جمهوری اسلامی ایران
مجلس شورای اسلامی
مرکز تحقیقات اسلامی

الگوی مفهومی استراتژی امنیت ملی سایبری جمهوری اسلامی ایران مبتنی بر جهاد تبیین

مرکز تحقیقات اسلامی
گروه فرهنگی و اجتماعی

مرکز تحقیقات اسلامی مجلس شورای اسلامی
گروه فرهنگی و اجتماعی

عنوان گزارش:

الگوی مفهومی استراتژی امنیت ملی سایبری جمهوری اسلامی ایران مبتنی بر جهاد تبیین

شماره ثبت در مرکز:

۶۲۵-۰۶/-/۰۳

تاریخ انتشار:

تابستان ۱۴۰۲

نویسنده:

محمدمهدی محققی

ارزیاب:

دکتر کمال اکبری

کارشناس مرکز:

دکتر جواد ابراهیمی

فهرست

خلاصه مدیریتی

توسعه فضای مجازی و ماهیت پیچیده، رقابتی، مرززُدا، هویت‌زدا و عدم قطعیت آن باعث شده کشورهای پیشرو برای تقویت حکمرانی، تحقق مقاصد و تأمین منافع ملی خود مکانیسم‌هایی از طریق تدوین «استراتژی امنیت ملی سایبری» طراحی و اجرا کنند. جمهوری اسلامی ایران با وجود اسناد بالادستی فراوان در خصوص فضای سایبر، هنوز موفق به تهیه سند استراتژی امنیت ملی سایبری نشده است. در ادامه ضمن آشنایی با ویژگی‌ها و الزامات این استراتژی، با تکیه بر مفهوم «جهاد تبیین»، الگوی مفهومی را برای تحقق این مهم صورت‌بندی می‌کنیم. این تحقیق، مفهوم «جهاد تبیین» را به‌عنوان استعاره مولّد و دارای قدرت آفرینش الگوی نوینی در سیاست‌گذاری فضای سایبر و جایگزین کردن آن با الگوهای پیشین انتخاب کرده است. الگوی مفهومی استراتژی امنیت سایبری جمهوری اسلامی ایران براساس تحقیق حاضر از چهار مضمون پایه، ۱۷ مضمون سازمان‌دهنده و ۴۱ مضمون فراگیر تشکیل شده است. مضامین چهارگانه اصلی که منتهی به توصیه‌های سیاستی در این خصوص می‌شوند، شامل عناصر سیاست‌گذاری، بازیگران، گفتمان و ژئوپلیتیک سایبری هستند. در پایان توصیه‌هایی در چهار حوزه سیاست‌گذاری، کنشگران، گفتمان و ژئوپلیتیک سایبری مدنظر قرار گرفته است. این توصیه‌ها در تمامی یا چند لایه از سطوح حکمرانی از سیاست‌گذاری، قانون‌گذاری، تنظیم‌گری، تسهیل‌گری، اجرا و نظارت قابل پیگیری و تصویب‌خواهی است.

در آغاز تذکر این نکته حائز اهمیت است که روند تدوین و اجرای سند استراتژی امنیت سایبری فرایندی تدریجی، پیوسته و پویاست، ساختارهای جاری در این روند هیچ‌گاه متوقف نمی‌شوند، بلکه با تکیه بر اقدامات راهبردی، فرایندها و اقدامات جاری خود را تسریع، بهبود یا از طریق مهندسی مجدد، اصلاح و تکمیل می‌کنند.

مقدمه

ساختار حاکم بر فضای مجازی، غیرمتمرکز، چندلایه، غیرسرزمینی، نهادگریز و هویت‌زداست. این ویژگی‌ها باعث دشواری و پیچیدگی حکمرانی بر این فضا شده است. چالش‌های نوین فضای مجازی سیاست‌گذاران کشورهای جهان را به تکاپو وا داشته تا در کشور خود الگویی برای راهبری فضای مجازی تدوین و اجرا کنند که تأمین‌کننده بیشترین منافع ملی آنها باشد. از طرفی، تحولات فناوری، دخالت‌های آمریکا و تعدد بازیگران غیردولتی، کنشگری دولت‌ها را در کنترل و اداره فضای مجازی تضعیف کرده است. جمهوری اسلامی ایران برای ارتقای خود به قدرت سایبری در طراز قدرت‌های جهانی تلاش دارد حکمرانی خود را در این فضا شکل دهد و با رویکردی همه‌جانبه، اخلاق‌مدار و عادلانه به ساخت تمدن نوین اسلامی، جامعه‌پردازی، تأمین منافع ملی، امنیت فراگیر، سالم‌سازی و مقابله با نفوذ بیگانه در این فضا بپردازد. ازاین‌رو نیازمند طراحی استراتژِی امنیت ملی سایبری خود براساس مبانی و اهداف نظام مقدس اسلامی هستیم.

۱. سؤالات تحقیق

سؤال اصلی تحقیق: استراتژی امنیت ملی سایبری جمهوری اسلامی ایران چیست؟

در همین ارتباط، سؤال‌های فرعی زیر مدنظر نویسنده مقاله بوده و تلاش شده به آنها پاسخ داده شود:

حکمرانی فضای مجازی جمهوری اسلامی ایران چیست؟

استعاره جهاد تبیین چه نقشی در تدوین الگوی حکمرانی فضای مجازی جمهوری اسلامی ایران دارد؟

الزامات سیاستی و تقنینی استراتژی امنیت ملی سایبری جمهوری اسلامی ایران مبتنی بر جهاد تبیین چیست؟

۲. شیوه تحقیق

با توجه به نوپیدا بودن مفهوم استراتژی امنیت ملی سایبری و کمبود منابع داخلی، برای رسیدن به راهبردهای اساسی جمهوری اسلامی ایران در حکمرانی فضای مجازی روش تحلیل مضمون انتخاب شده؛ زیرا این روش بهترین شیوه شناسایی، تحلیل و گزارش الگوهای موجود در داده‌های علمی نوین است تا داده‌های متنوع و پراکنده را به‌صورت دسته‌بندی‌شده و تفصیلی تبدیل کند (شیخ‌زاده و بنی‌اسد، ۱۳۹۹: ۲۴)؛ گرچه این روش با نقطه ضعف عدم نگاه به بیرون از متون، در نظر نگرفتن شرایط تکوین متون، عدم شناسایی تمام آنچه متن را متن کرده و لحاظ نکردن پیش‌فرض‌ها و مبانی نظری و گفتمانی روبه‌روست. داده‌های اولیه در خصوص مفهوم استراتژی امنیت ملی سایبری شامل مقاله‌های نشریات علمی و کنفرانس‌ها، هندبوک‌ها، کتاب‌ها و چکیده‌های منابع علمی معتبر منتشرشده به زبان انگلیسی در پایگاه نمایه‌های استنادی اسکوپوس[1] با کلیدواژه «استراتژی امنیت ملی سایبری»[2] و «حکمرانی فضای مجازی»[3] در دوره زمانی اسفند ۱۴۰۰ است. ملاک انتخاب متون، هرگونه پژوهش در موضوع سیاست‌گذاری فضای مجازی و مفاهیم مرتبط با استراتژی امنیت ملی سایبری با ادبیات علمی بود که سرانجام، ۲۴ مقاله و ۲۲ چکیده مقاله (فاقد متن کامل) در موضوع این تحقیق انتخاب و به فارسی ترجمه شد تا وارد فرایند تحلیل مضمون شوند. همچنین برای بومی‌سازی مفاهیم، از استعاره جهاد تبیین استفاده شده است. استعاره‌ها به‌خاطر ویژگی سازنده معانی، امکان درک و توصیف مفاهیم نوین را فراهم می‌کنند. استعاره جهاد تبیین نقش ساختار زیربنایی طرح‌ریزی و نیز تجویز خط‌مشی‌های استراتژی امنیت سایبری جمهوری اسلامی ایران را ایفا می‌کند.

1. https://www.scopus.com/
2. National cyber security strategy
3. cyber governance

۳. مبانی و چارچوب مفهومی

۳/۱. استراتژی امنیت ملی سایبری

اصلی‌ترین اصطلاح محوری این تحقیق مفهوم «استراتژی امنیت ملی سایبری» است. در دهه‌های گذشته، مفهوم امنیت براساس روابط قدرت و حفظ تمامیت سرزمینی کشورها تعریف می‌شد و تنها معنای نظامی داشت. تضمین امنیت در گرو تجهیزات و نیروی نظامی بود و تهدید نظامی مهم‌ترین تهدید امنیتی هر کشور تلقی می‌شد. اما امروزه امنیت از چندین ارزش ملی پویا مانند بقای سیاسی، انسجام اجتماعی، رفاه عمومی، شکوفایی اقتصادی و تولید دانش تشکیل شده است. مفهوم امنیت از ابعاد فردی و ملی تشکیل شده است. بُعد فردی شامل حریم خصوصی و امنیت فردی در جامعه است. برخی از تهدیدهای امنیتی در چارچوب و اندازه واحدهای ملی تعریف می‌شوند، مانند تجزیه‌طلبی، افراطی‌گری، وابستگی به بیگانه و ضعف ساختارها و نهادهای عمومی. کشورها برای مقابله با تهدیدها و تأمین امنیت خود اقدام به تدوین استراتژی‌های ملی می‌کنند. این استراتژی‌ها متناسب با نوع، شکل و ظرفیت عوامل تهدیدزا به‌صورت بلندمدت تهیه می‌شوند تا تهدیدها را به فرصت تبدیل کند. از مهم‌ترین الزامات تأمین امنیت ملی کسب قدرت در ابعاد اقتصادی، سیاسی، فرهنگی و فناوری است. بسیاری از کشورها برای تأمین امنیت ملی از عوامل بازدارنده و ایده‌هایی نظیر قدرت نرم، حمله پیش‌دستانه و دفاع پیشگیرانه استفاده می‌کنند. شرایط جهان امروز امنیت را از واحدهای ملی به سطوح منطقه‌ای و جهانی نیز تسری داده است (کاظمی، ۱۳۸۴: ۱۷ـ۲۴). امنیت ملی اهداف، انگیزه‌ها، مقاصد و مصالح عموم ملت است که تمامی سیاست‌ها و برنامه‌ها براساس آن تدوین می‌شوند. استقلال عمل، ثبات سیاسی، توانمندی اقتصادی، رشد علمی و انسجام اجتماعی آثار و پیامدهای تأمین امنیت ملی یک کشور محسوب و با معیارهایی مانند توان رویارویی با تهدیدها، احساس ایمنی و اعتلای شهروندان هر حاکمیتی شناخته می‌شود. استراتژی امنیت ملی روش‌های حفظ، ارتقا و تأمین منافع ملی و مصالح عمومی است. در سیاست‌گذاری فرهنگی جمهوری اسلامی ایران برای اقامه فرائض و احکام الهی و سایر غایات و اهداف نظام اسلامی در عصر تحولات سریع فناوری‌های ارتباطی نیازمند تدوین سند استراتژی امنیت سایبری در ذیل استراتژی امنیت ملی کشور هستیم؛ زیرا فضای مجازی به خاطر شرایط و ویژگی‌هایی همچون محرمانه بودن داده‌ها، سازماندهی زندگی خصوصی کاربران، سوءاستفاده دشمن، مرززُدایی، عدم برخورداری از قوانین و مکانیسم‌های نظارتی، ناشناخته بودن ارتباطات در این فضا، تغییر شدید ماهیت فاوا[۱]، درهم‌تنیدگی این فضا با پدیده‌های گوناگون مانند اقتصاد ملی، رقابت راهبردی قدرت‌ها، موضوعی فراملی و ذاتاً استراتژیک بوده، به امنیت ملی گره خورده و خصوصاً جمهوری اسلامی ایران به‌خاطر مقاومت در برابر استکبار آمریکا و فشار کشورهای غربی شدیداً نیازمند «استراتژی امنیت ملی سایبری» است.

۱. فناوری اطلاعات و ارتباطات.

۳/۲. حکمرانی فضای مجازی

مفهوم «حکمرانی فضای مجازی» مفهوم محوری مرتبط با استراتژی امنیت ملی سایبری است. «حکمرانی»[1] مجموعه‌ای نظام‌مند از ساختارها و فرایندهای سیاست‌گذای، قاعده‌گذاری، تنظیم‌گری، تسهیل‌گری، اجرا و کنترل را شامل می‌شود که در جهت رسیدن به اهداف مشترک در چارچوب مبانی و ارزش‌های یک حاکمیت سیاسی است. در این مفهوم، حکومت از طریق فرایندهای رسمی، نهادی و سازوکارهای نرم، اراده خود را بر ساختار، بازیگران و شهروندان در راستای تحقق اهداف و منافع عمومی اعمال می‌کند. این تلقی از حکمرانی مربوط به واحدهای سیاسی در جغرافیای درون مرزهای ملی کشورهاست. اما «حکمرانی جهانی»[2] مفهوم نوینی پیرامون فرایند جهانی شدن است که قدرت‌های بین‌المللی با استفاده از ابزارها و وجوه قدرت خود تلاش می‌کنند ائتلاف‌های منطقه‌ای، کشورها، شرکت‌های چندملیتی، بازیگران خصوصی و حتی افکار عمومی ملت‌ها را به سوی اهداف و خواسته‌های خود متمایل کنند و مشارکت کنترل‌شده‌ای پدید آورند. حکمرانی جهانی می‌تواند از طریق الگوی حل چالش‌های جهانی توسط ابرقدرت واحد یا الگوی چندجانبه اعمال شود. از آنجا که تبادل اطلاعات از طریق فضای مجازی از فضای جغرافیایی تحت مدیریت کشورها گذشته است، اهمیت حکمرانی فضای مجازی به‌قدری زیاد شده که در طول دو دهه گذشته، اصطلاح حکمرانی در بسیاری از گفتمان‌ها به مجموع تلاش‌های نظارتی، هدایت توسعه و تکامل آینده فضای مجازی اشاره دارد. ماهیت حکمرانی فضای مجازی با تعداد زیادی از بازیگران، جمعیت بالای کاربران، حوزه‌های موضوعی و مجامع درگیر در روندهای آینده عملکرد قلمرو دیجیتال مشخص می‌شود (Bovens, Goodin, & Schillemans, 2014, p. 52).

همچنین حکمرانی فضای مجازی به‌عنوان نتیجه اقدامات جمعی کشورهای کمترتوسعه‌یافته برای دفاع از منافع ملی خود در برابر کشورهای توسعه‌یافته‌تر تصور می‌شود (Zhang and Ren, 2016, p.14).

۳/۳. استعاره‌های مولد

«استعاره‌ها» نقش مهمی در گفتمان‌های سیاست‌گذاری کشورها ایفا می‌کنند و سیاست‌گذاران درگیر با استراتژی امنیت ملی سایبری از «استعاره‌های مولد» برای توصیف و درک فناوری‌های نوین بهره می‌برند؛ زیرا استعاره‌ها به‌خاطر ویژگی سازنده معانی، امکان درک پدیده‌های پیچیده و توصیف مفاهیم نوین را فراهم و یک ساختار فکری زیربنایی را برای چارچوب‌بندی وضعیت و راه‌حل‌های نوین در حل مشکلات از طریق مفهوم‌سازی مجدد آنها ایجاد می‌کنند (Schön, 2012, p. 19). استعاره‌ها قدرت آفرینش الگوی نوینی از پدیده‌ها و حتی جایگزین کردن آن با الگوهای پیشینی را دارند؛ مثلاً استعاره جنگ سرد، ماهیت رقابت میان دو بلوک شرق و غرب را مفهوم‌سازی می‌کند. استعاره‌های مولد درک ما را از مشکلات خط‌مشی‌گذاری با ارائه الگوهای ذهنی درباره مشکل و راه‌حل‌های ممکن شکل می‌دهند.

1. Governance
2. Global Governance

۳/۴. جهاد تبیین

اصطلاح «جهاد» برخلاف آنچه برخی به‌عنوان قتال و برخورد فیزیکی رو در رو تعریف کرده‌اند، دارای حقیقت شرعیه و متشرعیه متفاوت با معنای لغوی آن است و از مفاهیم مخترعه منظومه‌وار در اسلام به‌شمار می‌رود. مفهوم «جهاد فی سبیل الله» که ده‌ها بار در آیات قرآن به‌کار رفته، تداعی‌کننده مجموعه‌ای از قیود مانند استفاده از ظرفیت‌ها و نقاط قوّت و فرصت‌ها در راه تحقق اهداف شارع و غایات تشریع شرایع تحت رهبری فرستاده الهی است. جهاد در دوران نزول قرآن در مکه به معنی جهاد تبیین است که معنای گسترده‌ای دارد. یکی از اقسام آن جهاد فرهنگی است که آیه «وَمَا كَانَ الْمُؤْمِنُونَ لِيَنْفِرُوا كَافَّةً فَلَوْلَا نَفَرَ مِنْ كُلِّ فِرْقَةٍ مِنْهُمْ طَائِفَةٌ لِيَتَفَقَّهُوا فِي الدِّينِ» (سوره توبه، آیه ۱۲۲) مصداق آن است. بنابراین جهاد در حقیقت شرعیه به ابعاد اقتصادی، فرهنگی و امنیتی نیز تسری می‌یابد. مثلاً از آیه شریفه «انفِرُوا خِفَافًا وَثِقَالًا وَجَاهِدُوا بِأَمْوَالِكُمْ وَأَنفُسِكُمْ فِي سَبِيلِ اللَّهِ ذَلِكُمْ خَيْرٌ لَكُمْ إِنْ كُنتُمْ تَعْلَمُونَ» (همان، آیه ۴۱) مفهوم جهاد اقتصادی استفاده می‌شود. جهاد تبیین، تلاش عقلانی، خستگی‌ناپذیر، همه‌جانبه، منظوم و غایت‌مند برای تحقق اهداف و مقاصد نظام اسلامی است. بر این اساس، مفهوم «جهاد» در استراتژی امنیت ملی سایبری جهاد تبیین، از ابعاد کلیدی هدایت ولیّ شرعی، مقاومت در برابر دشمن، تولید و اعمال قدرت، غلبه بر دشمن، آمادگی دفاعی، سبیل الله، مانع‌زدایی، جریان‌سازی، آرمان‌گرایی واقع‌بینانه، استقلال، تقویت باورهای اعتقادی عموم، تحقق مصالح ملی و جهان اسلام، پیشرفت و تعالی جوامع اسلامی، ساختارسازی درونی، مرجعیت علمی و فکری، دفع فتنه‌های داخلی، تفاهم بین‌الادیانی براساس مفاهیم والایی مانند عدالت و کرامت انسان، تقویت وحدت امت اسلامی، و عقلانیت اسلامی برخوردار است. هریک از این ابعاد کلیدی، مؤلفه‌ها و شاخص‌هایی دارند. مثلاً بُعد «تولید قدرت» دارای مؤلفه‌هایی مانند قدرت سخت، قدرت نرم، (نرم ـ نرم، نرم ـ سخت)، و هوشمند است و اولین گام تولید قدرت، مستلزم پوشاندن آسیب‌ها و عبور از نقاط ضعف و تبدیل ضعف به قدرت است. مؤلفه‌های دیگر بُعد قدرت، عبارتند از: تهدیدزدایی، تبدیل تهدید به فرصت، بازدارندگی و پیشگیری (اعداد بالقوه)، فرصت‌سازی، خودکفایی، تولید هژمونی، ساماندهی، بسیج ظرفیت‌ها و امکانات، تقویت زیرساخت‌ها، ایجاد توازن و....

واژه «تبیین» اشاره به ایستادگی در برابر تحریف، ابهام‌افکنی، شبهه‌پراکنی و تردید در اذهان مخاطبان درباره انقلاب اسلامی و معارف اسلام دارد؛ چه‌اینکه جریان تحریف در داخل با همسویی شبهه‌افکنی‌ها و اقدامات تاکتیکی رسانه‌های دشمن، سعی در جدا کردن اقشار گوناگون خصوصاً جوانان و دانشجویان و نخبگان از نظام مقدس اسلامی دارد. جهاد تبیین در اندیشه رهبر معظّم انقلاب یک فریضه قطعی و فوری و عینی است.

۴. یافته‌های تحقیق

۴/۱. نقش استعاره‌های مولد در سیاست‌گذاری سایبری

در این تحقیق به چهار استعاره کلان درباره حکمرانی سایبری یعنی جنگ، سلامت، زیست‌بوم و زیرساخت تحلیل اشاره می‌شود (Wolff, 2014, p. 2). شایع‌ترین استعاره برای درک حکمرانی فضای مجازی، «جنگ سایبری» است. این استعاره درگیری و منازعه سایبری بین کشورها را به‌عنوان یک نبرد مفهوم‌سازی می‌کند. چه‌اینکه بحث در مورد وجود یک جنگ سایبری بین‌المللی در گفتمان سیاست‌مداران ارشد کشورها رواج دارد. برای مثال حمله باج‌افزار WannaCry را در نظر بگیرید که بیش از دویست هزار رایانه را در یکصدوپنجاه کشور تحت تأثیر قرار داد و خسارت‌های آن میلیاردها دلار برآورد شد (Berr, 2017).

استعاره دوم «سلامت سایبری» است که توسط برخی از سازمان‌های بین‌المللی مانند سازمان بهداشت جهانی[1] مطرح شده است. این استعاره به سیاست‌مداران کشورها کمک می‌کند تا ذی‌نفعان ملی را برای پیروی از یک مکانیسم حکمرانی متقاعد کنند و انگیزه دهند تا محیط سایبری خود را آلوده نکنند (Veksler et al., 2018, p. 12).

سومین استعاره «زیست‌بوم سایبری» است که بیشتر توسط متخصصانی به‌کار می‌رود که معتقدند جهان سایبر بخشی از زندگی جهان واقعی است که انسان‌ها در آن زندگی می‌کنند. آنان بر این باورند که فناوری اطلاعات و ارتباطات در حال ایجاد محیط اطلاعاتی نوینی است که نسل‌های آینده بیشتر زمان خود را در آن زندگی خواهند کرد. استعاره بوم‌شناختی وابستگی متقابل موجودات گوناگون و محیط اطلاعاتی آنها را منعکس و بر مسئولیت مشترک کشورها برای پیشگیری و ایجاد یک اکوسیستم جهانی سالم در فضای مجازی تأکید می‌کند؛ زیرا همه کشورها از یک زیست‌بوم جهانی سالم سایبری سود می‌برند (Fairclough, 2018). در چهارمین استعاره، فضای سایبری به‌عنوان یک «زیرساخت جهانی» مورد توجه قرار می‌گیرد. در این استعاره، امنیت سایبری به‌عنوان یک کالای عمومی جهانی فرض می‌شود که باید در برابر مداخله بی‌دلیل کشورها محافظت شود. سیاست‌مدارانی که از این استعاره برای درک حکمرانی فضای مجازی استفاده می‌کنند بر این باورند که اگر همهٔ انسان‌ها در ساختمانی با پایه‌های مشترک (یعنی اینترنت و فضای سایبر) زندگی می‌کردند، حمله به پایه‌های این ساختمان برای منافع شخصی غیراخلاقی بود و دولت‌ها از آن ممانعت می‌کردند (Smith, 2018).

بر این اساس، نظریه‌پردازان و سیاست‌گذاران هنگام تدوین استراتژی امنیت سایبری کشور خود باید چارچوب استعاری خود را انتخاب و براساس آن، سیاست‌های خاصی را تجویز کنند. سیاست‌گذاران و استراتژیست‌های امنیت سایبری ملی در یک جنگ سایبری باید از جمعیت خود محافظت و از حمله به اهداف زیرساخت ملی کشورهای دیگر اجتناب و مجرمان سایبری را مجازات کنند. در مقابل، سیاست‌گذاران در یک زیست‌بوم مشترک سایبری باید متعهد به کاهش خطرات سیستمی باشند که محیط مشترک فضای سایبر را تهدید می‌کند. حکمرانان

1. WHO

هنگام تدوین استراتژی امنیت سایبری براساس بهداشت عمومی، بر از بین بردن انگیزه‌های آلوده‌سازی فضای مجازی متمرکز می‌شوند و در استعاره زیرساخت به محافظت از زیرساخت‌های حیاتی سایبری اهتمام می‌ورزند.

۴/۲. دلالت‌های استعاره جهاد تبیین در سیاست‌گذاری سایبری

استعاره «جهاد تبیین» به‌عنوان یکی از مفاهیم اسلامی، نقش مهمی در استراتژی امنیت ملی جمهوری اسلامی ایران دارد. جهاد تبیین به معنای تبیین و توضیح اهداف، اصول و ارزش‌های انقلاب اسلامی و دفاع از آنها در برابر تهدیدهای خارجی و داخلی است. این مفهوم به منظور تقویت هویت اسلامی، افزایش انگیزه و تعهد مردم به اصول و ارزش‌های انقلاب، ترویج اصول انقلاب اسلامی در جامعه و مقابله با تبلیغات ضدانقلاب و تهدیدهای امنیت ملی کشور به کار می‌رود. استعاره جهاد تبیین به‌عنوان یک استراتژی فرهنگی و امنیتی مؤثر، در تقویت امنیت ملی و تحقق آرمان‌های نظام و ارتقای جمهوری اسلامی ایران نقش بسزایی دارد. ازاین‌رو می‌تواند بهترین الگو برای سیاست‌گذاران جمهوری اسلامی ایران در تدوین سند ملی استراتژی امنیت ملی سایبری باشد. براساس این مفهوم کشور ما در وضعیت حمله سایبری و اقدامات مخرب برای تضعیف کارکردهای فضای سایبری ایران با اهداف سیاسی و ضد امنیت ملی از سوی قدرت‌های استکباری جهانی قرار دارد. استعاره جهاد تبیین در سیاست‌گذاری سایبری به مفهوم استفاده از راهبردها، راهکارها و تکنیک‌های جهاد تبیین در فضای سایبری است.

استراتژی امنیت سایبری ملی مبتنی بر منطق مفهومی جهاد تبیین فرایند پیچیده و حساسی است که با توجه به تنوع کارکردها، بازیگران و کنشگری آنان، باید هماهنگی‌ها و همکاری‌های فرابخشی صورت گیرد تا شاهد تأثیرات مثبت آن در تقویت هویت اسلامی ایرانی و ارتقای امنیت سایبری کشور باشیم. در این خصوص نیازمند طراحی الگویی مفهومی برای تدوین استراتژی امنیت ملی سایبری هستیم که در ادامه تحقیق به آن می‌پردازیم.

۴/۳. الگوی مفهومی استراتژی امنیت ملی سایبری جمهوری اسلامی ایران

برای تفسیر ابعاد مسئله تحقیق براساس الگوهای معنایی تولیدشده و رسیدن به الگوی استراتژی امنیت ملی سایبری براساس استعاره جهاد تبیین، پس از مرتب کردن و حذف منابع غیرمرتبط با موضوع تحقیق، مقاله‌ها و داده‌های موجود ترجمه، شماره‌گذاری و از روش تحلیل مضمون استفاده شد تا تفکر تحلیلی پایه‌گذاران نظری سیاست‌گذاری فضای مجازی الگویابی شود. مفاهیم استنباط شده ابتدا در قالب مضامین سلسله‌مراتبی و خوشه‌ای از مضامین سطوح پایین تا کلان در یک جدول دارای پنج ستون از زیرمقوله تا مقوله اصلی سازماندهی شد. پس از حذف موارد غیرضروری و ادغام موارد مشابه، شبکه مضامین براساس رویه مضمون پایه (نکات کلیدی متون)، مضمون سازمان‌دهنده (ترکیب و تلخیص مضامین پایه) و مضمون فراگیر (دربردارنده اصول و کلیات) نظام‌مند و این مضامین به‌صورت نقشه شبکه تارنما ترسیم شد که به‌وسیله مضامین پایه و سازمان‌دهنده مجزایی در نمودار شماره ۱ پشتیبانی شده‌اند. هریک از این شبکه‌ها دارای مجموعه‌ای از گره‌ها و موجودیت‌های مرتبط به هم از طریق خطوطی هستند که جریان اقدام‌ها، روندها، رویدادها و فرایندهای یک موضوع مستقل را ترسیم می‌کنند

(شیخ‌زاده و بنی‌اسد، ۱۳۹۹: ۱۹۰). براساس این نمودار، «استراتژی امنیت سایبری جمهوری اسلامی ایران» شامل چهار مضمون پایه، ۱۷ مضمون سازمان‌دهنده و ۴۱ مضمون فراگیر است.

نمودار ۱. شبکه مضامین «استراتژی امنیت سایبری جمهوری اسلامی ایران» براساس جهاد تبیین

عناصر	چارچوب استراتژیک	هویت ملی
		حقوق مشروع
		استقلال
		استکبار ستیزی
		نفی سکولاریسم
		نفی ایران ستیزی
		اخلاق‌گرایی
		غلبه گفتمانی
	مبانی نظری	نظریه بازدارندگی جمعی
		نظریه امنیت سایبری داخلی
		نظریه توازن قوا
		نظریه ام القری
	سیاست استراتژیک	تهدیدزدایی
		ظرفیت‌سازی
		مصونیت‌سازی
		نظارت
		جرم‌ستیزی
		حفاظت اطلاعات
		الزام پیامرسان‌ها
		استانداردسازی
		مدیریت بحران
		تولید محتوا
		دفاع بازدارنده
بازیگران	بازیگران تهدید	آمریکا
		رژیم صهیونیستی
		رقبای منطقه‌ای
		ضدانقلاب
	بازیگران آسیب	مجرمان سایبری
		هکرها
		خودی‌های ناراضی
	روندسازان	شرکت‌های دانش‌بنیان
		استارتاپ‌ها

		مردم
	تصمیم‌سازان	بسیج ظرفیت‌ها
		همسویی و ادغام
		ارتقای بازیگر فراملی
	برنامه‌ریزان	کلان
		خرد
	مجریان	ساختارهای قانونی
		نیروی واکنش سریع
گفتمان	هویت‌زا	ارزش‌های اسلامی
		ارزش‌های ملی
		مرزهای اجتماعی
	بیگانه‌ستیز	نفی استکبار
		دوری از باطل
		شیطان‌گریز
	تمدن‌ساز	احیای تمدن اسلامی
		تقویت تمدن شرق
		ائتلاف‌های تمدنی
	تهدیدزدا	ایمن‌سازی
		مصون‌سازی
		الزام
ژئوپلیتیک	مقابله با نقض حاکمیت	تنبیه مجرمان
		حفاظت از حقوق شهروندان
		نظارت بر سرورها
	امنیت سایبری فراملی	رژیم عدم اشاعه
		ائتلاف جهانی
		توسعه هنجارها
		بازدارندگی جمعی
		تقویت حکمرانی متوازن
		دفاع مشروع
	تضعیف حکمرانی واحد	تضعیف حکمرانی ذی‌نفعان
		تقویت جایگزین‌های نظم آیکان
		تقویت حکمرانی چندجانبه
	شبکه ملی اطلاعات	توسعه زیرساخت
		افزایش کاربران شبکه‌های داخلی
		افزایش خدمات دیجیتال

۴/۳/۱. عناصر

اولین مضمون فراگیر سند استراتژی امنیت سایبری کشور «عناصر» استراتژی است که مضامین سازمان‌دهنده «چارچوب استراتژیک»، «مبانی نظری» و «سیاست استراتژیک» آن را می‌سازند. طراحی استراتژی امنیت سایبری متوقف بر عناصر حیاتی و ارکان حیاتی پیچیده‌ای است که بی‌توجهی به این عناصر در فرایند سندنویسی و اجرا، منجر به ضعف یا نابودی استراتژی می‌شود.

مضمون سازمان‌دهنده «چارچوب استراتژیک» اصول و مبادی خاص هر نظام سیاسی است که آن را از سایر نظام‌های مشابه متمایز و متفاوت می‌کند. چارچوب استراتژیک سند امنیت سایبری جمهوری اسلامی ایران در این تحلیل مضمون، از مضامین پایه هویت ملی، حقوق مشروع، استقلال، استکبارستیزی، نفی سکولاریسم، نفی ایران‌ستیزی و اخلاق‌گرایی تشکیل شده است.

۴/۳/۱/۱. هویت ملی

استفاده از فضای مجازی علاوه‌بر تضعیف ویژگی‌های هویت فردی مانند اعتماد به نفس و خودپنداره، باعث تضعیف انسجام اجتماعی و هویت جمعی کاربران نیز می‌شود، تا آنجا که گاه آنان را دچار آنومی ارزشی و سرگشتگی می‌کند (فیروزآبادی، ۱۳۹۶: ۳۵). هویت ملی در عصر فضای مجازی به‌خاطر مرززدایی، بیشتر فرسوده شده و در معرض تهدید قرار گرفته است. ازاین‌رو ترویج ارزش‌های ملی و مداخله فعال دولت در فضای مجازی برای تقویت و ارتقای فرهنگ عمومی از راه‌های متداول برای تأمین هویت ملی است (Guven, 2021, p. 27).

۴/۳/۱/۲. حقوق مشروع

براساس عرف، قانون اساسی، قوانین و مقررات حاکم در هر کشوری، شهروندان آن کشور دارای حقوق و امتیازاتی هستند که به آنها حقوق مشروع گفته می‌شود. مبنای حقوق در جمهوری اسلامی ایران، شارع مقدس است؛ زیرا ارزش‌ها و حق‌ها دارای نوعی واقعیت نفس‌الامری هستند. اعتبار همه حقوق، ناشی از جعل و وضع و «اراده تشریعی» خداوند است (مصباح یزدی، ۱۳۹۶: ج۱، ص۹۵). بر این اساس حقوق مشروع شهروندان کشور ما در قانون اساسی و سایر قوانین منعکس شده است؛ حقوقی مانند حریم خصوصی، آزادی بیان، دسترسی آزاد به اطلاعات، کرامت، رشد و اعتلا، برخورداری از امکانات و... بر این اساس هرگونه دخالت و نقض این حقوق از سوی ساختارهای رسمی باید مبتنی بر قانون و اجازه دادستان به‌عنوان مدعی‌العموم و با هدف تأمین منافع عمومی یا حقوق حاکمیتی باشد. برخی از دولت‌های ملی سیاست‌های حفظ حریم خصوصی اتخاذشده توسط شرکت‌های فراملی مانند گوگل، فیسبوک و توییتر را تهدیدی برای حاکمیت سایبری و در نتیجه امنیت ملی خود می‌دانند (Nocetti, 2015, p. 114).

۴/۳/۱/۳. استقلال

ایالات متحده با استقلال رأی و نقش فزاینده دولت‌ها در اداره فضای مجازی مخالف است. در عین حال، واشنگتن نزدیک به دو دهه اختیار خود را بر فضای مجازی و اینترنت از طریق شرکت آیکان و قرارداد IANA حفظ کرده است. کشورهایی که دارای قدرت ضعیف در برابر قدرت آمریکا در فضای مجازی هستند، تمام تلاش خود را می‌کنند تا توسعه فاوا و استقلال رأی خود را در ابعاد داخلی و جهانی تحت اصل برابری کشورها تأمین کنند. مطابق الگوی حکمرانی جهانی فضای مجازی این کشورها (حکمرانی چندجانبه یا چندذی‌ربطی)[1] حاکمیت‌ها نه‌تنها هنجارهای فضای مجازی را تولید و استانداردهای خود را تعیین می‌کنند، بلکه آن را راهبری کرده، پیامدها یا مجازات‌های احتمالی را برای عدم انطباق نیز تعریف می‌کنند. در مقابل این الگو، آمریکا با اداره مستقل فضای مجازی توسط سران کشورها مخالف است (Liaropoulos, 2017, p. 31). ایران و بسیاری از کشورهای دیگر احساس می‌کنند که عملاً نقشی در حکمرانی جهانی فضای مجازی و خصوصاً در آیکان ندارند، اما تحت تأثیر تصمیم‌گیری‌های ایالات متحده و آیکان قرار دارند و این، مخالف استقلال و حاکمیت ملی کشورهاست (باقرپور شیرازی، ۱۳۹۸: ۳۸). بنابراین تلاش دولتمردان و دستگاه دیپلماسی کشور باید معطوف به خروج اداره و حکمرانی جهانی فضای مجازی از انحصارگرایی آمریکایی در راستای تأمین منافع ملی باشد.

۴/۳/۱/۴. استکبارستیزی

پس از جنگ سرد، رقابت بلوک غرب و شرق برای راهبری فضای مجازی از طریق توسعه هنجارها و حکمرانی جهانی بر فضای مجازی نشان‌دهنده ادامه سیاست خارجی و استراتژیک اعمال‌شده قدرت‌های جهانی در حوزه سایبری است. هر اردوگاه از مجموعه‌ای از ترجیحات هنجاری دفاع می‌کند که ذاتاً با دیگری در تضاد است، که منجر به رقابت فزاینده برای تسلط در تجویز و ترویج هنجارهای فضای مجازی شده است. سیاست‌گذاران ایالات متحده راهبرد ثبات هژمونی و رهبری جهانی آمریکا را در پیش گرفتند و از فضای مجازی به‌عنوان بستری برای گسترش محصولات و آرمان‌های سیاسی آمریکایی سوءاستفاده می‌کنند. ثبات هژمونیک دقیقاً به این دلیل نظریه‌پردازی شد که سیاست‌گذاران ایالات متحده همچنان به این فکر می‌کنند که رهبری آمریکا برای امنیت جهانی ضروری است. سیاست‌مداران آمریکایی به‌خاطر خوی استکباری و امپریالیستی خود، تاکتیک‌هایی را به‌کار می‌گیرند که از اعمال فشار گرفته تا تأمین انگیزه‌های مادی، و انتشار گفتمانی هنجارها و ارزش‌های هژمون آمریکایی را در بر می‌گیرد. آنان از قدرت نرم استفاده می‌کنند تا دولت‌های دیگر را به مشارکت در فرایندی هدایت کنند که طی آن دولت‌ها درباره اهداف سیاست مشترک خود با آمریکا مذاکره و دوباره مذاکره می‌کنند و باج می‌دهند. سیاست‌گذاران ایالات متحده از طریق ارزش‌های لیبرالیسم، نظم نوین جهانی را دنبال می‌کنند که شامل محدودیت‌هایی بر حاکمیت‌های ملی کشورهای دیگر است. این محدودیت‌ها از طریق نهادها و رژیم‌های بین‌المللی به کشورهای دیگر تحمیل می‌شود (Kiggins, 2014, p. 172). نفی

1. multi-stakeholder governance

سلطه بیگانه و مقابله با سیطره کامل آمریکا بر حکمرانی جهانی فضای مجازی یکی از اصول سند استراتژی سایبری جمهوری اسلامی ایران است.

۴/۳/۱/۵. نفی سکولاریسم

آمریکا یک هژمونی جمعی متشکل از بلوک غرب را راهبری می‌کند که هنجارها و ارزش‌های خود را در ابعاد سیاسی، اقتصادی و فرهنگی در فضای مجازی به دیگر کشورها تحمیل می‌کند. یکی از مهم‌ترین اصول هنجاری و ارزشی تمدن غرب، ترویج و نهادینه‌سازی ارزش‌های سکولاریسم است. جریان سکولاریسم از طریق سیطره علم بر همه شئون بشر از جمله دین، سعی دارد دین را تحت مرجعیت عقل عرفی و ابزاری قرار دهد و آن را به پایین‌ترین سطح معرفتی بشر معاصر تنزل دهد. دین‌زدایی علم باعث می‌شود گزاره‌های ارزشی و متافیزیکی در نزد عقل ابزاری بشر مهمل به‌نظر آید و کنار گذاشته شود (پارسانیا، ۱۳۹۸: ۲۲). نگاه سکولار به جهان و انسان در تمدن غربی غلبه یافت و از سازمان‌ها و نهادهای اجتماعی تا اعلامیه جهانی حقوق بشر را فرا گرفت. این نگاه اینک با هژمونی مسلط آمریکا در فضای مجازی داعیه جهانی دارد و الزامات خود را به فرهنگ‌های بومی و کشورهای دیگر تحمیل می‌کند.

۴/۳/۱/۶. نفی ایران‌ستیزی

ایران به‌علت موقعیت استراتژیک، پیشرفت‌های علمی، منابع، نوگرایی، جمعیت جوان تحصیل‌کرده، نیروی نظامی قوی و پویایی اقتصادی با شعارها و سیاست‌های استکبارستیزانه خود رقیبی سرسخت برای ایالات متحده به‌شمار می‌رود. سوءظن سیاست‌مداران آمریکایی به جمهوری اسلامی ایران باعث شده دستگاه تبلیغی آمریکا سیاست ایران‌هراسی را در پیش گیرد. امید استراتژیست‌های آمریکایی به پیروزی جنبش به اصطلاح اصلاح‌گرایی با تغییرات اجتماعی گسترده است. استراتژی امنیت ملی آمریکا در قرن ۲۱ به سقوط حکومت مذهبی ایران از طریق اقدامات داخلی اصلاح‌طلبان، فشارهای منطقه‌ای و جهانی به جمهوری اسلامی ایران برای دست برداشتن از جمهوریت یا اسلامیت نظام تصریح کرده است (کمیسیون امنیت ملی آمریکا، ۱۳۸۲: ۱۷۲).

۴/۳/۱/۷. اخلاق‌گرایی

یکی از آرمان‌های جمهوری اسلامی ایران اخلاق‌محوری در سطوح گوناگون فردی، اجتماعی و حکمرانی است. رهبر معظّم انقلاب در این خصوص بر این باورند که متأسفانه امروزه با توسعه بی‌ضابطه فضای مجازی، اخلاق و آداب اسلامی کمرنگ شده و اهمیت اخلاق از عمل هم بیشتر است. فضای مجازی جای اخلاق سیئه مانند سوءظن و تهمت‌پراکنی نیست، باید فضای مجازی را جای آداب اخلاقی نیک مانند برادری، مهربانی و حسن ظن قرار دهیم (صلح میرزایی، ۱۴۰۰: ۱۰۲). برخی از الگوهای حاکمیتی غربی برای پیشبرد امور و تحقق اهداف از هر طریقی اقدام می‌کنند؛ هرچند به بهای زیر پا گذاشتن اصول اخلاقی. اما زنده نگه داشتن مبانی اخلاقی

در جامعه از اهداف نظام اسلامی است. بر این اساس ممنوعیت حمله به هسته عمومی و زیرساخت‌های حیاتی کشورهای دیگر یکی از اصول اخلاقی در استراتژی سایبری جمهوری اسلامی ایران به‌شمار می‌رود.

دومین مضمون سازمان‌دهنده عناصر استراتژی امنیت سایبری جمهوری اسلامی ایران را «مبانی نظری» تشکیل می‌دهد. واقع‌گرایی و تحولات سریع فناوری اطلاعات و ارتباطات باعث می‌شود سیاست‌گذاران سایبری از مبانی نظری نظام فاصله بگیرند. به همین منظور برای تنظیم یک استراتژی ژرف، آرمانی، عاقلانه و فراگیر، نیازمند تعریف و تبیین مبانی نظری سند استراتژی سایبری جمهوری اسلامی ایران هستیم. هر نظریه باید بتواند آرمان‌ها، اهداف، رویکردها، تحلیل مسائل، پیامدها و شیوه‌های متناسبی را در حوزه نظری خود توضیح دهد. البته نظریه‌ها لزوماً پیشینی نیستند، بلکه بسیاری از آنها پسینی هستند و اندیشمندان برای تحلیل سیاست‌ها و رفتارهای کشورها و قدرت‌ها سعی می‌کنند آنها را در قالب گزاره‌های نظری فهم کنند. عناصر نظری استراتژی سایبری حمهوری اسلامی ایران شامل مضامین پایه نظریه‌های بازدارندگی جمعی، امنیت سایبری داخلی، توازن قوا و ام‌القری است.

۴/۳/۱/۸. نظریه بازدارندگی

بازدارندگی راهبرد اسلامی با ریشه قرآنی بوده و از آیه شریفه «وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ» (سوره انفال، آیه ۶۰) گرفته شده است. براساس آیه شریفه «فَمَنْ اعْتَدَى عَلَيْكُمْ فَاعْتَدُوا عَلَيْهِ بِمِثْلِ مَا اعْتَدَى عَلَيْكُمْ» (سوره بقره، آیه ۱۹۴) و قواعد فقهی، استراتژی سایبری جمهوری اسلامی ایران باید بازدارنده باشد و معیارهای خاصی برای مقابله‌به‌مثل در برابر حملات سایبری با هدف بازدارندگی تعریف کند. نظریه بازدارندگی نوعی اقدام تلافی‌جویانه به شیوه تهاجم‌کننده را برای قدرت‌ها مشروع می‌داند و پاسخی به مجموعه‌ای از شرایط تاریخی، اجتماعی و استراتژیک منحصربه‌فرد در جنگ سرد است که در آن دو کشور دارای سلاح هسته‌ای برای کسب مزیت نسبی تحت خطر وقوع جنگ هسته‌ای در هر زمانی با یکدیگر رقابت می‌کنند. به‌روزرسانی این نظریه به حوزه سایبری باعث شد که قدرت‌های جهانی اتخاذ بازدارندگی سایبری را بخشی از استراتژی دفاع ملی خود تلقی کنند؛ مثلاً ایالات متحده اعلام می‌کند که «حق دفاع از خود در فضای سایبری» را از طریق اقدام تلافی‌جویانه مورد استفاده قرار می‌دهد. این راهبرد به این معنی است که ایالات متحده حق دارد زمانی که خود را در معرض تهدید می‌بیند به منبع تهدید حمله کند. نظریه بازدارندگی معتقد است عاملان حملات باید باور داشته باشند که مجازات دقیقاً همان‌گونه که مدافع بیان کرده است اجرا می‌شود. منطق تئوری بازدارندگی این است که دشمن بالقوه هنگامی از حمله منصرف می‌شود که «مجازات و تهدیدهای اعلام‌شده بیش از دستاوردهای حمله باشد». قابلیت اجرای مجازات یک مهاجم بالقوه از سه عنصر شناسایی عامل تهدید، انتخاب واکنش مناسب و اجرای واکنش تشکیل شده است. متأسفانه سیاست‌گذاران آمریکا با تحمیل یک آستانه خودسرانه، مجازات تحمیلی ایالات متحده را در حملات سایبری تا سقف حمله نظامی تنزل داده و بازدارندگی این نظریه را محدود کرده‌اند (Kiggins, 2014, p. 167).

۴/۳/۱/۹. نظریه امنیت سایبری داخلی

«امنیت سایبری» عبارتی است که درباره مراقبت هر حکومت از خود، نهادها و شهروندانش در برابر تهدیدها، جاسوسی، خرابکاری، جنایت، کلاهبرداری، سرقت و سایر تعاملات الکترونیکی مخرب به‌کار می‌رود. دولت‌ها در مواجهه با تهدیدهای ناشی از فضای مجازی، مجموعه‌ای از ابزارها، سیاست‌ها و اقدام‌ها را برای حفاظت از بُعد مجازی و غیرمجازی فضای سایبر کشور خود به‌کار می‌برند. سیاست‌گذاران فضای مجازی به چگونگی طراحی ترتیبات حکمرانی و در نتیجه اقدامات حاکمیتی برای حفاظت از فضای مجازی علاقه‌مند هستند و «امنیت سایبری» را به‌عنوان توانایی یک نظام سیاسی برای محافظت از فضای سایبری تحت حاکمیت خود درک می‌کنند. امنیت سایبری در دو ساحت داخلی و بین‌المللی کاربرد دارد. ساحت بین‌المللی برای مبارزه با تهدیدهای برون‌مرزی و خارج از قلمرو حکمرانی نظام‌های سیاسی به‌کار می‌رود. تهدید امنیتی داخل مرزهای کشورها هنگامی روی می‌دهد که بازیگرانی بالقوه وجود داشته باشند که انگیزه کافی و توانایی آسیب رساندن به امنیت نهادهای دولتی، عمومی، خصوصی یا شهروندان عادی آن کشور را داشته باشند. مصادیق استانداردهای امنیت در فضای مجازی داخل کشورها شامل الزامات عملکردی و تضمینی، سیاست‌های مدیریت اطلاعات، معیارهای ارزیابی اقدامات امنیتی، تکنیک‌های رسیدگی به نقص‌های فنی و رویه‌هایی برای نظارت بر حفره‌های امنیتی است. مفهوم امنیت سایبری داخلی دارای انواعی از استانداردها متناسب با خط‌مشی‌ها و ارزش‌های حاکم بر هر جامعه است؛ مثلاً در جوامع سرمایه‌داری، استاندارد «خصوصی» مبتنی بر بازار و در جوامع مدنی، استاندارد «پایین به بالا» وضع می‌شود. هدف کلی استانداردهای امنیت سایبری بهبود امنیت سیستم‌های فناوری اطلاعات، شبکه‌ها و زیرساخت‌های حیاتی است (Peng, 2018, p. 446).

۴/۳/۱/۱۰. نظریه توازن قوا

نظام سلطه جهانی برای توجیه خوی استکباری و اعتلاطلبی خود در تحمیل اراده بر سایر کشورها اقدام به تولید نظریه‌هایی مانند نظریه ثبات هژمونیک کرده است. براساس این نظریه نظام جهانی در عرصه‌های گوناگون نیازمند یک قدرت فائق است تا قواعد و نظم جهانی را حاکم کند. این قدرت‌ها دیگر کشورها را وادار به پیروی از این نظم و قواعد می‌کنند. آمریکا براساس نظریه ثبات هژمونیک، تسلط خود را بر فضای مجازی جهانی برای امنیت جهانی لازم می‌داند و دنبال حکمرانی واحد خود در فضای مجازی است. ازاین‌رو در پی توسعه همکاری بین سهامداران سایبری، محوریت آمریکا در همکاری امنیت سایبری کشورها و تولید هنجارهای مشترک در حوزه سایبری برای دستیابی به امنیت سایبری فراملی و کاهش تهدیدهای سایبری است (Kiggins, 2014, p. 162). در نظریه ثبات هژمونیک، ابرقدرت فائق بین‌المللی برای کشورهای مقابل هژمون در فضای مجازی، ساختارهای تقابل منطقه‌ای را در نظر می‌گیرد. بر این اساس در عرصه فضای مجازی یک ابرقدرت، در کنار چندین قدرت بزرگ و منطقه‌ای شکل گرفته است. ابرقدرت تسلط بر تمام سیستم فضای مجازی دارد و آن را مدیریت می‌کند. قدرت‌های بزرگ اختیارات فرامنطقه‌ای و فروابرقدرتی دارند. آمریکا به‌عنوان ابرقدرت در تمام

جهان دارای منافع است و هیچ بحران فراگیری را در هیچ منطقه‌ای نمی‌گذارد تمام شود مگر با حضور خود. قدرت‌های بزرگ گرچه از منطقه خود خارج شده‌اند، ولی در تمام جهان برای خود منافعی تعریف نکرده‌اند؛ مانند روسیه، چین و اتحادیه اروپا. در نظریه ثبات هژمونیک پنج تا هفت منطقه جهانی تعریف شده است که جمهوری اسلامی ایران به‌عنوان قدرت اول منطقه جنوب غرب آسیا شناخته می‌شود و رقیب او ابرقدرت است که در پی کنترل منطقه است. لذا حوزه تقابل ایران و آمریکا در منطقه شکل می‌گیرد. در منطقه دو لایه قدرت تعریف شده است: بازیگر اول ایران، بازیگران درجه دو عربستان و ترکیه هستند. پس کشورهای درجه دو با ابرقدرت در برابر قدرت منطقه‌ای ایران متحد می‌شوند. ساختار رفتاری جمهوری اسلامی ایران در برابر منطق ثبات هژمونیک، نظریه «توازن قوا» است. در این نظریه جهان فاقد ابرقدرت است و قدرت‌های منطقه‌ای دارای قدرت‌های نزدیک به هم و برابر هستند. مثلاً میزان تسلیحات نظامی قدرت‌ها براساس قراردادهای بین‌المللی به‌گونه‌ای متوازن می‌شوند که هیچ قدرتی بر دیگری برتری نداشته باشد و اگر کشوری در نقطه‌ای دارای قوّت بود، سعی می‌شود در نقاط دیگر برای او ضعف ایجاد کنند تا توازن قوا حفظ شود. در این ساختار، مناطق به‌صورت مستقل اداره می‌شوند و ابرقدرت حاکم وجود ندارد و ساختارهای بین‌المللی متشکل از دیدگاه‌های کشورهای مختلف تعریف می‌شود و هر قدرتی در منطقه خودش ساختار فکری خود را اجرا می‌کند. در منطقه جنوب غرب آسیا جریان مقاومت، در شرق آسیا، چین و در اوراسیا، روسیه قدرت فعال هستند. مقام معظّم رهبری در ۱۳۹۰/۱۱/۱۷ در پیوست حکم تشکیل شورای عالی فضای مجازی «ایمن‌سازی فضای مجازی و امکان بهره‌گیری همهٔ کشورها از فضا براساس حاکمیت ملی و عدالت» را از مهم‌ترین اهداف این شورا بیان کردند. ازاین‌رو جمهوری اسلامی ایران دنبال توازن قوا در عرصه حکمرانی جهانی فضای مجازی است و در منطقه به‌دنبال تسلط بر منطقه و کوتاه کردن دست ابرقدرت آمریکاست و رقیبانش در حال اتحاد با آمریکا. در برابر این اتحاد، کشورها براساس منافع خود اتحادهایی را برای اداره امور بین‌المللی تشکیل می‌دهند و در برابر زیاده‌طلبی نظام سلطه و دست‌اندازی قرون وسطایی استکبار به منافع ملت‌های ضعیف ایستادگی می‌کنند (نامه رهبر معظّم انقلاب به رئیس‌جمهور وقت درباره الزامات اجرای برجام، ۱۳۹۴/۷/۲۹، قابل دسترسی در نشانی https://khl.ink/f/31168).

۴/۳/۱/۱۱. نظریه ام‌القری

پیش از این، الگوهای هنجاری مسلط در عرصه‌های گوناگون ازجمله فضای مجازی با ذهنیت و باور برتری و توان غیرچالش آمریکا در معادلات جهانی شکل گرفته بود. این باور ناشی از «نظریه رهبری» بود که بر تولید ثبات بین‌المللی توسط آمریکا تمرکز می‌کند، در حالی که آمریکا برای تأمین امنیت فراملی خود، استفاده از قدرت نرم برای هدایت دولت‌های دیگر به مشارکت در فرایند مذاکره درباره اهداف سیاست مشترک خود را دنبال می‌کند. سیاست‌گذاران ایالات متحده فضای سایبری را به‌عنوان رسانه‌ای برای تبادل اطلاعات جهانی و اقتصادی، یک کالای عمومی جهانی می‌دانند که نیازمند رهبری برای جلوگیری از بالکانیزاسیون (تکه‌تکه شدن) و عدم برابری ملت‌های دیگر با قدرت آمریکاست. هدایت سایر بازیگران ائتلاف جهانی امنیت سایبری چندجانبه

به رهبری آمریکا شامل رسیدگی به وظایف ذیل است: ایجاد یک رژیم عدم اشاعه تسلیحات سایبری، اشتراک‌گذاری اطلاعات، دستگیری، استرداد و تعقیب مجرمان سایبری، تعیین معیارهای خاصی برای مقابله به مثل در برابر حملات سایبری، باز نگه داشتن مسیرهای ارتباطی و تجارت سایبری. جمهوری اسلامی ایران در مقابل رویکرد برتری‌جویانه آمریکا و متحدانش، استراتژی ام‌القری را دنبال می‌کند. جمهوری اسلامی ایران در مقیاس عملیاتی در برابر ادعای آمریکا بر رهبری فضای مجازی، دو منطق را ذیل نظریه ام‌القری دنبال می‌کند: «منطق عزت، حکمت و مصلحت» و «منطق مقاومت». طبق چارچوب ام‌القری، جمهوری اسلامی ایران به‌عنوان محور جهان اسلام و حامی مستضعفان جهان، کنشگری می‌کند و تمام اتحادها حول آن شکل می‌گیرد. براساس منطق مقاومت، ذهنیت توانمندی غیرقابل‌چالش و قدرت بلامنازع آمریکا جای خود را به باور به افول آمریکا و غلبه نرم‌افزاری بر هیمنه استکبار جهانی داده و بر همین اساس محور مقاومت در منطقه و جهان شکل گرفته است. مقاومت جهانی در برابر رهبری بلامنازع آمریکا بر فضای مجازی باعث عقب‌نشینی تاکتیکی آمریکا از نظریه رهبری سایبری شده است.

مضمون سوم سازمان‌دهنده عناصر استراتژی امنیت سایبری کشورمان عبارت است از: «سیاست استراتژیک». امنیت سایبری کشور متضمن تدوین سیاست‌های استراتژیک هوشمندانه و بر پایه عقلانیت نظام است. در شرایطی که در داخل کشور نیروهای قدرتمند سیاسی، اجتماعی، اقتصادی، فرهنگی و نظامی در جهت تأمین اهداف و منافع خاص خود حرکت می‌کنند، و در خارج کشور قدرت‌های منطقه‌ای و جهانی برای تحمیل اراده خود مقامات کشور را تحت فشار قرار می‌دهند، سیاست و استراتژی باید هوشمندانه طراحی شوند و در راستای اهداف عالی نظام قرار گیرند تا شاهد افزایش انسجام عمومی و تأمین منافع ملی باشیم. این سیاست‌ها به دو صورت اعلامی و اعمالی قابل‌تقسیم هستند. سیاست‌های استراتژیک اعلامی آن دسته از سیاست‌هایی هستند که در فرایند خط‌مشی‌گذاری و سیاست‌گذاری رسمی توسط نهادهای متولی فرایند تصویب‌خواهی را طی کرده و رسماً به اطلاع عموم می‌رسند. این سیاست‌ها لزوماً به مرحله اجرا نمی‌رسند و گاه به‌خاطر دشواری‌ها، موانع و عوامل ساختاری هیچ‌گاه برنامه‌ای برای عملی شدن آنها طراحی نمی‌شود. همچنین سیاست‌های اعمالی نیز الزاماً مسبوق به اعلام به عموم مردم نیستند و گاه به‌خاطر شرایط پیش‌بینی‌نشده و برخی مصالح، سیاست‌هایی در دستور اقدام دولت‌ها قرار می‌گیرد که به هیچ عنوان به آنها تصریحی نمی‌شود. آمریکا با وجود آنکه استراتژی امنیت ملی و حتی راهبردهای سایبری خود را اعلام عمومی کرده، سیاست‌های اعمالی بسیاری برای تأمین منافع ملی خود در فضای مجازی در پیش گرفته که هرگز تصریحی به آنها نکرده و حتی در مواردی آنها را تکذیب نیز کرده است؛ مانند تقویت نظارت داخلی بر فضای مجازی از طریق تسهیل جمع‌آوری داده‌های شخصی و تجاری از شرکت‌های اینترنتی آمریکایی ازجمله گوگل، فیسبوک، یاهو، اپل و مایکروسافت توسط آژانس امنیت ملی آمریکا، نظارت بر نهادهای سایبری کشورهای چین و روسیه، بلکه متحدان ایالات متحده مانند اتحادیه اروپا، عدم پذیرش ضمنی فضای مجازی به‌عنوان یک فضای مشترک جهانی فراتر از حاکمیت کشورها با هدف حکمرانی بر فضای مجازی

بدون دولت‌ها، استفاده از هژمونی فضای مجازی برای تغییر نظام سیاسی کشورهای در حال توسعه و اعمال استاندارد دوگانه. سیاست استراتژیک جمهوری اسلامی ایران برای تأمین امنیت سایبری دربردارنده مضامین پایه: تهدیدزدایی، ظرفیت‌سازی، مصونیت‌سازی، نظارت، جرم‌ستیزی، حفاظت اطلاعات، الزام پیامرسان‌ها، استانداردسازی، مدیریت بحران، تولید محتوا و دفاع بازدارنده است.

۴/۳/۱/۱۲. تهدیدزدایی

فضای مجازی محیطی پرمخاطره و همراه با تهدیدهای بسیاری، خصوصاً برای دولت‌هاست. برخی از مخاطرات امنیتی برای حکومت‌ها ناشی از آسیب‌پذیری‌های پنهان فضای مجازی هستند. این نوع از تهدید، ساختاری است. اما برخی از تهدیدهای امنیتی، کنشگرمحور است. تهدیدهای ساختاری بیشتر فرصت‌های بهره‌برداری بالقوه دولت‌ها از فضای مجازی را سلب می‌کنند، در حالی که تهدیدهای امنیتی کنشگرمحور، توسط بازیگران سازمان‌یافته‌ای ایجاد می‌شوند که بیشتر به اهداف مشخص حکومتی حمله می‌کنند (Weiss & Jankauskas, 2019, p. 260). دو رویکرد اساسی برای مقابله با تهدیدهای سایبری وجود دارد: رویکرد حفاظتی و رویکرد واکنشی. هدف رویکرد حفاظتی بازدارندگی مجرمان از طریق اقداماتی است که دسترسی را محدود یا یک هدف بالقوه را کمتر در برابر حمله آسیب‌پذیر می‌کند. این رویکرد بر دفاع فعال متمرکز و شامل فرایندهای طراحی پروتکل‌های سایبری ایمن‌تر، معرفی روترهای قابل‌اعتماد و شبکه‌های خصوصی مجازی، استفاده از فایروال‌ها، رمزگذاری، سیستم‌های تشخیص نفوذ خودکار و سایر اقدامات امنیتی است. رویکرد واکنشی، به‌دنبال جلوگیری از تهدید از طریق تحقیقات مؤثر، پیگرد قانونی و مجازات است. هر دو رویکرد شامل نظارت و تشخیص فعالیت غیرعادی و غیرمجاز است. رویکرد حفاظتی فعال به نفع اتوماسیون و همچنین نظارت و تصمیم‌گیری توسط کارشناسان امنیت رایانه است. رویکرد واکنشی بیشتر به مشارکت مجری قانون بستگی دارد و نیاز به تجزیه و تحلیل ترافیک کاربرمحور دارد، که ممکن است به اندازه اسکن فایل‌های پیوست، جستجوی کلمات کلیدی، و فیلتر کردن محتوا برای نشانه‌هایی از نقض احتمالی قوانین کیفری مزاحم باشد. این دو رویکرد می‌توانند مکمل یکدیگر باشند. وزن نسبی آنها به ترجیحات و قابلیت‌های طرف‌های اجراکننده بستگی دارد. رویکرد حفاظتی کمتر مداخله‌گر است و احتمالاً امنیت سایبری بیشتری برای کاربران خود به ارمغان می‌آورد. رویکرد واکنشی با وجود محدود کردن برخی از آزادی‌های کاربران، اما برای محافظت از کاربرانی که توانایی پرداخت هزینه‌ها را ندارند یا تمایلی به اجرای اقدامات حفاظتی کافی ندارند، مؤثرتر است (Berman, 2017, p. 218).

۴/۳/۱/۱۳. ظرفیت‌سازی

در خارج از ساختارهای رسمی حاکمیتی ظرفیت‌های فراوانی برای ارتقای فضای مجازی و دفع تهدیدها نهفته است که دولت می‌تواند واسطه‌هایی را با ظرفیت‌های مفید بسیج کند تا آنها را در قبال حملات علیه دولت به‌کار

گیرد. این واسطه‌ها می‌توانند در داخل یا خارج از دولت باشند. ظرفیت‌سازی می‌تواند از طریق واگذاری وظیفه مهار خطرات سایبری به یک عامل ثالث مانند مؤسسه نظارتی برای خطرات سایبری، فراخوان عمومی و خصوصی برای سالم‌سازی فضای مجازی، تشویق شرکت‌های خصوصی برای اشتراک تجربیات و توسعه سیاست‌های سایبری و ایجاد انگیزه‌های اقتصادی برای رعایت حداقل استانداردهای ایمن‌سازی فضای مجازی دنبال شود. این استانداردها شامل طراحی پروتکل‌های اینترنتی ایمن‌تر، معرفی روترهای قابل‌اعتماد و شبکه‌های خصوصی مجازی، استفاده از فایروال‌ها، رمزگذاری، سیستم‌های تشخیص نفوذ خودکار و سایر اقدامات امنیت‌ساز است.

۴/۳/۱/۱۴. مصونیت‌سازی

فضای مجازی به‌خاطر آسیب‌های فرهنگی و تهدیدهای امنیتی محیطی پرمخاطره است و حکومت‌ها اقدام به ایجاد مصونیت در این زمینه می‌کنند. تهدید بازیگران بدخواه یکی از این مخاطرات است. این بازیگران شامل هکرها، متعصبان، خودی‌های ناراضی، جنایتکاران، تروریست‌های سایبری غیردولتی و فرماندهی سایبری دولت‌های متخاصم هستند که اقدام به ایجاد اختلال در زیرساخت‌های حیاتی و سرقت اطلاعات می‌کنند. برخی از قدرت‌ها مانند چین در خصوص آسیب‌های فرهنگی اجتماعی، اقدام به مقابله با اطلاعات غیرقانونی و مضر مانند شایعه، فحاشی، خشونت، خرافات و فرقه‌گرایی می‌کنند. طنز اینترنتی، فرهنگ منحط، پورنوگرافی و اطلاعات مضر، آسیب‌های اصلی اجتماعی در فضای مجازی هستند. اولویت مصون‌سازی در برابر تهدیدهای امنیتی، تأمین امنیت زیرساخت‌های مجازی و فیزیکی در برابر تهدیدهای سایبری است. طبق استراتژی ایالات متحده، زیرساخت‌های سایبری حیاتی، شبکه‌های فدرال و اطلاعات باید برای حفاظت از شهروندان ایالات متحده ایمن شوند. روش‌های ایمن‌سازی فضای سایبری شامل افزایش ظرفیت فنی، توسعه فناوری‌های سایبری، قانون‌گذاری، سیاست‌ها، استانداردها و دستورالعمل‌های جدید است. بیشترین ضعف حکومت‌ها در ایمن‌سازی فضای مجازی ناشی از فقدان تخصص بازیگران دولتی، ناکارآمدی و طولانی بودن تصمیمات بروکراسی اداری در برابر حملات سایبری است (Abbott, 2018, p. 37).

۴/۳/۱/۱۵. نظارت

حکمرانی فضای مجازی به‌دور از یک سیستم نظارتی منسجم، شبیه جنگلی از تلاش‌های متفاوت و گاه متضاد است. تلاش‌های نظارتی می‌تواند شکل‌های گوناگونی داشته باشد: سلسله‌مراتبی با تحریم‌های واضح قوانین و احکام حقوقی، یا نرم‌تر مانند استانداردها و پروتکل‌های فنی داوطلبانه و آیین‌نامه‌های غیررسمی رفتار. ازاین‌رو ایالات متحده و متحدانش در راستای اِعمال سیاست نظارت در استراتژی امنیت سایبری ملی و حتی فراملی، بزرگ‌ترین و تواناترین سیستم نظارتی و تحلیلی را در تاریخ بشر ایجاد کرده‌اند؛ سیستمی با دسترسی نزدیک به جهان. برنامه کنترل فراگیر پریسم آژانس امنیت ملی ایالات متحده در این خصوص سرآمدترین است. بهبود امنیت سایبری از طریق الگوی نظارتی خودتنظیمی و هم‌تنظیمی نیز توسط برخی از کشورها دنبال می‌شود

(Austin, 2017, p. 216). سیاست نظارت شامل نظارت بر تولید محتوا، فرایندهای رسانه‌ها و شبکه‌های اجتماعی مجازی نیز می‌شود.

۴/۳/۱/۱۶. جرم‌ستیزی

فناوری‌های جرم و مجازات در حال تحول سریع و عمیق هستند. ارتکاب جنایت در فضای مجازی مفهومی نوین و پیچیده پیدا کرده و مجرمان به‌راحتی و بدون دغدغه از تعقیب و کیفر تخلفات و جرایم ارتکابی اقدام به جرم و جنایت می‌کنند؛ زیرا در زمینه مبارزه با جرایم سایبری با خلأ قانونی، فقدان ضابط قضایی و نهاد دادرسی، تغییر مفهوم ادله اثبات و راه‌های پیشگیری از جرم روبه‌رو هستیم. بیشتر جرایم ارتکابی در فضای مجازی از مرزهای بین‌المللی عبور می‌کنند و مجرمان سایبری ممکن است در یک کشور مستقر شوند؛ در حالی که از طریق فضای مجازی در کشور دیگری مرتکب جرم شوند. ازاین‌رو مبارزه با جرایم سایبری نه‌تنها نیازمند سیاست‌گذاری داخلی است، بلکه باید یک رژیم بین‌المللی بین کشورها در زمینه توافق بر شناسایی جرم و مجرمان و مجازات آنها همراه با جلوگیری از سوءاستفاده دولت‌ها علیه اهداف متخاصم پدید آید.

۴/۳/۱/۱۷. حفاظت اطلاعات

فضای مجازی محیطی ناامن برای مراقبت از داده‌های ملی و فراملی است؛ خصوصاً هک و سرقت داده‌ها از مصادیق تهدیدهای امنیتی به‌شمار می‌رود. بنابراین دولت‌ها مجموعه‌ای از ابزارها، سیاست‌ها و اقدامات را برای مقابله با هک، رصد شبکه و سرقت اطلاعات و نیز حفاظت از بُعد مجازی و غیرمجازی شبکه‌ها و داده‌های سایبری به‌کار می‌گیرند. مراقبت دولت‌ها از خود و نهادهایشان در برابر تهدیدها، جاسوسی، خرابکاری، جرم و کلاهبرداری، شناسایی سرقت و سایر تعاملات الکترونیکی مخرب و معاملات الکترونیکی است. لذا یکی از راهبردهای اساسی و ریشه‌ای برای حفاظت از اطلاعات، تأسیس و تقویت شبکه ملی اطلاعات است.

۴/۳/۱/۱۸. الزام پیامرسان‌ها

یکی از چالش‌های حکمرانی فضای مجازی، رعایت قوانین کشورها توسط اپراتورها، پیامرسان‌ها و پلتفرم‌های خارجی است. از آنجا که در کشور ما حجم اطلاعات گسترده اقتصادی، سیاسی، فرهنگی و حتی شخصی کاربران ایرانی در اختیار شرکت‌های خارجی سرویس‌دهنده پلتفرم‌ها، شبکه‌های اجتماعی مجازی و پیامرسان‌ها قرار دارد، این حجم از داده، دارای ابعاد امنیت ملی است. همچنین برخی از جرایم سایبری از طریق این پلتفرم‌ها، پیامرسان‌ها و شبکه‌های مجازی انجام می‌شود که دارای شاکی خصوصی یا مدعی‌العموم است. پس انتقال سِرورهای سرویس‌دهنده پلتفرم‌ها، شبکه‌های اجتماعی و پیامرسان‌های خارجی به ایران و نیز تأسیس دفتر نمایندگی برای پیگیری‌های رسمی و قضایی ضروری به‌نظر می‌رسد. به همین خاطر الزام پلتفرم‌ها، شبکه‌های اجتماعی مجازی و پیامرسان‌های خارجی به رعایت قوانین جمهوری اسلامی ایران از طریق انتقال سِرور و تأسیس دفتر نمایندگی با مکانیسم‌های قانون‌گذاری و دیپلماسی سایبری و سایر راهبردها قابل‌تحقق است. سیاست الزام پیامرسان‌ها در برخی

از کشورهای منطقه به اجرا درآمده است؛ مثلاً در ترکیه، قانون ۷۲۵۳ مورخ اول اکتبر ۲۰۲۰ تمام شبکه‌های اجتماعی مجازی که دارای بیش از یک میلیون کاربر ترکیه‌ای هستند باید نمایندگی حقوقی در ترکیه تأسیس کنند و در صورت عدم افتتاح دفتر رسمی، از سوی دولت ترکیه با جریمه روبه‌رو خواهند شد.

۴/۳/۱/۱۹. استانداردسازی

یکی از کارکردهای حکمرانی فضای مجازی، استانداردسازی این فضا در ابعاد فنی و امنیتی برای افزایش کارآیی و دفع آسیب‌هاست. با توجه به تحولات سریع فناوری، استانداردسازی فنی تصمیمات مربوط به پروتکل‌های شبکه، برنامه‌های کاربردی نرم‌افزاری و استانداردهای قالب داده را در نظر می‌گیرد. استانداردهای امنیت سایبری از طریق الزامات امنیتی مشترک و قابلیت‌های مورد نیاز برای راه‌حل‌های امن ایجاد می‌شوند. در حالی که حذف همه تهدیدات غیرممکن است، استانداردهای امنیت سایبری حملات را سخت‌تر می‌کنند یا حداقل تأثیر حملات را کاهش می‌دهند. هدف کلی استانداردهای امنیت سایبری بهبود امنیت سیستم‌های فناوری اطلاعات، شبکه‌ها و زیرساخت‌های حیاتی است. استانداردهای امنیت سایبری الزامات عملکردی و تضمینی، سیاست‌های مدیریت اطلاعات، معیارهای ارزیابی اقدامات امنیتی، تکنیک‌های رسیدگی به نقص‌های امنیتی و رویه‌هایی برای نظارت بر نقض‌های امنیتی را در بر دارند. در سطح جهانی و سایر کشورها، چنین استانداردهایی بسیار متنوع هستند و انبوهی از استانداردهای بین‌المللی را تشکیل می‌دهند. پس هماهنگ‌سازی استانداردهای امنیت سایبری از طریق تنظیم نهادی و مکانیسم هماهنگی صورت می‌پذیرد (Shin, 2018, p. 453).

۴/۳/۱/۲۰. مدیریت بحران

دولت‌ها برای از بین بردن و کاهش خسارت‌های ناشی از بحران‌های سایبری پیش‌بینی‌نشده، از طریق مجموعه‌ای از اقدامات قانون‌گذاری، نهادسازی و عملیاتی خود را آماده می‌کنند. در عرصه فضای مجازی هدف هر حاکمیت، ایجاد اطمینان در بین شهروندان برای استفاده از شبکه ملی و جهانی به‌عنوان رسانه پایدار، قابل‌اعتماد و امن در تبادل اطلاعات، تأمین نیازهای زندگی و اهداف اقتصادی است. حکومت‌ها سیاست کنترل بحران و بازگرداندن وضعیت بحرانی به شرایط عادی پیش از وقوع بحرام را به اجرا می‌گذارند. کاهش عدم اطمینان و ایجاد هماهنگی بین بازیگران دولتی و خصوصی از مهم‌ترین اقدامات برای کنترل بحران‌های سایبری است. ازاین‌رو دولت‌ها اختیاراتی به سرویس‌های اطلاعاتی به‌عنوان مأمور برای جمع‌آوری داده‌ها و اجازه ارزیابی مخاطرات با توجه به فعالیت‌های دشمنان و اهداف متخاصم واگذار می‌کنند. در برخی موارد، سرویس‌های اطلاعاتی حتی دارای واحدهای سایبری مجزا برای انجام عملیات علیه اهداف خاص هستند (Boeke, 2015, p. 74).

۴/۳/۱/۲۱. تولید محتوا

رویکرد عوام‌فریبانه آمریکا و کشورهای غربی درباره تولید محتوای فضای مجازی توسط دولت‌ها مخالفت است و چنین استدلال می‌کنند که این امر موجب تضعیف آزادی بیان و نقض حقوق کاربران خصوصی می‌شود؛ زیرا تولید و تنظیم محتوای آنلاین توسط دولت‌ها، ناشی از نگرانی در مورد حفظ مشروعیت، پایگاه اجتماعی و انعطاف‌پذیری در یک جامعه چندنژادی و چندفرهنگی با سابقه تنش‌ها و شورش‌هاست (Ad'ha Aljunied, 2019, p. 1). سیاست اعلامی دولت‌های غربی به‌جای تولید محتوا، تمرکز بر معماری اطلاعات است. آنان با تزویر چنین وانمود می‌کنند که با ورود دولت‌ها به تولید محتوا، فضای مجازی به ابزاری برای تقویت اقتدار دولتی در برخورد با مشکلات داخلی تبدیل می‌شود. این در حالی است که سیاست اعمالی ایالات متحده و کشورهای اروپایی با شعارها و سیاست اعلامی آنها متغایر است؛ مثلاً آمریکا برای سرکوب مخالفان داخلی یا در جنگ علیه کوبا سیاست تشدید تهاجم روانی را در پیش گرفت و با هدف شستشوی مغزی مخالفان، بی‌ثبات کردن جامعه و تضعیف دولت مقابل، در کنار دیگر استفاده‌های خصمانه از مخابرات، به تولید محتوای رادیویی و تلویزیونی علیه کوبا پرداخت (UNGA, 2017). در حال حاضر نیز برای تولید محتوای سایبری در زمینه‌های تقویت منافع خود از طریق دولتی و بخش خصوصی اقدام می‌کند. ایالات متحده در جنگ عراق نیز همین سیاست را در تبلیغات شبکه‌های ماهواره‌ای و فضای مجازی در پیش گرفت. در شرایطی که دشمنان اسلام و جمهوری اسلامی ایران از فضای مجازی به‌عنوان ابزاری برای کوبیدن فضایل، از بین بردن حقانیت ایران، تشویه معنویات و سوق دادن مخاطبان به ارزش‌های غربی سوءاستفاده می‌کنند، بر کسانی که توانایی تولید محتوا در راستای تبیین ارزش‌ها و مبانی نظام را دارند، لازم است حقانیت جمهوری اسلامی و ارزش‌های دینی را به مخاطبان برسانند. نظام اسلامی به دستگاه تولید محتوا نیاز دارد و نمی‌تواند در این خصوص بدون برنامه باشد و به تولیدات اتفاقی خودجوش اکتفا کند. بر این اساس رهبر معظّم انقلاب از شورای عالی فضای مجازی طراحی، برنامه‌ریزی و تقویت دستگاه تولید محتوا را از طریق استفاده از ظرفیت حوزه‌های علمیه، نخبگان دانشگاهی و جوانان خوش‌فکرِ متدین مطالبه کرده‌اند (صلح میرزایی، ۱۴۰۰: ۱۶۴).

۴/۳/۱/۲۲. دفاع بازدارنده

به هرگونه اقدام مخرب برای تضعیف کارکردهای شبکه با اهداف سیاسی یا امنیت ملی، حمله سایبری گفته می‌شود. حملات سایبری در چند عرصه انجام می‌شود. عرصه اول «مدیر سیستم علیه مدیر سیستم» نام دارد که از طریق نرم‌افزارها، تروجان‌ها و نفوذ به حفره‌های امنیتی انجام می‌شود و غالباً به جاسوسی سایبری منتهی می‌شود. عرصه دوم «چالش سینتیک با کمک فضای مجازی» است که در آن بازیگر بدخواه اثر سینتیک ایجاد می‌کند؛ مثلاً سعی می‌کند در عملکرد سیستم کنترل رادار ضد هوایی، اختلال ایجاد کند. عرصه سوم «دستکاری مخرب» نام دارد و در این نوع از حمله، سیستم‌های متصل به شبکه، در مقیاس گسترده و آنی از بین می‌روند؛ مثلاً خط انتقال نیرو متلاشی می‌شود (جمعی از نویسندگان، ۱۳۹۱: ج۱، ص۸۶ـ۹۰).

کشورها در برابر حملات اهداف متخاصم به دفاع از خود می‌پردازند، اما آیا در برابر حملات بالقوه یا قریب‌الوقوع، حق دفاع پیش‌دستانه یا بازدارنده وجود دارد؟ برخی با استناد به حقوق بین‌الملل خصوصاً ماده ۵۱ منشور ملل متحد قائل به حق دفاع بازدارنده در آستانه حملات دشمن هستند. سیاست بازدارندگی معتقد است که دشمن بالقوه زمانی از حمله منصرف می‌شود که «مجازات تهدیدشده بیشتر از دستاوردهای حمله باشد». استراتژی بازدارندگی محور سیاست امنیت سایبری ایالات متحده است. طبق سیاست بازدارندگی، عاملان حملات باید باور داشته باشند که مجازات دقیقاً همان‌گونه که مدافع بیان کرده است اجرا می‌شود. سیاست‌گذاران ایالات متحده به این نتیجه رسیده‌اند که همان قوانینی که در مورد جنگ در حوزه‌های هوا، زمین، دریا و فضا اعمال می‌شود، در حوزه سایبری نیز باید اعمال شود و حق استفاده از نیروی نظامی در پاسخ به حمله سایبری را برای خود محفوظ می‌دانند (Kiggins, 2014, p. 167). سوگمندانه، سیاست‌گذاران ایالات متحده به آستانه خودسرانه‌ای متعهد شده‌اند که در صورت عبور کشورهای متخاصم در فضای سایبری، پاسخ ایالات متحده ممکن است شامل حمله نظامی با استفاده از موشک، بمب، یا تهاجم زمینی باشد. این آستانه تأثیری بر محدود کردن اعتبار تهدید ایالات متحده برای مقابله‌به‌مثل در برابر یک حمله سایبری دارد. روسیه، چین و کوبا با این سیاست یک‌جانبه آمریکا مخالفت دارند؛ زیرا معتقدند که این منطق، اقدامات نظامی را در چارچوب فناوری اطلاعات و ارتباطات مشروعیت می‌بخشد و درگیری سایبری را به درگیری جنبشی و نظامی منجر می‌کند؛ به‌گونه‌ای که به نفع قدرت‌های نظامی قوی‌تر است. سیاست چین در این خصوص، دفاع نرم در برابر «تهاجم» ایده‌های لیبرال غربی است. شماری از کشورها در حال تقویت استراتژی بازدارندگی سایبری و تشدید مسابقه تسلیحاتی در فضای سایبری هستند. براساس مبانی فقهی رهبر معظّم انقلاب، هنگامی امکان این امر وجود دارد که متخاصم ابتدا نقض عهد کرده و آغازگر حمله باشد (امام خامنه‌ای، ۱۳۹۷: ۲۷۵). همچنین مقام معظّم رهبری جنگ نرم را مهم‌تر از جنگ آشکار نظامی ارزیابی کرده و اهداف دشمن را در این نبرد، تبلیغات منفی علیه نظام، قطع زنجیره تواصی و وارونه نشان دادن حقایق می‌دانند و الگوی «جهاد تبیین» را برای مقابله با اهداف دشمن در فضای مجازی تجویز کرده‌اند (صلح میرزایی، ۱۴۰۰: ۳۴).

۴/۳/۲. بازیگران

به کنشگران و فعالان تأثیرگذار در هر عرصه، بازیگران آن عرصه گفته می‌شود. مثلاً به عناصر و پدیده‌های تأثیرگذار در روابط بین‌الملل، بازیگران روابط بین‌الملل می‌گویند که شامل دولت‌ها و سازمان‌های مردم‌نهاد فروملی و اشخاص حقوقی غیردولتی فراملی هستند. بازیگران حکمرانی فضای مجازی، کنشگرانی هستند که در پی اعمال اراده بر فضای مجازی برای تحقق اهداف و منافع خود هستند و شامل بازیگران دولتی، شرکت‌های چندملیتی و سازمان‌های غیردولتی می‌شود. هریک از این بازیگران ارزش‌ها، منافع و غایات خاصی را در فضای مجازی دنبال می‌کنند. بازیگران مؤثر بر مضمون فراگیر استراتژی امنیت سایبری ایران به اقسام بازیگران تهدید و آسیب، روندسازان، برنامه‌سازان، تصمیم‌سازان و مجریان تقسیم می‌شوند.

۴/۳/۲/۱. بازیگران تهدید و آسیب

«تهدید» هر عنصر یا وضعیتی است که ادامه موجودیت و بقای یک پدیده یا ساختار را به مخاطره می‌اندازد، اما آسیب فشار بر یک ساختار یا پدیده با هدف ایجاد اخلال و ناکارآمدی در کارکردهای مورد انتظار آن ساختار یا پدیده است. فضای مجازی عرصه رقابت و تعارض اهداف و منافع قدرت‌های جهانی و منطقه‌ای است. هدف بازیگران تهدید و آماج حملات تهدیدکنندگان حکمرانی فضای مجازی جمهوری اسلامی ایران، براندازی نظام یا ایراد ضربه اساسی به موجودیت و اعتبار جمهوری اسلامی ایران از طریق فضای مجازی است. بازیگران تهدید دولتی شامل آمریکا و رژیم صهیونیستی و کشورهای هم پیمان آنها مانند عربستان سعودی است؛ زیرا جمهوری اسلامی ایران منافع استکباری ایالات متحده را در منطقه و جهان به چالش کشیده و دولت آمریکا بارها اقدام به براندازی نظام اسلامی از طریق نرم مانند انقلاب مخملی در فتنه سال ۱۳۸۸ کرده است. رژیم صهیونیستی نیز ادامه حیات خود را در دشمنی آشکار با هدف براندازی جمهوری اسلامی ایران و محور مقاومت در منطقه می‌داند. از آنجا که ایران قدرت اول منطقه جنوب غرب آسیاست، قدرت‌های درجه دو منطقه‌ای در دشمنی با ایران پیمان همکاری و اتحاد با ابرقدرت آمریکا دارند و در عرصه منطقه‌ای در سوریه و یمن به‌صورت نیابتی به دشمنی آشکار با ایران پرداخته‌اند. بازیگران تهدید غیردولتی شامل تروریست‌ها و گروهک‌های ضدانقلاب و برانداز است. این بازیگران در فضای مجازی از ایراد هرگونه ضربه به جمهوری اسلامی ایران و منافع ملی کشورمان کوتاهی نمی‌کنند. هدف بازیگران آسیب، ناتوان کردن ساختار حکومتی از اعمال حاکمیت و ایجاد مانع در راه تحقق اهداف حاکمیتی است. این بازیگران شامل مجرمان سازمان‌یافته سایبری، هکرها، تندروها یا خودی‌های ناراضی هستند. اقدامات بازیگران بدخواه در فضای مجازی می‌تواند منجر به ناامنی در سطوح کلان، میانی و خرد از طریق اختلال در امنیت ملی، امنیت دولتی، امنیت خصوصی کاربران و امنیت شبکه شود. ارتکاب جرایم دیگر از طریق فضای مجازی مانند جاسوسی، اعمال منافی عفت، تبلیغ افکار انحرافی، نشر اکاذیب، سرقت، ربایش اطلاعات، تهدید و تضعیف باورهای باطل و مانند آن نیز می‌تواند در زمره انواع آسیب‌های فضای مجازی قرار گیرد.

۴/۳/۲/۲. روندسازان

به تغییرات و تحولات منظم پدیده‌های اجتماعی و داده‌ها در طول زمان، روند می‌گویند. روند هنگامی بروز می‌کند که چند رویداد یا پدیده دارای جهت‌گیری یا گرایش عمومی با عوامل یکسان باشند. برخی از عوامل انسانی بر کاهش یا افزایش تغییرات دخیل هستند. روندسازان به مجموعه‌ای از عوامل انسانی دخیل در فناوری ارتباطات و اطلاعات و نیز حکمرانی فضای مجازی اطلاق می‌شود که الگوی رفتاری آنها قابل هدایت و مدیریت است. مثلاً روندسازان پدیده جهانی شدن، عوامل انسانی و ساختاری اعم از دانشمندان، سیاست‌مداران، دولت‌ها و شرکت‌های چندملیتی هستند که بر سرعت رشد یا کاهش این پدیده اثرگذار هستند. روندسازان امنیت سایبری، عوامل اصلی ایجاد تغییرات و تحولات پدیده حکمرانی فضای مجازی هستند؛ عواملی مانند شرکت‌های

دانش‌بنیان، استارتاپ‌ها و مردم. کشورهای توسعه‌یافته از طریق پارک‌های علم و فناوری، دانش را به میان مردم آورده و بر سرعت رشد فاوا تأثیر زیادی داشته‌اند. استارتاپ‌ها یک زنجیره منسجم ارزش به همراه خود می‌آورند که بر تمامی نهادهای تأثیرگذار بر حکمرانی، اثر می‌گذارند. مردم نیز از طریق انتخاب‌های خود، حاکمیت را به سوی سلایق خود سوق می‌دهند؛ مثلاً روند ترافیک فضای مجازی در بیشتر کشورها به سوی تماشای ویدیو است (فیروزآبادی، ۱۳۹۶: ۱۲۹). همچنین عموم کاربران، پلتفرم‌هایی انتخاب می‌کنند که بیشترین خدمات را می‌دهند و نیازهای آنان را مرتفع می‌کنند.

۴/۳/۲/۳. تصمیم‌سازان

دولت‌ها رفتار خود را براساس تصمیماتی تنظیم می‌کنند که در سطوح سیاست‌گذاری به آنان ابلاغ می‌شود. در تبادل بین سیستم و محیط نیز دولت‌ها نهاده‌ها را به داده‌ها یا تصمیمات حکومتی تبدیل می‌کنند. رفتار و تصمیمات دولت‌ها از طریق داده‌هایی که سیاست‌مداران و دولتمردان وارد محیط می‌کنند، زمینه بروز و ارزیابی پیدا می‌کند. بر همین اساس، منافع، کارکردها، ادراکات، القائات و کنش‌های برخی از شخصیت‌های حقیقی، ساختارها، گروه‌ها و جریان‌ها بر راهبردها، سیاست‌ها، فرایند تصمیم‌گیری و تدابیر عملیاتی دولت‌ها و مسئولان حاکمیتی تأثیرگذار بوده و منشأ سازنده تصمیمات آنها می‌شود. در برخی از ساختارهای حکومتی، کارکرد برخی از نهادها تصمیم‌سازی است؛ این ساختارهای قانونی با تکیه بر مبانی ارزشی، تجارب و افق‌های پیش‌رِو در فرایند خط‌مشی‌گذاری عمومی ورود پیدا کرده و اولویت‌های سیاست‌ها را براساس تدابیر و قواعد خود تعریف می‌کنند؛ مانند اتاق‌های فکر، نهادهای پژوهشی برخی از قوا و مراکز تحقیقی وزارت‌خانه‌ها. استراتژی امنیت سایبری جمهوری اسلامی ایران در کنشگری تصمیم‌سازی نیازمند بسیج ظرفیت‌ها در برابر آسیب‌پذیری‌های حاکمیت در فضای مجازی و همسویی یا ادغام مراکز تحقیقی، سازمان‌های مطالعاتی و اتاق‌های فکر موازی و ارتقای آنها به یک بازیگر تصمیم‌ساز فراملی است.

۴/۳/۲/۴. برنامه‌ریزان

با ورود نگاه راهبردی به نظام مدیران کشور، فرهنگ برنامه‌ریزی در سطح خرد و کلان در ساختارهای حاکمیتی نهادینه شده است. تلاش هدفمند برای رسیدن به اهداف کلان و سیاست‌های کلی در سطح رؤسای قوا و کلان ساختارها انجام می‌شود؛ مانند برنامه‌های پنج‌ساله توسعه. جمهوری اسلامی ایران نیازمند برنامه ملی دفاع سایبری در راستای تأمین منافع ملی می‌باشد. در سطح خرد، اهداف عملیاتی توسط وزیران، مدیران میانی و منطقه‌ای در دوره‌های کوتاه برنامه‌ریزی می‌شود.

۴/۳/۲/۵. مجریان

تحقق امنیت سایبری کشور به ساختارهای تأمین‌کننده، دفاعی، علمی و اجراکننده قوانین و برنامه‌های فضای مجازی بستگی دارد تا علاوه‌بر دفع تهدیدها، از تحصیل و حفظ منافع ملی نیز اطمینان خاطر ایجاد شود. براساس

تلقی سنتی از امنیت ملی، برخی کشورها در برابر حملات سایبری اقدام به راه اندازی نیروی واکنش سریع یا گروه‌های واکنش اضطراری کرده‌اند؛ مانند فرماندهی سایبری ایالات متحده۱، نیروی پشتیبانی استراتژیک چین۲، تیم‌های ملی واکنش اضطراری رایانه‌ای اتریش۳ یا نیروی واکنش سریع آلمان. کارکرد این مجریان، استفاده به‌هنگام و کارآمد از دارایی‌های سایبری علیه سیستم‌های فرماندهی و کنترل نظامی دشمن با هدف کاهش خسارت‌های حملات دشمن و مراقبت از منافع ملی در فضای مجازی است. اما در تلقی مدرن، امنیت سایبری چندبُعدی است و مجریان امنیت سایبری علاوه‌بر دفع حملات، درباره جلب منافع، ثبات سیاسی، شکوفایی اقتصادی و رشد علمی نیز کنشگری دارند. همچنین در صورت ضعف یا حتی شکست در یک عرصه، امکان جبران و حتی پیروزی در سایر عرصه‌ها وجود دارد.

۴/۳/۳. گفتمان

گفتمان، دستگاه بینشی و نظام ارزشی اثرگذار بر ادراکات مخاطبان از طریق ساختار زبانی است. امروزه بیشتر مرزهای اجتماعی و واقعیت‌های بازنمایی‌شده از طریق گفتمان‌ها ساخته می‌شود. گفتمان امنیت سایبری جمهوری اسلامی ایران، «هویت‌زا، بیگانه‌ستیز، هژمونی‌ساز و تهدیدزدا» است.

۴/۳/۳/۱. هویت‌زا

برخلاف ویژگی مرکزیت زدای گفتمان پست مدرن، امنیت سایبری جمهوری اسلامی ایران بر مفاهیم هویتی مانند دین، ارزش‌ها، سرزمین، زبان، اعتبار و مرزهای اجتماعی تأکید دارد. رویکرد پست مدرن، ساختارهای نوین اجتماعی را براساس ولنگاری ارزشی جایگزین ساختارهای سنتی از قبیل حزب می‌کند و در فضای مجازی به‌دنبال فروپاشی مرزهای هویتی است. در حالی که گفتمان سایبری ایران، معنابخش و هویت‌دهنده ارزش‌های اخلاقی است، از فرهنگ شیعی و سبک زندگی ایرانی اسلامی محافظت می‌کند.

۴/۳/۳/۲. بیگانه‌ستیز

ویژگی بیشتر گفتمان‌ها تولید دوگانه‌های خودی و دیگری است. مفهوم دیگری، سازنده منطق تمایز، مرز و تضادهای هویتی است. گفتمان سایبری جمهوری اسلامی ایران بر مرزهای هویتی بنیان نهاده خواهد شد که در آن دوگانه‌های مستضعفین ـ مستکبرین، خودی ـ بیگانه، حق ـ باطل، فرشته ـ شیطان در مظاهر و نمادهای بیرونی تمایزگذاری می‌شوند.

۴/۳/۳/۳. تمدن‌ساز

1. USCYBERCOM
2. PLA
3. GovCERT6

ایالات متحده افق نوینی از استراتژی بین‌المللی فضای مجازی را دنبال می‌کند که در آن نسخه تمدنی غرب نوعی نظم هژمونیک در فضای مجازی جهانی ایجاد می‌کند تا ارزش‌های غربی و سبک زندگی آمریکایی به‌عنوان آرمان سایر ملت‌ها دنبال شود. ازاین‌رو از طریق ظرفیت‌های فضای مجازی توانست بهار عربی (بیداری اسلامی) کشورهای عربی را به انحراف کشانده و نیز قدرت چین در فضای مجازی را به سوی کاهش تهدید علیه منافع تمدنی آمریکا مدیریت کند (Shen, 2016, p. 82). گفتمان جمهوری اسلامی ایران در برابر نفوذ تمدن غرب در فضای مجازی، احیای تمدن اسلامی و در برابر گسترش هژمونی آمریکا بر جهان، توسعه ارزش‌های تمدنی شرق و ایجاد ائتلاف‌های تمدنی است. خصوصاً در شرایط بن‌بست تمدن غرب و افول آمریکا، ظرفیت‌های تمدن اسلامی نوین توان تولید هندسه نوین قدرت در فضای مجازی را داراست.

۴/۳/۳/۴. تهدیدزدا

گفتمان جمهوری اسلامی ایران در برابر تهدیدهای فضای مجازی، ایمن‌سازی، مصون‌سازی فضا از انتشار داده‌های مضرّ و الزام بازیگران به رعایت هنجارهای ملی است.

۴/۳/۴. ژئوپلیتیک

درک واقعیت‌های محیط به‌منظور دستیابی به قدرت و مطرح کردن خود به‌عنوان بازیگر برتر جهانی و منطقه‌ای را دانش ژئوپلیتیک می‌نامند. فضای مجازی باعث شده قدرت در دست بازیگرانی قرار گیرد که امکان تولید، کنترل و توسعه مؤثرتر اطلاعات در این فضا را داشته باشند. قدرت نرم حاصل از این فضا نقش مهمی در میزان همراه‌سازی دیگران در تحقق اهداف و منافع ملی کشورها دارد (مولانا، ۱۳۸۷: ۷۵). حکمرانی فضای مجازی امکان نفوذ، برتری، اثرگذاری و منفعل‌سازی طرف‌های مقابل را اعطا می‌کند. لذا برای تأمین منافع ملی، یکی از ارکان مهم استراتژی امنیت سایبری جمهوری اسلامی ایران، توجه به ژئوپلیتیک فضای مجازی و مفاهیم سازنده آن است. مضامین سازنده ژئوپلیتیک فضای مجازی در استراتژی امنیت سایبری ایران عبارتند از: مقابله با نقض حاکمیت، امنیت سایبری فراملی، تضعیف حکمرانی واحد، شبکه ملی اطلاعات.

۴/۳/۴/۱. مقابله با نقض حاکمیت

حقوق بین‌الملل «حکومت» را در قالب سرزمینی تعریف کرده که شامل جمعیتی است که توسط یک نهاد دولتی کارآمد نمایندگی می‌شود. این مبنای سرزمینی برای حکومت سیاسی با پیدایش فضای مجازی، فناوری ارتباطات و اطلاعات، واقعیت مجازی، افزایش سفر، مهاجرت و مبادلات اقتصادی زیر سؤال رفته است. از طرفی، همواره قدرت‌هایی خارج از اراده حکومت‌ها وجود دارند که با فرامین و سیاست‌ها مخالف هستند و به مبارزه و مخالفت با آنها برمی‌خیزند. حکومت‌ها نیز به مقابله و مجازات نیروهای مخالف اقدام می‌کنند تا آنان را به تمکین وادار کنند. فضای مجازی نیز عرصه به چالش کشیدن حاکمیت‌هاست و نیروهای مخالف، انواع جرایم، قاچاق، معارضه و تهدیدها را درباره قدرت مرکزی به عمل می‌آورند. قاچاق مجازی از طریق انتقال پول، کالا، انسان و

اندیشه برخلاف قوانین سرزمینی انجام می‌شود. بیشتر جرایم مجازی نیازمند برنامه‌ریزی قبلی و برخی از آنها در خارج از مرزهای سرزمینی است و عاملان آن اغلب افراد دارای مهارت هستند. حکومت‌ها در مقابله با این جرایم، مبادرت به شناسایی، تنبیه مجرمان، خصوصاً در خارج از مرزها و حفاظت از حریم و حقوق شهروندان می‌کنند. دولت‌ها اکنون حداقل برخی از جنبه‌های قضایی را در مورد تعداد قابل توجهی از جرایم خارج از کشور اعمال می‌کنند. با وجود اینکه دولت‌ها به‌طور فزاینده‌ای فضای مجازی ملی خود را کنترل می‌کنند و حتی با وجود اینکه اصل قلمروی مقرر می‌دارد که یک دولت بر سِرورها و گروه‌های داخل مرزهای شناخته‌شده خود صلاحیت قضایی دارد، در فضای بین‌المللی جرایم زیادی رخ می‌دهد که بیشتر توسط شبکه‌های خصوصی اداره می‌شوند که توسط هیچ دولتی کنترل نمی‌شوند، بسیاری از دارایی‌های ملی مجازی در سِرورهای خارج از کشور ذخیره می‌شوند (Karim, 2019, 2636). عواملی که حاکمیت مرکزی را در فضای مجازی تهدید می‌کند عبارتند از: سرقت اطلاعات، جاسوس‌افزارها، رصد شبکه، حمله به زیرساخت‌ها، بدافزارها.

۴/۳/۴/۲. امنیت سایبری فراملی

سازمان‌های فراملی در فضای مجازی فعالیت قابل توجهی دارند که باعث پیدایش چالش برای حکومت‌ها می‌شود. مثلاً دولت‌های ملی سیاست‌های اتخاذشده توسط شرکت‌های فراملی مانند گوگل، فیسبوک و توییتر را تهدیدی برای حاکمیت دیجیتال و در نتیجه امنیت ملی خود می‌دانند (Liaropoulos, 2017, p. 28). جمهوری اسلامی ایران در برابر ناامنی‌های فراتر از مرزهای خود می‌تواند استراتژی‌های ذیل را برای تأمین امنیت سایبری خود در فراتر از مرزها در پیش گیرد: ایجاد سازمان‌های فراملی و فراملیتی، همکاری‌های بین‌المللی برای ایجاد رژیم عدم اشاعه تسلیحات سایبری، ائتلاف منطقه‌ای و جهانی برای امنیت سایبری، اجماع روی مجموعه‌ای از هنجارهای سایبری، تولید هنجارهای مشترک، تقویت جایگزین‌های نظم آیکان، بازدارندگی جمعی، جدا کردن واشنگتن از متحدانش، بیرون راندن آمریکا از دخالت در حکمرانی جهانی فضای مجازی، نظم بخشیدن دوباره به حکمرانی جهانی و منطقه‌ای فضای مجازی، حق دفاع مشروع و حمله پیشگیرانه.

۴/۳/۴/۳. تضعیف حکمرانی واحد

الگوی حکمرانی آمریکا بر فضای مجازی یک‌جانبه‌گرایی است و آمریکا به‌دلیل استقرار شرکت‌های بزرگ و زیرساخت‌های فضای مجازی در این کشور و به بهانه جلوگیری از بالکانیزه شدن (تکه‌تکه شدن) فضای مجازی، خود را حکمران واحد فضای مجازی می‌داند. کشورهای مخالف حکمرانی آمریکا (حکمرانی چندذی‌نفعی) قائل به رویکرد چندجانبه‌گرایی در حکمرانی بین‌المللی فضای مجازی هستند. الگوی حکمرانی چندجانبه، فضای مجازی را حوزه‌ای پرهرج‌ومرج می‌داند که ناامنی را در ابعاد جهانی تقویت می‌کند. بنابراین دولت‌ها باید در فضای مجازی سیاست‌گذاری کنند. این رویکرد مستلزم ایجاد نهادی در سازمان ملل متحد است که مسئولیت حکمرانی جهانی فضای مجازی را بر عهده خواهد داشت، اما در عین حال دولت‌ها قدرت تعیین سیاست‌های ملی

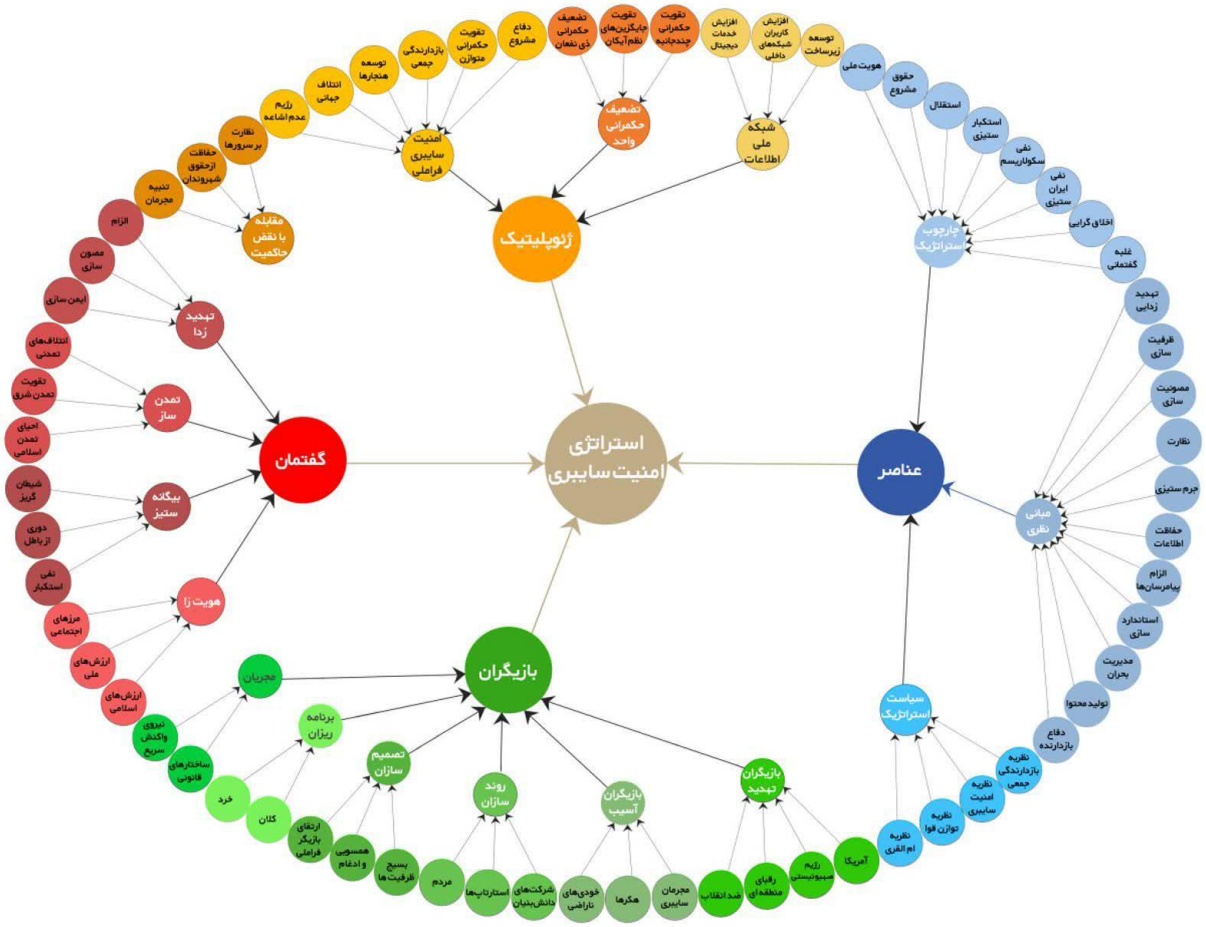
خود را خواهند داشت. این الگو همچنین با منطق و نظریه توازن قوا همخوانی دارد. الگوی حکمرانی چندجانبه توسط روسیه، چین، ایران و هند حمایت شده است. خصوصاً پس از افشای ادوارد اسنودن، حتی در میان برخی از کشورهای عضو اتحادیه اروپا که دنبال محافظت از مرزهای سایبری و داده‌های خود در برابر سیستم‌های نظارتی ایالات متحده هستند، شتاب بیشتری به دست آورده است (West, 2016, p.7).

۴/۳/۴/۴. شبکه ملی اطلاعات

یکی از صائب‌ترین دیدگاه‌ها درباره تعریف مرز در فضای مجازی، استفاده از از مکان‌های جغرافیایی زیرساخت‌های مجازی برای تعیین مرزهای شبکه است تا مسئولیت تنظیم رفتارها در فضای مجازی برعهده دولتی باشد که آن فعالیت‌ها در داخل مرزهای سرزمینی متعارف آن صورت می‌گیرد. حملات سایبری از مبدأ کشورهای توسعه‌یافته علیه اهدافی در کشورهای کمترتوسعه‌یافته باعث شده کشورهای کمترتوسعه‌یافته را برانگیزد تا فناوری‌های دفاع شبکه و حفاظت از امکانات فیزیکی را در اولویت قرار دهند. از سوی دیگر دو نوع مرز شبکه وجود دارد: ملموس و ناملموس؛ مرزهای شبکه ملموس شامل زیرساخت شبکه ملی و سیستم‌های شبکه اصلی مانند امور مالی، مخابرات، حمل‌ونقل و انرژی است. سه لایه مرز شبکه وجود دارد. بیرونی‌ترین لایه «مرز انعطاف‌پذیر» است که شامل ظرفیت اینترنت ملی یک کشور می‌شود. لایه میانی به مرز جغرافیایی شامل زیرساخت‌های سایبری و میدان افکار عمومی داخلی اشاره دارد که از شبکه ملموس فراتر می‌رود؛ زیرا حوزه افکار عمومی را در بر می‌گیرد. درباره کشورهای مورد هدف ایالات متحده، دفاع از این مرز به این معنی است که دولت باید فعالانه در برابر «تهاجم» مبانی و نظریه‌های غربی مانند اومانیسم، لیبرالیسم و سرمایه‌داری ایستادگی کند. جمهوری اسلامی ایران برای تأمین امنیت سایبری و منافع ملی خود و ارتقا به «قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی و برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه»[۱] ناچار به توسعه زیرساخت اطلاعاتی امن و پایدار ملی از طریق ایجاد و توسعه شبکه ملی اطلاعات است.

۱. حکم انتصاب اعضای شورای عالی فضای مجازی توسط رهبر معظّم انقلاب، ۱۳۹۴/۶/۱۴؛ قابل دسترسی در نشانی https://khl.ink/f/30658، ۱۴۰۱/۳/۶.

شکل ۱. شبکه مضامین استراتژی امنیت سایبری جمهوری اسلامی ایران



نتیجه‌گیری

فناوری اطلاعات و ارتباطات یک فضای عمومی بدون مرز را در فضای مجازی پدید آورده که چالش‌های بسیاری برای دولت‌ها پدید آورده است. به تبع در کشور ما نیز حاکمیت با چالش‌ها و خلاهایی در این خصوص روبه‌رو است. رهبر معظّم انقلاب دغدغه سامان‌دهی فضای مجازی را داشته و از طریق راه‌اندازی شورای عالی فضای مجازی و اعطای اختیارات به آن و نیز ارائه الگوی جهاد تبیین در این خصوص برای سیاست‌گذاران و مسئولان سطوح گوناگون حاکمیت راهگشایی کردند. الگوی امنیت ملی سایبری استراتژیک جهاد تبیین نشان می‌دهد که چگونه قابلیت سایبری تهاجمی باید به‌عنوان یک جزء حیاتی در ارائه استراتژی امنیت ملی سایبری کشور عملیاتی شود. تدورین این استراتژی فرایندی پیچیده و حساسی است که با توجه به تنوع کارکردها، بازیگران و کنشگری آنان، باید هماهنگی‌ها و همکاری‌های فرابخشی صورت گیرد تا شاهد تأثیرات مثبت آن در ارتقای امنیت سایبری کشور باشیم.

براساس آنچه در یافته‌های تحقیق تصریح شد، استراتژی امنیت ملی سایبری نظام جمهوری اسلامی ایران به‌عنوان یک سند بالادستی جامع و هماهنگ‌کننده برای رویارویی با تهدیدهای سایبری و حفاظت از منافع ملی، شامل چندین رکن و عامل سازنده می‌شود. اولین رکن و عامل سازنده، «عناصر» است. چارچوب استراتژیک از مهم‌ترین عناصر این سند است که به ترسیم وضعیت مطلوب امنیت سایبری کشور در آینده، مانند تبدیل شدن به یکی از امن‌ترین کشورها در فضای سایبر با هویت ملی منسجم، برخوردار از حقوق و خودکفایی داخلی از طریق تبیین ارزش های اسلامی و نفی ارزش‌های تمدن غرب مانند سکولاریسم می‌پردازد. برخی از بنیان‌های نظری برای رسیدن به این وضعیت، نیازمند تبیین و تحقق هستند؛ مثلاً برای عدم پیدایش شکاف‌های قدرت در سطوح حاکمیت، که مطمح نظر دشمن است، تدبیراندیشی می‌شود و برای تحقق تمدن نوین اسلامی از طریق تقویت فرهنگ مقاومت در برابر سلطه جهانی جبهه کفر، تسهیل تعاملات فرهنگی ملت‌های مسلمان و تلاش برای ارتقای دنیوی و اخروی آحاد بشر زمینه‌سازی می‌شود.

دومین رکن و عامل اصلی استراتژی فوق، «بازیگران» هستند که باید تعریف و شناخت و اشراف اطلاعاتی کاملی درباره آنها داشته باشیم. برای رویارویی با بازیگران تهدید در فضای سایبری مجموعه‌ای از اقدامات و استراتژی‌های جامع و هماهنگ نیاز است. این اقدامات شامل ابعاد فنی (تقویت زیرساخت‌های امنیتی)، قانونی (تدوین و به‌روزرسانی قوانین و مقررات برای مقابله با جرائم سایبری و حمایت از حقوق کاربران)، آموزشی (افزایش سواد رسانه ایرانیان) و همکاری‌های بین‌المللی (مشارکت در توافق‌نامه‌ها و کنوانسیون‌های بین‌المللی برای مقابله با جرائم سایبری و تقویت همکاری‌های امنیتی) است. در این باره خصوصاً همکاری قضایی بین‌المللی برای پیگیری و محاکمه مجرمان سایبری که در کشورهای دیگر فعالیت می‌کنند، نیازمند تقویت است. همچنین در خصوص استرداد مجرمان سایبری، امضای توافق‌نامه‌های استرداد مجرمان سایبری با کشورهای دیگر برای تضمین پیگیری قانونی مجرمان ضروری است.

برای تأمین رکن و عامل سازنده سوم، «گفتمان» باید اقدامات گوناگونی در حوزه‌های تقویت هویت ایرانی اسلامی و ارزش‌های بیانیه گام دوم انقلاب اسلامی انجام شود. گفتمان بیگانه‌ستیزی و تمدن‌سازی و تهدیدزدایی نیز از طریق جهاد تبیین ارتقا یافته و به مبادی اجرایی نزدیک شود. با اجرای این اقدامات، می‌توان به ایجاد یک گفتمان مؤثر و پایدار درباره امنیت ملی سایبری دست یافت و جامعه اسلامی را به سمت ارتقای فرهنگ اصیل ایرانی اسلامی و مقابله با تهدیدهای سایبری هدایت کرد.

چهارمین رکن و عامل سازنده استراتژی امنیت ملی سایبری، «ژئوپلیتیک» است. در عرصه ژئوپلیتیک استراتژی امنیت ملی سایبری، اقدامات مرتبط با تأمین امنیت ملی سایبری باید براساس ایستادگی در برابر نقض حاکمیت ملی، امنیت سایبری فراملی، تضعیف حکمرانی جهانی آمریکا بر فضای سایبر، استقرار شبکه ملی اطلاعات و رسیدن به نقطه خودکفایی سایبری متمرکز باشند. این اقدامات به کشور کمک می‌کنند به‌طور مؤثرتر با تهدیدهای سایبری بین‌المللی مقابله و امنیت و منافع ملی خود را در فضای سایبری حفظ و مقاصد عالی نظام تأمین کند.

منطق مفهومی جهاد تبیین، پیش‌فرض‌ها و مفروضاتی پیشِ‌روی خط‌مشی‌گذاران و متولیان این امر قرار می‌دهد که قابلیت ابتکاربخشی و اثردهی در جهت نظریه‌پردازی و تحلیل روندهای منجر به تولید الگوی مفهومی حکمرانی فضای مجازی کشور خواهد شد. روند تدوین و اجرای سند استراتژی امنیت سایبری فرایندی پیوسته و پویاست، سازمان‌ها و ساختارهای جاری در این روند هیچ‌گاه متوقف نمی‌شوند، بلکه با تکیه بر اقدامات راهبردی، فرایندها و اقدامات جاری خود را تسریع، بهبود یا از طریق مهندسی مجدد، اصلاح و تکمیل می‌کنند. گرچه سیاست‌گذاری فضای مجازی جمهوری اسلامی ایران فرایندی در حال ساخت و تکامل است و متولیان امور خصوصاً شورای عالی فضای مجازی زحمات زیادی در این خصوص متحمل شده‌اند، اما باید این واقعیت را پذیرفت که کشور ما در مقایسه با پیشرفت‌های فناوری و الگوهای حکمرانی برخی از کشورهای پیشرفته و رقیبان منطقه‌ای تأخیر زیادی دارد. برای جبران این تأخیر، ابتدا باید رویکرد کلان نظام اسلامی در سیاست‌گذاری سایبری تعیین شود. چهار رویکرد کلی حکمرانی بر فضای مجازی در جهان رایج است: آمریکا براساس نظام لیبرالیستی رویکرد آزادی ـ کنترل را دنبال می‌کند که در آن، مالکان پلتفرم‌ها و سکوهای جهانی دارای آزادی عمل هستند. در رویکرد اروپایی، حکمرانی بر فضای مجازی از طریق مشارکت دولت و شهروندان در توزیع آزاد اطلاعات و تعاملات اجتماعی شکل می‌گیرد. سومین رویکرد، در آسیای شرقی (ژاپن و کره جنوبی) دنبال می‌شود که به‌صورت توسعه‌ای بیشترین ارزش‌ها و سیاست‌های جهانی پذیرفته می‌شود. در رویکرد چهارم، حکمرانی بر فضای مجازی از طریق سیاست‌های کنترلی و اعمال نظارت تنها در اختیار دولت است و در کشورهایی مانند کوبا، چین و روسیه اعمال می‌شود. تحقق این فرایند و تأمین امنیت ملی سایبری کشور نیازمند مشارکت همه ظرفیت‌ها و بخش‌های کشور خصوصاً مجلس شورای اسلامی است. بر این اساس، نهاد تقنینی کشور باید قوانینی برای عملیاتی شدن این الگو به تصویب برساند. مثلاً دستگاه دیپلماسی کشور در برابر رویکرد چندذی‌نفعی که آمریکا را به‌عنوان حکمران اصلی جهان سایبری به رسمیت می‌شناسد و دولت‌ها نقش فرمایشی دارند، براساس منطق توازن قوا، باید

موظف شود که رویکرد چندجانبه را در عرصه بین‌المللی با کنشگری سازمان ملل متحد یا نهادی تازه‌تأسیس دنبال کند که در آن با انحصارطلبی آمریکا مقابله شود و کشورها قدرت تعیین سیاست‌های ملی و منطقه‌ای خود را داشته باشند. همچنین مرکز ملی فضای مجازی برای تولید و اجرای الگوی استراتژی امنیت ملی سایبری باید با تمرکز بر منطق جهاد تبیین، کنشگری بیشتری داشته باشد تا بتواند ظرفیت‌های کشور را در این عرصه فعال کند؛ زیرا به‌علت مخالفت آمریکا تاکنون هیچ رژیم یا معاهده الزامی درباره سیاست‌گذاری جهانی فضای مجازی و مقابله با جرایم سایبری به وجود نیامده است؛ ازاین‌رو دستگاه دیپلماسی کشور باید در این زمینه فعال‌تر عمل کند. از آنجا که تأمین امنیت سایبری از مهم‌ترین وظایف و کارکردهای حاکمیت است، ایجاد تقارن بین جرم و مجازات با هدف کاهش هزینه‌ای حملات سایبری به زیرساخت‌های کشور ضروری است. برای تولید علوم متناسب با نیاز سیاست‌گذاری فضای مجازی، باید توسعه رشته‌های دانشگاهی و دانش‌های بین‌رشته‌ای از علوم اجتماعی، مهندسی، رایانه‌ای و نانوتکنولوژی در دستور کار متولیان امر قرار گیرد. در زمینه تولید پیامرسان ملی، هماهنگی و همکاری دستگاه‌های داخلی خصوصاً نیروهای مسلح راهگشا خواهد بود. حوزه‌های علمیه نیز ظرفیت‌های زیادی برای سیاست‌گذاری در عرصه تولید نظامات و هنجارهای فضای مجازی منطبق بر منطق مفهومی جهاد تبیین دارند و برای استراتژی امنیت ملی سایبری در عرصه تولید عناصر و گفتمان اثربخش خواهند بود. در این خصوص باید تعاملات تعریف‌شده و منضبطی بین حوزه‌های علمیه و حکمرانان در سطوح گوناگون برقرار شود.

توصیه‌های سیاستی

با توجه به آنچه درباره استراتژی امنیت ملی سایبری در تحقیق حاضر صورت‌بندی شد، می‌توان توصیه‌های سیاستی را در چهار حوزه مدنظر قرار داد. این توصیه‌ها در تمامی یا چند لایه از سطوح حکمرانی از سیاست‌گذاری، قانون‌گذاری، تنظیم‌گری، تسهیل‌گری، اجرا و نظارت قابل پیگیری و تصویب خواهی است.

الف) حوزه مربوط به سیاست‌گذاری

دکترین‌های بازدارندگی سایبری جمهوری اسلامی ایران نیازمند صورت‌بندی و توسعه هستند. این کار از طریق تدوین و اعلان دکترین‌های بازدارندگی سایبری به‌منظور هشدار به دشمنان بالقوه و جلوگیری از حملات سایبری در عالی‌ترین سطوح سیاست‌گذاری نهاد دولت و نیروهای نظامی، امنیتی و انتظامی انجام می‌شود. سیاست راهبردی جمهوری اسلامی ایران در تأمین مصالح ملی خود در فضای مجازی متضمن تهدیدزدایی، ظرفیت‌سازی، مصون‌سازی، نظارت، جرم‌ستیزی، حفظ داده‌ها، تولید محتوا و بازدارندگی مبتنی بر عقلانیت نظام مقدس اسلامی است. بر این اساس کلیه ظرفیت‌های داخلی باید معطوف به کنشگری خردمندانه، پیشرو، آینده‌ساز و الهام‌بخش در مسیر ترسیم الگوی جهانی تمدن نوین اسلامی باشد.

ب) حوزه مربوط به کنشگران

برنامه‌ریزی بلندمدت و میان‌مدت برای الزام بازیگران تهدید و آسیب به پاسخگویی در برابر قوانین و رعایت هنجارهای داخلی؛

استفاده از ظرفیت و تقویت روندسازان در راستای تحقق استقلال سایبری و رفع نیازهای مشروع کاربران داخلی؛

بسیج امکانات و همسوسازی اندیشکده‌ها، اتاق‌های فکر و نهادهای پژوهشی برای رویارویی با آسیب‌پذیری‌های سایبری؛

تدوین برنامه ملی دفاع سایبری و افزایش توانمندی‌های تهاجمی سایبری به‌عنوان ابزار بازدارنده و پاسخگو به حمله‌های سایبری؛

راه‌اندازی و تقویت تیم‌های ملی واکنش اضطراری سایبری با هدف کاهش خسارت حملات سایبری دشمن و اقدامات متقابل بازدارنده؛

سازماندهی برای هنجارسازی حضور مسئولانه کاربران در فضای مجازی.

ج) حوزه مربوط به گفتمان

گفتمان جمهوری اسلامی ایران در فضای سایبری باید مبتنی بر بیگانه‌ستیزی، هژمونی‌سازی و تهدیدزدایی باشد. بر این اساس توصیه‌های سیاستی زیر پیشنهاد می‌شود:

احیا و تقویت گفتمان تمدن نوین اسلامی در منطقه و جهان؛

تقویت گفتمان مقاومت در برابر گسترش هژمونی آمریکا بر جهان؛

توسعه ارزش‌های تمدنی شرق؛

ایجاد یا حضور در ائتلاف‌های تمدنی و جهانی با کشورهای همسو؛

تولید هندسه نوین قدرت در فضای مجازی.

د) حوزه مربوط به ژئوپلیتیک سایبری

مقابله با نقض حاکمیت از طریق قلمروسازی و تنبیه مجرمان؛

ایفای نقش فعال در مجامع جهانی (حضور فعال در کنفرانس‌های بین‌المللی مربوط به امنیت سایبری) برای تقویت نقش و نفوذ کشور در عرصه بین‌المللی؛

ایجاد ظرفیت‌های قانونی و قضایی بین‌المللی؛

راه‌اندازی ائتلاف برای ایجاد رژیم بین‌المللی عدم اشاعه تسلیحات سایبری؛

ایجاد اختلاف بین آمریکا و متحدانش از طریق تقویت گسل‌های منافع ملی اروپا با آمریکا؛

تضعیف حکمرانی واحد آمریکا بر فضای مجازی از طریق تقویت جایگزین‌های شرکت آیکان زیر نظر سازمان ملل متحد یا یک سازمان بین‌المللی خارج از اراده و تأثیرگذاری آمریکا؛

شرکت در گفت‌وگوها و مذاکرات بین‌المللی درباره امنیت سایبری و تدوین سیاست‌ها و راهبردهای مشترک برای مقابله با تهدیدها؛

تقویت و توسعه شبکه ملی اطلاعات و حرکت به سوی خودکفایی سایبری؛

ایجاد مکانیسم‌های تبعیض مثبت[1] نسبت به سکوهای داخلی.

1. Positive Diacimination

منابع

الف) فارسی

امام خامنه‌ای، سید علی، (۱۳۹۷)، ثلاث رسائل فی الجهاد (الامان و الصائبه و المهادنه)، تهران: فقه روز.

باقرپور شیرازی، امیر رضا، (۱۳۹۸)، حکمرانی چندذی‌ربطی فضای مجازی، تهران: پژوهشگاه مرکز ملی فضای مجازی.

پارسانیا، حمید، (۱۳۹۸)، سکولاریسم پنهان، قم: کتاب فردا.

شیخ زاده، محمد و رضا بنی اسد، (۱۳۹۹)، تحلیل مضمون؛ مفاهیم، رویکردها و کاربردها، تهران: لوگوس.

صلح میرزایی، سعید، (۱۴۰۰)، جهاد تبیین در اندیشه حضرت آیت‌الله العظمی خامنه‌ای، تهران: انقلاب اسلامی، هشتم.

فیروزآبادی، سید ابوالحسن، (۱۳۹۶)، فضای مجازی؛ اجتماع و فرهنگ، تهران: علمی و فرهنگی.

کاظمی، احمد، (۱۳۸۴)، امنیت در قفقاز جنوبی، تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

کمیسیون امنیت ملی آمریکا، (۱۳۸۲)، استراتژی امنیت ملی آمریکا در قرن ۲۱، ترجمه جلال دهمشگی و بابک فرهنگی و ابوالقاسم راه‌چمنی، تهران: موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، چاپ سوم.

مصباح یزدی، محمد تقی (۱۳۹۶)، نظریه حقوقی اسلام، ج۱، قم: مؤسسه آموزشی و پژوهشی امام خمینی، چاپ ششم.

مولانا، حمید (۱۳۸۷)، جریان بین‌المللی اطلاعات؛ گزارش و تحلیل جهانی، ترجمه یونس شکرخواه، تهران: دفتر مطالعات و برنامه‌ریزی رسانه‌ها، چاپ دوم (دیجیتالی).

ب) لاتین

Abbott, K. W., Genschel, P., Snidal, D., Zangl, B. (2018), "Competence-control theory: Introducing the governor's dilemma", Paper presented at the International Studies Association Meetings, San Francisco, CA.

Ad'ha Aljunied, S. M. (2019), "The securitisation of cyberspace governance in Singapore", Asian Security.

An, Jing (2017), "Internet Sovereignty is a necessary choice of global cyber governance", Red Flag manuscript, Vol. 4, No. 30-31.

Austin, G. (2017), "Restraint and governance in cyberspace balancing war and justice imperatives", Global Insecurity: Futures of Global Chaos and Governance.

Berman, Paul Schiff (2017), Law and society approaches to cyberspace, Routledge.

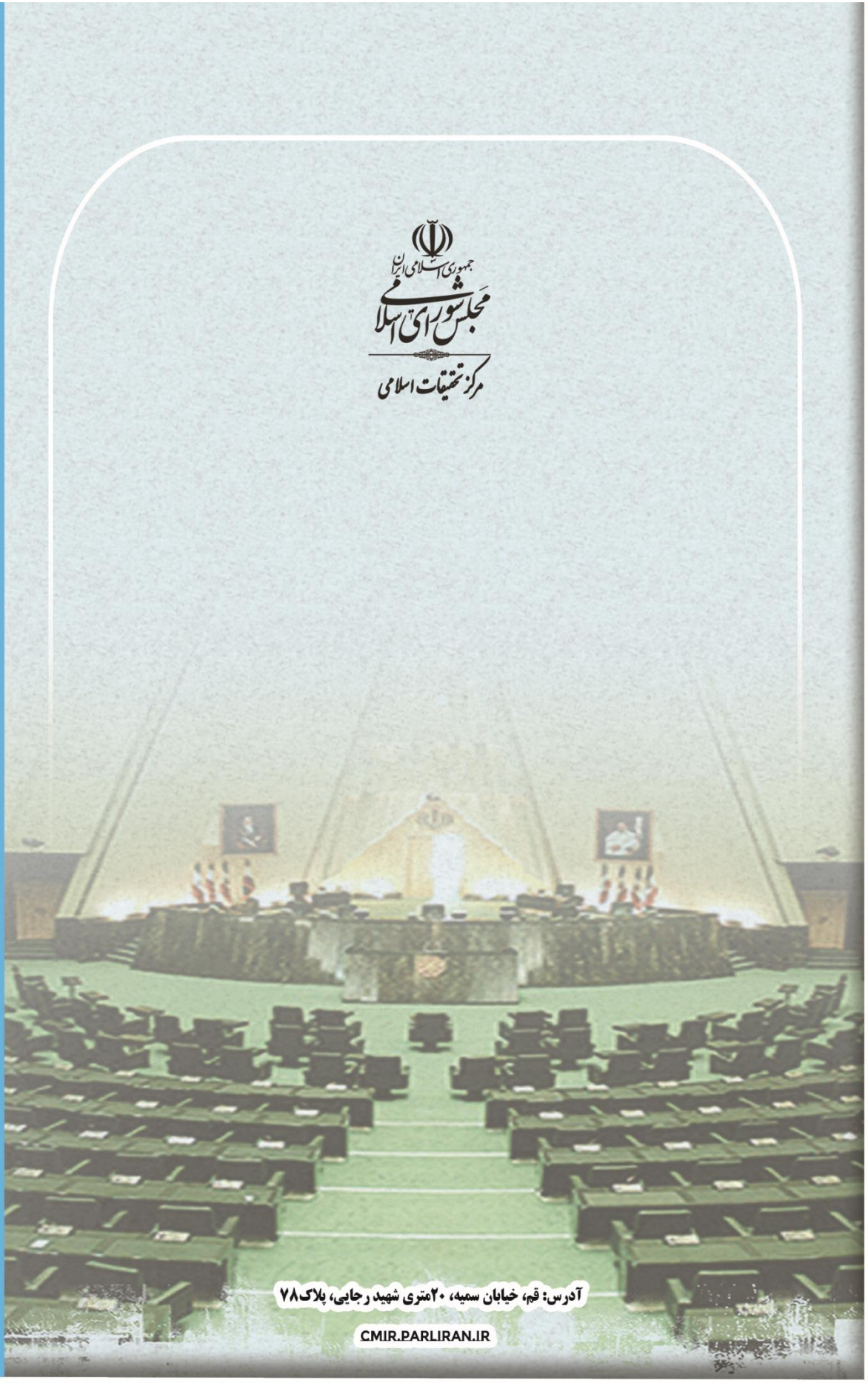
Berr, Jonathan, (2017). "WannaCry" Ransomware attack losses could reach $4 billion. CBS News

Boeke, S, Heinl, C. H., & Veenendaal, M. A. (2015), "Civil-military relations and international military cooperation in cyber security: Common challenges & state practices across Asia and Europe", Paper presented at the 7th International Conference on Cyber Conflict: Architectures in Cyberspace.
Bovens, Mark, Goodin, Robert E., & Schillemans, Thomas (2014). The Oxford Handbook Public Accountability. (M. Bovens, R. E. Goodin, & T. Schillemans, Eds.). Oxford University Press.
Fairclough, G, (2018), Offensive cyber, ecology and the competition for security in cyberspace: The UK's approach, http://podcasts.ox.ac.uk/offensive-cyber-ecology-and-competition-security-cyberspaceuksapproach.
Guven, Durukan (2021), Securitization of Cyberspace Governance and the Right to Privacy: Case of the Us, China, and Icland, Ankara: Publisher Bilkent University.
Karim, Ridoan & Bonhi, Tasmeem Chowdhury. Afroze, Rawnak (2019), "Governance of cyberspace: personal liberty vs. National security", International Journal of Scientific and Technology Research, Volume 8, Issue 11.
Kiggins, Ryan David (2014), "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance", Cyberspace and International Relations: Theory, Prospects and Challenges, Berlin: Springer.
Liaropoulos, Andrew N. (2016), "Reconceptualising cyber security: Safeguarding human rights in the era of cyber surveillance", International Journal of Cyber Warfare and Terrorism, Vol. 6.
Liaropoulos, Andrew N. (2017), "Cyberspace governance and state sovereignty", Democracy and an Open-Economy World Order, Switzerland: Publishing AG.
National Cyber Strategy of the United States of America, 2018.
Nocetti, J. (2015), "Contest and conquest: Russia and global internet governance", International Affairs, Vol. 99.
Peng, Shin-yi (2018), "“Private” cybersecurity standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime", Cornell International Law Journal, Vol. 51, No. 2.
Schön, Donald. A. (2012). Generative metaphor: A perspective on problem-setting in social policy, Published online by Cambridge University Press
Shen, Yi (2016), "Cyber Sovereignty and the Governance of Global Cyberspace", Chinese Political Science Review, Vol. 1, No. 1.
Shin, yi Peng (2018), "“Private” cybersecurity standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime", Cornell International Law Journal, Vol. 51, No. 2.
Smith, B. (2017a). The need for a digital Geneva convention.
Smith, B. (2018), The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack. Microsoft on the issues. https://blogs.microsoft.com/on-the-issues/2017/05/14/needurgentcollective-

action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.000bi5yyf12twdrz104kfp70qrzfk. Accessed 10 May 2018.
UNESCAP: United Nations Economic and Social Commission for Asia and the Pacific (2008), What is Good Governance?, Available at: http://www.unescap.org/ pdd/prs/ProjectActivities/Ongoing/gg/ governance.pdf.
UNGA. (2017), Report of the secretary-general developments in the field of information and telecommunications in the context of international security.
Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018), "Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. Frontiers in Psychology", Front. Psychol, Vol. 9.
Weiss, Moritz & Jankauskas, Vytautas (2019), "Securing cyberspace: how states design governance arrangements", Governance, Vol. 32, No. 2.
West, Sarah (2016), "Globalizing Internet Governance: Negotiating Cyberspace Agreements in the Post-Snowden Era", Conference Paper, TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy.
Wolff, Josephine (2014), "Cybersecurity as metaphor: Policy and defense implications of computer security metaphors", TPRC Conference.
Zhang, Xinbao & Ren, Yan (2017), The theory of Internet Sovereignty and rule of law in cyberapace", Legal Daily, Vol. 28.

۰۳/-/۰۶-۶۲۵

جمهوری اسلامی ایران
مجلس شورای اسلامی
مرکز تحقیقات اسلامی



آدرس: قم، خیابان سمیه، ۲۰متری شهید رجایی، پلاک۷۸
CMIR.PARLIRAN.IR