ترسیم سناریوهای فرا روی شبکه ملی اطلاعات جمهوری اسلامی ایران در افق ۱۴۰۷ با تأکید بر پیامدهای امنیتی

مسلم شیروانی ناغانی،* خلیل کولیوند،** ابراهیم ایجابی*** و مریم حیدری****

نوع مقاله: پژوهشی	تاریخ دریافت: ۱۴۰۱/۱۰/۰۱	تاریخ پذیرش: ۱۴۰۲/۰۵/۱۷	شماره صفحه: ۱۰۸-۶۳

شبکه ملی اطلاعات به‌عنوان راهبردی اساسی در فضای سایبر می‌تواند در اعمال حاکمیت کشور و ارائه خدمات در این بستر، تأثیر قابل‌توجهی بر امنیت ملی داشته باشد که راه‌اندازی این شبکه با سناریوهای مختلفی مواجه خواهد بود. ازاین‌رو پژوهش به‌دنبال ترسیم این سناریوها با تأکید بر پیامدهای امنیتی مستتر در هرکدام از آنها است که با هدف کاربردی و از حیث ماهیت و روش، توصیفی-اکتشافی و برپایه رویکرد کیفی انجام شده و در پی گردآوری داده‌ها به‌منظور مفهوم‌سازی و ارائه تحلیل‌های تجویزی است. جامعه مورد مطالعه پژوهش ۲۰ نفر از اساتید دانشگاه‌های تهران، دانشگاه عالی دفاع ملی و برخی مدیران دولتی شاغل در وزارت ارتباطات و فناوری اطلاعات، مرکز ملی فضای مجازی، سازمان برنامه‌وبودجه و سازمان فناوری اطلاعات کشور هستند. شیوه گردآوری اطلاعات و روش تجزیه‌وتحلیل به‌صورت بررسی کتابخانه‌ای علمی و تخصصی و بهره‌گیری از روش‌های ذهن‌انگیزی و نشست‌های هم‌اندیشی بوده است. روش اصلی تجزیه‌وتحلیل پژوهش برپایه سناریوپردازی و الگوی شبکه جهانی کسب‌وکار است. با استفاده از روش مذکور ۱۵ کنشگر، ۹۲ پیشران و چهار عدم قطعیت شناسایی شد که از برهم‌کنش عدم قطعیت‌ها ۱۶ حالت شناسایی و درنهایت با تأیید خبرگان پنج سناریو باورپذیر ترسیم شد. سناریوهای باورپذیر به نام‌های «خانه امن و هوشمند»، «اسیری و آوارگی»، «کورسوی امید»، «پادشاهی تاریک» و «استمرار دوگانگی» ترسیم شد. این سناریوها می‌تواند مبنایی برای پیش‌نگری درباره پیامدهای امنیتی فراروی شبکه ملی اطلاعات و پیش‌آزمون سیاست‌های کلی نظام در این حوزه قرار گیرد.

کلیدواژه‌ها: شبکه ملی اطلاعات؛ سناریوپردازی؛ پیامدهای امنیتی؛ جمهوری اسلامی ایران؛ نیروی پیشران؛ عدم قطعیت

* استادیار گروه آینده‌پژوهی، دانشگاه بین المللی امام خمینی(ره)، قزوین، ایران؛
Email: shirvani@soc.ikiu.ac.ir

** دانشجوی دکتری آینده‌پژوهی، دانشگاه بین المللی امام خمینی(ره)، قزوین، ایران (نویسنده مسئول)؛
Email: K.koulivand@casu.ac.ir

*** دانشیار گروه آینده‌پژوهی، دانشکده علوم اجتماعی، دانشگاه فرماندهی و ستاد اجا، تهران، ایران؛
Email: e.ejabi@casu.ac.ir

**** کارشناسی ارشد علوم سیاسی، دانشکده اقتصاد و علوم سیاسی، دانشگاه شهید بهشتی، تهران، ایران؛
Email: maryamheydari.sbu@gmail.com

فصلنامه مجلس و راهبرد، سال سی و یکم، شماره یکصدوبیستم، زمستان ۱۴۰۳
doi: 10.22034/MR-2023.5676.5357

مقدمه

در برخی کشورها، گسترش و توسعه فضای مجازی به‌دلیل وابستگی به صاحبان فناوری، بیش از آنکه در راستای تأمین منافع ملی و کسب امنیت ملی باشد تهدیدی جدی علیه آن محسوب می‌شود. این مسئله برای جمهوری اسلامی ایران که برمبنای باورها و ارزش‌های دینی و گفتمان سلطه‌ناپذیری انقلاب اسلامی در جبهه مقابل جهانی‌سازی و استعمار نوین مجازی قرار گرفته، تهدیدهای افزون‌تری را به دنبال دارد. مهم‌ترین فلسفه شکل‌گیری شبکه ملی اطلاعات در مقابل شبکه جهانی اینترنت را می‌توان به مدیریت یا مقابله با تهدیدها و ایجاد فرصت و ارائه خدمات مناسب، امن و کم‌هزینه در جامعه برشمرد.

وابستگی زیرساخت‌های اقتصادی، اجتماعی، سیاسی، فرهنگی و نظامی به فضای مجازی شرایط را به‌گونه‌ای رقم زد که هرگونه چالش در این فضا می‌تواند مؤلفه‌های امنیت ملی را دستخوش تغییر و تحول کند. فضای مجازی علاوه بر اینکه ابزاری برای ارتقای امنیت ملی محسوب می‌شود، بستری برای تهدیدهای امنیت ملی نیز به‌شمار می‌آید. ازاین‌رو امنیت این فضا، مؤلفه مهمی از امنیت ملی محسوب می‌شود. ارتقا و تحکیم امنیت ملی، نیاز اساسی و اصلی‌ترین وظیفه دولت در قلمرو حاکمیتی آن تلقی می‌شود که پیاده‌سازی و پایداری آن مستلزم شناخت محیط به‌خصوص فرصت‌ها و تهدیدهای جاری در آن است. شناخت محیط با همه پیچیدگی‌ها و تغییرات آن، همواره دغدغه مدیریت در سطوح راهبردی بوده و بدون آن منافع ملی در سطوح مختلف به اهداف خود نائل نخواهد شد (Rippy, 2020: 48).

امنیت ملی، وضعیت یا شرایطی است که در آن ارزش‌های اساسی و باورهای دینی، منافع حیاتی، شیوه زندگی ایرانی–اسلامی ارکان و نهادهای حکومتی، اتحاد و انسجام و رفاه ملی به‌طور دائم محافظت شده و به‌صورت مستمر تقویت می‌شود. امنیت ملی امروزه از رایج‌ترین مفاهیم در قلمرو مناسبات جهانی و مباحث سیاسی است. امروزه این مفهوم از عرصه مطالعات دانشگاهی و فعالیت‌های دیپلماتیک پا را فراتر نهاده و به حوزه مطبوعات و رسانه‌های همگانی نیز کشیده شده است (بیات، ۱۳۹۸: ۳۳).

در دنیای فناوری اطلاعات کنونی، نیاز دولت‌ها، سازمان‌ها و افراد به شبکه‌های رایانه‌ای به‌طور گسترده و سریع افزایش یافته است. هرچقدر گستردگی شبکه‌ها بیشتر شود، چالش‌های امنیتی بیشتر شده و به حفظ و امنیت اطلاعات درون شبکه بیشتر احساس نیاز می‌شود، به‌طوری‌که بسیاری از کشورهای صاحب قدرت سایبری و نرم‌افزاری برای مدیریت فضای سایبر خود به طراحی و اجرای شبکه ملی اطلاعات بومی مبادرت کرده‌اند. ازسوی‌دیگر هرچقدر دسترسی و ارتباط به سرویس‌ها یا سایت‌های موردنظر به سرور یا مرکز داده سرویس‌دهنده کوتاه‌تر باشد، سرعت دریافت خدمات برای کاربران بیشتر و تأخیر در دریافت داده کمتر خواهد بود. به همین دلیل بسیاری از کشورها و حتی برخی از ایالت‌ها و مناطق در سطح منطقه‌ای، به راه‌اندازی شبکه داخلی تحت عناوینی همچون شبکه ملی اطلاعات اقدام می‌کنند تا ارتباطات داخلی‌شان سریع‌تر انجام شود (نصرت‌آبادی و همکاران، ۱۳۹۸: ۲۴-۷)

درواقع شبکه ملی اطلاعات به‌منظور کاهش وابستگی به شبکه جهانی اینترنت و ارائه خدمات مناسب، امن و ارزان در فضای مجازی طرح‌ریزی شده که در طراحی آن، ویژگی‌ها و قابلیت‌های خاص بومی مانند استقلال از شبکه جهانی توأم با دسترسی مدیریت شده به آن، نظارت، مدیریت و کنترل در همه سطوح شبکه، سازگاری با فناوری‌های نسل جدید و مورد توجه سیاستگذاران و متولیان راه‌اندازی، مدنظر قرار گرفته است. شکل‌گیری و توسعه شبکه جهانی اینترنت به‌گونه‌ای است که اصولاً مسئله‌ای به نام امنیت ملی برای کشورها مطرح نبوده و حتی بعضی به‌دنبال از بین بردن مرزها هستند و شبکه جهانی را فضایی می‌دانند که مرزهای ملی در آن بی‌معناست، درحالی‌که این طرز فکر را ابداع‌کنندگان این فضا ایجاد کرده‌اند تا در پس آن بتوانند سلطه جهانی خود را پیش برند (رحمانی و همکاران، ۱۳۹۹: ۳۶۲-۳۳۱).

امنیت در شبکه ملی اطلاعات به‌معنای امن بودن آن در تمامی لایه‌ها و تضمین امنیت برای فضای مجازی جاری در کشور است. در سند امنیت فضای تولید و تبادل اطلاعات، امنیت فضای مجازی به‌معنای پیشگیری، دفاع و ارتقای توان بازدارندگی آن

در مقابل هرگونه تهدید یا کاهش آسیب‌پذیری‌ها و حمله‌های سایبری و کنترل شنود برای ردیابی جرائم به‌منظور صیانت از اطلاعات کشور، حراست از حریم خصوصی و سرمایه‌های مادی و معنوی معرفی شده است. براساس این سند راهبردی، امنیت در لایه فیزیکی، مسیریابی، مراکز داده و غیره باید در بستری امن صورت گیرد و تبادل اطلاعات خارجی و دسترسی به اینترنت نیز برای کاربران به‌صورت حفاظت شده و تعاملی انجام شود. بنابراین در امنیت شبکه ملی اطلاعات همه مکانیسم‌های امنیتی مانند جامعیت داده، محرمانگی، احراز هویت، کنترل دسترسی، انکارناپذیری و دسترس‌پذیری مورد توجه قرار گرفته است.

ایجاد و راه‌اندازی شبکه ملی اطلاعات متأثر از مؤلفه‌هایی در ابعاد اقتصادی، فرهنگی–اجتماعی، سیاسی، نظامی و فناورانه است که هرکدام از ابعاد مطرح شده، سناریوهایی را برای شبکه رقم می‌زند و این سناریوها نیز پیامدهای امنیتی را در خود خواهد داشت (Yoon, 2016: 41-59). برنامه‌ریزی بلندمدت برای شبکه ملی اطلاعات و جلوگیری از غافلگیری در برابر پیامدهای امنیتی ناشی از آن، مستلزم شناسایی سناریوهای پیش روی شبکه ملی اطلاعات است. ازاین‌رو پژوهش حاضر به‌دنبال تحقق این هدف است.

با توجه به اینکه هدف از این پژوهش، ترسیم سناریوهای فراروی شبکه ملی اطلاعات ایران در افق ۱۴۰۷ با تأکید بر پیامدهای امنیتی مستتر در هر سناریو است، بدین‌منظور ضروری است به پرسش‌های زیر پاسخ داده شود:

- کنشگران تأثیرگذار بر آینده شبکه ملی اطلاعات در ایران کدامند؟
- چه گزینه‌هایی به‌عنوان عوامل کلیدی مؤثر بر شبکه ملی اطلاعات شناخته می‌شود؟
- نیروهای پیشران مؤثر بر شبکه ملی اطلاعات در ایران کدامند؟
- عدم قطعیت‌های کلیدی مؤثر بر شبکه ملی اطلاعات در ایران کدامند؟

شایان ذکر است علت در نظر گرفتن افق ۱۴۰۷ برای سناریوپردازی در این پژوهش، پایان دهه اول بیانیه گام دوم انقلاب به‌عنوان مهم‌ترین سند بالادستی کشور است که در سال ۱۳۹۷ ابلاغ شده است.

۱. پیشینه پژوهش

بررسی‌های انجام شده در منابع فارسی، نشان داد پژوهشی با موضوع مدنظر این تحقیق انجام نشده، اما در منابع لاتین و در پایگاه‌های اطلاعاتی و نشریات معتبر علمی، مواردی شناسایی شد که به‌نوعی با پژوهش مرتبط بودند که این منابع نیز همه متغیرها و ابعاد این پژوهش را با هم بررسی نکرده و فقط به برخی از مؤلفه‌های مدنظر محققان توجه شده است. در ادامه پژوهش‌های مرتبط در جدول ۱ لیست شده است.

جدول ۱. پیشینه‌های مرتبط با موضوع

محقق / محققان	سال	عنوان پژوهش	یافته‌ها
عیوضی، رضایی و محمدی خانقاهی	۱۴۰۰	نقش شبکه ملی اطلاعات در تحکیم استقلال و امنیت ملی در گام دوم انقلاب اسلامی	هدف این پژوهش، تبیین نقش شبکه ملی اطلاعات در تحکیم استقلال و امنیت ملی در گام دوم انقلاب اسلامی است. بنابراین سؤال اصلی پژوهش عبارت است از: «نقش شبکه ملی اطلاعات در تحکیم استقلال و امنیت ملی در گام دوم انقلاب اسلامی چیست؟». برای انجام این پژوهش، از روش تحلیل اسنادی و برای گردآوری داده‌ها از ابزار فیش‌برداری بهره گرفته شده است. براساس یافته‌های پژوهش، تحقق شبکه ملی اطلاعات می‌تواند زمینه مصونیت ذخایر اطلاعات ملی، ارتقای توان بازدارندگی در مقابل تهدیدهای سایبری، حراست از حریم خصوصی و آزادی‌های مشروع، توسعه پدافند غیرعامل و ... شود. مهم‌تر از همه، تضمین استقلال، امنیت کشور و تحقق حاکمیت در فضای سایبر است که این امر وابستگی کلیدی به تحقق شبکه ملی اطلاعات در سه بعد زیرساخت، سرویس و محتوا دارد.

محقق / محققان	سال	عنوان پژوهش	یافته‌ها
عبیری و همکاران	۱۳۹۹	تبیین نقش شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدهای فضای مجازی	این پژوهش با هدف تبیین فرصت‌ها و تهدیدهای شبکه ملی اطلاعات و نقش این شبکه در مدیریت فضای مجازی کشور تدوین شده است. روش انجام پژوهش به‌صورت آمیخته اکتشافی و روش گردآوری داده‌های آن توصیفی بوده است. پژوهشگران عنوان می‌کنند که شبکه ملی اطلاعات دارای فرصت‌هایی ازجمله تسریع در عرضه محتوا، اطلاعات و دانش، تسهیل و فراگیری خدمات الکترونیکی، کاهش هزینه‌ها، افزایش سلامت اداری، ایجاد و استفاده از موتور جستجوی داخلی، امنیت شبکه‌های اجتماعی و رایانش ابری بومی است که ایجاد و ارتقای شبکه ملی اطلاعات به امنیت اطلاعات کاربران، حفظ حریم خصوصی و قطع وابستگی به کشورهای بیگانه منجر می‌شود. سؤال اصلی پژوهش این است که شبکه ملی اطلاعات چه نقشی در مدیریت فرصت‌ها و تهدیدهای فضای مجازی کشور خواهد داشت؟
همایون و هاشمی	۱۳۹۶	جایگاه شبکه ملی اطلاعات در سپهر سیاست فرهنگی جمهوری اسلامی ایران	در این پژوهش به نیازهای فرهنگی نشئت‌گرفته از سیاست‌های کلی مربوط به شبکه ملی اطلاعات پرداخته می‌شود که لزوم طراحی و پیاده‌سازی این شبکه را یادآور می‌شود و نیز نقشی که این طرح می‌تواند در پیشبرد اهداف و سیاست‌های فرهنگی کشور ایفا کند. اهمیت این مطالعه در آن است که اسناد و سیاست‌های پشتیبان شبکه ملی اطلاعات در این حوزه و به‌طورکلی زمینه سیاستی این طرح نشان داده می‌شود. روش انجام پژوهش به‌صورت کیفی است و یافته‌ها نشان می‌دهد که سیاست‌های مربوط به راهبری و مدیریت راهبردی فضای مجازی در سطوح ملی و فراملی و درنهایت سیاست‌های ناظر به ایجاد نظام جامع اطلاعات و ارتباطات در کشور است که مجموعه این سیاست‌ها ازیک‌طرف اهمیت راه‌اندازی شبکه ملی اطلاعات را در کشور یادآور می‌شود و ازطرف‌دیگر گویای نقش محوری این شبکه در «زمینه‌سازی» و «فراهم کردن بسترهای لازم» برای پیشبرد سیاست‌های فرهنگی کشور در عرصه فضای مجازی است. سؤال اصلی پژوهش این است که جایگاه شبکه ملی اطلاعات در سپهر سیاست فرهنگی جمهوری اسلامی ایران چگونه است؟

محقق / محققان	سال	عنوان پژوهش	یافته‌ها
لیخاچف[1]	۲۰۱۵	بیست‌ویکمین سالگرد شبکه ملی روسیه (رونت)[2]	این پژوهش با هدف تبیین ضرورت‌های برقراری شبکه ملی اطلاعات روسیه (رونت) به نوعی به‌صورت کیفی انجام شده است. پژوهشگر در این تحقیق به معرفی شبکه ملی اطلاعات روسیه و تأثیر آن بر فضای سایبر حاکم بر روسیه پرداخته و عنوان می‌دارد درصد چشمگیری از حریم خصوصی کاربران در روسیه تحت برقراری این شبکه از امنیت و سلامت بالایی برخوردار شده است.
اسلان بیکف[3]	۲۰۱۷	معرفی ساختار شبکه داخلی روسیه	پژوهشگر در این تحقیق به بایدها و نبایدها و ضرورت‌های برقراری شبکه ملی داخلی روسیه در فضای داخلی سازمان‌ها و نهادهای روسیه پرداخته و ضمن تشریح ساختارهای حاکم بر این شبکه، میزان علاقه‌مندی و تمایلات شهروندان در استفاده از این شبکه را بررسی کرده است. هدف اصلی محقق از انجام این پژوهش معرفی و شناسایی ساختار و زیرساخت‌های شبکه ملی اطلاعات روسیه است.
رحمانی و همکاران	۱۳۹۹	شناسایی و رتبه بندی عوامل مؤثر بر شبکه ملی امن اطلاعات جمهوری اسلامی ایران	هدف اصلی این تحقیق، شناسایی و رتبه‌بندی عوامل مؤثر بر شبکه ملی امن اطلاعات جمهوری اسلامی ایران است. مهم‌ترین شاخص‌ها و متغیرهای مؤثر در شبکه ملی اطلاعات کشور با روش کیفی تحلیل مضمون استخراج شده و با توجه به ماهیت و نقش آنها، این عوامل در ابعاد امنیتی، فناورانه و مدیریتی طبقه‌بندی شده است. یافته‌ها بیانگر این است که رتبه‌بندی عوامل مؤثر بر شبکه ملی امن اطلاعات تأثیر تقریباً یکسانی از نظر میانگین دارد و تفاوت معناداری با یکدیگر ندارد.

با توجه به بررسی پیشینه پژوهش، نکات زیر مشاهده می‌شود:

- توجه ویژه برخی دولت‌ها و کشورها به اهمیت شبکه ملی اطلاعات با توجه به مقوله‌های امنیتی-اقتصادی آن؛
- ضرورت ایجاد شبکه ملی اطلاعات کشور در جهت پیش‌بینی، نظارت و استقرار حکمرانی مبتنی‌بر فضای مجازی؛

1. Likhachev
2. Runet
3. Aslanbekov

- اهمیت نظارت بر داده‌های جاری شبکه در راستای استحکام امنیت ملی؛
- اهتمام برخی دولت‌ها به تدوین سند ملی امنیت داده در قالب شبکه ملی اطلاعات.

موارد زیر را می‌توان به‌عنوان ضرورت‌های انجام این پژوهش برشمرد:

- لحاظ کردن نگاه آینده‌نگارانه در سیاستگذاری و برنامه‌ریزی بلندمدت فضای مجازی کشور؛
- توجه به تهدیدها و فرصت‌های مطرح در حوزه فضای مجازی با توجه به بستر راه‌اندازی شبکه ملی اطلاعات؛
- بررسی میزان اثر شبکه ملی اطلاعات در ایجاد زمینه‌های لازم برای توسعه علمی کشور؛
- شناسایی شاخص‌های امنیتی شبکه ملی اطلاعات و پایین آوردن ریسک ضربه‌پذیری و مقابله با تحریم‌های احتمالی؛
- برآورد میزان ایجاد امنیت و مصون ماندن اطلاعات از حمله‌های سایبری؛
- شناسایی و معرفی میزان اثر شبکه ملی اطلاعات در ایجاد زمینه‌های نوین شغلی و افزایش تولید ناخالص ملی؛
- تعیین نقش شبکه ملی اطلاعات در بومی‌سازی فناوری‌های سخت‌افزاری و نرم‌افزاری با تکیه بر نرم‌افزارهای متن باز و توسعه معماری باز.

همچنین گفتنی است نوآوری این پژوهش در این است که برای نخستین بار با رویکرد سناریوپردازی، ترسیم وضعیت فضای سایبری کشور را در صورت تحقق یا عدم تحقق شبکه ملی اطلاعات رقم می‌زند. در پژوهش‌های سابق که با موضوع شبکه ملی اطلاعات مربوط بوده، هیچ‌یک به شناسایی کنشگران و نیروهای پیشران وارد بر شبکه ملی اطلاعات نپرداخته‌اند، اما رویکرد سناریوپردازانه این تحقیق ایجاب کرد که این موارد شناسایی و احصا شود.

۲. ادبیات نظری

امروزه هیچ کشوری در تأمین امنیت ملی تنها به مقابله با تهدیدهای نظامی بسنده نمی‌کند، بلکه انواع تهدیدهای سیاسی، اقتصادی، فرهنگی، روانی، رسانه‌ای، فضای مجازی و ... را در نظر می‌گیرد. امنیت ملی درواقع ازیک‌سو به شرایط تأمین و حفظ موجودیت نظام درون و بیرون مرزها و ازسوی‌دیگر به توانایی‌های نظام در محیط درونی و پیرامونی توجه دارد. در این سطح، وجوه امنیت دفاعی–نظامی بوده و منشأ بروز تهدید، داخلی و خارجی است و حوزه تحلیل آن هم محیط ملی و فراملی و واحد تحلیل آن نیز دولت–ملت در نظام بین‌الملل است. در امنیت ملی محور تحلیل، عبارت است از منافع و مصالح ملی و همچنین بحران‌ها و تهدیدهای ناشی از ترتیبات قدرت در جهان، منطقه و محیط داخلی. منظر نگرش در این سطح شامل موارد امنیتی، دفاعی و نظامی بوده و هدف آن مصونیت منافع ملی است. در این سطح، وظیفه کلی حفاظت با نیروهای مسلح است. با گسترش اینترنت در کنار خدمات گسترده آن، تهدیدهای متعددی از بستر آن خارج شده که در موارد عدیده‌ای این تهدیدها بر امنیت ملی اثرگذارند (بیات، ۱۳۹۸: ۳۵).

تحول در مفهوم امنیت ملی برمبنای خارج شدن آن از سایه تمام‌عیار تهدید نظامی و نقش‌یابی بیشتر مؤلفه‌های جدید است. در یک تعریف جامع از امنیت ملی که امروزه متناسب با وضع نوین جهانی است می‌توان گفت امنیت ملی دستیابی هر ملت به امکانات، توانمندی و ابزاری است که بتواند با تمسک به آنها از تهدیدهای خارجی و داخلی در امان باشد؛ سلطه سیاسی، اقتصادی، فرهنگی و نظامی بیگانه را دفع کند؛ محافظ ارزش‌های حیاتی خود در صلح و جنگ، دفاع و حراست باشد؛ از موجودیت کشور و تمامیت ارضی آن محافظت کند و سیر صعودی در افزایش قدرت و توان ملی در عرصه‌های مختلف داشته باشد و در راه پیش‌برد امر توسعه متوازن و پویا و تحکیم وحدت ملی و ارتقای سطح مشارکت سیاسی جامعه موفق باشد (همان: ۳۶).

با گذشت حدود چهل سال از ظهور اینترنت، کشورهای مختلف برای حاکمیت بر عرصه فضای مجازی ملی خود به‌صورت حداقلی به سیاستگذاری‌های فناورانه،

اقتصادی، فرهنگی، اجتماعی و سیاسی اقدام کرده‌اند و در آینده نیز در حوزه‌های گوناگون برای مسائل مختلف مرتبط با فضای مجازی این سیاستگذاری‌ها را انجام خواهند داد (Shark, 2015: 13-42).

در زمینه سیاست‌ها و برنامه‌های فرهنگی و اجتماعی کشورها در قبال فضای مجازی، از یک نگاه کلان می‌توان به سیاست‌های سلبی و ایجابی تقسیم کرد. سیاست‌های سلبی برنامه‌هایی معطوف به حذف، کنترل و نظارت است و سیاست‌های ایجابی را می‌توان برنامه‌های معطوف به تولید محتوا، مدیریت محتوا، برنامه‌های دیجیتالی‌سازی اطلاعات و دسترس‌پذیر ساختن اطلاعات و محتوا در شبکه اینترنت نام برد (هاشمی و همایون، ۱۳۹۶: ۱۶۱-۱۱۹). براساس مدل چهار لایه‌ای فضای مجازی که مرکز ملی فضای مجازی در سال ۱۳۹۶ منتشر کرده است، شبکه ملی اطلاعات به‌عنوان بستر یا زیرساخت این مدل لحاظ شده و امنیت برای این شبکه در لایه‌های زیرساخت، خدمات و محتوا مورد بررسی قرار گرفته که برای هر لایه نیز شاخص‌های امنیتی احصا شده است. بر این اساس امنیت در لایه زیرساخت شامل امن بودن اجزای این لایه مانند تجهیزات ارتباطی، سوئیچینگ، مسیریاب‌ها، مراکز داده و تجهیزات امنیتی است که پیش‌نیاز امنیت در لایه خدمات و محتوا است. در لایه خدمات، امنیت خود خدمات، ارائه امنیت به‌عنوان خدمت، خدمات مربوط به احراز هویت، جامعیت و محرمانگی و همچنین امنیت مواردی مانند سیستم عامل، منابع و بانک‌های اطلاعاتی، خدمات، پورتال‌ها، شبکه‌های اینترانتی و اختصاصی، پروتکل‌های ارتباطی، رابط‌ها و میان‌افزارهای لازم برای تعامل سیستم‌ها، نرم‌افزارها، پردازش‌ها و برنامه‌های کاربردی مطرح است (عصاریان‌نژاد و شریفی، ۱۳۹۵: ۳۳-۹)

توجه به این نکته ضروری است که امنیت به توان دولت‌ها و جوامع برای حفظ هویت مستقل و تمامیت عملی آن مربوط می‌شود. ضمن اینکه امنیت نمود مستقیم تهدیدهای عینی نیست بلکه تلقی امنیت به‌عنوان یک عمل گفتمانی است و این در حالی است که به‌جای افزایش امنیت، باید به امنیت‌زدایی از موضوع‌های امنیتی توجه کرد (عبداله‌خانی، ۱۳۸۳: ۴۸).

ازاین‌رو بخش اعظمی از کشورهای پیشرفته یا درحال‌توسعه به‌منظور مدیریت بهینه کشور و دسترسی به خدمات و اطلاعات به طرح‌ریزی و پیاده‌سازی زیرساخت ارتباطی و مستقل از اینترنت با مدیریت داخلی اقدام کرده‌اند. مثلاً در کره‌جنوبی طرح تجمیع حکمرانی الکترونیکی و ارتباطی بخش همگانی با ایجاد بستر ۵۰ مگابیتی اجرا شده است و در آمریکا یک شبکه عمومی برای دسترسی مقرون‌به‌صرفه به‌منظور حدود ۱۰۰ میلیون خانوار در نظر گرفته شده است. استرالیا یکی دیگر از پیشگامان توسعه شبکه پهن باند ملی[1] است، که در این کشور خدمات پهن‌باند و پرسرعت با ترکیبی از روش‌های مختلف مخابراتی ارائه می‌شود (Lindwall, 2017: 41-59). در کشور چین از موتور جستجو و شبکه‌های پیام‌رسان بومی استفاده می‌شود. یکی از اهداف کشور چین داشتن فناوری ابداعی و رقابت صنعتی مطابق با استانداردهای پیشرو سیستم و شبکه با امنیت اطلاعات بالا است (شهیر، ۱۳۹۶: ۸۷).

در مورد تأثیر فناوری اطلاعات بر امنیت ملی، با دو دسته از مطالعات روبه‌رو هستیم؛ دسته نخست، مطالعاتی است که بر تأثیر فناوری اطلاعات بر امنیت ملی از بُعد مفهومی و بدون در نظر گرفتن شرایط سیاسی‌ـامنیتی خاص هر کشور به آن پرداخته؛ به‌عبارت‌دیگر، این دسته از منابع، بیشتر به دنبال یافتن نگرش امنیتی بهتر درخصوص فناوری‌ها است. این‌گونه منابع، نگاهی تجویزی دارد و غالباً نمی‌تواند تأثیر ملموسی را که ظهور این فناوری‌ها در بدو ورود به یک جامعه دارد، نشان دهد؛ هرچند چنین منابعی در تدوین سیاست‌های امنیتی با محوریت امنیت شهروندان یا امنیت انسانی، در تقابل با محوریت دولت و تبدیل تهدیدهای آن به فرصت، سودمند است. دسته دوم، مطالعاتی است که عمدتاً بر کشور یا کشورهایی مشخص تمرکز دارد و تأثیرات فناوری‌ها را بر امنیت ملی آنها بررسی می‌کند (همایون و هاشمی، ۱۳۹۶: ۱۳۲-۱۱۳).

امنیت ملی در حوزه سایبری، درواقع کارکرد یکپارچگی و انسجام نظام را عهده‌دار است، ازاین‌رو درخصوص امنیت سایبر اختلاف بر سر مفهوم آن وجود دارد. برخی

1. National Broadband Network (NBN)

امنیت سایبر را یکی از ابعاد امنیت ملی دانسته و در کنار ابعادی مانند اجتماعی و اقتصادی قلمداد کرده‌اند. برخی دیگر امنیت سایبری را هم‌سنگ امنیت ملی دانسته‌اند. توجه به شأن و جایگاه امنیت سایبری در زندگی اجتماعی و کارکرد آن در سیاست‌های اقتصادی، اجتماعی و فرهنگی دولت‌ها به‌نحو فزاینده در حال رشد است. امنیت سایبری در حوزه داخلی بروز نظری و عملی عمده‌ای پیدا کرده و در این حوزه میزان حضور این بعد از امنیت در بستر جامعه و در سطح بهره‌مندی شهروندان هر کشور به‌عنوان حقی مهم در زندگی اجتماعی در نظر گرفته می‌شود (بیات، ۱۳۹۸: ۵۳).

پنه‌لوپه هارتلند[1] معتقد است که امنیت ملی یعنی توانایی هر ملت برای تحقق موفقیت‌آمیز منافع ملی خود در هر جای دنیا به‌نحوی‌که می‌بینند. مایکل لوه[2] امنیت ملی را شامل سیاست دفاع ملی و اقدام‌های غیرنظامی دولت برای تضمین ظرفیت کامل بقای خود به‌منظور اعمال نفوذ و حصول اهداف داخلی و بین‌المللی می‌داند. جیاکومو لوچیان[3] امنیت ملی را توانایی رویارویی در مقابل تجاوز از خارج تعریف می‌کند (همان: ۳۳).

امنیت ملی با توجه به اینکه با ارزش‌های اساسی و منافع حیاتی هر کشور ارتباط پیدا می‌کند، حائز اهمیت است (عبداله‌خانی، ۱۳۸۳: ۶۵). آنچه مسلم است، اینکه امنیت مورد نظر در این دسته از مطالعات، به‌طور کامل، قابل انطباق با امنیت ملی کشورهای جهان سوم، ازجمله ایران نیست؛ زیرا وابستگی زیرساخت‌ها در کشورهای اخیر، به گستردگی کشورهای توسعه‌یافته نبوده و نمی‌تواند تهدیدی جدی برای این کشورها دربر داشته باشد؛ اما گروهی دیگر، تأثیر فناوری اطلاعات را در کشورهای جهان سوم مورد مطالعه قرار دادند. در این‌گونه منابع، تمرکز اصلی بر ابعاد سیاسی، اجتماعی و فرهنگی امنیت ملی است که تفاوت آشکاری با مطالعات نظامی‌محور در گروه اول دارد (همایون و هاشمی، ۱۳۹۶: ۱۳۲-۱۱۳).

---

1. Penelope Hartland
2. Michael Loh
3. Giacomo Lucian

البته گفتنی است کشورهای پیشرو برای شناسایی تهدیدها و فرصت‌های آینده فضای سایبر در سطوح مختلف راهبردی و عملیاتی، سناریوهای مختلفی را متناسب با نیازمندی‌ها و الگوهای حاکم بر کشورهای خود طراحی کرده‌اند. برای نمونه مؤسسه تحقیقاتی رند،[1] مرکز اینترنت و جامعه برکمن[2] و همچنین مؤسسه تحقیقاتی اسکریپس[3] ازجمله مؤسسه‌های آمریکایی متعلق به نهادهای امنیتی - نظامی است که نسبت به ارائه تصویری از آینده فضای مجازی و آینده مطلوب خود اقدام کرده است (بیات و فتحیان، ۱۴۰۰: ۱۰۶-۹۰).

یکی از مباحث مهم امنیت در شبکه ملی اطلاعات، امن بودن شبکه است. شبکه ملی اطلاعات در صورتی می‌تواند امنیت فضای مجازی کشور را تأمین کند که در همه اجزا و حوزه‌های کاربردی خدمات و محتوا، از سطح مطلوب امنیتی برخوردار باشد؛ در غیر این صورت، ناامن بودن این شبکه، تهدیدهای امنیتی را در سطوح مختلف کاربران، جامعه و دولت ایجاد خواهد کرد. براساس اسناد بالادستی، راه‌اندازی شبکه ملی اطلاعات، گامی مهم و حیاتی برای بهره‌برداری از فرصت‌ها و قابلیت‌های فضای مجازی لحاظ شده است. این شبکه عملاً امکان صرفه‌جویی اقتصادی، توسعه فضای کسب‌وکار، افزایش سرعت دسترسی کاربران به منابع داخلی و تحقق دولت الکترونیک را فراهم خواهد کرد که تحقق این اهداف به امنیت این شبکه وابسته است. از مهم‌ترین پیامدهای امنیت شبکه ملی اطلاعات از منظر راهبردی می‌توان به موارد زیر اشاره کرد:

- جلوگیری از قطع ارتباطات اینترنتی به‌خصوص ارتباطات داخلی توسط بیگانگان؛
- جلوگیری از تحلیل اطلاعات توسط بیگانگان به سبب عدم خروج اطلاعات داخلی به بیرون از کشور؛
- جلوگیری از ذهن‌خوانی، داده‌کاوی، ذائقه‌سنجی و رفتارشناسی کاربران ایرانی

1. RAND Corporation
2. Berkman Center for Internet and Society
3. Scripps Research Institute

ازسوی کشورهای بیگانه به‌خصوص از طریق شرکت‌های بزرگ و غول‌های فناوری دنیا؛

- عدم وابستگی به بیگانگان در ارتباطات داخلی؛
- جلوگیری از گمنامی و فعالیت‌های پنهانی افراد در شبکه ملی اطلاعات؛
- کاهش جرائم و تخلفات به سبب احراز هویت کاربران در شبکه ملی اطلاعات؛
- جلوگیری از فعالیت‌های اقتصادی خارج از قوانین و مقررات کشور؛
- شناسایی متخلفان و مجرمان سایبری در شبکه ملی اطلاعات؛
- جلوگیری بیگانگان از خروج اطلاعات و سرقت آن؛
- ایجاد مدیریت مستقل برای ارتباطات داخل و خارج از کشور؛
- جلوگیری از حمله‌های سایبری کشورهای بیگانه؛
- جلوگیری از تهاجم فرهنگی، تبلیغات اغواگرانه، ترویج پروپاگاندا، عملیات روانی و نفوذ اجرایی؛
- توانایی سازمان‌دهی تهدیدهای سایبری رخ داده شده علیه جمهوری اسلامی ایران؛
- جلوگیری از ترویج یأس و ناامیدی، ایجاد تفرقه و اختلاف‌های قومی و مذهبی در بین آحاد جامعه و تغییر بنیان‌های اعتقادی، اخلاقی و فرهنگی از طریق فضای سایبر؛
- مدیریت هوشمند انتشار و دسترسی به اطلاعات الکترونیکی در شبکه ملی اطلاعات؛
- ارتقای سطح دانش کارشناسان و متخصصان داخلی؛
- جلوگیری از خروج ارز و دارایی‌های کشور به خارج از کشور (عبیری و همکاران، ۱۳۹۹: ۴۵۰-۴۲۱).

امروزه دولت‌ها و حکومت‌هایشان می‌توانند از اهرم‌ها و سیاست‌های مختلفی برای شکل دادن و بهره‌برداری از سیستم‌های داده داخلی و شبکه ملی اطلاعات استفاده کنند. این موارد می‌تواند شامل مقررات مربوط به حریم خصوصی و محافظت از داده‌ها، سیاست‌های اقتصادی مبتنی‌بر استفاده از داده‌ها برای امنیت ملی، نظارت‌های قانونی و به اشتراک‌گذاری داده‌های بخش دولتی باشد. رویکردهای منطقه‌ای برخی از کشورها در این خصوص به توسعه ارگانیک با توجه به هنجارهای موجود تمایل دارد که با اهداف ژئوپلیتیک سازگار با آینده باشد. در یک دسته‌بندی کلی می‌توان رفتارهای سه منطقه جغرافیایی متفاوت را به شکل زیر تفکیک کرد:

دولت چین، کنترل قوی شهروندان همراه با محدودیت در انتقال بین‌المللی، امنیت اقتصادی و اجتماعی ملی را در اولویت شبکه ملی خود قرار داده است. چین با کمک سیستمی به نام «سیستم اعتباری-اجتماعی ملی»[1] اهداف تعریف شده در امنیت ملی خود را شامل جمع‌آوری داده‌های مالی، انتظامی، تجاری، رسانه‌های اجتماعی و سایر داده‌ها به‌منظور نظارت بر انطباق شهروندان با تعهدات شهروندی، تعیین مجازات و تشویق برخی رفتارها، مدیریت می‌کند (Tanner, 2017: 56).

اتحادیه اروپا با اندکی تفاوت در بین برخی کشورهای عضو، رویکردهای امنیت ملی، حقوق شهروندی و رقابت در بازار داخلی را در اولویت قرار داده است. ایجاد سپر حریم خصوصی اتحادیه اروپا، توسعه قوانین و مقررات مربوط به داده‌ها مانند مقررات جامع عمومی حفاظت از داده‌ها ازجمله اقدام‌هایی بوده که به‌نظر می‌رسد پیرامون حقوق و مسئولیت‌های جدید اعمال شده این‌گونه آیین‌نامه‌ها درخصوص شبکه‌های ملی به‌طور گسترده مورد استفاده قرار گرفته است(Scott and Cerulus, 2018: 34).

ایالات متحده آمریکا، مطابق با مواضع اقتصادی گسترده‌تر خود، رویکرد کاملاً مداخله‌جویانه‌تری نسبت به داده‌ها اتخاذ کرده و به‌طور فعال در تلاش است از شبکه ملی خود در حمایت از امنیت ملی استفاده کند، اگرچه در حال حاضر قانون جامع حفاظت از داده‌های فدرال وجود ندارد اما قوانینی مربوط به بخش‌های خاص وضع

1. Chinese Social Credit System

شده و به‌رغم وجود تفاوت‌هایی در روش پیاده‌سازی قوانین فوق در بین ایالت‌های مختلف، با توجه ویژه‌ای از این قوانین پشتیبانی می‌شود(Noordyke, 2020: 69).

شبکه ملی اطلاعات یکی از موضوع‌های راهبردی و مهم است که در صورت تحقق، می‌تواند امنیت و آرامش را برای جامعه به ارمغان آورد و بی‌توجهی به آن می‌تواند امنیت ملی کشور را به چالش کشد. در شرایط کنونی به‌دلیل عجین شدن زندگی مردم با فضای مجازی و نقش پررنگ شبکه ملی اطلاعات در ارتقای امنیت و آسایش مردم، شناسایی سناریوهای پیش روی شبکه ملی اطلاعات از منظر امنیتی، می‌تواند به ارتقای حاکمیت ملی در جمهوری اسلامی ایران منجر شود. اگر جمهوری اسلامی ایران نیز بخواهد از ارزش‌های اساسی، زیرساخت‌های حیاتی و اطلاعات ارزشمند ملی در جهت حفظ و ارتقای امنیت ملی خود محافظت کند و به‌عنوان بازیگری فعال به ایفای نقش بپردازد؛ باید تصویر درستی از وضعیت خود، محیط پیرامونی و عوامل تأثیرگذار بر آینده داشته باشد تا بتواند ساخت آینده را در جهت تحقق اهداف ملی برنامه‌ریزی کند که این مستلزم شناخت از آینده‌های محتمل و روندهای تأثیرگذار بر آن است.

۳. تعاریف نظری

امنیت ملی را نخستین بار «والتر لیپمن»[1] محقق و نویسنده آمریکایی مطرح کرد، وی مفهوم امنیت ملی را به‌روشنی تعریف کرده و عنوان می‌کند که «یک ملت وقتی دارای امنیت است که در صورت اجتناب از جنگ بتواند ارزش‌های اساسی خود را حفظ کرده و در صورت اقدام به جنگ، بتواند آن را پیش برد». رابرت مک‌نامارا[2] نیز می‌گوید اگر امنیت دال بر وضعیتی باشد، آن وضع حداقل نظم و ثبات خواهد

1. Walter Lippman
2. Robert Mc Namara

بود. ریچارد کوپر[1] نیز معتقد اســت: توان جامعــه در حفظ و بهره‌گیری از فرهنگ و ارزش‌هایش امنیت ملی است (بیات، ۱۳۹۸: ۳۱).

شبکه ملی اطلاعات:[2] بستری امن، پیشــرفته و متــکی به جدیدترین فناوری‌های نوین و بومی برای تحقق فضای مجازی براساس ارزش‌های والای اسلامی-ایرانی برای رسیدن به اهداف چشــم‌انداز ایران است (اصلی‌زاده و زین‌الدینی بیدمشکی، ۱۳۹۵: ۶۱-۵۳). این شبکه به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه مبتنی‌بر قــرارداد اینترنت به همراه ســوئیچ،[3] مسیریاب‌ها[4] و مراکز داده[5] اســت به‌صورتی‌که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شود به‌هیچ‌وجه از خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت، خصوصی و امن داخلی در آن فراهم باشد (مرکز ملی فضای مجازی، ۱۳۹۲: ۸).

ســـناریو:[6] نگاه به آینده از دریچه و چشــم‌اندازی ویژه اســت که در چارچوب آن، داستان تصویر شده دارای سازگاری منطقی بوده و رخدادهای بیرون از حقیقت‌نمایی و خردورزی در تاروپود آن، راهی ندارد. سناریو، یعنی داستانی درباره آینده که معمولاً شامل داستان‌هایی از گذشته و حال هم می‌شود (Bell,2004 :523).

عدم قطعیت:[7] عواملی که نتایج ناشناخته دارد و هنوز اتفاق نیفتاده است و نمی‌توان برای آن میزان احتمال وقوع خاصی را پیش‌بینی کرد. این عناصر همواره به‌طور ذاتی به عناصر نسبتاً مشــخص مرتبطند و می‌توان با به سؤال کشیدن مفروضات خود در

---

1. Richard Kuper
2. National Information Network
3. Switches
4. Routers
5. Data Centers
6. Scenario
7. Uncertainty

زمینه این عناصر، آنها را پیدا کرد (شوارتز،[1] ۱۳۹۰: ۲۲۶).

پیشـــران:[2] ســـاده‌ترین و شیواترین تعریف پیشـــران، نیروهای بزرگ تغییر است. پیشران‌ها نیروهایی است که بر پیامد رویدادها تأثیر دارد. به‌عبارت‌دیگر عناصری که باعث حرکت و تغییر در طرح اصلی ســـناریوها شده و سرانجام داستان‌ها را مشخص می‌کند (پدرام و احمدیان، ۱۳۹۴: ۱۸۶-۱۸۵).

کنشـــگران:[3] اگر رخدادها را به دو بخش طبیعی و انسان‌ساز تقسیم کنیم، هسته اصلی عموم پژوهش‌های سناریونویسی، مطالعه رفتار اجتماعی انسان‌ها و رخدادهای انسان‌ســـاز است. در حوزه مســـائل امنیتی، سیاسی و فرهنگی، اهمیت مطالعه رفتار بازیگران بیشتر از حوزه‌های اقتصادی، علمی و فنی است (رضایان قیه‌باشی، پورعزت و سرمست، ۱۳۹۶: ۱۲۸-۱۰۳).

۴. روش شناسی پژوهش

پژوهش حاضر ازنظر هدف، کاربردی است که با رویکرد اکتشافی انجام شده است. ایـن پـژوهش بـرپایـه رویکـرد کیفی انجام و در پی گردآوری داده‌ها به‌منظور مفهوم‌سازی و ارائه تحلیل‌های تجویزی است. با توجه به اهمیت موضوع پژوهش و نظر به اینکه یکی از اهداف اصلی آن بسط نگاه راهبردی مدیران و سیاستگذاران کلان کشور به ظرفیت نااندیشیده درخصوص شبکه ملی اطلاعات و پیامدهای امنیتی آن است، سعی شده عوامل و پیشران‌های مؤثر در حوزه‌های مختلف و گوناگون مورد توجه قرار گیرد. برای پژوهش از روش نمونه‌گیری هدفمند در جامعه آماری ۲۰ نفره با مشخصات زیر استفاده شد که شامل اساتید دانشگاه‌های تهران و دانشگاه عالی دفاع ملی و برخی مدیران شاغل در وزارت ارتباطات و فناوری اطلاعات، مرکز ملی

1. Schwartz
2. Driving Force
3. Activist

فضای مجازی، سازمان برنامه‌وبودجه و فناوری اطلاعات بود. ویژگی‌های انتخاب نمونه آماری براساس داشتن نگاه راهبردی و عمیق به موضوع تحقیق، داشتن تحصیلات عالی در حوزه‌های آینده‌پژوهی و فناوری اطلاعات، داشتن بیش از ۱۰ سال سابقه در حوزه‌های مختلف تصمیم‌گیری و سیاستگذاری کلان و دارا بودن سابقه پژوهشی به‌منظور درک بیشتر و عمیق‌تر هدف از انجام پژوهش بوده است.

درخصوص شیوه‌های گردآوری اطلاعات و روش تجزیه‌وتحلیل، ابتدا به‌منظور مرور ادبیات، بررسی کتابخانه‌ای علمی و تخصصی انجام و در ادامه از روش‌های ذهن‌انگیزی و پنل‌های خبرگان استفاده شد.

سناریوها نمایندگان برگزیده شده از فضای آینده‌های بدیل هستند. برای شناسایی آینده‌های بدیل و تبدیل آنها به مجموعه سناریوها سه رویکرد کلی پیشنهاد شده است: رویکردهای استقرایی، فزاینده و استنتاجی (پدرام و احمدیان، ۱۳۹۴: ۱۸۱). رویکردهای فزاینده و استقرایی به‌دلیل پیچیدگی‌های روش‌شناختی به‌شدت نیازمند تبحر و تجربه است. یکی دیگر از رویکردهای سناریوپردازی استنتاجی[1] است. این رویکرد کاربرد گسترده‌ای در سناریونویسی کیفی دارد و به شکلی منظم به تحلیل عدم قطعیت‌ها و سناریوها می‌پردازد (پدرام و زالی، ۱۳۹۷: ۲۶-۱). برپایه این رویکرد، الگوهای اجرایی متنوعی برای سناریوپردازی پیشنهاد شده است که مرسوم‌ترین آنها در مکتب آمریکایی، الگوی «شبکه جهانی کسب‌وکار» معروف به GBN[2] است که پیتر شوارتز در کتاب هنر دورنگری، آن را شامل شناسایی موضوع یا تصمیم اصلی، شناسایی نیروهای کلیدی در محیط نزدیک، شناسایی نیروهای پیشران، طبقه‌بندی براساس اهمیت و عدم قطعیت، برپا کردن سناریوها یا ترسیم آنها و شناسایی پیامدها و شاخص‌های راهنمای آنها می‌داند (شوارتز، ۱۳۹۰: ۲۲۴).

با توجه به موضوع پژوهش که در حوزه سناریوپردازی است و ضرورت دارد به جهت سناریوپردازی در موضوع شبکه ملی اطلاعات ابتدا کنشگران، عوامل کلیدی و

1. Deductive
2. Global Business Network

نیروهای پیشران شناسایی شود، ازاین‌رو پژوهشگران این تحقیق با اقتباس از الگوی جهانی کسب‌وکار، روش اجرای پژوهش خود را برپایه مراحل فوق بنا نهادند.

۵. یافته‌های پژوهش

در گام نخست، تأثیرگذارترین بازیگران در موضوع پژوهش شناسایی شد. خبرگان در اولین نشست هم‌اندیشی، این بازیگران را از نظر اهمیت مورد بررسی قرار دادند. در گام دوم، شناسایی عوامل تأثیرگذار بر موضوع در دستور کار قرار گرفت. در گام سوم پیشران‌ها و عدم قطعیت‌های مرتبط با آنها از طریق مرور اسناد، مصاحبه نیمه‌ساختاریافته و تحلیل آنها در پنل‌ها با مشارکت خبرگان، بررسی و احصا شد. در گام چهارم مطلوب‌ترین آینده ممکن مورد بررسی خبرگان قرار گرفت و در گام پنجم، فضای کلی سناریوها ترسیم شد. در این گام کوشش شد تا سناریوهای اصلی (باورپذیرتر) برای آینده پیش روی شبکه ملی اطلاعات ایران با تأکید بر پیامدهای امنیتی آنها ترسیم شود. اهم یافته‌های پژوهش براساس گام‌های فوق از این قرار است:

۵-۱. کنشگران

شناخت کنشگران از حیث توانمندی‌ها، اهداف، انگیزه‌ها، نقاط ضعف و مطلوبیت‌ها به ما کمک می‌کند تا بتوانیم شناخت بهتری از آینده موضوع به‌دست آوریم. پس از مشخص شدن فهرست و دسته‌بندی کنشگران، باید وزن آنها در مسئله سازمان مشخص شود. معمولاً این وزن‌دهی به شکل نمادین (با نمره دادن از ۰ تا ۳) یا با اعداد معادل نماها انجام می‌شود. برای مثال وزن کنشگران با عددی بین ۰ تا ۳ مشخص می‌شود که عدد ۳ معادل واژه «کلیدی»، عدد ۲ معادل واژه «بسیار مهم» و عدد ۱ معادل واژه «مهم» است. کنشگری که وزن صفر داشته باشد از فهرست اصلی کنار گذاشته می‌شود. نتایج حاصل از برگزاری پنل خبرگان درخصوص کنشگران

تأثیرگذار بر سناریوهای فراروی شبکه ملی اطلاعات در ایران با تأکید بر پیامدهای امنیتی آنها در جدول ۲ منعکس شده است. خبرگان به هریک از کنشگران امتیازی بین ۱ تا ۳ اختصاص دادند که میانگین نظر کارشناسانه خبرگان براساس میانگین وزن‌های اعلام شده محاسبه و عدد نهایی در ستون میزان اهمیت، درج شد.

جدول ۲. کنشگران مؤثر بر موضوع

ردیف	کنشگران	میزان اهمیت کنشگر
۱	نهادهای حقوقی و امنیتی (مانند قوه قضائیه، وزارت اطلاعات و ...)	۲/۷۵
۲	نهادهای قانونگذاری و نظارتی (مانند سازمان تنظیم مقررات فضای مجازی)	۲/۴
۳	تأمین‌کنندگان منابع مالی و پشتیبانی طرح (مانند سازمان برنامه‌وبودجه و وزارت ارتباطات و فناوری اطلاعات)	۲/۴
۴	رسانه‌ها و شبکه‌های اجتماعی داخلی با کاربران بسیار زیاد و پرمخاطب در کشور (مانند صداوسیما، آی‌گپ و ...)	۲/۱۵
۵	مجامع علمی و دانشگاهی داخل و خارج کشور	۲/۱
۶	گروه‌های مرجع شامل افراد شاخص سیاسی، اجتماعی، هنری و ورزشی (مانند سلیبریتی‌ها، چهره‌های سرشناس ورزشی و ...)	۱/۹۵
۷	کشورهای دارای شبکه ملی اطلاعات (مثل چین، اسکاتلند، روسیه و کره جنوبی و ...)	۱/۹
۸	رسانه‌ها و شبکه‌های اجتماعی خارجی با کاربران بسیار زیاد و پرمخاطب در کشور (مانند فیس‌بوک، توییتر، اینستاگرام و ...)	۱/۹
۹	دولت‌های پیشرو در فناوری اطلاعات و ارتباطات و شبکه‌های رایانه‌ای (مانند ژاپن و ایالات متحده آمریکا)	۱/۸
۱۰	شرکت‌های بزرگ فناوری–اطلاعات و ارتباطات داخل کشور (مانند ارتباطات سیار، خدمات انفورماتیک و ...)	۱/۷۵
۱۱	شرکت‌های بزرگ و صاحب برندهای معروف اقتصادی (شرکت مبین نت، آسیا تک و ...)	۱/۷
۱۲	شبکه‌ها و گروه‌های معاند خارج کشور	۱/۴

ردیف	کنشگران	میزان اهمیت کنشگر
۱۳	سامانه‌های خودگردان در شبکه جهانی اینترنت (مانند سازمان فناوری اطلاعات ایران، همراه اول، ایرانسل و ...)	۱/۳
۱۴	نهادهای اجتماعی بین‌المللی (مانند یونیسف)	۱/۲
۱۵	سازمان‌ها و انجمن‌های مردم‌نهاد و فعال مدنی	۱/۱۵

مأخذ: یافته‌های تحقیق.

۲-۵. نیروهای پیشران تغییر

پیشران‌هایی که پیشامد آنها می‌تواند موضوع مورد پژوهش را با تحولی جدی روبه‌رو سازد، براساس پنل خبرگان در جدول ۳ لیست شده‌اند. لیست اولیه پیشران‌های یادشده در ابتدا طی مرور اسناد و مدارک کتابخانه‌ای، بررسی پیشینه پژوهش‌های مطرح شده و مصاحبه با تعدادی از خبرگان، احصا و سپس با طرح آنها در پنل‌های خبرگی، موارد مشابه ادغام و مواردی نیز براساس نظر ایشان و با توجه به کنش احتمالی کنشگران شناسایی شده در آینده، اضافه شد. خبرگان از نظر اهمیت به هریک از نیروهای پیشران امتیازی بین ۰ تا ۳ دادند.

با توجه به شمار بالای پیشران‌های شناسایی شده و با توجه به این نکته که احتمالاً پاسخگویی کارشناسانه از حوصله خبرگان خارج می‌شود، درنهایت کنشگران و پیشران‌های منتج از آنها، به سه دسته پنج‌تایی با توجه به تخصص‌های خبرگان تقسیم و در اختیار آنها قرار گرفت که یک گروه شش نفره و دو گروه هفت نفره شدند. پنج کنشگر دولت‌های پیشرو در فناوری اطلاعات و ارتباطات و شبکه‌های رایانه‌ای، شرکت‌های بزرگ فناوری-اطلاعات و ارتباطات داخل کشور، سازمان‌ها و انجمن‌های مردم‌نهاد و فعال مدنی، گروه‌های مرجع شامل افراد شاخص سیاسی، اجتماعی، هنری و ورزشی و مجامع علمی و دانشگاهی داخل و خارج کشور در اختیار یک گروه خبره شش نفره قرار گرفت و سایر کنشگرها در اختیار کمیته‌های هفت نفره قرار گرفت و از ایشان خواسته شد نظر خود را در قالب اعداد ۰ تا ۳ به هریک از این پیشران‌ها اعلام کنند که در جدول ۳ میانگین نظر خبرگان در مورد هر پیشران در

ستون «میانگین امتیازات» نمایش داده شده است.

جدول ۳. میانگین نظر خبرگان در مورد هر پیشران

کنشگران	پیشران‌ها	میانگین امتیازات
دولت‌های پیشرو در فناوری اطلاعات و ارتباطات و شبکه‌های رایانه‌ای	اعتماد کاربران در بهره‌برداری از شبکه ملی اطلاعات	۲/۸۳
	اینترنت بین‌المللی و ماهواره‌ای برای مثال استارلینک[1]	۲/۶۶
	دسترسی حداکثری جمعیت مقیم به اینترنت	۲/۳۳
	توسعه حکمرانی دیجیتالی بر جهان	۲/۱۶
	سیاست‌های غلبه فناورانه و اقتصادی بر سایر کشورها	۲
	ارائه خدمات مبتنی‌بر محتوای داده‌های اینترنتی و فضای ابری	۱/۸۳
	سیاست‌های استقرار دولت هوشمند و الکترونیک	۱/۸۳
	اعمال فشارهای بین‌المللی بر کشورهای هدف	۱/۶۶
	تدوین سیاست‌های امنیتی-اطلاعاتی و سلطه‌جویانه	۱/۶۶
	ایجاد روال‌های مرتبط با داده‌های شبکه و اقتضائات آن	۱/۵
	مدیریت بهره‌مندی از مزایای شبکه	۱/۵

1. Starlink

کنشگران	پیشران‌ها	میانگین امتیازات
نهادهای قانونگذاری و نظارتی داخلی و بین‌المللی	بازیگران کلیدی و تأثیرگذار شبکه ملی اطلاعات	۲/۸۵
	رسمی کردن هویت دیجیتالی افراد و دیجیتالیزه‌سازی افراد	۲/۷۱
	سیاست‌ها و قوانین نظارت بر تبادل داده‌های شبکه	۲/۷۱
	سیاست‌های اعمال صلاحیت و کنترل اینترنت	۲/۵۷
	تصویب ضوابط همکاری‌های بین‌المللی دو یا چندجانبه	۲/۴۲
	قوانین مالکیت معنوی داده‌های شبکه	۲/۲۸
	سیاست‌های توسعه یا محدودسازی استفاده از داده‌های شبکه در محاکم بین‌المللی	۲/۱۴
	انجمن اینترنت برای اسامی و اعداد تعیین‌شده (IP)[1]	۲/۱۴
	نهادهای غیردولتی مانند سندیکاها و اتحادیه‌های قانونگذار	۱/۸۵
نهادهای حقوقی و امنیتی	کنترل و دسترسی به داده‌های شبکه	۲/۸۵
	پایش و رصد نظام‌مند و مستمر فرصت‌ها و تهدیدها	۲/۸۵
	کمیته بررسی جرائم رایانه‌ای و اینترنتی	۲/۵۷
	مقررات مربوط به حریم خصوصی و حفاظت از داده‌های افراد و سازمان‌ها	۲/۵۷
	وضع قوانین مرتبط با جرائم سایبری	۲/۱۴
	نظارت بر زیرساخت‌های حیاتی در برابر حمله‌های سایبری	۲/۱۴
	هماهنگ‌سازی قوانین سایبری با نیازهای روز	۲
	سیاست‌های مواجهه فعال و مبتکرانه با فضای مجازی در سطح ملی	۱/۸۵
	چارچوب‌گذاری در تبادل و استعلام داده‌های افراد بین سازمان‌ها و برعکس	۱/۸۵

1. Internet Protocol

کنشگران	پیشران‌ها	میانگین امتیازات
شرکت‌های بزرگ فناوری-اطلاعات و ارتباطات داخل کشور	توسعه اقتصاد دیجیتالی	۲/۶۶
	توسعه و ارائه پلتفرم‌های جدید مبتنی‌بر فناوری اطلاعات	۲/۱۶
	خانوارهای دارای دسترسی به اینترنت در خانه	۲/۱۶
	پهنای باند به‌ازای هر کاربر	۱/۸۳
	خدمات مبتنی‌بر ایجاد ارزش‌افزوده اینترنت	۱/۸۳
	کاربرد فناوری اطلاعات در اقتصاد هر کشور	۱/۶۶
	کاربردی و عمومی کردن فناوری‌های نوین مانند اینترنت اشیا در سطح جوامع	۱/۶۶
	میزان به‌کارگیری هوش مصنوعی و ربات‌ها در زندگی روزمره	۱/۶۶
	تجاری‌سازی فناوری‌های نوظهور برای دولت‌ها و شرکت‌ها	۱/۵
	ارائه خدمات جدید محاسباتی و تحلیل داده‌ها	۱/۵
رسانه‌ها و شبکه‌های اجتماعی خارجی با کاربران بسیار زیاد و پرمخاطب در کشور	ایجاد بسترهای جدید تبادل داده در فضای مجازی	۲/۸۳
	ایجاد داده‌های حجیم از اطلاعات کاربران و در اختیار گذاردن آن به دولت‌ها و مشتریان خاص	۲/۱۶
	عوامل انگیزشی برای تولید داده و اشتراک‌گذاری اطلاعات شخصی کاربران	۱/۸۳
	هم‌افزایی رسانه‌های اجتماعی درخصوص تبیین آینده داده‌های افراد	۱/۶۶
رسانه‌ها و شبکه‌های اجتماعی داخلی با کاربران بسیار زیاد و پرمخاطب در کشور (مانند صداوسیما، آی‌گپ و ...)	صیانت از هویت دینی، ملی و ارزش‌های انسانی جامعه	۲/۸۵
	توسعه فرهنگ بهره‌گیری از فضای مجازی	۲/۸۵
	آموزش به کمک رایانه و فراگیری رایانه	۲/۷۱
	میزان استقبال از پذیرش شبکه‌های اجتماعی داخلی	۲/۵۷
	برنامه‌های تبلیغاتی صداوسیما در روشنگری نسبت به شبکه ملی اطلاعات	۲/۴۲
	ایجاد سامان‌دهی و تقویت نظام ملی اطلاع‌رسانی رایانه‌ای	۲/۱۴
	برنامه‌ها و سیاست‌های معطوف به تولید محتوا	۱/۸۵

کنشگران	پیشران‌ها	میانگین امتیازات
سازمان‌ها و انجمن‌های مردم‌نهاد و فعال مدنی	تشکیل کمپین‌ها و تجمعات درخصوص راه‌اندازی شبکه و حفظ حریم خصوصی	۲/۶۶
	هم‌افزایی و همراهی با نهادهای بین‌المللی درخصوص بهره‌برداری مناسب از داده‌های اشخاص	۲/۳۳
	توسعه ارزش‌های اجتماعی-شبکه‌ای شهروندان	۱/۸۳
	اقناع‌سازی افکار عمومی پیرامون سیاست‌های کلان وضع‌شده توسط شبکه ملی اطلاعات	۱/۶۶
گروه‌های مرجع شامل افراد شاخص سیاسی، اجتماعی، هنری و ورزشی (مانند سلیبریتی‌ها، چهره‌های سرشناس ورزشی و ...)	سپهر فرهنگی در شبکه ملی اطلاعات	۲/۸۳
	گسستگی فرهنگی در شبکه ملی اطلاعات	۲/۸۳
	رسمیت‌بخشی به هویت دیجیتالی افراد	۲/۶۶
	حفظ حریم خصوصی و آزادی‌های مشروع	۲/۵
	ترویج سبک زندگی فناورانه	۱/۵
	الگوسازی برای هویت دیجیتالی مخاطبان	۱/۵
مجامع علمی و دانشگاهی داخل و خارج کشور	فارغ‌التحصیلان دانش‌آموخته حوزه فناوری اطلاعات و ارتباطات در مقاطع مختلف تحصیلی	۲/۳۳
	توسعه سیستم‌ها و فناوری‌های مبتنی‌بر داده‌کاوی	۱/۸۳
نهادهای اجتماعی بین‌المللی (مانند یونیسف)	وضع سیاست‌های اجتماعی پیرامون حقوق سایبری	۲/۸۵
	ایجاد سیاست‌های رفاهی و حمایتی در حوزه فناوری اطلاعات	۲/۴۲
	مدیریت شکاف‌های اجتماعی ایجاد شده	۱/۸۵
	بحران‌های جهانی (مانند همه‌گیری بیماری کرونا)	۱/۷۱
شبکه‌ها و گروه‌های معاند خارج کشور	ممانعت از راه‌اندازی شبکه ملی اطلاعات با هجمه تبلیغاتی	۲/۲۸
	مختل‌سازی مدیریت امور جاری کشورها	۲/۴۲
	جمع‌آوری اطلاعات و فعالیت‌های جاسوسی	۲

کنشگران	پیشران‌ها	میانگین امتیازات
شرکت‌های بزرگ و صاحب برندهای معروف اقتصادی (شرکت مبین نت، آسیا تک و ...)	رعایت حقوق اجتماعی و صیانت فرهنگی و فنی	۲/۷۱
	توسعه اقتصاد مبتنی‌بر وب	۲/۷۱
	ایجاد سبک زندگی مبتنی‌بر فضای مجازی	۲/۴۲
	فروش اطلاعات افراد و تحلیل رفتار کاربران	۲/۲۸
	انگیزه‌های تجاری در استفاده از اینترنت	۱/۸۵
سامانه‌های خودگردان در شبکه جهانی اینترنت (مانند سازمان فناوری اطلاعات ایران، همراه اول و ایرانسل و ...)	اتصال به اینترنت در شبکه ملی اطلاعات	۲/۸۵
	تقویت هویت ایرانی–اسلامی و گسترش فرهنگ ایرانی	۲/۲۸
	اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه فضای مجازی	۲/۱۴
	تهیه و تأمین محتوای الکترونیکی فرهنگی–اسلامی	۱/۵۷
	توسعه خط و زبان فارسی در محیط رایانه‌ای	۱/۴۲
	حضور فعال و اثرگذار در شبکه‌های جهانی	۱/۲۸
کشورهای دارای شبکه ملی اطلاعات (مثل چین، اسکاتلند، روسیه، کره جنوبی و ...)	ایجاد حداکثر سهولت در ارائه خدمات اطلاع‌رسانی و اینترنت به عموم جامعه	۲/۸۵
	تولید و نشر محتوای سالم الکترونیکی	۲/۷۱
	آموزش الکترونیکی و از راه دور	۲/۴۲
	برقراری سامانه‌های آموزشی برخط مدارس مبتنی‌بر وب	۲/۴۲
	افزایش آگاهی عمومی و سواد دیجیتالی جامعه	۲/۴۲
	تولید ملی در حوزه نرم‌افزار و سخت‌افزار	۲/۱۴
	فرصت‌های برابر، عادلانه و امن فناوری اطلاعات برای همه شهروندان	۱/۷۱
	گسترش عدالت اجتماعی و اطلاع‌رسانی شفاف	۱/۵۷

کنشگران	پیشران‌ها	میانگین امتیازات
تأمین‌کنندگان منابع مالی و پشتیبانی طرح (مانند سازمان برنامه‌وبودجه و وزارت ارتباطات و فناوری اطلاعات)	تخصیص بودجه به زیرساخت‌های شبکه	۲/۸۵
	تولید محتوای نرم‌افزاری مورد نیاز شبکه	۲/۷۱
	تخصیص ابنیه به زیرساخت‌های شبکه	۲/۱۴
	تولید و ساخت سخت‌افزارهای مورد نیاز	۱/۲۸

مأخذ: همان.

با توجه به میزان اهمیت اعلام شده خبرگان پژوهش برای هر پیشران براساس جدول فوق، ۳۹ مورد از پیشران‌هایی که بالاترین امتیاز را داشتند احصا و مجدداً نظر جمع برگزیده‌ای از خبرگان درخصوص مهم‌ترین و مؤثرترین پیشران‌های مؤثر بر موضوع پژوهش مورد بررسی قرار گرفت. پس از نمره‌دهی و میانگین‌گیری، ۲۰ نیروی پیشران زیر به‌عنوان نیروهای پیشران اهم با اجماع‌نظر خبرگان انتخاب شد:

۱. اینترنت بین‌المللی و ماهواره‌ای برای مثال استارلینک؛
۲. سیاست‌ها و قوانین نظارت بر تبادل داده‌های شبکه؛
۳. رسمی کردن هویت دیجیتالی افراد و دیجیتالیزه‌سازی افراد؛
۴. اعتماد کاربران در بهره‌برداری از شبکه ملی اطلاعات؛
۵. بازیگران کلیدی و تأثیرگذار شبکه ملی اطلاعات؛
۶. پایش و رصد نظام‌مند و مستمر فرصت‌ها و تهدیدها؛
۷. کنترل و دسترسی به داده‌های شبکه؛
۸. توسعه اقتصاد دیجیتالی؛
۹. اتصال به اینترنت در شبکه ملی اطلاعات؛
۱۰. ایجاد بسترهای جدید تبادل داده در فضای مجازی؛
۱۱. صیانت از هویت دینی، ملی و ارزش‌های انسانی جامعه؛
۱۲. تشکیل کمپین‌ها و تجمعات درخصوص راه‌اندازی شبکه و حفظ حریم خصوصی؛
۱۳. رسمیت‌بخشی به هویت دیجیتالی افراد؛

۱۴. سپهر فرهنگی در شبکه ملی اطلاعات؛
۱۵. گسستگی فرهنگی در شبکه ملی اطلاعات؛
۱۶. فارغ‌التحصیلان دانش‌آموخته حوزه فناوری اطلاعات و ارتباطات در مقاطع مختلف تحصیلی؛
۱۷. وضع سیاست‌های اجتماعی پیرامون حقوق سایبری؛
۱۸. رعایت حقوق اجتماعی و صیانت فرهنگی و فنی؛
۱۹. ایجاد حداکثر سهولت در ارائه خدمات اطلاع‌رسانی و اینترنت به عموم جامعه؛
۲۰. تخصیص بودجه به زیرساخت‌های شبکه.

۳-۵. عدم قطعیت‌های کلیدی و تدوین چارچوب سناریوها

به‌منظور شناسایی عدم قطعیت‌های کلیدی، با توجه به پیشران‌های بااهمیت شناسایی شده در پنل خبرگان، حالت‌های احتمالی آینده این پیشران‌ها بررسی شد. براساس نظر خبرگان، چند شرط برای شناسایی عدم قطعیت‌های کلیدی در نظر گرفته شد:

عدم قطعیت‌ها با توجه هم‌زمان به دو فاکتور بالاترین اهمیت و بیشترین تأثیرگذاری تعیین شود؛

این اطمینان به‌وجود آید که عدم قطعیت‌های کلیدی حداکثر فضای نااطمینانی را پوشش می‌دهد؛

به ویژگی بارز عدم قطعیت یعنی پیش‌بینی‌ناپذیری توجه شود و اگر رویدادی حتی با احتمال نه‌چندان زیاد، قابل پیش‌بینی است دیگر عدم قطعیت به‌شمار نمی‌آید.

با منطق ترسیم شده، عدم قطعیت‌های کلیدی با اجماع خبرگان از میان ۲۰ پیشران کلیدی در چهار دسته اصلی تقسیم‌بندی شد:

۱. همکاری یا درگیری و عدم همکاری میان بازیگران کلیدی و تأثیرگذار شبکه ملی اطلاعات؛

۲. اعتماد یا عدم اعتماد در بهره‌برداری از شبکه ملی اطلاعات ازسوی کاربران؛

۳. برقراری یا عدم برقراری ارتباط کاربران به اینترنت در شبکه ملی اطلاعات؛

۴. سپهر یا گسستگی فرهنگی در میان کاربران شبکه ملی اطلاعات.

از برهم‌کنش عدم قطعیت‌های کلیدی فوق، ۱۶ فضای نااطمینانی آینده حاصل که با کمک خبرگان و صاحب‌نظران درخصوص باورپذیری یا باورناپذیری آنها، ارزیابی‌های لازم صورت گرفت. خبرگان با استناد به نظر و تجربه تخصصی خود و نیز با توجه به کلان‌روندهای ترسیم شده موضوع مورد پژوهش، سازگاری درونی و باورپذیری هر حالت را تعیین کردند. در جدول ۴ جمع‌بندی نظر خبرگان ارائه شده است.

جدول ۴. سازگاری عدم قطعیت‌ها و باورپذیری سناریوها

نام سناریو	مطلوبیت	عدم قطعیت ۴	عدم قطعیت ۳	عدم قطعیت ۲	عدم قطعیت ۱	باورپذیری
خانه امن و هوشمند	بسیار مطلوب	بله	بله	بله	بله	+
پادشاهی تاریک	بسیار نامطلوب	خیر	خیر	خیر	خیر	+
غیرباورپذیر	مطلوب	خیر	بله	بله	بله	–
غیرباورپذیر	مطلوب	بله	خیر	بله	بله	–
کورسوی امید	مطلوب	بله	بله	خیر	بله	+
غیرباورپذیر	مطلوب	بله	بله	بله	خیر	–
غیرباورپذیر	نامطلوب	بله	خیر	خیر	خیر	–
غیرباورپذیر	نامطلوب	خیر	بله	خیر	خیر	–
غیرباورپذیر	نامطلوب	خیر	خیر	بله	خیر	–
اسیری و آوارگی	نامطلوب	خیر	خیر	خیر	بله	+
غیرباورپذیر	بینابینی	خیر	خیر	بله	بله	–

نام سناریو	مطلوبیت	عدم قطعیت ۴	عدم قطعیت ۳	عدم قطعیت ۲	عدم قطعیت ۱	باورپذیری
غیرباورپذیر	بینابینی	بله	بله	خیر	خیر	–
غیرباورپذیر	بینابینی	خیر	بله	بله	خیر	–
غیرباورپذیر	بینابینی	بله	خیر	خیر	بله	–
استمرار دوگانگی	بینابینی	خیر	بله	خیر	بله	+
غیرباورپذیر	بینابینی	بله	خیر	بله	خیر	–

مأخذ: همان.

۴-۵. تدوین سناریوها

بعد از تدوین اولیه سناریوها و با جمع‌بندی نهایی نتایج حاصله، پنج سناریوی زیر نام‌گذاری، ترسیم و توصیف شد.

سناریو اول- خانه امن و هوشمند

در راستای دسترسی عمومی به فضای مجازی، حفظ و صیانت داده‌های کاربران، بهبود و تقویت امنیت ملی و از همه مهم‌تر اعتماد دوطرفه بین مردم و حکومت، باعث می‌شود دولت به راه‌اندازی شبکه اقدام کرده و کاربران از آن استقبال می‌کنند. دسترسی کاربران مزایای زیادی به‌همراه آورده و تبادل امن داده‌ها در بستر شبکه، تمایل کاربران را در سطح عموم جامعه به استفاده بیشتر از آن، افزایش داده است. تقویت مؤلفه‌های امنیت ملی و رشد خدمات دولت هوشمند، افکار عمومی را موافق استفاده از شبکه کرده است. حفظ حریم خصوصی در کنار ارائه خدمات شهر هوشمند و شهروند الکترونیک به‌راحتی امکان‌پذیر و این شبکه همانند بازوی قدرتمند برای حفظ و افزایش ضریب امنیت ملی عمل می‌کند. با استفاده از شبکه، امکان اعمال نظارت‌های قانونی فراهم می‌شود و بهره‌وری در حوزه تجارت الکترونیکی افزایش می‌یابد. ازسویی، توسعه آن در کنار نظارت و پایش مداوم داده‌ها، به سازمان‌های

امنیتی اجازه می‌دهد در شناسایی و مواجهه با تهدیدهای سایبری موفق‌تر عمل کند. در پرتو شبکه امن ایجاد شده، شرکت‌های تولیدکننده سخت‌افزار و نرم‌افزار از تعامل اثربخشی برخوردار و محصولات جدیدتری را روانه بازار می‌کنند. درنتیجه این تعاملات خدمات جذابی مانند خرید آنلاین، سرویس‌های هوشمند، خدمات الکترونیکی سفر، آموزش مجازی و از راه دور، گردشگری، سلامت الکترونیک و ... ارائه می‌شود. سطح تعاملات فرهنگی و سطح نفوذ و تبادلات مرتبط با آن بالا رفته و مرزها، ساختارها و هویت‌های فرهنگی–اجتماعی در بستر امن شبکه ملی مصون مانده و سپهر فرهنگی در جامعه شکل گرفته است. در راستای صیانت و جلوگیری از آسیب‌های فرهنگی ناشی از فضای مجازی جهانی به پیشبرد سیاست‌های فرهنگی کشور در شبکه پرداخته شده است. سیاست‌های مربوط به بهره‌گیری از فرصت‌های فضای مجازی، صیانت از تهدیدهای آن، حمایتی از ظرفیت‌های مردمی، توسعه جامعه شبکه‌محور، ایجاد فرصت‌های برابر، دسترسی به خدمات شبکه، راهبری و مدیریت فضای مجازی در سطوح ملی و فراملی به‌صورت مؤثر عملیاتی می‌شود. در تعاملات بین‌المللی شبکه ملی، اطلاعات تأثیر بسیار مؤثری در مقابله با تروریسم سایبری داشته است. این هم‌افزایی باعث شده نهادهای مسئول در حمله‌های سایبری موفق‌تر عمل کنند. به‌دلیل نرفتن ترافیک شبکه به سمت شبکه جهانی، پهنای باند و قابلیت دسترسی عموم، از مطلوبیت بالایی برخوردار می‌شود و هزینه استفاده از اینترنت به‌دلیل استفاده از پهنای باند داخلی به مقدار چشمگیری کاهش می‌یابد.

شاخص‌های راهنمای سناریو:

- استقبال کاربران از راه‌اندازی شبکه ملی اطلاعات؛
- تقویت مؤلفه‌های امنیت ملی و رشد خدمات دولت هوشمند؛
- امکان اعمال نظارت‌های قانونی و بهره‌وری در حوزه تجارت الکترونیکی؛
- ایجاد هم‌افزایی در بین دستگاه‌ها و متولیان امر برای مقابله با حمله‌های سایبری.

سناریو دوم– پادشاهی تاریک

دستگاه سیاسی و حاکمیتی کشور با نگاهی قلدرمآبانه و غیرمشارکتی، به راه‌اندازی شبکه ملی اطلاعات در راستای اهداف از پیش نوشته شده اقدام کرده و اعتماد دوطرفه بین مردم و حکومت برقرار نیست. امکان استفاده از فضای مجازی، فقط در بستر داخلی وجود دارد. دسترسی کاربران تنها به سایت‌های داخلی امکان‌پذیر بوده و عملاً هیچ کانال ارتباطی با دنیای خارج مهیا نیست و کاربران به استفاده از بستر داخلی مجبور هستند. نهادهای امنیتی و نظارتی حداکثر کنترل را برقرار و نوعی ترس و واهمه در استفاده از اینترنت جهانی از طریق ماهواره و خارج مرزها وجود دارد. هر روز شاهد دستگیری و بازداشت شمار زیادی از کاربران به‌دلیل نقض قوانین حکومتی هستیم و سیاست خفقان در جامعه برقرار است. نامطلوب‌ترین سناریوی ممکن اتفاق افتاده و بعد از مدت اندکی، نارضایتی‌ها رنگ و بوی اعتراض به خود می‌گیرد. کاربران هیچ اعتمادی به شبکه ندارند. خشونت و رفتارهای اعتراضی در میان مردم افزایش یافته و مرزهای امنیت ملی شکسته شده است. حکومت از قدرت خود برای کنترل هرچه بیشتر کاربران استفاده می‌کند. تسلط بر گردش اطلاعات در کشور به‌طور کامل برقرار است. تمرکز و ذخیره‌سازی اطلاعات ریزودرشت بخش‌های مختلف به افزایش قدرت اطلاعاتی و سلطه اطلاعاتی بر کاربران انجامیده، اندیشه جریان آزاد اطلاعات نقض و وجه تاریکی برای کاربران رخ داده، کشور به‌طور کامل از اینترنت جهانی مجزا و فقط نقاط دسترسی کنترل‌شده و محدودی وجود دارد. این امر در کنار کاهش سطح تعاملات جهانی، برخلاف تصور اولیه، به رشد میزان تهدیدهای سایبری و جرائم امنیتی و بروز نارضایتی‌های مدنی منجر شده که روابط تجاری، فرهنگی و اجتماعی با سایر کشورها را با بی‌ثباتی جدیدی روبه‌رو کرده است. تداوم روند به‌وجود آمده، مسئولان کشور را بر سر دوراهی تعامل آزاد با دنیا یا آمادگی برای انزوای بیشتر قرار می‌دهد. کشور به دلایل مسدودسازی مرزهای اطلاعاتی و شبکه‌ای خود، با چالش‌های جدی در تجارت و سایر مناسبات بین‌المللی و نیز مطالبات مدنی و اجتماعی شهروندان مواجه می‌کند. عدم دسترسی کاربران به اینترنت جهانی، راهبری و مدیریت راهبردی فضای مجازی برای مقابله با جنگ نرم

و تهاجم فرهنگی و نیز حضور مؤثر و هدفمند کشور در تعاملات بین‌المللی فضای مجازی، به‌منظور مقابله با سلطه جهانی در این عرصه و ایجاد توازن قدرت در سطح بین‌الملل را عملاً از مردم و گروه‌های مردم‌نهاد گرفته است. این اقدام امکان ایجاد فرصت‌های برابر و عادلانه در برخورداری از امکانات فرهنگی–اجتماعی از کاربران را سلب و جامعه عملاً دچار گسستگی فرهنگی شده است.

شاخص‌های راهنمای سناریو:

- نگاه قلدرمآبانه حاکمیت به شبکه ملی اطلاعات؛
- افزایش خشونت و رفتارهای اعتراضی در میان مردم و شکسته شدن مرزهای امنیت ملی؛
- رشد میزان تهدیدهای سایبری و جرائم امنیتی و بروز نارضایتی‌های مدنی.

سناریو سوم– اسیری و آوارگی

در راستای دسترسی عمومی کاربران به شبکه و حفظ و صیانت از هویت مجازی کاربران، شبکه راه‌اندازی شده و برای همه کاربران این امکان مهیاست تا به شبکه دسترسی داشته باشند، اما کاربران به‌دلیل عدم اعتماد به سیاست‌های اعمال‌شده از آن استقبال نکرده و مردم در استفاده از شبکه و امکانات آن نگران هستند. درصد کمی به استفاده از شبکه تمایل دارند. ازاین‌رو به شبکه به‌مثابه اسلحه نگاه می‌شود، هرچند امنیت رشد کرده است. کسب‌وکارهای الکترونیکی به‌دلیل عدم استقبال از حضور کاربران در بستر شبکه رشد کمتری دارد. با راه‌اندازی اینترنت ماهواره‌ای برخی از کاربران که از تمکن مالی برخوردارند، به استفاده از این بستر تمایل دارند و به‌رغم خروج مبالغ زیادی ارز، تداخل و تضاد در استفاده از اینترنت و فضای مجازی در کشور برقرار است. گسستگی فرهنگی در بستر شبکه رقم خورده و شبکه‌های اجتماعی به بستری برای خبرپراکنی دوگانه تبدیل شده است. پایگاه‌های خبری و اطلاع‌رسانی ملی در اختیار بستر شبکه است و در بین کاربران برای استفاده تمایلی وجود ندارد. اصل قانون آزادی در فضای مجازی نقض، و قوانین و مقررات داخلی

کشور، حاکمیت داده‌ها و ایجاد سامانه‌های مبتنی‌بر داده‌های شهروندان در کنار ایجاد نقاط دسترسی تحت شبکه ملی اطلاعات فراهم شده است.

شاخص‌های راهنمای سناریو:

- عدم اعتماد کاربران به شبکه ملی اطلاعات؛
- رشد کم کسب‌وکارهای اینترنتی به‌دلیل عدم استقبال کاربران از شبکه ملی اطلاعات؛
- تداخل و تضاد در استفاده از اینترنت و فضای مجازی در کشور.

سناریو چهارم- استمرار دوگانگی

دولت در راستای حفظ و صیانت از فضای مجازی، ضروری است شبکه را راه‌اندازی کند. به‌دلیل مشکلات اقتصادی ناشی از تحریم‌های بین‌المللی و عدم دسترسی به منابع ارزی و مالی حاصل از فروش صادرات نفتی و غیرنفتی و همچنین ناتوانایی در کنترل نرخ ارز، تورم بالای جامعه و توزیع نامناسب امکانات اقتصادی در جامعه، اعتبارات لازم برای راه‌اندازی و استقرار شبکه ملی اطلاعات مهیا نیست. مسئولان از بستر جاری استفاده کرده و به‌رغم هدررفت اعتبارات هنگفت ارزی، این همت نیز در بین مسئولان به‌منظور استقرار شبکه وجود ندارد، دولت به‌ناچار در بعد مالی ازجمله بانک‌ها و تبادلات مالی از شبکه داخلی استفاده می‌کند که در حال حاضر نیز برقرار است، تا لااقل از جرائم سایبری در بخش شبکه بانکی کشور ایمن بماند. مردم عادی از بستر شبکه جهانی استفاده می‌کنند و تنها برخی شبکه‌های اجتماعی دچار محدودیت فعالیت شده و فیلتر می‌شود. با وجود اعمال فیلترینگ، اما با ظهور فیلترشکن‌ها شاهد تبعات امنیتی بالایی برای کاربران هستیم. گسستگی فرهنگی ناشی از دسترسی عمومی به فضای مجازی و اینترنت جهانی و عدم صحت‌سنجی برخی افکار و اخبار در جامعه حکم‌فرما شده است. دسترسی اطفال، کودکان و نوجوانان به اینترنت جهانی پیامدهای فرهنگی ناگزیری را به دنبال آورده و شرکت‌های تولیدکننده فناوری، بازار خوبی را به‌دست آورده‌اند و پذیرش اجتماعی حضور این

فناوری‌ها در زندگی روزمره مردم در حال افزایش است. دستگاه حاکمیتی مجبور است برای ادامه حیات اقتصادی و تأمین امنیت ملی خود به سمت کشورهای پیشرو در فناوری‌های اطلاعاتی متمایل شود. شوک‌های اقتصادی و به‌تبع آن ناآرامی‌های اجتماعی در جامعه دیده می‌شود. شرکت‌های بزرگ مانند فیس‌بوک، گوگل و ... با ارائه سرویس‌های متنوع و ارائه خدمات شهروندمحور، مرزهای جغرافیایی را کنار زده و فعالیت‌های خود را در کشورهای دیگر به‌سرعت افزایش داده‌اند و وابستگی شهروندان به سرویس‌های شرکت‌ها در امور روزمره، به تهدیدی برای امنیت ملی تبدیل می‌شود و عملاً نبض داده‌های کشور در اختیار شرکت‌های بزرگ بین‌المللی قرار دارد، ادامه این روند نگرانی‌های زیادی برای نهادهای اطلاعاتی و نظارتی ایجاد می‌کند.

شاخص‌های راهنمای سناریو:

- مهیا نبودن اعتبارات لازم برای راه‌اندازی و استقرار شبکه ملی اطلاعات به‌دلیل مشکلات عدیده اقتصادی کشور؛
- تبعات سنگین امنیتی در استفاده کاربران از VPNها.

سناریو پنجم- کورسوی امید

شبکه ملی اطلاعات به‌منظور دسترسی عموم کاربران به فضای مجازی و بهره‌مندی از مزایای آن در عصر دیجیتال راه‌اندازی شده تا امکان دسترسی راحت‌تر، سریع‌تر و امن‌تر به خدمات شبکه جهانی برای کاربران مهیا شود. کاربران از اینترنت بین‌المللی بهره‌مندند و به‌علت استفاده از ترافیک داخلی، سرعت و هزینه‌های بهره‌مندی آنها از اینترنت در بستر شبکه ملی اطلاعات به میزان چشمگیری کاهش می‌یابد. همکاری مناسب و اثرگذاری در بین بازیگران و ذی‌نفعان کلیدی که در شبکه ملی اطلاعات دخیل هستند ایجاد شده و وجه مثبتی از ارتباط در شبکه به‌وجود آورده‌اند. کنترل و نظارت شبکه در دسترس و مدیریت امور فرهنگی در فضای مجازی و شبکه جهانی در زیر سامانه‌های شبکه داخلی صورت می‌پذیرد که به شکل‌گیری سپهر فرهنگی در

بخش‌های مختلف کشور منجر شده و عملاً بسیاری از تهدیدهای اخلاقی، فرهنگی و اجتماعی کاربران دفع می‌شود. نهادهای نظارتی و امنیتی بر پایش شبکه در راستای جلوگیری از حمله‌های سایبری که به آسیب داده‌ها و اطلاعات کاربران منجر می‌شود، اقدام‌های لازم را به‌عمل آورده و این پایش در مواقع لزوم به حفظ امنیت و هویت داده‌ها منجر می‌شود، هرچند در مواقعی که سطح حمله‌ها از سطح هشدار فراتر می‌رود، نهادهای مربوطه به قطع ارتباط اینترنت مجبور می‌شوند. ازسوی‌دیگر دستگاه‌ها و سازمان‌های دولتی که تا پیش از استقرار شبکه داخلی از زیر بار فشار الکترونیکی کردن سرویس‌های خود شانه خالی می‌کردند و به هر بهانه‌ای از ارائه سرویس به‌صورت الکترونیکی طفره می‌رفتند، برای ارائه خدمات به شهروندان راهی جز الکترونیکی کردن سرویس‌ها ندارند. با همه این اوصاف، مردم هنوز اعتماد کافی به بهره‌برداری از شبکه داخلی را نداشته و شبکه، موفق به جلب اعتماد کاربران نشده است. گرچه با توجه به مثبت بودن وضعیت کلی عدم قطعیت‌های دیگر در این سناریو، امید می‌رود که به‌مرور زمان این اعتماد در بین مردم و عموم کاربران به‌وجود آید و به‌صورت پلکانی، نرخ استفاده از شبکه ملی اطلاعات در میان عموم شهروندان روندی تصاعدی را در پیش گیرد.

شاخص‌های راهنمای سناریو:

- افزایش قابل‌توجه سرعت بهره‌مندی از اینترنت در بستر شبکه ملی اطلاعات؛
- کاهش هزینه‌های جاری شهروندان در استفاده از شبکه ملی اطلاعات؛
- دفع بسیاری از تهدیدهای اخلاقی، فرهنگی و اجتماعی متوجه کاربران؛
- پایش مداوم نهادهای نظارتی و امنیتی بر شبکه در راستای جلوگیری از حمله‌های سایبری.

به این‌ترتیب بعد از تهیه و تدوین سناریوها، با رجوع به‌عنوان سناریوهای شناخته شده، به اولویت‌بندی سناریوها اقدام می‌شود تا از این طریق امکان پایش مستمر ظهور و بروز سناریوها در افق زمانی ۱۴۰۷ تعیین و تخصیص منابع در این راستا

امکان‌پذیر شود (جدول ۵). برای این منظور ترجیح‌های قضاوتی ارزیابی وضعیت سناریوها به‌صورت کمترین (۱)، کم (۳)، متوسط (۵)، مناسب (۷) و بیشترین (۹) در نظر گرفته شده است.

جدول ۵. ارزیابی وضعیت سناریوها با پنج ویژگی

ردیف	ویژگی سناریوهای تهیه شده	سناریوها				
		اول	دوم	سوم	چهارم	پنجم
الف	آیا سناریو موجه و قابل‌قبول است؟ (یعنی امکان وقوع دارد؟)	۷	۹	۵	۹	۹
ب	آیا سناریو برای تصمیم‌گیری‌ها مؤثر واقع می‌شود؟	۵	۱	۳	۵	۷
ج	آیا در سناریو چالش‌های آینده موضوع پژوهش به چشم می‌آید؟	۳	۵	۳	۹	۹
د	آیا سازگاری درونی در اجزای تشکیل‌دهنده سناریو مشاهده می‌شود؟	۷	۵	۷	۷	۹
ه	آیا روابط علّی و معلولی در سناریو رعایت شده است؟	۷	۷	۵	۵	۷
	جمع	۲۹	۲۷	۲۳	۳۵	۴۱

مأخذ: همان.

با ارزیابی صورت پذیرفته با فاکتورها و ویژگی‌های پنجگانه مندرج در جدول ۵ سناریوی پنجم با بیشترین امتیاز در رده اول، سناریو چهارم در رده دوم، سناریو اول در رده سوم، سناریو دوم در رده چهارم و نهایتاً سناریو سوم در رده پنجم اولویتی قرار می‌گیرد. فصل مشترک سناریوها در جدول ۶ نشان داده شده است.

جدول ۶. تعیین فصل مشترک بین سناریوها

سناریوها		سناریوها				
		اول	دوم	سوم	چهارم	پنجم
سناریوها	اول		۱	۳	۵	۳
	دوم	۱		۳	۱	۲
	سوم	۳	۳		۱	۱
	چهارم	۵	۱	۱		۵
	پنجم	۳	۲	۱	۵	

نتایج حاصله از جدول تعیین فصل مشترک بین سناریوها حاکی از وجود فصل مشترک یا اشتراکاتی در بین سناریوها هرچند در مواردی بسیار کم است.

۶. جمع‌بندی، نتیجه گیری و پیشنهادها

در این پژوهش که مبتنی‌بر روش سناریو با رویکرد استنتاجی است، تلاش شد ضمن شناسایی کنشگران مهم و اثرگذار بر شبکه ملی اطلاعات، پیشران‌های مؤثر و عدم قطعیت‌های مرتبط نیز شناسایی شود تا نگارش سناریوهای باورپذیر امکان یابد. یافته‌های پژوهش نشان داد کنشگران کلیدی اثرگذار شامل نهادهای قانونگذاری و نظارتی (مانند سازمان تنظیم مقررات فضای مجازی)، نهادهای حقوقی و امنیتی (مانند قوه قضائیه، وزارت اطلاعات و ...)، رسانه‌ها و شبکه‌های اجتماعی داخلی با کاربران بسیار زیاد و پرمخاطب در کشور (مانند صداوسیما، آی‌گپ و ...)، مجامع علمی و دانشگاهی داخل و خارج کشور و تأمین‌کننده منابع مالی و پشتیبانی طرح (مانند سازمان برنامه‌وبودجه و وزارت ارتباطات و فناوری اطلاعات) است.

مهم‌ترین پیشران‌ها نیز با استفاده از نظر خبرگان و اجماع آرا حاصل شده میان آنها شناسایی شدند. ضمن اینکه براساس نظر ایشان چهار عدم قطعیت کلیدی و مؤثر شناسایی شد که از برهم‌کنش این چهار عدم قطعیت، شانزده فضای نااطمینانی به‌دست آمد که با بررسی باورپذیری آنها، نگارش سناریوها انجام شد.

با شناسایی کنشگران، اثر تعاملی پیشران‌ها و شناسایی عدم قطعیت‌های موجود، پنج سناریوی باورپذیر تعریف شد که برای راحتی کار، پژوهشگران با ترکیب کلمات، اسامی خودنوشتی را با توجه به ماهیت سناریوها برای آنها تعیین کردند. اسامی این پنج سناریو به‌صورت سناریوی بسیار مطلوب «خانه امن و هوشمند»، سناریو مطلوب «کورسوی امید»، سناریو بینابینی «استمرار دوگانگی»، سناریو نامطلوب «اسیری و آوارگی» و سناریو بسیار نامطلوب «پادشاهی تاریک» تعیین شد.

در سناریو بسیار مطلوبِ خانه امن و هوشمند، مسیر رشد و تعالی کشور در راستای اعتماد دوطرف حاصل می‌شود و مردم به مسئولان و مسئولان نیز به مردم اعتماد

دارند. این سناریو در تأیید نظریه‌های امنیت ملی مطرح شده بیات (۱۳۹۸) ترسیم شده است. وی عنوان می‌دارد که «دستیابی یک ملت به امکانات و توانمندی و ابزاری که بتواند با تمسک به آنها از تهدیدهای خارجی و داخلی در امان ماند؛ موجب می‌شود سلطه سیاسی، اقتصادی، فرهنگی و نظامی بیگانه را دفع کند؛ از ارزش‌های حیاتی خود در صلح و جنگ، دفاع و حراست کند؛ از موجودیت کشور و تمامیت ارضی آن محافظت کند، سیر صعودی در افزایش قدرت و توان ملی در عرصه‌های مختلف داشته باشد و در راه پیشبرد امر توسعه متوازن و پویا و تحکیم وحدت ملی و ارتقای سطح مشارکت سیاسی جامعه موفق باشد». سناریوی مذکور با ترسیم آنچه که مطلوب امنیت هر ملت در حفظ و حراست آنها از هرگونه تهدید داخلی و خارجی و در راستای اعتماد دوطرفه بین ملت و حکومت تعریف می‌شود، نگاشته شده است.

سناریو مطلوبِ کورسوی امید، امیدها را در کاربران نسبت به اعتماد به شبکه به‌طور نسبی زنده نگه داشته و علی‌رغم وجود سه عدم قطعیت مثبت به دنبال اعتمادسازی در سطح جامعه و کاربران، به‌منظور تحقق مطلوب این عدم قطعیت‌ها است. این سناریو از یک نگاه سلبی—ایجابی برخوردار است که مصلحت ملی را بر مصلحت عموم برتری داده و اولویت خود را در حفظ امنیت ملی ترسیم می‌کند. درک پیامدهای امنیتی، مستلزم حصول معرفت به نسبت مصلحت و امنیت است. در این راستا، دو نوع رابطه از یکدیگر تمیز داده شده‌اند، رابطه طولی مبتنی‌بر جانشینی یکی از متعلقات به‌جای سایر متعلقات که پیامدهای امنیتی ناگوار آن معطوف به مراجع سه‌گانه سیاسی، اجتماعی و فرهنگی امنیت است.

سناریو بینابینیِ استمرار دوگانگی، وضعیت دوگانه‌ای از شبکه و فضای مجازی را ترسیم می‌کند و به‌نوعی استمرار وضعیت کنونی کشور در این عرصه است. رویکرد این سناریو در توصیف امنیت و تاب‌آوری شبکه ملی اطلاعات به‌عنوان یک شبکه حیاتی بسیار مهم است، اما ازآنجاکه زیرساخت‌های کنونی شبکه ملی اطلاعات و بستر جاری فناوری اطلاعات در کشور از خارج تأمین می‌شود طبیعتاً خود وضعیت دوگانه ناامنی را رقم خواهد زد. در این رویکرد توجه به این نکته بسیار مهم و حیاتی است

که هر زمان پلتفرمی به‌صورت ملی و فراگیر خدماتی را ارائه می‌کند، طبعاً حاکمیت نیز وظایفی را برای حفظ و صیانت از آن در حوزه‌های سیاستگذاری‌های زیرساختی، مالیاتی، حقوقی و بیمه دارد تا این پلتفرم‌ها بتواند وارد حوزه صادرات شود که این امر می‌تواند اتفاق مهمی در زیست‌بوم فناوری اطلاعات کشور شود. ضمن اینکه براساس مدل چهار لایه‌ای فضای مجازی، باید تجهیزات زیرساختی شبکه ملی اطلاعات از امنیت لازم برخوردار باشد، اما این سناریو عملاً نقض آنچه گفته شده، است و عدم تأمین زیرساخت‌های مکفی، سبب استمرار دوگانگی شده است.

سناریو نامطلوبِ اسیری و آوارگی، مطلوبیت اجباری، شکننده و از روی ناچاری را برای حکومت ترسیم و نامطلوبِ کاربران است. این سناریو با این رویکرد ترسیم شده است که راه‌اندازی شبکه ملی اطلاعات می‌تواند بهبودهایی را در کیفیت ارتباطی کشور ایجاد کند و از دور زدن داده در مسیرهای طولانی جلوگیری کند، اما رویکرد سیاستگذاران در پیشبرد این شبکه، مقاومت‌هایی را در افکار عمومی ایجاد کرده است. رویکرد حاکمیت در این سناریو بر این دیدگاه شکل گرفته است که سرویس‌هایی را در بستر شبکه ملی ارائه کند. هرچند پس از تکمیل این سرویس‌ها نیز به‌جای تلاش در جهت مزیت‌زایی برای کاربران و ترغیب آنها به استفاده از این سرویس‌ها، الزام کاربران و محدود کردن برخی دسترسی‌ها به سرویس خارجی مشابه در دستور کار قرار گرفته، ولی درنهایت شکست این پروژه‌ها و بی‌میلی کاربران به استفاده از این خدمات را رقم زده است.

درنهایت سناریو بسیار نامطلوبِ پادشاهی تاریک، بدترین حالت از برقراری شبکه ملی در جامعه را به تصویر کشیده که هر چهار عدم قطعیت کلیدی آن، وضعیت نامطلوبی دارد و وقوع چنین سناریویی می‌تواند به‌شدت بر امنیت ملی تأثیرگذار باشد. آنچه که می‌توان با نگاه به نظریه‌های امنیتی درباره این سناریو توصیف کرد رویکرد صرف دیدگاه سلبی است که حاکمیت با سیاست کانالیزه کردن محیط پیرامونی کشور، قطع کامل دسترسی کاربران به شبکه جهانی را رقم زده است تا از این طریق بتواند هدف خود را محقق کند که افزایش سطح امنیت ملی است.

پیشنهادها

با توجه به سیاست‌های استعمارطلبانه و زورگویانه اغلب کشورهای صاحب فناوری برتر در حوزه اینترنت و همچنین نیاز واجب و ضروری جامعه به برقراری تعامل در بستر شبکه که زیرساخت ارتباطی فضای مجازی برای سازمان‌ها، دستگاه‌های اجرایی و کسب‌وکارها است، باید با همت مسئولان و نهادهای متولی، شبکه ملی اطلاعات راه‌اندازی شود، ازاین‌رو در جهت تحقق صحیح این موضوع، پیشنهادهای پژوهش به شرح موارد زیر مطرح می‌شود:

۱. براساس آنچه که در سناریو نخست «خانه امن و هوشمند» ترسیم شده؛ در راستای ارتقای سطح امنیتی بالا و مطلوب برای شبکه، مستقل بودن شبکه ملی اطلاعات مدنظر قرار گیرد و از طریق مجاری مربوطه مانند صداوسیما و مطبوعات، مزایای بهره‌مندی و استفاده از آن به اطلاع عموم برسد.

۲. مدیران راهبردی، امنیتی و دفاعی کشور برای مقابله پیش‌فعالانه و به‌منظور جلوگیری از هرگونه غافلگیری، با توجه به پیچیدگی تهدیدهای سایبری و ضعف نظارت بر بخش خصوصی، اشراف اطلاعاتی و توان دفاعی خود را در این زمینه افزایش دهند تا به‌نوعی هم از افزایش خشونت و رفتارهای اعتراضی در میان مردم جلوگیری شود و هم از شکسته شدن مرزهای امنیت ملی جلوگیری به‌عمل آید.

۳. دستیابی به فضای مجازی مطلوب بدون تحقق بستر آن یا شبکه ملی اطلاعات معنا ندارد، لذا تحقق شبکه ملی اطلاعات ترسیم شده در سناریو نخست «خانه امن و هوشمند»، درواقع تحقق بستر مناسب برای فضای مجازی مطلوب کشور است. بدون تردید، توسعه دانش‌بنیان این شبکه، انعطاف و انطباق همیشگی آن با الزامات جدید فضای مجازی را تضمین خواهد کرد.

۴. در مواجهه پیش‌دستانه با سناریو چهارم (استمرار دوگانگی) و با نگاه به تبعات سنگین وارده به کشور در صورت عدم استفاده از شبکه ملی اطلاعات، بسترهای قانونی و حقوقی نظارت بر فضای سایبر از طریق مجاری مربوطه فراهم شود.

۵. با توجه به آنچه که در سناریو پنجم (کورسوی امید) ترسیم شده است که به کاهش هزینه‌های جاری شهروندان در صورت استفاده از شبکه ملی اطلاعات منجر می‌شود و همچنین با امعان‌نظر به تهاجم اقتصادی که امروزه در ابعاد مختلف دامن‌گیر کشور شده است، دولت و سازمان‌های متولی امر، اعتبارات ریالی مناسب را به‌منظور توسعه زیرساخت‌های شبکه ملی اطلاعات فراهم کنند؛

۶. مزایای متعدد برقراری شبکه ملی اطلاعات ازجمله فعالیت در محیط امن، سالم و کنترل‌شده برای همه افراد جامعه خانواده‌ها، بی‌نیازی و وابسته نبودن به کشورهای سلطه‌طلب، در امان بودن اطلاعات مهم نظامی و امنیتی، حفظ جامعه از تهاجم فرهنگی و کمک اقتصادی به کشور که در سناریوی بسیار مطلوب «خانه امن و هوشمند» با وجه مثبت و در سناریوی بسیار نامطلوب «پادشاهی تاریک» با وجه منفی توصیف شد، اتخاذ رویکرد فوق فعالانه درخصوص ضرورت ایجاد این شبکه را طلب می‌کند.

۷. با توجه به بررسی‌هایی که این پژوهش در اسناد و مدارک مربوطه به شبکه ملی اطلاعات انجام داد در کنار چیستی و مستقل بودن یا نبودن شبکه ملی اطلاعات، اینکه چه ارگان یا نهادی مسئول اصلی راه‌اندازی بخش‌های مختلف این شبکه است، هنوز محلی از اعراب ندارد و به‌طور مشخص نهادی مسئول و متولی اصلی این قضیه نشده است. اصلح است در سند مادر شبکه ملی اطلاعات با توجه به اقتضائات روز بازنگری مجدد به‌عمل آید.

۸. مقوله شبکه ملی اطلاعات و اینترنت ملی در ادبیات و گفتار مسئولان و نهادهای ذی‌ربط از هم تمییز داده شود و به‌جای هم استفاده نشود.

۹. تخمین پیامدهای دسته دوم و دسته سوم هریک از سناریوها، در کنار پیامدهای دسته اول آنها، به پیش‌نگری و برنامه‌ریزی پیش‌دستانه در حوزه فضای مجازی کشور کمک می‌کند و باید ازسوی مدیران و مسئولان متولی در این حوزه مورد توجه قرار گیرد.

منابع و مآخذ

۱. اصلی‌زاده، احمد و حسین زین‌الدینی‌بیدمشکی (۱۳۹۵). «استخراج شاخص‌ها و آسیب‌شناسی ارائه خدمات ارتباطی بر روی شبکه ملی اطلاعات»، *مدیریت توسعه و تحول*، ۹ (۲۸).

۲. بیات، ابوالقاسم و محمد فتحیان (۱۴۰۰). «تبیین انگاره «اینترنت ملی» برپایه رویکرد تحلیل موقعیت»، *سیاست علم و فناوری*، ۱۴ (۳).

۳. بیات، بهرام (۱۳۹۸). *نظریه‌های امنیت ملی*، تهران، انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی.

۴. پدرام، عبدالرحیم و سلمان زالی (۱۳۹۷). «الگویی نوین برای سناریونویسی در موضوعات راهبردی (مطالعه موردی: سناریوهای آینده بحران سوریه)»، *مطالعات سیاسی جهان اسلام*، ۷ (۲).

۵. پدرام، عبدالرحیم و مهدی احمدیان (۱۳۹۴). *آموزه‌ها و آزموده‌های آینده‌پژوهی*، چاپ اول، تهران، نشر مؤسسه افق راهبردی.

۶. رحمانی، علیرضا، علیرضا احمدی، محسن کاظمی و محسن آقایی (۱۳۹۹). «شناسایی و رتبه‌بندی عوامل مؤثر بر شبکه ملی امن اطلاعات جمهوری اسلامی ایران»، *امنیت ملی*، ۱۰ (۳۸).

۷. رصاف‌بخش، رضا (۱۳۹۵). «بررسی تهدیدات فناوری اطلاعات و راه‌های مقابله با حملات جهت بهبود امنیت شبکه‌های کامپیوتری»، سومین کنفرانس بین‌المللی پژوهش در علوم و تکنولوژی، برلین، آلمان.

۸. رضایان قیه‌باشی، احد، علی‌اصغر پورعزت و بهرام سرمست (۱۳۹۶). «ارائه چارچوبی برای مطالعه شگفتی‌سازهای نظامی-دفاعی پیش‌روی جمهوری اسلامی ایران»، *آینده‌پژوهی دفاعی*، ۲ (۷).

۹. شوارتز، پیتر (۱۳۹۰). *هنر دورنگری: برنامه‌ریزی برای آینده در دنیایی با عدم قطعیت*، ترجمه عزیز علیزاده، چاپ اول، تهران، مرکز آینده‌پژوهی علوم و فناوری دفاعی، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

۱۰. شهیر، احسان (۱۳۹۶). «طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور»، رساله دکتری دانشگاه عالی دفاع ملی.

۱۱. عبداله‌خانی، علـــی (۱۳۸۳). *نظریه‌های امنیت (جلد اول): مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی*، چاپ اول، تهران، انتشارات مؤسسه ابرار معاصر.

۱۲. عبیری، داوود، رحیم یزدانی‌چهاربرج، خداداد هلیلی و کامیار سقفی (۱۳۹۹). «تبیین نقش شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدهای فضای مجازی»، *امنیت ملی*، سال ۱۰ (۳۷).

۱۳. عصاریان‌نژاد، حســـین و احمدعلی شـــریفی (۱۳۹۵). «نقش و جایگاه مدل شـــبکه‌ای، در اشراف ملی اطلاعات»، *امنیت ملی*، ۶ (۲۰).

۱۴. عیوضی، محمدرحیم، صفیه رضایی و محســـن محمدی خانقاهی (۱۴۰۰). «نقش شبکه ملی اطلاعات در تحکیم استقلال و امنیت ملی در گام دوم انقلاب اسلامی»، فصلنامه علمی *پژوهش‌های انقلاب اسلامی*، ۱۰ (۴).

۱۵. مرکز ملی فضای مجازی (۱۳۹۲).« شبکه ملی اطلاعات »، بازیابی از سایت http://majazi.ir/page/national-information-network

۱۶. نصرت‌آبادی، جمشـــید، محسن مؤمنه، محمدحسین یاقوت‌پور و محمد مهدی‌نژادنوری (۱۳۹۸). «ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات»، *امنیت ملی*، ۹ (۳۳).

۱۷. هاشمی، محمدســـاجد و محمدهادی همایون (۱۳۹۶). «بازنمایی شـــبکه ملی اطلاعات در رسانه‌های برون‌مرزی»، *مطالعات رسانه‌های نوین*، ۳ (۹).

۱۸. همایون، محمدهادی و محمدســـاجد هاشمی (۱۳۹۶). «جایگاه شبکه ملی اطلاعات در سپهر سیاست فرهنگی جمهوری اسلامی ایران»، *مطالعات راهبردی سیاستگذاری عمومی*، ۷ (۲۳).

19. Aslanbekov, R. (2017). "Chto Velikiy Dyadya Dumal 11 Iyunya 1997 Goda" [What the Great Man Was Thinking on the 1997], Cityline.ru. Retrieved 2017, from https://web. archive.org/web/19970730114907/www.cityline.ru/uncle/thinks/110697.html.

20. Beagrie, N. and J. Houghton (2016). *The Value and Impact of the European Bioinformatics Institute,* EMBL-EBI.

21. Bell, W. (2004). *Values, Objectivty, and the Good Society*, Vol II of Foundation of Futures Studies, New Brunswick, U.S.A and London, U.K.

22. Likhachev, N. (2015). "The Rise of Runet", 21-Retiye runeta [21st Anniversary of Runet], T Journal, Retrieved 2017, from https://tjournal.ru/54646-runet-21.

23. Lindwall, P. (2017). "Australian Medical Association-Productivity Commission", World Bank Group Publication, www.pc.gov.au.Implementation

24. Noordyke, M. (2020)."US State Comprehensive Privacy Law Comparison", International Association of Privacy Professionals.

25. Rippy, S. (2020). "US State Comprehensive Privacy Law Comparison", International Association of Privacy Professionals-Resource Center (blog).

26. Scott, M. and L. Cerulus (2018). *Europe's new Data Protection Rules Export Privacy Standards Worldwide*, Politico.

27. Shark Alan, R. (2015). *Technology and Public Management*, Rutledge Publisher, First Edition.

28. Tanner, M.S. (2017). *Beijing's New National Intelligence Law: From Defense to Offense,* Lawfare.

29. Yoon, Jeongwon (2016). "Korean Digital Government Infrastructure Building and Implementation", World Bank Group Publication.