مرکز پژوهش‌های مجلس شورای اسلامی
دفتر مطالعات حکمرانی
مسلسل: ۲۰۸۳۰ ■ تیر ۱۴۰۴

قدرت سایبری؛ ماهیت، ابعاد، مؤلفه‌ها و شاخص‌های جهانی


بسم الله الرحمن الرحيم

تاریخ انتشار:
۱۴۰۴/۴/۲۵

شماره مسلسل: ۲۰۸۳۰
کد موضوعی: ۳۵۰

مرکز پژوهش‌های مجلس شورای اسلامی

عنوان گزارش:
قدرت سایبری؛ ماهیت، ابعاد، مؤلفه‌ها و شاخص‌های جهانی

نوع گزارش: طرح ولایحه□ ، نظارتی□ ، راهبردی■ ، پیش‌نویس قانونی□

نام دفتر:
مطالعات حکمرانی (گروه بنیادین حکومتی)

تهیه و تدوین:
مهران مظفری‌نیا (دانشجوی دکتری فلسفه علوم اجتماعی دانشگاه باقرالعلوم(ع))

مدیر مطالعه:
توحید اسماعیل‌پور

اظهارنظرکنندگان:
طه اکرمی (دفتر مطالعات سیاسی)، عبدالرحیم قاسمی‌نژاد (دفتر مطالعات فرهنگی)

اظهارنظرکننده خارج از مرکز:
محمد راییجی (دکتری فلسفه علوم اجتماعی دانشگاه باقرالعلوم(علیه اسلام))

ناظر علمی:
مهدی عبدالحمید

گرافیک و صفحه آرایی:
سارا پیرولی
ساجده زارع مرزی

ویراستار ادبی:
شیوا امین اسکندری

واژه‌های کلیدی:
۱. قدرت سایبری
۲. عصر دیجیتال
۳. فضای سایبر
۴. قدرت ملی
۵. حکمرانی سایبری

تاریخ شروع مطالعه:
۱۴۰۲/۰۷/۰۱

دفتر مطالعات حکمرانی

فهرست مطالب

فهرست جداول

فهرست شکل‌ها

قدرت سایبری؛ ماهیت، ابعاد، مؤلفه‌ها و شاخص‌های جهانی

چکیده

«قدرت» از بنیادی‌ترین مفاهیم در اندیشه سیاسی از دوران باستان تا عصر مدرن است. فیلسوفان زیادی از افلاطون تا متفکران پست‌مدرن، با توجه به ساختار و زمینه‌های اجتماعی، سیاسی و فرهنگی به تبیین مفهوم «قدرت» پرداخته‌اند. در عصر حاضر، ظهور فضای سایبری و فناوری‌های دیجیتال، معماری جدیدی از قدرت را شکل داده که تحت عنوان «قدرت سایبری» شناخته می‌شود. این نوع قدرت، ترکیبی از عناصر نرم و سخت قدرت ملی است و به‌عنوان مهم‌ترین منابع قدرت در قرن بیست‌ویکم، نقشی تعیین‌کننده در معادلات جهانی ایفا می‌کند. قدرت سایبری نه‌تنها ابزارهای سنتی قدرت مانند دیپلماسی و نظامی‌گری را بازتعریف کرده، بلکه با ایجاد فرصت‌های جدید در حوزه‌های اطلاعاتی، اقتصادی و فرهنگی، امکان نقش‌آفرینی کشورهای جهان را گسترش داده است. هدف این نوشتار، تعمیق شناخت از ماهیت، ابعاد و ظرفیت‌های قدرت سایبری است تا با درک روشن‌تر از فرصت‌ها و چالش‌های آن، زمینه‌ای برای خط‌گذاری و برنامه‌ریزی ملی فراهم شود. این الگو به کشورها، به‌ویژه کشور ما، کمک می‌کند تا با بهره‌گیری از قدرت سایبری، امنیت ملی و جایگاه بین‌المللی خود را تقویت کنند. در گزارش‌های بعدی، به اقتضائات حکمرانی سایبری در ایران، شامل زیرساخت‌ها، سیاست‌های دفاعی و تهاجمی، و الزامات حقوقی و اخلاقی پرداخته خواهد شد تا چارچوبی جامع برای توسعه این قدرت ارائه شود.

خلاصه مدیریتی

بیان / شرح مسئله

از دوران باستان تا عصر کنونی، مفهوم «قدرت» همواره در کانون تفکر سیاسی قرار داشته و با پیدایش فضای سایبری و پیشرفت فناوری‌های دیجیتال، دستخوش دگرگونی عمیقی شده است. این تحول، گونه نوینی از قدرت را به نام «قدرت سایبری» معرفی کرده که دربرگیرنده ترکیبی از مؤلفه‌های سخت و نرم قدرت ملی است و به یکی از کلیدی‌ترین منابع قدرت در سده بیست‌ویکم بدل شده است. قدرت سایبری، با تأثیرگذاری گسترده بر حوزه‌های اقتصادی، نظامی، سیاسی، اجتماعی و فرهنگی، امکاناتی بی‌نظیر برای حضور فعال در صحنه جهانی، تقویت بنیان‌های امنیت ملی و ارتقای جایگاه بین‌المللی کشورها فراهم می‌آورد. بااین‌حال، نبود درک عمیق از ماهیت، اجزا و کنشگران این نوع قدرت می‌تواند به سیاستگذاری‌های ناکارآمد، از دست رفتن فرصت‌های استراتژیک و افزایش آسیب‌پذیری در برابر تهدیدهای سایبری منجر شود.

در ایران، با توجه به چالش‌های ناشی از تهدیدهای خارجی، فشارهای تحریمی و تأکید مقام معظم رهبری در سال ۱۳۹۴ بر لزوم دستیابی جمهوری اسلامی به جایگاه یک قدرت سایبری در جهان با رویکردی اخلاق‌محور و عدالت‌مدار، ضرورت تدوین یک چارچوب منسجم برای توسعه این قدرت بیش‌ازپیش آشکار است. این گزارش با هدف تعمیق فهم از مفهوم قدرت سایبری، تحلیل ابعاد، مؤلفه‌ها و شاخص‌های جهانی آن، و ارائه پیشنهادهای سیاستی، به دنبال پاسخگویی به این نیاز حیاتی است.

نقطه‌نظرات / یافته‌های کلیدی

ماهیت و ویژگی‌های قدرت سایبری

قدرت سایبری، توانایی استفاده از فضای سایبری برای ایجاد برتری و تأثیرگذاری بر محیط‌های عملیاتی (زمین، دریا، هوا و فضا) و ابزارهای قدرت (دیپلماسی، اطلاعات، نظامی و اقتصاد) است. این قدرت، به‌دلیل پراکندگی، هزینه کم ورود، ناشناس ماندن کنشگران و امکان تأثیرگذاری هم‌زمان در حوزه‌های مختلف، از قدرت سنتی متمایز است. جوزف نای قدرت سایبری را به دو دسته منابع (زیرساخت‌ها، شبکه‌ها، نرم‌افزارها و مهارت‌های انسانی) و رفتار (دستیابی به نتایج دلخواه از طریق منابع اطلاعاتی) تقسیم می‌کند. این قدرت می‌تواند به‌صورت سخت (مانند حملات سایبری) یا نرم (مانند دیپلماسی عمومی) اعمال شود.

ابعاد و لایه‌های قدرت سایبری

قدرت سایبری در دو بعد سخت (مانند تخریب زیرساخت‌ها) و نرم (مانند ترغیب و تنظیم دستور کار) عمل می‌کند. این قدرت در چهار لایه زیرساختی (سخت‌افزار و شبکه‌ها)، فیزیکی (دستگاه‌های کاربر مانند رایانه‌ها)، ساختاری (پروتکل‌ها و نرم‌افزارها) و معنایی (محتوا و تعاملات انسانی) سازمان‌دهی می‌شود. این لایه‌ها، از اجزای فیزیکی تا محتوای اطلاعاتی و تعاملات اجتماعی را دربرمی‌گیرد و امکان تحلیل جامع قدرت سایبری را فراهم می‌کند. لایه معنایی، با تأثیر بر فرهنگ و افکار عمومی، نقش کلیدی در دیپلماسی سایبری دارد.

بازیگران و اهرم‌های قدرت سایبری

بازیگران قدرت سایبری شامل دولت‌ها، شرکت‌های چندملیتی، گروه‌های هکری، سازمان‌های تروریستی و افراد هستند. ویژگی‌هایی مانند کم‌رنگ شدن محدودیت‌های جغرافیایی، هزینه کم فناوری و امکان ناشناس ماندن، تعداد و تنوع بازیگران را افزایش داده است. اهرم‌های اصلی قدرت سایبری شامل اقتصاد پیشرفته فناوری‌محور، همکاری دولت و بخش خصوصی، آژانس‌های اطلاعاتی خلاق و ارائه روایت جذاب از فضای سایبری است. آدام سگال تأکید می‌کند که اقتصادهای بزرگ با زیرساخت‌های پیشرفته، مانند آمریکا، برتری نسبی دارند، اما پیچیدگی فناوری نیز آسیب‌پذیری‌هایی ایجاد می‌کند.

اهمیت استراتژیک و شاخص‌های جهانی

قدرت سایبری با تقویت حوزه‌های سنتی قدرت (اقتصادی، نظامی، دیپلماتیک و اطلاعاتی)، نقش کلیدی در امنیت ملی و رقابت جهانی ایفا می‌کند. این قدرت امکان نظارت بر اطلاعات، مدیریت افکار عمومی، جاسوسی سایبری و تخریب زیرساخت‌های دشمن

را فراهم می‌سازد. شاخص‌های جهانی، مانند گزارش مرکز بلفر (۲۰۲۲)، شامل هشت هدف است: نظارت داخلی، دفاع سایبری، کنترل اطلاعات، جاسوسی خارجی، توسعه فناوری، تخریب زیرساخت دشمن، تعیین هنجارهای بین‌المللی و انباشت ثروت سایبری. ایران در این رتبه‌بندی در جایگاه دهم قرار دارد، اما به شاخص‌های بومی با تأکید بر وجوه فرهنگی و اخلاقی احساس نیاز می‌شود.

چالش‌ها و فرصت‌ها

قدرت سایبری فرصت‌هایی مانند کاهش هزینه‌های اعمال قدرت، افزایش نفوذ جهانی و توسعه اقتصادی را فراهم می‌کند، اما چالش‌هایی مانند جرائم سایبری، حملات زیرساختی و سلطه قدرت‌های بزرگ را نیز به همراه دارد. برای ایران، بهره‌گیری از این فرصت‌ها به توسعه زیرساخت‌های بومی، کاهش وابستگی به فناوری‌های خارجی و تقویت همکاری‌های بین‌المللی نیاز است.

پیشنهاد راهکارهای تقنینی، نظارتی یا سیاستی

تدوین استراتژی ملی قدرت سایبری

پیشنهاد می‌شود استراتژی ملی با تمرکز بر توسعه زیرساخت‌های بومی، تقویت توان تهاجمی و دفاعی و آموزش نیروی انسانی متخصص تدوین شود که هم‌راستا با اهداف کلان کشور باشد.

تقویت دیپلماسی سایبری

از نکات برجسته توسعه سایبری، توجه به سایبر دیپلماسی به‌عنوان ابزاری برای تأثیرگذاری بر افکار عمومی و روابط بین‌المللی است. لذا پیشنهاد می‌شود با مشارکت فعال در مجامع بین‌المللی و امضای پیمان‌های سایبری، ایران در تعیین هنجارهای جهانی نقش‌آفرینی کند و از رویکرد عادلانه و اخلاق‌مدار حمایت نماید.

حمایت از بخش خصوصی و کاهش وابستگی خارجی

با توجه به برتری شرکت‌های فناوری آمریکا به‌دلیل اقتصاد پیشرفته، پیشنهاد می‌شود سیاست‌هایی برای حمایت از شرکت‌های فناوری داخلی از طریق تسهیلات سرمایه‌گذاری و ایجاد بازارهای رقابتی اجرا شود تا وابستگی به فناوری‌های خارجی کاهش یابد.

ارتقای سواد سایبری عمومی

با توجه به نقش لایه معنایی و تأثیر آن بر افکار عمومی، پیشنهاد می‌شود برنامه‌های آموزشی همگانی برای افزایش آگاهی عمومی از تهدیدهای سایبری و تقویت فرهنگ امنیت سایبری در مدارس و رسانه‌ها اجرا شود.

طراحی شاخص‌های بومی قدرت سایبری

با توجه به کاستی‌های شاخص‌های جهانی مانند گزارش بلفر و نیاز به وجوه فرهنگی، پیشنهاد می‌شود شاخص‌های بومی با تأکید بر ارزش‌های اسلامی، فرهنگی و اخلاقی طراحی شود تا وضعیت قدرت سایبری ایران به‌صورت دقیق‌تر ارزیابی گردد.

قدرت سایبری، به‌عنوان مهم‌ترین ابزارهای قدرت ملی در قرن بیست‌ویکم، فرصت‌های بی‌نظیری برای ارتقای جایگاه جهانی، تقویت امنیت ملی و توسعه اقتصادی فراهم می‌کند. ایران، با توجه به ظرفیت‌های انسانی، جغرافیایی و فرهنگی خود می‌تواند به قدرتی تأثیرگذار در فضای سایبری تبدیل شود. طراحی استراتژی ملی با تأکید بر زیرساخت‌های بومی و دیپلماسی سایبری، از مهم‌ترین اقدام‌های پیشنهادی است. تأکید مقام معظم رهبری بر دستیابی به قدرت سایبری جهانی، مسئولیت سیاستگذاران را برای برنامه‌ریزی دقیق و بهره‌گیری از این ظرفیت مضاعف می‌کند.

۱. مقدمه

جامعه سرمایه‌داری از سقوط فئودالیسم تاکنون، ادوار و مراحل گوناگونی را پشت سر نهاده است. بعد از دوره‌ای که کشاورزی و استخراج مواد خام در اقتصاد، نقش مسلط را داشت، در مرحله نخست، شاهد گذار از سلطه کشاورزی به سلطه صنعت هستیم. در این مرحله که در قرن هفدهم میلادی به‌وقوع پیوست، صنعت و تولید کالاهای صنعتی نقشی مسلط و موقعیت ممتاز در اقتصاد دارد. تولید محصولات صنعتی و افزایش تیراژ آنها از اهداف حاکم بر جوامع آن روزگار بود. با تولید نیمه‌هادی‌ها و توسعه قلمرو دانش در حوزه فناوری اطلاعات بشر به سمت انقلابی جدید هدایت می‌شود و سرمایه‌داری از چیرگی صنعت هم عبور می‌کند و وارد دوره‌ای می‌شود که خدمات و اطلاعات در قلب نظام سرمایه‌داری و تولید اقتصادی جای می‌گیرد.[۱] در این مرحله که از آن به «عصر اطلاعات»[۲] تعبیر شده است، توسعه فناوری‌های ارتباطی و اطلاعاتی مانند رایانه، شبکه‌های متنوع محلی، جهانی و اینترنت باعث شده تا اطلاعات و داده‌ها، نقش و موقعیت ممتازی را که صنعت در اقتصاد داشت، کنار بزند و محور تولید اقتصادی قرار گیرد تا جایی‌که در فاصله کوتاهی از این عصر، آشنایی با برخی از تکنولوژی‌های ارتباطی مانند رایانه و مهارت استفاده از آن به‌شرط عمومی و اولیه کار در کشورهای فرادست تبدیل می‌شود [۱]. زمانی که با آمدن اینترنت و رایانه، به‌خصوص رایانه‌های شخصی، فضای تولید و انتشار اطلاعات و تولید دانش توسعه یافت و شکل جدیدی به خود گرفت تا به امروز، ما دهه‌هاست که در عصر اطلاعات زندگی می‌کنیم اما با رشد شتابنده فناوری‌های ارتباطی‌ـاطلاعاتی و تولید فزاینده داده‌ها از منابع مختلفی نظیر «شبکه‌های اجتماعی»، «تجارت الکترونیکی»، «اینترنت اشیا» و همچنین آمدن «هوش مصنوعی» و ظهور «پردازشگرهای کوانتومی»، دنیای تازه‌ای از این عصر به روی ما گشوده شد. این تغییرات که از آن به «انقلاب چهارم صنعتی» تعبیر می‌شود، باعث شد تا دگرگونی عظیمی در شیوه نگرش، فرماسیون و شیوه‌های زیست اجتماعی ما ایجاد شود.

گفته شده که در انقلاب صنعتی چهارم، یک شبکه جهانی درهم‌تنیده‌ای وجود خواهد داشت که در آن همه‌چیز به همه‌کس متصل می‌شود. مردم، دستگاه‌ها، منابع طبیعی، خطوط تولید صنعتی، شبکه‌های تهیه و توزیع محصول و خدمات، مزارع کشاورزی، مراکز تولید، انتقال و توزیع انرژی و درواقع همه جوانب زندگی اقتصادی و اجتماعی از طریق حسگرها و نرم‌افزارها به شبکه مجازی متصل می‌شود. جهانی ایجاد خواهد شد که مردم و همه‌چیز و ازجمله اشیای بی‌جان دارای هویتی دیجیتال در دنیای مجازی خواهند شد و چندین میلیارد بشر و شیء با همدیگر ارتباط خواهند داشت. این پایگاه و شبکه مجازی لحظه‌به‌لحظه کلان‌داده‌ها را به هر نقطه‌ای مانند مؤسسه‌های بازرگانی، منازل و وسایل نقلیه ارسال می‌کنند. در پی آن، کلان‌داده‌ها با دانش تجزیه و تحلیل پیشرفته پردازش می‌شوند. درحقیقت، جهان فیزیکی از طریق حسگرها و محرک‌هایی که در بطن اشیای فیزیکی قرار گرفته‌اند، از طریق شبکه‌های بی‌سیم یا باسیم، به یکدیگر متصل می‌شوند [۲]. طبیعتاً این تحولات که بخشی از آن رنگ واقعیت به خود گرفته، بافت اجتماعی زیست بشر را تغییر داده است. با تحول در فرماسیون یا وضعیت واقعی حیات بشر، مفاهیم اساسی سیاسی و اجتماعی او هم دستخوش تحول شده است. لذا با ورود جامعه سرمایه‌داری به عصر اطلاعات و دنیای دیجیتال، مفاهیم بنیادینی که بشر براساس آنها مناسبات جهانی و ارتباطات اجتماعی خود را شکل می‌داد، تغییر یافته است. یکی از آن مفاهیم و حوزه‌هایی که تحت تأثیر فناوری‌های اطلاعاتی دستخوش تحول شده و توانسته خود را در عرصه حیات اجتماعی با توجه به بافت و اقتضائات نوین جامعه شبکه‌ای، بازتولید نماید، «قدرت»[۳] است.

---

۱. البته عبور از هر دوره‌ای به‌معنای نفی نظام تولید اقتصادی پیشین نیست مثلاً زمانی که از مرحله کشاورزی به صنعتی می‌رویم، معنایش این نیست که کشاورزی از بین رفته است، بلکه وضعیت و نقش آن در نظام تولید اقتصادی تغییر می‌کند و از موقعیت سلطه به موقعیت تابعیت جابه‌جا و تابع مناسبات صنعتی در نظام جهانی می‌شود. در مرحله اطلاعاتی‌سازی هم این‌گونه نیست که تولیدات صنعتی متوقف شده است یا دیگر نقش مهمی در اقتصاد جهانی ندارد، بلکه منظور این است که انقلاب اطلاعاتی، مناسبات تولید صنعتی و فرایند تولید کارخانه‌ای را دستخوش دگرگونی کرده است.

2 .Information Age

3. Power

«قدرت»، کانونی‌ترین و بنیادی‌ترین مفهوم در اندیشه سیاسی از عصر باستان تا دوره جدید است. فیلسوفان زیادی به فراخور پایگاه اندیشگانی خود از افلاطون گرفته تا فیلسوفان پست‌مدرن، وابسته به ساختار و بافتی که قدرت در آن تعین یافته مفهوم‌پردازی کرده‌اند. این مفهوم‌پردازی‌ها چون تابع فرماسیون و ساخت اقتصادی یا اجتماعی متفاوتی، شکل گرفته‌اند، لذا بر مسائل و پرسش‌های متفاوتی متمرکزند. در عصر حاضر نیز با گذار از جامعه صنعتی و ظهور و رشد فوق‌العاده اطلاعات و فناوری‌های ارتباطی، شاهد این هستیم که فرماسیون اجتماعی و اقتصادی جامعه در حال دگرگونی است. لذا فهم متعارف و به تعبیر فوکو فهم انضباطی که از «قدرت» وجود داشته، با محیط عملیات جدیدی که یافته است، دگرگون شده و ما با «معماری جدیدی از قدرت مواجهیم که سودای فرارفتن از قلمرو فیزیکی را دارد» [۳]. این معماری جدید که امروزه خود را در سیمایی از قدرت به‌نام «قدرت سایبر»[1] نشان می‌دهد، که به‌دلیل رشد سریع فضای سایبر و ایجاد زمینه‌های جدید و مهم در سیاست، قدرت و حاکمیت در ابعاد ملی و جهانی، به‌عنوان یکی از مهم‌ترین منابع قدرت در قرن ۲۱ محسوب می‌شود. بازیگران دولتی و غیردولتی می‌توانند از این قدرت که نگاشتی از قدرت ملی با همه ابعاد و عناصر سخت و نرم آن است می‌توانند برای دستیابی به اهداف مالی، نظامی، سیاسی، ایدئولوژیک یا اجتماعی در فضای مجازی یا دنیای فیزیکی استفاده کنند [۴]. رهبر معظم انقلاب نیز با توجه به همین مسئله - و تأثیرات شگرف آن که هر روز در ابعاد فرهنگی، اجتماعی، اقتصادی، سیاسی، امنیتی و دفاعی در عرصه ملی و بین‌المللی نمود بیشتری پیدا می‌کند- در حکمی که سال ۱۳۹۴ در انتصاب اعضای شورای عالی فضای مجازی ابلاغ فرمودند بر ارتقای جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی و برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه، تأکید فرمودند.

بی‌تردید هرچه شناخت ما از این پدیده و تحلیل ماهیت و ابعاد آن که رسالت مهم نوشتار پیش‌رو هم هست، از عمق و غنای بیشتری برخوردار باشد، هم خودآگاهی ما در چگونگی مواجهه سلبی یا ایجابی با این پدیده را ارتقا خواهد داد و هم کمک خواهد کرد تا با تصویر روشن‌تری از امکان‌ها و فرصت‌هایی که این پدیده پیش‌روی ما - برای نقش‌آفرینی در ابعاد جهانی و ارتقای قدرت و امنیت ملی- قرار می‌دهد، به خط‌مشی‌گذاری و برنامه‌ریزی ملی برای توسعه آن ورود کنیم.

این گزارش از چند بخش تشکیل شده است: در بخش اول که «ایضاح مفهومی» است، ابتدا مفهوم قدرت و سیر تاریخی تطور آن به‌مثابه صورتی از نظم اجتماعی تا دوره حاضر مورد بررسی قرار می‌گیرد. در ادامه، چیستی فضای سایبر مورد مداقه قرار خواهد گرفت و سپس به بررسی مفهوم قدرت سایبر و تعاریف آن خواهیم پرداخت. بعد از ایضاح مفهومی، بررسی ابعاد مختلف آن اهمیت وافری می‌یابد که بخش دوم را به خود اختصاص می‌دهد. در این بخش به بررسی سیمای قدرت سایبر، ابعاد، لایه‌ها و بازیگران قدرت سایبری پرداخته می‌شود. در بخش سوم نیز اهرم‌های قدرت سایبری و مهم‌ترین شاخص‌های جهانی آن مرور خواهد شد. البته با توجه به گستردگی و اهمیت الگوهای راهبردی ارزیابی قدرت سایبری در حکمرانی فضای مجازی، این بخش به پژوهش مستقلی نیاز دارد که در گزارش بعدی به آن پرداخته خواهد شد. لذا در تحقیق حاضر صرفاً در حد مرور ادبیات به بیان مهم‌ترین شاخص‌ها اکتفا شده است.

1. Cyber Power

۲. پیشینه پژوهش

۲-۱. سوابق مطالعاتی در مرکز

جدول ۱. تحلیل پیشینه پژوهشی

ردیف	عنوان گزارش	سال انتشار	شماره مسلسل	نام دفتر/ سازمان/نهاد	توضیحات
۱	مفهوم قدرت هوشمند و نقش آن در سیاست جدید	۱۳۹۸	۱۶۶۸۴	مطالعات بنیادین حکومتی	این پژوهش از جهت موضوع مشابه تحقیق حاضر است. با این تفاوت که پژوهش حاضر تلاش کرده به ابعاد و لایه‌های بیشتری از تحلیل ماهیت متناسب با تحولات اخیر حوزه سایبر و همچنین شاخص‌های جهانی آن ورود کند.
۲	بررسی نقش فناوری در رقابت نظامی قدرت‌های بزرگ	۱۴۰۳	۲۰۰۰۲	مطالعات راهبردی	این پژوهش به بررسی نقش فناوری در رقابت نظامی قدرت‌های بزرگ می‌پردازد، لذا کمتر به تحولات ساختاری در مفهوم قدرت یا بازتعریف آن در بستر فضای سایبر توجه دارد. در مقابل، این پژوهش به دنبال تبیین شکل‌گیری نوع جدیدی از قدرت است که با ظهور فضای سایبر پدید آمده و از چارچوب‌های سنتی قدرت فراتر می‌رود. این تفاوت در رویکرد، پژوهش حاضر را به سمت تحلیل معماری جدید قدرت در عصر دیجیتال هدایت می‌کند، درحالی‌که پژوهش پیشین در محدوده تقویت ابزارهای نظامی باقی می‌ماند.

مأخذ: یافته‌های پژوهش.

۲-۲. سوابق تقنینی به همراه آسیب‌شناسی

جدول ۲. تحلیل پیشینه تقنینی

ردیف	نام سند (قانون... / تصویب‌نامه.../...)	مرجع تصویب	تاریخ تصویب	شماره ماده / صفحه	نکات برجسته / نقاط ضعف و قوت / پیامدهای اجرا
۱	قانون جرایم رایانه‌ای	مجلس شورای اسلامی	۱۳۸۸/۰۳/۰۵	ماده ۷۴۱	این قانون، یکی از مهم‌ترین اسناد تقنینی ایران در حوزه سایبر است. قانون جرایم رایانه‌ای به تعریف و جرم‌انگاری فعالیت‌های غیرقانونی در فضای سایبر، ازجمله هک، سرقت داده‌ها، جاسوسی سایبری، کلاهبرداری اینترنتی و نقض حریم خصوصی می‌پردازد. این قانون به‌عنوان اولین تلاش منسجم برای قانونگذاری در حوزه جرایم سایبری، پایه‌ای برای سایر مقررات و سیاست‌های بعدی فراهم کرد. مطالعه‌ای تطبیقی با قوانین کیفری آمریکا که نشان می‌دهد قانون جرایم رایانه‌ای ایران در زمینه‌هایی نظیر به‌روزرسانی همگام با فناوری‌های نوین و پوشش جامع تهدیدهای سایبری مانند تروریسم سایبری نیاز به غنای بیشتری دارد.

ردیف	نام سند (قانون... / تصویب‌نامه.../...)	مرجع تصویب	تاریخ تصویب	شماره ماده / صفحه	نکات برجسته / نقاط ضعف و قوت / پیامدهای اجرا
۲	سند امنیت فضای تولید و تبادل اطلاعات (افتا)	هیئت وزیران	۱۳۸۷		این سند را هیئت وزیران در سال ۱۳۸۷ تصویب کرد و به‌عنوان یکی از اسناد کلیدی برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی کشور شناخته می‌شود. سند افتا بر ایجاد چارچوب‌های امنیتی برای مدیریت و بهره‌برداری از زیرساخت‌های سایبری تأکید دارد و راهکارهایی برای پیشگیری از حملات سایبری ارائه می‌دهد.
۳	سند راهبردی پدافند سایبری	سازمان پدافند غیرعامل	۱۳۹۰		این سند توسط سازمان پدافند غیرعامل در سال ۱۳۹۰ تدوین شد و به‌طور خاص بر دفاع سایبری در برابر تهدیدهای خارجی و داخلی تمرکز دارد. این سند، فضای سایبر را به‌عنوان «عرصه پنجم جنگ» معرفی کرده و بر ضرورت مصون‌سازی زیرساخت‌های سایبری در برابر حملات تأکید دارد. این سند به‌ویژه در واکنش به حملات سایبری پیچیده مانند ویروس استاکس‌نت (۲۰۱۰) که تأسیسات هسته‌ای ایران را هدف قرار داد، تدوین شد و نشان‌دهنده توجه ایران به تهدیدهای سایبری با ماهیت نظامی و امنیتی است.
۴	سند نظام جامع فناوری اطلاعات	وزارت ارتباطات و فناوری اطلاعات	۱۳۸۶		این سند را وزارت ارتباطات و فناوری اطلاعات تدوین کرد و به‌عنوان چارچوبی برای توسعه زیرساخت‌های فناوری اطلاعات و امنیت سایبری در کشور عمل می‌کند. این سند بر ایجاد هماهنگی بین بخش‌های مختلف برای تقویت امنیت سایبری و توسعه فناوری‌های بومی تأکید دارد.
۵	امنیت سایبری	برنامه هفتم	۱۴۰۳		وزارت ارتباطات و فناوری اطلاعات مکلف شده است با هماهنگی و همکاری وزارت اطلاعات، سازمان اطلاعات سپاه، سازمان پدافند غیرعامل و بهره‌گیری از شرکت‌ها و مؤسسه‌های دارای پروانه یا گواهینامه ممیزی امن از سازمان فناوری اطلاعات ایران، نسبت به ارائه خدمات امن‌سازی، ارزیابی و رتبه‌بندی سالیانه امنیت سایبری دستگاه‌های اجرایی اقدام کند.

مأخذ: یافته‌های پژوهش.

۳. مفهوم‌شناسی

۳-۱. قدرت

۳-۱-۱. ماهیت قدرت

وقتی پای مفهوم قدرت به میان می‌آید، درمی‌یابیم که آشوبی تئوریک بر معنای این مفهوم حاکم است. درحالی‌که نمی‌شود به‌وجود خود این پدیده شک کرد، مفهومش تماماً مبهم است. برای عده‌ای قدرت یعنی سرکوب؛ برای عده‌ای دیگر، قدرت عنصری سازنده است برای ارتباط. قدرت گاهی با آزادی منطبق می‌شود، گاهی با اجبار. برای عده‌ای اساس قدرت کنش جمعی است، برای عده‌ای اساسش بر کشمکش بنا نهاده شده است. برخی به رابطه مشخص بین خشونت و قدرت قائل‌اند؛ و برای عده‌ای خشونت فقط شکل حداکثری از قدرت است [۳]. در مواجهه با یک چنین آشفتگی تئوریکی، ارائه مبنایی وحدت‌بخش که بتواند صورت‌بندی منسجمی

از تلقی‌هایی که گاهاً در نقطه مقابل یکدیگر قرار دارند ارائه دهد، کار مشکلی است. گویی در مواجهه با قدرتی قرار داریم که مدام سعی می‌کند بر این آشفتگی تئوریک بیفزاید. وقتی با چنین نیرویی مواجه هستیم باید به‌دنبال ایده‌ای باشیم که به‌طور نسبی قدرت بیشتری در انسجام‌بخشی و غلبه بر واگرایی‌های تئوریک موجود داشته باشد. به‌زعم نگارنده درمجموع آثاری که به بررسی مفهوم قدرت به‌عنوان یکی از مجادله‌برانگیزترین مفاهیم حوزه اندیشه سیاسی پرداخته‌اند با دو تلقی از آن مواجهیم؛ یک، «قدرت به‌مثابه امر سیاسی» و دو، «قدرت به‌مثابه امر ارتباطی». رویکرد اول که می‌توان آن را تلقی هابزی از قدرت نام نهاد، ناظر به آثاری است که با تکیه بر تلقی رایج از قدرت به بررسی این مفهوم پرداخته است. «اساساً بخش عمده بحث قدرت در اندیشه سیاسی غرب توسط دغدغه‌های وسیع‌تر در مورد هیئت سیاسی جامعه و شهروندانش جان می‌گیرد» [۵] در این تلقی، با شکلی غیردیالکتیکی از قدرت مواجهیم که در آن قدرت، سلسله‌مراتبی و از بالا به پایین اعمال می‌شود. قدرت در این معنا محدود به رابطه حاکم و رعیت یا بازتاب یافته در ساختارها و نهادهایی متمرکز و محدود نظیر دولت و احزاب است. جنس قدرت در این نگاه منفی و به‌عنوان یک پدیده در اختیار و متعلق به طبقه حاکم (دولت) است.

در گفتمان هابز، قدرت ابزاری در مالکیت دولت که آن را برای تحمیل نظم به جامعه مورد استفاده قرار می‌دهد. کارگزار قدرت در الگوی هابزی، دولت و ساخت سیاسی است. قدرت در اندیشه هابز با وجود ارائه دمکراتیک‌ترین نظریه مدرن یعنی قرارداد اجتماعی که در آن قدرت، منبعث شده از مردم بوده، و همین مردم قدرت را به دستگاه‌های دولتی و سیاسی تقدیم می‌کنند، ساختی سلسله‌مراتبی داشته و در آن قدرت از بالا بر مردم اعمال می‌شود [۶].

«هابز، فیلسوف انگلیسی و اولین نظریه‌پرداز قدرت دولت، ذات قدرت را حاکمیت دولت می‌دانست. هابز معتقد بود قدرت در بهترین و خالص‌ترین شکل از موقعیت منحصربه‌فرد حاکمیت اعمال می‌شود. او این حکومت را «لویاتان» می‌نامد» [۷].

گفتمان هابز در قدرت، سالیانی دراز با کمی تعدیل و تغییر به تأیید شخصیت‌های فکری بعدی درآمد. اما در میانه قرن بیستم و با آثار میشل فوکو شاهد چرخشی اساسی در این روایت از قدرت هستیم. لذا رویکرد دوم که می‌توان آن را تلقی فوکویی از قدرت نامید، ناظر به آثاری است که با تکیه بر یک تحول اساسی در فهم قدرت شکل گرفته است.

البته فوکو هرگز حقیقتِ قدرتِ دولت در معنای هابزی آن را انکار نکرد؛ اما فلسفه سیاسیِ او از شکاکیت او نسبت به این فرض سرچشمه می‌گیرد که تنها قدرت حقیقی، قدرت حاکمه است [۷]. فوکو نشان داد قدرت حاکمه لویاتان (مثلاً دادگاه، کنگره و سرمایه) چطور در طول دویست سال گذشته در مقابل دو شکل جدید از قدرت قرار گرفته است: «قدرت انضباطی» که او آن را به‌دلیل توجه مبسوط به تربیت بدن انسان، کالبد-سیاست و «زیست‌سیاست» نیز می‌نامید [۷].

در این رویکرد، نظام قدرت در جهان و جامعه مدرن بسیار ریشه‌دارتر و نامرئی‌تر و اغواکننده‌تر از قدرت در نظام سنتی است. در نظر فوکو، قدرت فراتر از مباحث دولت و حاکمیت، شامل گستره وسیعی است که همه سطوح را دربرمی‌گیرد. در این شکل، قدرت دیگر در جایی متمرکز نمی‌شود و این درست برخلاف نظر هابز است که در آن قدرت در ساختار دولت عینیت می‌یابد [۶]. کار قدرت، ساکن شدن در یکجا یا نابود کردن چیزی نیست. قدرت عمیقاً ریشه در شبکه روابط اجتماعی دارد و می‌توان آن را در تمامی عرصه‌های اجتماع و روابط انسانی مانند رابطه استاد و شاگرد، پزشک و بیمار حتی رابطه عاشقانه مورد ملاحظه قرار داد. ازاین‌رو نباید منشأ روابط قدرت را در نهادها جستجو کرد؛ زیرا باعث توضیح قدرت با قدرت می‌شود و روابط قدرت را صرفاً به‌صورت اشکال قانونی یا مبتنی بر اجبار آن محدود می‌کند [۸]. بنابراین فوکو قدرت را از نظریه‌ای در چارچوب دولت و حاکمیت به معنای هابزی آن دور کرده و با واژگون‌سازی بحث هابز و مدل لویاتانی قدرت، بجای تمرکز بر حاکمیت قدرت، بر بی‌شمار پیکری که در نتیجه تأثیرات قدرت به‌صورت سوژه‌های فرعی و حاشیه‌ای درآمده‌اند، تأکید دارد.

برخلاف رویکرد اول که قدرت را از منظر عاملیت بررسی می‌کند در این رویکرد تأکید اصلی بر پرسش از چگونگی اعمال قدرت است. لذا این پرسش که «قدرت چیست؟» بی‌وجه است. همان‌طور که دلوز در «تفاوت و تکرار» نشان می‌دهد که پرسشِ «چیست؟»، پرسش نادقیقی است که باید جای خود را به پرسش‌های قدرتمندتر دهند، مانند: چه‌قدر؟ چگونه؟ در کدام موارد؟ هگل در نظر دلوز اوج سنتی است که پرسش «چیست؟» را جدی می‌گرفت، حال‌آنکه فلسفه باید پرسش‌های عَرَض، رخداد، کثرت و تفاوت را در برابر پرسش‌های ذات، واحد، تضاد و تناقض جای دهد [۹]. این درست همان کاری است که فوکو در قبال قدرت در شکل عام و هر شکل

خاص قدرت، ازجمله «حکومت‌مندی» انجام می‌دهد. قدرت مجموعه‌ای از روندهاست و نه یک ذات متعال. قدرت ذاتی متعال و این همان ندارد و برخودش متکی نیست. قدرت یک ذات اسپینوزایی است، یک کثرت و نه یک ایده افلاطونی یا ذات ارسطویی [۱۰].
منابع و پژوهش‌هایی که با تکیه بر هر یک از این دو رویکرد سعی در مفهوم‌پردازی قدرت در فضای سایبر کرده‌اند زیاد نیست، هرچند به‌زعم نگارنده هیچ منبعی وجود ندارد که دقیق، جامع و مستوفا به بررسی چگونگی تأثیر اقتضائات اشکال نوین تکنولوژی‌های ارتباطی و اطلاعاتی بر مفهوم قدرت و شبکه موضوع‌ها و مفاهیم مرتبط با آن پرداخته باشد. بااین‌حال در ادامه به برخی منابع و پژوهش‌های صورت گرفته اشاره می‌شود:
دسته اول، منابعی است که با تلقی رایج از قدرت به بررسی تأثیرات انقلاب اطلاعاتی بر مفهوم قدرت در حوزه اندیشه سیاسی و روابط بین‌الملل پرداخته‌اند. برجسته‌ترین متفکری که با این رویکرد به تحلیل مفهوم قدرت پرداخته است، دانشمند و پژوهشگر سیاسی آمریکا؛ جوزف نای است. او در دو اثر «آینده قدرت» و «قدرت در عصر اطلاعات: از واقع‌گرایی تا جهانی شدن» تلاش کرده تا ضمن کندوکاوی در آینده قدرت آمریکا نشان دهد انقلاب نوین اطلاعاتی چه تأثیری بر ماهیت قدرت، منابع و مأموریت بازیگران دولتی و غیردولتی داشته است.
دسته دوم، منابعی است که با رویکرد اجتماعی به تحلیل ماهیت قدرت در عصر دیجیتال پرداخته‌اند. با توجه به غلبه نگاه‌های سیاسی به مفهوم قدرت، آثار کمی یافت می‌شود که با رویکرد اجتماعی به دگرگونی ماهیت قدرت در فضای سایبر و رژیم‌های نئولیبرال توجه کرده باشند. مهم‌ترین اثری که در این رویکرد وجود دارد کتاب «روان سیاست؛ نئولیبرالیسم و فناوری‌های جدید قدرت» نوشته بیونگ چول هان است. دغدغه اصلی هان به‌عنوان یک فیلسوف، روشن‌ساختن دگرگونی‌ها در تجربه سوبژکتیویته طی گذار از جامعه پساصنعتی به جامعه دیجیتال است.

۲-۱-۳. سیر تطور مفهوم «قدرت» به‌مثابه صورتی از نظم اجتماعی

ما با اشکال متفاوتی از قدرت و چگونگی اعمال آن مواجهیم. سرراست‌ترین و روشن‌ترین شکل اعمال قدرت، همانا «نفی آزادی» است. دارندگان این قدرت قادرند تا اراده خود را بر دیگری و درصورت نیاز با استفاده از خشونت اعمال کنند [۱۱] فوکو تبارشناسی خود را از قدرت با این شکل از قدرت[۱] آغاز می‌کند. اما قدرت، محدود به از بین بردن مقاومت و مجبور کردن به اطاعت نیست. قدرتی که مبتنی‌بر خشونت است، معرف برترین شکل قدرت نیست. این واقعیت که اراده دیگری بنا به میل دارنده قدرت تغییر کند، نشان‌دهنده ضعف این شکل از قدرت است. اما قدرت هرگز این‌گونه عمل نمی‌کند. قدرت هرچقدر بزرگ‌تر باشد، آرام‌تر و بی‌صداتر حرکت می‌کند. لذا صرفاً متکی به زور نیست، حتی موضعی ضدآزادی نیز اختیار نمی‌کند و بلکه از آزادی در راستای نیل به اهدافش بهره‌برداری می‌کند. صرفاً در شکل منفی اعمال قدرت است که قدرت خود را همچون خشونت «نه» گفتن برای شکستن اراده و از بین بردن آزادی نشان می‌دهد [۳].
بنابراین قدرت نیاز ندارد شکلی تحمیلی داشته باشد. اساساً اینکه مقاومت و اراده‌ای در مقابل صاحب قدرت، ایجاد می‌شود، نشان‌دهنده ضعف آن قدرت است. مناسبات میان ما و کودکمان گاه به‌گونه‌ای است که کودک داوطلبانه و از روی میل، خواسته ما که در راستای خیر و صلاح خودش هم هست را می‌پذیرد و حتی بالاتر خواسته ما را خواسته خودش هم می‌داند؛ اما گاه به‌گونه‌ای شکل گرفته که دائم با مقاومت او در پذیرش کارهایی که به او محول می‌شود، مواجهیم تا جایی‌که گاه پدر و مادر ناتوان از تحکم و تحمیل اراده خود بر او می‌شوند که شاهدی عیان بر ضعف قدرت آنهاست. بنابراین آن اشکالی از قدرت برتری دارند آنهایی که تحت انقیاد قدرت قرار دارند، آشکارا خواهان همانی باشند که صاحب قدرت می‌خواهد؛ چراکه گویی اراده صاحب قدرت، اراده خودشان است یا حتی انتظار رسیدن به آن اراده را دارند.
ریشه این نوع نگاه به قدرت که آن را ضرورتاً با خشونت و سلب هم‌نشین نمی‌سازد، رابطه درونی است که میان قدرت و آزادی وجود دارد. به تعبیر فوکو، قدرت صرفاً بر افراد آزاد، یعنی کسانی که در موضع انتخاب قرار دارند اعمال می‌شود، زیرا هدفش نفوذ بر گزینش‌های انسان و شکل دادن به اعمال اوست. ازاین‌رو، به‌نظر می‌رسد نمی‌توان رابطه ارباب و رعیت را رابطهٔ قدرت به‌معنای متقارن و کامل آن دانست، بلکه در اینجا نوعی رابطه اجبار جسمانی برقرار است که بیشتر با مفهوم سلطه سنخیت دارد [۸]. این

۱. قدرت معطوف به حکمرانی.

معنای قدرت که معطوف به زور و سلطه[1] است، قدرتی است که کارکرد اصلی آن سلب آزادی، نفی زندگی و تهدید به مرگ است که غالباً در جوامع پیشین به‌خصوص جوامع سلطنتی و فئودال نمود داشت.

اما از قرن هفدهم به این‌سو و گذار از عصر فئودالیسم به دوره صنعتی، قدرت، اقتدار خودش را، نه در توانایی خدای‌گونه بر مرگ و غلبه بر حیات، بلکه بسط هرچه بیشتر زندگی و انضباط و تولید به نمایش می‌گذارد و زندگی به ابژه‌ای برای قدرت بدل می‌شود. در این مقطع ما با یک جهش بزرگ تکنولوژیک قدرت مواجهیم به نام قدرت انضباطی[2] که به تعبیر فوکو کارکرد اولی، اساسی و دائمی این قدرت این است که مولد یک کارایی، محصول و بازدهی بهتر باشد. این قدرت فاقد عیوبی بود که نظام قدرت پیشین برای توسعه سرمایه‌داری نیاز داشت. نظام سرمایه‌داری از یک‌سو استقرار قدرتی پیوسته، دقیق و ذره‌ای را اقتضا می‌کرد تا بتواند فرایندهای اقتصادی و سازوکارهای گوناگون را در کنترل خود درآورد و ازطرفی پرهزینه نباشد. نظام قدرتی که سلطنت از پایان قرون وسطی به بعد موفق به سازماندهی‌اش شده بود، فاقد اینها، خلأمند و پرهزینه بود. لذا گذار از قدرتی خلأمند و بیش از اندازه پرهزینه به قدرتی پیوسته و کم‌هزینه صورت گرفت [۱۲]. این شکل از قدرت به دنبال این است که ناآشکارا و به‌صورت نامرئی با مجموعه‌ای از قوانین و قواعد، در همه اعضای بدنِ جامعه نفوذ کرده و با تأثیرگذاری بر حتی عادت‌های غیرارادی، بدن‌ها را تحت اشراف خود درآورد و امکان کج‌روی و رفتارهای خلاف قاعده را از بین برد. استعاره فوکو برای توضیح این فناوری، «زندان سراسربین بنتام» است؛ اما محدود به آن نبوده و در قالب‌های بسیاری نظیر خانواده، مدرسه، دانشگاه، کارخانه و ... بر زندگی انسان سیطره داشته است که نقطه اوج آن جوامع قرن بیستمی است که فرد مدام در حال عبور از محیطی بسته به محیط بسته دیگری است؛ نخست خانواده، سپس مدرسه، سپس سربازخانه، سپس کارخانه، هرازچندگاهی هم بیمارستان و احتمالاً زندان [۱۳] این فناوری (شیوه اعمال قدرت) اگرچه در سودای فرارفتن از قلمرو فیزیکی و به چنگ آوردن فضای ذهنی است، اما ازآنجاکه نظارتی بیرونی را اعمال می‌کند ناتوان از رسوخ به لایه‌های عمیق ذهن و دستیابی به روان و تفکرات درونی است [۱۱]. لذا به تعبیر استیگلر[3] نمی‌تواند برای درک جهان معاصر و نظام سرمایه‌داری جدید کاربرد داشته باشد که با انقلاب عظیم اطلاعاتی و ظهور تکنولوژی‌های نوین ارتباطی و اطلاعاتی نظیر پلتفرم‌ها و شبکه‌های اجتماعی چون اینستاگرام و فیسبوک، تمام محیط‌های حریم‌بندی شده مانند مدرسه، کارخانه و غیره را دستخوش بحران‌های فراگیری کرده است و سودای بازآفرینی رویکردهای استثماری و پسااستعماری خود از طریق دستکاری روان و میل انسان‌ها و بازتولید آن را دارد. لذا برنارد استیگلر برای اولین‌بار اصطلاح «روان سیاست» را به‌عنوان مفهومی جدید در برابر «زیست سیاست» برای درک جامعه فرافناوری شده معرفی می‌کند. او با بسط مفهوم قدرت زیستی فوکو، می‌کوشد شیوه جدیدی را که در آن قدرت در جامعه فرافناوری شده و اقتصاد بازار اعمال می‌شود را نشان دهد. استیگلر به پیامدهایی که جامعه فرافناوری شده برای آگاهی انسان دارد علاقه‌مند است و تلاش می‌کند راه‌هایی برای اصلاح افراط‌های جامعه سرمایه‌داری بیابد. او از روانقدرت به‌عنوان شکل جدیدی از کنترل صحبت می‌کند که از بیرون اعمال نمی‌شود. بلکه از طریق مکانیسم‌های روانی کار می‌کند که به ناخودآگاه نفوذ می‌کند و فرد را به یک مصرف‌کننده تبدیل می‌کند. ابزار اصلی اعمال قدرت در این جامعه، استفاده از فناوری است. درواقع در یک جامعه انضباطی (زیست‌سیاست) هدف اصلی به‌دست آوردن و تولید کالاهای اساسی برای بقا بود و کنترل از طریق انضباط به سمت افزایش تولید هدایت میشد. هدف اصلی در جامعه روان‌سیاست افزایش فروش است و راه رسیدن به آن بازاریابی و رسانه‌های جمعی است. این به معنای اعمال قدرت از طریق مکانیسم میل است که به تحریک بیش از حد میل منجر می‌شود [۱۴]. عرصه و چگونگی اعمال قدرت در چنین نظامی که بر شیوه‌های تولید غیرمادی و غیرفیزیکی استوار است، بدن اجتماعی و بهنجارسازی افراد نابهنجار از طریق ایجاد محیط‌های حبسی نظیر زندان، کارخانه یا مدرسه نیست، بلکه روان و ذهن انسان‌هاست که استثمار می‌شود. به‌نحوی‌که دیگر سوژه‌ها به تشخیص استثمارشدگی قادر نیستند و حتی مهم‌تر از این خود را استثمار می‌کنند. به عقیده هان[4] این قدرت متکی بر ظرافت، انعطاف‌پذیری و هوشمندی است. لذا کل میدان سلطه به‌طور کامل پنهان است. درنتیجه سوژه از انقیاد خودآگاه نیست و تصور می‌کند که آزاد و رها است. این قدرت در جستجوی انگیزش‌های مثبت و استثمار آنهاست؛

1. Power of Sovereignty
2. Disciplinary Power
3. Stiegler
4. Han

لذا با اغواگری، اراده سوژه را به سود خود هدایت می‌کند. این قدرت تحمیل‌کننده سکوت نیست، در عوض ما را به اعتماد کردن، اشتراک‌گذاشتن و مشارکت فرامی‌خواند. این قدرت انرژی خود را از خودکنترلی و خودبهینه‌سازی داوطلبانه اخذ می‌کند درنتیجه اصرار بر غلبه یافتن ندارد[۱۱].

۲-۳. فضای سایبر[1]

جدیدترین و درعین‌حال پرچالش‌ترین حوزه‌ای است که بشر در طول حیات خود با آن مواجه بوده، شاید «فضای سایبر» باشد. زمانی که کامپیوترهای اولیه در آمریکا اختراع شدند، کمتر کسی فکر می‌کرد انقلاب اطلاعاتی و داده‌ایِ ناشی از این امکان جدید، می‌تواند تبعات و آثار پیچیده‌تری نیز در اختیار بشر قرار دهد. رایانه‌ها - قبل از ورود به حوزه شبکه - دستگاه‌های پردازشگری بودند که دورنمای سرعت و دقت را برای شرکت‌ها و نهادهای دولتی و غیردولتی فراهم کرده بودند. اما زمانی که این پردازشگرها برای اولین‌بار به‌صورت شبکه‌ای در یکی از اتاق‌های وزارت دفاع آمریکا درآمدند، اولین نطفه‌های فضای سایبر را نیز بنا نهادند. هرچند به لحاظ تاریخی برای اولین بار مفهوم «فضای سایبر» توسط «ویلیام گیبسون» نویسنده داستان‌های علمی تخیلی در سال ۱۹۸۶ ارائه شد [۱۵].

اما برای توضیح چیستی و ماهیت پدیده‌ای که امروزه با عناوینی چون «فضای سایبر» یا «فضای مجازی» از آن یاد می‌کنیم، تعاریف و توصیفات متعدد و متنوعی ازسوی صاحب‌نظران و محققان ارائه شده است که در هریک از آنها بر یک یا چند جنبه از جنبه‌ها و ویژگی‌های متنوع این پدیده تأکید و توجه بیشتری شده است. لذا به‌اختصار و جهت نشان دادن تنوع دیدگاه‌ها در تعاریف به برخی از آنها اشاره می‌شود. برخی از تعاریف، تعاریف «فناورانه» است. در این تعاریف به مؤلفه‌ها و عناصری چون کامپیوتر، شبکه‌های ارتباطی و جنبه‌های فناورانه این پدیده بیشتر توجه شده و نسبت به سایر جنبه‌ها بی‌توجهی یا کم‌توجهی شده است؛ مانند تعریفی که از فضای مجازی در دایره‌المعارف هریتیج (Heritage) یا لغت‌نامه دانشگاه پرینستون (Princeton University) ارائه شده و از آن تعبیر به رسانه الکترونیکی یا شبکه‌های کامپیوتری شده است. در برخی دیگر از تعاریف علاوه بر وجوه فناورانه، به وجوه کارکردیِ آن نسبت به اطلاعات هم توجه شده است.

دسته دیگر، تعاریفی است که به ارتباطات میان انسان‌ها و فضای جدید تعاملی و ارتباطاتی اشاره شده است که میان افراد و جوامع شکل می‌گیرد که گاه با تعابیر «دنیای موازی» و «جهان جدید» هم از آن یاد شده است. در این تعاریف کمتر به وجوه فناورانه آن اشاره شده، بلکه برعکس تأثیر و جایگاه عامل‌های انسانی و روابط اجتماعی در قوام و کیفیت آن مورد تصریح واقع شده است. مانند تعریفی که بل[2] از فضای مجازی ارائه می‌دهد. او بیان می‌کند که فضای مجازی «یک دنیای موازی است که با خطوط ارتباطی و کامپیوترهای جهان خلق و نگهداری می‌شود. دنیایی که در آن تردد جهانی دانش، سنجش‌ها و سرگرمی‌ها شکل می‌گیرد. محیطی است که از طریق فناوری اطلاعات و ارتباطات ساخته شده است و در آن مردم قادرند تا با یکدیگر در ارتباط باشند و فعالیت‌هایی انجام دهند» [۱۶]؛ یا تعریفی که در مقاله «قدرت بازدارندگی در فضای سایبر» از بندیکت (۱۹۹۲) و لتو ارائه شده است. بندیکت معتقد است «[فضای مجازی] یک جهان جدید و موازی با دنیای روزمره بشر است، که با کامپیوتر و خطوط ارتباطی جهانی ایجاد شده است [۱۵]. لتو نیز معتقد است: «فضای سایبر یک اکوسیستم ساخته بشری است و برخلاف فضاهای دیگر مانند زمین، هوا یا دریا، به فعالیت‌ها و حضور متداوم انسان نیاز دارد. لتو می‌گوید فضای سایبر نه‌تنها شامل اطلاعات ذخیره شده، سیستم‌های نرم‌افزاری و دنیاهای مصنوعی است، بلکه نیازمند حضور فعال انسان، فرهنگ، ارتباطات و معنا نیز هست؛ یعنی فضای سایبر بدون حضور فعال و تعاملات انسانی که به انتقال فرهنگ و معنا منجر می‌شود، تنها داده‌های بی‌جانی خواهد بود و کاربردی ندارد». «محیط‌های تعاملی»، تعبیر دیگری است که ذیل همین دسته از تعاریف برای فضای مجازی به‌کار رفته است. باری[3] فضای مجازی را این‌گونه تعریف می‌کند: «فضای سایبر به‌معنای مجموعه کاملی از محیط‌های تعاملی است که شبکه‌های رایانه‌ای به‌طور عام و اینترنت به‌طور خاص، آن را به وجود آورده‌اند» [۱۷]

1. Cyber Space
2. Bell
3. Barry

بندیکت (۱۹۹۲) تعریف دیگری نیز از این فضا ارائه می‌کند او فضای سایبر را مکانی بدون محدودیت می‌داند که همزمان افرادی از زیرزمین خود در ونکوور کانادا، از یک قایق در پرتو پرنس، 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 [۱۵].
در برخی دیگر از تعاریف که بیشتر در اسناد و اظهارات مربوط به اندیشمندان امنیت ملی آمریکا مشاهده می‌شود تعبیر قلمروی عملیاتی و محیط اطلاعاتی نیز به تعابیر فوق افزوده می‌شود و اساساً فضای مجازی با رویکردی عملیاتی و به تعبیری دیگر رویکردی مبتنی‌بر تصور فضای تقابلی و جنگ در نظام جهانی تعریف می‌شود. مانند تعریفی که جوزف نای و کوئل ارائه می‌دهند:
«[فضای سایبر]، حوزه‌ای عملیاتی است با هدف بهره‌برداری از اطلاعات از طریق سیستم‌های به هم پیوسته که زیرساخت آنها، با استفاده از علم الکترونیک تأمین می‌شود».
«[فضای سایبر] قلمروی جهانی درون محیط اطلاعاتی است که خصوصیت برجسته و منحصربه‌فرد آن براساس استفاده از الکترونیک و طیف الکترومغناطیسی برای خلق، ذخیره، اصلاح، تبادل و بهره‌برداری از اطلاعات با استفاده از شبکه‌های وابسته و به هم پیوسته‌ای که از فناوری‌های اطلاعاتی و ارتباطاتی استفاده می‌کنند، شکل می‌گیرد.»
گروهی دیگر از تعاریف وجود دارد که در آنها بر «فضا» و عناوینی چون «فضای داده»، «فضای دیجیتال»، «فضای اطلاعات»، «فضای الکترونیک» و «فضای شبکه‌ای» تکیه شده است. اصطلاح فضای داده برای نخستین‌بار آلون هالوی؛ رئیس بخش تحقیقاتی مدیریت داده در گوگل در سال ۲۰۰۵ به‌کار برد که وی از این مفهوم به‌عنوان «استعاره‌ای برای مدیریت جدید داده‌ها» استفاده کرد که «پایگاه‌های داده‌های پراکنده را به هم متصل می‌ساخت». گروهی از محققان مانند کالانزیس‌کوپ و قراب‌مارتین از عنوان «فضای دیجیتال» برای نامیدن فضای مجازی استفاده می‌کنند و معتقدند که دیجیتال است که فضاهای اجتماعی را می‌سازد و آن را تنظیم مجدد می‌کند. دیجیتالی شدن یکی از پایه‌های اصلی تحولات رایانه‌ای و ارتباطی در عصر حاضر بوده و این امکان را فراهم کرده است که دستگاه‌های رایانه‌ای با انواع کاربردهای متفاوت امکان برقراری ارتباط با یکدیگر را داشته باشند. در فضای دیجیتالی، «وجود دیجیتال عددی» در مقابل «وجود آنالوگ شیئی» قرار می‌گیرد و صحبت از فضایی می‌شود که تابع جهان محاسبات و قاعده‌های ریاضی است و از انعطاف جهان ریاضی برخوردار است. بر این اساس، تغییر در این فضا نیز «جنس نرم‌افزار» است.
«فضای الکترونیکی» از دیگر اصطلاحاتی که برخی از محققان از آن نام برده‌اند. برای مثال لی (۲۰۰۰) معتقد است که ظهور فضای الکترونیکی تا اندازه زیادی پیچیدگی جغرافیایی جامعه و اقتصاد ما را افزایش داده است. «فضای اطلاعات» و «فضای شبکه‌ای» از دیگر عناوینی است که برای نامیدن فضای مجازی وجود دارد. افرادی مانند اکدیجی (۲۰۰۴)، از تعبیر «فضای اطلاعات» استفاده کرده‌اند. در این رویکرد، این باور وجود دارد که اطلاعات به‌عنوان ویژگی تعیین‌کننده جهان مدرن محسوب می‌شود و گفته می‌شود که «زندگی اجتماعی، اطلاعاتی شده است» و ما «وارد عصر اطلاعات شده‌ایم» که حالت جدیدی از نفوذ اطلاعات است [۱۸]. در «فضای شبکه‌ای» بر بعد شبکه‌ای این فضا تأکید می‌شود، آن هم به این دلیل که فرایند شبکه‌ای شدن تعاملات صورت گرفته و شبکه‌ها نه‌تنها در سطح کلان جامعه، بلکه در سطح فردی نیز مسلط شده‌اند. درواقع فضای شبکه‌ای، به‌طور فزاینده روابط خود را در شبکه‌های رسانه‌ای سازمان می‌دهد و تمامی افراد، گروه‌ها و سازمان‌ها را به هم متصل می‌کند.
با تمام این تعاریف و اوصاف، چنین می‌توان نتیجه گرفت که فضای سایبر، جهانی ناشناخته و موازی جهان موجود است که با تکیه بر اطلاعات و داده که از طریق شبکه‌های اینترنتی به هم متصل می‌گردند، الگوی ارتباطی جدیدی را به بشر ارائه می‌دهد که برخلاف محیط روزمره زندگی انسان که سرشار از واقعیت‌هاست، به‌صورت مجازی تبادل را امکان‌پذیر می‌سازد. درحقیقت هر جا[1] بودن و هیچ‌جا[2] نبودن با فضای مجازی تحقق پیدا می‌کند [۱۹]. لذا امکان بازیگری جدید را برای تمام بشریت ایجاد می‌کند؛ از کودکان خردسال گرفته تا سازمان‌ها و شرکت‌های چندملیتی و نیز دولت‌های قدرتمند. محدودیت‌های دنیای فیزیکی را از بین می‌برد، ایده‌ها را گسترش می‌دهد، جغرافیا را از بین می‌برد و انسان را از فاعل بودن در محیط اجتماعی، به سوژگی در محیط مجازی سوق می‌دهد. کنترل‌پذیری را بی‌معنا می‌سازد و دولت را به‌عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و غیره خلع سلاح می‌کند.

1. Everywhere
2. Nowhere

۳-۳. قدرت سایبری

امروزه با توجه به اینکه فضای سایبری به بخشی جدایی‌ناپذیر از زندگی ما انسان‌ها تبدیل شده است، تأثیر بسزایی در ابعاد اساسی حیات ما یعنی امنیت و اقتصاد یافته است. لذا باعث شده تا بسیاری از کشورها، قدرت سایبری را امری در اِعداد قدرت ملی تلقی کرده و به‌عنوان یکی از عوامل مهم و حیاتی در پی ارتقای شاخص‌های آن در این فضا باشند. تدوین سند استراتژی سایبری ملی آمریکا، محصول این نگاه به قدرت سایبری در جهت افزایش امنیت و پایداری اطلاعات کشور و سیستم‌های اطلاعاتی آمریکا در مواجهه با خطرات و حملات و جرائم سایبری و همچنین جاه‌طلبی‌های آمریکا برای شکل دادن به فضای سایبری جهانی در آینده است. «دفاع از زیرساخت‌های حیاتی»، «مختل کردن و از بین بردن عوامل تهدید»، «شکل دادن به نیروهای بازار برای ایجاد امنیت و انعطاف‌پذیری»، «سرمایه‌گذاری برای آینده مقاوم و پایدار» و «مشارکت‌های بین‌المللی برای دنبال کردن اهداف مشترک»، پنج رکن اساسی سازمان‌دهی استراتژی سایبری است که حاکی از اهمیت امنیت سایبری برای آمریکا است.

این مقوله در کشور ما نیز که همواره با تهدیدها و تحریم‌های خارجی مواجه است از اهمیت بسزایی برخوردار است. مقام معظم رهبری نیز در بند سوم از حکم اعضای دور دوم شورای عالی فضای مجازی، در شهریورماه ۱۳۹۴ با اشاره به «ارتقای جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی» به‌طور صریح بر قدرت سایبری تأکید فرموده‌اند.

۱-۳-۳. پارادایم‌های اصلی در نسبت میان تکنولوژی اطلاعات و سیاست

سیاستمداران، اندیشمندان، دولت‌ها و بازیگران بین‌المللی هرکدام به‌صورت ناخودآگاه دارای پیش‌فرض‌ها و منطق‌های آشکار و پنهانی نسبت به تکنولوژی، حوزه سایبر و مفاهیم و موضوع‌های مرتبط با آن هستند که اغلب دارای نظم و ساختاری نااندیشیده است؛ اما بر تلقی یا توضیحی که از یک مفهوم یا پدیده می‌دهند تأثیر مستقیم دارد. ازجمله آن مفاهیم حوزه سایبری، «قدرت سایبری» است که نوعی قدرت نوظهور برآمده از فضای سایبر است که با فراگیر شدن فناوری اطلاعات و ارتباطات به‌وجود آمده است. لذا شایسته است پیش از ایضاح مفهومی آن و ورود به تعاریف مشهوری که از این مفهوم شده است، منطق و پارادایمی که به نوعی خاستگاه و پایگاه فکری طرح آن است، شناخته شود و آن پارادایمی است که رابطه «تکنولوژی اطلاعات» و «سیاست» را توضیح می‌دهد.

در این خصوص و مفاهیم مرتبط با آن به‌نظر می‌رسد که با سه پارادایم اصلی مواجهیم که هرکدام مبنا، روش و رویکردهای درونی متفاوتی دارد.

جدول ۳. پارادایم‌های اصلی در نسبت میان تکنولوژی اطلاعات و سیاست

پارادایم اول	پارادایم دوم	پارادایم سوم
نگاه انتقادی رادیکال و بدبینانه‌ای به عصر اطلاعات دارند. طرفداران این پارادایم معتقدند انسان، هیچ‌گاه آزادی و دمکراسی را تجربه نخواهد کرد.	نگاهی اعتدالی و میانه به رابطه تکنولوژی اطلاعات و سیاست دارند.	نگاه خوشبینانه‌ای به رابطه تکنولوژی اطلاعات و سیاست دارند. اغلب افرادی که در این پارادایم قرار می‌گیرند، معتقدند اینترنت، شبکه‌های اجتماعی، هوش مصنوعی و ... همانند تمام دستاوردهای تکنیکی و اختراعات بشر، روزگار بهتر و آینده‌ای رو به آزادی و آگاهی برای بشر در پیش خواهند داشت.

مأخذ: یافته‌های پژوهش.

پارادایم نخست، پارادایمی است که در عین اینکه عصر اطلاعات را انکار نمی‌کند، نگاه انتقادی رادیکالی به آن دارد. طرفداران این پارادایم معتقدند انسان، هیچ‌گاه آزادی و دمکراسی را تجربه نخواهد کرد. به اعتقاد بسیاری از متفکران انتقادی رادیکال، نه جنگ حذف و نه سلطه نابود می‌شود. «رژیم‌های کنترلی»، «رژیم‌های انضباطی»، «امپریالیسم سایبر» و «شبیه‌سازی اطلاعاتی»، مفاهیم و رویکردهای بسیار بدبینانه و استبدادی در رابطه تکنولوژی اطلاعات و سیاست را در این پارادایم نشان می‌دهد [۲۰].

در پارادایم دوم، وجه اعتدال بیشتری وجود دارد. اعتدال در میانه ایستادن دعواهای پوزیتیویست‌ها و پسامدرن‌ها و اعتدال در میانه ایستادن آنان که بسیار خوش‌بین به عصر اطلاعات‌اند، با آنان که نگاهی به شدت بدبین دارند. آرا و عقاید متفکرانی چون هابرماس، فوکویاما، کین، کوهن، آرنت در این دسته جای می‌گیرد [۲۰].

پارادایم سوم، نگاه خوشبینانه‌ای به رابطه تکنولوژی اطلاعات و سیاست دارد. اغلب افرادی که در این پارادایم قرار می‌گیرند، معتقدند اینترنت، شبکه‌های اجتماعی، هوش مصنوعی و غیره همانند تمام دستاوردهای تکنیکی و اختراعات بشر، روزگار بهتر و آینده‌ای رو به آزادی و آگاهی برای بشر در پیش خواهند داشت. رسانه‌های الکترونیکی و تعاملی نوین، مانند شبکه‌های جهانی اینترنت و دیگر تکنولوژی‌های فضای سایبری می‌توانند به‌نحو ساختاری و اعجاب‌انگیزی زنده‌کننده دمکراسی، جامعه مدنی و تفکر انتقادی برای دفاع از انسانیت باشند [۲۰]. از پیشاهنگان و متفکران سنتی این پارادایم می‌توان به الوین تافلر، دانیل بل، آنتونی گیدنز و دیوید هلد اشاره کرد.

البته نگاه خوش‌بینانه تافلر یا کسانی مانند گیدنز، دانیل بل یا هلد که به نوعی متفکران کلاسیک این نوع نگاه هستند، هنوز وارد دوران جدید اطلاعاتی نشده و نگرش آنها به رابطه تکنولوژی اطلاعات و سیاست در ابزارها و وسایل پیش از دنیای کامپیوتر و اینترنت سیر می‌کند. از کلیدواژه‌های این رویکرد پیرامون سودمندی‌ها و فرصت‌های تکنولوژی اطلاعات و سیاست می‌توان به «امنیت اطلاعاتی»، «جنگ اطلاعاتی»، «دولت الکترونیک» و «حکمرانی خوب» اشاره کرد. این مفاهیم کلیدواژه‌هایی هستند که درنتیجه نگاه مثبت و خوشبینانه به رابطه تکنولوژی اطلاعات و سیاست پدید آمده‌اند. مانند اینکه از سال ۱۹۹۰ با پدید آمدن فضای جدید در عصر اطلاعات است که تفکیک میان مدیریت عمومی و خط‌مشی‌گذاری ازیک‌سو و سیاستگذاری و حکمرانی ازسوی‌دیگر ایجاد می‌شود و الگوی حکمرانی خوب جای الگوی مدیریت دولتی نوین را می‌گیرد [۲۰]. لذا دولت کوچک می‌شود و تنها به سازوکارهای کنترلی، نظارتی و تنظیمی می‌پردازد. از دیگر کلیدواژه‌های اصلی آشکارشدگی نگاه خوشبینانه به رابطه سیاست و اطلاعات، «امنیت اطلاعاتی» و «قدرت سایبری» است. حقیقت این است که فضای مجازی مشابه مواردی که پیش از این اشاره شد، ماهیت قدرت و جریان نظم‌دهنده و کنترلی جامعه را به‌ویژه برای دولت ملت‌ها را تغییر داده است. در سبک سنتی قدرت، عموماً دولت‌ها و نیروهای رسمی انحصار قدرت را در دست داشتند و از طریق سازمان‌های بسیار بوروکراتیزه شده، به اعمال آن برای کشورداری و تنظیم روابط بین‌الملل می‌پرداختند اما با شکل دیگری از قدرت مواجهیم که پیدایش تغییراتی در آن و امکان‌های جدیدی که یافته است، باعث شده ماهیت سنتی خود را از دست دهد. بازیگران جدید شکل گرفته‌اند و موضوع‌های جدیدی مانند امنیت سایبری، حاکمیت سایبری و کنترل و نظارت سایبری پدید آمده است.

۲-۳-۳. تعریف قدرت سایبری

با ذکر این مقدمه از زمینه پارادایمیک طرح قدرت سایبری، برای توضیح چیستی و واقعیت این پدیده، به تعاریف و توصیفات متعددی می‌پردازیم که ازسوی صاحب‌نظران و محققان ارائه شده است. در هریک از این تعاریف بر یک یا چند جنبه از جنبه‌ها و ویژگی‌های متنوع این پدیده تأکید و توجه بیشتری شده است. البته تعاریف ارائه شده از این پدیده بیشتر در اسناد و اظهارات مربوط به اندیشمندان حوزه امنیت ملی آمریکا مشاهده می‌شود که اساساً فضای مجازی و قدرت سایبری را با رویکردی عملیاتی و مبتنی‌بر محیط‌های عملیاتی و تصور فضای تقابلی و جنگ در نظام جهانی تعریف می‌کنند.

کوئل[1] قدرت سایبری را این‌گونه تعریف می‌کند: «قدرت سایبری، توانایی استفاده از فضای سایبری برای ایجاد برتری و تأثیرگذاری بر همه محیط‌های عملیاتی و همه ابزارهای قدرت است». محیط‌های عملیاتی در تعریف کوئل با پنج حوزه قدرت «زمین»، «دریا»، «هوا»، «فضا» و «فضای مجازی» و ابزار قدرت با چهار بعد قدرت «دیپلماسی»، «اطلاعات»، «نظامی» و «اقتصاد» انطباق دارد.

1. Daniel T. Kuehl

شلدون[1]؛ استاد سابق مطالعات راهبردی فضای سایبری دانشکده مطالعات هوایی و فضایی پیشرفته نیروی هوایی آمریکا، قدرت سایبری را «ابزار مکمل برای قدرت ملی» می‌داند که می‌تواند برای استفاده دولت‌مردان یک کشور جذاب باشد [۲۱]. او به ویژگی‌هایی برای قدرت سایبری اشاره می‌کند که آن را از قدرت در معنای سنتی خود متمایز می‌سازد. البته او بیان می‌کند که دیگر نظریه‌پردازان ممکن است ویژگی‌های بیشتری از آنچه در اینجا از قدرت سایبری توضیح داده شد را شناسایی کنند، اما معتقد است اینها برجسته‌ترین ویژگی‌هاست.

او معتقد است «قدرت سایبری همه‌جا حاضر است»[2] و به‌طور مطلق و هم‌زمان در همه حوزه‌ها اثر استراتژیک ایجاد می‌کند. «نیروی زمین، دریا، هوا و فضا به ایجاد اثر استراتژیک بر هریک از حوزه‌های دیگر قادر هستند، اما هیچ‌چیز به اندازه قدرت سایبری به‌طور مطلق و هم‌زمان در همه حوزه‌ها اثر استراتژیک ایجاد نمی‌کند. با توجه به وابستگی‌های سایبری ارتش، اقتصاد و جامعه در تعداد زیادی از کشورها، و با توجه به اینکه فضای سایبری به‌طور اساسی قدرت زمین، دریا، هوا و فضا و همچنین ابزارهای دیگر قدرت، مانند دیپلماسی، رسانه‌ها و تجارت را امکان‌پذیر می‌کند، می‌توان گفت که قدرت سایبری در همه‌جا وجود دارد».

ویژگی دومی که برای قدرت سایبری بیان می‌کند این است که: «قدرت سایبری برخلاف نیروی زمینی، دریایی و هوایی، اما از بسیاری جهات مانند نیروی فضایی، یک ابزار مکمل است».[3] او به منازعه روسیه و استونی و همچنین جنگ روسیه و گرجستان اشاره می‌کند و بیان می‌کند که حملات سایبری روسیه، تنها عامل تعیین‌کننده این جنگ‌ها نبوده است.

البته او بیان می‌کند این ادعا که «قدرت سایبری یک ابزار مکمل است»، مبتنی‌بر نوع استفاده‌ای است که تاکنون از قدرت سایبری شده است و اگر سناریوهای کابوس‌وار سایبری که مورد علاقه هالیوود هم هست رخ دهد مانند خاموش کردن شبکه‌های برق، اختلال در کنترل ترافیک هوایی، یا سقوط وال‌استریت با چند ضربه کلید، در آن صورت این ادعا باید به‌طور کامل بازنگری شود. اما برای اینکه این اتفاق بیفتد باید استقلال و اجبار قدرت سایبری ثابت شود. برای مثال، خاموش کردن یک شبکه برق از طریق قدرت سایبری، بدون‌شک عواقب فاجعه‌باری خواهد داشت، اما به‌جای اینکه قربانیِ خود را مجبور به پذیرش خواسته‌هایش کند، ممکن است پاسخ حتی فاجعه‌بارتری را به دنبال داشته باشد.

ویژگی سومی که برای قدرت سایبری معتقد است اینکه قدرت سایبری می‌تواند پنهان باشد.[4] او این ویژگی را از جذابیت‌های قدرت سایبری برای بسیاری از کاربران می‌داند چراکه بدون اینکه کسی متوجه نقش و عاملیت آنها شود می‌تواند در مقیاس جهانی تأثیرگذار باشد. او همچنین به جذابیت این ویژگی برای دولت‌ها هم اشاره می‌کند و این توانایی در استفاده مخفیانه از قدرت سایبری، ازآنجایی‌که باعث می‌شود هویت و انگیزه مهاجمان به راحتی قابل شناسایی نباشد، آن را به ابزاری بسیار جذاب برای دولت‌ها و سایر بازیگران تبدیل می‌کند.

دیدگاه دیگر در تعریف قدرت سایبری، توصیفی است که جوزف نای[5]؛ اندیشمند حوزه مطالعات سیاسی آمریکا و دستیار سابق وزیر دفاع و معاون وزیر خارجه این کشور ارائه می‌دهد. توصیفی که نای از قدرت سایبری ارائه می‌دهد، در عین اینکه تفاوت‌هایی با دیدگاه‌های پیشین دارد، اما متناقض نیست. او دو تعریف از قدرت سایبری ارائه می‌دهد. تعریف اول، تعریفی است از زاویه «منابع قدرت سایبری» است. او می‌گوید: «قدرت سایبری به منابعی بستگی دارد که حوزه فضای سایبری را مشخص می‌کند مانند: زیرساخت، شبکه‌ها، نرم‌افزار و مهارت‌های انسانی». او از زاویه دیگری قدرت سایبری را تعریف می‌کند و آن زاویه «رفتاری» است. نای از این زاویه، قدرت سایبری را «توانایی دستیابی به نتایج دلخواه از طریق استفاده از منابع اطلاعاتی به هم پیوسته از طریق الکترونیک» تعریف کرده است. در نگاه اول، تصور نای از قدرت سایبری بسیار ساده به‌نظر می‌رسد: «استفاده از منابع اطلاعاتی به

---

۱. جان بی. شلدون (John B. Sheldon)، دکترای مطالعات راهبردی و امنیت بین‌الملل، مدیر اجرایی مؤسسه جورج سی. مارشال (George C. Marshall Institute) در آرلینگتون، ویرجینیا است. او همچنین مؤسس و مدیر Torridon Group LLC، یک شرکت مشاوره تخصصی در حوزه سیاست‌گذاری فضایی و امنیت سایبری، و عضو ارشد در شورای آتلانتیک (Atlantic Council) و مرکز مطالعات امنیت جهانی (Centre for Global Security Studies) در دانشکده امور جهانی مونک (Munk School of Global Affairs) دانشگاه تورنتو است. شلدون سابقه فعالیت به عنوان دیپلمات وزارت امور خارجه بریتانیا را نیز در کارنامه دارد. او دارای مدرک کارشناسی و کارشناسی ارشد از دانشگاه هال (University of Hull) بریتانیا و دکترای مطالعات امنیتی است.

2. Cyberpower is Everywhere
3. Cyberpower is Complementary
4. Cyberpower Can Be Stealthy
5. Nye

هم پیوسته حوزه سایبری برای کسب نتایج دلخواه درون فضای سایبری» اما قدرت سایبری مدنظر نای، با توانایی استفاده از فضای سایبری برای ایجاد مزیت‌ها و تأثیرگذاری بر رویدادها در سایر محیط‌های عملیاتی و ابزارهای قدرت مشخص می‌شود؛ یعنی همان نکته‌ای که در تعریف شلدون و کوئل هم بر آن تأکید شده بود. این بدین معناست که این قدرت می‌تواند از اهرم‌های سایبری برای کسب نتایج دلخواه در دامنه‌هایی بیرون از فضای سایبری هم بهره‌برداری کند. بنابراین این مفهوم بیش از استفاده صرف از ابزارهای سایبری در فضای سایبری برای رسیدن به آنچه می‌خواهید دلالت دارد [۲۲].

از نظر نای، ویژگی بارز قدرت سایبری، «پراکندگی» آن است که ثمره سهولت گذار از موانع ورود به آن است. موانع دامنه سایبری آنچنان آسان فرو می‌ریزند که بازیگرانی سوای دولت‌ها و نیز کشورهایی کوچک قادرند با هزینه‌ای اندک نقشی کلان در این دامنه ایفا کنند. «اجتماعی/مردمی شدن قدرت» و «غیرمتمرکز شدن حکمرانی جهانی» از آثار و پیامدهایی است که درنتیجه این ویژگی(پراکندگی قدرت) ایجاد شده است.

از دیگر تعاریف مشهور از قدرت سایبری، تعریفی است که سرهنگ جیسون.ام اسپید[1] ارائه می‌دهد. در تعریفی که اسپید ارائه می‌دهد، کمتر به منابع قدرت سایبری اشاره شده و وجه رفتاری قدرت سایبری بیشتر مورد توجه بوده است. از نظر اسپید قدرت سایبری توانایی یک دولت-ملت برای ایجاد کنترل و اعمال نفوذ در داخل و از طریق فضای سایبری، در پشتیبانی و ارتباط با سایر حوزه‌ها و عناصر قدرت ملی است. او معتقد است دستیابی به قدرت سایبری به توانایی دولت برای توسعه منابع برای فعالیت در فضای سایبری بستگی دارد. قدرت سایبری به‌عنوان یک قابلیت دولت-ملت تفاوتی با قدرت زمینی، دریایی، هوایی یا فضایی ندارد؛ با این تفاوت که دولت به‌جای تانک، کشتی و هواپیما، به رایانه‌های شبکه‌ای، زیرساخت‌های مخابراتی، برنامه‌ها و نرم‌افزارها و افرادی با مهارت‌های لازم نیاز دارد. لذا همانند حوزه‌های زمینی، دریایی، هوایی و فضایی، دولت می‌تواند از طریق فضای سایبری تأثیراتی را در فضای سایبری یا در حوزه‌های دیگر ایجاد کند. حمله سایبری می‌تواند پایگاه داده لجستیکی دشمن را خراب کند و توانایی‌های استقرار سریع دشمن را تضعیف کند. ساقط کردن یک شبکه دفاع هوایی، امکان حمله هوایی یا سیگنال‌های یک ماهواره موقعیت‌یاب جهانی را مختل می‌کند و در توانایی کشتی جنگی برای هدایت یا هدف قرار دادن سیستم‌های تسلیحاتی خود اختلال ایجاد می‌کند [۲۳].

تعریفی که زیمت و باری[2] ارائه می‌دهند فناورانه و در پشتیبانی از سایر حوزه‌های قدرت به‌خصوص قدرت نظامی است. آنها قدرت سایبری را قابلیت کنترل سامانه‌های فناوری اطلاعات و شبکه‌های فضای سایبر می‌دانند که برای انجام مأموریت‌های نظامی و پشتیبانی از حوزه‌های اقتصادی و سیاسی قابل استفاده است [۱۷]. همان طور که در تعاریف فوق دیده می‌شود، ماهیت و ویژگی‌های قدرت سایبری از جهاتی با ماهیت سنتی از قدرت و قدرت ملی منطبق است و از جهاتی به‌دلیل امکان‌های جدید و دامنه تحولات وسیعی که در سایه تحولات فناورانه پذیرفته است، از قدرت در ماهیت سنتی خود متمایز شده است. مضاف بر اینکه از حیث کاربرد نیز دامنه وسیع‌تری یافته است و همین هم باعث شده در ابعاد تهاجمی، دفاعی و بین‌المللی از وزن و اثرگذاری بیشتری برخوردار شود. قدرت سایبری در بعد تهاجمی، با هدف ضربه به زیرساخت‌های حیاتی و تخریب تأسیسات نظامی و هسته‌ای دشمن با حملات سایبری و اجبار و ارعاب کشورها کاربرد دارد. در بعد تدافعی نیز نشان‌دهنده میزان آمادگی هر کشور در مقابله با بحران‌های سایبری و قدرت بازدارندگی است. دستیابی به این قدرت، نسبت به سایر شکل‌های قدرت، هزینه کمتری دارد و می‌تواند ازطرف کشورهای کوچک برای پیگیری سیاست‌های خود به‌کار رود. در معاهدات بین‌الملل نیز نمونه‌هایی از توجه به قدرت سایبری دیده می‌شود. به‌عنوان مثال ناتو از سال ۲۰۰۷ کنترل تهدیدهای سایبری و دستیابی به قدرت سایبری را در دستور کار خود قرار داده است. در سال ۲۰۱۱ فضای سایبر به‌عنوان فضای امنیتی و نظامی مورد توجه قرار گرفت و پذیرش حمله سایبری در سطح حمله نظامی و مجوز دفاع سایبری و اقدام متقابل نظامی به اعضای ناتو مطرح شد؛ بنابراین قدرت سایبری از موضوع‌های کلیدی و راهبردی است که برای نشان دادن نقش و تأثیر آن در امنیت ملی باید به‌طور دقیق شناخته شده و در سطح ملی بازتعریف شود.

1. Spade
2. Zimet and Barry

۴. بررسی ابعاد، لایه‌ها و بازیگران قدرت سایبری

پس از ارائه تعاریف ارائه شده از قدرت سایبری و مفاهیم زمینه‌ای و مرتبط با آن که مبیّن جهت‌گیری و اقتضائات اساسی ماهیت آن است، سیر تطور مفهوم قدرت از اشکال ابتدایی تا اشکال نوین آن مشخص شد که تاریخ و شیوه اِعمال آن متناسب با زیست و فرماسیون اجتماعی بشر را نشان می‌دهد. ضروری است تا در این بخش، پدیدارشناسانه و با توجه به تعینی که قدرت سایبری در حوزه‌های مختلف نرم و سخت حکمرانی در مقیاس ملی و بین‌المللی پیدا کرده، اشکال اِعمال قدرت، مقومات و ابعاد اصلی سازنده آن و همچنین زمینه‌ها و حوزه‌های مهم و استراتژیکی که در رابطه‌ای دیالکتیکی با آن قرار دارند، توضیح داده شود تا درنهایت بتوانیم به تصویری کامل از قدرت سایبری و مختصات و کارکردهای آن دست یابیم.

۴-۱. سیمای قدرت سایبری و شکل اِعمال آن

قدرت در مفهوم کلی و متعارفی که از آن وجود دارد عبارت است از توان شخص (الف) در تحمیل اراده خود بر شخص (ب)، به‌گونه‌ای که در صورت فقدان آن توان، (ب) مجبور، متمایل یا مشتاق به اطاعت از اراده (الف) نیست. ازاین‌رو بحث قدرت به توان یک طرف در تحمیل اراده خود بر طرف دیگر به سه روش مختلف «اجباری»، «ترغیبی» و «القایی- اقناعی» دلالت دارد. جوزف نای (۱۳۹۵) این سه وجه و سیمای قدرت را به‌گونه‌ای دقیق‌تر بیان می‌کند. او معتقد است توان واداشتن دیگران به تغییر رفتار در قیاس با خواسته‌های اولیه‌شان، وجهی مهم از سیمای قدرت است، اما تنها وجه نیست و اساساً کژاندیشی است که قدرت را جز تحکم به قصد تغییر ندانیم. وجه دیگر آن توان اثرگذاری بر خواسته‌های دیگران است تا بدون هیچ فشار و تحکمی همان را بخواهد که شما می‌خواهید. این قدرتی است هم‌گزین و درعین‌حال معارض قدرت تحکمی. چنین وجهی از قدرت ناظر بر قابلیت ترغیب دیگران به اقدامی است خلاف خواسته‌ها و راهبردهای ابتدایی آنان. در این وجه می‌توان با اثرگذاری بر تلقی و توقع دیگران نسبت به آنچه موجه و ممکن است، ترجیحات را قاب‌بندی کرد. مطابق این وجه از قدرت، می‌توان گفت بازیگرانی در عرصه بین‌الملل قدرتمندند که بتوانند سد راه حضور آنان که قدرت کمتر دارند بر سر میز مذاکره شوند یا اگر نتوانند، با پیش‌دستی در حضور خود قواعد بازی را پیشاپیش معین کنند. آنان که با چنین سیمایی از قدرت مواجه‌اند چه‌بسا خود واقف به این مواجهه نباشند یا باشند. اما در سال‌های ۱۹۷۰، جامعه‌شناسی به نام استیون لیوکز،[1] به نقش انگاره‌ها و باورها در شکل‌دهی خواسته‌های ابتدایی دیگران انگشت گذاشت. بر این اساس می‌توان با شکل دادن ترجیحات بنیانی یا ابتدایی فرد، بر آنان اعمال قدرت کرد. لیوکز چنین وجهی را «سیمای سوم قدرت» نامیده است.

جدول ۴. سه وجه و سیمای قدرت

سیمای نخست	فرد (الف) برای تغییر رفتار فرد (ب) نسبت به خواسته‌ها و راهبردهای اولیه‌اش از تهدید یا پاداش استفاده می‌کند. فرد (ب)، واقف به این مسئله، قدرت فرد (الف) را احساس می‌کند.
سیمای دوم	فرد (الف) برنامه کار را به شیوه‌ای پیش می‌برد که فرد (ب) را در انتخاب‌های راهبردی خود مقید و محدود سازد. فرد (ب) چه‌بسا ناآگاه از این شیوه باشد اما اقتدار فرد (الف) را احساس کند.
سیمای سوم	فرد (الف) می‌کوشد تا به باورهای اساسی، برداشت‌ها و خواسته‌های فرد (ب) شکل دهد. بعید است فرد (ب) از این شیوه آگاه باشد یا تأثیر قدرت (الف) را دریابد.

مأخذ: یافته‌های پژوهش.

1. Steven Lukes

قدرت سایبری نیز از آن جهت که ماهیت آن از جنس قدرت در مفهوم عام است می‌تواند از زاویه وجوه سه‌گانه قدرت مورد توجه قرار گیرد. بر این اساس به اعتقاد جوزف نای (۱۳۹۵) با سه سیمای قدرت سایبری مواجهیم که شواهدی از رفتارهایی با نمود قدرت نرم و سخت در آن قابل مشاهده است. البته ذکر این نکته لازم است که آنچه به‌عنوان شواهدی برای این سه سیمای قدرت گفته می‌شود، براساس تجربیات و نمونه‌هایی است که در سایر کشورهای دنیا اتفاق افتاد و به‌منزله تأیید یا تجویز این اقدام‌ها نبوده و صرفاً بیان امکان‌هایی است که این شیوه از قدرت در اختیار بازیگران قرار می‌دهد. بنابراین طبیعتاً در کشور ما براساس آنچه در چارچوب قوانین اسلامی تعریف می‌گردد، این راهبردها تجویز یا رد می‌شود.

اولین وجه قدرت عبارت از توان بازیگر در واداشتن و اجبار دیگران به انجام کاری است خلاف ترجیحات یا راهبردهای اولیه آنان. آنچه دایره این ممنوعیت و اجبار را تعیین می‌کند یا مجوزی برای تعیین نوع اقدام است، بسته به نظام ارزشی، پروتکل‌ها و قوانین آن کشور یا سرویس میزبان متفاوت است. «حملات رد خدمات» مانند آنچه در سال ۲۰۰۸ در مورد گرجستان اتفاق افتاد و اینترنت آن قطع شد یا تعبیه رمز خرابکار با غرض اختلال در سامانه‌های یک کشور که عمدتاً کشورها یا گروه‌های متخاصم انجام می‌دهند، نمودهایی از قدرت سخت است. از زاویه قدرت نرم، فرد یا سازمان قادر است دیگران را به تغییر رفتارشان ترغیب کند به‌گونه‌ای که این تغییر از طریق جلب حمایت، شکل‌دهی به افکار عمومی یا ایجاد جذابیت فرهنگی و ایدئولوژیک، بدون اجبار مستقیم، رخ دهد. دولت چین، در موارد موضع‌گیری نامساعد مقامات ژاپنی نسبت به نظرهای چینی‌ها درباره مناسبات دو کشور در سال‌های ۱۹۳۰، گاه از اینترنت برای بسیج دانشجویان چینی برای تظاهرات علیه ژاپن استفاده کرده است. ویدئوهای القاعده یا داعش در اینترنت با غرض جلب توجه عمومی به آمال این سازمان، نمونه دیگری از کاربرد قدرت نرم در فرایند تغییر ترجیحات یا راهبردهای اصلی مردم است.

وجه دوم، قدرت تنظیم یا قاب‌بندی دستور کار است که در آن بازیگر با رد و نفی راهبردهای دیگران سد راه آنان می‌شود. تنظیم دستور کار از نوع «اعمال فیلترها» مانند انسداد وب‌سایت‌هایی با مضامین اجتماعی نظیر سایت‌های غیراخلاقی، قمار و مواد مخدر وجهی از این نوع قدرت سخت به‌حساب می‌آید. البته در توضیح این قدرت و تفکیک میان قدرت نرم و سخت در این معنای از قدرت، تفاوتی اعتباری وجود دارد. چنانچه این اعمال قدرت، خلاف خواست گروه بازیگران باشد، قدرت سخت و چنانچه قانونی به‌حساب آید، نمونه‌ای از قدرت نرم است. بنابراین در مواردی آنچه برای گروهی قدرت سخت به‌حساب می‌آید، برای گروه دیگری نرم و جذاب است. چین، در پی شورش‌های شینگ جیان در سال ۲۰۰۹، هزاران وب‌سایت را مسدود و پیام‌های متنی پرشماری را سانسور کرد. این اقدام، درعین‌حال که ارتباطات سکنه منطقه را دشوارتر می‌ساخت، به پیدایش بدیل‌های محلی وب‌سایت‌های بیگانه، از قبیل یوتیوب، فیس‌بوک و توئیتر منجر شد که برای هکرهای ناسیونالیست جذابیت ویژه‌ای داشت. در آمریکا، وقتی شرکت‌های دست‌اندرکار تولید موسیقی بیش از ۱۲،۰۰۰ آمریکایی را به جرم سرقت مالکیت معنوی از راه دانلود غیرقانونی محصولاتشان، تحت پیگرد حقوقی قرار دادند، تلقی افراد تحت پیگرد و نیز بسیاری از کسانی که تحت پیگرد نیز نبودند، از اقدام آنان نوعی اعمال قدرت سخت بود. اما هنگامی که شرکتی فراملیتی چون اپل تصمیم به انسداد دانلود برخی برنامه‌های کاربردی روی محصول آیفون خود می‌گیرد، بسیاری از مصرف‌کنندگان حتی متوجه چنین اقدامی نمی‌شوند، و تنها شماری اندک به الگوریتم‌های هادیِ جستجوها پی می‌برند.

در سیمای سوم قدرت، بازیگری خاص ترجیحات ابتدایی دیگری را به‌نحوی شکل می‌دهد که برخی راهبردها اصولاً مدنظر قرار نمی‌گیرند. وقتی شرکت‌ها تصمیم به جایگزین‌سازی رمزی به‌جای رمزی دیگر در محصولات نرم‌افزاری خود می‌گیرند، مصرف‌کنندگانی اندک متوجه آن خواهند شد. به‌عنوان مثال برخی کشورها با سامان‌دهی برنامه‌هایی -بدون اینکه شهروندان متوجه خط‌دهی حکمرانان خود شوند- در مسیر آگاهی شهروندان سنگ‌اندازی می‌کنند و مانع دسترسی آنان به دیگر عقاید و افکار می‌شوند. نمونه واقعی این شیوه از قدرت را می‌توان در شبکه‌هایی مانند اینستاگرام دید که با اعمال محدودیت‌هایی بدون اینکه کاربر متوجه آن باشد، مانع دسترسی کاربر به اطلاعات و تصاویر مخالف و معارض با عقاید و افکارشان می‌شوند.

۲-۴. بازیگران قدرت سایبری

«کم‌رنگ شدن نقش جغرافیا و سهولت فرارفتن از محدوده جغرافیایی»، «ناشناس ماندن کنشگران و عدم قابلیت ردیابی»، «هزینه کم ورود»، «هزینه کم فناوری رایانه‌ای» و «اتصال گسترده به اینترنت و سهولت ایجاد یا به‌دست آوردن نرم‌افزارهای مخرب»،

بخشی از ویژگی‌های فضای سایبری است که فراوانی شمار بازیگرانی غیر از بازیگران سنتی عرصه قدرت را موجب شده است که به موازات یکدیگر با نیازها، اهداف و نیات متفاوت وجود دارند. «فضای مجازی یک دامنه جهانی است که تقریباً برای هرکسی که به اینترنت با اتصال رایانه، تلفن هوشمند یا هر نوع دستگاه دیگری دسترسی دارد، در دسترس است. در این حوزه، بسیاری از بازیگران مختلف به موازات یکدیگر، با نیازها، اهداف و نیات متفاوت وجود دارند.» [۲۴].

برخی از این بازیگران به تنهایی عمل می‌کنند، برخی دیگر در شبکه‌های به‌هم متصل یا در ساختارهای رسمی‌تر. لذا به تعبیر برخی محققان با سه گروه از بازیگران مواجهیم: «بازیگران دولتی»، «بازیگران غیردولتی با شبکه‌هایی به‌شدت ساختارمند» و «افراد با شبکه‌هایی کمتر ساختارمند». نقش‌ها نیز ممکن است بسته به موقعیت متفاوت باشد و ممکن است همپوشانی داشته باشد. ضمن اینکه بازیگران می‌توانند در طول زمان و بسته به مأموریت و اهداف فعلی خود بین نقش‌ها جابه‌جا شوند [۲۵].

بنابراین، علاوه بر دولت-ملت‌ها، موجودیت‌های سایبری دیگری نیز وجود دارد که باید در معادله قدرت در نظر گرفته شود. این بازیگران با وجود اینکه خود مشتمل بر بازیگران فرعی گسترده‌ای مانند شرکت‌های چندملیتی، گروه‌های جنایت سازمان‌یافته و سازمان‌های تروریستی، گروه‌های هکری و اشخاص هستند، در یک تقسیم‌بندی کلی، بازیگران غیردولتی نامیده می‌شوند. نکته قابل ملاحظه در مناسبات این بازیگران کاهش نسبی اختلاف و دامنه قدرت میان آنان است تا جایی که در مواردی بسیار کاهش بیش‌ازپیش شکاف میان میزان قدرت دولت‌ها و بازیگرانی غیر از دولت‌ها را شاهد هستیم.

با این وجود حاکمیت دولت‌ها بر فضای سایبر برای اعمال قدرت در داخل مرزهای زمینی، محدود است؛ زیرا بخش‌های زیادی از فضای سایبر تحت نظارت نهادهای بین‌المللی مانند آیکان، گروه مهندسی اینترنت و اتحادیه بین‌المللی مخابرات اداره می‌شود. هرچند احتمال این نهادها تأثیرپذیری قدرت‌های بزرگ جهانی به‌ویژه آمریکا است. فناوری‌های فضای سایبر ابزار اداره و تسخیر دنیا و جایگزین قدرت هسته‌ای و بستری برای جهانی‌سازی است، به‌گونه‌ای که قوام و تداوم اقتدار دولت‌ها متأثر از قدرت سایبری شده است. کشورهایی که به فناوری فضای سایبر مجهز نباشند و خود را به بهره‌گیری از قابلیت‌های آن در قالب قدرت سایبری ملزم ندانند، در صحنه جهانی مجالی برای قدرت‌نمایی نخواهند داشت.

۱-۲-۴. بازیگران دولتی

می‌دانیم که بخش‌های زیادی از فضای سایبر تحت نظارت نهادهای بین‌المللی مانند آیکان، گروه مهندسی اینترنت و اتحادیه بین‌المللی مخابرات اداره می‌شود و حاکمیت دولت‌ها بر فضای سایبر برای اعمال قدرت در داخل مرزهای زمینی، محدود است. بااین‌حال نمی‌توان چنین نتیجه گرفت که نقش دولت‌ها و به‌تبع آن بازیگران دولتی با برداشته شدن محدودیت‌های جغرافیایی در فضای سایبر و سرزمین‌زدایی ناشی از آن حذف خواهد شد. هرچند قهراً کشورهایی که به فناوری فضای سایبر مجهز نباشند و خود را به بهره‌گیری از قابلیت‌های آن در قالب قدرت سایبری ملزم ندانند، در صحنه جهانی مجالی برای قدرت‌نمایی نخواهند داشت. بنابراین دولت‌ها همچنان مهم‌اند، به این دلیل که جغرافیا همچنان مهم است.

واقعیت این است که به‌رغم این اتفاق و کم‌رنگ شدن محدودیت‌های ناشی از موقعیت و مکان، جغرافیا همچنان در استفاده از قدرت سایبری اهمیت دارد. دلیل آن هم این است که «فضای سایبری به‌دلیل زیرساخت فیزیکی آن که مشتمل بر رایانه‌های شبکه‌ای، کابل‌ها و ماهواره‌هاست و همچنین اداره و نگهداری آن توسط انسان‌هایی که بنا به ضرورت باید روی زمین در جوامع سازمان‌یافته سیاسی در مناطق فیزیکی متمایز و مشخص زندگی می‌کنند، پایه‌ای جغرافیایی دارد» (Sheldon). بنابراین طبیعی و اجتناب ناپذیر است که قدرت سایبری مانند سایر حوزه‌های استراتژیک مانند زمین، دریا، هوا و فضا دارای ابعاد ژئوپلتیکی قابل توجهی باشد.

مضاف بر این جغرافیا، امکان‌های دیگری را در نسبت با دولت‌های ملی ایجاد می‌کند که مجموعاً موجب تحکیم نقش دولت‌ها و بازیگران دولتی در حوزه قدرت و امنیت سایبری می‌شود. جغرافیا ابزار قدرتمندی برای اعمال فشار و نظارت قانونی دولت‌ها بر عملکرد شرکت‌ها، اشخاص و فعالیت‌های گروه‌های تروریستی و براندازان داخلی و خارجی است. روترها و سرورهای فیزیکی و کابل‌های شبکه در اماکن جغرافیایی قرار دارند که تحت حاکمیت دولت‌هاست، بنابراین شرکت‌های اینترنتی مانند گوگل، فیس‌بوک و غیره نیز به رعایت قوانین این دولت‌ها ملزم هستند. به‌خصوص «اگر دولت‌هایی حاکم بر بازارهایی بزرگ باشند این شرکت‌ها به‌جای

دست شستن از این بازارها، ترجیح می‌دهند از مقررات این کشورها تبعیت کنند»[۲۲] یا چنانچه اشخاص یا گروه‌هایی از طریق سایت‌ها یا شبکه‌های پیام‌رسان به دنبال ایجاد شورش باشند، دولت‌ها می‌توانند با اخلال در اتصال اینترنتی و محدود یا قطع کردن دسترسی مردم آن منطقه به شبکه‌ها یا سایت‌های اینترنتی مانع تحقق اهداف آنها شوند. بنابراین دولت‌ها همچنان توان ایراد فشار فیزیکی بر شرکت‌ها و اشخاص را دارند.

۲-۲-۴. بازیگران غیردولتی

همان‌طور که در بخش قبل بحث شد، موجودیت‌های سایبری دیگری نیز وجود دارد که باید در معادله قدرت در نظر گرفته شود. اینها شامل شرکت‌ها، جنبش‌های سیاسی، اجتماعی و مذهبی، گروه‌های جنایی سازمان‌یافته و سازمان‌های تروریستی و اشخاص است که می‌توانند از فناوری برای جذب و تأثیرگذاری بر تعداد زیادی از افراد و جوامع استفاده کنند [۲۴]. برخی از محققان پتانسیل بازیگران غیردولتی در فضای مجازی را بالا می‌دانند و معتقدند درحالی‌که تفاوت قدرت سایبری چشمگیری در فضای سایبری میان بازیگران دولتی و غیردولتی وجود دارد، معتقدند شکاف قدرت بین این بازیگران در حوزه سایبری در حال کاهش است. راتری[۱] و هیلی[۲] معتقدند که بازیگران غیردولتی در حوزه سایبری نفوذ بیشتری نسبت به سایر حوزه‌ها دارند که آن را هم عمدتاً به هزینه‌های پایین و موانع ورود به این حوزه نسبت می‌دهند.[۳] برخی شرکت‌های چندملیتی برخوردار از منابع مالی هنگفت و نیروی انسانی ماهر و نیز مسلط بر مرزهای مالکیتی خاص خود، اقتداری فراتر از بسیاری از دولت‌ها دارند. ساختار فراملیتی این شرکت‌ها امکان بهره‌گیری آنها از بازارها و منابعی در پهنه جهانی را فراهم می‌سازد. اگر به‌طورکلی «منابع» و «نفوذ» را دو معیار قدرت در نظر بگیریم، نهادهای سایبری غیردولتی می‌توانند قدرتی برابر بازیگران دولتی داشته باشند. برای مثال می‌توان به گوگل، آمازون و فیس‌بوک در دنیای شرکت‌ها اشاره کرد. ویکی لیکس یک نهاد فضای مجازی با ماهیت فراملی دارد که به ارسال و افشای اسناد ازسوی منابع ناشناس می‌پردازد. این مؤسسه حامیان سرسخت دارد و نشان داده است که می‌تواند ابرقدرت‌ها را با چالش‌های سختی روبه‌رو کند و مدیریت تحولات را در اختیار گیرد. در کنار تمام اسناد منتشر شده ازسوی این سایت، باید افشای اسناد طبقه‌بندی شده در مورد جنگ افغانستان، جنگ عراق و وزارت امور خارجه آمریکا را به‌عنوان مهم‌ترین و جنجالی‌ترین اسنادی نام برد که ازسوی این سایت در اختیار عموم قرار گرفته است. این قدرت‌های سایبری غیردولتی، مولد قدرت‌های سایبری آینده هستند که از فضای سایبری و فضای فیزیکی برای اعمال نفوذ در ابعاد دیپلماتیک، اطلاعاتی، نظامی و اقتصادی استفاده می‌کنند.

فضای سایبری علاوه بر همه آثار مثبتی که داشته، هم‌زمان، رسانه‌ای بوده است که برای بیش از دو دهه در تهدید و درگیری استفاده می‌شده است. لذا در این فضا با بازیگرانی غیردولتی مواجهیم که نقشی مخرب را ایفا می‌کنند. «اداره تحقیقات فدرال (FBI) بازیگران فضای سایبری را مشتمل بر عوامل تهدیدکننده دسته‌بندی می‌کند. بنابراین، علاوه بر دولت-ملت‌ها، گروه‌های جنایت سازمان‌یافته و سازمان‌های تروریستی را به‌عنوان بازیگران سایبری (تهدید) معرفی می‌کند».[۴] همان‌طور که در جدول ۵ نشان داده شده است، نمونه‌های اولیه از اقدام‌های سایبری به اواخر دهه ۱۹۸۰ برمی‌گردد که در دهه‌های بعد ادامه یافته است.

1. Rattray
2. Healey
3. G. Rattray, J. Healey,
4. Federal Bureau of Investigation, The Cyber Threat, Washington, DC

جدول ۵. نمونه‌های اولیه از اقدام‌های سایبری غیردولتی «هکتیویسم»

۱۹۸۹	کرم «Wank» نفوذ به شبکه کامپیوتری ناسا در اعتراض به سلاح‌های هسته‌ای و استفاده از پلوتونیوم برای سوخت کاوشگر گالیله. این کرم اینترنتی باعث شد تا تصویری روی صفحه کامپیوترها ظاهر شود که به استفاده از راکت‌هایی با سوخت «پلوتونیمی» در طرح اکتشاف سیاره مشتری با ناسا اعتراض داشتند.
۱۹۹۵	تحصن شبکه «Strano» هکرها معمولاً وقتی توان نفوذ به روش‌های معمول به شبکه‌های رایانه‌ای هدف را ندارند، به حمله بی‌رحمانه‌ای به نام اختلال در سرویس‌دهی یا Denial-of-Service(DoS) دست می‌زنند. نوع پیشرفته و توزیع شده این حمله سایبری، DDoS است که در آن تعداد مهاجمان به شبکه هدف به‌مراتب بیشتر از نوع معمولی آن است. DDoS مخفف عبارت Distributed Denial of Service است و به هدفِ از کار انداختن موقت و یا دائمی یک وب‌سایت یا سرور انجام می‌شود. حملات DDoS از گذشته‌ای نسبتاً دور وجود داشته‌اند و معمولاً هم برای بیان اعتراض به‌کار برده می‌شدند. شاید اولین حمله DDoS را بتوان مربوط به سال ۱۹۹۵ و شبکه Strano Network دانست که در اعتراض به سیاست‌های هسته‌ای دولت فرانسه انجام شد.
۱۹۹۸	هک‌های UrBaN Kaos تخریب وب‌سایت‌های دولت اندونزی با تمرکز بر ظلم به مردم تیمور شرقی
۲۰۱۰	در روز شنبه ۲۹ مه ۲۰۱۰، هکری که خود را «کاکا آرژانتینی» می‌نامید وب‌سایت دولت اوگاندا را هک و تصویری از آدولف هیتلر با صلیب شکسته که نماد حزب نازی بود، منتشر کرد.
۲۰۱۱	گوگل با مهندسان SayNow و توئیتر همکاری کرد تا در پاسخ به قطعی اینترنت تحریم شده توسط دولت مصر در جریان اعتراضات سال ۲۰۱۱، برای مردم مصر راه ارتباطی فراهم کند. نتیجه، سرویسی به نام Speak To Tweet بود که در آن پست صوتی باقی‌مانده از طریق تلفن، سپس از طریق توئیتر با پیوندی به پیام صوتی در SayNow گوگل توئیت می‌شد.
۲۰۲۱	در سال ۲۰۲۱، انانیموس پایگاه داده‌های شرکت میزبان وب آمریکایی Epik را هک و اسناد آن را افشا کرد.
۲۰۲۲	در تلافی حمله روسیه به اوکراین در سال ۲۰۲۲، انانیموس حملات سایبری متعددی را علیه سیستم‌های کامپیوتری روسیه انجام داد.

مأخذ: یافته‌های پژوهش.

نکته قابل ملاحظه در اینجا نوع مواجهه دولت‌های قربانی با بازیگران غیردولتی مخرب است. اینکه چگونه دولت‌های آسیب‌دیده می‌توانند به بازیگران غیردولتی واقع در قلمرو یک کشور دیگر دسترسی داشته باشند. این مسئله به مسئولیت‌پذیری دولت و کنترل دولت بر بازیگران غیردولتی گره خورده است. برخی از دولت‌ها از طریق محدود کردن دسترسی به محتوای اینترنت در سرزمین‌های خود، حاکمیت بیشتری در فضای مجازی دارند. بعضی از کشورها، ازجمله چین، تصمیم به فیلتر بخشی از محتوای خاص اینترنت گرفته‌اند که ممکن است به مردم آسیب برساند. درحالی‌که این امر حاکمیت یک دولت بر قلمرو خود را نشان می‌دهد و تأثیر سیاسی و بر روابط بین‌الملل نیز دارد. به عقیده دمچاک[1] و دامبروسکی[2]، چنین رفتارهایی، شواهدی از سیستم وستفالی در حال توسعه در فضای مجازی است.

۳-۴. ابعاد و لایه‌های قدرت سایبری

با توجه به اهمیت و تأثیری که امروزه قدرت سایبری به‌عنوان پیشران توسعه کشورها در مقیاس جهانی، منطقه‌ای و ملی در حوزه‌های مختلف نظامی، امنیتی، سیاسی، اجتماعی و اقتصادی یافته است، توجه به ابعاد و لایه‌های مختلف آن برای تولید قدرت ضروری است. بی‌تردید درکی عمیق‌تر از «کارکردهای قدرت سایبری و حوزه‌های نرم و سخت تأثیرگذاری و اثرپذیری» و شناسایی ابعاد و لایه‌های آن، امکان «شناسایی نقاط آسیب و ضعف و نیز برنامه‌ریزی و توسعه جامع قدرت سایبری» را خواهد داد.

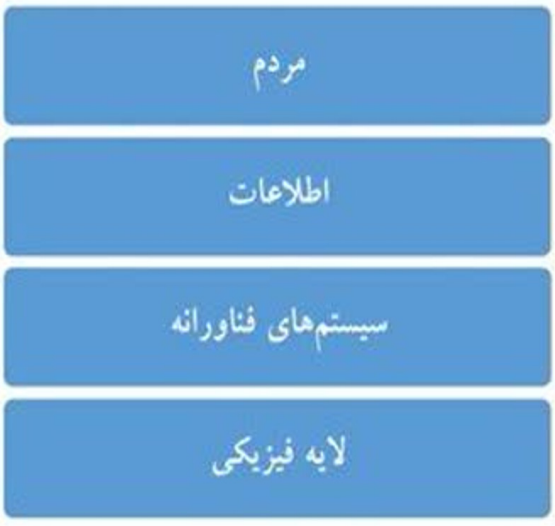
1. Demchak
2. Dombrowski

درمجموع دیدگاه‌های که در معرفی ابعاد قدرت سایبری وجود دارد، دو رویکرد اتخاذ شده است. رویکرد اول، شامل نظریه‌پردازانی است که با توجه به دامنه اثرگذاری قدرت سایبری به بیان ابعاد آن می‌پردازند. ویژگی این رویکرد در ابعاد قدرت سایبری، شناسایی فرصت‌ها و ظرفیت‌های پیش روی قدرت سایبری و محدودیت‌ها و تهدیدهایی است که در این پدیده وجود دارد. ازجمله نظریه‌پردازانی که با این رویکرد ابعاد قدرت سایبری را بیان می‌کنند، جوزف نای است. او معتقد است قدرت سایبری بر بسیاری از حوزه‌ها؛ درون و بیرون دامنه سایبری اثرگذار است و می‌تواند به زایش قدرت نرم و سخت در هریک از این دو فضا منجر شود. این بدین معناست که قدرت سایبری می‌تواند در شکل نرم قدرت مانند «تنظیم دستورکار، جذب و ترغیب» و شکل سخت آن مانند «اعمال زور و محدودیت» تبلور یابد. بر این اساس او ابعاد فضای مجازی را به دو بعد «سخت» و «نرم» تقسیم می‌کند که در بخش قبل به آن اشاره شد.

رویکرد دوم، شامل نظریه‌پردازانی است که تلاش کرده‌اند از طریق ارائه لایه‌های فضای مجازی به روشن ساختن ابعاد قدرت سایبری بپردازند. تقسیم فضای سایبری به لایه‌های متعدد، فرصتی برای حفظ آگاهی و شناخت جامع از وضعیت سایبری و توانایی مقابله در برابر حملات سایبری را ارائه می‌دهد. همچنین از طریق پیش‌بینی، بازخورد، اصلاح و تکمیل، به تاب‌آوری به‌عنوان عامل مهم در ایجاد قدرت سایبری کمک می‌کند. ترکیب آگاهی وضعیتی با ارزیابی لایه‌های مختلف سایبری می‌تواند فهم فضای سایبری و نحوه برنامه‌ریزی قدرت سایبری را بهبود بخشد.

در ادامه به برخی از چارچوب‌های ارائه لایه‌های فضای مجازی که حوزه‌های قدرت در فضای سایبری را مشخص می‌کند اشاره می‌شود. کوئل فضای مجازی را به چهار لایه «مردم»، «اطلاعات»، «سیستم‌های فناورانه» و «لایه فیزیکی» تقسیم می‌کند. «لایه فیزیکی» شامل اجزا و مشخصه‌های فیزیکی فضای مجازی است. «سیستم‌های فناورانه» شامل پلتفرم‌ها و سیستم‌های فناورانه است که مشخصه نرم‌افزاری دارند که برای ایجاد، ذخیره، اصلاح، تبادل و بهره‌برداری از اطلاعات در تمام اشکال بی‌شمار آن ایجاد و به‌کار گرفته می‌شود. اینجاست که ما فضای سایبری را طراحی و می‌سازیم، زیرا هریک از این پلتفرم‌های سایبری با هدفی ایجاد شده‌اند و ما آنها را برای ایجاد سیستم‌ها و شبکه‌های جدیدتر و پیچیده‌تر و با قابلیت‌تر ترکیب می‌کنیم. لایه بعدی خود «اطلاعات» است. درنهایت و مهم‌تر از همه، «عنصر انسانی» است؛ افرادی که از ارتباط و محتوا برای تأثیرگذاری بر شناخت استفاده می‌کنند و کارهای مختلفی را انجام می‌دهند که افراد با اطلاعات انجام می‌دهند [۳].

شکل ۱. لایه‌های فضای سایبر از نظر کوئل



مأخذ: یافته‌های پژوهش.

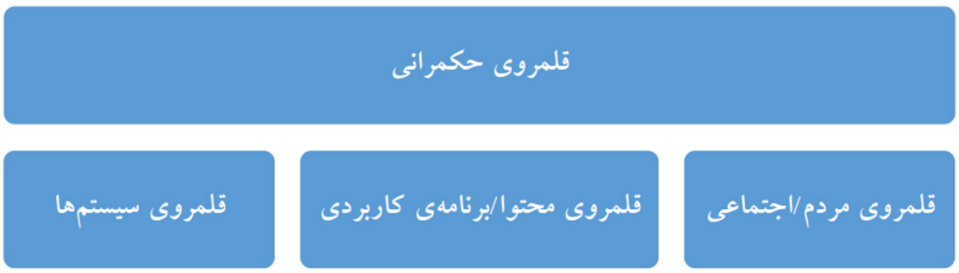
به‌طور مشابه کلارک در سال ۲۰۱۰ مدلی چهار لایه‌ای ارائه می‌کند که تفاوتی جزئی با مدل کوئل دارد. کلارک به‌جای سیستم‌های فناورانه در مدل کوئل، «لایه منطقی» را پیشنهاد می‌کند و ضمن تأکید بر اهمیت لایه فیزیکی مشتمل بر دستگاه‌های محاسباتی به هم متصل، ماهیت فضای مجازی و قوت و محدودیت آن را عمدتاً ناشی از لایه منطقی می‌داند. لایه منطقی عبارت است از ساختارهای منطقی که خدمات را می‌سازند و از ماهیت پلتفرمی فضای سایبری پشتیبانی می‌کنند» .
لایه اطلاعات، شامل اشکال مختلف محتوا و لایه مردم شامل کاربران هستند. نکته مهم اینکه در نگاه کلارک کاربران منفعل نبوده و از طریق گزینش روش‌های استفاده از فضای مجازی خصوصیات آن را شکل می‌دهند.

شکل ۲.اجزای فضای سایبر از نظر کلارک (۲۰۱۰)

مأخذ: یافته‌های پژوهش.

مدل زیمت و اسکودیس (۲۰۰۹) نیز مشابهت زیادی با دو مدل قبلی دارد. البته آنها فضای سایبر را به‌عنوان یک قلمروی حکمرانی می‌دانند که خود تقسیم به سه قلمروی «مردم/ اجتماعی»، «محتوا / برنامه کاربردی» و «سیستم‌ها» می‌شود. در مقایسه با دو مدل قبلی تقریباً می‌توان گفت دو لایه منطقی و فیزیکی در مدل کلارک یا سیستم‌های فناورانه و فیزیکی در مدل کوئل در این مدل ذیل «قلمروی سیستمّ‌ها» تجمیع شده است.

شکل ۳.قلمروی فضای سایبر در آمریکا (زیمت و اسکودیس)



مأخذ: یافته‌های پژوهش.

با توسعه رویکرد ارائه شده شلدون که براساس توسعه چارچوب کلارک ارائه شده است، چهار لایه برای فضای سایبری پیشنهاد می‌شود. ایـــن لایه‌ها عبارتند از: «زیرســـاختی»، «فیزیکی»، «ساختاری» و «معنایی».

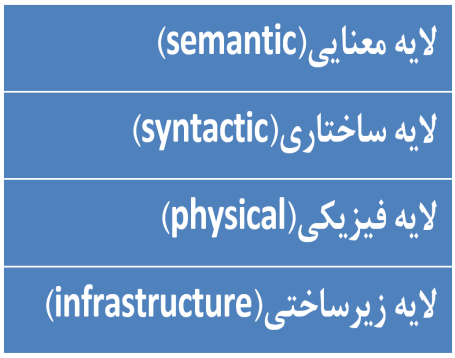
لایه زیرساختی: زیرساخت فضای سایبری شامل سخت‌افزار، سرورها، مؤلفه‌های شـبکه، کابل‌کشی، ماهواره‌هـا و سایر تجهیـزات است. ایـن لایه می‌تواند بـا شاخص‌هایی نظیر نسبت جمعیت دارای دسترسی به اینترنت، بازه زمانی که کاربران سخت‌افزار را ارتقا می‌دهد، سـطح مالکیـت اسمارت فون‌ها و تعـداد ISP ها نسبت بـه جمعیت و تعداد گذرگاه‌های بین‌المللی ارائه‌دهنده اتصالات سراسری اندازه‌گیری شود.

لایه فیزیکی: شامل ابزارهایی ماننـد PC2 هـا، لپتـاپ‌ها، تبلت‌ها و اسمارت‌فون‌ها است کـه کاربران بـا استفاده از آنها بـا یکدیگر تعامل می‌کنند. شاخص‌های اندازه‌گیری این لایه می‌تواند نسبت به‌کارگیری کابل مسی در مقایسه با کابل‌های فیبر نوری بـا سرعت بـالا، تعـداد نقـاط نقـاط Wi -Fi در هـر جمعیت، پوشش تلفن همراه، متوسـط مصرف داده‌ها توسـط هر مشترک و هزینه دسترسی در مقایسه بـا حقوق متوسـط ملـی باشـد.

لایه ساختاری: وظایف این لایه عبارت است از نحوه ساختاردهی به داده‌ها برای تسهیل ارتباط بین اجزای تشـــکیل‌دهنده و درون لایه زیرساخت که شامل پروتکل‌های ارتباطی، اجزای نرم‌افزاری و الگوریتم‌های مسیریابی شبکه است. شاخص‌های اندازه‌گیـری ایـن لایه شامل سطح رمزنگاری داده‌هـا، نسبت کامپیوترهـای محافظت شده توسط آنتی‌ویروس و سطح دستگاه‌های آلوده، درجه اولویت‌بندی شبکه (بی‌طرفی شبکه) و تعداد ثبت‌نام دامنه باشد.

لایه معنایی: این لایه امکان درک اطلاعات را به کاربران می‌دهد تا به شکل مفیـد از آن بهره‌گیری کنند و شامل عناصری مانند نوع و محبوبیـت رابط کاربر، نرم‌افزار کاربردی و همچنیـن ملاحظات زبانی، فرهنگی و فکری است کـه در طراحی آنها مورد استفاده قرار می‌گیرد. شاخص‌های اندازه‌گیری این لایه عبارتند از: نسبت تولیـد ناخالص داخلی از تجارت آنلاین، درصد صفحات وب تولید شده در زبان بومی، درصد کاربران فعال شبکه‌های اجتماعی به جمعیـت، سطح جرائم اینترنتـی و میزان اثربخشـی قانـون و اجـرای آن.

شکل ۴. لایه‌های فضای سایبری



مأخذ: یافته‌های پژوهش.

در سند ۱۲-۳ ستاد مشترک ارتش آمریکا (JP3-12) که به عملیات سایبری مربوط است، فضای سایبر در قالب سه لایه معرفی می‌شود. «لایه شبکه فیزیکی» متشکل از دستگاه‌ها و زیرساخت IT در قلمرو فیزیکی که امکان ذخیره، انتقال و پردازش اطلاعات را درون فضای سایبری فراهم می‌آورد. «لایه شبکه منطقی» متشکل از آن دسته از عناصر شبکه مرتبط با یکدیگر است که به‌صورتی مجزا از لایه فیزیکی، مبتنی‌بر برنامه‌نویسی منطقی (کد) اجزای شبکه را مدیریت می‌کند. «لایه هویت سایبری» منظری از فضای سایبری است که با انتزاع داده از لایه شبکه منطقی با استفاده از قواعد به‌کار رفته در لایه شبکه منطقی، برای توصیف بازنمایی دیجیتال یک بازیگر یا هویت موجود در فضای سایبر ایجاد می‌شود.

۵. اهرم‌های قدرت سایبری و مهم‌ترین شاخص‌های جهانی آن

۵-۱. مؤلفه‌ها و اهرم‌های برتری قدرت سایبری

قرن بیست‌ویکم عرصه قدرت‌نمایی در فضای سایبر است. فضایی که در آن مانند هر عرصه دیگری، قدرت‌ها به قوی، متوسط و ضعیف تقسیم می‌شود. امروز دیگر قدرت نظامی حرف اول را نمی‌زند. کشور یا بازیگری قدرتمندتر است که شرایط را برای دفاع در برابر حملات سایبری فراهم کند یا در تهاجم سایبری حرفی برای گفتن داشته باشد. اکنون دولت‌ها به‌منظور نشان دادن برتری خود، در حال سرمایه‌گذاری در فضای سایبر هستند تا همچنان برتری خود را حفظ کنند. «اساساً اینترنت به‌عنوان ابزاری جدید برای جنگ میان دولت‌ها به میدان آمده است. برای مثال تلاش رژیم صهیونیستی برای حمله به تأسیسات هسته‌ای ایران، اقدام هند برای جلوگیری از هک کردن گوشی‌های بلک‌بری این کشور توسط هکرهای پاکستان و استفاده از کابل‌های فیبر نوری جدید و پرتاب ماهواره اینترنتی اختصاصی به فضا در برزیل به‌منظور رهایی از گذشتن اطلاعات این کشور از مسیر میامی، همگی حاکی از آماده شدن بالقوه دولت‌ها برای مقابله با حمله احتمالی سایبری به اطلاعات محرمانه خود ازسوی دیگران حکایت دارد».

اما ماندن در عرصه قدرت سایبری ملزوماتی نیاز دارد. آدام سگال[1]، پژوهشگر ارشد روابط خارجی آمریکا در کتاب خود با نام «نظم جهانی هک‌شده» به چهار عنصر برای ماندن و برتری در عرصه قدرت سایبری اشاره می‌کند: «دارا بودن اقتصادی بزرگ و پیشرفته از لحاظ فناوری»؛ «سازمان‌های دولتی که انرژی و نوآوری را به سمت بخش خصوصی هدایت کنند»؛ «آژانس‌های اطلاعاتی و نظامی ماجراجو و تاحدی درنده»؛ «ارائه روایتی جذاب از فضای مجازی».

رکن اول، «اندازه قدرت اقتصادی و پیشرفته از لحاظ فنی» است که بسیار ضروری به‌نظر می‌رسد. اگر شرکت‌ها و سرورهای ذخیره داده‌های اینترنتی‌شان، تلفن‌ها و رایانه‌های شخصی مورد استفاده مردم و نرم‌افزارها و سرویس‌های وب که به‌مثابه دروازه‌ای به‌سوی اینترنت عمل می‌کنند را گسترش دهند تا سهم بالایی در اقتصاد اینترنتی داشته باشند، دولت‌ها نسبت به رقبایشان برتری غالبی خواهند داشت؛ مانند شرکت‌های فناوری آمریکا که بر اقتصاد اینترنت تسلط دارند. آمریکا ۳۵ درصد از درآمدهای مخابراتی جهان و بیش از ۴۰ درصد از درآمد خالصِ تولید شده آنلاین را به خود اختصاص داده است. در هند، ۲۵ وب‌سایت برتر، سایت‌های مستقر در آمریکا مانند گوگل، فیس‌بوک، توئیتر و لینکدین هستند. بیش از ۵۰ درصد از ۲۵ سایت برتر در برزیل و آفریقای جنوبی را شرکت‌های آمریکایی اداره می‌کنند. «گوگل» پیشرو در موتورهای جستجو است و سیستم عامل اندروید آن در اکثریت گوشی‌های هوشمند ساخته شده در جهان قرار دارد.

شکل و ساختار اینترنت به آمریکا وزن زیادی می‌بخشد. تعداد کمی از ارائه‌دهندگان اینترنت، بخش عمده‌ای از داده‌ها را روی «ستون فقرات» حمل می‌کنند و اکثر داده‌های اینترنتی به آمریکا کشیده شده و از طریق آن هدایت می‌شود؛ حتی اگر این موضوع، منطقی جغرافیایی کمی داشته باشد. برای مثال، ایمیلی که از برزیل به پرو فرستاده می‌شود، ممکن است به برازیلیا سفر کند، فورتالزا را در ساحل از طریق کابل زیردریایی ترک کند، از طریق میامی وارد آمریکا شود، از کالیفرنیا عبور کند و سپس به سمت پایین اقیانوس آرام به لیما برود. مایکل هیدن، مدیر سابق آژانس امنیت ملی[2] وقتی برخی از فعالیت‌های آژانس امنیت ملی را توجیه می‌کرد، به‌صراحت گفت: «این یک بازی خانگی برای ما است. آیا قرار نیست از این که بسیاری از [داده‌ها] آن از طریق ردموند، واشنگتن می‌رود، بهره ببریم؟ چرا قوی‌ترین ساختار مدیریت مخابرات و محاسبات روی کره زمین را به استفاده خود نمی‌زنیم؟»

یک پارادوکس اصلی برای آمریکا وجود دارد: پیچیدگی‌های اقتصادی و فناوری نیز منابع آسیب‌پذیری هستند. موتورهای جدید رشد اقتصادی و فرصت‌ها - اینترنت اشیا، ماشین‌های خودران، شهرهای هوشمند - در معرض حملات سایبری مخرب هستند. پیشرفت باعث قرار گرفتن در معرض بیشتر می‌شود. همان‌طور که اقتصاد چین از نظر فناوری پیشرفته‌تر می‌شود، پکن با همان چالش تشویق نوآوری و درعین‌حال محافظت از سیستم‌های فناورانه مواجه خواهد شد، اما در حال حاضر آمریکا به‌طور منحصربه‌فردی قدرتمند و مستعد است. حتی اگر کشوری به‌عنوان رهبر فناوری شناخته نشود، اندازه بازار اهمیت دارد. آمریکا اینترنت را اختراع کرد، اما آینده فضای مجازی حداقل از نظر کاربران آن آمریکایی نیست. توزیع جهانی قدرت تغییر خواهد کرد. در حال حاضر، آسیا ۴۲ درصد از

1. Adam Segal
2. NSA

جمعیت اینترنت جهان را تشکیل می‌دهد (بیشترین آنها براساس منطقه)، اما از نظر ضریب نفوذ با ۲۱,۴ درصد تنها در رتبه ششم قرار دارد، به این معنا که جمعیت بسیار زیاد و عمدتاً جوان هنوز به اینترنت متصل نشده‌اند. چین بیشترین تعداد کاربران اینترنت را در جهان دارد - ۶۴۹ میلیون در سال ۲۰۱۴ - اما کمی بیش از نیمی از جمعیت آنلاین هستند. ۶۰ درصد از کاربران اینترنت در چین زیر سی سال هستند. درحالی‌که برزیل در لبه نرم‌افزار منبع باز (یا رایگان) قرار دارد، تأثیری که بر شرکت‌های خارجی و حاکمیت فضای سایبری اعمال می‌کند تا حدی به تعداد بیشتر و رو به رشد کاربران اینترنت برزیلی بستگی دارد. اندونزی و آفریقای جنوبی از نفوذ مشابهی برخوردارند، هرچند تاکنون در صحنه جهانی بسیار کمتر از برزیل فعال بوده‌اند.

رکن دوم قدرت سایبری، «**توانایی دولت در همکاری با بخش خصوصی است**». این وابستگی منشأ قابلیت‌های حکومت مردمی و آسیب‌پذیری‌هاست و شاخص‌ترین بحث در مقوله دفاع به‌شمار می‌رود چراکه بخش اعظم ارتباطات دوربُرد، انرژی و شبکه‌های حمل‌ونقل در اختیار شرکت‌های خصوصی است. باراک اوباما، رئیس‌جمهور آمریکا، در فوریه ۲۰۱۵ در نشست امنیت سایبری در palo Alto گفت: «امنیت سایبری ملی باید یک مأموریت مشترک باشد. بسیاری از شبکه‌های رایانه‌ای و ساختارهای زیربنایی ما در اختیار بخش خصوصی است و این به این معناست که دولت به‌تنهایی نمی‌تواند کاری از پیش برد».

رکن سوم، «**وجود آژانس‌های اطلاعاتی و نظامی خلاق و ماجراجو است**». چهل‌ویک دولت دارای دکترین جنگ سایبری هستند و هفده دولت، ظرفیت‌های تهاجمی دارند. هک دستگاه‌ها، کار ارزان و راحتی است، آنچه سخت است طراحی حمله‌ای است که تأثیری ملموس از خود برجای بگذارد و این نیازمند داشتن اطلاعات مهم، تحلیل و بررسی، تحقیق و توسعه است. طبق آمارها، آمریکا در بحث تهاجمی سه یا چهار برابر بیشتر از مقوله دفاعی هزینه صرف می‌کند.

آخرین رکن قدرت سایبری، ارائه «**روایتی جذاب از فضای سایبر است**». با اینکه اینترنت کار خود را از شبکه آژانس پروژه‌های تحقیقاتی پیشرفته (ARPANET) زیرنظر وزارت دفاع آمریکا آغاز کرد، اما طی دو دهه گذشته، دولت آمریکا همگام با شرکت‌های بزرگ فناوری و اینترنت، از هنجارهایی مانند «دسترسی آزاد» و «آزادی بیان» با دخالت و نظارت حداقلی دولت حمایت کرده است؛ چراکه اولاً سرعتش مدیون بازیگران و بنگاه‌های خصوصی الگوی غیرمتمرکز حکومت است و ثانیاً امنیت سایبری قدرتمند، به‌خودی‌خود به‌ویژه توسط شرکت‌های بزرگ و افراد حقیقی، به‌مثابه یک ارزش تلقی شده و به‌عنوان سبب‌ساز جریان آزاد اطلاعات تقویت شد.

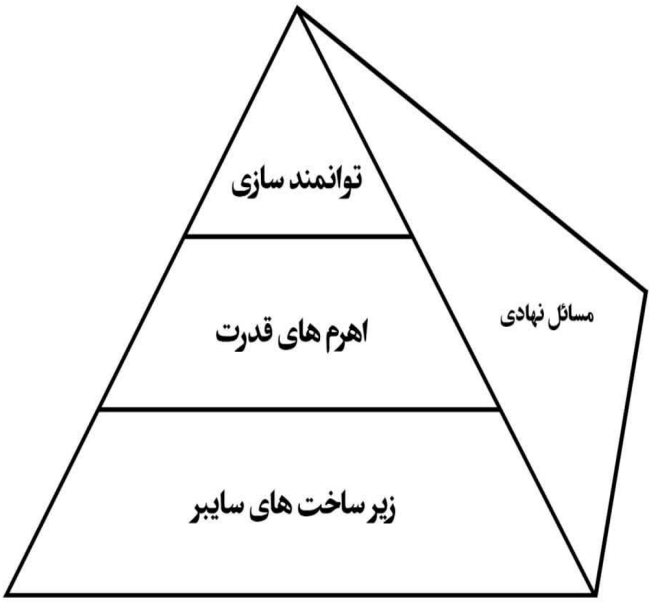
استراتژی بین‌المللی کاخ سفید برای فضای سایبری در سال ۲۰۱۱، تمام اینها را در یک جمله خلاصه کرد و آن اینکه «آمریکا به سمت زیرساخت‌های ارتباطی و اطلاعاتی آزاد، تبادل‌پذیر، امن و قابل اطمینان حرکت می‌کند»، اما افشاگری‌های ادوارد اسنودن[1] - کارمند سابق سازمان اطلاعات مرکزی آمریکا و پیمانکار سابق آژانس امنیت ملی- درجه بالایی از تعارض و البته ریاکاری موضع واشنگتن را آشکار کرد؛ چراکه آمریکا هم‌زمان با نظارتِ گسترده، خود را به‌عنوان مدافع اینترنتِ باز و آزاد معرفی می‌کرد. این نشان می‌دهد به‌رغم اینکه آزادی جهانی اینترنت و امنیت ملی متقابل نیستند، اما آشتی دادن آنها کار آسانی نیست.

۲-۵. حوزه‌های تأثیر قدرت سایبری بر تقویت سطوح سنتی قدرت

استوارت اچ استار[2] با ارائه یک چارچوب نظری، قدرت سایبر را در حوزه‌های متعددی بررسی می‌کند. وی با ترسیم نموداری، قدرت‌گیری بازیگران بین‌المللی را در عرصه سایبر مبتنی‌بر اهرم‌های قدرتی می‌داند که این عرصه ارائه می‌کند. از نظر او اهرم‌های قدرت در قالب سیاسی، اقتصادی، نظامی، اطلاعاتی تعریف می‌شود. 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 قدرت به‌نوبه خود، پایه‌هایی را برای توانمندسازی بازیگران در رأس هرم فراهم می‌کند. این بازیگران عبارتند از: شرکت‌ها، دولت-ملت‌ها و سازمان‌های بین‌المللی، افراد، تروریست‌ها، جنایتکاران فراملی. گفتنی است که برخلاف دولت‌ها، احتمال دارد سایر بازیگران به همه وجوه و زیرساخت‌های فضای سایبر دسترسی نداشته باشند. اما برعکس، بازیگران غیردولتی با محدودیت‌های ساختاری چون موافقت‌نامه‌های بین‌المللی که امکان توانمندسازی را محدود می‌کند، مواجه نیستند.

1. Edward Joseph Snowden
2. Starr. H Stuart

شکل ۵. چارچوب مفهومی قدرت سایبر [۱۷]



این هرم و چارچوب مفهومی سویه دیگری نیز دارد و آن «مسائل نهادی» است. این مسائل شامل عواملی چون حکومت، ملاحظات حقوقی و قانونی، نظم‌دهی، بـه اشـتراک‌گذاری اطلاعات و ملاحظاتی درخصوص آزادی‌های مدنی است.

حوزه اطلاعات

عنصر اساسی که به قدرت سایبر ارتبـاط بسـیار نزدیکـی دارد، «اطلاعـات»[1] اسـت. فضای سایبر و قدرت سایبر بـه‌وضوح ابعادی از «قدرت اطلاعـاتی»[2] هستند. قدرت سایبری به کشورها امکان نظارت و پایش بر فضای اطلاعاتی داخلی و خارجی می‌دهد. این شامل تأثیر بر افکار عمومی، تصویرسازی و مدیریت دیدگاه‌ها می‌شود.

حوزه اقتصاد

قدرت سایبر به‌طور روزافزونی در توانایی اقتصادی نقش حیاتی ایفا می‌کند. حتـی دولـت ریگان در دهه ۱۹۸۰ میلادی در «استراتژی امنیـت ملـی» بـا اشـاره بـه نقـش اطلاعـات و تکنولوژی‌های جدید اطلاعاتی در قدرت اقتصادی اقتصاد آمریکا به این موضوع پرداخت. در اقتصاد جهانی قرن ۲۱ که اقتصادی جهان‌شمول و به‌هـم پیوسـته شده، فضای سایبر را می‌توان تنها عامل مهم به‌هم پیوستگی بازیگران با یکـدیگر دانسـت که تولید را تقویت می‌کند، بازارهای جدیـدی می‌گشاید و مـدیریت سـاختارهایی کـه ثروت‌های کلانی ایجاد می‌کند را ممکن می‌سازد.

حوزه سیاست و دیپلماسی

از دیگر حوزه‌های تأثیر قدرت سایبری، تـأثیر قدرت سایبر بر امور سیاسی و دیپلماتیک است. از مفاهیم شکل گرفته در نتیجه این تلاقی، مفهوم سایبر دیپلماسی است. سایبر دیپلماسی یک مفهوم نوین است که به تأثیرگذاری بر افکار و روابط کشورها در فضای مجازی می‌پردازد. این نوع دیپلماسی با استفاده از فناوری‌های نوین ارتباطات، به دولت‌ها امکان می‌دهد تا با مردم در تعامل باشند و ارتباط دیپلماسی با مردم به‌جای دولت‌ها، سبب به‌وجود آمدن دیپلماسی عمومی شده است. سایبر دیپلماسی از ابزارهای مختلفی مانند وب‌سایت‌ها، شبکه‌های اجتماعی و رسانه‌های دیجیتال استفاده می‌کند. این ابزارها به مقامات و سیاستمداران امکان می‌دهد نظرها و مطالب خود را در گستره وسیعی پخش کنند. یکی از اهداف استفاده از سایبر دیپلماسی، تأثیرگذاری بر افکار و به‌تبع آن روابط کشورها است. این دیپلماسی به‌عنوان یک تکامل در دیپلماسی عمومی شناخته می‌شود.

1. Information
2. Informational Power

حوزه 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 براساس 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 برپایه تکنولوژی‌های مدرن شکل گرفته است.

قدرت سایبر روزبه‌روز خود را به‌عنوان یک عامل تأثیرگذار در سیاستگذاری‌های ملی در تمام حوزه‌های مورد اشاره توسعه می‌دهد. از اقدام‌های 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 می‌کند. میزان تسهیل در دسترسی به این فضای تکنولوژیک، میزان موفقیت شهروندان و به تبع آن دولت را رقم می‌زند. قدرت سایبر میان دیگر عناصر و ابزارهای قدرت پیوند برقرار می‌سازد و آنها را برای بهتر شدن وضعیت یاری می‌رساند. به‌عبارت‌دیگر، فضای سایبر همانند مواد خامی است که سوخت اقتصاد و جامعه را فراهم می‌کند.

با توجه به توضیحاتی که داده شد، می‌توان به تعریفی که کوئل از قدرت سایبری ارائه داد بازگشت که قدرت سایبری، «توانایی استفاده از فضای سایبر برای ایجاد مزیت‌ها و تأثیرگذاری بر رویدادها در تمام محیط‌های عملیاتی و از طریق ابزارهای قدرت است». این تعریف همچنانکه مشاهده می‌شود، 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.

۳-۵. مهم‌ترین شاخص‌های جهانی ارزیابی قدرت سایبری

برنامه‌ریزی، سرمایه‌گذاری و سایر انواع مداخلات در عرصه قدرت سایبری، نیازمند شاخص‌گذاری است؛ زیرا بدون وجود شاخص‌ها و نشانگرها، امکان ارزیابی و سنجش برنامه‌ها و تصمیم‌های دولتی ممکن نیست. با استفاده از شاخص قدرت سایبری ملی استراتژی‌های دولت‌ها، قابلیت‌های آنها برای عملیات دفاعی و مخرب، تخصیص منابع و قابلیت‌های بخش خصوصی در کشور (مثلاً شرکت‌های فناوری، نیروی کار و نوآوری) اندازه‌گیری می‌شود. شاخص‌ها امکان بررسی‌های هم‌زمانی و در زمانی را فراهم می‌کنند. منظور از بررسی «هم‌زمانی» مقایسه وضعیت کشورهای مختلف در یک مقطع زمانی است و منظور از بررسی «در زمانی» این است که اندازه‌گیری یک شاخص در طول زمان و مقاطع زمانی مختلف، کمک می‌کند تا مسیر طی شده توسط کشورها (صعود یا تنزل) در شرایط مختلف و در بازه‌های زمانی تحلیل شود.

از میان مدل‌ها، مدل قدرت سایبری گروه مرکز بلفر تا به امروز از جامع‌ترین و موردتوجه‌ترین مدل‌ها برای سنجش قدرت سایبری است. رسالت مرکز بلفر این است که پیشرفت دانش خط‌مشی‌گذاری و انتقادی را درباره مسائل مهم امنیت بین‌المللی راهبری کند. انتشار گزارش «شاخص قدرت سایبری ملی ۲۰۲۲» مرکز بلفر، با همین هدف صورت گرفته است. مطابق این گزارش، قدرت سایبری شامل هشت هدف در نظر گرفته شده که در ادامه به آنها اشاره خواهد شد. در این گزارش وضعیت ۳۰ کشور در این شاخص و در هریک از اهداف هشت‌گانه ترسیم شده است. طبق گزارش تیم بلفر، ایران حائز رتبه دهم در میان قدرت‌های سایبری است. با توجه به صبغه مرکز بلفر این احتمال وجود دارد که اهدافی پشت پرده انتشار این گزارش وجود داشته باشد؛ به‌ویژه اینکه در متن اصلی گزارش در مواردی گزاره‌های نادرستی درخصوص ایران مطرح شده است.

از ویژگی‌های گزارش شاخص قدرت سایبری ملی مرکز بلفر این است که تلاش کرده رویکردی جامع به قدرت سایبری داشته باشد؛ هرچند هنوز وجوه نظامی و امنیتی برجسته است. این گزارش به جنبه‌های اقتصادی و رسانه‌ای دستکاری افکار عمومی و کنترل محیط اطلاعاتی قدرت سایبری پرداخته، اما هنوز جای خالی وجوه دیگر قدرت سایبری به‌ویژه وجوه فرهنگی محسوس است که باید در طراحی بومی شاخص قدرت سایبری ملی به این موضوع توجه شود.

۱-۳-۵. اهداف/ شاخص‌های هشت‌گانه

۱. نظارت و پایش گروه‌های داخلی (Surveilling and Monitoring Domestic Groups): استفاده از قابلیت‌های سایبری برای نظارت بر گروه‌های داخلی به‌منظور حفظ ثبات و امنیت داخلی. برای دستیابی به این هدف/شاخص، کشورها با ایجاد چارچوب‌های قانونی و توسعه قابلیت‌های سایبری، به پایش، شناسایی و جمع‌آوری اطلاعات از بازیگران داخلی و تهدیدهای پنهان داخل مرزهای خود می‌پردازند. این اقدام‌ها می‌تواند شامل نظارت بر فعالیت‌های شهروندان، رصد ترافیک اینترنتی، دور زدن رمزگذاری‌ها، یا شناسایی و خنثی‌سازی فعالیت‌های سرویس‌های اطلاعاتی خارجی، گروه‌های تبهکار و سازمان‌های تروریستی باشد.

۲. تقویت و بهبود دفاع سایبری ملی(Strengthening and Enhancing National Cyber Defenses): توسعه زیرساخت‌ها و سیاست‌هایی برای حفاظت از سیستم‌ها و شبکه‌های ملی در برابر حملات سایبری. کشوری که این هدف/شاخص را در اولویت قرار داده، بر تقویت امنیت و تاب‌آوری سایبری دارایی‌ها و سیستم‌های ملی تمرکز دارد. این اقدام‌ها شامل دفاع فعالانه از زیرساخت‌های دولتی، ارتقای امنیت و بهداشت سایبری در صنایع کلیدی و جامعه و افزایش آگاهی عمومی نسبت به تهدیدهای سایبری است.

۳. کنترل و دستکاری محیط اطلاعاتی(Controlling and Manipulating the Information Environment): مدیریت و شکل‌دهی به جریان اطلاعات و روایت‌های عمومی برای تأثیرگذاری بر افکار عمومی داخلی و خارجی. کشوری که این هدف/شاخص را دنبال می‌کند، از ابزارهای الکترونیکی برای کنترل اطلاعات و تغییر روایت‌ها بهره می‌گیرد که نشان‌دهنده دوگانگی در مدیریت اطلاعات است. این اقدام‌ها شامل انتشار تبلیغات هدفمند در داخل، ایجاد و تقویت اطلاعات نادرست در خارج و استفاده از قابلیت‌های سایبری برای هدف قرار دادن و خنثی‌سازی گروه‌هایی است که خارج از حوزه قضایی کشور فعالیت می‌کنند. همچنین، این هدف می‌تواند حذف محتوای افراط‌گرایانه در رسانه‌های اجتماعی و مقابله با تبلیغات خارجی را دربرگیرد.

۴. گردآوری اطلاعات پنهان (جاسوسی) خارجی برای امنیت ملی(Foreign Intelligence Collection for National Security): استفاده از ابزارهای سایبری برای جاسوسی و گردآوری اطلاعات استراتژیک از کشورهای دیگر. کشوری که این هدف/شاخص را دنبال می‌کند، با استفاده از روش‌های سایبری، اطلاعات حساس ملی از دشمنان خارجی خود استخراج می‌کند. این فعالیت‌ها به‌طور خاص بر گردآوری اطلاعاتی متمرکز است که جنبه تجاری ندارد، بلکه به حوزه‌هایی مانند فعالیت‌های دیپلماتیک، برنامه‌ریزی نظامی، نظارت بر پیمان‌ها و سایر مواردی مربوط می‌شود که دولت‌ها برای بهبود آگاهی و درک خود از وضعیت کشورهای خارجی به آنها نیاز دارد. این هدف شامل اقدام‌هایی نظیر هک، نفوذ به اطلاعات طبقه‌بندی‌شده مانند برنامه‌های نظامی، سرقت سوابق پرسنل و دسترسی به ارتباطات مقامات ارشد دولتی است.

۵. کسب سود تجاری یا تقویت صنعت داخلی(Commercial Gain or Enhancing Domestic Industry Growth): بهره‌برداری از قابلیت‌های سایبری برای توسعه فناوری، نوآوری و رشد اقتصادی داخلی. کشوری که این هدف/شاخص را دنبال می‌کند در تلاش است صنعت فناوری داخلی خود را ارتقا دهد یا از روش‌های سایبری برای توسعه سایر صنایع بهره برد. این اقدام‌ها ممکن است از طریق روش‌های قانونی یا غیرقانونی انجام شود. روش‌های غیرقانونی شامل جاسوسی صنعتی از شرکت‌ها و دولت‌های خارجی برای تسهیل انتقال فناوری است، درحالی‌که روش‌های قانونی شامل سرمایه‌گذاری در تحقیق و توسعه امنیت سایبری و اولویت‌بندی آموزش و پرورش نیروی کار متخصص در این حوزه می‌شود.

۶. تخریب یا از کارانداختن زیرساخت و قابلیت‌های دشمن تخریب یا غیرفعال‌سازی زیرساخت‌ها و قابلیت‌های دشمن (Destroying or Disabling an Adversary's Infrastructure and Capabilities): انجام حملات سایبری برای مختل کردن یا نابودی زیرساخت‌های حیاتی دشمن. کشوری که این هدف/شاخص را دنبال می‌کند، از تکنیک‌ها، تاکتیک‌ها و روش‌های سایبری مخرب برای بازدارندگی، تخریب یا کاهش توانایی دشمن در حوزه‌های سایبری یا سنتی استفاده می‌کند. این اقدام‌ها شامل حملات سایبری به زیرساخت‌های حیاتی، حملات توزیع‌شده قطع سرویس (DDoS) به شبکه‌های ارتباطی دولتی و حملات سایبری با هدف نمایش عزم و توان بازدارندگی در برابر اقدام‌های دشمن است.

۷. تعیین هنجارهای سایبری و استانداردهای فنی بین‌المللی(Defining International Cyber Norms and Technical Standards): مشارکت در شکل‌دهی به قوانین، پروتکل‌ها و استانداردهای جهانی در فضای سایبری. کشوری که این هدف/شاخص

را دنبال می‌کند، در گفتگوهای بین‌المللی، حقوقی، سیاستگذاری و فنی مرتبط با هنجارهای سایبری نقش مؤثری ایفا می‌کند. این اقدام‌ها می‌تواند شامل امضای پیمان‌های سایبری، مشارکت در کارگروه‌های فنی، پیوستن به ائتلاف‌ها و شراکت‌های سایبری برای مقابله با جرائم سایبری و به اشتراک‌گذاری تخصص و قابلیت‌های فنی باشد.

۸. انباشت ثروت یا استخراج رمزارز (Amassing and Protecting Wealth): بهره‌گیری از عملیات سایبری برای کسب ثروت، مانند سرقت مالی از طریق حملات سایبری نظیر باج‌افزار، اخاذی داده‌ها یا حملات به زیرساخت‌های مالی. کشوری که این هدف/شاخص را دنبال می‌کند، از روش‌های سایبری برای انباشت ثروت استفاده می‌کند. این اقدام‌ها شامل سرقت مالی از طریق باج‌افزار، اخاذی با استفاده از اطلاعات به‌دست‌آمده از نفوذ به داده‌ها و حملات به زیرساخت‌های دیجیتال مؤسسه‌های مالی برای اخاذی یا کسب سود است.

درک جامعه سایبری از عوامل دخیل در قدرت سایبری در شرف تکوین است و با توسعه این حوزه درک جامعه سایبری از عوامل دخیل در قابلیت‌های قدرت سایبری متحول خواهد شد و نشانگرهای ما هم باید به همراه آن متحول شود. به این حقیقت واقفیم که اهداف ملی با استفاده از روش‌های سایبری دنبال می‌شود در خلأ شکل نمی‌گیرد. قابلیت‌های سایبری تنها ابزاری از مجموعه ابزارهای کشورها (در کنار شیوه‌های نظامی، سنتی، دیپلماسی، تحریم‌ها و تعرفه‌هایی که دولت‌ها برای دستیابی به اهداف ملی‌شان به‌کار می‌گیرند) به‌شمار می‌روند. بنابراین جامع‌ترین قدرت سایبری دارای بالاترین قصد و قابلیت برای دستیابی به اکثریت اهداف با استفاده از روش‌های سایبری است و پایین‌ترین نمره به کشوری تعلق دارد که کمترین اهداف را با استفاده از روش‌های سایبری دنبال کند و کمترین سطح قصد و قابلیت را داشته باشد.

۶. جمع‌بندی و نتیجه‌گیری

در این گزارش تلاش شد تا مفهوم قدرت و سیر تطور تاریخی آن به‌مثابه صورتی از نظم اجتماعی توضیح داده شود. در ادامه تلاش شد تا شکل جدید قدرت که با ظهور و توسعه فضای مجازی تکوین یافته است، به نام «قدرت سایبر» توضیح داده شود. گفته شد که اساساً این اصطلاح که درواقع نمودار رابطه مثبت و خوشبینانه میان سیاست و فضای مجازی است، واجد تعاریفی است که هرکدام از منظری به آن پرداخته‌اند. برجسته‌ترین ویژگی این پدیده/کلیدواژه که تقریباً در همه تعاریف هم به آن اشاره شده بود، ابزار مکمل بودن و امکان تأثیرگذاری بر سایر حوزه‌های قدرت به‌صورت نرم و سخت است. جوزف نای، نظریه‌پرداز مشهور آمریکایی در حوزه قدرت نرم، اهداف و مرجع نهایی قدرت سایبر را در دو حوزه دسته‌بندی می‌کند. دسته اول درون فضای سایبر اتفاق می‌افتد که وجه سخت و نرم دارد مانند حملات سایبری که در وجه سخت جای می‌گیرد و تأثیرگذاری بر ارزش‌ها و معیارهای زندگی دیگران که در وجه نرم صورت‌بندی می‌شود. اما دسته دوم خارج از فضای سایبر روی می‌دهد که آن هم به وجه سخت و نرم تقسیم می‌شود. نای از کنترل بر سیستم‌های تبادل اطلاعات و جریان آزاد اطلاعات به‌عنوان وجه سخت و استفاده از فضای سایبر برای دیپلماسی عمومی در عرصه روابط خارجی و بین‌المللی کشور به‌عنوان وجه نرم یاد می‌کند.

ازآنجاکه فضای سایبر تمامی ابعاد زندگی را دربرگرفته؛ موضوع قدرت سایبری نیز تمامی حوزه‌های مرتبط با آن را دربرمی‌گیرد. قدرت سایبری در قلمرو فضای سایبر ملی ابعاد اقتصادی، فرهنگی، سیاسی، نظامی و حتی محیط زیستی دارد. قدرت سایبری در محیط پویا و پیچیده امروزی جهان، موجب افزایش نقش‌آفرینی در مدیریت فضای سایبر، دستیابی به امنیت ملی پایدار، توسعه سرمایه‌گذاری اقتصادی و افزایش نفوذ بین‌المللی خواهد شد. بنابراین هرقدر دولتی بتواند با استفاده از قدرت سایبری و ظرفیت‌های این پدیده به اهداف خود در سریع‌ترین و کم‌هزینه‌ترین راه دست پیدا کند، او را می‌توان به‌عنوان قدرت جهانی در نظر گرفت. کشوری که از قدرت سایبری بسیاری برخوردار باشد، می‌تواند دست به اقدام‌های زیادی بزند: می‌تواند از نظر اقتصادی سایر کشورها را تضعیف کند؛ می‌تواند اطلاعات سیاسی و نظامی را کارآمدتر از جاسوسی پیش‌دیجیتال جمع‌آوری کند؛ می‌تواند در گفتمان سیاست خارجی مداخله آنلاین کند؛ می‌تواند در زیرساخت‌های حیاتی دشمن نفوذ کند و باعث کاهش توانایی‌های جنگی دشمن شود. همه اینها را می‌توان از طریق استفاده هوشمندانه از فناوری دیجیتال و بدون استقرار نیروهای نظامی یا جاسوسان انسانی انجام دهد.

لذا ضروری و منطقی است که نه‌تنها قدرت‌های بزرگ، بلکه کشورهای کوچک‌تر، برای توسعه قدرت سایبری خود عجله کنند، به‌خصوص که هزینه پایین ورود، گمنامی و نامتقارن بودن در آسیب‌پذیری، باعث شده تا بازیگران کوچک‌تر در فضای سایبر نسبت به حوزه‌های سنتی‌تر سیاست جهانی ظرفیت بیشتری برای اعمال قدرت داشته باشند [۲۶].

داشتن منابع فیزیکی و غیرفیزیکی سایبری و تسلط فناورانه بر فضای سایبر شرط لازم برای قدرت سایبری است و تبدیل توانمندی‌های بالقوه به بالفعل با اتخاذ سیاست‌ها و راهبردهای مناسب و پدید آوردن آثار و نتایج مطلوب، برای کسب قدرت سایبری ضروری است. در فضای سایبر از ابزارهای غیرفیزیکی مانند سلطه اطلاعاتی، وضع قوانین و استانداردها و دیپلماسی سایبری، یا فیزیکی مانند انحصار فناوری زیرساخت و ارتباطات و تسلیحات سایبری برای اعمال قدرت استفاده می‌شود. به‌هرروی لازم است ابعاد و مؤلفه‌های قدرت سایبری چه در بعد ملی و چه در بعد نظامی را بازشناخت و برای آن شاخص‌ها و سنجه‌هایی تعیین کرد تا مشخص شود وضعیت قدرت سایبری جمهوری اسلامی ایران در جهان چگونه است. انجام این مهم مستلزم بررسی، تحلیل و تعیین ابعاد، مؤلفه‌ها، شاخص‌ها و سنجه‌های مورد نظر است. کما اینکه مقام معظم رهبری بر ارتقای جمهوری اسلامی ایران به قدرت سایبری در تراز قدرت‌های تأثیرگذار جهانی و برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه تأکید دارند.

جدول ۶. پیشنهاد توصیه سیاستی

ردیف	نوع توصیه		توصیه سیاستی	الزامات و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان‌بندی اجرا (کوتاه‌مدت، میان‌مدت و بلندمدت)	ملاحظات
	تداوم*	اصلاح**						
۱		**	تدوین استراتژی ملی قدرت سایبری	• تشکیل شورای راهبردی قدرت سایبری تحت نظارت شورای عالی فضای مجازی برای تدوین استراتژی • شناسایی اولویت‌های ملی در حوزه‌های زیرساختی، امنیتی، اقتصادی و نظامی	مرکز ملی فضای مجازی	وزارت ارتباطات و فناوری اطلاعات، ستاد کل نیروهای مسلح	–	–
۲		**	توسعه زیرساخت‌های بومی و کاهش وابستگی به فناوری خارجی	• ایجاد پارک‌های فناوری سایبری و مناطق ویژه اقتصادی برای استارتاپ‌های فناوری. • ارائه تسهیلات سرمایه‌گذاری و مشوق‌های مالیاتی به شرکت‌های دانش‌بنیان داخلی. • توسعه فناوری‌های پیشرفته مانند رایانش ابری بومی، هوش مصنوعی و پروتکل‌های امن	وزارت ارتباطات و فناوری اطلاعات	معاونت علمی و فناوری ریاست‌جمهوری، وزارت اقتصاد و دارایی	–	–
۳	*		تقویت امنیت سایبری و تاب‌آوری زیرساخت‌های حیاتی	• تشکیل کمیته‌های تخصصی برای ارزیابی و رتبه‌بندی سالیانه امنیت سایبری دستگاه‌ها. • توسعه سیستم‌های تشخیص و پاسخ به حملات سایبری	وزارت اطلاعات، سازمان پدافند غیرعامل	سازمان فناوری اطلاعات ایران		

ردیف	نوع توصیه		توصیه سیاستی	الزامات و قیود اجرایی	دستگاه متولی	دستگاه معین	زمان‌بندی اجرا (کوتاه‌مدت، میان‌مدت و بلندمدت)	ملاحظات
	تداوم*	اصلاح**						
۴	*		تقویت دیپلماسی سایبری و نقش‌آفرینی در هنجارسازی جهانی	• تشکیل کارگروه دیپلماسی سایبری در وزارت امور خارجه برای هماهنگی اقدام‌های بین‌المللی. • مشارکت فعال در مجامع جهانی مانند ITU، IGF و ICANN و امضای پیمان‌های سایبری. • تولید محتوای دیجیتال چندزبانه برای ترویج ارزش‌های اسلامی و فرهنگی ایران.	وزارت امور خارجه	مرکز ملی فضای مجازی، وزارت فرهنگ و ارشاد اسلامی		
۵		**	طراحی شاخص‌های بومی قدرت سایبری	• تشکیل کارگروه تخصصی با حضور دانشگاه‌ها، مراکز پژوهشی و دستگاه‌های اجرایی	مرکز ملی فضای مجازی	سازمان فناوری اطلاعات ایران، دانشگاه‌های برتر		
۶	*		ارتقای سواد سایبری عمومی و فرهنگ‌سازی	• طراحی برنامه‌های آموزشی همگانی در رسانه ملی، مدارس و دانشگاه‌ها. • تولید محتوای آموزشی در قالب اپلیکیشن‌ها، بازی‌های دیجیتال و پلتفرم‌های آنلاین. • برگزاری کمپین‌های ملی برای ترویج استفاده امن و اخلاق‌مدار از فضای مجازی	وزارت آموزش و پرورش، سازمان صداوسیما، وزارت فرهنگ و ارشاد اسلامی			

* تداوم یا تقویت آیتم‌ها یا اقدام‌ها
** اصلاح رویه‌ها یا ایجادسازوکارها
مأخذ: یافته‌های پژوهش.

منابع و مآخذ

[۱] نگری، آنتیونی. هارت، مایکل، امپراطوری. ۱۳۹۸، تهران: قصیده سرا.

[۲] مهدی، غیاثی، موج چهارم فضای مجازی. ۱۳۹۹، تهران: اندیشه احسان

[3] Chul-Han, B., What is Power? 2018: Polity.

[4] M. Lord, K.S., Travis America's Cyber Future: Security and Prosperity in the Information Age. Vol. 1. 2011: Center for a New American Security.

[۵] باری، هیندس، گفتارهای قدرت از هابز تا فوکو. ۱۳۹۰، تهران: شیرازه.

[۶] معصومه، محمدیاری، مقایسه مفهوم قدرت در آراء هابز و فوکو. اطلاعات حکمت و معرفت، بهمن ۱۳۹۱. ۷(۱۱).

[7] Koopman, C. Why Foucault's Work on Power Is More Important Than Ever. 2017; Available from: https://aeon.co/essays/why-foucaults-work-on-power-is-more-important-than-ever.

[۸] اشرف نظری، علی، چرخش در مفهوم قدرت: تصور فوکویی و پسافوکویی از قدرت. فصلنامه سیاست، مجله دانشکده حقوق و علوم سیاسی، پاییز ۱۳۹۰. ۴۱(۳).

[9] Deleuze, G., Difference and Repetition. 1995: Columbia University Press.

[۱۰] میشل، فوکو، امنیت، قلمرو، جمعیت. ۱۳۹۹، تهران: چشمه.

[۱۱] یونگ، چول هان، روان سیاست. ۱۳۹۸، تهران: لوگو.

[۱۲] میشل، فوکو، تئاتر فلسفه. ۱۳۹۱، تهران: نی.

[۱۳] نگری، آنتونیو. دلوز، ژیل. هارت، مایکل. بازگشت به آینده. ۱۳۸۶، تهران: گام نو.

[14] Landazuri, M.C.O., Psychopolitics and power in contemporary political thought. journal of political power, Feb 2019. 12(1).

[۱۵] زابلی‌زاده، اردشیر. قدرت بازدارندگی در فضای سایبر. دوفصلنامه علمی پژوهشی رسانه و فرهنگ، بهار و تابستان ۱۳۹۷. ۸(۱).

[16] Bell , D., An introduction to cyberculturse. 2001, USA: Routledge.

[17] D. Kramer, F.S., Stuart H; Wentz, Larry K, Cyberpower and National Security. 2009: University of Nebraska Press, Potomac Books.

[۱۸] وبستر، فرانک، نظریه‌های جامعه اطلاعاتی. ۱۳۸۰، تهران: قصیده سرا.

[19] Michael, B., Cyberspace: First Steps. 1992: Cambridge, MIT Press.

[۲۰] اسلامی، روح‌الله. رهایی یا انقیاد: فلسفه سیاسی تکنولوژی اطلاعات در قرن بیستم. ۱۳۹۳، تهران: تیسا.

[21] Sheldon, J.B., Deciphering Cyberpower: Strategic Purpose in Peace and War. Strategic Studies Quarterly, Summer 2011. 5(2): p. p.95-112.

[۲۲] جوزف، نای، قدرت سایبری. ۱۳۹۲، تهران: نی.

[23] Spade, J.M., China's Cyberpower and America's National Security. 2012, Carlisle Barracks, PA: US Army War College.

[24] Champion, T. Are We Living in a Post-Panoptic Society? 2019; Available from: https://www.e-ir.info/2019/04/16/are-we-living-in-a-post-panoptic-society/.

[25] Sigholm, J., Non-State Actors in Cyberspace Operations. Journal of Military Studies, 2016.

[۲۶] نصرت آبادی، جمشید. لشکریان، حمیدرضا. مردانی شهربابک، محمد. موحدی‌صفت، حمیدرضا. ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران. فصلنامه امنیت ملی, بهار ۹۸. ۹(۳۱).

گزیده سیاستی

استراتژی ملی قدرت سایبری با تمرکز بر زیرساخت بومی، توان تهاجمی/تدافعی تدوین شود. همچنین دیپلماسی سایبری تقویت، بخش خصوصی حمایت و وابستگی خارجی کاهش یابد و سواد سایبری عمومی ارتقا و شاخص‌های بومی طراحی شود.

مرکز پژوهش های مجلس شورای اسلامی

تهران، خیابان پاسداران، روبروی پارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۵۸۵۵-۱۵۸۷۵ پست الکترونیک: mrc@majles.ir

وب‌سایت: rc.majles.ir