قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر

خداداد هلیلی[1]
محمدرضا ولوی[2]
محمدرضا موحدی صفت[3]
مسعود باقری[4]

تاریخ دریافت: ۱۳۹۷/۰۱/۱۸ تاریخ پذیرش: ۱۳۹۷/۰۴/۰۹

چکیده:

در طول تاریخ، همواره قدرت‌طلبی و افزون‌خواهی، منشأ رقابت، تخاصم و تنازع بین دولت‌ها بوده است. برخورداری از منابع قدرت، جایگاه و نفوذ هر کشور در تعاملات جهانی را نشان می‌دهد. در دوران معاصر، جهت‌گیری اولویت‌های راهبردی کشورها، برای نیل به قدرت فائقه، به سمت بهره‌برداری از فضای سایبر تغییریافته و فناوری‌های پیشرفته سایبری، زمینه‌ساز تجدید بنای قدرت در قالب قدرت سایبری شده است. از جمله پیامدهای این تغییر بنیادین، تأثیر آن بر امنیت ملی کشورهاست. فرآیند جهانی‌شدن، ظهور جوامع شبکه‌ای و حملات سایبری سازمان‌یافته فرامرزی، از چالش‌های جدی و نوین در دستیابی و حفظ امنیت ملی است. هدف اصلی این مقاله مفهوم‌سازی قدرت سایبری با رویکرد فرکتالی و تأثیر آن بر امنیت ملی در فضای سایبر است. در این رویکرد، قدرت سایبری دارای تمامی ویژگی‌های قدرت ملی است. بدین منظور، مؤلفه‌ها و متغیرهای مؤثر در قدرت سایبری و امنیت ملی احصاء شده و رابطه میان آن‌ها تبیین شده است. تحقیق از نظر هدف کاربردی- توسعه‌ای، از نظر ماهیت از نوع توصیفی- همبستگی و از نظر روش تجزیه‌وتحلیل داده‌ها، آمیخته (کیفی و کمی) است. جامعه آماری شامل ۶۰ نفر از خبرگان و صاحب‌نظران فضای سایبر و امنیت ملی است که پس از توزیع پرسشنامه و جمع‌آوری آن، با استفاده از نرم‌افزار اسمارت پی. ال. اس نسبت به تجزیه‌وتحلیل آماری داده‌های کمی اقدام شد. نتایج این تحقیق نشان می‌دهد؛ داشتن منابع، تجهیزات و فناوری‌های سایبری، شرط لازم برای دستیابی به امنیت ملی است. بااین‌وجود، درک دقیق نخبگان و سیاست‌گذاران در تدوین راهبردهای مناسب، پیش‌بینی تهدیدات و فرصت‌های بالقوه و بالفعل برای طرح‌ریزی قدرت سایبری ضروری است.

کلیدواژه‌ها: قدرت سایبری، امنیت ملی، قدرت ملی، رویکرد فرکتالی

۱- دانشجوی دکترای مدیریت راهبردی امنیت سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول) - kh.halili@sndu.ac.ir
۲- دانشیار و عضو هیئت علمی دانشگاه صنعتی مالک اشتر- valavi@mut.ac.ir
۳- استادیار و عضو هیئت علمی دانشگاه عالی دفاع ملی- movahedi@sndu.ac.ir
۴- استادیار و عضو هیئت علمی دانشگاه امام حسین (ع) -Mbagheri@ihu.ac.ir

مقدمه:

مفاهیم «قدرت» و «امنیت» در حوزه‌های علـوم طبیعـی، اجتمـاعی، سیاسـی، نظـامی، روانشناسـی، حقوق و فلسفه، همواره مورد توجه اندیشمندان قرار گرفته است. از منظر اجتماعی و سیاسی، ایـن مفاهیم با شکل‌گیری دولت‌ها و اهمیت یـافتن نقـش آن‌هـا در کسـب قـدرت و تـأمین امنیـت در محدوده جغرافیایی کشورها، در قالب قدرت ملی و امنیت ملـی مطـرح مـی‌شـود. در هـر کشـور، قدرت بر مبنای ایدئولوژی، ارزش‌ها، معیارها و هنجارهای مورد توافـق در اختیـار حاکمیـت قـرار گرفته و مشروعیت و مقبولیت آن توسط جامعه به رسمیت شناخته می‌شود. امنیت ملی نیز از دیگر موضوعات اساسی و حائز اهمیت در صیانت از منافع ملی هر کشور و از وظایف دولت‌هاست.

دو مفهوم قدرت ملی و امنیت ملی در ابعاد سیاسـی، اجتمـاعی، فرهنگـی، اقتصـادی و دفـاعی دارای وجوه مشترک و ویژگی‌های مشابهی هستند که در ادبیات روابط بین‌الملـل از منظـر ذهنـی و انتزاعی و یا عینی و تجربی قابل بررسی است. در سه دهـه اخیـر، تغییـرات شـگرف فنـاوری‌هـای فضای سایبر این مفاهیم را نیز با چالش مفهـومی و برداشـت‌هـای متفـاوت مواجـه نمـوده اسـت. اندیشمندان معاصر با معرفی تعـاریف، اصـطلاحات و شـاخص‌هـای نـوین، سـعی در توصـیف و سنجش قدرت ملی و امنیت ملی نمـوده‌انـد. ظهـور مفـاهیمی ماننـد قـدرت سـایبری، هرچنـد بـا پدیده‌هایی مانند پراکندگی قدرت همراه بوده و امنیت ملی را نیز تحت تأثیر قرار داده است؛ اما راه برون‌رفت از بحـران‌هـا و چـالش‌هـای ایجـاد شـده نیـز، از درون فضـای سـایبر و بهـره‌گیـری از فناوری‌های سایبری می‌گذرد. ویژگی‌های قدرت سایبری مشابه قدرت ملـی و تکـرار پدیـده‌هـای قدرت ملی در فضای سایبر است. ازاین‌رو در این تحقیق، بررسی و مفهوم‌سازی قدرت سـایبری و امنیت ملی در فضای سایبر، مورد توجه قرار گرفته است.

جذابیت فناوری‌های نوین در فضای سایبر، زمینه شکل‌گیری جوامع اطلاعاتی با جمعیتی حتـی بیشتر از بزرگ‌ترین کشورهای دنیا و کمرنـگ شـدن مرزهـای جغرافیـایی شـده و کـاهش قـدرت دولت‌ها را به همراه داشته است. کشورهای صـنعتی و پیشـرو، بـه خـاطر پیشـتاز بـودن و داشـتن ابزارهای مهار، کنترل و مدیریت این فضاء، با چالش‌های کمتری در امنیت ملی مواجه هسـتند؛ امـا در کشورهای وابسته و پیرو، همواره دغدغه‌هـایی ماننـد تهدیـد بقـاء سیاسـی، اسـتحاله فرهنگـی، تضعیف وضعیت اقتصادی به‌عنوان چالش‌های تهدیدکننده امنیت ملی وجود دارد؛ بنابراین تسلط بر فضای سایبر و دستیابی به قدرت سایبری برای ارتقاء امنیت ملی امری ضروری به نظر می‌رسد. در

این مقاله، با بررسی مفهوم نوظهور قدرت سایبری، به بررسی تأثیر آن روی امنیت ملی پرداخته‌شده است.

بیان مسئله: قدرت سایبری، همچون سایر گونه‌های قدرت، از منظر پیامد به معنای قابلیت تأثیر بر رفتار دیگران برای کسب نتایج مطلوب است. این تأثیرگذاری می‌تواند در فضای سایبر یا از طریق فضای سایبر صورت گیرد. در دوران معاصر، ظهور مفاهیمی مانند، قدرت سخت، قدرت نرم و قدرت هوشمند بیانگر جابجایی و چرخش نشانگر قدرت به‌سوی قدرت سایبری است. به خاطر رابطه متقابل امنیت ملی با قدرت؛ تغییر بنیادین در مفهوم و ویژگی‌های قدرت در فضای سایبر، مخاطرات و تهدیدات جدیدی برای امنیت ملی به وجود آورده و از طرف دیگر، فناوری‌های مرتبط با فضای سایبر را به عاملی برای کسب قدرت و تأمین امنیت ملی تبدیل نموده است. این مسئله حاکی از عمق نفوذ فضای سایبر در تمامی حوزه‌های راهبردی کشور است؛ بنابراین دغدغه اصلی شکل‌گیری این تحقیق، تبیین نقش و جایگاه قدرت سایبری به‌عنوان عاملی اساسی برای مقابله با تهدیدات عینی و ذهنی فضای سایبر و ارتقاء امنیت ملی است.

قدرت سایبری، نوع متأخر قدرت است که مقام معظم رهبری در بند سوم از حکم اعضای دوره دوم شورای عالی فضای مجازی، در شهریور ۱۳۹۴ با اشاره به «ارتقای جمهوری اسلامی ایران به قدرت سایبری در تراز قدرت‌های تأثیرگذار جهانی» به‌طور صریح بر آن تأکید فرمودند. در سیاست‌های ابلاغی و اسناد بالادستی بر دستیابی به سطح مطلوبی از قدرت و امنیت تأکید شده است. برنامه‌ریزی راهبردی و سرمایه‌گذاری در این حوزه، مستلزم شناخت و درک عمیق سیاست‌گذاران و تصمیم‌گیران از ظرفیت‌های بالقوه و بالفعل و پیامدهای این پدیده نوظهور است. بااین‌وجود، به نظر می‌رسد این مسئله مهم و کلیدی، در هیاهوی توسعه تقلیدگونه فضای سایبر با غفلت راهبردی مواجه شده است. شناخت اهمیت و ویژگی‌های قدرت سایبری با معرفی رویکرد فرکتالی، تبیین چالش‌های فراروی امنیت ملی در فضای سایبر و بررسی نقش قدرت سایبری در افزایش قدرت ملی و تأمین امنیت ملی از جمله موضوعاتی است که در این تحقیق به آن پرداخته‌شده است.

اهمیت و ضرورت تحقیق: گستره فضای سایبر هر روز فراگیرتر می‌شود و در پیش گرفتن رویکرد انفعالی و تدافعی با پدیده‌های مهمی مانند قدرت و امنیت در این فضاء، حفظ و بقای دولت‌ها را تهدید می‌کند؛ بنابراین بازبینی و شناسایی عوامل مؤثر در ارتقاء قدرت ملی و رابطه آن

با امنیت ملی در فضای سایبر، از اهمیت بالایی برخوردار است. چراکه موجب ترغیب سیاست‌گذاران در تغییر پارادایم فکری و جهت‌گیری مناسب برای در دست گرفتن ابتکار عمل در فضای سایبر خواهد شد. در این تحقیق، با در نظر گرفتن دیدگاه فرکتالی برای قدرت سایبری بر هم‌ارز بودن آن با قدرت ملی تأکید شده است.

در جمهوری اسلامی ایران، با اینکه فناوری اطلاعات و ارتباطات از ضرورت‌های اجتناب‌ناپذیر توسعه و کسب قدرت محسوب می‌شود؛ اما به نظر می‌رسد روند این توسعه، با مؤلفه‌های تثبیت‌کننده امنیت ملی کشور هم‌راستا نیست و با چالش‌های زیادی همراه است. پدیده‌های فضای سایبر، نگاشتی از پدیده‌های جهان واقعی است و عناصر قدرت نیز در فضای سایبر، مشابه عناصر قدرت ملی فرض می‌شود. ازاین‌رو در این تحقیق، مفهوم‌سازی قدرت سایبری مبتنی بر رویکرد فرکتالی مورد توجه قرار گرفته است. در بسیاری از مقاطع زمانی، با غالب شدن دیدگاه تهدید محور توسط سیاست‌گذاران، امنیتی نمودن فضای سایبر برجسته شده است. این مسئله ناشی از فقدان دیدگاه آینده‌نگر و برآورد نادرست از منابع و توانمندی‌های مرتبط با قدرت سایبری است که ضرورت پرداختن به این موضوع را روشن می‌سازد.

هدف اصلی: شناخت قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر و اهداف فرعی:

مفهوم‌سازی رویکرد فرکتالی قدرت سایبری

احصاء مؤلفه‌ها و متغیرهای قدرت سایبری و امنیت ملی در فضای سایبر

بررسی تأثیر قدرت سایبری بر امنیت ملی در فضای سایبر است.

سؤال اصلی: قدرت سایبری از منظر فرکتالی چه ویژگی‌هایی دارد چه تأثیری بر امنیت ملی در فضای سایبر دارد؟ و سؤالات فرعی:

در رویکرد فرکتالی قدرت سایبری چه ویژگی‌هایی دارد؟

مؤلفه‌ها و متغیرهای قدرت سایبری و امنیت ملی در فضای سایبر کدامند؟

قدرت سایبری چه تأثیری بر امنیت ملی در فضای سایبر دارد؟ می‌باشد.

مبانی نظری

پیشینه تحقیق: مفاهیم قدرت و امنیت از واژه‌های کلیدی و محوری است که در ابعاد فردی، اجتماعی، سیاسی، اقتصادی و نظامی همواره مورد کنکاش نظریه‌پردازان قرار گرفته است. این مفاهیم در مکاتب فکری کلاسیک، مدرن، نوین و اسلامی، در سطوح داخلی/ خارجی، ملی/

بین‌المللی، منطقه‌ای/ فرا منطقه‌ای توسط اندیشمندان بررسی شده و تحقیقات و آثار علمی زیادی در مورد قدرت، قدرت ملی، امنیت و امنیت ملی منتشر شده است. تحقیقات مرتبط انجام شده داخلی و خارجی، تفاوت دیدگاه در مورد عناصر قدرت سایبری و امنیت ملی را نشان می‌دهد.

سلطانی‌نژاد در مقاله خود بررسی مفهومی تأثیر فناوری اطلاعات و ارتباطات (فاوا) بر امنیت ملی را نگاهی تجویزی می‌داند که تأثیرات ملموس آن در یک کشور خاص را در برنمی‌گیرد. علاوه بر آن چالش‌های امنیت ملی در کشورهای صنعتی پیشرو مانند ایالات‌متحده به خاطر وابستگی به زیرساخت‌های فاوا از نوع نظامی است؛ درحالی‌که در کشورهای جهان سوم به خاطر آسیب‌پذیری نظام‌های سیاسی چالش‌های فرهنگی، سیاسی و اجتماعی مربوط به امنیت ملی از اهمیت بالاتری برخوردار است. در این تحقیق، افزایش مهارت شهروندان و سمت‌گیری آن‌ها در تقابل با دولت، اقدامات بازیگران خارجی، تهدید ارزش‌های ملی و تضعیف انسجام ملی از جمله چالش‌های امنیت ملی کشور در فضای سایبر توصیف شده است (سلطانی نژاد و همکاران: ۱۳۹۲).

از دیدگاه حسن‌بیگی و کولیوند تهدیدات نوین امنیت ملی در فضای سایبر شامل تروریسم سایبری، خرابکاری، جاسوسی و براندازی است. در این تحقیق، مدیریت تحولات برآمده از توسعه فناوری اطلاعات و ارتباطات برای تأمین امنیت ملی در ابعاد سیاسی، اجتماعی، فنی، ساختاری، ظرفیت‌سازی و قوانین و مقررات اولویت‌بندی شده است. نتایج این تحقیق نشان می‌دهد بعد اجتماعی و سیاسی فضای سایبر در براندازی و بعد فنی در خرابکاری، موجب ایجاد چالش در امنیت ملی می‌شوند (حسن‌بیگی و کولیوند: ۱۳۹۶).

در مقاله توحیدی و همکاران، رابطه قدرت با امنیت بررسی‌شده و برداشتن یک رابطه مستحکم و ملموس بین مؤلفه‌های امنیت و قدرت در کشور تأکید شده است. نتایج این تحقیق نشان می‌دهد، بین قدرت و امنیت یک رابطه دوسویه وجود دارد. احساس امنیت موجب افزایش حس قدرت و احساس قدرت موجب ازدیاد حس امنیت می‌گردد؛ بنابراین مهار و افزایش قدرت و امنیت در یک کشور می‌تواند به ارتقای جایگاه مردم و افزایش سطح رضایت‌مندی آن‌ها و درنهایت دفع تهدیدات و رفاه و آسایش جامعه منجر شود (توحیدی و همکاران: ۱۳۹۶).

کرامر فرانکلین و همکاران در کتاب قدرت سایبری و امنیت ملی، نقش قدرت سایبری در سطوح تاکتیکی، عملیاتی و راهبردی را مورد بررسی قرار داده‌اند. نتایج این تحقیق نشان می‌دهد جرائم سایبری، تروریسم سایبری، نحوه حاکمیت اینترنت و امنیت سایبری از چالش‌های راهبردی

امنیت در سطوح ملی و بین‌المللی است که با توجه به پویایی فضای سایبر از طریق اقدامات نظامی سایبری و بازدارندگی قدرت سایبری می‌تواند برطرف شود (*Franklin et al, 2010*).

در زمینه رویکرد فرکتالی در علوم اجتماعی، پراویر مالیک در کتاب سازمان‌های فرکتالی با مقایسه تفکر فرکتالی نسبت به تفکر سلسه‌مراتبی در سازمان‌ها، ویژگی‌های پارادایم فرکتالی از جمله خودسازمان‌دهی، خود اقدامی و وحدت بین اجزاء یک سازمان (در عین کثرت) برای دستیابی به یک هدف یکسان را مطرح نموده است که می‌تواند در رویکرد فرکتالی به قدرت سایبری و تأثیر آن بر امنیت ملی در فضای سایبر مورد توجه قرار گیرد (*Pravir Malik،2015*).

مروری بر تحقیقات انجام‌شده، تأثیر متقابل قدرت و امنیت در فضای سایبر را نشان می‌دهد. در سطح ملی، قدرت سایبری و امنیت ملی از مفاهیم مهم و مورد توجه سیاست‌گذاران و تصمیم‌گیران است که با توجه به نفوذ گسترده فضای سایبر، نیازمند مفهوم‌سازی و بازبینی مجدد هستند. در این تحقیق، با ارائه رویکرد فرکتالی برای قدرت سایبری و احصاء مؤلفه‌ها و متغیرهای آن به بررسی تأثیر قدرت سایبری بر امنیت ملی در فضای سایبر پرداخته‌شده است؛ که وجه تمایز این تحقیق با تحقیقات مرتبط است.

مفاهیم و متغیرهای تحقیق:

در این تحقیق، تأثیر قدرت سایبری بر امنیت ملی بررسی شده است. بدین منظور قدرت سایبری، متغیر مستقل و امنیت ملی متغیر وابسته تحقیق در نظر گرفته شده‌اند. این دو متغیر اصلی، از منظر ویژگی‌ها، انواع و منابع مورد توجه اندیشمندان قرار گرفته است که ارائه یک تعریف کلی از این دو اصطلاح را دشوار می‌سازد. در این مقاله، پس از بررسی این مفاهیم در مراجع مختلف، تعاریف عملیاتی زیر برای این دو مفهوم و نیز رویکرد مورد استفاده برای قدرت سایبری ارائه می‌شود:

قدرت سایبری: توانایی به‌کارگیری منابع، ظرفیت‌ها و قابلیت‌های مبتنی بر فضای سایبر به‌منظور پشتیبانی از قدرت ملی و دستیابی به اهداف راهبردی در فضای سایبر و خارج از آن است.

امنیت ملی: وضعیت و شرایطی است که یک کشور، در بعد عینی علی‌رغم وجود تهدید، خود را قادر به حفظ منافع و ارزش‌های اساسی بداند و در بعد ذهنی نیز از هجوم (فیزیکی و غیر فیزیکی) به بنیان‌های ملی خود، هراسی نداشته باشد.

رویکرد فرکتالی: رویکردی است که در آن، عملکرد یک پدیده جزئی، به‌صورت نگاشتی از یک پدیده کلان با ویژگی‌های مشابه بررسی می‌شود.

قدرت و قدرت ملی: در یک نگاه کلی، قدرت به معنی استفاده از منابع مادی و معنوی به‌منظور اعمال اراده و تأثیرگذاری بر دیگران و ایجاد رفتار مطلوب توسط آن‌هاست؛ به‌طوری که در فقدان آن، طرف مقابل مجبور، متمایل یا مشتاق به اطاعت نباشد. در تقسیم‌بندی انواع قدرت، دیدگاه‌های مختلفی وجود دارد. نبوی در کتاب فلسفه قدرت آن‌ها به سه دسته الهی، ماشینی و انسانی تقسیم کرده است. در این دیدگاه، ابعاد اقتصادی، نظامی، سیاسی، دینی و فرهنگی زیرمجموعه قدرت انسانی است (نبوی، ۱۳۹۵: ۱۲۲).

در مکتب اسلام، قدرت اصلی از آن خداست و تمامی قدرت‌ها در طول قدرت الهی و در پرتو مشیت او قرار می‌گیرد. قدرت امانتی در اختیار انسان برای هدایت جامعه در مسیر تحقق اهداف صحیح سیاسی، برپایی عدالت و تأمین مصالح اجتماعی و کسب کمالات اخلاقی است و هدف غایی نیست (اسکندری و دارابکلایی،۱۳۹۱: ۱۰۴).

ریموند دوال و مایکل بارنت در کتاب «قدرت و سیاست در عرصه بین‌الملل» انواع قدرت را به چهار دسته اجباری (استفاده از منابع مادی و هنجاری یک بازیگر برای تحت تأثیر قرار دادن وضعیت و کنش‌های بازیگر دیگر)، ساختاری (توانایی تأثیرگذاری بر نتایج با استفاده فناوری و روابط ساختاری)، نهادی (کنترل بازیگر دیگر از طریق قواعد و رویه‌های خاص اجتماعی و نهادهای رسمی و غیررسمی) و مولد (تولید گفتمان، سوژه‌ها و معانی خاص برای جهت‌دهی روابط بین عوامل قدرت در جامعه) تقسیم‌بندی کرده‌اند (*Barnett, & Duvall, 2005: 75*).

برخی نیز مانند جوزف نای قدرت را به سه دسته نرم (کسب نتیجه مطلوب از طریق جاذبه و بدون استفاده از اجبار یا تطمیع)، سخت (توانایی تغییر رفتار دیگران از طریق اجبار یا تطمیع) و هوشمند (توانایی ترکیب قدرت نرم و قدرت سخت) تقسیم کرده‌اند (*Nye, 2011*).

قدرت ملی، وزن یک واحد سیاسی را در معادلات بین‌المللی را نشان داده و جهت‌گیری سیاست خارجی کشورها را تحت تأثیر قرار می‌دهد. در یک تعریف کلی، قدرت ملی شامل مجموعه‌ای از توانایی‌ها و ظرفیت‌های کشور به‌منظور حفظ ارزش‌ها و منافع ملی یک کشور است. منابع قدرت ملی شامل منابع ثابت (منابعی که از اراده رهبران سیاسی و گروه‌های اجتماعی خارج است مانند جغرافیای سیاسی، منابع طبیعی، فرهنگ سیاسی، روحیه ملی) و منابع متغیر (فرایند حاکم بر نظام بین‌الملل و برداشت و اراده نخبگان سیاسی حاکم، مانند فناوری‌های پیشرفته، تنظیم روابط خارجی، جذب یا طرد اندیشه‌ها) تقسیم می‌شود (اسکندری و دارابکلایی، ۱۳۹۱: ۲۹).

تعامل و همسویی مؤلفه‌های تشکیل‌دهنده قدرت، با مبانی ارزشی و آرمان‌های یک کشور موجب هم‌افزایی و همگرایی قدرت ملی خواهد شد. به همین نسبت اتکای این مؤلفه‌ها بر ارزش‌ها و هنجارهای وارداتی، ضعف و واگرایی آن‌ها را در بر خواهد داشت. با این حال، کشورها برای حفظ موجودیت خود و نقش‌آفرینی مؤثر در عرصه جهانی ناگزیر از انعطاف‌پذیری لازم برای تطبیق خود با محیط بین‌الملل در مقاطع زمانی مختلف هستند.

برای سنجش قدرت ملی کشورها، باید عناصر کمی و کیفی مرتبط با آن شناسایی شوند. زرقانی با مقایسه روش‌ها و مدل‌های مختلف، مؤلفه‌های کمی و کیفی مؤثر در قدرت ملی را بررسی نموده است (زرقانی: ۱۳۸۹). در ارزیابی و سنجش قدرت ملی، علاوه بر شناخت عوامل کیفی و کمی مؤثر، رابطه میان عناصر شکل‌دهنده قدرت باید مدنظر قرار گیرد. قدرت ملی حاصل ترکیب و جمع جبری وجوه مثبت و منفی عناصر و بنیان‌های قدرت یک کشور است که از پویایی برخوردار بوده و نسبت به ملت‌ها و کشورهای دیگر قابل فهم و درک است.

علاوه بر مفاهیم قدرت و قدرت ملی، مفاهیمی مانند اقتدار، نفوذ و هژمونی نیز در علوم اجتماعی و سیاسی از مشتقات قدرت محسوب می‌شوند. اقتدار به معنای قدرت مشروع و مقبول نظام حاکم بر یک کشور، نفوذ به معنای تسلط و حاکمیت پنهانی و وادار نمودن طرف مقابل به انجام عملی برخلاف میل و حتی بدون اطلاع وی (ره پیک و دیگران: ۱۳۸۷) و هژمونی به معنای تلاش برای دستیابی به سلطه ایدئولوژیک و فرهنگی بدون استفاده از زور و اجبار و با جلب توجه و متقاعد کردن طرف مقابل برای تن دادن به رهبری اعمال کننده قدرت در زمینه‌های فرهنگی و اجتماعی استفاده می‌شود (علی بابایی، ۱۳۹۱: ۶۷).

امنیت و امنیت ملی: مفهوم امنیت در طول زمان، در معرض برداشت‌های هرمنوتیک قرار گرفته است. تفسیرهای ذهنی/ عینی، سلبی/ ایجابی، نرم/ سخت و نسبی/ مطلق، نمونه‌ای از تلاش اندیشمندان برای دستیابی به درکی یکسان از این مفهوم است (شایگان: ۱۳۹۱). از دیدگاه قیصری، تغافل یا ناتوانی در ارائه تبیینی جامع و مانع از مقوله امنیت توسط مکاتب مختلف، عرصه را برای ظهور نظریات و مکاتب جدید باز گذاشته است. در مکاتب امنیتی علاوه بر چگونگی تضمین امنیت، در مورد چرایی امنیت و نقش نخبگان و تحلیل‌گران مسائل امنیتی در کشف و تأمین امنیت نیز بحث می‌شود (قیصری: ۱۳۹۳). سیر تحول مفهوم امنیت و تعبیرهای مختلف از آن نشان می‌دهد امنیت وابسته به زمان و زمینه مشخصی است؛ با این حال برداشت جدید از مفهوم امنیت لزوماً به معنای فراموشی و عدم به‌کارگیری مفاهیم قبلی نیست.

امنیت ملی از مشتقات امنیت است که در مرزهای جغرافیایی یک کشور به‌صورت امنیت داخلی (مصونیت بنیان‌های ایدئولوژیک مکتب حاکم و حفظ حاکمیت) و امنیت عمومی (حفظ حقوق و مصالح افراد، گروه‌ها و نهادهای اجتماعی) تعریف شده است. امنیت ملی معادل فقدان تهدید عینی و ذهنی علیه بنیان‌های حیاتی و مشروعیتی یک ساختار سیاسی و ایجاد بستر مناسب حیات، ترقی رفاه یا حتی نفوذ است (غرایاق زندی، ۱۳۹۰: ۲۸).

در تحقیقات انجام‌شده برای شناخت مفهوم امنیت ملی مباحث ذهنی، فلسفی و انتزاعی یا مؤلفه‌ها و مصادیق عینی و تجربی آن توسط اندیشمندان مختلف مورد توجه قرار گرفته است. در تلاش برای مفهوم‌سازی امنیت ملی از منظر تاریخی، خلیلی با تقسیم‌بندی جوامع به چهار دسته بدوی (سنتی)، مدنی (کلاسیک)، ملی (مدرن)، جهانی (فرا مدرن: جامعه فرا صنعتی و شبکه مبتنی بر فناوری اطلاعات و ارتباطات) گفتمان‌های امنیت ملی در هر دوره را بررسی کرده است (خلیلی: ۱۳۸۳). این گفتمان مرکز ثقل امنیت را از دولت به انسان و از ملی به جهانی تغییر می‌دهد که هرکدام تبعات و چالش‌های خاصی به همراه دارند.

امنیت ملی علاوه بر وابستگی به مفاهیمی مانند تهدید، قدرت و صلح، با منافع ملی نیز رابطه تنگاتنگی دارد به‌طوری‌که دستیابی به منافع ملی تنها در سایه امنیت ملی محقق خواهد شد. در بسیاری از منابع، امنیت ملی با مصادیقی مانند استقلال، ثبات سیاسی و حفاظت از تمامیت ارضی و منافع ملی در برابر تهدیدات خارجی مرتبط است؛ ازاین‌رو در هر کشور با توجه به منافع و ارزش‌های ملی، ایدئولوژی نظام سیاسی حاکم و نحوه تعامل با دیگر کشورها، تعریفی خاصی از امنیت ملی صورت می‌گیرد.

بوزان در کتاب «مردم، دولت‌ها و هراس»، تلفیقی از رویکرد واقع‌گرایانه امنیت ملی (مبتنی بر مفهوم قدرت) و رویکرد آرمان‌گرایانه (مبتنی بر مفهوم صلح) را ارائه داده است. وی معتقد است امنیت ملی از مؤلفه‌های عینی، مانند مؤلفه‌های اقتصادی (تولید ثروت)، سیاسی (نهادهای مسلط در حوزه قدرت)، زیست‌محیطی (صیانت از فضای طبیعی) و نظامی (استحکامات دفاعی و هجومی و بازدارندگی رقبا) تشکیل‌شده است و در صورت بروز تهدید برای هرکدام از این مؤلفه‌ها، دولت به‌عنوان بازیگر اصلی وارد عمل شده و با امنیتی کردن امور عادی، مبادرت به جلب منابع مالی و توجه اجتماعی می‌کند (نصری: ۱۳۹۰).

با مروری بر تحقیقات انجام‌شده در مورد امنیت ملی چند ویژگی زیر برای امنیت ملی مشخص می‌شود. این ویژگی‌های متضاد، منشأ دیدگاه‌های متناقض به امنیت است. اولویت‌بندی هرکدام از وجوه امنیت از مسائل راهبردی هر کشور و زمینه‌ساز جهت‌دهی سیاست‌های کلان است. برجسته کردن یک ویژگی یا غافل ماندن از ویژگی مقابل، ممکن است موجب غفلت راهبردی در تصمیم‌گیری مناسب را به همراه داشته باشد.

ذهنی– عینی: این ویژگی رابطه مستقیمی با تهدید دارد. تلقی عینی یا ذهنی از امنیت بستگی به نوع نگرش در مورد تهدید دارد. امنیت عینی در واقع برونداد امنیت ذهنی است. ممکن است با وجود تهدیدات قابل مشاهده و عینی، افراد یک کشور احساس امنیت کنند یا هر اقدامی از طرف دیگر کشورها در نظر سیاست‌گذاران توطئه و تهدید محسوب شود.

سلبی– ایجابی: در دیدگاه سلبی، امنیت معادل فقدان تهدید است و فقدان تهدید نیز از طریق انباشت قدرت سخت مانند دارایی‌های اقتصادی، تسلیحات و نیروی نظامی جبران می‌شود. در دیدگاه ایجابی کسب امنیت از طریق توانایی برقراری تعامل با دیگران و پایبندی به منافع مشترک تأمین می‌شود.

علّی – معلولی: این وجه از امنیت رابطه آن با مفهوم قدرت را نشان می‌دهد. بین امنیت و قدرت رابطه دوطرفه و منطقی وجود دارد. امنیت موجب ارتقاء قدرت می‌شود و قدرت نیز در افزایش امنیت تأثیرگذار است؛ بنابراین امنیت ملی می‌تواند علّت دستیابی به قدرت یا معلول آن باشد و برعکس.

نسبی– مطلق: امنیت ملی امری نسبی است. کنترل و مدیریت همه عوامل تأثیرگذار بر امنیت ملی و رسیدن به امنیت مطلق در جهان امروزی ادعایی دست‌نیافتنی و غیرقابل تصور است.

تحول در مفاهیم وابسته و مرتبط با امنیت ملی از جمله تهدید و قدرت، تعریف امنیت ملی را از اتکای آن به قدرت نظامی در دوران پس از جنگ سرد خارج نموده است در دوران معاصر، لزوم ایجاد توازن در انواع و منابع قدرت برای دستیابی و حفظ امنیت ملی همه‌جانبه بیش‌ازپیش، ضروری به نظر می‌رسد.

قدرت سایبری: روند تکامل منابع و عوامل قابل‌سنجش در قدرت، در دوره‌های زمانی مختلف از تجهیزات نظامی پیشرفته به تسلیحات هسته‌ای و سپس منابع قدرت در فضای سایبر تغییر یافته است. امروزه استفاده از تسلیحات و زرادخانه‌های سایبری (به‌جای هسته‌ای)، توسعه اقتصادی از

طریق فضای سایبر (به‌جای تکیه بر منابع تجدید ناپذیر) و اعمال نفوذ توسط رسانه‌های سایبری به شکل گسترده‌ای به‌عنوان منابع قدرت سایبری استفاده می‌شود؛ بنابراین قدرت سایبری موجب هم‌افزایی و توسعه فراوان در قدرت می‌شود.

قدرت سایبری از مفاهیم نوظهور قدرت در سال‌های اخیر است. این مفهوم در سطح کشور، اولین بار به‌طور صریح توسط مقام معظم رهبری در حکم انتصاب اعضای شورای عالی فضای مجازی (شهریور ۱۳۹۴) مورد توجه قرار گرفت. البته از دیدگاه معظم له، قدرت سایبری باید همراه با برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای سایبر در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه باشد؛ اما از دیدگاه دشمن، قدرت سایبری ایران به‌منظور انجام جنگ سایبری، ایجاد اختلال در سامانه‌های موشکی و فرماندهی و کنترل دشمن، سامانه‌های هوایی بدون سرنشین و... است و همچنان ایران-هراسی را در این حوزه القاء می‌کنند.

از دیدگاه دانیل کوهل، قدرت سایبری به معنای توانایی استفاده از فضای سایبر برای ایجاد برتری و تأثیرگذاری روی محیط‌های عملیاتی دیگر است (*Kuehl, 2009*). زیمت و باری 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. (*Zimet, and Barry, 2009*). جوزف نای قدرت سایبری را قدرت مبتنی بر منابع اطلاعاتی فناوری‌های ارتباطی می‌داند (*Nye* ۲۰۱۰). از دیدگاه شلدون، قدرت سایبری توانایی دستیابی به اهداف راهبردی و کاهش توانایی دشمن در بهره‌برداری یا حمله به زیرساخت‌های فضای سایبر است. وی قدرت سایبری را یک ابزار مکمل برای قدرت ملی می‌داند که می‌تواند برای استفاده توسط دولت‌مردان یک کشور جذاب باشد (*Sheldon, 2011*). از نظر اسپید، قدرت سایبری توانایی یک دولت- ملت برای برقراری، کنترل و اعمال نفوذ در داخل و از طریق فضای سایبر برای پشتیبانی و پیوستگی با دیگر عناصر حوزه قدرت ملی است. در این تعریف دستیابی به قدرت سایبری به توانایی دولت برای توسعه منابع جهت عملیات در فضای سایبر متکی است (*Spade, 2012*).

همان‌طور که در تعاریف فوق دیده می‌شود ماهیت و ویژگی‌های قدرت سایبری با تعاریف سنتی از قدرت و قدرت ملی منطبق است. قدرت سایبری در بعد تهاجمی، با هدف ضربه به زیرساخت‌های حیاتی و تخریب تأسیسات نظامی و هسته‌ای دشمن به‌وسیله حملات سایبری و

اجبار و ارعاب کشورها کاربرد دارد. در بعد تدافعی نیز نشان‌دهنده میزان آمادگی یک کشور در مقابله با بحران‌های سایبری و قدرت بازدارندگی است. دستیابی به این قدرت، نسبت به سایر شکل‌های قدرت هزینه کمتری دارد و می‌تواند از طرف کشورهای کوچک برای پیگیری سیاست‌های خود به‌کار رود.

در معاهدات بین‌الملل نیز نمونه‌هایی از توجه به قدرت سایبری دیده می‌شود به‌عنوان‌مثال ناتو از سال ۲۰۰۷ کنترل تهدیدات سایبری و دستیابی به قدرت سایبری را در دستور کار خود قرار داده است. در سال ۲۰۱۱ فضای سایبر را 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 موضوعات کلیدی و راهبردی است که برای نشان دادن نقش و تأثیر آن در امنیت ملی باید به‌طور دقیق شناخته‌شده و در سطح ملی بازتعریف شود.

رابطه قدرت سایبری و امنیت ملی در فضای سایبر: فضای سایبر بستر مناسبی برای آزادی بیان، القای اندیشه‌ها و ایدئولوژی‌ها و اظهار وجود نهادها و سازمان‌های اجتماعی، اقوام و نژادها، ادیان مختلف و حتی خرده‌فرهنگ‌ها فراهم نموده است. در این فضاء، با شکل‌گیری جوامع اطلاعاتی و هویت‌های مجازی، افراد در دام تبلیغات و القای نیازهای کاذب و تغییر در ترجیحات و علایق گرفتار شده‌اند. این مسئله درعین‌حال که انتشار و پراکندگی قدرت دولت‌ها را به همراه دارد؛ اما در صورت هدایت هدفمند، موجب اعتلای این منابع غیرمادی قدرت خواهد شد. منابعی که در دهه‌های دورتر به خاطر یک‌طرفه بودن و غیرتعاملی بودن فضای انتشار، در انحصار کشورها و گروه‌های خاصی بود.

قدرت سایبری، نوعی قدرت نوظهور در فضای سایبر است که به‌واسطه فراگیر شدن فناوری اطلاعات و ارتباطات و فضای سایبر به وجود آمده است. از آنجا که ماهیت آن، از جنس قدرت در مفهوم عام است؛ باید با تعاریف مطرح‌شده توسط اندیشمندان، همخوانی داشته باشد. قدرت از نظر مفهومی و انتزاعی پدیده‌ای با جلوه‌های ظاهری و عینی است. قدرت سایبری نیز از این قاعده مستثنی نیست.

امروزه در تمامی کشورها، علاوه بر توجه به منابع مادی قدرت سایبری (قدرت سخت)، رقابت و تلاش سرسختانه‌ای برای کسب و ترویج منابع غیرمادی قدرت سایبری از جمله فرهنگ، آرمان‌ها، ارزش‌های سیاسی (قدرت نرم) در حال انجام است که پیامدهای این اقدامات در قالب قدرت سایبری تجلی یافته است. اقدامات در زمینه سازمان‌دهی نیروهای سایبری و تلاش برای

دستیابی به تسلیحات و تجهیزات سایبری در راستای افزایش قدرت سایبری محسوب می‌شود. البته شایان‌ذکر است که تنها با دارا بودن منابع مادی و غیرمادی موصوف، قدرت سایبری ایجاد نمی‌شود بلکه داشتن اراده ملی و راهبردهای مناسب برای تبدیل منابع بالقوه به بالفعل نیز ضروری است.

از آنجا که فضای واقعی، تکیه‌گاه فضای سایبر محسوب می‌شود؛ داشتن تجهیزات سخت‌افزاری و نرم‌افزاری و موقعیت جغرافیایی کشورهایی که این منابع فیزیکی در آن‌ها موجود است را باید از منابع اصلی قدرت سایبری به‌حساب آورد. بدیهی است که از نقش تعیین‌کننده و پیشتازی کشورهایی که موقعیت سرورهای اساسی و سازمان‌های بین‌المللی در آن‌ها قرار گرفته است؛ نمی‌توان و نباید غافل شد. رشد فزاینده اقتصادی کشورهای پیشتاز در حوزه اقتصادی و بهره‌برداری هدفمند از رسانه‌های سایبری از دیگر مؤلفه‌های مشهود قدرت سایبری است.

همان‌طور که در فضای واقعی، قدرت و امنیت رابطه متقابلی با هم دارند؛ قدرت سایبری نیز رابطه‌ای انکارناپذیر با امنیت ملی دارد، چراکه فضای سایبر نوع جدیدی از تهدیدات، متفاوت با تهدیدات سنتی علیه امنیت ملی را به وجود آورده است. برخی از این تهدیدات مانند جرائم سایبری، جاسوسی سایبری، تروریسم سایبری و جنگ سایبری، منافع ملی کشورها را برای دستیابی به اهداف سیاسی و ایدئولوژیکی با چالش‌های جدی روبرو ساخته است. علاوه بر آن امنیت ملی در فضای سایبر با چالش‌های نوینی مانند صیانت از ارزش‌ها، هنجارها و هویت ملی، تلاش برای مشروع نشان دادن نظام سیاسی حاکم، تأمین امنیت مبادلات مالی و احقاق حقوق مادی و معنوی و اعمال قوانین و مقررات در فضای سایبر مواجه است.

هر چند، مجهز شدن کشور به فناوری‌های پیشرفته سایبری و قدرت سایبری، نقطه عطفی برجسته برای دستیابی به امنیت ملی است؛ اما وابستگی زیرساخت‌های حیاتی کشور به فضای سایبر، بیش از آنکه بتواند موجب ارتقای قدرت ملی شود؛ تهدیدات جدی برای امنیت ملی به ارمغان آورده است. غالب شدن رویکرد تهدید محور نسبت به فضای سایبر، ناشی از جدی بودن تحرکات دشمن در فضای سایبر برای ضربه زدن به منافع ملی و امنیت ملی است. در سال‌های اخیر، امنیت ملی، نقطه کانونی و مرکز ثقل راهبردها و اقدامات سیاسی در سطح کشور بوده است. گفتمان امنیت ملی، مبتنی بر ساختار ایدئولوژیک و متأثر از واکنش در مقابل تهدیدات امنیتی علیه آن است. احساس تهدید و نظریه توطئه قدرت‌های بزرگ علیه ساختار سیاسی و اجتماعی ایران همواره بخشی از واقعیت ذهنی و ادراکی جامعه ایرانی است که پس از انقلاب، عینیت بیشتری

پیداکرده است (پوستین‌دوز: ۱۳۸۹). موقعیت ژئوپلیتیکی خاص و داشتن منابع اقتصادی و راهبردی، ایران را با طیف متنوعی از تهدیدات مواجه نموده است. تعیین شاخص‌های این تهدیدات نیازمند بررسی نشانه‌های تاریخی و تبارشناسی آن‌هاست که در مقاله متقی بررسی شده است (متقی: ۱۳۸۹).

امنیت از عناصر تأثیرگذار و تأثیرپذیر در قدرت درون‌زای یک کشور است. در جمهوری اسلامی ایران، قدرت دارای ویژگی‌های خاص و منحصربه‌فردی مانند حاکمیت مبانی اسلامی و ایدئولوژی، الگوی مردم‌سالاری دینی و اتکاء به نظر مردم است. این عوامل اهمیت تبیین نقش کارکرد امنیت در استحکام ساخت درونی قدرت را دوچندان می‌سازد (شاه‌محمدی: ۱۳۹۵)؛ بنابراین با توجه به تغییر پارادایم تهدیدات در فضای سایبر، مقابله با عوامل تهدید و دستیابی به امنیت عینی و ذهنی در فضای سایبر مستلزم مجهز شدن به قابلیت‌های قدرت سایبری است. البته این مسئله به معنای فراموشی ابزارهای قدرت سخت مانند تسلیحات موشکی و قدرت نرم مانند دیپلماسی سیاسی نیست. بلکه با توجه به اهمیت یافتن تحرکات تهدیدآمیز دشمن در فضای سایبر، گامی راهبردی و مکمل اقدامات در فضای واقعی است.

به‌منظور تبیین رابطه بین قدرت سایبری و امنیت ملی در فضای سایبر، داده‌های مربوط به ادبیات تحقیق و مبانی نظری مرتبط، مورد مطالعه و بررسی مکرر، دقیق و موشکافانه قرار گرفت تا ایده‌ها و الگوهای نهفته در متون مشخص گردد. در این مرحله با جستجوی عمیق، فهرستی از عوامل مؤثر در متغیرهای تحقیق (قدرت سایبری و امنیت ملی در فضای سایبر) تهیه شد و پس از ترکیب و تلفیق آن‌ها و نظرخواهی از اساتید و خبرگان، مهم‌ترین عوامل تأثیرگذار در قدرت سایبری و امنیت ملی در فضای سایبر که نمایش جامع‌تری از پدیده تحت بررسی را آشکار می‌سازند؛ شناسایی شد. این عوامل در جدول (۱) آمده است.

عوامل مؤثر در قدرت سایبری	عوامل مؤثر در امنیت ملی در فضای سایبر
• القای فرهنگ، ارزش‌ها و هنجارهای موردنظر از طریق رسانه‌های سایبری • شکل‌دهی به ادراک، ترجیحات و علایق دیگران • ایجاد هویت جدید و تغییر هویت افراد جامعه • اعمال‌نفوذ در اجلاس‌های بین‌المللی سایبری • توانایی مشروع جلوه دادن اقدامات سیاسی در فضای سایبر • پروپاگاندا، جذابیت و القای نیازهای کاذب • توسعه اقتصادی مبتنی بر فناوری اطلاعات • ایجاد و توسعه جوامع اطلاعاتی • زیرساخت‌های سخت‌افزاری و نرم‌افزاری سایبری • زیرساخت‌های مدیریتی و دارایی‌های سایبری • تاب‌آوری زیرساخت‌های حیاتی • تسلیحات سایبری فعال و بالقوه • نیروی سایبری سازمان‌یافته • حملات سایبری و جنگ سایبری	• صیانت از ارزش‌ها، هنجارها و هویت ملی در فضای سایبر • مشروعیت و مقبولیت نظام سیاسی حاکم برای حاکمیت بر فضای سایبر • باور و اعتماد به صیانت از حریم خصوصی افراد در فضای سایبر • توانایی دولت در کنترل تحرکات تجزیه‌طلبانه در فضای سایبر • امنیت مبادلات مالی از طریق فضای سایبر • مقابله با تروریسم، جاسوسی و جرائم سایبری • اراده و انگیزه، سیاست‌گذاران برای مقابله با چالش‌های امنیتی فضای سایبر • ایفای نقش فعال در اجلاس‌های جهانی امنیت سایبر • اطمینان از توانمندی‌های علمی و فناورانه در حوزه امنیت سایبری • احقاق حقوق مادی و معنوی و اعمال قوانین و مقررات در فضای سایبر

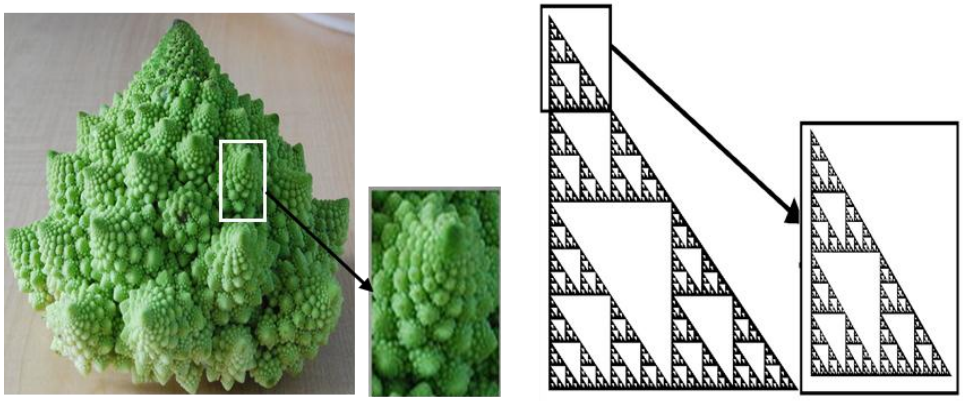
جدول ۱: عوامل مهم تأثیرگذار در قدرت سایبری و امنیت ملی در فضای سایبر

قدرت سایبری مبتنی بر رویکرد فرکتالی:

فرکتال از واژه لاتین فرکتوس[1]به معنی شکسته شدن به قطعات نامنظم گرفته شده است. در فارسی این کلمه با عنوان برخال نیز شناخته می‌شود. اولین بار مندلبروت[2]در مقاله‌ای برای بررسی ویژگی‌های هندسی سواحل انگلیس در سال ۱۹۷۵ از این کلمه استفاده کرد. از دیدگاه وی تمامی پدیده‌های طبیعی به‌نوعی فرکتال هستند و هندسه اقلیدسی (اشکال هندسی منظم مانند هرم، کره، مکعب و استوانه و...) قادر به تبیین و تشریح اشکال پیچیده و ظاهراً بی‌نظم طبیعی نیست. بسیاری از پدیده‌های طبیعی که در ظاهر بی‌نظم به نظر می‌رسند از یک تکرار منظم در مقیاس‌های متفاوت برخوردارند.

1- fractus
2- Benoit Mandelbrot

یکی از مهم‌ترین ویژگی‌های پدیده‌های فرکتالی خود متشابه بودن[1] آن‌هاست. اگر یک تصویر فرکتال را به چند بخش تقسیم کنیم، هر بخش یک نسخه از کل تصویر را نمایش می‌دهد و با آن مشابه است. ویژگی دیگر فرکتال‌ها تشکیل از راه تکرار[2] است. هر شکل پیچیده از طریق تکرار اشکال ساده‌تر به‌دست‌آمده است. در طبیعت نمونه‌های زیادی از فرکتال‌ها وجود دارد. در شکل (۱) یک فرکتال طبیعی (کلم رومی[3]) و یک فرکتال ریاضی (مثلث سرپینسکی[4]) برای نمونه نشان داده شده است.



شکل ۱: تصاویر فرکتالی در طبیعت و ریاضیات (کلم رومی و مثلث سرپینسکی)

فرکتال در کاربردهای مختلفی مانند ریاضیات، معماری، هنر، هواشناسی، زمین‌شناسی، شیمی، فشرده‌سازی اطلاعات و تصاویر و غیره استفاده می‌شود. یکی از اصلی‌ترین دلایل علاقه‌مندی به مفهوم فرکتال، آگاهی از مسئله ارتباط پدیده‌های مشابه با همدیگر است. با استفاده از این مفهوم می‌توان فرایندهای مشابه و خودسازمان‌ده را بررسی کرد (کرم: ۱۳۸۹).

در مباحث علوم شناختی ساختار سازمان‌ها را می‌توان با استفاده از فرکتال مدل‌سازی نمود. سازمان‌ها به اجزای کوچک‌تری تقسیم می‌شوند که هر بخش اهداف و عملکرد و ویژگی‌های کل سازمان را در خود دارد. سازمان‌های فرکتالی دارای ویژگی‌هایی مانند خودسازمان‌دهی، خود بهینه‌سازی، حیات و توسعه دائمی، تصمیم‌گیری بدون تأیید مرکزی (خودمختاری) هستند (*Bodunkova, 2012*).

1-Self-Similarity
2- Iterative formation
3-Romanesco broccoli
4-Sierpinski

تفکر فرکتالی یک پارادایم فکری است که می‌توان آن را در مباحث علـوم اجتمـاعی و سیاسـی نیز به‌کار برد و لذا در این مقاله بر مبنای نظریه دانیل کوهل، رویکرد فرکتالی برای قـدرت سـایبری انتخاب شده و مورد بررسی قرار گرفته است (*Kuehl, 2009*).

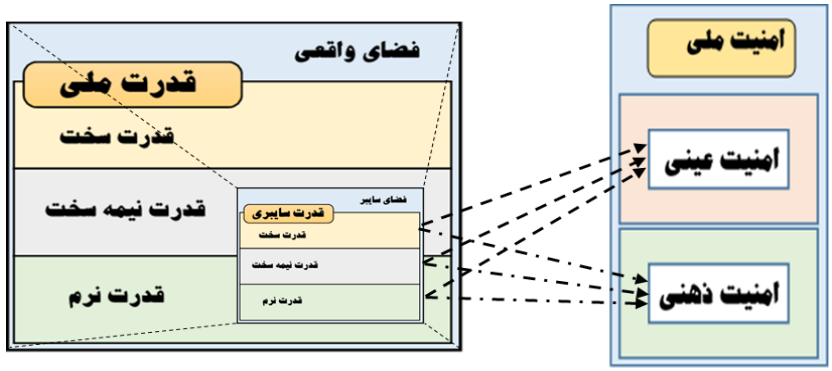
در این رویکرد، قدرت سایبری یک فرکتال از قدرت ملی محسوب می‌شود؛ چون دارای تمامی ویژگی‌های قدرت ملی در فضای سایبر است و تمامی منابع و فراینـدهای قـدرت ملـی در قـدرت سایبری نیز وجود دارد. امروزه دولت‌ها قدرت ملی خود را با قدرت سایبری پیوند زده‌انـد و از آن به‌عنوان کاتالیزور و شتاب‌دهنده قدرت استفاده می‌کنند. علاوه بر آن، توانایی دولت‌هـا بـرای مهـار چالش‌های امنیت ملی در فضای سایبر از مهم‌تـرین عوامـل قـدرت سـایبری دولـت‌هـا محسـوب می‌شود.

مدل مفهومی:

قدرت سایبری از مقوله‌های نوظهور در فضای سایبر است که هنوز هم ادبیات غنی و قابل‌تـوجهی در مورد ماهیت، ویژگی‌ها و پیامدهای آن تولید نشده است؛ از آنجا که کاربرد این مفهوم در سـطح ملی و موضوع روابط بین‌الملل به‌کار می‌رود؛ بنابراین در مقیاس قدرت ملی، قابل بررسی است. در سه دهه گذشته فضای سایبر موجب ظهور و بروز ایده‌ها و نظریه‌هایی ماننـد دهکـده جهـانی و از بین رفتن مرزهای جغرافیایی و قلمرو سرزمینی شده است؛ اما قدرت سایبری همچنان در محـدوده قلمرو کشورها قابل بررسی است. با این وجود، قدرت سایبری یک عنصر یا مؤلفه از قـدرت ملـی نیست چراکه تمامی ویژگی‌های قدرت ملی در فضای واقعی را می‌توان با یک نگاشـت در فضـای سایبر، به قدرت سایبری نسبت داد.

ویژگی فرکتالی موجب می‌شود فرایندها و پدیده‌های قدرت ملـی، بـا یـک نگاشـت در قالـب قدرت سایبری بررسی شوند. با توجه به آنکه پارادایم فرکتالی، یک پارادایم کل‌نگر است کـه تمـام پدیده‌های جهان را در یک کل شامل اجزای متفاوت می‌بیند و هرکدام از اجزاء می‌توانـد روی کـل اثر بگذارد؛ بنابراین به‌منظور بررسی تأثیر قدرت سایبری بر امنیت ملی در فضای سایبر، مؤلفه‌هـا و متغیرهای قدرت سایبری همانند قدرت ملی در نظر گرفته می‌شود. چراکه پدیـده‌هـا و فراینـدهای فضای سایبر انعکاسی از پدیده‌های جهان واقعی است. همچنین امنیت ملی در فضـای سـایبر نیـز، همانند فضای واقعی شامل دو مؤلفه امنیت عینی (فقدان تهدیـد) و امنیـت ذهنـی (فقـدان تـرس و

نگرانی) در نظر گرفته شد. بر این اساس در شکل (۲) مدل مفهومی پژوهش بر اساس رویکرد فرکتالی نشان داده شده است.



شکل ۲: مدل مفهومی تحقیق بر مبنای رویکرد فرکتالی

روش‌شناسی:

تحقیق حاضر از نظر هدف، از نوع کاربردی- توسعه‌ای است؛ چون با هدف شناسایی ابزار و مؤلفه‌های قدرت سایبری و بررسی نقش آن‌ها در تأمین امنیت ملی فضای سایبر کشور انجام‌شده است و با توجه به تحقیقات محدود در این زمینه می‌تواند مقدمه‌ای برای گسترش مرزهای دانش در این حوزه شود.

این تحقیق از نظر ماهیت، از نوع توصیفی- همبستگی است چون محقق به دنبال شناخت ویژگی‌های قدرت سایبری و رابطه آن با متغیر امنیت ملی است. در تحقیقات توصیفی، محقق دخالتی در موقعیت، وضعیت و نقش متغیرها ندارد و صرفاً با مطالعه آنچه وجود دارد، به توصیف و تشریح آن‌ها می‌پردازد. در تحقیقات همبستگی نیز به بررسی روابط دو متغیر و محاسبه همبستگی میان آن‌ها پرداخته می‌شود (حافظ نیا، ۱۳۹۲: ۷۴).

برای گردآوری داده‌ها از روش کتابخانه‌ای و مطالعه اکتشافی در متون و کتاب‌های مرتبط و سایت‌های اینترنتی (عمدتاً مجلات علمی- پژوهشی معتبر) استفاده شده است. رویکرد تجزیه‌وتحلیل داده‌ها نیز از نوع آمیخته (کمی و کیفی) است. در روش کیفی، برای احصاء مؤلفه‌ها و متغیرهای اصلی قدرت سایبری و امنیت ملی از روش فراترکیب[1] استفاده شد.

این روش شامل هفت مرحله است که عبارتند از: ۱) تنظیم سؤال پژوهش، ۲) مرور ادبیات به شکل نظام‌مند، ۳) جستجو و انتخاب متون مناسب، ۴) استخراج اطلاعات متون، ۵) تجزیه‌وتحلیل

1 Meta Synthesis

و ترکیب یافته‌های کیفی، ۶) کنترل کیفیت، ۷) ارائه یافته‌ها. در این روش، به‌جای ارائه خلاصه جامعی از یافته‌ها، یک ترکیب (سنتز) تفسیری از یافته‌ها ایجاد می‌شود و یک دید جامع و گسترده نسبت به مسائل به وجود می‌آید و پژوهشگر با ایجاد و آشکارسازی واژه‌های جدید، نمایش جامع‌تری از پدیده تحت بررسی را مشخص می‌سازد (سهرابی و همکاران: ۱۳۹۰). همچنین در روش کمی برای تجزیه‌وتحلیل آماری و بررسی میزان رابطه و همبستگی میان عوامل احصاء شده از مدل‌سازی معادلات ساختاری[1] استفاده شده است.

در این تحقیق، پس از مطالعات اکتشافی در مبانی نظری، با مبنا قرار دادن رویکرد فرکتالی، سه مؤلفه قدرت سخت، قدرت نیمه سخت و قدرت نرم، برای قدرت سایبری و دو مؤلفه امنیت عینی و امنیت ذهنی برای امنیت ملی در فضای سایبر (مطابق مدل مفهومی) در نظر گرفته شد. در مرحله بعد عوامل مؤثر شناسایی‌شده در جدول (۱) به هرکدام از این مؤلفه‌ها اختصاص داده شد و پس از تعیین مضامین پایه، سازمان دهنده و فراگیر، یک پرسشنامه محقق ساخته بر مبنای طیف پنج گزینه‌ای لیکرت طراحی شد. برای بررسی روایی ابزار اندازه‌گیری (پرسشنامه) از روش روایی صوری استفاده شد. در این روش، گویه‌ها از نظر ادبیات و قابل فهم بودن برای مخاطب از طریق جلسات خبرگی با اساتید مورد تأیید قرار گرفت و پس از انجام اصلاحات، پرسشنامه نهایی بین جامعه آماری توزیع شد. در پرسشنامه از خبرگان میزان تأثیر سازه‌ها و شاخص‌های قدرت سایبری در امنیت ملی پرسیده شد.

جامعه آماری این تحقیق نیز، شامل خبرگان و صاحب‌نظران و مدیران آشنا با فضای سایبر و امنیت ملی و دارای تحصیلات دانشگاهی کارشناسی ارشد و دکتری و سوابق مدیریتی در سطوح راهبردی و سیاست‌گذاری کلان است. در اینجا به خاطر تخصصی بودن موضوع تحقیق، روش نمونه‌گیری هدفمند (انتخاب افرادی که بیشترین اطلاعات را از موضوع دارند) همگون (انتخاب افراد با خصوصیات مشترک) و گلوله برفی (شناسایی افراد از طریق معرفی تا اشباع نظری) مدنظر قرار گرفت.

تجزیه‌وتحلیل یافته‌ها:

در این تحقیق، بر مبنای روش فراترکیب، از مضامین پایه، سازمان دهنده و فراگیر برای بررسی رابطه میان متغیرهای تحقیق در مدل مفهومی استفاده شده است. مضمون، ویژگی تکراری و

1- Structural Equation Modeling

متمایزی در متن است که به نظر پژوهشگر، نشان‌دهنده درک و تجربه خاصی در رابطه با سؤالات تحقیق است. در این مقاله، مضامین فراگیر، همان متغیرهای اصلی تحقیق (قدرت سایبری و امنیت ملی در فضای سایبر) انتخاب شده‌اند. برای هرکدام از این مضامین با توجه به ادبیات تحقیق و مطالعات اکتشافی، مضامین سازمان دهنده مرتبط مشخص گردید؛ سپس با مرور عوامل مؤثر در جدول (۱) کدها و نکات کلیدی احصاء شده از متون تحت عنوان مضامین پایه شناسایی گردید و هرکدام با یک نشانگر مشخص گردید. این متغیرها در جدول (۲) نشان داده‌شده است. در ادامه از نرم‌افزار Smart PLS که مبتنی بر رویکرد حداقل مربعات جزئی است برای بررسی روابط میان متغیرهای آشکار و پنهان استفاده شد و مدل مفهومی ترسیم گردید. همچنین اولویت‌بندی متغیرها نیز توسط این نرم‌افزار انجام شد.

در این نرم‌افزار، حجم نمونه از ضرب کردن ۱۰ در تعداد نشانگرهای مدل اندازه‌گیری که دارای بیشترین نشانگر است یا ضرب کردن ۱۰ در بیشترین روابط موجود در بخش ساختار مدل اصلی به دست می‌آید (داوری، رضازاده،۱۳۹۳:۶۲). در این مقاله متغیرهای مربوط به مؤلفه سخت در قدرت سخت و مؤلفه‌های عینی و ذهنی در امنیت ملی دارای بیشترین نشانگر (۶) هستند؛ بنابراین حجم نمونه برابر ۶۰ در نظر گرفته شده است.

مضمون فراگیر	مضامین سازمان دهنده	مضامین پایه	نشانگر
قدرت سایبری	سخت Hard	تسلیحات سایبری فعال و بالقوه	HP1
		نیروی سایبری سازمان‌یافته	HP2
		حملات سایبری و جنگ سایبری	HP3
		زیرساخت‌های سخت‌افزاری و نرم‌افزاری سایبری	HP4
		زیرساخت‌های مدیریتی و دارایی‌های سایبری	HP5
		تاب‌آوری زیرساخت‌های حیاتی	HP6
	نیمه سخت Semi-Hard	توسعه اقتصادی مبتنی بر فناوری اطلاعات	SHP1
		ایجاد و توسعه جوامع اطلاعاتی	SHP2
		اعمال نفوذ در اجلاس‌های بین‌المللی سایبری	SHP3
		توانایی مشروع جلوه دادن اقدامات سیاسی در فضای سایبر	SHP4
	نرم Soft	القای فرهنگ، ارزش‌ها و هنجارهای موردنظر	SP1
		شکل‌دهی به ادراک، ترجیحات و علایق دیگران	SP2

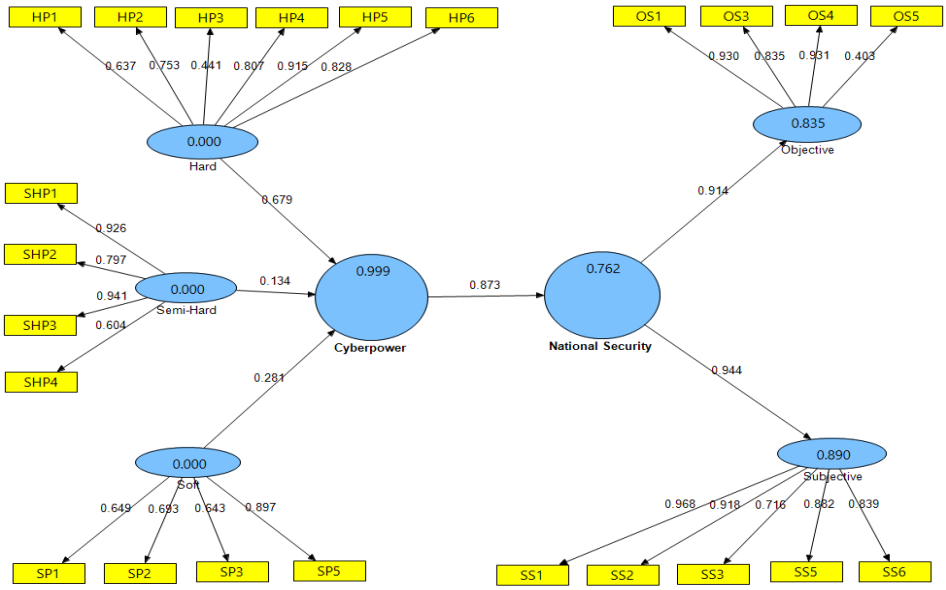
		ایجاد هویت جدید و تغییر هویت افراد جامعه	SP3
		پروپاگاندا، جذابیت و القای نیازهای کاذب	SP4
		رسانه‌های سایبری	SP5
امنیت ملی در فضای سایبر	عینی و ملموس (Objective)	ظرفیت دولت در مقابله با تروریسم، جاسوسی و جرائم سایبری	OS1
		توانایی دولت در کنترل تحرکات تجزیه‌طلبانه در فضای سایبر	OS2
		امنیت مبادلات مالی از طریق فضای سایبر	OS3
		میزان استقلال شبکه ملی و بومی بودن تجهیزات	OS4
		ایفای نقش فعال در اجلاس‌های جهانی امنیت سایبر	OS5
	ذهنی و ناملموس (Subjective)	اراده و انگیزه، سیاست‌گذاران برای مقابله با چالش‌های امنیتی فضای سایبر	SS1
		مشروعیت و مقبولیت نظام سیاسی حاکم برای حاکمیت بر فضای سایبر	SS2
		اطمینان از توانمندی‌های علمی و فناورانه در حوزه امنیت سایبری	SS3
		باور و اعتماد به صیانت از حریم خصوصی افراد در فضای سایبر	SS4
		احقاق حقوق مادی و معنوی و اعمال قوانین و مقررات در فضای سایبر	SS5
		صیانت از ارزش‌ها، هنجارها و هویت ملی در فضای سایبر	SS6

جدول ۲: مضامین پایه، سازمان دهنده و فراگیر در مدل پیشنهادی

تجزیه‌وتحلیل آماری:

پس از توزیع پرسشنامه بین جامعه آماری تعداد ۲۸ پاسخ جمع‌آوری شد، نتایج حاصل به‌صورت جداگانه در دو فایل با فرمت *CSV* در نرم‌افزار *SPSS* وارد شد تا توسط نرم‌افزار *Smart PLS* فراخوانی شده و پردازش‌های لازم انجام شود.

برای سنجش پایایی نشانگرها، در این نرم‌افزار از ضرایب بار عاملی، آلفای کرونباخ و پایایی ترکیبی و برای سنجش روایی از روایی همگرا (ضرایب *AVE*) و روایی واگرا (ماتریس بار عاملی متقابل) استفاده می‌شود. در اینجا سنجش پایایی از طریق ضرایب بار عاملی انجام شده است. پس از ترسیم مدل، فرمان *calculate/PLS Algorithm* اجرا شد. پس از اجرای نرم‌افزار، سه متغیر استفاده از ابزارهای تبلیغاتی (*SP4*)، کنترل تحرکات تجزیه‌طلبانه (*OS2*) و باور و اعتماد به صیانت از حریم خصوصی (*SS4*) به ترتیب با ضرایب بار عاملی ۰/۲۹۲، ۰/۱۴۲ و ۰/۱۰۱ ظاهر شدند که چون از ۰/۴ کمتر هستند حذف گردیدند. پس از حذف این متغیرها، مدل نهایی مطابق شکل (۳) به دست آمد که در آن، اعداد نوشته شده روی پیکان‌های متصل به متغیرها ضرایب بار عاملی را نشان می‌دهند و همگی بیشتر از ۰/۴ هستند. این مسئله پایایی این متغیرها را تأیید می‌کند.



شکل ۳. ضرایب بار عاملی برای برازش مدل اندازه‌گیری

برای سنجش روایی، از ضرایب متوسط واریانس استخراج‌شده[1] (*AVE*) که توسط فورنل و لارکر ارائه‌شده استفاده می‌شود. این معیار، میزان همبستگی هر مؤلفه با متغیرهای خود را نشان می‌دهد. طبق این روش این مقادیر، باید بالای ۰/۵ باشند که نشان دهنده این است که متغیر پنهان مورد نظر حداقل ۵۰ درصد واریانس مشاهده پذیره‌ای خود را تبیین می‌کند (همان: ۸۴). با استفاده از بخش *report html* در نرم‌افزار، *AVE* محاسبه می‌شوند که در جدول (۲) این مقادیر نشان داده‌شده است.

امنیت ذهنی	امنیت عینی	قدرت نرم	قدرت نیمه سخت	قدرت سخت	امنیت ملی	قدرت سایبری
۰/۷۵۴	۰/۶۴۸	۰/۵۲۹	۰/۶۸۵	۰/۵۵۷	۰/۶۰۴	۰/۵۱۶

جدول ۲. مقادیر ***AVE*** ابعاد و مؤلفه‌های مدل مفهومی

در مرحله بعد، برای اولویت‌بندی مؤلفه‌ها و متغیرهای تحقیق، از ضرایب معنادار مسیر (*t-values*) استفاده شده است. درصورتی‌که این مقادیر از ۱/۹۶ بیشتر باشد همبستگی میان متغیرها

1 Average Variance Extracted

بین آن‌ها در سطح اطمینان ۹۵٪ معنادار تفسیر می‌شود. این کار با اجرای فرمان *Bootstrapping* در نرم‌افزار انجام شد. در این حالت از آزمون معناداری z (مقادیر *t-Value*) محاسبه می‌شوند و بر اساس مقادیر به‌دست‌آمده اولویت‌بندی مؤلفه‌ها و متغیرهای مرتبط با آن‌ها در جدول (۳) ارائه‌شده است.

مفهوم	مؤلفه‌ها بر حسب اولویت	امتیاز	متغیرها برحسب اولویت	امتیاز
قدرت سایبری	سخت	۲۶/۱۷۸	زیرساخت‌های مدیریتی و دارایی‌های سایبری	۸۷/۵۰۸
			تاب‌آوری زیرساخت‌های حیاتی	۲۰/۷۶۲
			نیروی سایبری سازمان‌یافته	۱۳/۶۸۹
			زیرساخت‌های سخت‌افزاری و نرم‌افزاری سایبری	۸/۵۴۹
			تسلیحات سایبری فعال و بالقوه	۵/۱۶۲
			حملات سایبری و جنگ سایبری	۳/۷۳۱
	نرم	۱۴/۴۹۸	رسانه‌های سایبری	۲۲/۰۵۶
			القای فرهنگ، ارزش‌ها و هنجارهای موردنظر	۱۰/۴۲۸
			شکل‌دهی به ادراک، ترجیحات و علایق دیگران	۸/۸۳۸
			ایجاد هویت جدید و تغییر هویت افراد جامعه	۶/۸۳۲
	نیمه سخت	۵/۹۵۰	اعمال‌نفوذ در اجلاس‌های بین‌المللی سایبری	۶۲/۸۹۵
			توسعه اقتصادی مبتنی بر فناوری اطلاعات	۳۷/۸۳۹
			ایجاد و توسعه جوامع اطلاعاتی	۱۳/۷۶۶
			توانایی مشروع جلوه دادن اقدامات سیاسی در فضای سایبر	۷/۸۶۲
امنیت ملی در فضای سایبر	ذهنی و ناملموس	۱۲۱/۵۸۷	اراده و انگیزه، سیاست‌گذاران برای مقابله با چالش‌های امنیتی فضای سایبر	۸۸/۸۱۲
			مشروعیت و مقبولیت نظام سیاسی حاکم برای حاکمیت بر فضای سایبر	۸۱/۶۲۰
			احقاق حقوق مادی و معنوی و اعمال قوانین و مقررات در فضای سایبر	۳۳/۶۲۳
			صیانت از ارزش‌ها، هنجارها و هویت ملی در فضای سایبر	۲۵/۷۰۲
			اطمینان از توانمندی‌های علمی و فناورانه در حوزه امنیت سایبری	۱۴/۷۱۳
	عینی و ملموس	۵۸/۸۹۸	میزان استقلال شبکه ملی و بومی بودن تجهیزات	۶۳/۷۷۷
			ظرفیت دولت در مقابله با تروریسم، جاسوسی و جرائم سایبری	۱۳/۸۸۹
			امنیت مبادلات مالی از طریق فضای سایبر	۱۳/۵۰۸
			ایفای نقش فعال در اجلاس‌های جهانی امنیت سایبر	۷/۴۵۶

جدول ۳. اولویت‌بندی مؤلفه‌ها و متغیرها

تجزیه‌وتحلیل استنباطی:

تحلیل یافته‌های آماری این تحقیق نشان می‌دهد از میان مؤلفه‌های قدرت سایبری، قدرت سخت، قدرت نرم و قدرت نیمه‌سخت به ترتیب رتبه اول تا سوم را دارند. همچنین در میان مؤلفه‌های امنیت ملی، امنیت ذهنی و ناملموس رتبه بالاتری نسبت به امنیت عینی دارد.

از دیدگاه پاسخ‌دهندگان، در میان متغیرهای قدرت سخت سایبری، تسلط و حاکمیت بر زیرساخت‌های مدیریتی و دارایی‌های سایبری بیشترین تأثیر را در امنیت ملی دارد. در میان متغیرهای قدرت نرم سایبری نیز بهره‌گیری از رسانه‌های سایبری در تأمین امنیت ملی بالاترین نقش را دارد. همچنین در میان متغیرهای قدرت نیمه‌سخت سایبری حضور فعال و اعمال‌نفوذ در اجلاس‌های جهانی مرتبط با فضای سایبر در امنیت ملی از اهمیت بیشتری نسبت به سایر متغیرها برخوردار است. با بررسی مؤلفه‌های امنیت ملی نیز دیده می‌شود در میان متغیرهای امنیت ذهنی و ناملموس میزان تأثیر اراده و انگیزه سیاست‌گذاران برای مقابله با چالش‌ها امنیتی فضای سایبر بالاترین امتیاز را دارد و در میان متغیرهای امنیت عینی و ملموس، میزان استقلال شبکه ملی و بومی بودن تجهیزات از تأثیر بالاتری نسبت به سایر متغیرها برخوردار است که لزوم راه‌اندازی شبکه ملی اطلاعات برای ارتقاء قدرت سایبری و در نتیجه تأمین امنیت ملی را نشان می‌دهد.

نتیجه‌گیری و پیشنهاد

امروزه، فناوری‌های فضای سایبر، به ابزاری برای حکمرانی، نفوذ و قدرت‌طلبی تبدیل شده است. اعمال قدرت به‌طور مستقیم و غیرمستقیم به‌منظور جهت‌دهی باورها، ترجیحات و اولویت‌ها، الگوهای فکری و رفتاری در حال انجام است. افزایش نقش‌آفرینی در مدیریت فضای سایبر، توسعه سرمایه‌گذاری اقتصادی و افزایش نفوذ بین‌المللی از مصادیق قدرت سایبری است. در این محیط پیچیده و پویا، کشورهایی که مجهز به این فناوری‌های نوظهور نباشند و خود را ملزم به بهره‌گیری از قابلیت‌های آن در قالب قدرت سایبری ندانند، در صحنه جهانی، مجالی برای قدرت‌نمایی ندارند. اقداماتی مانند انحصار فناوری زیرساخت‌های سخت‌افزاری و نرم‌افزاری، استفاده از تسلیحات سایبری پیشرفته در جنگ‌های سایبری، سلطه اطلاعاتی، حاکمیت بر فضای سایبر، راه‌اندازی پویش‌ها برای تغییر نظام‌های سیاسی و... نمونه‌هایی از قدرت‌طلبی و امپریالیسم نوین جهانی در فضای سایبر است.

قدرت سایبری ارتباط تنگاتنگی با قدرت ملی و قدرت دولت‌ها دارد و نتیجه وفاق ملی و اقتدار سازمان‌یافته‌ای است که به دولت‌ها داده می‌شود. از منظر سیاسی نیز قدرت سایبری همچون قبل، ماهیت و نقشی محوری در نظریه‌های سیاسی دارد و انتظار می‌رود در آینده به نقطه کانونی در روابط بین‌الملل تبدیل شود. البته باید توجه داشت که داشتن منابع 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 این تحقیق، اتخاذ رویکرد فرکتالی برای قدرت سایبری، به معنای تشابه ویژگی‌های ذاتی و کارکردی مؤلفه‌های قدرت سایبری و قدرت ملی است. این رویکرد برای تأکید بر این نکته است که قدرت سایبری می‌تواند، پاسخگوی دغدغه‌ها و ابهامات ایجادشده برای امنیت ملی در فضای سایبر باشد.

در صورت دستیابی به سطح مطلوبی از قدرت سایبری، امکان پیش‌گیری خنثی‌سازی و مقابله با تهدیدات عینی و ذهنی مبتنی بر فناوری‌های فضای سایبر فراهم می‌شود که ارتقاء امنیت ملی را در پی خواهد داشت. به‌عبارت‌دیگر یکی از مهم‌ترین پیامدهای قدرت سایبری را می‌توان ارتقاء

امنیت ملی دانست. قدرت سایبری به‌عنوان ابزاری برای محافظت از منافع و ارزش‌های ملی نقش مهمی در افزایش امنیت ملی دارد.

تصریح مقام معظم رهبری بر ارتقاء جمهوری اسلامی ایران به قدرت سایبری، نشان‌دهنده اهمیت راهبردی قدرت سایبری است چراکه فرامین و رهنمودهای معظم له از یک منظومه فکری هدفمند و منسجم و متناسب با نیازها و شرایط جامعه نشأت می‌گیرد. برای تحقق این مهم، سازمان‌ها و نهادهای ذی‌ربط مانند وزارت ارتباطات و فناوری اطلاعات، شورای عالی فضای مجازی، سازمان‌های دفاعی، امنیتی و... باید برنامه اقدام خود را مشخص نمایند. لازمه این کار، در مرحله اول، شناسایی شاخص‌های قدرت سایبری و در مرحله بعد، انجام تحقیقات میدانی، جهت برآورد درست از وضعیت، ظرفیت‌ها و منابع قدرت سایبری کشور است. شناسایی و تبیین شاخص‌های امنیت ملی در فضای سایبر، با انجام مطالعات اکتشافی و تطبیقی در دیگر کشورها و رویکرد آینده‌پژوهانه به موضوعات و چالش‌های نوین امنیت ملی از دیگر اقداماتی است که می‌تواند از طرف نهادهای مسئول در سطوح عملیاتی و راهبردی مورد توجه و مطالبه قرار گیرد.

دیدگاه فرکتالی در نظر گرفته‌شده در این تحقیق، برای تأکید بر این واقعیت است که قدرت سایبری تمامی ویژگی‌ها و قابلیت‌های قدرت ملی را در بردارد؛ از آنجا که قدرت ملی دارای ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، فناوری و... است؛ بنابراین، برای دستیابی به قدرت سایبری باید به همه ابعاد آن توجه نمود.

قدرت سایبری همانند امنیت ملی از موضوعات کلان و راهبردی است و برای سیاست‌گذاری در موضوعات کلیدی از جمله قدرت سایبری و امنیت ملی، باید راهبردهایی پویا و انعطاف‌پذیر برای سازگاری با ساختارها و فرایندهای فضای سایبر در تحقیقات آتی مدنظر قرار گیرد. انجام پژوهش جامع و کامل با تمرکز روی هرکدام از ابعاد قدرت سایبری و بررسی تأثیر آن روی همان بعد از امنیت ملی، در تدقیق و توصیف رابطه این دو مفهوم اساسی، ضروری است و می‌تواند از موضوعات پیشنهادی مهم برای پژوهشگران باشد (مانند رابطه قدرت سایبری با امنیت ملی از منظر سیاسی، اجتماعی، اقتصادی و...). علاوه بر آن، تبیین ابعاد، مؤلفه‌ها و شاخص‌های قدرت سایبری، احصاء شاخص‌های کلان سنجش قدرت سایبری، بررسی میزان تأثیر دفاعی، امنیتی در ارتقاء قدرت سایبری به‌عنوان پیشنهادات دیگر این پژوهش مطرح می‌شود.

منابع:

- پایگاه اطلاع‌رسانی دفتر حفظ و نشر آثار ***امام خامنه‌ای (مدظله‌العالی)*** www.khamenei.ir
- اسکندری، محمدحسین و دارابکلایی، اسماعیل، (۱۳۹۱)، ***پژوهشی در موضوع قدرت***، پژوهشگاه حوزه و دانشگاه.
- پوستین‌دوز، زهره، (۱۳۸۹)، ***قدرت نرم در گفتمان امنیت ملی جمهوری اسلامی ایران***، فصلنامه آفاق امنیت، سال سوم، شماره هفتم.
- توحیدی، ارسطو؛ طاهری، سلیمان و گودرزی، محسن، (۱۳۹۶)، ***بررسی رابطه قدرت با امنیت (با رویکرد به مبانی اسلامی)***، فصلنامه مطالعات دفاعی راهبردی سال پانزدهم، شماره ۱۰۱.
- حسن بیگی، ابراهیم و کولیوند، ابراهیم، (۱۳۹۶)، ***ارائه الگوی راهبردی مدیریت تحولات برآمده از توسعه فناوری اطلاعات و ارتباطات بر امنیت داخلی جمهوری اسلامی ایران***، فصلنامه امنیت ملی، سال هفتم. شماره بیست و چهارم.
- خلیلی، رضا، (۱۳۸۳)، ***تحول تاریخی گفتمانی مفهوم امنیت***، فصلنامه مطالعات راهبردی سال هفتم شماره اول.
- زرقانی، سید هادی، (۱۳۸۹)، ***نقد و تحلیل مدل‌های سنجش قدرت ملی***. فصلنامه ژئوپلیتیک.
- ره‌پیک، سیامک، (۱۳۸۷)، ***نظریه امنیت جمهوری اسلامی ایران***، تهران: دانشگاه عالی دفاع ملی.
- سلطانی نژاد، احمد؛ موسوی شفایی، مسعود و اسدی نژاد، الهام، (۱۳۹۲)، ***تأثیر فناوری اطلاعات و ارتباطات بر امنیت ملی جمهوری اسلامی ایران در دهه ۸۰***، پژوهشنامه علوم سیاسی، سال هشتم شماره دوم.
- سهرابی، بابک؛ اعظمی، امیر و یزدانی، حمیدرضا، (۱۳۹۰)، ***آسیب‌شناسی پژوهش‌های انجام‌شده در زمینه مدیری اسلامی با رویکرد فراترکیب***، چشم‌انداز مدیریت دولتی، شماره ۶.
- شاه‌محمدی، محمد؛ صائبی، حسن و قیاسی کرمانی، علی‌اکبر، (۱۳۹۳)، ***نقش کارکردهای امنیت در تقویت استحکام ساخت درونی قدرت جمهوری اسلامی ایران***، فصلنامه امنیت-پژوهی سال پانزدهم، شماره ۵۳.
- شایگان، فریبا، (۱۳۹۱)، ***امنیت پایدار از دیدگاه مقام معظم رهبری***، فصلنامه آفاق امنیت، سال پنجم، شماره چهاردهم.
- علی بابایی، غلامرضا، (۱۳۹۱)، ***فرهنگ سیاسی آرش***، تهران: نشر آشیان.
- غرایاق زندی، داود، (۱۳۹۰)، ***سیاست‌گذاری امنیت ملی***، تهران: پژوهشکده مطالعات راهبردی.

- قیصری، نوراله، (۱۳۹۳)، ***مکاتب امنیتی***؛ نقدهای موجود و ضرورت طرح نگرشی نوین، فصلنامه آفاق امنیت، سال هفتم، شماره بیست و دوم.
- کرم، امیر، (۱۳۸۹)، ***نظریه آشوب، فرکتال و دستگاه‌ها غیرخطی در ژئومورفولوژی***، فصلنامه جغرافیای طبیعی، سال سوم، شماره ۸.
- متقی، ابراهیم، (۱۳۸۹)، ***گونه‌شناسی تهدیدهای امنیت ملی جمهوری اسلامی ایران***، فصلنامه آفاق امنیت، سال سوم، شماره هشتم.
- نصری، قدیر، (۱۳۹۰)، ***تأملی نظر در یافته‌ها و دشواری‌های «باری بوزان» در بررسی امنیت***، فصلنامه مطالعات راهبردی، سال چهاردهم شماره چهارم.
- _____ (۱۳۹۲)، ***امنیت جامعه‌ای به‌مثابه هسته حیاتی امنیت ملی پایدار***. فصلنامه امنیت‌پژوهی، سال دوازدهم شماره ۴۳.
- نبوی، عباس، (۱۳۹۵)، ***فلسفه قدرت***، تهران: انتشارات سمت، چاپ چهارم.

- Barnett, M. & Duvall, R. (2005). Power in international politics. International Organizations, Cambridge University Press.
- Bodunkova, A. G. & Chernaya, I. P. (2012). Fractal organization as innovative model for entrepreneurial university development. World Applied Sciences Journal, 18, 74-82
- Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, (2009) "Cyberpower and National Security", National Defense University Press, Washington DC
- Kuehl.D. T. (2009). From cyberspace to cyberpower: defining the problem. In F.D.Kramer, S.H.Starr, and l.Wentz. Cyberpower and National Security (National Defense University) (pp26-28) Washington: Potomac Books
- Nye, Joseph (2011); "The future of power", New York: Public Affairs.
- Pravir Malik, (2015), The Fractal Organization: Creating Enterprises of Tomorrow, SAGE
- Spade, J. M. (2012). China's Cyberpower and America's national security. Carlisle Barracks, PA: US ARMY WAR COLLEGE
- Sheldon, J.B. (2011).Deciphering Cyberpower: Strategic Purpose in peace and war. Restricted from: http://www.au.af.mil/au/ssq/2011/summer/sheldon.pdf
- Zimet, E. and Barry, C. (2009). Military Service of Cyber Overview in Military Perspective on Cyberpower, Washington DC Center for Technology and National Security Policy at the National Defense University.