برای پشتیبانی از فعالیت‌های نظامی و اقتصادی، نقاط ضعف جدیدی را در کشورهای بزرگ به وجود می‌آورد که می‌توانند مورد بهره‌برداری بازیگران غیر دولتی واقع شوند.

مناقشه در حوزه سایبر یا "جنگ سایبری" نیز با جنگ های معمول متفاوت است .در جهان فیزیکی، دست حکومت‌ها در استفاده از نیرو در مقیاس وسیع تقریبا باز است، کشور مدافع شناخت کامل از عوارض دارد، و حملات در نتیجه فرسایش یا خستگی پایان می‌یابند. منابع و تحرک، هر دو هزینه‌بر هستند. اما در دنیای مجازی، بازیگران متنوع و گاها ناشناس هستند، فاصله فیزیکی بی‌اهمیت است، و یک تهاجم مجازی تقریبا بدون هزینه تمام می‌شود .از آنجا که اینترنت بیشتر برای راحتی استفاده طراحی شده بود تا امنیت، در حال حاضر تهاجم بر دفاع مزیت دارد. طرف بزرگتر توانایی محدودی در خلع سلاح یا نابودی دشمن، اشغال سرزمین، یا استفاده موثر از سلاح‌های راهبردی دارد. ابهام در تمامی جنبه‌ها وجود دارد و هرج و مرج را تقویت می‌کند. افزونگی، انعطاف و بازسازی سریع، مولفه‌های حیاتی دفاع هستند. به طوریکه یک کارشناس عنوان کرده است، تلاش برای انتقال مفاهیم سیاسی از شکل‌های دیگر جنگ نه تنها ناکام خواهد ماند، بلکه در برنامه‌ریزی و سیاست اخلال ایجاد خواهد کرد .

قدرت سایبری بسیاری از حوزه‌های دیگر – از جنگ تا تجارت – را تحت تاثیر قرار می‌دهد. همانطور که در مورد قدرت دریایی می‌توان قدرت دریایی در اقیانوس‌ها را از قدرت دریایی در خشکی متمایز ساخت، در مورد قدرت سایبری هم دو نوع قدرت "داخل فضای سایبری" و "بیرون فضای سایبری" قابل تمایز هستند. به عنوان مثال، هواپیمای مستقر در ناو هواپیمابر می‌تواند در نبردهای خشکی شرکت کند؛ در نتیجه کارآیی نسل جدید کشتی‌های کانتینربر تجارت و بازرگانی می‌توانند رشد کنند؛ و قدرت نرم یک کشور می‌تواند با شرکت این کشتی‌ها در ماموریت‌های بشردوستانه افزایش یابد.

در داخل حوزه سایبر ابزار اطلاعاتی می‌توانند برای تولید قدرت نرم از طریق تدوین دستورکار، جذب یا ترغیب به کار روند. برای نمونه، ترغیب جامعه برنامه‌نویسان برنامه‌های

متن باز (open source) برای اتخاذ یک استاندارد جدید مثالی از یک هدف نرم در داخل فضای سایبر است.

منابع سایبری همچنین می‌توانند در داخل فضای سایبر قدرت سخت تولید کنند. برای مثال، بازیگران دولتی یا غیردولتی می‌توانند با استفاده از "باتنت‌های" مرکب از صدها هزار کامپیوتر آلوده (یا بیشتر) یک حمله انکار سرویس توزیع شده را سازماندهی کنند، به طوریکه سامانه اینترنت یک شرکت یا کشور را زیر حمله گرفته و آن را از کار بیاندازد . سازمان دادن یک باتنت با نفوذ دادن یک ویروس به رایانه های بدون محافظ کار نسبتا ساده‌ای است و با چند صد دلار می‌توان به طور غیرقانونی باتنت‌ها را در اینترنت کرایه کرد. بعضی وقت‌ها تبهکاران با هدف اخاذی به این کار مبادرت می‌ورزند.

موارد دیگر می‌تواند "هکتیویست‌ها" را شامل شود. هکتیویست‌ها نفوذگرانی هستند که انگیزه‌های ایدئولوژیک دارند .برای مثال، هکرهای تایوانی و چینی مرتبا سایت‌های یکدیگر را هک می‌کنند. در سال ۲۰۰۷، استونی دچار یک حمله "انکار سرویس توزیع‌شده" شد. این حمله به "هکرهای میهن‌پرست" روسی نسبت داده شد که از برداشتن یادبود سربازان شوروی مربوط به جنگ جهانی دوم آزرده‌خاطر شده بودند. در سال ۲۰۰۸، درست کمی پیش از تهاجم نیروهای روس، گرجستان مورد یک حمله انکار سرویس قرار گرفت که دسترسی به اینترنت را از کار انداخت. (اگرچه دولت روسیه تکذیب می‌کند، ولی به نظر می‌رسد که در هر دو مورد دولت روسیه هکرها را تشویق به این کار کرده است.)

شکل‌های دیگر قدرت سخت در داخل فضای سایبر شامل جاسازی کدهای مخرب برای اخلال در سامانه ها یا سرقت دارایی‌های اطلاعاتی می‌شود. گروه‌های تبهکار این کار را برای سود انجام می‌دهند، و حکومت‌ها ممکن است آن را به عنوان راهی برای افزایش منابع اقتصادی خود انجام دهند .

اطلاعات سایبری همچنین می‌توانند در فضای سایبری گردش کنند تا به وسیله جذب شهروندان کشورهای دیگر قدرت نرم به وجود بیاورند. یک برنامه تبلیغات سیاسی در اینترنت مثالی برای این موضوع است .اما اطلاعات سایبری همچنین می‌توانند به یک منبع

قدرت سخت تبدیل شوند، که می‌تواند به اهداف فیزیکی در یک کشور دیگر صدمه وارد کند .برای مثال، بیشتر صنایع مدرن و خدمات دولتی فرایندهایی دارند که با رایانه های متصل به سامانه های کنترل نظارتی و جمع‌آوری داده‌ها (SCADA) پردازش می‌شوند. نرم‌افزار مخربی که به این سامانه ها وارد می‌شود، می‌تواند برای خاموش کردن فرایندی که آثار کاملا فیزیکی دارد برنامه‌ریزی شده باشد. برای مثال، اگر یک هکر یا یک حکومت برق یک شهر شمالی مانند شیکاگو یا مسکو را در وسط ماه فوریه (بهمن) قطع کند، خسارت وارده خیلی بیشتر از بمباران این شهرها خواهد بود. در برخی تاسیسات نظیر بیمارستان‌ها، مولدهای اضطراری می‌توانند در صورت قطعی برق اوضاع را به حالت اول برگردانند، اما بر آمدن از عهده خاموشی‌های گسترده‌ی منطقه‌ای مشکل‌تر خواهد بود.

همچنین ابزار فیزیکی می‌توانند منابعی از قدرت باشند که از طریق آن می‌شود دنیای سایبر را هدف قرار داد. برای نمونه، مسیریاب ها و کارگزارهای فیزیکی و کابل‌های فیبر نوری منتقل‌کننده الکترون‌های اینترنت، موقعیت‌های جغرافیایی در داخل قلمروهای حکومتی دارند و شرکت‌های گرداننده و استفاده کننده اینترنت تابع قوانین آن حکومت‌ها هستند . حکومت‌ها می‌توانند اجبار مادی بر شرکت‌ها و افراد اعمال کنند. پیگرد قانونی یاهو را وادار کرد آنچه را که به فرانسه می‌فرستد کنترل کند و گوگل مجبور شد ادبیات ضد یهود را از جستجوهای آلمان حذف کند .اگرچه در کشور محل این شرکت‌ها، یعنی آمریکا، "دفاع از آزادی بیان" شعار رایج بود، اما زندان، جریمه، و کوتاه کردن دست آن‌ها از این بازارهای مهم تاوانی بود که در صورت عدم برآوردن این خواسته‌ها باید بپردازند .حکومت‌ها از طریق تهدید فیزیکی واسطه‌هایی چونISP ها، مرورگرها، موتورهای جستجو و واسطه‌های مالی، رفتار را در اینترنت کنترل می‌کنند.

در رابطه با سرمایه‌گذاری در منابع فیزیکی به وجود آورنده قدرت نرم، باید گفت که حکومت‌ها می‌توانند با راه‌اندازی کارگزارها و نرم‌افزار ویژه به هم پیمانان در کشورهای مختلف کمک کنند ، پیام‌های خود را منتشر سازند.

نکته آخر اینکه، ابزارهای فیزیکی می‌توانند هر دو منبع قدرت سخت و نرم را فراهم نمایند که می‌توانند علیه اینترنت به کار روند. لایه اطلاعات سایبری بر روی یک زیرساخت

فیزیکی قرار دارد که در مقابل حمله مستقیم نظامی یا خرابکاری از سوی حکومت‌ها یا بازیگران غیردولتی نظیر جنایتکاران و تروریست‌ها آسیب‌پذیر است. کارگزارها می‌توانند منفجر شوند و کابل‌ها می‌توانند قطع گردند. و در حوزه قدرت نرم، بازیگران غیردولتی و NGOها می‌توانند با ترتیب دادن تظاهرات‌های فیزیکی، شرکت‌ها (و حکومت‌هایی) را که به زعم آن‌ها از اینترنت سوءاستفاده می‌کنند، رسوا نمایند. به عنوان مثال، در سال ۲۰۰۶ تظاهر کنندگان در واشنگتن علیه یاهو و شرکت‌های دیگری که اسامی فعالان چینی را ارائه کرده و به دستگیری آن‌ها از سوی دولت چین منتهی شده بودند، دست به راهپیمایی زدند.