DOI:10.22124/wp.2022.5385

سیاست جهانی

فصلنامه علمی سیاست جهانی، دورهٔ دهم، شمارهٔ چهارم، زمستان ۱۴۰۰ ، پیاپی۳۸ (صفحات: ۶۲-۳۱)

ارائه مدل راهکارهای مقابله با تهدیدات فضای سایبری در توان‌افزایی امنیت ملی جهموری 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

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 سنتی 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 حوزهٔ 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 توان افزایی 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 حوزهٔ 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 مبرّا 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.

مقدمه

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 حوزهٔ 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 حوزهٔ قضایی معین در آن حوزهٔ 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 مسؤولیت 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. به‌طوری‌که 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، حوزهٔ ژئوپولیتیکی خاورمیانه به‌دلیل 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، ارایه الگوی راهکارهای مقابله با تهدیدات سایبری در توان‌افزایی امنیت ملی جهموری اسلامی ایران از منظر ژئوپولیتیک است.

بنابراین مسألهٔ اصلی شکل گرفته این است که راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک کدامند؟ فضای سایبری چگونه باعث توان افزایی 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 حوزۀ امنیت سایبری، جغرافیای سیاسی و علـوم سیاسـی بـر اسـاس روش تخمینی و در دسترس و به‌طور هدفمند انتخاب گردیدند کـه بـا اشـباع نظـری (۲۵ نفر)، مصاحبه‌ها انجام شده است. پرسش‌های مصاحبه، نیمـه اسـتاندارد و محقـق سـاخته بوده‌اند که روایی آنها از سوی تعدادی از اسـتادان دانشـگاه بـه طـور صـوری و محتـوایی مورد تأیید قـرار گرفتنـد. بـرای تحلیـل داده‌هـا، بـا توجـه بـه ماهیـت و روش تحقیـق و ضرورت تحلیل فرامتن، از روش تحلیل محتوای کیفـی اسـتفاده شـد. ایـن روش یکـی از روش‌های کاربردی است کـه پژوهشـگران بـا اسـتفاده از آن بـه وارسـی داده‌هـای خـود می‌پردازند. تحلیل محتوا فرایند درک، تفسیر و مفهوم‌سازی معانی درونی داده‌ها است.

پیشینه تحقیق

تحقیق‌ها و بررسی‌های فراوانی درباره اینترنت، فضای مجازی، فناوری‌های نـوین، فضـای سایبری و آثار تحولی آنها، همچنین تهدیدات ناشی از بهره‌گیـری از ایـن فضـا بـر امنیـت ملی انجام گرفته است که در زیر به برخی از پیشینه‌های مطالعاتی در ارتبـاط بـا موضـوع مقاله اشاره می‌گردد.

موسوی و همکاران (۱۳۹۲) در مقاله «تـأثیر تهدیـدات امنیتـی تروریسـم سـایبری بـر امنیت ملی جمهوری اسـلامی ایـران و راهکارهـای مقابلـه بـا آن» بـه روش اسـنادی و بـا استفاده از منابع کتابخانـه‌ای بـا ابـزار فـیش‌بـرداری، حـوزۀ سـایبری را بـه‌عنوان یکـی از محورهای اصلی تهدید امنیتی در عصر ارتباطات و جهانی‌شدن برای کشـورها در حـوزۀ سایبری می‌داننـد و نمونـه بـارز آن را حملـه رایانـه‌ای آمریکـا بـه تأسیسـات هسـته‌ای و الکترونیکی ایران معرفی می‌نمایند. آنها در این مقاله به بررسی تأثیر تروریسم سـایبری بـر امنیت ملی جمهوری اسلامی ایران پرداخته و آن را بـه مراتـب خطرنـاک‌تـر از تروریسـم سنتی می‌دانند. در نتیجه‌گیری بحث و پیشنهادها هم تصریح می‌نمایند: باید تا حـد ممکـن در محور سیاست‌های پیشگیرانه از آسیب و اقدامات حقوقی از طریق مراجـع و سـازمان‌های بین‌المللی و تدابیر نظارتی در این خصوص، برنامه‌ریزی شود. نـه مـی‌تـوان فنـاوری اطلاعات و ارتباطات الکترونیکی را کنار گذاشت و به یک جامعه عاری از آن تبـدیل شـد و نه امکان ریشه‌کنی هرگونـه اقـدام تروریسـتی علیـه کشـور وجـود دارد. لـذا تنهـا 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 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 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 ازجمله خرابکاری، اخلال، 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 حوزهٔ 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 حوزهٔ امنیت ملی، به‌رغم فعالیت‌ها 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.

دوتی.ای. دنینگ (۲۰۱۴) در مقاله‌ای بـا عنـوان «چـارچوب و اصـول دفـاع سـایبری فعال» تلاش می‌نماید ضمن مرور مفاهیم حوزهٔ دفاع هـوایی و موشـکی، همچنـین دفـاع سایبری فعال و غیرفعال و تسری این مفاهیم به فضای سایبری، اصول اخلاقـی و قـانونی برای راهبری دفاع سایبری فعال ارائه نماید. وی دفاع سـایبری فعـال را بـا چهـار ویژگـی تأثیرات (داخلی و خارجی)، درجه همکاری، نوع تأثیرات (انتشار اطلاعات، جمـع‌آوری، مسدودسازی فعالیت‌های خصمانه (و درجه مکانیزه بودن) در ارتباط بـا میـزان اثرگـذاری عامل انسانی) مورد ارزیابی قرار دهد.

آنـا ماریـا اسـولا (۲۰۱۸) در کتـاب «امنیـت سـایبری در انگلـیس» عنـوان مـی‌نمایـد: خدمات الکترونیک باید بسیار ساده و آسان باشد تا همه شـهروندان از آنهـا اسـتفاده کننـد و نمی‌توان هیچ شهروندی را نادیده گرفت. به این ترتیب، می‌توان گفت که انگلسـتان در حال ارتقای میزان دسترسی بـه ارتباطـات الکترونیکـی و گسـترش پهنـای بانـد ثابـت در سراسر کشور است. شورای امنیت ملی انگلیس با توجه بـه پیامـدهای حمـلات احتمـالی سایبری، حملات خصمانه به فضای سایبری انگلیس از سوی کشـورهای دیگـر و جـرائم سایبری گسترده را از مهمترین تهدیدات امنیـت ملـی در نظـر گرفتـه اسـت. وی بـا ایـن کتاب به متحدان ناتو در مورد مدیریت امنیت سایبری ملی انگلـیس کمـک مـی‌کنـد. ایـن پروژه با هدف حمایت از کشورها در ارتقای ساختار سازمانی خود، تشـویق بـه نـوآوری در شیوه‌ها و کمک به توسعه همکاری میان مؤسسات ملی مختلف انجـام شـده اسـت. در بخشی از این کتاب آمده است: دولت مجموعه مشـخص از الگوهـای مـدیریت حـوادث ملی را که به‌طور منظم، از جمله از سوی وزیران اجـرا مـی‌شـوند، تأییـد کـرده اسـت. بـا توجه به خطر حمله احتمالی علیه شـبکه‌هـای خبـری و نیروهـای مسـلح و دارایـی‌هـا و توانایی‌ها، دولت اظهار داشت که تعدادی از برنامه‌های کسب‌وکار و برنامـه‌هـای احتمـالی برای اطمینان از اینکه بتوانیم نقش خود را ایفا کنیم، برنامه‌ریزی و اجرا می‌شـود و امنیـت سایبری به طور کامل در مسیر فرایند برنامه‌ریزی عملیات احتمالی است.

راندل[1] (۲۰۲۱) در مقاله گزارش هشدارها و بـاج‌افـزار[2]، تهدیـدی بـرای امنیـت ملـی است، بیان می‌کند که مقامات دولتی و کارشناسان امنیـت سـایبری بـاج افـزار را تهدیـدی جدی برای امنیت ملی می‌دانند و پیشنهاد می‌کنند که دولت فدرال با همـان ابزارهـایی کـه برای پیگرد کارتلهای مواد مخدر و سایر سازمان‌های جنایتکار استفاده می‌شـود، بـه دنبـال باندهای باج‌افزار برود. فیلیپ راینر، مدیر اجرایی مؤسسه امنیت و فنـاوری، یـک سـازمان غیرانتفـاعی امنیـت سـایبری، گفتـه اسـت: افـزایش حمـلات بـه دولـت‌هـا، مـدارس و سازمان‌های بهداشتی در طی شیوع ویروس کرونا نشان‌دهنده خطر باج افزار است.

جنبه جدید بودن این مقاله پژوهشی در این است که نخست، به‌صورت جامع و کلـی به احصاء تهدیدات و فرصت‌های گوناگون فرهنگی، اجتماعی، سیاسی، امنیتـی، اقتصـادی و آموزشی از منظر صاحبنظران حوزهٔ امنیت ملی و فضـای سـایبری بـا روش کیفـی و بـه صورت تحلیل محتوا پرداخته شده است در صـورتی کـه اغلـب تحقیقـات انجـام گرفتـه قبلی با روش کمی و یا از پرسشنامه استفاده کرده‌اند. دوم: در این پژوهش به‌طور ویژه بـه تأثیر قدرت سایبری بر امنیت ملی جمهوری اسلامی ایران پرداخته شـده اسـت کـه مـورد مشابه یا پژوهش‌های مبسوطی در ایـن خصـوص انجـام نگرفتـه و در معـدود تحقیقـات انجام گرفته درباره قدرت سایبری، توجه چندانی به امنیت ملی جمهـوری اسـلامی ایـران نگردیده است. سوم: در اکثر پژوهش‌های مشابه، فضای سایبری بـه‌عنوان یکـی از عوامـل تهدید کننده امنیت ملی معرفی شده و دولـت‌هـا از آن بـه‌عنوان یـک حـوزهٔ تهدیـد یـاد می‌نمایند. ولی در این رساله، علاوه بر ذکر مؤلفه‌های تهدید سـایبری، از قـدرت سـایبری به عنوان یکی از مهمترین فضاهای افزایش دهنده سطح امنیت ملی در جمهـوری اسـلامی ایران پرداخته شده که تاکنون از این منظر، مقاله‌ای نگارش نشـده اسـت. چهـارم: در ایـن تحقیق به صورتی جـامع، موانـع موجـود در مسـیر حکمرانـی و سیاسـت‌گذاری فضـای سایبری احصاء شده که از جمله این موانع می‌توان به موانع شـناختی، فنـی- زیرسـاختی، نهادی قانونی، سیاستی و سیاسی - اجتماعی اشاره کرد که از این حیث هم ایـن پـژوهش، جدید و یک نوآوری محسوب می‌شود.

1. James Rundle
2. Ransomware

مبانی نظری

مفهوم فضای سایبری

واژه سایبر از ریشه یونانی سایبرنتیک[1] 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 این‌گونه 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(منتظرقائم،۱۳۸۱: ۲۳۱). در واقع، فضای سایبری محیطی است مجازی و غیرملموس در فضای شبکه‌های بین‌المللی. این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند که دراین محیط، تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طو کلی هر آنچه در کره خاکی به‌صورت 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 نظرگرفتن 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 بپردازد. در همین راستا، برخی از نظریه‌پردازان، امنیت ملی را معادل با ارزش‌های حیاتی کشور می‌دانند. بدان‌گونه که آرنولد ولفرز[1] آن را برابر با «نبود تهدید برای ارزشهای اکتسابی» می‌داند. 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

1. Arnold Wolfers

(Intelligence:2010. در همین راستا، ریچارد کلارک[1] 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 گسترهٔ 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 به عنوان 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[1] 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 تعین 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 محدوده‌ای 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

حمله‌های سایبری	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 جنگ های ترکیبی قرار گرفته است(تقی‌پور و اسماعیلی،۱۳۹۰: ۱۸۱)
تروریسم سایبری	اصطلاح تروریسم سایبری نخستین بار توسط کالین باری مورد استفاده قرار گرفته است برای تبیین این اقدام یا این نوع از تروریسم، تعاریف متعددی ذکر شده است. برخی از افراد معتقدند؛ تروریسم سایبری به پدیده‌ای 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).
جرایم سایبری	افزایش روزبه‌روز 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). تحلیل‌گران 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).
	جاسوسی سایبری، رصد و جمع‌آوری اطلاعات محرمانه از رایانه‌ها و سیستم‌های مربوطه، بدون اطلاع و اجازه صاحبان آنهاست. برخلاف جرایم سایبری که مسائل

جاسوسی سایبری	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 رقبای سیاسی، (Lord and Sharp, 2011: 17) ربایش اطلاعات با هدف ضربه زدن به اقتدار سیاسی و زیر سئوال بردن حاکمیت ملی کشورها جهت نیل به براندازی نظام سیاسی حاکم در کشورهای هدف، از دیگر مقاصدی است که سرویسهای جاسوسی در نبرد سایبری با یکدیگر از آن بهره می‌برند.
آشفتگی سایبری	آشفتگی 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 می کنند که غیرقانونی هستند. گروه‌های هکری آنارشیستی و نیهیلیست‌ها از آشفتگی سایبری استفاده می کنند. 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، آشفتگی 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 شبکه-های هدف وارد شود، اما قصد و نیت اصلی آشفتگی سایبری، آسیب رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند، ولی تا کنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده‌اند(Lord and Sharp,2011:18).

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 نیـز معنـی‌دار مـی‌کنـد کـه کالبـد شـکافی و تبیـین آنهـا بـه گسـترش دانـش ژئوپولیتیک در فضای سایبری می‌انجامد. ابعـاد مختلـف ژئوپولیتیـک در فضـای سـایبری عبارتند از : ۱. بعد مدیریتی و کنترل؛ ۲. بعد هویتی؛ ۳. بعد همگرایی و همکـاری؛ ۴. بعـد رقابتی و ستیز؛ ۵. بعد شکاف و توسعه؛ ۶. بعد تولید قـدرت؛ ۷. بعـد حـاکمیتی و کنتـرل ملی(حافظ‌نیا، ۱۳۹۰: ۳۲۹-۳۲۳).

حکومت‌ها و کشورها به عنوان بازیگران اصلی عرصه بین‌المللـی و نیـز شـرکت‌هـا و بنگاه‌های اقتصادی به عنوان بازیگران عرصه جهانی به شبکه اینترنـت و فضـای سـایبری، نگرشی ابزاری دارند که به تولید قدرت برای آنها منجر می‌شود. لاجرم دولـت‌هـا تـلاش می‌کنند هم از حیث توسعه فناوری اطلاعات و ارتباطات و هم از حیـث توسـعه ضـریب نفوذ اینترنت و افـزایش تعـداد کـاربران و هـم از حیـث دیجیتـالی کـردن امـور زنـدگی شهروندان و نیز امور عمومی و اداری کشور اقدام کنند و شرکت‌ها نیز مـی‌کوشـند بـرای افزایش سرعت انجام امور و نیز نوآوری فناورانـه در خـدمات خـود بـه مشـتریان و نیـز صرفه و صلاح شرکت در انجام خدمات به قابلیت‌های شبکه اینترنـت و فضـای مجـازی پناه ببرند(حافظ‌نیا، ۱۳۹۰: ۳۲۹). البته قابل ذکر است که برخلاف تأثیرات عمیقی که اندیشه مجازی شدن فضای سیاسی بر جهانی‌اندیشی ژئوپولیتیـک داشـته اسـت، ماهیـت فضـایی ژئوپولیتیک یعنی رقابت قدرت‌ها برای تسلط بر جهان یا منطقه با استفاده از امکانـاتی کـه زمین در اختیار می‌گذارد از میان نرفته است و دچـار دگرگـونی مـاهوی نشـده اسـت. در واقع، ژئوپولیتیک با پذیرفتن فلسفی موجودیت فضـای مجـازی در کنـار فضـای حقیقـی تلاش دارد بحث فضای سایبری را در چارچوب ایده‌آل‌های واقع‌گرایانه سروسامان دهـد. قابل دقت است که در مبحث فضـای سـایبری، مطالعـه کننـده در حقیقـت بـا دو مفهـوم جداگانه ولی مکمل هم سروکار دارد : ۱. اسباب و وسایل رسیدن به فضـای سـایبری کـه در اصطلاح انگلیسیCyber Space خوانده می‌شود؛ ۲. خود فضای مجـازی کـه آن را در اصطلاح انگلیسی Virtual Space گویند(مجتهدزاده، ۱۳۹۱: ۸۴-۷۸).

امروزه توانایی استفاده از فضای سایبری، یکی از مهمتـرین منـابع قـدرت در قـرن ۲۱ به حسـاب مـی‌آیـد. بـازیگران دولتی و غیردولتی از این قدرت اسـتفاده مـی‌کننـد تـا بـه اهـداف اجتمـاعی، ایـدئولوژیکی، سیاسـی، نظـامی و مـالی خـود در فضـای سـایبری و

دنیای واقعی دست یابند(Lord and Sharp, 2011:22). این نکته نباید نادیده گرفته شود که امروزه انگیزه‌های زیادی از قبیل ژئوپولیتیکی، 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(موحدی‌صفت،۱۳۸۶: ۲۴۷).

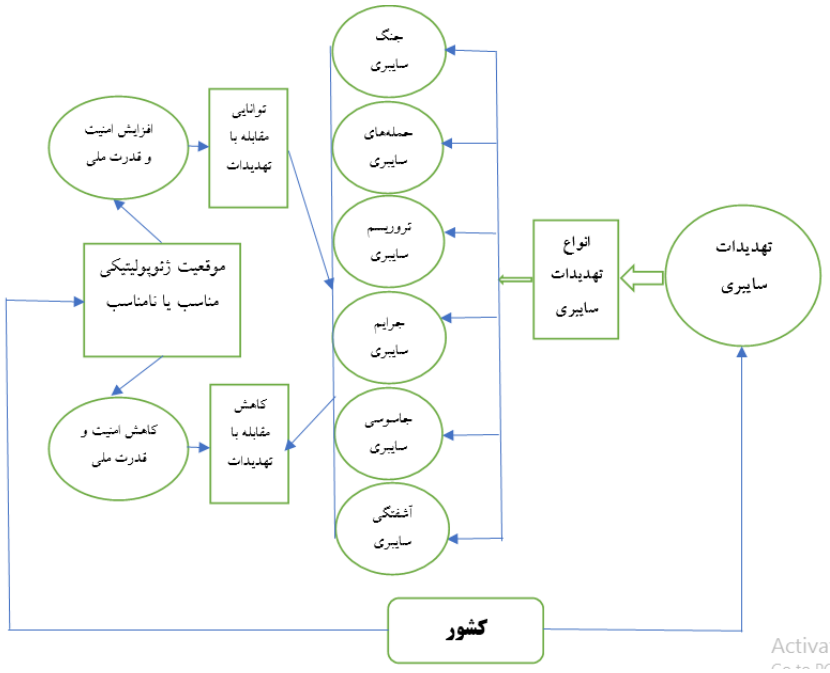
امروزه اکثر نظریه‌پردازان ژئوپولیتیک جهان اعتقاد دارند که مرزهای سیاسی دچار تغییر کاربرد شده و نمی‌توانند جلوی بسیاری از تهدیدات بگیرند. تروریسم نیز از دیگر سو به جنگی همطراز علیه جامعه جهانی بدل شده و امنیت دولت‌ها را با چالش‌های بسیاری مواجه می‌کنند(کریمی و همکاران، ۱۳۹۴: ۱۹۳). تأثیر فضای سایبری بر 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

دولتـی بیشـمار دیگر(کرامـر و همکـاران،۲۰۱۰: ۸۴). پیـام‌آوران انفجـار تکنولـوژی اطلاع‌رسانی و جهانی‌شدن ارتباطات اینترنتی در فضای مجازی بر این واقعیت نیـز چشـم بسته‌اند که ۸۵٪ از کاربران اینترنتی در کشورهای پساصـنعتی زنـدگی مـی‌کننـد. نـه تنهـا توزیع نابرابر امکانات در فضای مجازی سراسـر گیتـی را بـه معنـای واقعـی از دسترسـی برابر به اینترنت محروم کرده است بلکه اعمال محدودیت‌های دولتی نیـز اسـتفاده آزادانـه و مطلق از آن را در بسیاری از کشورها دشوار می‌کند. همچنین نه تنهـا اینترنـت و فراینـد سریع ارتباطات از راه دور همسویی فکری و هویتی گروه‌ها و ملـت‌هـا را بیشـتر نکـرده، بلکه در مواردی به تقویت هویت‌گرایی‌هـای محلـی و ملـی و یـا حتـی بـه واکـنش‌هـای هویتی خشونت‌آمیز نیز انجامید (مجتهدزاده،۱۳۹۱: ۸۳).

آنچه که در پیوند میان ژئوپولیتیک و فضای سایبری، نقش‌آفرینی مهمـی دارد، قـدرت است. قدرت دارای مفاهیم لغوی و اصطلاحی، همچنـین دیـدگاه‌هـای مختلفـی در علـوم گوناگون از جمله علوم انسانی، اجتماعی و سیاسی است. فرهنگ‌های زبـان فارسـی، واژه قدرت را در مفاهیم «توانستن»، «توانایی داشتن» و «توانایی» بکـار بـرده‌اند(دهخـدا،۱۳۳۹: ۳۶). همچنین به صفتی که تأثیر آن بر وفق اراده باشد، معنـا کـرده‌انـد(معین،۱۳۷۱: ۲). در فرهنگ سیاسی غرب، واژه‌هایی مثل Power و Authority به عنـوان معـادل کلمـه قـدرت به‌کار رفته است که به معنی استعداد و توانایی انجـام کـار مـی‌باشـد(Oxford,2000:970). در علوم سیاسی، قدرت مجموعه‌ای از عوامل مادی و معنوی است که موجب بـه اطاعـت در آوردن فرد یا گروه، توسط فرد یا گروه دیگر مـی‌گردد(آشـوری،۱۳۷۰: ۲۴۷). قـدرت در ژئوپولیتیک به نیروی به ثمر رساندن اراده یـا سیاسـت‌هـای ملـی یـک موجودیـت در ورای مرزهای کشوری‌اش گفته می‌شود. قدرت از منظر ژئوپولیتیک، هـم در وجـود یـک کشور با حکومت مقتدر برای نقش‌آفرینی‌های جهانی و منطقه‌ای و هم در وجـود جمعـی از کشورها، و باز هم در وجود شرکت‌های چندملیتی بزرگ و سـازمان‌هـای موضـوعی و منطقه‌ای واقعیت می‌یابد(مجتهدزاده،۱۳۹۱: ۱۰۵). می‌توان گفت که قدرت در جهان امروزی معنای جدیدتری نیز پیدا کرده است و این تغییر مفهـوم از قـدرت بـه دلیـل رشـد سـریع فضای سایبر و ایجاد زمینه‌های جدید و مهم در سیاسـت اسـت. امـروزه توانـایی نفـوذ در فضای سایبر به عنوان یکی از مهمترین منـابع قـدرت در قـرن۲۱ محسـوب مـی‌شـود. لـذا

بازیگران دولتی و غیردولتی برای دست یافتن بـه اهـداف نظـامی، ایـدئولوژی و اجتمـاعی فضای سایبر یا فضای فیزیکی، از این فضا استفاده مـی‌کننـد(Lord and Sharp, 2011:20). قدرت سایبری امروزه بُعد مهمی از زیست‌واره جهانی را شکل می‌دهد.

اطلاعات و فناوری‌های اطلاعاتی در سپهر سیاسی، اقتصـادی و نظـامی نقـش حیـاتی ایفا کرده و مقدمات فعالیت‌های عملیاتی را فراهم می‌آورنـد(منوچهری،۱۳۷۶:۳۳). مفهـوم قدرت سایبر را می‌توان در برابر مفاهیمی چون قـدرت دریـایی، قـدرت هـوایی، قـدرت زمینی و حتی قدرت فضایی بررسی کرد(کرامر و همکاران،۲۰۰۹: ۴-۵).



شکل ۱. مدل مفهومی پژوهش

یافته‌های کیفی تحقیق

برای تحلیل داده‌های کیفی مرتبط با راهکارهای مقابله با تهدیدات سایبری بر تـوان‌افزایـی امنیت ملی جمهوری اسلامی ایـران از منظـر ژئوپولیتیـک از تحلیـل مضـمون[1] و از میـان

1. Thematic Analysis

روشهای مختلف تحلیل مضمون از روش شبکه مضامین[1] استفاده می‌شود. یکی از روشهای ساده و کارامد 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[2] (۱۹۹۸، ص ۴) آن را نه روشی خاص بلکه ابزاری مناسب برای روش‌های مختلف، معرفی می‌کند. ریان و برنارد[3] (۲۰۰۰) نیز کدگذاری مضامین را فرایند پیش -نیازِ تحلیل‌های اصلی و رایجِ کیفی، معرفی می‌کنند تا روشی منحصربفرد و خاص. اما به عقیده براون و کلارک[4] (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 طورکلی، 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 آترایدِ استیرلینگ[5] (۲۰۰۱) آنرا توسعه داده است. برای دستیابی به شبکه مضامین باید مراحل سه گانه 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

مضـامین فراگیـر (مضـامین عـالی در برگیرنـده اصـول حـاکم بـر مـتن بـه عنـوان یـک کل)(عابدی‌جعفری و همکاران،۱۳۹۵ :۱۷۰-۱۵۹).

لاجرم با توجه به روش تحقیق، می‌توان چنین گفت که تهدیـدات امنیتـی مربـوط بـه تحلیل نقش قدرت سایبری بر توان‌افزایی امنیت ملـی جمهـوری اسـلامی ایـران از منظـر ژئوپولیتیک برای جامعه ایران عبارتند از:

الف) تهدیدات خـارجی: مضـمون فراگیـر تهدیـدات امنیتـی تحلیـل نقـش قـدرت سایبری بر توان افزایی امنیت ملـی جمهـوری اسـلامی ایـران از منظـر ژئوپولیتیـک دارای چهار مضمون سازمان یافته: ۱. تلاش در جهت منزوی نمودن ایـران (شـامل دو مضـمون پایه: تلاش در جهـت ایجـاد واگرایـی در داخـل و تـلاش در جهـت ایجـاد واگرایـی در خارج)، ۲. گسترش تهدیدات سایبری (شامل سه مضمون پایه: ایجـاد تهدیـدات سـایبری برای امنیت ملی، توسعه تهدیدات سایبری در ابعاد فرهنگی و اجتماعی و تشـدید جـرائم سایبری)، ۳. ایجاد جبهه واحد ضد انقـلاب (شـامل دو مضـمون پایـه: تـلاش در جهـت متحد نمودن گروه‌هـای ضـد انقـلاب و گسـترش حمـلات تروریسـتی) و ۴. تهدیـدات توأمان سخت‌افزی و نرم‌افزاری: (تهدیدات نرم افزاری و تهدیدات سخت افـزاری) مـی-باشد.

ب) تهدیدات داخلی: مضمون فراگیر تهدیدات داخلی گسترش اسلام‌گرایی افراطـی در آسیای میانه برای جامعه ایران دارای سه مضـمون سـازمان یافتـه: ۱. تهدیـدات امنیتـی (شامل شش مضـمون پایـه: تهدیـد گروهـای قـومی تجزیـه طلـب، تهدیـدات گروهـای معترض و منتقد داخلی، تضـعیف هویـت دینـی، ضـعف و شـناخت مـدیران و تصـمیم-گیرنـدگان، ضـعف برنامـه‌ریـزی صـحیح و مناسـب و ضـعف پروتکلهـای حفـاظتی) ۲. تهدیدات اجتماعی و فرهنگی (شامل هفت مضـمون پایـه: دگرگـونی سـاختار اجتمـاعی، هویت‌زدایی ملی، انتقال ارزش‌های ضد فرهنگی، حضور گسترده شـبکه‌های اجتمـاعی در جامعه، تغییر هویت فرهنگی جوانان بر اثر گستردگی شبکه‌های اجتماعی، ایجاد تشـکیک در بعد اعتقادی و تشدید شکاف هویتی) و ۳. تهدیدات سیاسی و اقتصادی (شـامل شـش مضمون پایه: درگیر شدن ایران در جنگ فرسایشی در مرزها، بدبینی نسـبت بـه عملکـرد حکومت بواسطه توسعه‌نیافتگی، ویرانی زیرساخت‌ها و دارایی‌های کشور، تحرک گـروه-

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

در ادامه به تحلیل داده‌های حاصل از مصاحبه نیمه ساخت یافته (نیمه استاندارد) با خبرگان حوزهٔ فضای سایبری به منظور ارائه مدل مطلوب راهکارهای مقابله با تهدیدات سایبری در توان افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک پرداخته شده است جامعه آماری این پژوهش شامل ۲۵ نفر از خبرگان دانشگاهی و متخصصان حوزهٔ 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 حوزهٔ 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 حوزه‌های 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 افزایی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک

مضامین فراگیر	مضامین سازمان یافته	مضامین پایه	گزاره‌های خبری
اتخاذ 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 حوزهٔ سایبری اتخاذ نمایند
		حکمرانی و دیپلماسی مناسب سایبری	حکمرانی و دیپلماسی مناسب سایبری از ضروریات و نیازهای مبرم دیپلماسی امنیتی کشور است.
		کاربردی بودن سیاست های اتخاذی در حوزهٔ	ارتقای دیپلماسی سایبری و کاربردی بودن سیاست‌ها در مواجه با سایر ملل

		سایبری	
	توجه جدی به دو مقوله سیاست‌گذاری و سیاست‌شناسی در حوزهٔ دیپلماسی	سیاست‌گذاری مناسب	ایجاد پیوستگی بین تدوین و اجرای سیاستها و تعبیه مکانیزم مناسب برای اجرای سیاستها
		تغییر نگاه سیاستگذاران	تغییر نگاه سیاستگذاران و مدیران و تصمیم‌گیران نظام به بهره‌برداری از این فضا
		اتخاذ سیاست‌گذاری مناسب بر اساس امکانات سخت افزاری و نرم افزاری	فراهم کردن امکانات سخت‌افزاری و نرم‌افزاری مناسب برای ارتقاء توان سایبری از طریق سیاست‌گذاری مناسب
		افزایش توان سیاست شناسی و سیاستمداری	ارتقاء ادراک شناسی سایبری با اتخاذ سیاست شناسی مناسب
افزایش توان و قدرت سایبری	ارتقای توان پدافندی و آفندی	استفاده از فناوری‌های نوین	به روز شوندگی و استفاده از فناوری‌های نوین
		راه‌اندازی اینترنت ملی و شبکه ملی اطلاعات	راه‌اندازی اینترنت ملی و شبکه ملی اطلاعات
		دستیابی به علوم و فناوری‌های پیشرفته	دستیابی به علوم و فناوری‌های پیشرفته
		ارتقاء توان پدافندی	ارتقاء توان پدافندی (تربیت و آموزش نیروهای مستعد و نخبه)
		ارتقای توان آفندی	ارعاب و ترساندن دشمن با ارتقاء توان آفندی و مقابله سایبری در برابر حملات
		به روز رسانی سخت افزاری و نرم‌افزاری	ارتقاء توان آفندی و پدافندی جمهوری اسلامی ایران با نوشوندگی و به روز رسانی سخت‌افزاری و نرم‌افزاری
		بهره‌برداری از توان داخلی	بهره‌برداری از توان داخلی در تولید تجهیزات سخت افزاری و نرم افزاری
	ایجاد جبهه واحد علیه سرویس های جاسوسی و ایادی ضد انقلاب وابسته به آنها در قالب محور مقاومت سایبری	استفاده از ظرفیت کشورهای مقاومت اسلامی	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 گروه‌های 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 گروه‌های آزادی خواه و ضد سلطه‌ی 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 و مصون‌سازی	تقویت زیرساخت- های سایبری	کاهش آسیب‌پذیری، پایدارسازی، مصون‌سازی، ارتقاء توان بازدارندگی زیرساختهای حیـاتی و حساس کشور در برابر تهدیدات و حملات سایبری
	اشراف اطلاعاتی		رصد، پایش، مراقبت، تشخیص و هشدار هوشمندانه و دستیابی به اشراف اطلاعاتی در برابـر تهدیدات فضای سایبری از طریق سازماندهی مراکز رصد و پدافند سایبری با رویکرد شـناخت پیش دستانه تهدید
	مدیریت و کنترل حملات سایبری		مدیریت و کنترل پیامدهای تهدیدات و حملات سایبری
	تقویت دستگاه‌های ناظر		تقویت ساختار دستگاه‌های ناظر بر فضای سایبر و تبادل اطلاعات.
	اتخاذ رویکرد تعاملی در حوزهٔ امنیت سایبری		رویکرد تعامل محور و همپوشانی نقش دستگاه‌های مختلف متولی امنیت در فضای سایبر و ایجاد وحدت رویه در حوزهٔ امنیت سایبری
	تأسیس ساختاری قدرتمند و فراقوه‌ای برای سیاست‌گذاری فضای مجازی		تأسیس ساختاری قدرتمند و فراقوه‌ای برای سیاست‌گذاری فضای مجازی کشور و ساماندهی و ایجاد هماهنگی بخشی
	ایجاد سیستم امنیتی سایبری		ایجاد سیستم امنیتی برای ایمن‌سازی زیرساختهای ارتباطی کشور و کنترل و نظارت دائم بر محتوای داده‌های مبادله شده در فضای سایبر برای پیشگیری از گسترش فساد، تهدیدات امنیتی، نفوذ سرویس‌های جاسوسی، خرابکاری الکترونیک و توسعه ظرفیت بازدارندگی در برابر تهدیدات نوین
	توسعه توانمندیهای زیرساختی سایبری		توسعه توانمندیهای زیرساختی کشور متناسب با سیاستهای فضای سایبر
	دشمن شناسی		شناخت درست از توان رقباء و دشمنان نظام در عرصه رقابت یا جنگ سایبری
	مقابله به مثل در برابر حملات سایبری		مقابله به مثل در برابر حملات سایبری
	رعایت همه‌جانبه اصول حفاظتی		ارتقاء پروتکل‌ها و رعایت همه جانبه اصول حفاظتی
اتخاذ سیاست گذاری فرهنگی،	ایجاد قوانین مناسب	اتخاذ سیاست گذاری قضایی	ایجاد قوانین مناسب توسط قوه قضائیه در برخورد با مجرمین سایبری
	به روزرسانی قوانین		به روز رسانی قوانین سایبری توسط

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

		متخصص و توانمند	توانمند
	توجه به سیاست گذاری فرهنگی	سرمایه‌گذاری در حوزهٔ فرهنگ سازی و تربیت و آموزش ملی	سرمایه گذاری در حوزهٔ فرهنگ‌سازی 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	فرهنگ‌سازی در جهت آگاهی مردم از تهدیدات
		توجه به آموزش همگانی	توجه به آموزش همگانی
		فرهنگ‌سازی از طریق رسانه‌ها	استفاده از رسانه‌های جمعی در راستای فرهنگ‌سازی
		بهره‌گیری از مراکز فرهنگی و آموزشی نظیر دانشگاها	بهره‌گیری از مراکز فرهنگی و آموزشی نظیر دانشگاه‌ها
طراحی و پیاده‌سازی پدافند سایبری بومی	توجه به دانش و مهارت‌های بومی در حوزهٔ سایبری	طراحی، پیاده‌سازی الگوهای سایبری بومی	طراحی، پیاده‌سازی و اجرای نظریه‌ها و الگوهای پدافند سایبری بومی، دانش محور و پاسخگو به تهدید
		طراحی، پیاده‌سازی الگوهای سایبری بومی در مقابل تهدیدات	طراحی، پیاده‌سازی و اجرای نظام پدافند سایبری درمقابل تهدیدات و حملات سایبری با ویژگی بومی‌سازی فرایندها، نظامات و استانداردها، پروتکلها، رویه‌ها و روال‌ها
		طراحی، پیاده‌سازی و اجرای مراکز رصد	طراحی، پیاده‌سازی و اجرای مراکز رصد، پایش و کنترل زیرساختهای حیاتی به صورت بومی
		نهادینه‌سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیر عامل و پدافند سایبری	نهادینه‌سازی اصول، راهبردها، ملاحظات و الزامات پدافند غیرعامل و پدافند سایبری در طرح های توسعه ملی و استانی پدافند سایبری کشور
		بومی و ایمنی‌سازی تجهیزات	بومی و ایمن‌سازی تجهیزات مورد استفاده در زیرساخت‌های حیاتی و حساس کشور در جهت کاهش وابستگی به فناوری‌ها و محصولات غیربومی و ممنوعیت کاربرد سامانه‌های خارجی در آنها
		تقویت صنعت پدافند سایبری بومی	تقویت صنعت پدافند سایبری بومی و حمایت از سازمان‌ها و شرکتهای تولیدکننده سامانه‌ها و محصولات بومی
		ایجاد زیست بوم سایبری	الزام و همراه‌سازی سازمان‌های متولی زیرساخت‌های حیاتی و حساس کشور در ایجاد زیست بوم سایبری و

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

جدول ۳) تعداد مضامین فراگیر، سازمان یافته و پایه‌ای راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایی 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 حوزهٔ سایبری	۳	۲۱
۴	طراحی و پیاده‌سازی پدافند سایبری بومی	۲	۱۱
۵	تقویت سازمانهای مردم نهاد و NGO	۲	۸
	جمع کل	۱۲	۶۸

همان گونه که جدول ۳ نیز نشان می‌دهد راهکارهای مقابله با تهدیدات فضای سایبری در توان افزایی 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 حوزهٔ 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 توان‌افزایی 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 تـوان‌افزایـی امنیت ملی جمهوری اسلامی ایران از منظر ژئوپولیتیک براساس مضامین فراگیر و سازمان یافته

بنابراین با توجه به جدول ۳ و نیز نمـودار ۲ مـی‌تـوان چنـین گفـت کـه راهکارهـای مقابله با تهدیدات فضای سایبری در توان‌افزایی امنیـت ملـی جمهـوری اسـلامی ایـران از منظر ژئوپولیتیک عبارتند از:

۱) **اتخاذ دیپلماسی سـایبری**: مضـمون فراگیـر اتخـاذ دیپلماسـی سـایبری دارای دو مضمون سازمان یافته: الف) توجه به دیپلماسی سایبری و ب) توجه جـدی بـه دو مقولـه سیاست‌گذاری و سیاست‌شناسی تشکیل شده است.

۲) **افزایش توان و قدرت سایبری**: مضمون فراگیری افزایش توان و قـدرت سـایبری دارای سه مضمون سازمان یافته: الف) ارتقای توان پدافندی و آفنـدی و ب) ایجـاد جبهـه واحد علیه سرویسهای جاسوسی و ایادی ضد انقلاب وابسته به آنها در قالب محـور مقاومـت سایبری و ج) تقویت زیرساخت‌های سایبری تشکیل شده است.

۳) اتخاذ سیاست‌گذاری فرهنگی، قضایی و آموزشی- تربیتی مناسب در حوزهٔ سایبری: مضمون فراگیر اتخاذ سیاست‌گذاری فرهنگی، قضایی و آموزشی- تربیتی مناسب در حوزهٔ سایبری دارای سه مضمون سازمان یافته: الف) توجه به سیاست‌گذاری فرهنگی، ب) سیاست‌گذاری در حوزهٔ 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 حوزهٔ سایبری تشکیل شده است.

۵) تقویت سازمان‌های مردم نهاد و NGO ها: مضمون فراگیر تقویت سازمان‌های مردم نهاد و NGOها دارای دو مضمون سازمان یافته: الف) توجه به سازمانهای مردم نهاد و ب) بهره‌مندی از ظرفیت نهادی 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 حوزهٔ 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 به‌دلیل 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 حوزهٔ قضایی معین در آن حوزهٔ 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 حوزهٔ ارتقاء بخشد. 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

خلیلی‌پور 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 جمهوربی اسلامی ایران»، **فصلنامه علمی امنیت ملی**، سال دهم، شماره ۳۸، صص ۳۳۱-۲۹۳.

عابدی‌جعفری، 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 واجرای 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

کربلایی تاج‌الدین، محمد و محمدنژاد، حسن و سلیمی، سعید (۱۳۹۵)، **فضای مجازی و شبکه های 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 دکترین 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 تأکیدها 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 بین المللی پلیس**، دوره چهارم، شماره ۱۴، صص ۱۰۱-۱۱۷

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

ولی‌زاده‌میدانی، رامین (۱۳۹۹)، **درآمدی بر تروریسم سایبری و ویژگی های 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 Intelligeence. (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 Qrganisation 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.