نشریه علمی مدیریت و پژوهش‌های دفاعی، سال بیستم، شماره ۹۲، تابستان ۱۴۰۰: ۱۴۹ ـ ۱۲۵

ارائه مدل تأثیر تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران

سید علی موسی‌زاده[۱]
حجت مهکویی[۲]
رضا سیمبر[۳]
سیامک باقری چوکامی[۴]

تاریخ دریافت: ۱۴۰۰/۰۵/۰۱
تاریخ پذیرش: ۱۴۰۰/۰۹/۱۵

چکیده

پژوهش حاضر درصدد پاسخ به این سؤال است که تهدیدات سایبری چه نقشی در تضعیف امنیت ملی جمهوری اسلامی ایران داشته است؟ برای پاسخ به سؤال، از میان روش‌های کیفی، از روش تحلیل مضمون بهره گرفته شده است. داده‌های پژوهش با استفاده از مصاحبه نیمه‌ساختاریافته از ۲۵ نفر از خبرگان حوزه صلح و امنیت سایبری که با استفاده از روش نمونه‌گیری نظری انتخاب شده‌اند، گردآوری گردید و مدل، با کاربست روش تحلیل مضمون از نوع شبکه مضامین مورد تحلیل و مدل مفهومی اندازه‌گیری شبکه‌ای برساخته شد. یافته‌های این پژوهش نشان داد که مدل معطوف به تأثیر تهدیدات سایبری شامل دو مضمون فراگیرِ تهدیدات داخلی و تهدیدات خارجی می‌باشد. علاوه بر آن، برای «اعتبارسنجی» مضامین و مدل برساخته‌شده، از دو روش ارزیابی اعتبار به شیوه ارتباطی و نیز روش ممیزی و برای «پایایی‌سنجی» از دو روش قابلیت تکرارپذیری و نیز قابلیت انتقال یا تعمیم‌پذیری استفاده شده است.

کلیدواژه‌ها: تهدیدات سایبری، امنیت ملی، جمهوری اسلامی ایران، تحلیل مضمون.

۱. دانشجوی دکتری گروه جغرافیا، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
Seyyedali3023@gmail.com
۲. نویسنده مسئول:استادیار، گروه جغرافیا، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
Hojat_59_m@yahoo.com
۳. استاد، گروه علوم سیاسی و روابط بین الملل، دانشگاه گیلان، گیلان، ایران Rezasimbar@hotmail.com
۴. دانشیار، پژوهشگاه علوم اسلامی امام صادق(ع)، تهران، ایران S.bagheri6@gmail.com

مقدمه

امروزه در عصر جهانی شدن، کشورهای با تهدیدات فراوانی روبه‌رو هستند که متناسب با توسعه ارتباطات و فضای مجازی این نوع از تهدیدات نیز متنوع و پیچیده شده‌اند که از نمونه این تهدیدات می‌توان به تهدیدات فضای سایبری اشاره نمود؛ چرا که فضای سایبری و شبکه جهانی اینترنت به دلیل ماهیت عملکردی فراکشوری و نیز قابلیت برقراری ارتباط و جابه‌جایی اطلاعات و داده در مقیاس جهانی و اتصال کاربران و ابناء بشر از سراسر جهان صرف نظر از ملیت، قومیت، مذهب، نژاد، زبان و غیره، عملاً در تعارض با منافع حکومت‌ها و کشورها و دولت‌های محلی قرار می‌گیرد. به عبارتی فضای سایبری، قدرت حکومت‌ها و دولت‌های ملی و نیز حاکمیت آنها بر فضای ملی را به چالش می‌کشد. این خاصیت فضای سایبری می‌تواند به تولد و رشد نیروهای ضد حکومتی، کاهش مقبولیت حکومت‌ها نزد شهروندان، افزایش قدرت مانور نیروهای ضدحکومتی چه در مقیاس شهروندی و فضای ملی و چه در مقیاس فراکشوری و جهانی و به طورکلی امکان تهدید، تضعیف، سقوط و جابجایی دولتها و حکومت‌های ملی و ارزشهای مورد نظر آنها و جایگزینی نیروهای رقیب و نیز کاهش اقتدار حاکمیتی آنان منجر گردد. از این رو حکومت‌ها و دولت‌های ملی به تکاپو افتاده‌اند تا از پس این چالش، برایند و تهدیدات علیه خود را کاهش داده و یا از بین ببرند. آنها گاهی اوقات تهدیدات علیه خود را به تهدیدات علیه امنیت ملی بقیه، تفسیر و معنی می‌کنند و از آن بر علیه نیروهای رقیب و ضد خود استفاده می‌نمایند. بنابراین حکومت‌ها و دولت‌ها و نیروهای خود آن‌ها چه با مبدأ و مقیاس ملی و چه با مبدأ و مقیاس فراکشوری و جهانی، در فضای سایبری و بر سر فرصت‌ها و قابلیت‌های آنان با یکدیگر به رقابت و نبرد می‌پردازند و همدیگر را به چالش می‌کشند (احمدی‌پور و همکاران،۱۳۹۱).

متأثر از تهدیدات فضای سایبری می‌توان بیان داشت که حاکمیت جمهوری اسلامی نیز، به لحاظ ژئوپولیتیکی با چالش‌های ویژه قرن حاضر مواجه است؛ چرا که امروزه انگیزه‌های زیادی از قبیل ژئوپولیتیکی، جغرافیایی، اقتصادی، مذهبی، سیاسی و ... برای مبارزه با نظام جمهوری اسلامی ایران از سوی کشورهای منطقه‌ای و فرامنطقه‌ای، و گروه‌های مخالف نظام جمهوری اسلامی ایران وجود دارد که دشمنان را ترغیب به جاسوسی سایبری، خرابکاری سیابری، حمله‌های سایبری یا هدف ضربه به زیرساخت‌های جمهوری اسلامی و تلاش برای براندازی و تغییر حاکمیت آن می‌نماید. ساده‌ترین روش مبارزه با جمهوری اسلامی ایران، سعی در عدم توسعه یافتگی و اختلال در زیرساخت‌های حیاتی آن است که اجباراً باید در فضای سایبری قرار گیرند (موحدی‌صفت،۱۳۸۶). از این رو هدف از انجام این مقاله ارائه الگوی نقش تهدیدات سایبری بر امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک

است. در راستای ضرورت و اهمیت این مقاله می‌توان بیان داشت تهدیدهای سایبری برخلاف تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند و بازیگران آن را دولت-ملت‌هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارامد به حساب آید. لذا بررسی و مشخص نمودن تهدیدات فضای سایبری برای امنیت ملی ایران از اهمیت فراوانی برخوردار است؛ زیرا به دست‌اندرکاران حوزه سیاست‌گذاری و امنیتی در جهت ترسیم محیط مناسب امنیتیِ سایبری بر اساس روند تحولات جاری و آینده و همچنین ارتباط بین تهدیدات نوین از جمله تهدیدات سایبری و بروز مشکلات برای امنیت در متن منافع ملی ایران کمک کند. در راستای ضرورت مقاله نیز می‌توان بیان داشت این مقاله با ارائه درکی درست از وضعیت تهدیدات سایبری نشان می‌دهد که چگونه علیرغم برخورداری ایران از قدرت و توان سایبری، نتوانسته است با حجم بالای تهدیدات مقابله کند و استانداردهای لازم برای کاهش تهدیدات را فراهم نماید. همین موضوعات ضمن تشدید تهدیدات در بعد سایبری آن، زمینه برای رشد و گسترش انواع تهدیدات سایبری را فراهم نموده است لذا، عدم انجام این مقاله می‌تواند باعث ابهام و غفلت در نوع نگاه راهبردی ایران به فضای سایبری شود؛ زیرا عدم شناخت درست از روند گسترش و تهدیدات سایبری ضمن تأثیر منفی بر منافع ملی ایران می‌تواند در شکل‌دهی به بحران‌های متعدد مثمرثمر واقع گردد.

پیشینه پژوهش

تحقیق‌ها و بررسی‌های فراوانی درباره اینترنت، فضای مجازی، فناوری‌های نوین، فضای سایبری و آثار تحولی آن‌ها، همچنین تهدیدات ناشی از بهره‌گیری از این فضا بر امنیت ملی انجام گرفته است که در زیر به تعدادی از آنها اشاره می‌گردد:

علی‌اصغر جعفری‌لاری (۱۳۹۴) در کتاب «امنیت سایبری و جنگ سایبری» به بررسی تهدیدها، آسیب‌پذیری‌ها، تروریسم سایبری و مبانی دفاعی آن می‌پردازد. در این کتاب، داستان‌هایی واقعی از حملات سایبری و نقش دولت‌ها در جنگ سایبری و جوانب حقوقی تعارض سایبر، رویکرد نظامی آمریکا و چین در جنگ سایبری، بررسی رویکردهای بهبود فضای سایبری و هماهنگی و آمادگی دفاع در مقابل حوادث سایبری پرداخته شده است.

میرسمیعی، سیدمحمد و اصلی‌نژاد، مهدی (۱۳۹۷) در کتاب «ماهیت نبرد سایبری» به بررسی شیوه‌های جنگ نرم و تدابیر ایمنی فضای مجازی بر اساس سند راهبردی پدافند سایبر کشور

پرداخته‌اند. سیر تحول جنگ‌ها، ارزش‌های اساسی حاکم بر حوزه پدافند سایبری کشور، مأموریت قرارگاه پدافند سایبری کشور و چشم‌انداز آن، مروری بر تهدیدات فضای سایبر و ویژگی‌های این فضا، بد افزارهای رایانه‌ای و راهکارهای مقابله با نرم‌افزارهای جاسوسی برخی از فصول این کتاب هستند که نویسندگان به تشریح آنها پرداخته‌اند.

حسن‌بیگی و کولیوند (۱۳۹۶) در مقاله «ارائه الگوی راهبردی مدیریت تحولات برآمده از توسعه فناوری اطلاعات و ارتباطات بر امنیت داخلی جمهوری اسلامی ایران»، با بهره‌گیری از روش توصیفی تحلیلی و مطالعات کتابخانه‌ای معتقدند تهدیدات نوین امنیت ملی در فضای سایبر، شامل تروریسم سایبری، خرابکاری، جاسوسی و براندازی است. در این مقاله، مدیریت تحولات بر آمده 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.

غلامرضا ندری (۱۳۹۷) در رساله «سیاستگذاری امنیت اجتماعی: بررسی تأثیر شبکه‌های اجتماعی بر امنیت اجتماعی جمهوری اسلامی ایران»، شناسایی اثرات شبکه‌های اجتماعی مجازی بر امنیت اجتماعی و دگرگونی‌های بنیادین ارتباطی را که به محیط تولید و حفظ نظم و امنیت اجتماعی نفوذ پیدا نموده‌اند، مورد مطالعه قرار داده است. یافته‌های پژوهش نیز منجر به شناخت ماهیت و عملکرد شبکه‌های اجتماعی مجازی و پی بردن به سازوکارهای اثرگذاری آن در تجزیه‌وتحلیل آسیب‌پذیری امنیت اجتماعی و هدایت و سیاست‌گذاری درست در جهت رصد پیامدهای وقوع این نوآوری‌ها گردیده است.

هلیلی، ولوی و موحدی‌صفت و باقری (۱۳۹۷) در مقاله «قدرت سایبری، مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر» با استفاده از روش تجزیه‌وتحلیل آماری داده‌های کمی، فرآیند جهانی شدن، ظهور جوامع شبکه‌ای و حملات سایبری سازمان‌یافته فرامرزی را از چالش‌های جدی و نوین در دستیابی و حفظ امنیت ملی عنوان می‌نمایند. 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. نتایج این تحقیق نشان می‌دهد داشتن منابع، تجهیزات و فناوری‌های سایبری، شرط لازم برای دستیابی به امنیت ملی

است. با این وجود، درک دقیق نخبگان و سیاست‌گذاران در تدوین راهبردهای مناسب، پیش‌بینی تهدیدات و فرصت‌های بالقوه و بالفعل برای طرح‌ریزی قدرت سایبری ضروری است.

صیادی و همکاران (۱۳۹۹) در مقاله تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات‌متحده آمریکا و جمهوری اسلامی ایران، بیان می‌کنند که امروزه فناوری، اینترنت و تجارت رایانه‌ای، نقش بسزایی در ارتباطات جهانی ایفا می‌کند. این پدیده، مرز جدیدی میان دنیای سایبری و دنیای حقیقی به وجود آورده است، ولی ضعف ذاتی فناوری ارتباطات، این سامانه را در معرض تهدیدهای امنیتی بی‌شماری قرار داده است. استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای تهدیدات امنیتی ازجمله خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته است. هدف در این پژوهش، بررسی راهبرد ها و رویکردهای دو کشور ایران و آمریکا و همچنین کشف نقاط ضعف و یا کاستی های موجود در حوزه امنیت سایبری با توجه به تهدیدات موجود در فضای مجازی بوده است. در این پژوهش ضمن بررسی تهدیدات امنیتی متأثر از فضای مجازی در دو کشور ایران و آمریکا، اقدامات امنیتی در مواجهه با این تهدیدات بررسی شده است. نتایج پژوهش نشان داد که متخصصان فضای سایبری در ایران به شناسایی تهدیدهای سایبری از پیش توجه کمتری داشته و درنتیجه در حوزه امنیت ملی، به‌رغم فعالیت ها و تدابیر خوب اندیشیده شده پیشین، راهکارهای مقابله با تهدیدهای سایبری با توجه به روند تهدیدات باید به‌روزرسانی‌شده و تدابیر جدیدی اتخاذ شود. در این زمینه بایستی در زمینه بسترسازی فناوری، قانون‌گذاری و فرهنگ‌سازی، برنامه‌هایی مشخص تدوین شود و اقدامات مؤثری انجام پذیرد.

فروزان و همکاران (۱۴۰۰) در مقاله ارائه راهبردهای مصون‌سازی شناورهای رزمی در برابر تهدیدات سایبری، بیان می‌کنند که نگرشی تحقیقی به آمار و سوابق نشان می‌دهد که یکی از تهدیدات مهم شناورهای رزمی، تهدیدات سایبری علیه زیرساخت های حیاتی و حساس سایبری و متکی به سایبر شناورهای رزمی می‌باشد. به‌منظور مقابله با این تهدیدات، کاهش آسیب‌پذیری و تداوم عملکرد شناور در دریا نیاز به راهکارها و راهبردهایی می‌باشد که در این تحقیق به عنوان هدف اصلی مطرح گردیده و بر این اساس محقق به دنبال پاسخ به این سؤال است که راهبردهای مصون سازی شناورهای رزمی در برابر تهدیدات سایبری چیست؟ این تحقیق از نوع کاربردی- توسعه‌ای است و روش آن اکتشافی و موردی- زمینه‌ای با رویکرد آمیخته می‌باشد. جامعه آماری این تحقیق به دلیل محدود بودن متخصصین آشنا به حوزه پدافند غیرعامل و تهدیدات سایبری شناورهای رزمی با حجم نمونه یکی بوده و از تعداد ۳۰ نفر کارشناسان خبره تشکیل گردیده است و روش نمونه‌گیری تمام شمار می‌باشد. پس از بررسی

اسناد بالادستی، اسناد حوزه‌های پدافند سایبری و شناورهای رزمی، در بخش کیفی به روش تحلیل محتوا و در بخش کمی توسط نرم‌افزار آماری، تجزیه‌وتحلیل ها انجام پذیرفت. در ارزیابی محیطی تعداد ۲۶ عامل در حوزه‌های داخلی و خارجی شناسایی شد و با استفاده از روش دیوید راهبردهای مصون‌سازی تدوین گردید. نتایج تحقیق نشان می‌دهد که با تلاش در جهت اجرای راهبردها و سازمان‌دهی ساختار تجهیزاتی، بومی‌سازی، ایجاد سامانه‌های امداد و نجات تخصصی، ایجاد سامانه‌های امنیتی صنعتی و طراحی نظام عملیاتی سایبری در شناور رزمی می توان زیرساخت‌های سایبری و متکی به سایبر شناورهای رزمی را در برابر تهدیدات سایبری به میزان قابل‌قبول و بالایی مصونیت بخشید.

کرامر فرانکلین[1] و همکاران (۲۰۱۰) در مقاله «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.

نای[2] (۲۰۱۷) در مقاله‌ای با عنوان «منع و بازدارندگی در فضای سایبری» معنای بازدارندگی را بسیار گسترده‌تر از آن می‌داند که مردم می‌پندارند و صرفاً بر نیروی نظامی تکیه ندارد. وی در ادامه عنوان می‌نماید: در بازدارندگی عنصر روانشناسی نیز بسیار اهمیت دارد و در صورت عدم امکان فهم یکسان طرفین، شکست خواهد خورد. وی در یافته‌های خود از این پژوهش نشان می‌دهد که مفهوم بازدارندگی از زمانهای قبل از بمب هسته‌ای هم وجود داشته و اکنون نیز در صورت تغییر درک ما و گسترش مفهوم، می‌توان آن را به فضای سایبر اطلاق کرد.

کتاب استراتژی امنیت ملی سایبری ایالات متحده آمریکا (۲۰۱۸) سندی است که به فضای مجازی به عنوان موتور رشد باز اقتصادی و پایداری ملی نگریسته و توسعه اینترنت نامحدود را در تمام دنیا و استفاده از آن را برای افزایش نفوذ آمریکا مورد تشویق قرار می‌دهد. اهداف اصلی این سند عبارتند از: ایجاد زیرساخت‌های حیاتی، شبکه‌های فدرال و سیستم‌های دولتی برای مبارزه با جرائم سایبری، بهبود گزارش حملات سایبری در ۱۵ سال اخیر آمریکا، آموزش نیروهای سایبری با مهارت بسیار زیاد، تعیین استاندارد رفتار مسئولانه دولتی.

1.Kramer Franklyn
2.Joseph Nye

میک راد[1] (۲۰۱۸) در کتاب «امنیت سایبری در چین» بیان می‌کند که چین به طور فزاینده‌ای به دارایی‌های مختلف سایبری وابسته است و بر این اساس، مقامات چینی بر اقدامات امنیتی سایبری و همچنین افزایش آمادگی این کشور برای استفاده از فرصت‌هایی که اینترنت فراهم می‌کند و پاسخ دادن به تهدیدات امنیت ملی تأکید بسیاری کرده‌اند. این سند، اهداف چین برای نوآوری بومی در فناوری را نشان می‌دهد و لزوم افزایش سرمایه‌گذاری در تحقیق و توسعه را به رسمیت می‌شناسد.

مزدوران سایبری: «دولت، هکرها و قدرت» (۲۰۱۸) اثر مکتوب دانشگاه کمبریج در حوزه امنیت سایبری است که به بررسی روابط پنهان میان دولت‌ها و هکرها در سال‌های اخیر پرداخته است. این کتاب به منظور پدید آوردن درک بهتر از تأثیر و خطرات روابط جانشینی میان دولت‌ها و هکرها، به بررسی موشکافانه نتایج راهبردی و هزینه اجرای عملیات رایانه‌های کشورها علیه یکدیگر و مطالعه موردی راهبرد جنگ سایبری نیابتی ایالات متحده، ایران، سوریه، روسیه و چین پرداخته است.

بی‌نام (۲۰۲۰) در مقاله «چرا امنیت سایبری برای امنیت میهن حیاتی است؟» بیان کرده است ایالات متحده هر ساله با هزاران تهدید از طرف دولت‌های خارجی، سازمان های تروریستی و افرادی که قصد ایجاد هرج و مرج دارند روبه‌رو می‌شود. مأموریت وزارت امنیت داخلی در حفاظت از منافع و دارایی‌های آمریکا در سال‌های اخیر بسیار دشوارتر شده است. ارتباط متقابل سیستم‌های حیاتی، آسیب‌پذیری‌های بزرگ در امنیت شبکه و حجم گسترده‌ای از اطلاعات که باید پردازش شود، ماهیت متحول تهدیدهایی را نشان می‌دهد که وزارت امنیت داخلی باید روزانه مرتفع کند. وزارت امنیت داخلی با افزایش تهدیدات سایبری سازگاری دارد و از ابزار کلان داده برای امنیت بیشتر کشور و زیرساخت‌های آن استفاده می‌کند.

راندل[2] (۲۰۲۱) در مقاله «گزارش هشدارها و باج‌افزار[3]، تهدیدی برای امنیت ملی است» بیان می‌کند که مقامات دولتی و کارشناسان امنیت سایبری باج‌افزار را تهدیدی جدی برای امنیت ملی می‌دانند و پیشنهاد می‌کنند که دولت فدرال با همان ابزارهایی که برای پیگرد کارتل‌های مواد مخدر و سایر سازمان‌های جنایتکار استفاده می‌شود، به دنبال باندهای باج‌افزار برود. فیلیپ راینر، مدیر اجرایی مؤسسه امنیت و فناوری، یک سازمان غیرانتفاعی امنیت سایبری، گفته است: «افزایش حملات به دولت‌ها، مدارس و سازمان‌های بهداشتی در طی شیوع ویروس کرونا نشان‌دهنده خطر باج‌افزار است.»

1.Mikk Raud
2.James Rundle
3. Ransomware

در پیشینه‌های بررسی شده موضوعاتی از جمله «سیستم‌های دولتی برای مبارزه با جرائم سایبری»، «افزایش آمادگی دولت‌ها برای پاسخ دادن به تهدیدات امنیت ملی»، «جرائم سایبری» و «تروریسم سایبری پرداخته شده است. اما نقش «تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک» مغفول واقع شده است. بنابراین پژوهش پیش رو تلاش دارد تا تهدیدات سایبری و نقش این تهدیدات در تضعیف امنیت ملی ایران را مورد بررسی قرار دهد و خلاء موجود در این زمینه را برطرف نماید. لذا در راستای نوآوری مقاله می‌توان بیان داشت به رغم نو بودن پدیده و موضوع قدرت سایبری در جهان و ایران، پژوهش‌های متعددی که درباره آن و سایر موضوعات مرتبط با آن مانند فناوری‌های نوین ارتباطی، شبکه‌های اجتماعی، اینترنت، قدرت نرم، رسانه‌های نوین اجتماعی و ... انجام شده، هنوز به طور شایسته و دقیق، قدرت سایبری از منظر تهدید بر شئونات امنیت و به ویژه امنیت ملی کشور جمهوری اسلامی ایران از منظر ژئوپولیتیک مورد بررسی قرار نگرفته است. به عبارتی همین وضعیت موجب شده که در سطوح تصمیم‌گیری و تصمیم‌سازی کشور به طورکلی شناخت دقیقی راجع به تهدیدات سایبری و نقش و تأثیر آن‌ها در جامعه حال و آینده وجود نداشته باشد.

روش تحقیق

پژوهش حاضر به لحاظ ماهیت در زمره تحقیقات اکتشافی، به لحاظ نوع تحقیق کاربردی و به لحاظ استراتژی پژوهش دارای استراتژی استقرایی و به لحاظ ماهیت داده‌ها در زمره طرح پژوهشی کیفی و از نوع تحلیل مضمون بوده است. جامعه آماری تحقیق شامل خبرگان دانشگاهی و اجرایی در رشته مطالعات امنیتی به ویژه فضای سایبری و تهدیدات آن بوده است که از طریق روش نمونه‌گیری نظری انتخاب شده‌اند که این روش در پژوهش‌های کیفی، به عنوان استاندارد طلایی پایان نمونه‌گیری در نظر گرفته می‌شود و به معنای انتخاب هدف‌دار واحدهای پژوهش برای کسب دانش یا اطلاعات، سعی در شناخت بهتر هر پدیده در زمینه خاص دارد. در نمونه‌گیری نظری که به عنوان روش غالب در تئوری زمینه‌ای شناخته می‌شود، نمونه‌ها به شکلی انتخاب می‌شوند که به خلق تئوری کمک کنند(Giaser and Strauss,1968: 271). در ابتدا پژوهشگر بر اساس قضاوت خود از بهترین منابع اطلاعاتی از قبیل مشاهده، مصاحبه یا منابع مکتوب، بهترین انتخاب‌ها را انجام می‌دهد و سپس به‌دنبال نمونه‌هایی می‌رود که تئوری ایجاد شده را کامل کنند. در تئوری زمینه‌ای ابتدا نمونه‌گیری به صورت آسان آغاز می‌شود و سپس به صورت هدفمند در جهت حداکثر تفاوت برای مفاهیم ایجاد شده حرکت می‌کند و نهایتا به نمونه‌گیری نظری می‌رسد (Munhaii PL, 2012). پایان نمونه‌گیری نظری

نیز بر اساس اشباع داده‌ها مشخص می‌شود. لذا داده‌های پژوهش پس از انجام مصاحبه نیمه‌ساخت‌یافته (نیمه‌استاندارد) با ۲۵ مصاحبه، به حالت اشباع نظری رسید و انجام مصاحبه متوقف شد.

در تعریف مضمون می توان چنین گفت: «مضمون الگویی است که در داده‌ها یافت می‌شود که به توصیف، سازماندهی مشاهدات و تفسیر جنبه‌هایی از پدیده می‌پردازد. این روش، واحدی برای تحلیل داده‌های متنی است و داده‌های متنوع و پراکنده را به داده‌های فنی و تفصیلی تبدیل می‌کند» (Braun and Clarke, and Others, 2011: 153). تحلیل مضمون به روش‌های مختلف انجام می‌گیرد که در این پژوهش از شبکه مضامین[1] (برای نشان دادن ارتباط و وابستگی مضامین) استفاده شده است. شبکه مضامین روشی در تحلیل مضامین است که آترایدِ استیرلینگ[2] (۲۰۰۱) آن را توسعه داده است. برای دستیابی به شبکه مضامین باید مراحل ذیل انجام شود:

الف) کشف مضامین اصلی و (شناسه‌ها و نکات کلیدی متن)،

ب) کشف مضامین سازمان‌یافته (مضامین به دست آمده از تلخیص و ترکیب مضمون های پایه‌ای) و

ج) کشف مضامین فراگیر (مضامین عالی در برگیرنده اصول حاکم بر متن به عنوان یک کل).

بعد از طی این مراحل، مضمون‌های به دست آمده به صورت نقشه‌های شبکه وب ترسیم می‌شوند که در آن مضامین برجسته همراه با روابط میان آنها نشان داده می شود. مضامین فراگیر در کانون شبکه مضامین قرار می‌گیرد؛ مضامین سازمان‌یافته واسط مضامین فراگیر و مضامین پایه‌ای شبکه است (Abedi Jafari and Others, 2011: 170 Quoted from).

علاوه بر آن، جهت اعتبارسنجی (قابلیت اطمینان و باورپذیری) مضامین و نیز مدل برساخته شده از دو روش ارزیابی اعتبار به شیوه ارتباطی که به معنای رجوع به مشارکت‌کنندگان (در اینجا مصاحبه‌شوندگان) است (Felik, 2006: 415) و نیز روش ممیزی (رجوع به خبرگان و ارزیابان) استفاده شده است. همچنین برای پایایی‌سنجی مضامین از دو روش قابلیت تکرارپذیری و نیز قابلیت انتقال و یا تعمیم‌پذیری استفاده شده است. قابلیت تکرارپذیری به واسطه روش ضریب توافق درونی بین دو کدگذاری در رابطه فرایند کدگذاری اطلاق می‌شود (Sarookhani, 2008: 289). لذا ناهماهنگی‌های به وجود آمده از طریق بازنگری در فرایند کدگذاری داده‌ها مرتفع شده است. همچنین به منظور قابلیت انتقال یا تعمیم پذیری سعی شد تا حد امکان از صاحبنظران مختلف حوزه های دانشگاهی و نیز اجرایی

1.Thematic Network
2. Atride Stirling

مرتبط با موضوع تحقیق در پژوهش استفاده شود؛ یعنی سعی شده است که نمونه‌گیری نظری به طور منظم و جامع انجام گیرد (Astrauss and Karbin, 2018: 284-283).

بسط فضای مفهومی پژوهش

الف) فضای سایبری

مفهوم فضای سایبر برای اولین بار توسط «ویلیام گیبسون»[1] نویسنده داستان‌های علمی- تخیلی در سال ۱۹۸۴ ارائه گردید (Gibson, 1984). تعریف‌های ارائه شده از فضای سایبری، معانی مختلفی از این مفهوم را به دست می‌دهند. دسته اول از این تعاریف، فضای سایبری را غیرواقعی تلقی می‌کنند و بر این باور هستند که این فضا در عرض دنیای واقعی قرار دارد. دومین دسته از تعریف‌ها، این فضا را محلی برای انتقال اطلاعات دانسته‌اند. دسته‌ای دیگر از تعاریف نیز با دریچه سخت‌افزاری به فضای سایبری می‌نگرند و این فضا را متشکل از اتصال تعداد بسیاری از سیستم‌ها می‌دانند. یکی از تعریف‌ها بر اساس فرهنگ لغت «مریام وبستر»[2] اشاره می‌کند که فضای سایبر دنیای آنلاین از شبکه‌های کامپیوتری است. تعریف دیگر که از سوی وزارت دفاع آمریکا ارائه شده است، اشاره می‌کند که فضای مجازی قلمرویی جهانی در فضای اطلاعات است که این محیط شبکه‌ای متصل به هم از زیرساخت‌ها را تشکیل داده است. این فضا در بردارنده شبکه‌های ارتباطات، سامانه‌ها، کنترل‌کننده‌ها و پردازشگرها است. تعریف دیگر از فضای سایبری که از سوی وینگفیلد[3] ارائه شده است، بیان می‌دارد که این فضا یک محیط فیزیکی محسوب نمی‌شود؛ بلکه فضایی است که از آن با عنوان «شبکه فراگیر جهانی» یاد می‌شود (ولی‌زاده،۱۳۹۹: ۵-۴). نکته بسیار مهم در بحث فضای سایبری خطرات این فضا برای امنیت و منافع ملی است. از جمله اینکه فضای مجازی تبادل اطلاعات، این فرصت را به خاطیان عرصه اجتماعی داده تا اعمال تروریستی خود را به آسانی با استفاده از این فضا متحول سازند. با توجه به اینکه فضای سایبری دنیای بیکرانی از امکانات و قابلیت‌های بیشمار است که بدون محدودیت در دسترس همگان قرار دارد و هرکس با هر انگیزه و هدفی می‌تواند از این موهبت بهره‌برداری کند (علیدوست و پورقهرمانی، ۱۳۹۸: ۲-۹).

1.William Gibson
2.Merriam Webster
3.Wingfield

ب) قدرت سایبری

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 سایبری یا از طریق فضای سایبر انجام گیرد. در دوران معاصر، ظهور مفاهیمی مانند قدرت سخت، قدرت نرم و قدرت هوشمند بیانگر جابجایی و چرخش نشانگر قدرت به سوی 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 مسأله حاکی از عمق نفوذ فضای سایبر در تمامی حوزه‌های راهبردی کشور است. بنابراین دغدغه اصلی شکل‌گیری این تحقیق، تبیین نقش و جایگاه قدرت سایبری به عنوان عاملی اساسی برای مقابله با تهدیدات عینی و ذهنی فضای سایبر و ارتقاء امنیت ملی است. بنابراین می‌توان قدرت سایبری را توانایی به‌کارگیری منابع، ظرفیت‌ها و قابلیت‌های مبتنی بر فضای سایبر به منظور پشتیبانی از قدرت ملی و دستیابی به اهداف راهبردی در فضای سایبر و خارج از آن دانست (هلیلی و همکاران،۱۳۹۷: ۱۷۶).

ج) تهدیدهای سایبری و ویژگی‌های آن‌ها

تهدیدهای سایبری پدیده‌ای جدید است که در دهه‌های اخیر، همزمان با تحول فناوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به‌گونه‌ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت جدید تهدیدهای سایبری و ویژگی‌ها و نمودهای منحصربفردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید (وظیفه‌دان،۱۳۹۵: ۱۶۰-۱۶۱) چرا که با افزایش فعالیت‌ها به‌ویژه در مشاغل الکترونیکی اهمیت امنیت سایبری نیز افزایش یافت و اکنون این حوزه یکی از حیاتی‌ترین بخش‌های مشاغل مختلف به حساب می‌آید. نادیده گرفتن امنیت سایبری می‌تواند باعث استخراج غیرقانونی داده‌ها شود و عوارض مخربی را به جای بگذارد (Sarfraz & Noor, 2020: 1-4). بنابراین می‌توان بیان داشت که فضای سایبری و شبکه جهانی اینترنت به دلیل ماهیت عملکردی فراکشوری و نیز قابلیت برقراری ارتباط و جابه‌جایی اطلاعات و داده در مقیاس جهانی و اتصال کاربران و ابناء بشر از سراسر جهان صرف‌نظر از ملیت، قومیت، مذهب، نژاد، زبان و غیره، عملاً در تعارض با منافع حکومت‌ها و کشورها و دولت‌های محلی قرار می‌گیرد. به عبارتی فضای سایبری، قدرت حکومت‌ها و دولت‌های ملی و نیز حاکمیت آن‌ها بر

فضای ملی را به چالش می‌کشد. این خاصیت فضای سایبری می‌تواند به تولد و رشد نیروهای ضدحکومتی، کاهش مقبولیت حکومت‌ها نزد شهروندان، افزایش قدرت مانور نیروهای ضدحکومتی چه در مقیاس شهروندی و فضای ملی و چه در مقیاس فراکشوری و جهانی و به طورکلی امکان تهدید، تضعیف، سقوط و جابجایی دولت‌ها و حکومت‌های ملی و ارزش‌های مورد نظر آنها و جایگزینی نیروهای رقیب و نیز کاهش اقتدار حاکمیتی آنان منجر گردد. به عنوان مثال می‌توان به شایعه‌پراکنی و دروغ‌پردازی و همچنین اختلال در کارکرد نهادها را از جمله تهدیدات فضای سایبری به حساب آورد. در اینترنت، به ویژه هنگامی که اطلاعات موجود نباشد، شایعات ممکن است قبل از اطلاع رسانی درست منابع معتبر، گسترش یابد (Tim & San, 2020: 1-10).

از این رو حکومت‌ها و دولت‌های ملی به تکاپو افتاده‌اند تا از پس این چالش، برآیند و تهدیدات علیه خود را کاهش داده و یا از بین ببرند. دنیای امروز که دنیای رایانه بوده و در ارتباط با زندگی مردم است، هر لحظه مورد تهدید تروریست‌هاست. این نگرانی و احتمال وقوع این اتفاق، روزبه‌روز مردم جوامع را دچار ترس و وحشت می‌کند. تروریست‌ها با استفاده از رایانه‌ها می‌توانند در بین مردم ترس و وحشت ایجاد کرده و با از کار انداختن امکانات فنی، رایانه‌ها را که زندگی اقتصادی و اجتماعی و حتی فرهنگی و سیاسی مردم وابسته به آن است، در مقیاس وسیعی بر آنها زیان رسانده و در سطح گسترده‌ای، جنگ رسانه‌ای و کُشت و کشتار راه بیندازند و از این طریق و نیز از طریق تهدید به حمله بیشتر، از طرف‌های مقابل خود امتیاز بگیرند (طیب،۱۳۸۴: ۸۹). فضای سایبری، همچون فضای فیزیکی، فضایی واقعی محسوب می‌شود که بسیاری از امور روزانه شهروندان در آن انجام می‌گیرد. با رشد روزافزون فضای سایبری، بر پیچیدگی‌های آن نیز افزوده می‌گردد و در کنار فرصت‌های متعددی که این فضا برای بشر به ارمغان می‌آورد، تهدیدهای آن نیز به مرور شناسایی می‌شود. شناخت و فهم صحیح این تهدیدات، نخستین گام برای مقابله با آن‌ها محسوب می‌شود (ولی‌زاده،۱۳۹۹: ۲). تهدیدهای سایبری ویژگی‌های خاصی دارند. از یک سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران زیادی به این عرصه وارد شوند (خلیلی‌پور و نورعلی‌وند،۱۳۹۱).

د) امنیت از منظر ژئوپولیتیک

ملاحظات امنیت ملی هر کشوری از عوامل کلانی تأثیر می‌پذیرد. این عوامل با توجه به استثنائات ملی و نقش عوامل زیربنایی هر یک از دولت- ملت‌ها، از تفاوت‌هایی برخوردار است. به عنوان مثال

نقش عامل ژئوپولیتیک در تأثیربخشی بر تصمیم‌گیری‌های ملی، برای تمامی کشورها از جایگاه یکسانی برخوردار نیست. چه بسا این عامل کشوری را کاملاً در تنگنا قرار دهد و مسیر سیاست‌گذاری‌ها را به تنهایی شکل دهد و چه بسا در نزد کشوری دیگر با توجه به نوع نگاه بیرونی به آن، از اهمیت زیادی برخوردار نباشد. از سوی دیگر، باید توجه داشت که نگاه به همین عامل ممکن است در اثر مرور زمان و با تغییرات راهبردی، دچار تحول گردد. یکی از مهم‌ترین شاخص‌های تأثیرگذار بر ملاحظات امنیت ملی، نقش عوامل طبیعی و جایگاه یک کشور در مجموعه نظام جهانی است که به ژئوپولیتیک تعبیر می‌شود (بصیرت، ۱۳۹۲). خلیلی و همکارانش در تعریفی از ژئوپولیتیک آورده‌اند: ژئوپولیتیک تأثیر عوامل جغرافیایی بر سیاست و روابط دولت‌ها و جزو عوامل تأثیرگذار بر تولید قدرت است. حافظ‌نیا معتقد است: دانش ژئوپولیتیک، به مطالعه ابعاد فضای جغرافیایی مناسبات قدرت و رفتار سیاسی بازیگران عرصه ملی و بین‌المللی می‌پردازد. قالیباف و همکارانش در مقاله‌ای عنوان نموده‌اند که ژئوپولیتیک به عنوان یک عرصه مطالعاتی می‌تواند راهبردهای سیاست خارجی کشورها در حوزه امنیت ملی تعیین و اولویت سیاسی آن‌ها را مشخص سازد. احمدی‌پور و لشگری معتقدند همان طور که عوامل ژئوپولیتیک یک کشور می‌تواند تولیدکننده فرصت برای یک کشور باشد، به همان شکل می‌تواند محدودیت‌هایی را برای کشورها ایجاد کند. برخی از ژئوپولیتیسین‌ها معتقدند: عوامل جغرافیایی، سیاست و استراتژی ملی کشور را در حوزه ژئوپولیتیک منفعل و برای آن کشور، نوعی چالش ژئوپولیتیک ایجاد کند. برخی دیگر عنوان می‌نمایند: به طورکلی، ژئوپولیتیک علاوه بر کارکردهایی که در «سیاست قدرت» دارند، در نگرش بخشی به هویت کشور و شکل‌گیری و تعریف منافع ملی و امنیت ملی در داخل و خارج، تأثیرات مشهودی دارند (علی‌حسینی،۱۳۹۶).

گراهام فولر[1] در کتاب «قبله عالم: ژئوپلیتیک ایران» تصریح می‌نماید: شناخت ژئوپولیتیک بخشی یک فن قدیمی است که در هیأت کلاسیک خود بر جغرافیا به عنوان عامل تعیین کننده اصلی رفتار یک دولت تأکید می‌کند(فولر،۱۳۷۷: ۲). پیروز مجتهدزاده نیز در تبیین اهمیت ژئوپولیتیک و نقش‌آفرینی آن در نظام‌های سیاسی کشورها عنوان می‌نماید: «بر هر ملتی است که هوشیارانه پیگیر نقش آفرینی مکانیزم جغرافیای سیاسی در داخل کشور خود و در منطقه و چگونگی دگرگونی‌ها در نظام ژئوپولیتیک جهانی و منطقه‌ای باشد و شرایطی را فراهم آورد تا این نقش‌آفرینی‌ها و این دگرگونی‌ها در محیطی به دور از واکنش‌ها و کوششهای دسیسه‌آمیزِ قدرت‌های فرامنطقه‌ای شکل گیرند ... بر ایرانیان نیز چاره‌ای نیست جز این که با گسترش جنبه‌های کاربردی جغرافیای سیاسی و ژئوپولیتیک در

1.Graham Fuller

این مرز و بوم، بتوانند توانمندی سیاسی، اقتصادی، استراتژیک و استعدادهای محیطی را از ژرفای موقعیت و زمینه‌های جغرافیای ایرانی بیرون کشند و جغرافیای کشور را در عمل به «قدرت» تبدیل نمایند ... هر ملتی در این راه خطیر دو وظیفه دارد: نخست این که هوشیارانه به پیرامون خویش بنگرد. تمهیدات دیگران را در راستای جا انداختن ژئوپولیتیک ویژه‌شان بشناسد و اگر تمهیدات و آن ژئوپولیتیک را به زیان منافع ملی خود یافت، در راه خنثی ساختن آن بکوشد. دوم این که هوشیارانه تلاش کند تا ژئوپولیتیک ویژه خود را که متکی بر منافع ملی است در جهان، یا دست کم، در منطقه خود جا اندازد.» (مجتهدزاده،۱۳۸۱).

نظریه‌ها و رهیافت‌های قدرت سایبری

نظریه‌های متعددی در حوزه قدرت سایبری وجود دارد که در این بخش به تعدادی از آنها به طور خلاصه در جدول زیر به آنه اشاره می‌گردد و نظریه جوزف نای[1] به عنوان نظریه اصلی که چارچوب مقاله بر مبنای آن به موضوع پرداخته است، بیان می‌شود.

جدول ۱. نظریه‌های مرتبط با قدرت سایبری و تهدیدهای ناشی از آن

ردیف	نام نظریه‌پرداز	مشخصه قدرت سایبری	تهدید ناشی از قدرت سایبری
۱	ریچارد کلارک (Cornis and Et al, 2010: 12-13)	جنگ سایبری شکل جدیدی از مبارزه است که ما هنوز نمی‌توانیم آن را به طور کامل درک کنیم.	در دنیای امروز، میدان جنگ حوزه خود را به فضای سایبری گسترش داده و باید آن را به عنوان پنجمین عرصه جنگ در کنار عرصه‌های سنتی زمین، هوا، دریا و فضا در نظر گرفت.
۲	امانوئل کاستلز (کاستلز، ۱۳۸۵، ج۱: ۶۰-۱۱۳)	اطلاعات و ارتباطات، بیشتر از طریق شبکه جهانی اینترنت، ماهواره‌ها و خبرگزاریها انتشار می‌یابد، بازی سیاسی به گونه فزاینده‌ای در فضای رسانه‌ها انجام می‌شود.	ویژگی تمامی انقلاب‌های فناورانه این است که تمامی قلمرو فعالیت انسانی را تحت تأثیر قرار می‌دهند، به این معنا که به عنوان بافتاری که فعالیت انسانی در آن جاری است، عمل می‌کند. فناوری اطلاعات و توانایی کاربرد و سازگار کردن آن را عامل حیاتی در تولید و دسترسی به ثروت، قدرت و دانش در عصر حاضر می‌داند.

1.Joseph Nye

ردیف	نام نظریه‌پرداز	مشخصه قدرت سایبری	تهدید ناشی از قدرت سایبری
۳	تافلر (آلبرتس و پاپ،۱۳۸۵: ۵۱)	در عصر اطلاعات، آن دسته از دولت‌هایی که از فناوری‌های عصر اطلاعات استفاده می‌کنند و بیشترین منافع را از آن‌ها به دست می‌آورند، در قله ساختار قدرت جهانی سه‌گانه قرار خواهند گرفت که تحت سیطره دانش و امور نامحسوس مرتبط با دانش است.	توانمندی این گونه دولت‌ها، برتر از کشورهایی خواهد بود که وابستگی خویش به اقتصاد صنعتی یا کشاورزی را حفظ کنند.
۴	شالدون (Sheldon, 2011)	قدرت سایبری را یک ابزار مکمل برای قدرت ملی می‌داند که می‌تواند برای استفاده توسط دولتمردان یک کشور جذاب باشد. چهار لایه برای فضای سایبری پیشنهاد می‌گردد. این لایه‌ها عبارتند از: زیرساخت، فیزیکی، ساختاری و معنایی.	قدرت سایبری توانایی دستیابی به اهداف راهبردی و کاهش توانایی دشمن در بهره‌برداری یا حمله به زیرساخت‌های فضای سایبر است.
۵	یورگن هابر ماس (نورمحمدی،۱۳۹۰)	می‌توان از اینترنت برای توانمندسازی جنبش‌های مدنی، اجتماعی و سیاسی استفاده کرد. اینترنت با امکاناتی که در تشکل‌سازی مجازی آسان و ناپیدا دارد، فرآیند شکل‌گیری جنبش‌های مدنی و سیاسی را نه تنها ایجاد می‌کند بلکه توسعه و تشویق می‌نماید.	در این فضا، جنبش‌سازی و فعالیت اعتراضی نه تنها آسان بلکه کم خطرتر از فضای واقعی است.
۶	زیمت و باری Zemit and) (Barry,2009	قدرت سایبری قابلیت کنترل سامانه‌های فناوری اطلاعات و شبکه‌های فضای سایبر را دارد.	برای انجام مأموریت‌های نظامی و پشتیبانی از حوزه‌های اقتصادی و سیاسی قابل استفاده است.
۷	اسپید (Spade, 2012)	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.	دستیابی به قدرت سایبری به توانایی دولت برای توسعه منابع برای عملیات در فضای سایبر متکی است.

نظریه جوزف نای: فضای سایبر، کلید قدرت در قرن ۲۱ خواهد بود.

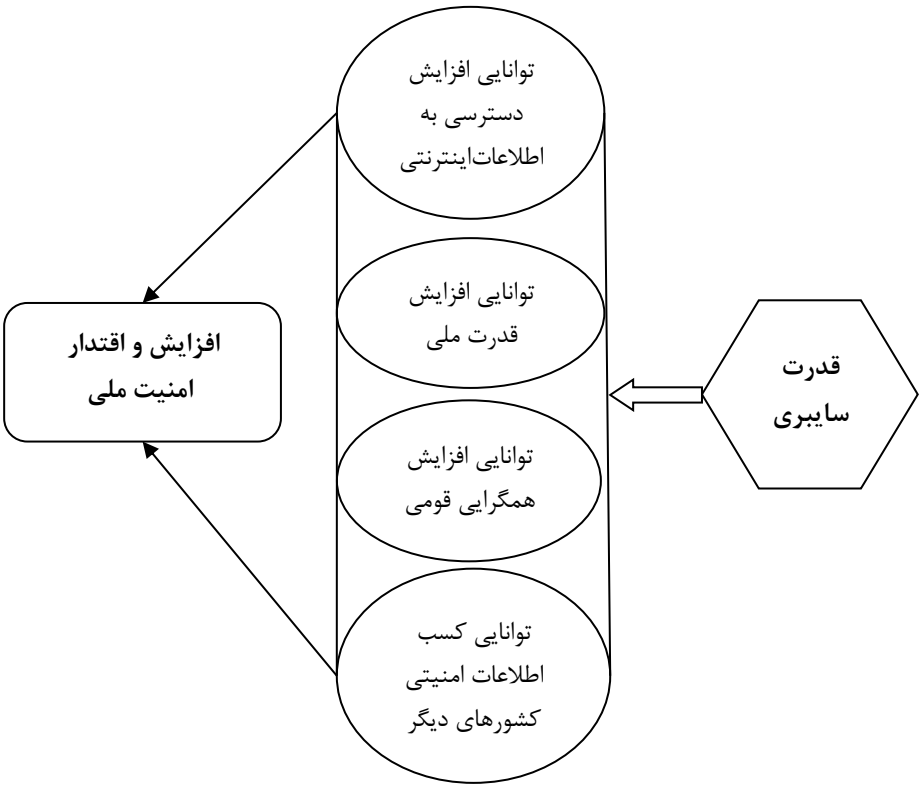
نای قدرت سایبر را احراز نتایج ترجیحی از طریق استفاده از منابع اطلاعاتی به هم پیوسته الکترونیکی در حوزه سایبر تعریف می‌کند. وی برای قدرت سایبری دو بعد قائل است: وجه فیزیکی قدرت سایبر و وجه مجازی قدرت سایبر. بر همین اساس، اهداف و مرجع نهایی قدرت سایبر را نیز در

دو حوزه دسته‌بندی می‌کند. دسته اول، در درون فضای سایبر اتفاق می‌افتد که وجه سخت و نرم دارد. مانند «حملات سایبری» که در وجه سخت جای می‌گیرد. تأثیرگذاری بر ارزش‌ها و معیارهای زندگی دیگران 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 به عنوان وجه سخت و استفاده از فضای سایبر برای دیپلماسی عمومی در عرصه روابط خارجی و بین‌المللی کشور به عنوان وجه نرم یاد می‌کند. آنچه که نای انجام داده است، بی‌شک مهم‌ترین بستری است که سایر محققین و پژوهشگران می‌توانند از آن بهره‌برداری کنند. اما نای به بررسی رویکردهای تئوریک نسبت به فضای سایبر و این که جریان اصلی روابط بین‌الملل و سایر نظریه‌های اجتماعی نسبت به آن چه دیدگاهی دارند، مطلب زیادی به ما نمی‌گوید. از سوی دیگر وی، به تمام وجوه قدرت به ویژه مقایسه قدرت در فضای سایبر با آنچه که نظریه‌های اجتماعی و پست مدرن از آن به عنوان وجه نامرئی قدرت یاد می‌کنند، اشاره‌ای نمی‌کند (زابلی‌زاده و وهاب‌پور،۱۳۹۷).

وی در ادامه می‌افزاید: منابع قدرت عموماً در حال تغییرند؛ بدین گونه که به تدریج تأکید کمتری روی نیروی نظامی به عنوان منبع قدرت انجام می‌گیرد. امروزه در ارزیابی قدرت بین‌المللی، عواملی همچون فناوری، آموزش و رشد اقتصادی اهمیت بیشتری یافته‌اند و در همین حال، اهمیت جغرافیا و مواد خام کاهش یافته است. با نگاهی به قرون گذشته روشن می‌شود که در هر دوره، منابع متفاوتی از قدرت نقش بیشتری ایفا کرده‌اند. منابع قدرت هیچگاه حالت ایستا ندارد و در دنیای امروز نیز همچنان تغییرات را تجربه می‌کند (نای،۱۳۸۷: ۹۸).

جوزف نای برای تبیین و تشریح قدرت در عصر اطلاعات از مفهوم «انتشار قدرت» بهره می‌گیرد. وی قدرت وابسته به فضای سایبری را یکی از مهم‌ترین زمینه‌های جدید در سیاست جهانی دانسته و آن را اینگونه تعریف می‌کند: «قدرت سایبری توانایی به دست آوردن نتایج ترجیح داده شده از طریق استفاده از منابع الکترونیکی در ارتباط با اطلاعات در دامنه سایبری است» (Nye,2010:4). او می‌افزاید؛ قیمت پایین ورود، گمنامی، آسیب‌پذیری و نامتقارن بودن به این معنی است که بازیگران کوچکتر، از ظرفیت بیشتری برای اعمال قدرت سخت و نرم در فضای سایبری در حوزه‌های سنتی‌تر سیاست جهانی برخوردارند. از ویژگی‌های فضای سایبری این است که تفاوت قدرت میان بازیگران را کاهش می‌دهد و زمینه انتشار قدرت را فراهم می‌کند که مشکل تمامی کشورها در عصر اطلاعات بوده و نشانگر سیاست جهانی در قرن ۲۱ است. نای اضافه می‌کند که بزرگترین قدرت، بعید است که قادر به تسلط در این حوزه به اندازه دیگر حوزه‌ها، همچون دریا و هوا باشد. با وجود این، فضای سایبری این نکته را

نشان می‌دهد که انتشار قدرت به معنی برابری قدرت یا جایگزینی دولت به عنوان قدرتمندترین بازیگر در سیاست جهانی نیست (Nye,2010:19).



نمودار ۱. مدل مفهومی (طراحی شده توسط نویسندگان)

یافته‌های کیفی پژوهش

در ادامه به تحلیل داده های حاصل از مصاحبه نیمه‌ساخت‌یافته (نیمه استاندارد) با خبرگان حوزه فضای سایبری به منظور ارائه مدل تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران پرداخته شده است. جامعه آماری این پژوهش شامل ۲۵ نفر از خبرگان دانشگاهی و متخصصان حوزه‌های مطالعات امنیتی به ویژه فضای سایبری و تهدیدات آن بوده است. از این تعداد، ۱۵ نفر دارای تخصص و تحصیلات در علوم رایانه‌ای و سایبری، ۷ نفر دارای تخصص و تحصیلات مطالعات امنیتی و ۳ نفر نیز دانش آموخته و متخصص در حوزه‌های علوم سیاسی، روابط بین‌الملل و جغرافیای سیاسی بوده‌اند. ۱۰ نفر آنها از مدیران مراکز سایبری در نیروهای مسلح و سازمان‌های اطلاعاتی جمهوری

اسلامی ایران بوده، ۱۲ نفر کارشناس ارشد اجرایی در نهادهای یاد شده و ۳ نفر دارای مطالعات، کتاب و مقاله در حوزه‌های سایبری و شبکه‌های اجتماعی می‌باشند. ۱۰ نفر آنها دارای تحصیلات دکتری، ۲ نفر دانشجوی دکتری و ۱۳ نفر دارای تحصیلات کارشناسی ارشد هستند.

جدول۲. تحلیل مضمون مصاحبه‌های خبرگانی و فرایند استخراج مضامین فراگیر، سازمان‌یافته و پایه مرتبط با تأثیر تهدیدات سایبری (تهدیدات داخلی) در تضعیف امنیت ملی جمهوری اسلامی ایران

مضامین فراگیر	مضامین سازمان یافته	مضامین پایه	گزاره خبری
تهدیدات داخلی	تهدیدات امنیتی	تهدید گروه‌های قومی تجزیه‌طلب	تهدید گروه‌های قومی تجزیه‌طلب مانند اکراد، پان ترک‌ها، اعراب جدایی‌طلب، بلوچ‌ها و ...
		تهدیدات گروه‌های معترض و منتقد داخلی	تهدیدات گروه‌های معترض یا منتقد داخلی در زمان بروز وقایع اجتماعی اعتراضی مانند حوادث ۸۸، اعتراضات ۹۶ و ۹۸
		تضعیف هویت دینی	هویت دینی در تعامل با فضای سایبر تضعیف می‌شود و با افزایش میزان مصرف و دسترسی به اینترنت از برجستگی هویت دینی نزد جوانان کاسته می‌شود.
		ضعف و شناخت مدیران و تصمیم‌گیرندگان	ضعف شناخت مدیران و تصمیم‌گیران از فضای سایبر بسیار تهدیدزا تلقی می‌شود.
		ضعف برنامه‌ریزی صحیح و مناسب	ضعف برنامه‌ریزی صحیح و مناسب از سوی مدیران در قبال فضای سایبری بسیار تهدیدزا خواهد بود.
		ضعف پروتکل‌های حفاظتی	ضعف پروتکل‌های حفاظتی در حفاظت از زیرساخت‌ها و داده‌ها تهدیدزا خواهد بود.
	تهدیدات اجتماعی و فرهنگی	دگرگونی ساختار اجتماعی	تهدیدزا بودن انتقال ارزش‌های مشدد ضد فرهنگی در فضای سایبر با هدف دگرگونی ساختار اجتماعی
		هویت‌زدایی ملی	تهدیدزا بودن هویت‌زدایی ملی در جامعه ایران
		انتقال ارزش‌های ضد فرهنگی	انتقال ارزش‌های ضد فرهنگی در فضای سایبر: اعم از ترویج فسادهای اخلاقی، تغییر الگوی مصرف، تغییر نمادهای فرهنگی ملی
		حضور گسترده شبکه‌های اجتماعی در جامعه	حضور گسترده شبکه های اجتماعی در جامعه باعث بوجود آمدن پدیده «هویت زدایی» شده است، بدین معنا که افراد می توانند در این فضا هویت خود را تغییر دهند و با تکثیر و توزیع محتوای جریان ساز، فعالیت کنند.

مضامین فراگیر	مضامین سازمان یافته	مضامین پایه	گزاره خبری
		تغییر هویت فرهنگی جوانان بر اثر گستردگی شبکه‌های اجتماعی	هویت فرهنگی جوانان بر اثر حضور گستره شبکه‌های اجتماعی دچار تغییر شده است.
		ایجاد تشکیک در بعد اعتقادی	ایجاد تعارض و چالش در ابعاد اعتقادی در جامعه تهدیدزا تلقی می‌شود.
		تشدید شکاف هویتی	مهم‌ترین تهدید سایبری در حوزه فرهنگ و اجتماع شکاف هویتی است.
	تهدیدات سیاسی و اقتصادی	درگیر شدن ایران در جنگ فرسایشی در مرزها	رشد گروه‌های تجزیه‌طلب و درگیر شدن ایران در جنگ فرسایشی در مرزها شرقی و شمالی خود می‌شود.
		بدبینی نسبت به عملکرد حکومت به واسطه توسعه‌نیافتگی	توسعه‌نیافتگی‌ها اختلافات قومی و مذهبی را پر رنگ‌تر کرده و باعث ایجاد بدبینی نسبت به حکام شود.
		ویرانی زیرساخت‌ها و دارایی‌های کشور	حملات سایبری به زیرساخت‌ها و دارایی‌های جمهوری اسلامی ایران از طریق کشورهای متخاصم، رقیب توسط برخی ویروس‌ها و کرم‌ها یا همان بدافزارها نظیر (استاکس نت) سبب ضررهای اقتصادی می‌شود.
		تحرک گروهک نفاق و اقدام به براندازی	تحرک گروهک نفاق از طریق جمع‌آوری اطلاعات طبقه‌بندی نظام و نیروهای مسلح و ارسال آنها به سرویس‌های جاسوسی و دول متخاصم جهت براندازی نظام جمهوری اسلامی ایران
		ترویج تفکرات تفرقه افکنانه	تحرکات گروهک‌های تکفیری از طریق ایجاد انحرافات عقیدتی و ضدیت با مبانی اسلام، ضدیت با شیعه سبب ترویج تفکرات تفرقه افکنانه خواهد شد.
		محروم کردن ایران از درآمدهای ترانزیتی خود	تهدیدات ناشی از عدم عبور ترافیک بین‌الملل از خاک ج.ا.ا که از نظر مالی مشکلاتی را برای کشور به دنبال خواهد داشت.

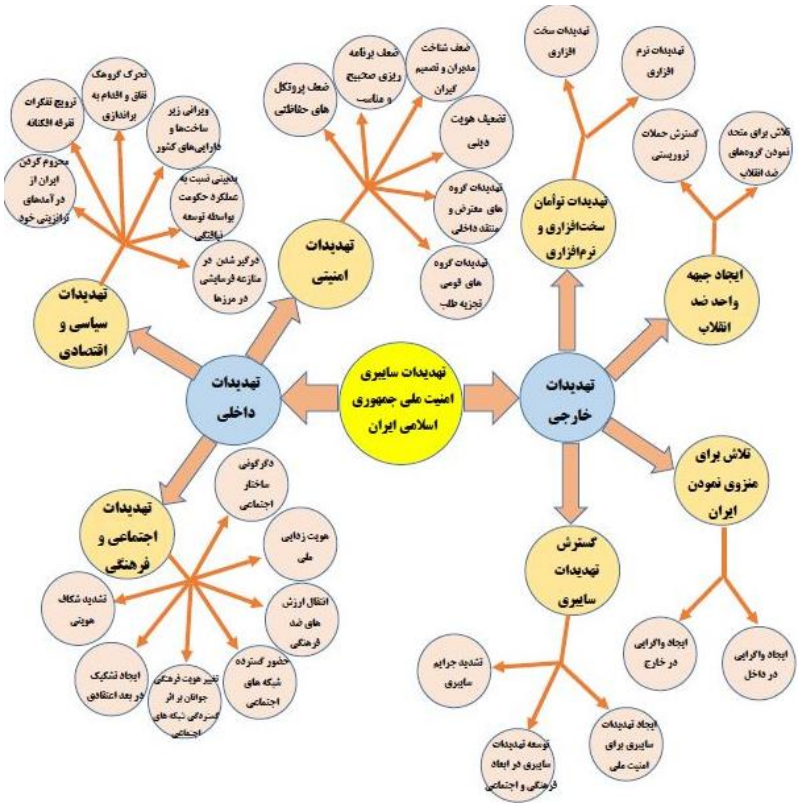
جدول ۳. تحلیل مضمون مصاحبه‌های خبرگانی و فرایند استخراج مضامین فراگیر، سازمان‌یافته و پایه مرتبط با تأثیر تهدیدات سایبری (تهدیدات خارجی) در تضعیف امنیت ملی جمهوری اسلامی ایران

مضامین فراگیر	مضامین سازمان‌یافته	مضامین پایه	گزاره خبری
تهدیدات خارجی	تهدیدات توأمان سخت‌افزاری و نرم‌افزاری	تهدیدات نرم‌افزاری	تهدیدات کشورهای معاند از طریق بدافزارها و کرم‌ها و سخت افزارها
		تهدیدات سخت‌افزاری	تهدید گروه‌های تندرو شیعی منتسب به برخی مراجع ساکن خارج و گروهک‌های معاند با هدف براندازی تهدید خارجی جدی تلقی می‌شود.
	تلاش در جهت ایجاد جبهه واحد ضد انقلاب	تلاش در جهت متحد نمودن گروهای ضدانقلاب	تهدید امینت ملی به‌وسیله اتحاد میان گروه نفاق، تکفیری و سلطنت طلبی و ضدانقلاب کردی
		گسترش حملات تروریستی	ایجاد ناامنی و تشدید بحران امنیتی در کشور از طریق حملات گروهای تروریستی
	گسترش تهدیدات سایبری	ایجاد تهدیدات سایبری برای امنیت ملی	ایجاد تعارضات ضد امنیتی از طریق جاسوسی سایبری، تروریسم سایبری، جنگ سایبری و تهاجمات سایبری
		توسعه تهدیدات سایبری در ابعاد فرهنگی و اجتماعی	انتقال ارزش‌های مشدد ضد فرهنگی در فضای سایبر با هدف دگرگونی ساختار اجتماعی
		تشدید جرایم سایبری	گسترش جرایم سایبری در کشور همچون کلاهبرداری‌های اینترنتی، مواد مخدر، قاچاق کالا
	تلاش در جهت منزوی نمودن ایران	ایجاد واگرایی در داخل	تشدید واگرایی در سه سطح اقوام، اقلیت‌های دینی و مردم با حکومت
		ایجاد واگرایی در خارج	تشدید واگرایی بین کشورهای همسایه ایران از طریق ایران هراسی و اسلام هراسی

جدول ۴. تعداد مضامین فراگیر، سازمان یافته و پایه تأثیر تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران

ردیف	مضامین فراگیر	مضامین سازمان‌یافته	مضامین پایه
۱	تهدیدات داخلی	۳	۱۹
۲	تهدیدات خارجی	۴	۹
۳	۲	۷	۲۸

همانگونه که جدول ۴ نیز نشان می‌دهد، تأثیر تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران بر اساس مصاحبه نیمه استاندارد با ۲۵ نفر از خبرگان خبرگان و صاحبنظران از ۲ مضمون فراگیر تهدیدات داخلی و تهدیدات خارجی، ۷ مضمون سازمان‌یافته و در نهایت با ۲۸ مضمون پایه‌ای به اشباع نظری رسیده است. پس از احصاء و استخراج مضامین فراگیر، مضامین سازمان‌یافته و مضامین پایه نقش تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران، در این قسمت به ترسیم مدل پژوهشی و یا همان تشکیل شبکه مضامین در ذیل نمودار ۲ مبادرت می‌شود.



نمودار ۲. مدل تأثیر تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران

(طراحی شده توسط نویسندگان)

نتیجه‌گیری

امروزه گسترش فضای سایبری باعث حذف مرزهای سیاسی و ایجاد مرزهای جدید شده و از این جهت درک واقع‌بینانه از تهدیدات امنیتی در گرو توجه به عوامل نرم‌افزاری است که در واقع، حلقه واسط بین محیط امنیتی کشورها و سخت‌افزارها قرار دارند و بر این اساس، برداشت‌ها از مفهوم امنیت ملی در این فضا به چالش کشیده شده است. یکی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی شدن برای کشورها را باید در حوزه سایبری دانست از این رو در استای مقابله به تهدیدات سایبری نخستین گام مشخص نمودن نوع تهدیدات است بر اساس بررسی این مقاله و مصاحبه با خبرگان مهم‌ترین تهدیدات فضای سایبری برای ایران در دو بُعد تهدیدات داخلی و خارجی به شرح زیر قابل ارزیابی می‌باشد.

الف- تهدیدات خارجی

مضمون فراگیر ارائه الگوی نقش تهدیدات سایبری در تضعیف امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک دارای چهار مضمون سازمان یافته:

۱- تلاش در جهت منزوی نمودن ایران (شامل دو مضمون پایه: تلاش در جهت ایجاد واگرایی در داخل و تلاش در جهت ایجاد واگرایی در خارج)،

۲- گسترش تهدیدات سایبری (شامل سه مضمون پایه: ایجاد تهدیدات سایبری برای امنیت ملی، توسعه تهدیدات سایبری در ابعاد فرهنگی و اجتماعی و تشدید جرائم سایبری)،

۳- ایجاد جبهه واحد ضد انقلاب (شامل دو مضمون پایه: تلاش در جهت متحد نمودن گروههای ضد انقلاب و گسترش حملات تروریستی) و

۴- تهدیدات توامان سخت‌افزی و نرم‌افزاری: (تهدیدات نرم‌افزاری و تهدیدات سخت‌افزاری) می‌باشد.

ب- تهدیدات داخلی

مضمون فراگیر تهدیدات داخلی گسترش اسلام گرایی افراطی در آسیای میانه برای جامعه ایران دارای سه مضمون سازمان یافته:

۱- تهدیدات امنیتی (شامل شش مضمون پایه: تهدید گروههای قومی تجزیه‌طلب، تهدیدات گروهای معترض و منتقد داخلی، تضعیف هویت دینی، ضعف و شناخت مدیران و تصمیم گیرندگان، ضعف برنامه ریزی صحیح و مناسب و ضعف پروتکلهای حفاظتی)

۲- تهدیدات اجتماعی و فرهنگی (شامل هفت مضمون پایه: دگرگونی ساختار اجتماعی، هویت‌زدایی ملی، انتقال ارزش‌های ضد فرهنگی، حضور گسترده شبکه های اجتماعی در جامعه، تغییر هویت فرهنگی جوانان بر اثر گستردگی شبکه‌های اجتماعی، ایجاد تشکیک در بعد اعتقادی و تشدید شکاف هویتی) و

۳- تهدیدات سیاسی و اقتصادی (شامل شش مضمون پایه: درگیر شدن ایران در جنگ فرسایشی در مرزها، بدبینی نسبت به عملکرد حکومت بواسطه توسعه نیافتگی، ویرانی زیرساخت‌ها و دارایی‌های کشور، تحرک گروهک نفاق و اقدام به براندازی، ترویج تفکرات تفرقه افکنانه، و محروم کردن ایران از درآمدهای ترانزیتی خود) می‌باشد.

یافته‌های پژوهش حاضر با نتایج پژوهش‌های سند ملی سایبری ایالات متحده آمریکا، (۲۰۱۸)، میک راود، (۲۰۱۸)، مزدوران سایبری: دولت، هکرها و قدرت، (۲۰۱۸) ، علی اصغر جعفری لاری، (۱۳۹۴)، غلامرضا ندری، (۱۳۹۷) شبکه‌های فدرال و سیستمهای دولتی برای مبارزه با جرائم سایبری، افزایش آمادگی چین برای پاسخ دادن به تهدیدات امنیت ملی، جرائم سایبری، تروریسم سایبری، نقش دولت‌ها در جنگ سایبری و جوانب حقوقی تعارض سایبر و شناسایی اثرات شبکه‌های اجتماعی مجازی بر امنیت اجتماعی و دگرگونی‌های بنیادین همخوانی دارند.

منابع

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

۲. احمدی‌پور، زهرا و جنیدی، رضا و خوجم‌لی، عبدالوهاب و پارسایی، اسماعیل (۱۳۹۱)، ابعاد ژئوپولیتیک فضای مجازی در عصر فناوری اطلاعات، مجله سیاست دفاعی، سال بیستم، شماره ۷۹

۳. بصیرت، وبگاه (۱۳۹۲)، «جایگاه عوامل تعیین‌کننده در امنیت ملی» بعد سیاسی، تهران: ، شناسه : ۲٦۱۹۷٤

٤. خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، تهران: فصلنامه مطالعات راهبردی، دوره ۱۵، شماره ٥٦

۵. زابلی‌زاده، اردشیر و وهاب‌پور، پیمان (۱۳۹۷)، قدرت بازدارندگی در فضای سایبر، تهران: دوفصلنامه رسانه و فرهنگ، پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال هشتم، شماره اول

٦. طیب، علیرضا (۱۳۸٤)، تروریسم در فراز و فرود تاریخ، تهران: نشر نی

۷. علی‌حسینی، علی و مهدیان، حسین و آقا حسینی، علیرضا (۱۳۹٦)، تحلیل تأثیرگذاری عوامل ژئوپولیتیکی بر سیاست امنیت ملی جمهوری اسلامی ایران در پرونده هسته ای، تهران: فصلنامه ژئوپولیتیک، سال ۱۳۹٦، شماره ۲.

۸. علیدوست، شیدا و پورقهرمانی (۱۳۹۸) نقش فضای سایبر در تامین مالی تروریسم، دومین کنفرانس ملی پدافند سایبری.

۹. فولر، گراهام (۱۳۷۷)، قبله عالم، ژئوپولیتیک ایران، ترجمه عباس مخبر، تهران: نشر مرکز، چاپ دوم

۱۰. کاستلز، امانوئل (۱۳۸۵)، عصر اطلاعات: اقتصاد، جامه و فرهنگ (ظهور جامعه شبکه ای)، ترجمه احد علیقلیان و افشین خاکباز، تهران: انتشارات طرح نو. جلد اول، چاپ پنجم.

۱۱. مجتهدزاده، پیروز (۱۳۸۱)، امنیت ملی جغرافیای سیاسی و سیاست جغرافیایی، چاپ اول، تهران: سمت

۱۲. موحدی صفت، علیرضا (۱۳۸٦)، امنیت ملی در فضای سایبر، فرصت‌ها و تأکیدها با تأکید بر استقرار دولت الکترونیکی، فصلنامه مطالعات دفاعی استراتژیک، شماره ۳۰

۱۳. نای، جوزف (۱۳۸۷)، قدرت در عصر اطلاعات (از واقع‌گرایی تا جهانی شدن)، ترجمه سعید میرترابی، تهران: پژوهشکده مطالعات راهبردی

۱٤. نورمحمدی، مرتضی (۱۳۹۰)، جنگ نرم، فضای سایبر و امنیت ملی جمهوری اسلامی ایران، راهبرد فرهنگ، شماره شانزدهم

۱۵. وظیفه‌دان، سارا (۱۳۹۵) انواع تهدیدات در فضای سایبری و راهکارهای مقابله با آن، کنفرانس ملی پدافند غیرعامل در قلمرو فضای سایبر.

۱٦. ولی‌زاده میدانی، رامین (۱۳۹۹)، درآمدی بر تروریسم سایبری و ویژگی‌های آن، تهران: مرکز ملی فضای مجازی، پژوهشگاه فضای مجازی، گروه مطالعات بنیادین

۱۷. هلیلی، خداداد و همکاران (۱۳۹۷) قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر، فصلنامه امنیت ملی، سال هشتم، شماره ۲۹

18. Astrauss, Enslam and Juliet Karbin (2018), Fundamentals of Qualitative Research (Techniques and Stages of Producing Background Theory), Translated by Ebrahim Afshar, Seventh Edition, Tehran: Ney [in Persian].
19. Cornis, Paul & Livingstone, David & Clemente، Dave & Yorke, Claire (November 2010); "On Cyber Warfare", A Chatham House Report, www.chathamhouse.org.uk "Cyber Security: accept vulnerability World Foresight Forum is an initiative of Doctrine Command", Handbook No. 1.02, www.worldforesightforum.org; (accessed by September 5, 2011).
20. Felik, Oveh (2006), An Introduction to Qualitative Research, Translated by Hadi Jalili, Second Edition, Tehran: Ney [in Persian].
21. Gibson, W. (1984) Neuromancer. New York, Ace Books.
22. Glaser BG, Strauss, Strauss AL. The Discovery of grounded theory. Strategies for qualitative research. pp. x. 271. Weidenfeld & Nicolson: London; printed in U.S.A.; 1968.
23. Khan, Navid & Brohi, Sarfraz & Zaman, Noor. (2020). Ten Deadly Cyber Security Threats AmidCOVID-19Pandemic. 10.36227/techrxiv.12278792.v1
24. Munhall PL. Nursing research: a qualitative perspective. 5th ed. Sudbury, MA: Jones & Bartlett Learning; 2012.
25. Saroukhani, Bagher (2008), Research methods in social sciences, Tehran, Institute of Humanities and Cultural Studies, volume 1, Fourteenth Edition. [in Persian].
26. 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
27. Spade, J. M. (2012). China's Cyberpower and America's national security. Carlisle Barracks, PA: US ARMY WAR COLLEGE
28. Weil, Tim & Murugesan, San. (2020). IT Risk and Resilience—Cybersecurity Response to COVID-19. IT Professional. Vol. 22. No. 3.
29. 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.

Presenting the Role Model for Cyber Threats in Weakening the National Security of the Islamic Republic of Iran

Seyyed Ali Mousazadeh [1]
Hojjat Mahkouee [2]
Reza Simbar [3]
Siamak Bagheri Choukami [4]

ABSTRACT

The present study seeks to model the role of cyber threats in undermining the national security of the Islamic Republic of Iran from a geopolitical perspective. To process the problem, a qualitative research method and content analysis have been used. Research data using semi-structured interviews of 25 experts in the field of cyber peace and security who were selected using theoretical sampling method; and using the content analysis method of the network of themes analyzed and modeled. A network measurement concept was developed. The findings of this study showed that the optimal model of security threats Cyber power role analysis includes two comprehensive themes: internal threats and external threats. In addition, in order to "validate" the themes and the model, there are two methods of evaluating the validity of the communication method and also the audit method, and in order to "validate" the reliability of the two methods,reproducibility and transferability or generalizability were also used..

Keywords: Cyber Threats, National Security, Islamic Republic of Iran , Content Analysis,.

1. PH.D Candidate in Political Geography, Department of Geography, Najafabad Branch, Islamic Azad University, Najafabad, Iran. Seyyedali3023@gmail.com
2. Assistant Professor, Department of Geography, Najafabad Branch, Islamic Azad University, Najafabad, Iran Hojat_59_m@yahoo.com
3. Full Professor, Department of Political Sciences and International Ties, Gilan University, Gilan, Iran Rezasimbar@hotmail.com
4. Associate Professor, Islamic Sciences Research Center, Tehran, Iran
Iran S.bagheri6@gmail.com