

ارائه مدل راهکارهای مقابله با تهدیدات فضای سایبری در توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک

سیدعلی موسی‌زاده^۱

حجت مهکویی^{۲*}

سیامک باقری چوکامی^۳

تاریخ دریافت: ۱۴۰۰/۹/۸

تاریخ پذیرش: ۱۴۰۰/۱۲/۲۶

۳۹

چکیده

در عصر ارتباطات، قدرت تکنولوژی و فناوری به‌عنوان یکی از منابع قدرت برای مقابله با تهدیدات فضای سایبری برای حکومت‌ها و کشورها مطرح است. با توجه به تغییر ماهیت سستی قدرت و امنیت و شکل‌گیری بعد جدیدی از تهدیدات برای کشورها، توجه به اینترنت و فضای سایبری، از ارکان اصلی سیاست‌گذاری‌ها و تصمیم‌گیری‌ها در درون دولت‌ها تبدیل شده است و یا خواهد شد. جمهوری اسلامی ایران به‌عنوان یکی از کشورهای با موقعیت ژئوپولیتیکی مناسب در منطقه غرب آسیا، از تهدیدات فضای سایبری مبرا و جدا نیست. لذا توجه به توسعه و پیشرفت در حوزه فضای مجازی و سایبری، لازمه ادامه کشورداری و حکومت‌داری برای مسئولان است. پرسش اصلی مطرح این است که راهکارهای مقابله با تهدیدات فضای سایبری در توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک کدامند؟ این تحقیق از حیث هدف کاربردی و از نظر ماهیت و روش تحقیق، توصیفی-تحلیلی و بر پایه روش کتابخانه‌ای و مصاحبه با ۲۵ نفر از نخبگان حوزه سایبری انجام پذیرفته است. به منظور تحلیل داده‌ها و ارائه مدل، با توجه به ماهیت و روش تحقیق و ضرورت تحلیل فرامتن، از روش تحلیل محتوای کیفی (تحلیل مضمون) استفاده شده است. نتایج یافته‌ها نشان می‌دهند که جمهوری اسلامی ایران از تهدیدات فضای سایبری مبرا نیست و امنیت ملی کشور از طریق فضای سایبری مورد تهاجم قرار می‌گیرد و با مخاطراتی مواجه است که راهکارهای به‌دست آمده در این پژوهش، سبب توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک خواهد شد.

واژگان کلیدی: فضای سایبری، تهدیدات فضای سایبری، توان‌افزایی، امنیت ملی، جمهوری اسلامی ایران، ژئوپولیتیک

۱. دانشجوی دکتری جغرافیای سیاسی، گروه جغرافیا، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران

۲. استادیار جغرافیای سیاسی، گروه جغرافیا، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران

* نویسنده مسئول: hojat_59_m@yahoo.com

۳. دانشیار و عضو هیئت علمی پژوهشگاه علوم اسلامی امام صادق(ع)، تهران، ایران.

امروزه گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و به این دلیل، 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 بدین دلیل، 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 که نمونه بارز آن حمله رایانه‌ای به تأسیسات هسته‌ای و الکترونیکی ایران توسط سرویس‌های جاسوسی کشورهای خارجی می‌باشد. امروزه تکنولوژی اطلاعات، صرف‌نظر از موقعیت جغرافیایی در تمام شئون زندگی وارد شده است، لیکن این رشد باوجود مزایای خود جنبه‌های منفی هم در بر داشته است. بدین مفهوم که امکان رفتارهای ضداجتماعی و مجرمانه را به‌وجود آورده که پیش از این به هیچ وجه امکان‌پذیر نبوده است و با روند رو به رشد این جرایم روبه‌رو هستیم. زیرا جرایم رایانه‌ای به دلیل ویژگی‌هایی که دارند، نسبت به سایر طرق ارتکاب جرایم مرجح می‌باشند. اول آنکه، شیوه ارتکاب آنها آسان است، با مبالغ اندک، خسارات هنگفتی می‌توانند وارد نمایند، می‌توان بدون حضور فیزیکی در یک حوزه قضایی معین در آن حوزه مرتکب این‌گونه جرایم شد، دست آخر این که در اغلب موارد غیرقانونی بودن آنها روشن نمی‌باشد.

از مهم‌ترین شاخصه‌های یک حکومت پویا و مقتدر، تضمین امنیت ملی است که رجال سیاسی، نظامی و امنیتی حاکمیت، خود را متعهد به تأمین آن می‌دانند. در گفتمان مدرن، امنیت عبارت است از نیل به سطحی از اطمینان خاطر برای تحصیل و صیانت از منافع ملی. به تعبیر «رابرت ماندل»، امنیت ملی شامل تعقیب روانی و مادی ایمنی است و اصولاً جزء مسئولیت حکومت‌های ملی است. بر همین اساس تدوین راهبرد امنیت ملی از راهبردی‌ترین اقدامات نرم‌افزاری در جهت تأمین امنیت ملی محسوب می‌شود. نگاه مدرن به امنیت، نگاهی چندسویه است و طیفی از عوامل (فرصت‌ساز و تهدیدآفرین) را شامل می‌شود که در زمینه‌های گوناگون فرصت ظهور و بروز پیدا می‌کنند. یکی از عوامل مهم در این زمینه، عامل ژئوپولیتیک و موقعیت سرزمینی است.



کشور ایران به علت قرار گرفتن در منطقه راهبردی حساس خاورمیانه از یک موقعیت ویژه‌ای برخوردار است. به طوری که نه تنها خود یک کانون ژئوپولیتیکی محسوب می‌شود، بلکه با حوزه‌های مهم ژئوپولیتیکی دیگری نیز در ارتباط می‌باشد. این حوزه‌ها با عنایت به وزن و موقعیت خود در تدوین راهبرد امنیت ملی ایران تأثیرگذار هستند. اما در میان این حوزه‌ها، حوزه ژئوپولیتیکی خاورمیانه به دلیل شأن ژئوپولیتیکی در معادلات سیاسی، اقتصادی، فرهنگی و امنیتی در منطقه و جهان، نقش بسیار فعال و تعیین‌کننده‌ای در امنیت ملی ایران دارد.

حاکمیت جمهوری اسلامی، به لحاظ ژئوپولیتیکی با فرصت‌ها و چالش‌های ویژه قرن حاضر مواجه است. عوامل ژئوپولیتیکی متعددی بر حاکمیت جمهوری اسلامی ایران تأثیر می‌گذارند. این عوامل که در برگیرنده بعد ملی حاکمیت جمهوری اسلامی ایران است، با تهدیدهای منطقه‌ای و فرامنطقه‌ای که ناشی از رقابت کشور ما برای تأمین هر چه بیشتر منافع ملی خود می‌باشند، مواجه است. لذا نقش‌آفرینی جمهوری اسلامی و اعمال حاکمیت آن علاوه بر توجه به عوامل قدرت سخت، توجه به عوامل قدرت نرم و قدرت سایبری را نیز طلب می‌کند. در واقع، با ایجاد یک راهبرد ملی در استقرار حداکثر امنیت در فضای سایبری می‌توان به کاهش آسیب‌پذیری کشور در مقابل حمله‌های سایبری، تروریسم سایبری، جاسوسی سایبری، جنگ اطلاعاتی و ... پرداخته و از بروز خسارت به زیرساخت‌های اطلاعاتی پایه و حیاتی و همچنین دارایی‌های ملی جلوگیری نمود. هدف اصلی این پژوهش، ارائه الگوی راهکارهای مقابله با تهدیدات سایبری در توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک است.

بنابراین مسأله اصلی شکل گرفته این است که راهکارهای مقابله با تهدیدات فضای سایبری در توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک کدامند؟ فضای سایبری چگونه باعث توان‌افزایی امنیت ملی جمهوری اسلامی ایران می‌شود؟

روش تحقیق

این مقاله به روش کیفی و با ماهیت روش توصیفی - تحلیلی با استفاده از منابع کتابخانه‌ای و مصاحبه، انجام گرفته است. برای انجام مصاحبه، تعداد ۶۵ نفر از



کارشناسان مرتبط با حوزه امنیت سایبری، جغرافیای سیاسی و علوم سیاسی بر اساس روش تخمینی و در دسترس و به طور هدفمند انتخاب گردیدند که با اشباع نظری (۲۵ نفر)، مصاحبه‌ها انجام شده است. پرسش‌های مصاحبه، نیمه استاندارد و محقق ساخته بوده‌اند که روایی آنها از سوی تعدادی از استادان دانشگاه به طور صوری و محتوایی مورد تأیید قرار گرفتند. برای تحلیل داده‌ها، با توجه به ماهیت و روش تحقیق و ضرورت تحلیل فرامتن، از روش تحلیل محتوای کیفی استفاده شد. این روش یکی از روش‌های کاربردی است که پژوهشگران با استفاده از آن به واریسی داده‌های خود می‌پردازند. تحلیل محتوا فرایند درک، تفسیر و مفهوم‌سازی معانی درونی داده‌ها است.

پیشینه تحقیق

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 برخی از پیشینه‌های مطالعاتی در ارتباط با موضوع مقاله اشاره می‌گردد.

موسوی و همکاران (۱۳۹۲) در مقاله «تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن» به روش اسنادی و با استفاده از منابع کتابخانه‌ای با ابزار فیش‌برداری، حوزه سایبری را به‌عنوان یکی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی‌شدن برای کشورها در حوزه سایبری می‌دانند و نمونه بارز آن را حمله رایانه‌ای آمریکا به تأسیسات هسته‌ای و الکترونیکی ایران معرفی می‌نمایند. آنها در این مقاله به بررسی تأثیر تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران پرداخته و آن را به مراتب خطرناک‌تر از تروریسم سنتی می‌دانند. در نتیجه‌گیری بحث و پیشنهادها هم تصریح می‌نمایند: باید تا حد ممکن در محور سیاست‌های پیشگیرانه از آسیب و اقدامات حقوقی از طریق مراجع و سازمان‌های بین‌المللی و تدابیر نظارتی در این خصوص، برنامه‌ریزی شود. نه می‌توان فناوری اطلاعات و ارتباطات الکترونیکی را کنار گذاشت و به یک جامعه عاری از آن تبدیل شد و نه امکان ریشه‌کنی هرگونه اقدام تروریستی علیه کشور وجود دارد. لذا تنها راه،

چاره‌جویی در جهت کاستن از تهدیدات یا عواقب اقدامات تروریستی سایبری در مفهوم موسع آن است.

کربلایی‌تاج‌الدین، و همکاران (۱۳۹۵) در کتاب «فضای مجازی و شبکه‌های اجتماعی» به بررسی و تشریح ابعاد جنگ نرم در فضای مجازی پرداخته‌اند. در این کتاب به اهمیت فوق‌العاده عملیات روانی در پیشبرد اهداف مورد نظر کشورها اشاره شده و عملیات روانی در فضای مجازی را به‌عنوان یکی از شیوه‌های شکست دادن حریف و کاهش توان رزمی حریف معرفی نموده است. نویسندگان کتاب عنوان می‌نمایند: عملیات روانی می‌تواند به‌عنوان پشتوانه عملیات نظامی در راستای ارتقاء روحیه و آمادگی نیروهای مسلح و مردم یک کشور مؤثر باشد.

صیاد و همکاران (۱۳۹۹) در مقاله تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات متحده 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 به‌وجود 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 از جمله خرابکاری، اختلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته است. هدف در این پژوهش، بررسی راهبردها و رویکردهای دو کشور ایران و آمریکا و همچنین کشف نقاط ضعف و یا کاستی‌های 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 در نتیجه در حوزه امنیت ملی، به‌رغم فعالیت‌ها و تدابیر خوب اندیشیده شده پیشین، راهکارهای مقابله با تهدیدهای سایبری با توجه به روند تهدیدات باید به‌روزرسانی شده 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.

دوئی.ای. دنینگ (۲۰۱۴) در مقاله‌ای با عنوان «چارچوب و اصول دفاع سایبری فعال» تلاش می‌نماید ضمن مرور مفاهیم حوزه دفاع هوایی و موشکی، همچنین دفاع سایبری فعال و غیرفعال و تسری این مفاهیم به فضای سایبری، اصول اخلاقی و قانونی برای راهبری دفاع سایبری فعال ارائه نماید. وی دفاع سایبری فعال را با چهار ویژگی تأثیرات (داخلی و خارجی)، درجه همکاری، نوع تأثیرات (انتشار اطلاعات، جمع‌آوری، مسدودسازی فعالیت‌های خصمانه (و درجه مکانیزه بودن) در ارتباط با میزان اثرگذاری عامل انسانی) مورد ارزیابی قرار دهد.

آنا ماریا اسولا (۲۰۱۸) در کتاب «امنیت سایبری در انگلیس» عنوان می‌نماید: خدمات الکترونیک باید بسیار ساده و آسان باشد تا همه شهروندان از آنها استفاده کنند و نمی‌توان هیچ شهروندی را نادیده گرفت. به این ترتیب، می‌توان گفت که انگلستان در حال ارتقای میزان دسترسی به ارتباطات الکترونیکی و گسترش پهنای باند ثابت در سراسر کشور است. شورای امنیت ملی انگلیس با توجه به پیامدهای حملات احتمالی سایبری، حملات خصمانه به فضای سایبری انگلیس از سوی کشورهای دیگر و جرائم سایبری گسترده را از مهمترین تهدیدات امنیت ملی در نظر گرفته است. وی با این کتاب به متحدان ناتو در مورد مدیریت امنیت سایبری ملی انگلیس کمک می‌کند. این پروژه با هدف حمایت از کشورها در ارتقای ساختار سازمانی خود، تشویق به نوآوری در شیوه‌ها و کمک به توسعه همکاری میان مؤسسات ملی مختلف انجام شده است. در بخشی از این کتاب آمده است: دولت مجموعه مشخص از الگوهای مدیریت حوادث ملی را که به‌طور منظم، از جمله از سوی وزیران اجرا می‌شوند، تأیید کرده است. با توجه به خطر حمله احتمالی علیه شبکه‌های خبری و نیروهای مسلح و دارایی‌ها و توانایی‌ها، دولت اظهار داشت که تعدادی از برنامه‌های کسب‌وکار و برنامه‌های احتمالی برای اطمینان از اینکه بتوانیم نقش خود را ایفا کنیم، برنامه‌ریزی و اجرا می‌شود و امنیت سایبری به طور کامل در مسیر فرایند برنامه‌ریزی عملیات احتمالی است.

راندل^۱ (۲۰۲۱) در مقاله گزارش هشدارها و باج‌افزار^۲، 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.

جنبه جدید بودن این مقاله پژوهشی در این است که نخست، به صورت جامع و کلی به احصاء تهدیدات و فرصت‌های گوناگون فرهنگی، اجتماعی، سیاسی، امنیتی، اقتصادی و آموزشی از منظر صاحب‌نظران حوزه امنیت ملی و فضای سایبری با روش کیفی و به صورت تحلیل محتوا پرداخته شده است در صورتی که اغلب تحقیقات انجام گرفته قبلی با روش کمی و یا از پرسشنامه استفاده کرده‌اند. دوم: در این پژوهش به‌طور ویژه به تأثیر قدرت سایبری بر امنیت ملی جمهوری اسلامی ایران پرداخته شده است که مورد مشابه یا پژوهش‌های مبسوطی در این خصوص انجام نگرفته و در معدود تحقیقات انجام گرفته درباره قدرت سایبری، توجه چندانی به امنیت ملی جمهوری اسلامی ایران نگردیده است. سوم: در اکثر پژوهش‌های مشابه، فضای سایبری به‌عنوان یکی از عوامل تهدید کننده امنیت ملی معرفی شده و دولت‌ها از آن به‌عنوان یک حوزه تهدید یاد می‌نمایند. ولی در این رساله، علاوه بر ذکر مؤلفه‌های تهدید سایبری، از قدرت سایبری به‌عنوان یکی از مهمترین فضاها با افزایش دهنده سطح امنیت ملی در جمهوری اسلامی ایران پرداخته شده که تاکنون از این منظر، مقاله‌ای نگارش نشده است. چهارم: در این تحقیق به صورتی جامع، موانع موجود در مسیر حکمرانی و سیاست‌گذاری فضای سایبری احصاء شده که از جمله این موانع می‌توان به موانع شناختی، فنی - زیرساختی، نهادی قانونی، سیاستی و سیاسی - اجتماعی اشاره کرد که از این حیث هم این پژوهش، جدید و یک نوآوری محسوب می‌شود.

1. James Rundle
2. Ransomware

مبانی نظری

مفهوم فضای سایبری

واژه سایبر از ریشه یونانی سایبرنتیک^۱ به معنای سکاندار یا راهنماست و اصل ریشه‌ای واژه اشاره به یک سلسله از ارتباطات درونی انسانها دارد بدون در نظر گرفتن فضای حقیقی که می‌تواند با اصطلاح فارسی-عربی فضای مجازی برابری یابد. از دهه ۱۹۹۰ و همزمان با فروپاشی نظام ژئوپولیتیک دوقطبی، دو روند توأمان در عالم اندیشه و عمل، دگرگون کردن فضای مدیریت اقتصادی و سیاسی جهان را آغاز کردند. این دو روند به هم پیوسته عبارتند از: اشاعه اندیشه جهانی شدن اقتصاد بازار آزاد و بروز انقلاب در تکنولوژی اطلاع‌رسانی. رشد فناوری شبکه‌های ارتباطی اینترنتی در رابطه با پیشرفت فناوری کامپیوتری مبادله آزاد اطلاعات، خدمات و کالا از راه‌های جدید فرامرزی و فراسرزمینی را میسر ساخت و این گونه بود که جهان ژئوپولیتیک پا به دورانی گذاشت که ویژگی‌اش مجازی شدن فضای انسانی در ارتباط با ادوات مربوط به ارتباطات است (مجتهدزاده، ۱۳۹۱: ۷۹-۷۸). گفته می‌شود از خصوصیات بارز این فضا، بی‌مکانی و بی‌زمانی است. در این فضا، از بین رفتن فاصله مکانی، افزایش بی‌سابقه توان انسان‌ها برای مبادله و مراوده با یکدیگر، فرایند هویت‌یابی جمعی افراد را دگرگون کرده است (منتظر قائم، ۱۳۸۱: ۲۳۱). در واقع، فضای سایبری محیطی است مجازی و غیر ملموس در فضای شبکه‌های بین‌المللی. این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند که در این محیط، تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طو کلی هر آنچه در کره خاکی به صورت فیزیکی ملموس وجود دارد، به صورت نوشته، تصویر، صوت و اسناد در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران می‌باشند و به طریق کامپیوتر، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط می‌باشند. در این فضا، کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون در نظر گرفتن اینکه این اطلاعات و خدمات در کدام نقطه دنیا واقع شده است. محدوده فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار و حتی مرزهای یک کشور محدود نبوده و

1. Cybernetic

در یک سطح کم هزینه هر کاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد (کریم‌آبادی، ۱۳۹۲: ۷).

امنیت ملی و تهدیدات فضای سایبری

چند بعدی بودن مفهوم امنیت ملی سبب شده است دیدگاه‌های بسیار متنوعی راجع به آن وجود داشته باشد و هر کسی از زاویه دید خود به تعریف آن پردازد. در همین راستا، برخی از نظریه‌پردازان، امنیت ملی را معادل با ارزش‌های حیاتی کشور می‌دانند. بدان‌گونه که آرنولد و لفرز^۱ آن را برابر با «نبود تهدید برای ارزش‌های اکتسابی» می‌دانند. بری بوزان نیز امنیت را «رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل و یکپارچگی کارکردی در مقابل نیروی تغییردهنده» تعریف می‌کند.

در عین حال، یکی از کامل‌ترین تعاریف را ریچارد اولمن ارائه کرده است: تهدید امنیت ملی اقدام یا سلسله رویدادهایی است که نخست، به شکلی مؤثر و در دوره زمانی کوتاه خطر افت کیفیت زندگی را برای ساکنان کشور پیش آورد و دوم، با خطر جدی کاهش طیف خط‌مشی‌هایی که حکومت یا واحدهای غیرحکومتی خصوصی موجود در داخل کشور (اشخاص، گروه‌ها، شرکت‌ها) می‌توانند از میان آنها دست به انتخاب زنند، همراه باشد. مسلماً با این تعریف، تصور ما از عوامل تهدیدزا دامنه بیشتری می‌یابد (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۵۶-۵۵). امروزه عوامل تهدیدزا بر امنیت ملی متنوع شده است؛ تا یک قرن پیش، کمتر کسی به این فکر می‌کرد که اینترنت و فضای سایبری حاصل از آن به عنوان یک عامل تهدید نمایان شود. در حال حاضر، تهدیدات سایبری به قدری خطرناک و پیچیده هستند که اداره اطلاعات ملی آمریکا که وظیفه هماهنگی ۱۶ سازمان اطلاعاتی آمریکا را بر عهده دارد، در گزارش فوریه ۲۰۱۰ که به بررسی تهدیدهای امنیت ملی آمریکا می‌پردازد، تهدیدهای سایبری را از مهمترین تهدیدهای فراروی امنیت ملی آمریکا ذکر کرده است (Director of National

(Intelligence:2010). در همین راستا، ریچارد کلارک^۱ مشاور عالی ضد تروریسم آمریکا در دوره جرج بوش و بیل کلینتون طی اظهاراتی در می ۲۰۱۰ اظهار داشت: آمریکا توانایی لازم برای مقابله با تلاش تروریستها برای دستیابی به سیستم رایانه‌ای ایالات متحده را پرل هاربر الکترونیکی ندارد و این موضوع ممکن است به فاجعه در ایالات متحده منجر شود (نور محمدی، ۱۳۹۲: ۱۱). فضای سایبری، فراهم کننده رابطه‌ای است که در آن مردم بی‌نیاز از اتکا بر روابط چهره‌به‌چهره، می‌توانند دست به تعامل و هماهنگی اقداماتشان بزنند (جالینوسی و همکاران، ۱۳۹۱: ۴). این فضا، 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 مشخصات خاصی دارند. از یک‌سو، 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. مهم‌ترین مشخصات تهدیدهای سایبری را می‌توان به‌طور خلاصه این‌گونه عنوان نمود: (۱) گستردگی عاملان و تعدد بازیگران در فضای سایبری؛ (۲) هزینه پایین ورود، صرف زمان اندک و سرعت بالای اقدام؛ (۳) پنهان ماندن بازیگران و عدم قطعیت در شناسایی و ردیابی آنها؛ (۴) تأثیرگذاری شگرف و آسیب‌زایی گسترده؛ (۵) کم‌رنگ شدن نقش و اهمیت جغرافیا؛ (۶) ساختار فضای اینترنت؛ (۷) ضعف قوانین موجود در برخورد با اقدامهای مجرمانه در فضای سایبری (خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۷۱-۱۶۹).

1. Richard Clarke

انواع تهدیدهای سایبری

نشت اطلاعات، سرقت داده‌های حیاتی کشور و آسیب پذیری شبکه‌های جامع اطلاع‌رسان به‌عنوان مهم‌ترین اشکالات امنیتی در این فضا می‌باشند که اگر از طرف حکومت‌ها توجه ویژه‌ای به آنها نشود به‌عنوان تهدیدات جدی برای منافع پایه‌ای کشورها تلقی می‌شود. وجود شبکه جهانی اینترنت که امکان دسترسی‌های مختلف را برای همه افراد در سراسر جهان امکان‌پذیر ساخته است، واقعیتی انکارناپذیر است که به‌عنوان مهمترین بستر فضای سایبر و مهمترین عامل در امنیت ملی و زیرساخت‌های کشورهای توسعه یافته است که تهدیدهای سایبری درون آن شکل گرفته و فعال می‌شوند (موحدی‌صفت، ۱۳۸۶: ۲۵۲-۲۵۱). مهمترین این تهدیدها در جدول شماره ۱ آورده شده‌اند.

جدول ۱. انواع تهدیدهای فضای سایبری و مشخصات آنها

تهدید	مشخصات
جنگ سایبری	جنگ سایبری ^۱ در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی دشمن (اطلاعات، پروسه‌های مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای) در یک فضای سایبری است (غروی و محمدی، ۱۳۹۰: ۷۷). عرصه سایبر نیز همانند عرصه‌های هوایی، زمینی، دریایی و حتی فضایی، دارای ابزارهای جنگی است. حملات سایبر امروزه امری واقعی و تعیین یافته است که در حیات بشری دیده می‌شود. حملات سایبری قدرت نسبی دولت‌ها را و به تبع آن، بقاء آنان را در نظام بین‌الملل متأثر می‌سازد. جنگ سایبری محدوده‌های جدید از نزاع، قدرت و امنیت است که پیش از این برخلاف نظرات واقع‌گرایان به هیچ وجه در دایره عناصر قدرت تعریف نمی‌شد. اما شاید بتوان تعریف مورگنتا از قدرت را در این خصوص مستثنی کرد: برای مورگنتا قدرت «... ممکن است شامل هر چیزی که کنترل بر انسان را ایجاد و حفظ کند» معنی می‌شود. «قدرت همه روابط اجتماعی را که در اختیار این هدف باشد، از خشونت فیزیکی گرفته تا پیوندهای لطیف روانشناختی که ذهن فرد را کنترل می‌کند، شامل می‌شود» (زابلی‌زاده و وهاب‌پور، ۱۳۹۷: ۶۰-۵۹). در فضای سایبری تکنیک‌های جنگ به محدودسازی، خودمختاری و کنترل دولت‌ها تمایل دارد (Lin, 2011: 63).
	در واقع، حمله سایبری رفتاری متفاوت از جنگ سایبری را به نمایش می‌گذارد.

1. Cyber Warfare

<p>حمله سایبری اختلال در صحت یا درستی داده‌هاست که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که منجر به خروجی‌های اشتباه می‌شود، انجام می‌گیرد (Rodriguez, 2006:9-10). حملات سایبری به عنوان جدیدترین و پیچیده‌ترین نبردها ذیل عملیات‌های نظامی به شمار می‌آیند. حملات سایبری به دلیل جدید بودن، درصد هزینه پایین و فایده بالا، عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید و عدم توانایی در تعیین میزان و دامنه خسارات وارد شده در مراحل اولیه شروع حمله، مورد توجه کشورهای متخاصم به ویژه در جنگ‌های ترکیبی قرار گرفته است (تقی‌پور و اسماعیلی، ۱۳۹۰: ۱۸۱)</p>	<p>حمله‌های سایبری</p>
<p>اصطلاح تروریسم سایبری نخستین بار توسط کالین باری مورد استفاده قرار گرفته است برای تبیین این اقدام یا نوع از تروریسم، تعاریف متعددی ذکر شده است. برخی از افراد معتقدند؛ تروریسم سایبری به پدیده‌های گفته می‌شود که از بستر اینترنت برای اهداف تروریستی استفاده می‌کند. در تعریفی دیگر آمده است؛ تروریسم سایبری را می‌توان هرگونه اقدام خشونت‌آمیز در فضای سایبری تعریف کرد که به منظور ایجاد هراس و با اغراض سیاسی، شبکه‌های زیربنایی بازیگران هدف از جمله انرژی، راه‌های ارتباطی و تأسیسات دولتی، در دایره اهداف تروریسم سایبری قرار می‌گیرند. بسیاری از حملاتی که در قالب تروریسم سایبری انجام می‌گیرد، آن دسته از اقداماتی هستند که هکرها به آن دست می‌زنند. این رفتارها با تبعات زیان بار همراه است (Oliverio and Lauderdale, 2016: 75-76).</p>	<p>تروریسم سایبری</p>
<p>افزایش روبه‌روز نفوذگرها (هکرها) و سرقت‌های اطلاعاتی و مالی، نشانگر آسیب‌پذیری بالای جامعه در قبال این پدیده مخرب است (قدسی، ۱۳۹۲). جرایم اینترنتی می‌تواند نقض حق مالکیت معنوی، نقض حق اختراع، ربودن اسرار خصوصی اشخاص و واگذاری آنها به دولتها و شرکتهای تجاری و غیره باشد. این جرایم، همچنین شامل حمله عمدی به رایانه‌ها به منظور مختل کردن آنها و یا کپی از اطلاعات طبقه‌بندی شده می‌شود (Nagre and Warade, 2008:5). تحلیل - گران هزینه جرایم اینترنتی را برای صنعت جهانی بیش از هزار میلیارد دلار در موارد نقض مالکیت فکری و از دست دادن اطلاعات تخمین زده‌اند. برای مثال، شخصی در سال ۲۰۰۹، چندین ترابایت از داده‌های مربوط به سیستم الکترونیکی و طراحی اطلاعات از برنامه جنگنده‌های مشترک ۳۰۰ میلیارد دلاری پنتاگون را به سرقت برد. علاوه بر این، بیشتر مجرمان اینترنتی از مجازات فرار کرده‌اند. بدیهی است این فعالیت پرسود و اغلب بدون مجازات، در واقع تهدیدی برای امنیت ملی است (Peritz and Sechrist, 2010:5-7).</p>	<p>جرایم سایبری</p>
<p>جاسوسی سایبری، رصد و جمع‌آوری اطلاعات محرمانه از رایانه‌ها و سیستم‌های مربوطه، بدون اطلاع و اجازه صاحبان آنهاست. برخلاف جرایم سایبری که مسائل</p>	

<p>مالی و اقتصادی عامل اصلی تحریک مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرکهای اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقابتی سیاسی، (Lord and Sharp, 2011: 17) ربایش اطلاعات با هدف ضربه زدن به اقتدار سیاسی و زیر سؤال بردن حاکمیت ملی کشورها جهت نیل به براندازی نظام سیاسی حاکم در کشورهای هدف، از دیگر مقاصد است که سرویسهای جاسوسی در نبرد سایبری با یکدیگر از آن بهره می‌برند.</p>	<p>جاسوسی سایبری</p>
<p>آشفته‌گی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرار داده و یا آن را آزار دهد. اهداف سیاسی و ایدئولوژیکی در پشت این اقدامات وجود دارد و افراد از ابزاری استفاده می‌کنند که غیرقانونی هستند. گروه‌های هکری آنارشیستی و نیهیلیست‌ها از آشفته‌گی سایبری استفاده می‌کنند. به عنوان مثال، گروهی با عنوان «ناشناخته‌ها» در واکنش به دستگیری جولیان آسانژ، مدیر سایت جنجالی ویکی لیکس، حمله‌های سایبری گسترده‌ای انجام دادند. برخلاف جرایم سایبری و جاسوسی سایبری که هدفشان دزدی یا تغییر اطلاعات است، آشفته‌گی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدفهای خود دارد. ممکن است طی این مرحله، اطلاعات زیادی دزدیده شده و یا تغییر یابد و یا هزینه‌های مادی فراوانی به شبکه‌های هدف وارد شود، اما قصد و نیت اصلی آشفته‌گی سایبری، آسیب رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند، ولی تا کنون آشفته‌گی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده‌اند (Lord and Sharp, 2011: 18).</p>	<p>آشفته‌گی سایبری</p>

ژئوپولیتیک و فضای سایبری

ژئوپولیتیک فضای سایبری بدون آنکه از اهمیت رقابت‌های کلاسیک قدرتی بکاهد یا آن را انکار کند، بُعد تازه‌ای به رقابت قدرت‌ها بخشیده که با امکانات و شرایط پدید آمده در جهان پست مدرن سازگار است. البته باید متذکر شد که چگونه می‌توان ژئوپولیتیک را که از رقابت‌های قدرتی در فضاهای جغرافیایی ناهموار و غیر یکدست سخن می‌گوید و فضای سایبری که بدون بدنه است و همانند توپ صاف و صیقلی، در یک اصطلاح ترکیبی (ژئوپولیتیک فضای سایبری) کنار هم قرار داد (مجتهدزاده، ۱۳۹۱: ۸۰). با بررسی مشخصات و ویژگی‌های فراوان در فضای سایبری و شبکه اینترنت، آن را از نظر

ژئوپولیتیک نیز معنی دار می‌کند که کالبد شکافی و تبیین آنها به گسترش دانش ژئوپولیتیک در فضای سایبری می‌انجامد. ابعاد مختلف ژئوپولیتیک در فضای سایبری عبارتند از: ۱. بعد مدیریتی و کنترل؛ ۲. بعد هویتی؛ ۳. بعد همگرایی و همکاری؛ ۴. بعد رقابتی و ستیز؛ ۵. بعد شکاف و توسعه؛ ۶. بعد تولید قدرت؛ ۷. بعد حاکمیتی و کنترل ملی (حافظ‌نیا، ۱۳۹۰: ۳۲۹-۳۲۳).

حکومت‌ها و کشورها به عنوان بازیگران اصلی عرصه بین‌المللی و نیز شرکت‌ها و بنگاه‌های اقتصادی به عنوان بازیگران عرصه جهانی به شبکه اینترنت و فضای سایبری، نگرشی ایزاری دارند که به تولید قدرت برای آنها منجر می‌شود. لاجرم دولت‌ها تلاش می‌کنند هم از حیث توسعه فناوری اطلاعات و ارتباطات و هم از حیث توسعه ضریب نفوذ اینترنت و افزایش تعداد کاربران و هم از حیث دیجیتالی کردن امور زندگی شهروندان و نیز امور عمومی و اداری کشور اقدام کنند و شرکت‌ها نیز می‌کوشند برای افزایش سرعت انجام امور و نیز نوآوری فناورانه در خدمات خود به مشتریان و نیز صرفه و صلاح شرکت در انجام خدمات به قابلیت‌های شبکه اینترنت و فضای مجازی پناه ببرند (حافظ‌نیا، ۱۳۹۰: ۳۲۹). البته قابل ذکر است که برخلاف تأثیرات عمیقی که اندیشه مجازی شدن فضای سیاسی بر جهانی‌اندیشی ژئوپولیتیک داشته است، ماهیت فضایی ژئوپولیتیک یعنی رقابت قدرت‌ها برای تسلط بر جهان یا منطقه با استفاده از امکاناتی که زمین در اختیار می‌گذارد از میان نرفته است و دچار دگرگونی ماهوی نشده است. در واقع، ژئوپولیتیک با پذیرفتن فلسفی موجودیت فضای مجازی در کنار فضای حقیقی تلاش دارد بحث فضای سایبری را در چارچوب ایده‌آل‌های واقع‌گرایانه سروسامان دهد. قابل دقت است که در مبحث فضای سایبری، مطالعه کننده در حقیقت با دو مفهوم جداگانه ولی مکمل هم سروکار دارد: ۱. اسباب و وسایل رسیدن به فضای سایبری که در اصطلاح انگلیسی Cyber Space خوانده می‌شود؛ ۲. خود فضای مجازی که آن را در اصطلاح انگلیسی Virtual Space گویند (مجتهدزاده، ۱۳۹۱: ۸۴-۷۸).

امروزه توانایی استفاده از فضای سایبری، یکی از مهمترین منابع قدرت در قرن ۲۱ به حساب می‌آید. بازیگران دولتی و غیردولتی از این قدرت استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و

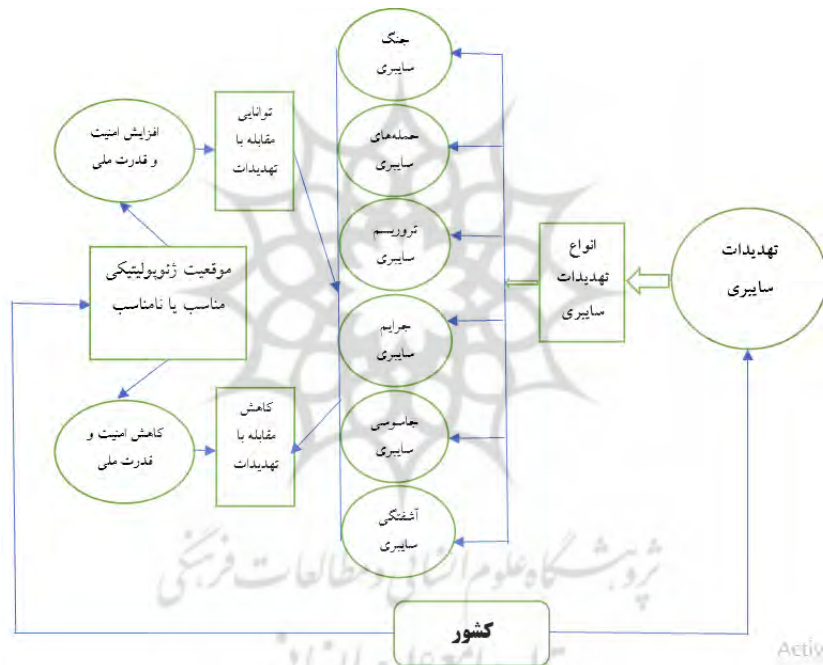
دنیای واقعی دست یابند (Lord and Sharp, 2011:22). این نکته نباید نادیده گرفته شود که امروزه انگیزه‌های زیادی از قبیل ژئوپولیتیک، جغرافیایی، اقتصادی، مذهبی، سیاسی و... برای مبارزه با نظام جمهوری اسلامی ایران از سوی کشورهای منطقه‌ای و فرا منطقه‌ای، و گروه‌های مخالف نظام جمهوری اسلامی ایران وجود دارد که دشمنان را ترغیب به جاسوسی سایبری، خرابکاری سایبری، 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 توسعه‌یافتگی و اختلال در زیرساخت‌های حیاتی آن است که اجباراً باید در فضای سایبری قرار گیرند (موحدی صفت، ۱۳۸۶: ۲۴۷).

امروزه اکثر نظریه‌پردازان ژئوپولیتیک جهان اعتقاد دارند که مرزهای سیاسی دچار تغییر کاربرد شده و نمی‌توانند جلوی بسیاری از تهدیدات بگیرند. تروریسم نیز از دیگر سو به جنگی هم‌تراز علیه جامعه جهانی بدل شده و امنیت دولت‌ها را با چالش‌های بسیاری مواجه می‌کنند (کریمی و همکاران، ۱۳۹۴: ۱۹۳). تأثیر فضای سایبری بر موضوعات سیاسی و دیپلماتیک به ندرت محدود به نظر می‌رسد. مؤثرترین و نفوذی‌ترین ابزار جهانی امروز که در همه جا حضور دارد، تلویزیون ماهواره‌ای است که توسط سیستم‌ها و شبکه‌هایی اداره می‌شود که خود از طریق فضای سایبری به هم مرتبط شده‌اند. کمپین‌های نفوذی که از سوی دولت آمریکا تأمین می‌شوند یا شبکه‌های تروریستی مخفی القاعده، هر دو از قدرت سایبری به‌عنوان توانمندی مهم در چالش و مبارزه با افکار و ایده‌ها استفاده می‌کنند. قدرت سایبری به لحاظ نظامی پر نفوذترین ابزار طی دو دهه اخیر بوده است. از «انقلاب فنی نظامی» در دهه ۱۹۸۰ که ریشه در روسیه دارد تا توسعه موضوعات شبکه محور و تغییرات دفاعی در نیروی نظامی آمریکا، قدرت سایبری و فضای سایبری در قلب موضوعات و دکترین‌های جدید حضور دارد. در سراسر سطوح منازعه از جاسوسی گرفته تا نبردهای معمولی مبتنی بر ارتش، قدرت سایبری جزء لاینفک توانمندی نظامی مدرن مبتنی بر فناوری شده است. قدرت سایبری خود به‌عنوان یک اهرم کلیدی در توسعه و اجرای سیاست ملی عمل می‌کند. خواه در مبارزه با تروریسم، رشته اقتصادی و موضوعات دیپلماتیک باشد و خواه یکی از عملیات

دولتی بیشمار دیگر (کرامر و همکاران، ۲۰۱۰: ۸۴). پیام‌آوران انفجار تکنولوژی اطلاع‌رسانی و جهانی شدن ارتباطات اینترنتی در فضای مجازی بر این واقعیت نیز چشم بسته‌اند که ۸۵٪ از کاربران اینترنتی در کشورهای پسا صنعتی زندگی می‌کنند. نه تنها توزیع نابرابر امکانات در فضای مجازی سراسر گیتی را به معنای واقعی از دسترسی برابر به اینترنت محروم کرده است بلکه اعمال محدودیت‌های دولتی نیز استفاده آزادانه و مطلق از آن را در بسیاری از کشورها دشوار می‌کند. همچنین نه تنها اینترنت و فرایند سریع ارتباطات از راه دور همسویی فکری و هویتی گروه‌ها و ملت‌ها را بیشتر نکرده، بلکه در مواردی به تقویت هویت‌گرایی‌های محلی و ملی و یا حتی به واکنش‌های هویتی خشونت‌آمیز نیز انجامید (مجتهدزاده، ۱۳۹۱: ۸۳).

آنچه که در پیوند میان ژئوپولیتیک و فضای سایبری، نقش‌آفرینی مهمی دارد، قدرت است. قدرت دارای مفاهیم لغوی و اصطلاحی، همچنین دیدگاه‌های مختلفی در علوم گوناگون از جمله علوم انسانی، اجتماعی و سیاسی است. فرهنگ‌های زبان فارسی، واژه قدرت را در مفاهیم «توانستن»، «توانایی داشتن» و «توانایی» بکار برده‌اند (دهخدا، ۱۳۳۹: ۳۶). همچنین به صفتی که تأثیر آن بر وفق اراده باشد، معنا کرده‌اند (معین، ۱۳۷۱: ۲). در فرهنگ سیاسی غرب، واژه‌هایی مثل Power و Authority به عنوان معادل کلمه قدرت به کار رفته است که به معنی استعداد و توانایی انجام کار می‌باشد (Oxford, 2000: 970). در علوم سیاسی، قدرت مجموعه‌ای از عوامل مادی و معنوی است که موجب به اطاعت در آوردن فرد یا گروه، توسط فرد یا گروه دیگر می‌گردد (آشوری، ۱۳۷۰: ۲۴۷). قدرت در ژئوپولیتیک به نیروی به ثمر رساندن اراده یا سیاست‌های ملی یک موجودیت در ورای مرزهای کشوری‌اش گفته می‌شود. قدرت از منظر ژئوپولیتیک، هم در وجود یک کشور با حکومت مقتدر برای نقش‌آفرینی‌های جهانی و منطقه‌ای و هم در وجود جمعی از کشورها، و باز هم در وجود شرکت‌های چندملیتی بزرگ و سازمان‌های موضوعی و منطقه‌ای واقعیت می‌یابد (مجتهدزاده، ۱۳۹۱: ۱۰۵). می‌توان گفت که قدرت در جهان امروزی معنای جدیدتری نیز پیدا کرده است و این تغییر مفهوم از قدرت به دلیل رشد سریع فضای سایبر و ایجاد زمینه‌های جدید و مهم در سیاست است. امروزه توانایی نفوذ در فضای سایبر به عنوان یکی از مهمترین منابع قدرت در قرن ۲۱ محسوب می‌شود. لذا

بازیگران دولتی و غیردولتی برای دست یافتن به اهداف نظامی، ایدئولوژی و اجتماعی فضای سایبر یا فضای فیزیکی، از این فضا استفاده می کنند (Lord and Sharp, 2011:20). قدرت سایبری امروزه بُعد مهمی از زیست‌واره جهانی را شکل می دهد. اطلاعات و فناوری های اطلاعاتی در سپهر سیاسی، اقتصادی و نظامی نقش حیاتی ایفا کرده و مقدمات فعالیت های عملیاتی را فراهم می آورند (منوچهری، ۱۳۷۶:۳۳). مفهوم قدرت سایبر را می توان در برابر مفاهیمی چون قدرت دریایی، قدرت هوایی، قدرت زمینی و حتی قدرت فضایی بررسی کرد (کرامر و همکاران، ۲۰۰۹: ۴-۵).



شکل ۱. مدل مفهومی پژوهش

یافته های کیفی تحقیق

برای تحلیل داده های کیفی مرتبط با راهکارهای مقابله با تهدیدات سایبری بر توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک از تحلیل مضمون^۱ و از میان

1. Thematic Analysis

روشهای مختلف تحلیل مضمون از روش شبکه مضامین^۱ استفاده می‌شود. یکی از روشهای ساده و کارآمد تحلیل کیفی، تحلیل مضمون است. در واقع، تحلیل مضمون، اولین روش تحلیل کیفی است که پژوهش‌گران باید یاد بگیرند. این روش، مهارت‌های اساسی مورد نیاز برای بسیاری از تحلیل‌های کیفی را فراهم می‌کند. تحلیل مضمون، یکی از مهارت‌های عام و مشترک در تحلیل‌های کیفی است؛ به همین دلیل، بویاتزیس^۲ (۱۹۹۸، ص ۴) آن را نه روشی خاص بلکه ابزاری مناسب برای روش‌های مختلف، معرفی می‌کند. ریان و برنارد^۳ (۲۰۰۰) نیز کدگذاری مضامین را فرایند پیش‌نیاز تحلیل‌های اصلی و رایج کیفی، معرفی می‌کنند تا روشی منحصر بفرد و خاص. اما به عقیده براون و کلارک^۴ (۲۰۰۶) تحلیل مضمون را باید روش ویژه‌ای در نظر گرفت که یکی از مزایای آن، انعطاف‌پذیری است. تحلیل مضمون، روشی برای شناخت، تحلیل و گزارش الگوهای موجود در داده‌های کیفی است. این روش، فرایندی برای تحلیل داده‌های متنی است و داده‌های پراکنده و متنوع را به داده‌هایی غنی و تفصیلی تبدیل می‌کند. در تعریف مضمون می‌توان چنین گفت: مضمون الگویی است که در داده‌ها یافت می‌شود که به توصیف، سازماندهی مشاهدات و تفسیر جنبه‌هایی از پدیده می‌پردازد. به طور کلی، مضمون، ویژگی تکراری و متمایزی در متن است که به نظر پژوهشگر، نشان دهنده درک و تجربه خاصی در رابطه با پرسش‌های تحقیق است. تحلیل مضمون به روش‌های مختلف انجام می‌گیرد که از جمله می‌توان به قالب مضامین (برای نشان دادن سطوح سلسله‌مرتب‌های مضامین مستخرج)، ماتریس مضامین (برای مقایسه مضامین) و شبکه مضامین (برای نشان دادن ارتباط و وابستگی مضامین) اشاره کرد. شبکه مضامین روشی در تحلیل مضامین است که آتراید استیرلینگ^۵ (۲۰۰۱) آنرا توسعه داده است. برای دستیابی به شبکه مضامین باید مراحل سه‌گانه انجام شود: الف) کشف مضامین اصلی و (شناسه‌ها و نکات کلیدی متن)؛ ب) کشف مضامین سازمان یافته (مضامین به دست آمده از تلخیص و ترکیب مضمونهای پایه‌ای)؛ ج) کشف

-
1. Thematic Network
 2. Boyatzis
 3. Ryan & Bernard
 4. Braun & Clarke
 5. Attride Stirling

مضامین فراگیر (مضامین عالی در برگیرنده اصول حاکم بر متن به عنوان یک کل) (عابدی جعفری و همکاران، ۱۳۹۵: ۱۷۰-۱۵۹).

لاجرم با توجه به روش تحقیق، می‌توان چنین گفت که تهدیدات امنیتی مربوط به تحلیل نقش قدرت سایبری بر توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک برای جامعه ایران عبارتند از:

الف) تهدیدات خارجی: مضمون فراگیر تهدیدات امنیتی تحلیل نقش قدرت سایبری بر توان‌افزایی 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 توأمان سخت‌افزی و نرم‌افزاری: (تهدیدات نرم‌افزاری و تهدیدات سخت‌افزاری) می‌باشد.

ب) تهدیدات داخلی: مضمون فراگیر تهدیدات داخلی گسترش اسلام‌گرایی افراطی در آسیای میانه برای جامعه ایران دارای سه مضمون سازمان یافته: ۱. تهدیدات امنیتی (شامل شش مضمون پایه: تهدید گروه‌های قومی تجزیه طلب، تهدیدات گروه‌های معترض و منتقد داخلی، تضعیف هویت دینی، ضعف و شناخت مدیران و تصمیم‌گیرندگان، ضعف برنامه‌ریزی 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 شبکه‌های 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 گروه-

های نفاق و اقدام به براندازی، ترویج تفکرات تفرقه‌افکنانه، و محروم کردن ایران از درآمدهای ترانزیتی خود) می‌باشد.

در ادامه به تحلیل داده‌های حاصل از مصاحبه نیمه ساخت یافته (نیمه استاندارد) با خبرگان حوزه فضای سایبری به منظور ارائه مدل مطلوب راهکارهای مقابله با تهدیدات سایبری در توان افزایشی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک پرداخته شده است. جامعه آماری این پژوهش شامل ۲۵ نفر از خبرگان دانشگاهی و متخصصان حوزه های 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 حوزه های علوم سیاسی، روابط بین الملل و جغرافیای سیاسی بوده‌اند. ۱۰ نفر آنها از مدیران مراکز سایبری در نیروهای مسلح و سازمان های اطلاعاتی جمهوری اسلامی ایران بوده، ۱۲ نفر کارشناس ارشد اجرایی در نهادهای یاد شده و ۳ نفر دارای مطالعات، کتاب و مقاله در حوزه های سایبری و شبکه های اجتماعی می باشند. ۱۰ نفر آنها دارای تحصیلات دکتری، ۲ نفر دانشجوی دکتری و ۱۳ نفر دارای تحصیلات کارشناسی ارشد هستند.

جدول ۲. فرایند کدگذاری باز، محوری و گزینشی در راستای دستیابی به مضامین مرتبط با راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایشی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک

مضامین فراگیر	مضامین سازمان یافته	مضامین پایه	گزاره های خبری
انتخاب دیپلماسی سایبری	توجه به دیپلماسی سایبری	ارتقای دیپلماسی سایبری	دیپلماسی سایبری ایران نیاز به ارتقاء دارد
		دیپلماسی درست و فعال	دولتمردان جمهوری اسلامی ایران می بایست دیپلماسی درست و فعال در حوزه سایبری اتخاذ نمایند
	حکمرانی و دیپلماسی مناسب سایبری	حکمرانی و دیپلماسی مناسب سایبری از ضروریات و نیازهای مبرم دیپلماسی امنیتی کشور است.	
	کاربرد بودن سیاست های اتخاذی در حوزه	ارتقای دیپلماسی سایبری و کاربردی بودن سیاست ها در مواجه با سایر ملل	

	سایبری		
	سیاست گذاری مناسب	توجه جدی به دو مقوله سیاست گذاری و سیاست شناسی در حوزه دیپلماسی	
	ایجاد پیوستگی بین تدوین و اجرای سیاستها و تعبیه مکانیزم مناسب برای اجرای سیاستها		
	تغییر نگاه سیاستگذاران و مدیران و تصمیم گیران نظام به بهره برداری از این فضا		
	اتخاذ سیاست گذاری مناسب بر اساس امکانات سخت افزاری و نرم افزاری		
	افزایش توان سیاست شناسی و سیاستمداری		
	ارتقاء ادراک شناسی سایبری با اتخاذ سیاست شناسی مناسب		
	استفاده از فناوری های نوین		
	راه اندازی اینترنت ملی و شبکه ملی اطلاعات		
	دستیابی به علوم و فناوری های پیشرفته		
	ارتقاء توان پدافندی (تربیت و آموزش نیروهای مستعد و نخبه)		
	ارتقای توان آفندی	ارتقای توان پدافندی	
	ارباب و ترساندن دشمن با ارتقاء توان آفندی و مقابله سایبری در برابر حملات		
	ارتقاء توان آفندی و پدافندی جمهوری اسلامی ایران با نوآندگی و به روز رسانی سخت افزاری و نرم افزاری		
	بهره برداری از توان داخلی تجهیزات سخت افزاری و نرم افزاری		
	استفاده از ظرفیت کشورهای مقاومت اسلامی	ایجاد جبهه واحد علیه سرویس های جاسوسی و ایادی ضد انقلاب وابسته به آنها در قالب محور مقاومت سایبری	افزایش توان و قدرت سایبری
	اقدامات تحکیمی و تقویت روابط مثبت با کشورهای اسلامی به منظور استفاده از ظرفیت آنها برای تشکیل محور مقاومت سایبری علیه کشورهای متخاصم و مقابله به مثل با آنها با هدف بازدارندگی در برابر حملات و تهاجم سایبری دشمن و تبادل نظر با آنها در تأمین امنیت جهانی و مقابله با تروریسم جهانی		
	استفاده از ظرفیت گروه های آزادی خواه و ضد استعماری در دنیا		
	اقدامات تحکیمی و تقویت روابط مثبت با کشورهای غیر اسلامی همسو با نظام جمهوری اسلامی ایران به منظور استفاده از ظرفیت آنها و گروه های آزادی خواه و ضد سلطه ی غیر اسلامی، جهت مقابله به مثل در برابر حملات و تهاجم سایبری دشمن و تبادل نظر با آنها در تأمین امنیت جهانی و مقابله با تروریسم جهانی		

کاهش آسیب پذیری، پایدارسازی، مصون سازی، ارتقاء توان بازدارندگی زیرساختهای حیاتی و حساس کشور در برابر تهدیدات و حملات سایبری	کاهش آسیب پذیری، پایدارسازی و مصون سازی	تقویت زیر ساخت های سایبری -	
رصد، پایش، مراقبت، تشخیص و هشدار هوشمندانه و دستیابی به اشراف اطلاعاتی در برابر تهدیدات فضای سایبری از طریق سازماندهی مراکز رصد و پدافند سایبری با رویکرد شناخت پیش دستانه تهدید	اشراف اطلاعاتی		
مدیریت و کنترل پیامدهای تهدیدات و حملات سایبری	مدیریت و کنترل حملات سایبری		
تقویت ساختار دستگاه های ناظر بر فضای سایبر و تبادل اطلاعات.	تقویت دستگاه های ناظر		
رویکرد تعامل محور و همپوشانی نقش دستگاه های مختلف متولی امنیت در فضای سایبر و ایجاد وحدت رویه در حوزه امنیت سایبری	اتخاذ رویکرد تعاملی در حوزه امنیت سایبری		
تأسیس ساختاری قدرتمند و فراقوه ای برای سیاست گذاری فضای مجازی کشور و ساماندهی و ایجاد هماهنگی بخشی	تأسیس ساختاری قدرتمند و فراقوه ای برای سیاست گذاری فضای مجازی		
ایجاد سیستم امنیتی برای ایمن سازی زیرساختهای ارتباطی کشور و کنترل و نظارت دائم بر محتوای داده های مبادله شده در فضای سایبر برای پیشگیری از گسترش فساد، تهدیدات امنیتی، نفوذ سرویس های جاسوسی، خرابکاری الکترونیکی و توسعه ظرفیت بازدارندگی در برابر تهدیدات نوین	ایجاد سیستم امنیتی سایبری		
توسعه توانمندیهای زیرساختی کشور متناسب با سیاستهای فضای سایبر	توسعه توانمندیهای زیرساختی سایبری		
شناخت درست از توان رقیب و دشمنان نظام در عرصه رقابت یا جنگ سایبری	دشمن شناسی		
مقابله به مثل در برابر حملات سایبری	مقابله به مثل در برابر حملات سایبری		
ارتقاء پروتکل ها و رعایت همه جانبه اصول حفاظتی	رعایت همه جانبه اصول حفاظتی		
ایجاد قوانین مناسب توسط قوه قضائیه در برخورد با مجرمین سایبری	ایجاد قوانین مناسب	اتخاذ سیاست گذاری فرهنگی،	اتخاذ سیاست گذاری فرهنگی،
به روز رسانی قوانین سایبری توسط	به روز رسانی قوانین		

قضایی و
آموزشی -
تربیتی
مناسب در
حوزه سایبری

دستگاه قضا جهت برخورد با مجرمین سایبری و تناسب قوانین با جرائم نوظهور سایبری	سایبری	مناسب
ایجاد ضمانت اجرا برای تصمیمات شورای عالی فضای مجازی توسط دستگاه قضا	تقویت ضمانت اجرایی تصمیمات	
تأسیس ساختاری قدرتمند و فراقوه‌ای برای سیاست‌گذاری فضای مجازی کشور و ساماندهی و ایجاد هماهنگی بخشی توسط دستگاه قضا	تأسیس ساختاری قدرتمند و فراقوه‌ای برای سیاست‌گذاری فضای مجازی	
اتخاذ تدابیر هوشمندانه و وضع قوانین مناسب در قبال کشورهای مهاجم به زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران از طریق فضای سایبر	وضع قوانین مناسب در قبال کشورهای مهاجم	
حمایت از سرمایه‌های انسانی و نخبگان سایبری توسط دستگاه قضا	حمایت از سرمایه‌های انسانی	
سیاست‌گذاری مناسب توسط دولت‌مردان در حفاظت از منابع حیاتی	سیاست‌گذاری مناسب توسط دولت‌مردان در حفاظت از منابع حیاتی	
سیاست‌گذاری مناسب توسط دولت‌مردان در قبال حملات و تهاجمات سایبری بیگانگان به زیرساخت‌های اطلاعاتی جمهوری اسلامی ایران	سیاست‌گذاری مناسب در قبال حملات و تهاجمات	
سیاست‌گذاری مناسب در جهت حمایت از سرمایه‌های انسانی و نخبگان سایبری توسط دستگاه‌های دولتی و متولیان امر	حمایت از سرمایه‌های انسانی و نخبگان سایبری	سیاست‌گذاری در حوزه آموزش و تربیت نیروی متخصص سایبری توسط دولت‌مردان
ساماندهی و ارتقا دانشی و بکارگیری منابع انسانی متخصص در حوزه پدافند سایبری	ساماندهی و بکارگیری منابع انسانی	
به روز رسانی سیاست‌های جمهوری اسلامی ایران در حوزه فضای سایبری و همکاری دستگاه‌های اجرایی کشور با متولیان امر در حوزه پدافند سایبری	به روز رسانی سیاست‌ها در حوزه فضای سایبری	
توجه به امر تولید محتوا	توجه به امر تولید محتوا	
تربیت و آموزش نیروهای جوان و تبدیل آنها به نخبگان عرصه سایبری	تربیت و آموزش نیروی جوان	
برگزاری دوره‌های مهارتی و آموزشی	برگزاری دوره‌های مهارتی و آموزشی	
بهره‌گیری از نیروهای متخصص و	بهره‌گیری از نیروهای	



	متخصص و توانمند	توانمند	
توجه به سیاست گذاری فرهنگی	سرمایه گذاری در حوزه فرهنگ سازی و تربیت و آموزش ملی	سرمایه گذاری در حوزه فرهنگ سازی و تربیت و آموزش ملی	
	آمادگی آرمانی پدافند سایبری	آموزش، فرهنگ سازی و برگزاری رزمایش به منظور نیل به آمادگی آرمانی پدافند سایبری	
	آگاه نمودن مردم	فرهنگ سازی در جهت آگاهی مردم از تهدیدات	
	توجه به آموزش همگانی	توجه به آموزش همگانی	
	فرهنگ سازی از طریق رسانه ها	استفاده از رسانه های جمعی در راستای فرهنگ سازی	
	بهره گیری از مراکز فرهنگی و آموزشی	بهره گیری از مراکز فرهنگی و آموزشی نظیر دانشگاه ها	
	طراحی، پیاده سازی الگوهای سایبری بومی	طراحی، پیاده سازی الگوهای پدافند سایبری بومی، دانش محور و پاسخگو به تهدید	
توجه به دانش و مهارت های بومی در حوزه سایبری	طراحی، پیاده سازی الگوهای سایبری بومی در مقابل تهدیدات	طراحی، پیاده سازی و اجرای نظام پدافند سایبری در مقابل تهدیدات و حملات سایبری با ویژگی بومی سازی فرایندها، نظامات و استانداردها، پروتکلها، رویه ها و روالها	
	طراحی، پیاده سازی و اجرای مراکز رصد	طراحی، پیاده سازی و اجرای مراکز رصد، پایش و کنترل زیرساخت های حیاتی به صورت بومی	
	نهادینه سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیرعامل و پدافند سایبری	نهادینه سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیرعامل و پدافند سایبری در طرح های توسعه ملی و استانی پدافند سایبری کشور	
	بومی و ایمنی سازی تجهیزات	بومی و ایمنی سازی تجهیزات مورد استفاده در زیرساخت های حیاتی و حساس کشور در جهت کاهش وابستگی به فناوری ها و محصولات غیربومی و ممنوعیت کاربرد سامانه های خارجی در آنها	
	تقویت صنعت پدافند سایبری بومی	تقویت صنعت پدافند سایبری بومی و حمایت از سازمان ها و شرکتهای تولیدکننده سامانه ها و محصولات بومی	
	ایجاد زیست بوم سایبری	الزام و همراه سازی سازمان های متولی زیرساخت های حیاتی و حساس کشور در ایجاد زیست بوم سایبری و	

استفاده از محصولات امن داخلی			
طراحی، پیاده سازی و اجرای نظریه‌ها و الگوهای پدافند سایبری بومی، دانش محور و پاسخگو به تهدید	ایجاد پدافند سایبری بومی و دانش محور		
کاهش وابستگی به فناوری‌ها و محصولات غیربومی و ممنوعیت کاربرد سامانه‌های خارجی در آنها	ممنوعیت کاربرد سامانه‌های خارجی		
نهادینه‌سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیر عامل و پدافند سایبری در طرح‌های توسعه ملی و استانی پدافند سایبری کشور	نهادینه‌سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیر عامل	توجه و تقویت پدافند غیر عامل	
سرمایه‌گذاری در حوزه پدافند غیر عامل و مؤلفه‌های آن	سرمایه‌گذاری در حوزه پدافند غیر عامل		
الزام و همراه‌سازی سازمان‌های متولی زیرساخت‌های حیاتی و حساس کشور در ایجاد و تقویت پدافند غیر عامل	تقویت پدافند غیر عامل		
بهره‌گیری از قابلیت‌های بسیج و سازمان‌های مردم نهاد در پدافند سایبری	توجه به نهاد مردمی بسیج	بهره‌مندی از ظرفیت نهادهای مردمی	تقویت سازمانهای مردم نهاد و NGO
بهره‌گیری از قابلیت‌های بخش خصوصی در پدافند سایبری	توجه به بخش خصوصی		
رویکرد تعامل محور و همپوشانی نقش دستگاه‌های مختلف متولی امنیت در فضای سایبر	اتخاذ رویکرد تعاملی میان نهادهای مردمی		
ایجاد وحدت رویه در حوزه امنیت سایبری	وحدت رویه در حوزه امنیت سایبری		
توجه به فرهنگ ملی و نمادهای ملی جهت تحکیم وحدت در جامعه و اقوام توسط نهادهای مردمی	توجه به فرهنگ ملی و نمادهای ملی		
راه اندازی گروه‌ها و شبکه‌های انسانی متنوع و متکثر در فضای سایبری در حوزه‌های اقتصادی، فرهنگی و رسانه‌ای جهت بالا بردن تاب‌آوری و مقاوم‌سازی نظام در برابر تهاجمات و حملات سایبری	راه‌اندازی گروه‌ها و شبکه‌های انسانی متنوع و متکثر	توجه به سازمان‌های مردم نهاد و NGO	
بسط و گسترش سازمان‌های مردم نهاد	گسترش سازمان‌های مردم نهاد		
توجه به NGO ها	توجه به NGO		



جدول ۳) تعداد مضامین فراگیر، سازمان یافته و پایه‌ای راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایشی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک

ردیف	مضامین فراگیر	مضامین سازمان یافته	مضامین پایه
۱	اتخاذ دیپلماسی سایبری	۲	۸
۲	افزایش توان و قدرت سایبری	۳	۲۰
۳	اتخاذ سیاست گذاری فرهنگی، قضایی و آموزشی - تربیتی مناسب در حوزه سایبری	۳	۲۱
۴	طراحی و پیاده‌سازی پدافند سایبری بومی	۲	۱۱
۵	NGO تقویت سازمانهای مردم نهاد و	۲	۸
	جمع کل	۱۲	۶۸

همان گونه که جدول ۳ نیز نشان می‌دهد راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایشی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک، براساس مصاحبه نیمه‌استاندارد با ۱۰ نفر از خبرگان و صاحب نظران از ۵ مضمون فراگیر: اتخاذ دیپلماسی سایبری، افزایش توان و قدرت سایبری، اتخاذ سیاست‌گذاری فرهنگی، قضایی و آموزشی - تربیتی مناسب در حوزه سایبری، طراحی و پیاده‌سازی پدافند سایبری بومی و تقویت سازمانهای مردم نهاد و NGO، از ۱۱ مضمون سازمان یافته و در نهایت با ۶۸ مضمون پایه‌ای به اشباع نظری رسیده است. پس از احصاء و استخراج مضامین فراگیر، مضامین سازمان یافته و مضامین پایه‌ای راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایشی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک، در این قسمت به ترسیم مدل مفهومی شبکه‌ای و یا همان تشکیل شبکه مضامین در نمودار ۲ مبادرت می‌شود.



نمودار ۲. مدل مفهومی شبکه‌ای راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک براساس مضامین فراگیر و سازمان یافته

بنابراین با توجه به جدول ۳ و نیز نمودار ۲ می‌توان چنین گفت که راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک عبارتند از:

(۱) **انحاز دیپلماسی سایبری:** مضمون فراگیر انحاز دیپلماسی سایبری دارای دو مضمون سازمان یافته: الف) توجه به دیپلماسی سایبری و ب) توجه جدی به دو مقوله سیاست‌گذاری و سیاست‌شناسی تشکیل شده است.

(۲) **افزایش توان و قدرت سایبری:** مضمون فراگیری افزایش توان و قدرت سایبری دارای سه مضمون سازمان یافته: الف) ارتقای توان پدافندی و آفندی و ب) ایجاد جبهه واحد علیه سرویس‌های جاسوسی و ایادی ضد انقلاب وابسته به آنها در قالب محور مقاومت سایبری و ج) تقویت زیرساخت‌های سایبری تشکیل شده است.

- ۳) اتخاذ سیاست‌گذاری فرهنگی، قضایی و آموزشی - تربیتی مناسب در حوزه سایبری: مضمون فراگیر اتخاذ سیاست‌گذاری فرهنگی، قضایی و آموزشی - تربیتی مناسب در حوزه سایبری دارای سه مضمون سازمان یافته: الف) توجه به سیاست‌گذاری فرهنگی، ب) سیاست‌گذاری در حوزه آموزش و تربیت نیروی متخصص سایبری و ج) اتخاذ سیاست‌گذاری قضایی مناسب تشکیل شده است.
- ۴) طراحی و پیاده‌سازی پدافند سایبری بومی: مضمون فراگیر طراحی و پیاده‌سازی پدافند سایبری بومی دارای دو مضمون سازمان یافته: الف) توجه و تقویت پدافند غیرعامل و ب) توجه به دانش و مهارت‌های بومی در حوزه سایبری تشکیل شده است.
- ۵) تقویت سازمان‌های مردم نهاد و NGO ها: مضمون فراگیر تقویت سازمان‌های مردم نهاد و NGO ها دارای دو مضمون سازمان یافته: الف) توجه به سازمان‌های مردم نهاد و ب) بهره‌مندی از ظرفیت‌های مردمی تشکیل شده است.

نتیجه‌گیری

امروزه گسترش فضای سایبر باعث پیدایش مرزهای مجازی شده و به این دلیل، درک واقع‌بینانه از تهدیدات امنیتی فضای سایبری در گرو توجه به عوامل نرم‌افزاری است که در واقع، حلقه واسط بین محیط امنیتی کشورها و سخت‌افزارها قرار دارند و بدین علت، برداشتها از مفهوم امنیت ملی در این فضا به چالش کشیده شده است. یکی از محورهای اصلی تهدیدات امنیتی در عصر ارتباطات و جهانی‌شدن برای کشورها را باید در حوزه سایبری دانست که نمونه بارز آن حمله رایانه‌ای به تأسیسات هسته‌ای و الکترونیکی ایران توسط سرویس جاسوسی کشور آمریکا می‌باشد. تکنولوژی اطلاعات، صرف‌نظر از موقعیت جغرافیایی در تمام شئون زندگی وارد شده است، لیکن این رشد علیرغم مزایای خود جنبه‌های منفی هم در بر داشته است. بدین مفهوم که امکان رفتارهای ضداجتماعی و مجرمانه را به وجود آورده که پیش از این به هیچ وجه امکان‌پذیر نبوده است و با روند رو به رشد این جرایم روبرو هستیم. زیرا جرایم رایانه‌ای به دلیل ویژگی‌هایی که دارند، نسبت به سایر طرق ارتکاب جرایم مرجح می‌باشند. اول آنکه، شیوه ارتکاب آنها آسان است، با مبالغ اندک، خسارات هنگفتی می‌توانند وارد نمایند، می‌توان بدون حضور

فیزیکی در یک حوزه قضایی معین در آن حوزه مرتکب این‌گونه جرایم شد، دست آخر اینکه در اغلب موارد غیرقانونی بودن آنها روشن نمی‌باشد.

قدرت و توان ملی و امنیتی یک کشور با توجه به منابع و نیروی انسانی، قادر به مقابله به تهدیدات فضای سایبری است. برحسب میزان توانایی که دولتها در استفاده از تکنولوژی اطلاعات دارند روشها و راهکارهای مقابله با تهدیدات فضای سایبری هم برای آنها آسان خواهد بود. جمهوری اسلامی ایران، طی یک دهه اخیر، نیز سیاست‌گذاری‌هایش بر این پایه استوار بوده که بتوانند با گسترش توان و افزایش قدرت سایبری، جایگاه خود را در سلسله‌مراتب توان جهانی در این حوزه ارتقاء بخشند. با توجه به رویکرد فعلی کشورهای متخاصم در استفاده ابزاری در حملات سایبری علیه جمهوری اسلامی ایران در حوزه‌های مختلف نظامی، اقتصادی، علمی و فرهنگی، ارتقای قدرت سایبری دستگاه‌های متولی امنیت ملی، علی‌الخصوص نیروهای مسلح جمهوری اسلامی ایران، با حمایت‌های نهادهای تصمیم‌گیر نظام از جمله شورای عالی فضای مجازی، امری دارای اهمیت و با اولویت بالا می‌باشد. با توجه به انواع تهدیدات فضای سایبری که در جدول شماره ۱ آورده شده‌اند، هر کدام از این تهدیدات، علیه ج.ا.ایران از سوی کشورهای متخاصم می‌تواند مورد استفاده قرار گیرد. با توجه به نمودار شماره ۲، مدل راهکارهای مقابله با تهدیدات فضای سایبری در توان‌افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک ارائه گردیده است.

منابع

- آشوری، داریوش (۱۳۷۰)، *دانشنامه سیاسی*، تهران: انتشارات مروارید.
- تقی‌پور، رضا و اسماعیلی، علی (۱۳۹۷)، «طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران»، *فصلنامه علمی پژوهشی امنیت ملی*، دوره ۸ شماره ۳۰، صص ۲۰۲-۱۸۱.
- جالینوسی، احمد و ابراهیمی، شهروز و قنواتی، طیبه (۱۳۹۲)، «جایگاه فضای سایبر و تهدیدهای سایبری در استراتژی امنیت ملی ایالات متحده آمریکا»، *فصلنامه دانش سیاسی و بین‌الملل*، سال دوم، شماره پنجم، بهار، صص ۲۰-۱.

حافظ‌نیا، محمدرضا (۱۳۹۰)، **جغرافیای سیاسی فضای مجازی**، تهران: انتشارات سمت،

چاپ اول

خلیلی پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱)، «تهدیدات سایبری و تأثیر آن بر امنیت ملی»، **فصلنامه مطالعات راهبردی**، سال پانزدهم، شماره ۲، صص ۱۹۵-۱۶۷.

دهخدا، علی‌اکبر (۱۳۳۹)، **لغت نامه**، جلد ۳۶، تهران: چاپ سیروس

صیاد، محمدکاظم و بزرگمهر، علی و امینی، آرمین و طاهری، ابوالقاسم (۱۳۹۹)، «تهدیدهای سایبری و اقدامات امنیتی در فضای مجازی؛ بررسی رویکردهای ایالات متحده آمریکا و جمهوری اسلامی ایران»، **فصلنامه علمی امنیت ملی**، سال دهم، شماره ۳۸، صص ۳۳۱-۲۹۳.

عابدی جعفری، حسن و تسلیمی، محمدسعید و فقیهی، ابوالحسن و شیخ‌زاده، محمد (۱۳۹۵)، «تحلیل مضمون و شبکه مضامین: روشی ساده و کارآمد برای تبیین الگوهای موجود در داده‌های کیفی»، **فصلنامه اندیشه مدیریت راهبردی**، سال پنجم، شماره ۲، شماره پیاپی ۱۰، صص ۱۵۱-۱۹۸.

غروی، حسین و محمدی، علی (۱۳۹۰)، **معرفی رویکردها و متدولوژی‌های طراحی و اجرای سناریوهای مقابله با تهدیدات سایبری**، تهران: انتشارات دانشگاه دفاع ملی قدسی، امیر (۱۳۹۲)، «تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی ایران و ارائه راهبرد، **فصلنامه راهبرد دفاعی**، سال یازدهم»، شماره ۴۴، صص ۱۸۶-۱۴۹.

کرامر، فرانکلین و استار، استیوارت و ونتز، لری (۱۳۹۴)، **قدرت سایبری و امنیت ملی**، تهران: مؤسسه چاپ و انتشارات دانشکده اطلاعات

کربلابی تاج‌الدین، محمد و محمدنژاد، حسن و سلیمی، سعید (۱۳۹۵)، **فضای مجازی و شبکه‌های اجتماعی**، تهران: انتشارات پشتیبان

کریم‌آبادی، پیام (۱۳۹۲)، **امنیت در فضای سایبری**، www.parsbook.org

کریمی، سجاد و منعم، علیرضا و کاظمی‌پور، علی (۱۳۹۴)، «تحلیلی بر مؤلفه‌های دکتربین سایبری (مطالعه موردی: جمهوری اسلامی ایران)»، **فصلنامه پژوهش‌های**

روابط بین‌الملل، سال چهارم، شماره ۱۵، صص ۲۲۰-۱۹۳.

مجتهدزاده، پیروز (۱۳۹۱)، فلسفه و کارکرد ژئوپولیتیک (مفاهیم و نظریه‌ها در عصر فضای مجازی)، تهران: انتشارات سمت، چاپ اول

معین، محمد (۱۳۷۱)، فرهنگ فارسی، جلد ۲، تهران: انتشارات امیر کبیر
 منتظر قائم، مهدی (۱۳۸۱)، امنیت در فضای مجازی، تهران: انتشارات پژوهشگاه فرهنگ، هنر و ادبیات

موحدی صفت، علیرضا (۱۳۸۶)، «امنیت ملی در فضای سایبر، فرصتها و تأکیدهها با تأکید بر استقرار دولت الکترونیکی»، فصلنامه مطالعات دفاعی استراتژیک، سال هشتم، شماره ۳۰، صص ۲۷۶-۲۴۵.

موسوی، سید محمد رضا و حیدری، خدیجه و قنبری، علی (۱۳۹۲)، «تاثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن»، فصلنامه علمی مطالعات بین‌المللی پلیس، دوره چهارم، شماره ۱۴، صص ۱۱۷-۱۰۱

نورمحمدی، مرتضی (۱۳۹۲/۰۵/۰۸)، «واکاوی ابعاد سایبر تروریسم علیه امنیت ملی ایران»، تاریخ استخراج: ۱۴۰۰/۰۲/۱۵، پایگاه خبری تحلیلی مطالعات تروریسم: هایلیان، <https://www.hablian.ir>

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

Denning, D. E. (2014). Framework and principles for active cyber defense. Computers & Security, 40, 108-113.

Director of National Intelligence. (2010). Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. United State of America, February

Kristin M, Lord & Sharp, Travis. (2011). "America's Cyber future Security and Prosperity in the Information Age", Center for a New American Security, Volume I.

Lin, Herbert. (2011). 'Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion', in Georgetown Journal of International Affairs, Special Issue, International Engagement on Cyber : Establishing International Norms and Improved Cybersecurity, pp.127-135.

Nagre, Dhanashree & Warade, Priyanka (2008). "Cyber Terrorism Vulnerabilities and Policy Issues "Facts Behind The Myth", <http://www.andrew.cmu.edu/user/dnagre/>

Oliverio, Annamarie and Lauderdale, Pat. (2016). terrorism as deviance or social control, Sage Publication, London, Thousand Oaks and New Delhi.
Osula, Anna Maria (2018), National Cyber Security Organisation United Kingdom, NATO Cyber Defence Training Center
Oxford advanced learners dictionary. (2000). Oxford University Press
Peritz, Akij & Sechrist, Michael. (2010); "Protecting Cyberspace and the U.S. National Interest", Belfer Center for Science and International Affairs.
Rodriguez, Carlos A. (2006). "Cyber terrorism", Inter-American Defense College as a prerequisite for the Diploma approved Starr, Stuart H. (2009). "Towards an Evolving
Rndle, James(2021), Ransomware Poses a Threat to National Security, Report Wares. The Wall Street Journal.

