فصلنامه علمی امنیت ملی
سال دهم، شماره سی‌وهفتم، پاییز ۱۳۹۹
مقاله سیزدهم از صفحات ۴۶۶-۴۳۷

مقاله پژوهشی: تبیین نقش شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدهای فضای مجازی کشور

داود عبیری[۱]، رحیم یزدانی چهار برج[۲]، خداداد هلیلی[۳]، کامیار ثقفی[۴]

تاریخ دریافت:۱۳۹۷/۱۲/۰۴ **تاریخ پذیرش:۱۳۹۷/۱۲/۱۴**

چکیده

شبکه ملی اطلاعات به‌منظور کاهش وابستگی به شبکه جهانی اینترنت و ارائه خدمات مناسب، امن و ارزان در فضای مجازی طرح‌ریزی شده است. این شبکه، دارای فرصت‌های فراوانی ازجمله تسریع در عرضه محتوا، اطلاعات و دانش، تسهیل و فراگیری خدمات الکترونیکی، کاهش هزینه‌ها، افزایش سلامت اداری، ایجاد و استفاده از موتور جستجو، شبکه‌های اجتماعی، رایانش ابری بومی و... می‌باشد. ایجاد و ارتقاء شبکه ملی اطلاعات منجر به امنیت اطلاعات، کاربران، حفظ حریم خصوصی و قطع وابستگی به کشورهای بیگانه می‌گردد؛ اما در کنار تمام مزایای مذکور، این شبکه دارای تهدیدهای متعددی است که در صورت عدم توجه به آن، علاوه بر اینکه امنیت اطلاعات و کاربران را دچار چالش می‌کند، منجر به هدررفت هزینه‌ها و درنهایت تضعیف امنیت ملی خواهد شد. تأمین امنیت فضای سایبر به‌منظور حفاظت از سرمایه‌های سایبری و صیانت از منافع ملی در راستای امنیت ملی کشور از دغدغه‌های مهم حاکمیت ا ست، این امر مهم محقق نمی‌گردد مگر با مدیریت فر صت‌ها و تهدیدهای ف ضای مجازی از طریق شبکه ملی اطلاعات. تحقیق حاضر از نظر هدف، کاربردی و از نظر ماهیت و روش گردآوری داده‌ها، توصیفی است. در این تحقیق با استفاده از روش کتابخانه‌ای نسبت به جمع‌آوری داده‌ها و دسته‌بندی آن‌ها اقدام شده و از طریق پرسشنامه محقق‌ساخته و جامعه آماری با حجم نمونه برابر فرمول کوکران ۹۶ نفر محا سبه و اطلاعات جمع‌آوری شده و مورد ارزیابی قرار گرفته ا ست. با استفاده از نرم‌افزارهای تحلیل داده، لیزرل و SPSS روایی و پایایی به تصویب رسیده و نتایج حاکی از آن است که میانگین فرصت‌های فضای مجازی با بار عاملی ۸۸/۴۵ و میانگین تهدیدهای فضای مجازی با بار عاملی ۸۷/۸۹ از طریق شبکه ملی قابل مدیریت است و درنهایت پیشنهادهای کاربردی در پایان ارائه شده است.

کلیدواژه‌ها: شبکه ملی اطلاعات، مدیریت، تهدیدها، فرصت‌ها، فضای مجازی

[۱]. دانشجوی دکترای امنیت سایبر، دانشگاه عالی دفاع ملی (نویسنده مسئول) ab.davood@chmail.ir
[۲]. دانشجوی دکترای امنیت سایبر، دانشگاه عالی دفاع ملی r.yazdani@sndu.ac.ir
[۳]. استادیار، عضو هیئت‌علمی دانشگاه شهید ستاری
[۴]. استاد، عضو هیئت‌علمی دانشگاه شاهد

مقدمه

در برخی از کشورها، گسترش و توسعه فضای مجازی به دلیل وابستگی به صاحبان تکنولوژی، بیش از آنکه در راستای تأمین منافع ملی و کسب امنیت ملی باشد؛ تهدیدی جدی علیه آن محسوب می‌گردد. این مسئله برای جمهوری اسلامی ایران که بر مبنای باورها و ارزش‌های دینی و گفتمان سلطه ناپذیری انقلاب اسلامی در جبهه مقابل جهانی‌سازی و استعمار نوین مجازی قرار گرفته، تهدیدات افزون‌تری را به همراه دارد. تقابل با هژمونی جریان سلطه و دشمنان نظام اسلامی به فضای سایبر کشیده شده و مواجهه مبتکرانه در این منازعه، مستلزم ایجاد یک زیر ساخت امن برای مدیریت، کنترل، نظارت بر تبادل اطلاعات و فراهم ساختن امنیت در این فضا است.

شبکه ملی اطلاعات یکی از کلان‌پروژه‌های ملی است که اولین بار در اواخر سال ۱۳۸۴ تحت عنوان اینترنت ملی و به‌منظور کاهش وابستگی به شبکه جهانی اینترنت و بهره‌گیری از فرصت‌های فضای مجازی برای نشر و اشاعه فرهنگ والای اسلامی مطرح شد. در سال ۱۳۸۹ در ماده ۴۶ برنامه پنجم توسعه به‌طورجدی به این مهم پرداخته شده و مقرر گردید تا پایان این برنامه در سال ۱۳۹۴، شبکه ملی اطلاعات به سطحی از توسعه و گستردگی برسد که ۶۰ درصد خانوارها و کسب‌وکارها به شبکه ملی اطلاعات متصل شوند.[1] پس از شکل‌گیری شورای عالی فضای مجازی در سال ۱۳۹۰، این شورا در جلسه پانزدهم خود در دی‌ماه ۱۳۹۲ الزامات شش‌گانه حاکم بر تحقق شبکه ملی اطلاعات را تصویب نمود؛ اما تبیین این الزامات سه سال بعد در جلسه سی و پنجم این شورا و در آذر ۱۳۹۵ انجام شد. طبق اعلام وزارت ارتباطات و فناوری اطلاعات، فاز سوم این شبکه در مرداد ۱۳۹۶ افتتاح شد؛[2] اما همچنان نقدهای جدی بر نحوه پیاده سازی و راه‌اندازی این شبکه وجود دارد(مرکز ملی فضای مجازی، ب، ۱۳۹۶).

---

[1]. به نقل از روزنامه اطلاعات در تاریخ ۱۳۹۲/۴/۲۰ (http://www.ettelaat.com)

[2]. به نقل از خبرگزاری صدا و سیما در تاریخ ۱۳۹۶/۵/۱ (http://www.iribnews.ir)

مهم‌ترین فلسفه شکل‌گیری شبکه ملی اطلاعات در مقابل شبکه جهانی اینترنت در کشور را می‌توان به مدیریت یا مقابله با تهدیدها و ایجاد فرصت‌ها و ارائه خدمات مناسب، امن و کم‌هزینه برای جامعه برشمرد.

بیان مسئله

راه‌اندازی شبکه ملی اطلاعات گامی مهم و اساسی در راستای تحقق آرمان‌ها و ارزش‌های متعالی انقلاب اسلامی و تحقق منویات و تأکیدات مقام معظم رهبری است. در این بخش مبانی ارزشی و دینی که اهمیت وجودی تشکیل و راه‌اندازی شبکه ملی اطلاعات را نشان می‌دهد؛ مورد بررسی قرار گرفته است.

از مهم‌ترین اهداف استکبار جهانی، تسلط بر کل جهان و حکومت بر آن است که دلیل بر این مدعی، پروتکل دانشوران صهیون می‌باشد (عجاج، ۱۳۸۷). نظام جمهوری اسلامی ایران، مانعی در مسیر نائل شدن آنان به هدفشان است. ازاین‌رو درصدد حذف و یا استحاله این نظام مقدس هستند. این مسئله باعث شده این نظام، همواره آماج هجمه حملات و تهدیدات مستکبرین چه به‌صورت سخت و چه به‌صورت نرم قرار گیرد. از مهم‌ترین ابزارهایی که استکبار جهانی به جهت حملات و اعمال تهدیدات از آن بهره می‌جوید، فضای مجازی است. بنا بر آیه ۱۹۴ سوره مبارکه بقره «...پس هر آن کس بر شما تعدی کرد شما هم به مثل او بر آن تعدی کنید ...». لزوم بهره‌گیری از فضای مجازی، جهت دادن پاسخ مشابه و هم‌جنس به مستکبرین و به موازات آن استفاده از فرصت‌های فضای مجازی مشخص می‌گردد. این نوع رویکرد در خصوص استفاده از فضای مجازی را می‌توان رویکرد تهدیدمحور یا مبتنی بر دفع تهدید دانست (قرآن کریم، بقره ۱۹۴).

مقام معظم رهبری می‌فرمایند: «آن‌ها (دشمنان) غافلند از اینکه این ابزارها می‌توانند مورد استفاده ما هم قرار بگیرد؛ یعنی وقتی اینترنت به وجود آمد، یک ابزار اختصاصی نبود، ما هم می‌توانیم از آن استفاده بکنیم، یعنی یک راه دوطرفه است. اگر دشمن می‌تواند از علوم ارتباطات و از پیشرفت‌ها و تازه‌های علمی این رشته استفاده کند، ما هم می‌توانیم

استفاده کنیم. ما هم باید دنبالش برویم تا استفاده کنیم. چه مانعی دارد؟ از همان شیوه‌هایی که ضلالت منتشر می‌کنند، می‌شود ما استفاده کنیم و هدایت را منتشر کنیم. استعداد ما در استفاده از ابزارها، استعداد بالایی است. باید از این‌گونه ابزارها استفاده کرد تا هرچه ممکن است دایره اثرگذاری خود را وسیع‌تر کنید»؛ بنابراین در مواجهه با فضای مجازی، از رویکرد فرصت‌محور نیز، نباید غافل شد.

در طراحی این شبکه، ویژگی‌ها و قابلیت‌های خاص بومی مانند استقلال از شبکه جهانی توأم با دسترسی مدیریت‌شده به آن، نظارت، مدیریت و کنترل در همه سطوح شبکه، سازگاری با فناوری‌های نسل جدید و... مورد توجه سیاست‌گذاران و متولیان راه‌اندازی قرار گرفته است. با این وجود، همواره یکی از مهم‌ترین دغدغه‌ها و مطالبات ذینفعان این شبکه، شفاف‌سازی چگونگی پیشگیری از حملات سایبری و مقابله با تهدیدات امنیتی فضای سایبر توسط این شبکه است.

بنابراین دغدغه اصلی شکل‌گیری این تحقیق، احصاء فرصت‌ها و تهدیدهای فضای مجازی و مدیریت آن‌ها از طریق شبکه ملی اطلاعات به‌منظور کاهش یا حذف تهدیدها و افزایش فرصت‌های فضای مجازی است.

اهمیت و ضرورت تحقیق

وابستگی زیرساخت‌های اقتصادی، اجتماعی، سیاسی، فرهنگی و نظامی به فضای مجازی، شرایط را به‌گونه‌ای رقم زده که هرگونه چالش در این فضا می‌تواند مؤلفه‌های امنیت ملی را دستخوش تغییر و تحول نماید. فضای مجازی علاوه بر اینکه ابزاری برای ارتقاء امنیت ملی محسوب می‌شود، بستری برای تهدید مؤلفه‌های امنیت ملی نیز محسوب می‌گردد. به این دلیل امنیت این فضا مؤلفه مهمی از امنیت ملی محسوب می‌گردد.

ارتقاء و تحکیم امنیت ملی، نیاز اساسی و اصلی‌ترین وظیفه دولت در قلمرو حاکمیتی آن، مفهومی گسترده است که پیاده‌سازی و پایداری آن مستلزم شناخت محیط به‌خصوص فرصت‌ها و تهدیدهاست. 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. ارگان‌ها و نهادهای سیاسی در نیل به آرمان‌ها، تعیین و تحصیل منافع امنیت ملی، تعقیب اهداف و اولویت‌های خود، قدرت ملی را بسیج کرده و آسیب‌ها، چالش‌ها و تهدیدات در محیط هدف را مدیریت می‌کنند (کرمی، ۱۳۸۰: ۷۰-۶۷)

مقام معظم رهبری، این مهم را به‌خوبی پیش‌بینی نموده و مجدانه آن را پیگیری می‌نمایند و در فرازی از فرمایشاتشان می‌فرمایند: «نسبت به مخدوش کردن آرامش و امنیت ملی هوشیار باشید». واقعیت آن است که جدید بودن حوزه فضای مجازی و نقش آن در امنیت ملی، بیانگر لزوم توجه و ورود هوشمندانه به این عرصه است.

شبکه ملی اطلاعات یکی از موضوعات راهبردی و مهم است که در صورت تحقق آن، می‌تواند امنیت و آرامش را برای جامعه به ارمغان آورد و در صورت بی‌توجهی به آن، می‌تواند امنیت ملی کشور را به چالش بکشد. در شرایط کنونی به دلیل عجین شدن زندگی مردم با فضای مجازی و نقش پررنگ شبکه ملی اطلاعات در ارتقاء امنیت و آسایش مردم، مدیریت فرصت‌ها و تهدیدهای فضای مجازی می‌تواند منجر به ارتقاء حاکمیت نظام مقدس جمهوری اسلامی ایران گردد.

بنابراین در بخش اهمیت، انجام این تحقیق می‌تواند منجر به؛

۱. ارتقاء امنیت ملی کشور گردد.
۲. ارتقاء آسایش مردم جامعه گردد.
۳. از غافلگیری راهبردی جلوگیری نماید.
۴. از دستیابی به اهداف شوم دشمن جلوگیری نماید.

و همچنین در بخش ضرورت، در صورت عدم انجام این تحقیق؛

۱. منجر به سلطه دشمن از طریق فضای مجازی گردد.
۲. ضمن خروج اطلاعات از کشور، منجر به نقض حریم خصوصی گردد.
۳. منجر به ضعف در مدیریت فرصت‌ها و تهدیدها و درنهایت تضعیف حاکمیت گردد.

اهداف تحقیق

هدف اصلی: تبیین نقش شبکه ملی اطلاعات در مدیریت تهدیدها و فرصت‌های فضای مجازی

اهداف فرعی

۱. میزان مدیریت فرصت‌های فضای مجازی از طریق شبکه ملی اطلاعات
۲. میزان مدیریت تهدیدهای فضای مجازی از طریق شبکه ملی اطلاعات

سؤالات تحقیق

سؤال اصلی: آیا شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدهای فضای مجازی نقش دارد؟

سؤالات فرعی

۱. شبکه ملی اطلاعات در مدیریت فرصت‌های فضای مجازی به چه میزان نقش دارد؟
۲. شبکه ملی اطلاعات در مدیریت تهدیدهای فضای مجازی به چه میزان نقش دارد؟

مبانی نظری و ادبیات تحقیق

پیشینه تحقیق

تحقیقی با موضوع «امنیت ملی در فضای سایبر» توسط دکتر مرتضی واحدی و دکتر محمدحسین صنیعی در داعا انجام شده که در آن ذکر شده با توجه به اینکه بنیان‌های اقتصادی و حتی سیاسی، فرهنگی و نظامی به‌گونه‌ای بر بستر فضای سایبر قرار گرفته و یا در حال قرار گرفتن است. ازاین‌رو ایجاد هرگونه اشکال در این فضا می‌تواند چالش‌های پیچیده و فلج‌کننده‌ای را برای نظام پدید آورد. این چالش‌ها می‌تواند امنیت ملی را مخدوش

کند. برای تأمین امنیت ملی باید از حوزه شناخت خودی صیانت نمود و بر حوزه شناخت دشمن اثر گذاشت. این کار با بهره‌گیری از فضای سایبر انجام می‌شود. بهره‌برداری از فضای سایبر در این حوزه انتخابی نیست، بلکه اجباری است. در این طرح پژوهشی مؤلفه‌های حفظ و تحکیم امنیت ملی در فضای سایبر طبقه‌بندی شده و مورد بررسی قرار گرفته است (واحدی، ۱۳۹۲).

تحقیق دیگری با عنوان «راهبردهای پدافند غیرعامل زیرساخت‌های ارتباطی شبکه ملی اطلاعات کشور در برابر تهدیدات سایبری» توسط سید علی میررفیع، در سال ۱۳۹۴ در دانشگاه عالی دفاع ملی انجام گرفته که به نتایجی از قبیل؛ مصون‌سازی، استحکام‌بخشی و امن‌سازی زیرساخت‌های ارتباطی حیاتی، حساس و مهم شبکه ملی اطلاعات در برابر تهدیدات و حملات سایبری و الکترومغناطیسی، بهره‌گیری از زیرساخت‌های ارتباطی خاص مراکز حیاتی و حساس شبکه ملی اطلاعات کشور بر اساس ملاحظات، اصول و ضوابط پدافند غیرعامل با سطح پایداری ملی و حمایت از محصولات سایبری بومی و افزایش سالانه سهم این محصولات در سبد خرید زیرساخت ارتباطی شبکه ملی اطلاعات کشور پرداخته است (میررفیع، ۱۳۹۴).

بسیاری از کشورها به‌منظور مدیریت بهینه کشور و دسترسی به خدمات و اطلاعات، اقدام به طرح‌ریزی و پیاده‌سازی زیرساخت ارتباطی پهن‌باند و مستقل از اینترنت با مدیریت داخلی نموده‌اند. به‌عنوان مثال در کره جنوبی طرح تجمیع حکمرانی الکترونیکی و ارتباطات پخش همگانی با ایجاد بستری ۵۰ مگابیتی در همه مناطق شهری و روستایی بر بستر فیبر نوری در سال ۲۰۱۰ اجرا شده است (Yoon, 2016: 47). در ایالات‌متحده یک شبکه عمومی پهن‌باند برای دسترسی ارزان و مقرون‌به‌صرفه برای بیش از صد میلیون خانوار در سال ۲۰۱۵ میلادی در نظر گرفته شده است(Shark, 2015). استرالیا یکی دیگر از پیشگامان توسعه شبکه پهن‌باند ملی (NBN)[1] است. در این کشور، خدمات پهن‌باند و پرسرعت با ترکیبی از روش‌های مختلف مخابراتی ارائه می‌شود(Lindwall, 2017). در کشور چین نیز از موتور جستجو و شبکه‌های پیام‌رسان بومی استفاده می‌شود؛ این کشور قصد دارد تا سال

1. National Broadband Network

۲۰۲۰ سرعت اینترنت خود را تا ۵۰ مگابیت بر ثانیه برساند، این کشور قصد دارد تا سال ۲۰۲۰ سرعت اینترنت خود در مناطق شهری را به ۵۰ مگابیت بر ثانیه و سرعت اینترنت در مناطق روستایی را به ۱۲ مگابیت در ثانیه و سرعت اینترنت در شهرهای بزرگ و پیشرفته‌تر این کشور را به ۱۰۰۰ مگابیت در ثانیه افزایش دهد. یکی از اهداف کشور چین، داشتن فناوری ابداعی، رقابت صنعتی، تطبیق با استانداردهای پیشرو، سیستم و شبکه‌ای با امنیت اطلاعات است(Ben & Others, 2017: 26).

به‌هرحال استفاده از فضای مجازی در شرایط کنونی امری اجتناب‌ناپذیر و اجباری است، این فضا دارای فرصت‌ها و تهدیدهای متعددی است که سایر کشورها از طریق شبکه بومی یا داخلی، درصدد مدیریت فرصت‌ها و تهدیدهای آن هستند.

مفاهیم و اصطلاحات تحقیق

شبکه ملی اطلاعات: در منابع مختلفی؛ مانند کتاب «شبکه ملی اینترنت» (ریاضی،۱۳۸۸:۱۶)، پروژه تحقیقاتی بازنگری مفاهیم شبکه ملی اطلاعات، سازمان فناوری اطلاعات و تبصره ۲ ماده ۴۶ قانون برنامه پنجم توسعه، تعاریفی برای شبکه ملی اطلاعات ارائه شده است. شورای عالی فضای مجازی این شبکه را به‌صورت زیر تعریف نموده که در این مقاله پس از بررسی تعاریف مختلف، به‌عنوان تعریف عملیاتی انتخاب شده است:

«شبکه ملی اطلاعات، به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است، به‌صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شود، به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود».

امنیت ملی: امنیت ملی با نگاه سلبی عبارت است از: وضعیتی که منافع حیاتی بازیگر از سوی دیگر بازیگران یا در معرض تهدید نباشد و یا در صورت وجود تهدید احتمالی، بازیگر توان دفع و مدیریت آن را با هدف صیانت از منافع خود داشته باشد.

امنیت ملی با نگاه ایجابی؛ امنیت ملی وضـــعیتی مبتنی بر وجود نوعی رابطه معقول و متناسب بین خواسته‌های بازیگران با داشته‌های ایشان درون یک واحد سیاسی است که درنهایت تولید رضـــایت‌مندی نزد بازیگران می‌کند (بالایی و همکاران، ۱۳۹۲). امنیت ملی عبارت است از: ایجاد شرایط مساعد ملی و بین‌المللی، جهت حفظ یا بسط ارزش‌های حیاتی ملی (ماندل، ۱۳۸۷:۴۱).

امنیت در شبکه ملی اطلاعات: امنیت در شـبکه ملی اطلاعات به معنای امن بودن این شبکه در تمامی لایه‌ها و تضمین امنیت برای فضای مجازی کشور است. در سند افتا (امنیت فضای تولید و تبادل اطلاعات) امنیت فضای مجازی به معنای پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید (کاهش آسیب‌پذیری‌ها و حملات سایبری) و کنترل و شنود جهت ردیابی جرائم به‌منظور صیانت از اسرار کشور، حراست اطلاعات حساس و سرمایه‌های مادی و معنوی معرفی شده است. بر اساس این سند راهبردی، امنیت در لایه فیزیکی، مسـیریابی، مراکز داده و... باید در یک بسـتر امن صـورت گیرد و تبادل اطلاعات خارجی و دسـترسـی به اینترنت نیز برای کاربران باید به‌صـورت حفاظت‌شـده و تعاملی انجام شود؛ بنابراین در امنیت شبکه ملی اطلاعات، تمامی مکانیزم‌های امنیتی؛ مانند جامعیت داده، محرمانگی، احراز هویت، کنترل دسـترسـی، انکارناپذیری و دسـترس‌پذیری باید مورد توجه قرار گیرد[1](سند افتا).

تعریف فرصت: فرصت پتانسیل نهفته‌ای است که بهره‌گیری از آن سازمان را در جهت مثبت رشد خواهد داد، به‌عبارت‌دیگر منفعت بالقوه‌ای است که هنوز بالفعل نشده است (علی احمدی،۱۳۸۲: ۱۸۳).

تعریف تهدید: هر عنصر یا وضعیتی که موجودیت منافع یا ارزش‌های حیاتی سازمان را به خطر اندازد، تهدید محسوب می‌شود (حسن‌بیگی،۱۳۹۰: ۳۰۹).

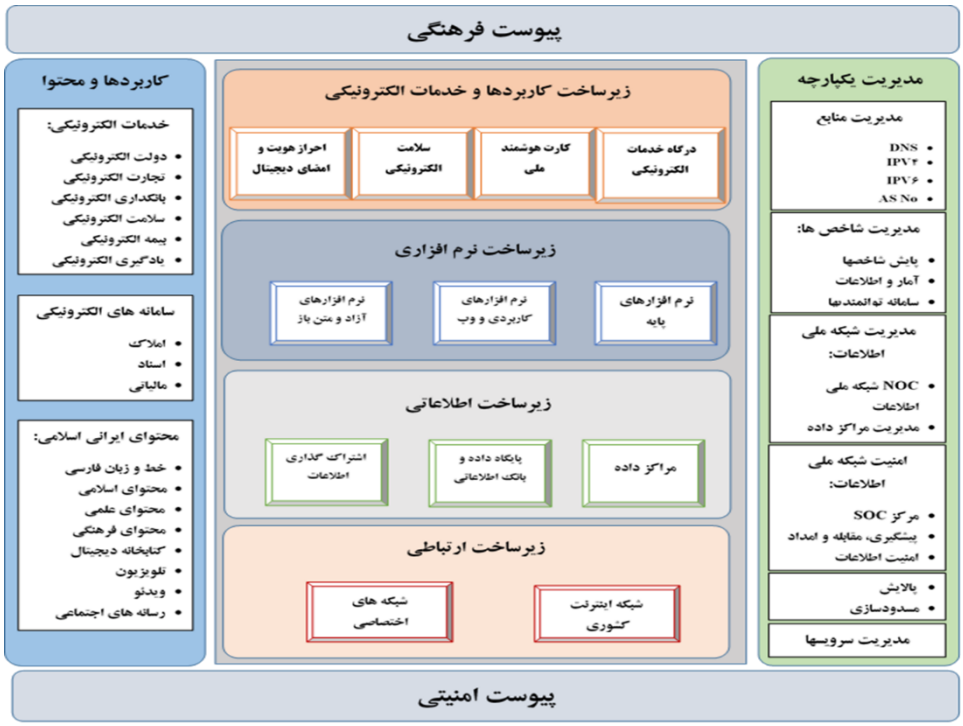
مفاهیم و مبانی شبکه ملی اطلاعات

شبکه ملی اطلاعات، از سه جزء اصلی زیرساخت‌ها، مدیریت یکپارچه و کاربردها و

---

[1]. سیاست‌های کلی نظام در امنیت فضای تولید و تبادل اطلاعات (سند افتا)

محتوا و دو پیوست امنیتی و فرهنگی تشکیل شده است. زیرساخت؛ شامل زیرساخت‌های ارتباطی، اطلاعاتی، نرم‌افزاری و کاربردی (خدمات الکترونیکی) اســت. مدیریت یکپارچه به مدیریت منابع، مدیریت شاخص‌ها، امنیت و مدیریت خدمات شبکه تق سیم می شود. بخش کاربردها و محتوا نیز؛ شامل خدمات الکترونیکی، سامانه‌های الکترونیکی و محتوای ایرانی- ا سلامی می شود. در شکل (۱-۱) اجزای شبکه ملی اطلاعات ن شان داده شده است(مرادحاصل، ۱۳۹۱: ۱۰۰).



شکل شماره ۱-۱: اجزای شبکه ملی اطلاعات (مرادحاصل، ۱۳۹۱: ۱۰۰).

در مدل چهارلایه‌ای فضای مجازی کشور، فضای مجازی کشور در صورتی می‌تواند کاملاً بومی، قابل کنترل و تحت حاکمیت باشــد که تمامی لایه‌های آن بر مبنای منافع و اهداف کلان ملی پایه گذاری شود. این بدان معنا ست که لایه محتوا بر مبنای ارزش‌های ایرانی- اسلامی، لایه خدمات بر مبنای نیازهای متعارف و واقعی داخلی، لایه زیرساخت

دارای قابلیت مدیریت مستقل داخلی و کاربران امکان تعامل مدیریت‌شده را در این فضا داشته باشند. البته باید به این نکته نیز توجه داشت، فضای مجازی کشور در عین استقلال داخلی باید قابلیت تعامل با شبکه جهانی اینترنت را داشته باشد تا هم بتوان از ظرفیت فضای مجازی جهت جهانی‌سازی بر مبنای ایدئولوژی تمدن اسلامی بهره برد و هم از محتوا و خدمات مفید بین‌المللی استفاده کرد (مرکز ملی فضای مجازی، الف، ۱۳۹۶).

بسیاری از کشورها ازجمله ایالات‌متحده آمریکا[۱] انگلستان و اتحادیه اروپا[۲] اقدام به تدوین راهبردهای امنیت فضای سایبری و انتشار آن نموده‌اند. در جمهوری اسلامی ایران نیز امنیت شبکه ملی اطلاعات به خاطر تأثیرگذاری بر تمامی حوزه‌های ابعاد امنیت ملی، از موضوعات راهبردی محسوب می‌شود و نیل به آن مستلزم داشتن نقشه راه، سیاست‌گذاری و راهبردهای مناسب است (سایت دولت آمریکا و اروپا، ۱۳۹۶).

در جدول (۱-۱) اهم مطالب مرتبط با موضوع شبکه ملی اطلاعات و امنیت فضای مجازی در بیانات و فرامین مقام معظم رهبری (مدظله‌العالی)، سیاست‌های ابلاغی و اسناد بالادستی ارائه شده است.

---

۱. https://www.gov.uk

۲. https://www.enisa.europa.eu

جدول (۱-۱): مطالب مرتبط با شبکه ملی اطلاعات در بیانات مقام معظم رهبری (مدظله‌العالی)، سیاست‌های ابلاغی و اسناد بالادستی

در فضای مجازی، بهمنی از مسائل ضد ارزشی و مخالف منافع ملی، مطالب درست و نادرست، اطلاعات غلط یا صحیح و حتی شبه‌اطلاعات بر ذهن جامعه فرود می‌آید که باید این فضا کنترل شود، اما نباید ملت را از فضای مجازی محروم کرد. ... باید همه مردم بتوانند از منافع فضای مجازی استفاده کنند و در زمینه‌هایی که به ضرر کشور، افکار عمومی و به‌ویژه جوانان نیست، سرعت اینترنت افزایش یابد و هر کار لازم دیگر نیز انجام شود... شماری از کشورها با ایجاد شبکه ملی اطلاعات، ضمن رعایت خطوط قرمز خود و کنترل صحیح فضای مجازی، از اینترنت برای تأمین منافعشان بهره گرفته‌اند. ...در مسئله فضای مجازی، آنچه از همه مهم‌تر است، مسئله شبکه ملّی اطلاعات است. متأسفانه در این زمینه کوتاهی شده، کاری که باید انجام بگیرد، انجام نگرفته؛ این [طور] نمی‌شود. اینکه ما به‌عنوان اینکه نباید جلوی فضای مجازی را گرفت، در این زمینه‌ها کوتاهی کنیم، این مسئله‌ای را حل نمی‌کند و منطق درستی هم نیست. خب امروز فضای مجازی مخصوص ما که نیست، همه دنیا امروز درگیرند با فضای مجازی؛ کشورهایی که شبکه ملی اطلاعات درست کرده‌اند و [فضای مجازی را] کنترل کرده‌اند به نفع خودشان و به نفع ارزش‌های مورد نظر خودشان، یکی دو تا نیستند. بهترینِ کشورها، قوی‌ترینِ کشورها، در این زمینه‌ها خط قرمز دارند؛ راه نمی‌دهند؛ خیلی از بخش‌های فضای مجازی اعزام‌شده از سوی آمریکا و دستگاه‌های پشت سر و پشت‌صحنه این قضیه را راه نمی‌دهند؛ کنترل می‌کنند. ما هم باید کنترل کنیم.	بیانات در دیدار مسئولان نظام در تاریخ ۱۳۹۶/۳/۲۲
فضای مجازی واقعاً یک دنیای رو به رشدِ غیرقابل توقف است، یعنی واقعاً آخر ندارد؛ آدم هرچه نگاه می‌کند، آن چیزِ اولِ بلاآخر، فضای مجازی است. هرچه انسان پیش می‌رود در این فضا، این همین‌طور ادامه دارد. این یک فرصت‌های بزرگی در اختیار هر کشوری می‌گذارد، تهدیدهایی هم در کنارش دارد؛ ما بایستی کاری کنیم که از آن فرصت‌ها حداکثر استفاده را بکنیم، از این تهدیدها تا آنجایی که ممکن است خودمان را برکنار نگه بداریم... . شورای عالی فضای مجازی به این منظور تشکیل شد. ... شبکه ملی اطلاعات را -که خیلی مهم است آن شبکه داخلی- ما هنوز پیش نرفته‌ایم؛... با اینکه همه معتقدند به این قضیه، اما این پیشرفت نداشته؛ این را بایستی ان‌شاءالله دنبال کنیم که ضربه‌های بی‌جبرانی نزنیم... .	بیانات در دیدار رئیس‌جمهور و اعضای هیئت دولت در تاریخ ۱۳۹۵/۶/۳
وزارت ارتباطات و فناوری اطلاعات مکلف است تا پایان اجرای قانون برنامه نسبت به توسعه و تکمیل شبکه ملی اطلاعات، امن و پایدار اقدام نماید تا امکان دسترسی به سطح یکی از سه کشور اول منطقه فراهم شود.	ماده ۶۸ قانون برنامه پنج‌ساله ششم توسعه مجلس شورای اسلامی در تاریخ ۱۳۹۵/۱۲/۱۴

تسریع در راه‌اندازی شبکه ملی اطلاعات پس از تصویب طرح آن در شورای عالی و نظارت مستمر و مؤثر مرکز ملی بر مراحل راه‌اندازی و بهره‌برداری از آن.	حکم انتصاب اعضای شورای عالی فضای مجازی در تاریخ ۱۳۹۴/۶/۱۴
– ایجاد، تکمیل و توسعه شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمندانه و ساماندهی، احراز هویت و تحول در شاخص ترافیکی شبکه به‌طوری‌که ۵۱ درصد آن داخلی باشد. – افزایش ظرفیت‌های قدرت نرم و دفاع سایبری و تأمین پدافند و امنیت سایبری برای زیرساخت‌های کشور در چارچوب سیاست‌های کلی مصوب.	بند ۳۴ و بند ۵۳ سیاست‌های کلی برنامه ششم توسعه در تاریخ ۱۳۹۴/۴/۹
الزامات حاکم بر تحقق شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباط فضای مجازی کشور: ۱. شبکه‌ای متشکل از زیرساخت‌های ارتباطی با مدیریت مستقل کاملاً داخلی؛ ۲. شبکه‌ای کاملاً مستقل و حفاظت‌شده نسبت به دیگر شبکه‌ها (ازجمله اینترنت) با امکان تعامل مدیریت‌شده با آن‌ها؛ ۳. شبکه‌ای با امکان عرضه انواع محتوا و خدمات ارتباطی سراسری برای آحاد مردم با تضمین کیفیت ازجمله قابلیت تحرک؛ ۴. شبکه‌ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتالی به کلیه کاربران؛ ۵. شبکه‌ای با قابلیت برقراری ارتباطات امن و پایدار میان دستگاه‌ها و مراکز حیاتی کشور؛ ۶. شبکه‌ای پرظرفیت، پهن‌باند و با تعرفه رقابتی شامل مراکز داده و میزبانی داخلی	مصوبه جلسه پانزدهم شورای عالی فضای مجازی در تاریخ ۱۳۹۲/۱۱/۱۲
وزارت ارتباطات و فناوری اطلاعات مکلف است نسبت به ایجاد و توسعه شبکه ملی اطلاعات و مراکز داده داخلی امن و پایدار با پهنای باند مناسب با رعایت موازین شرعی و امنیتی کشور مناسب اقدام و با استفاده از توان و ظرفیت بخش‌های عمومی غیردولتی، خصوصی و تعاونی، امکان دسترسی پرسرعت مبتنی بر توافقنامه سطح خدمات را به صورتی فراهم نماید که تا پایان سال دوم کلیه دستگاه‌های اجرایی و واحدهای تابعه و وابسته و تا پایان برنامه، شصت درصد (۶۰٪) خانوارها و کلیه کسب‌وکارها بتوانند به شبکه ملی اطلاعات و اینترنت متصل شوند.	ماده ۴۶ قانون برنامه پنج‌ساله پنجم توسعه در تاریخ ۱۳۸۹/۱۰/۱۵
– ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی ساختارهای حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات – ارتقاء مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور – توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی – تعامل مؤثر و سازنده منطقه‌ای و جهانی و همکاری و سرمایه‌گذاری مشترک در حوزه‌های دانش، فناوری و امور مربوط به امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی با حفظ منافع و امنیت ملی – تعیین نهاد متولی و هماهنگ‌کننده زیر نظر دولت به‌منظور هدایت، نظارت و تدوین استانداردهای لازم برای حفظ و توسعه امنیت فضای تولید و تبادل اطلاعات و ارتباطات	سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)» در تاریخ ۱۳۸۹/۱۱/۲۹

شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی است و فضای مجازی نیز مولود فناوری اطلاعات محسوب می‌شود. این فناوری در کنار سه فناوری نانو، زیستی و شناختی به‌عنوان فناوری‌های همگرا شناخته می‌شود[1] در کتاب «همگرایی دانش، فناوری و جامعه، فراتر از همگرایی فناوری‌های نانو، زیستی، اطلاعاتی و شناختی»، تأمین نیازهای جامعه بشری و بهبود کیفیت زندگی به‌عنوان مهم‌ترین استفاده از فناوری مطرح شده است (میهایل و همکاران، ۲۰۱۳). فناوری اطلاعات نیز موجب تسهیل و تسریع در برآورده شدن بسیاری از نیازهای جامعه شده است؛ اما نباید از تهدیدات امنیتی این فناوری نیز غافل شد.

با مروری بر موارد مطرح‌شده در جدول (۱-۱) در اسناد بالادستی از سال ۱۳۸۹ تاکنون، می‌توان گفت راه‌اندازی شبکه ملی اطلاعات گامی مهم و حیاتی برای بهره‌برداری از فرصت‌ها و قابلیت‌ها فضای مجازی است. این شبکه امکان صرفه‌جویی اقتصادی، توسعه فضای کسب‌وکار، افزایش سرعت دسترسی کاربران به منابع داخلی و تحقق دولت الکترونیکی را فراهم خواهد نمود و تحقق این اهداف به امنیت این شبکه وابسته است. برخی دیگر از پیامدهای امنیت شبکه ملی اطلاعات از منظر راهبردی که در جلسات خبرگی احصاء شده است عبارت‌اند از:

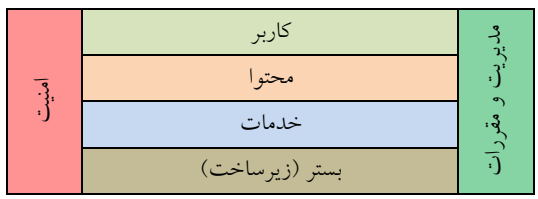
۱. جلوگیری از قطع ارتباطات اینترنتی به‌خصوص ارتباطات داخلی توسط بیگانگان
۲. جلوگیری از تحلیل اطلاعات توسط بیگانگان به سبب عدم خروج اطلاعات داخلی به بیرون از کشور
۳. جلوگیری از ذهن‌خوانی، داده‌کاوی، ذائقه سنجی و رفتارشناسی کاربران ایرانی توسط کشورهای بیگانه به‌خصوص از طریق شرکت‌های بزرگ و غول‌های فناوری دنیا
۴. عدم وابستگی به بیگانگان در ارتباطات داخلی
۵. جلوگیری از گمنامی و فعالیت‌های پنهانی افراد در شبکه ملی اطلاعات
۶. کاهش جرائم و تخلفات به سبب احراز هویت کاربران در شبکه ملی اطلاعات
۷. جلوگیری از فعالیت‌های اقتصادی خارج از قوانین و مقررات کشور

---

1. Nano – Bio – Information – Cognitive (NBIC)

۸. شناسایی متخلفین و مجرمین در شبکه ملی اطلاعات
۹. جلوگیری از فعالیت‌های ضد دین و نظام در شبکه ملی اطلاعات
۱۰.جلوگیری از خروج اطلاعات و سرقت اطلاعات توسط بیگانگان
۱۱.ایجاد مدیریت مستقل برای ارتباطات داخل و خارج از کشور
۱۲.جلوگیری از حملات سایبری کشورهای بیگانه
۱۳.جلوگیری از تهاجم فرهنگی، تبلیغات اغواگر، ترویج پروپاگاندا، عملیات روانی و نفوذ جریانی
۱۴.سازماندهی تهدیدات سایبری علیه جمهوری اسلامی ایران
۱۵.جلوگیری از ترویج یاس و ناامیدی، ایجاد تفرقه و اختلافات قومی و مذهبی در بین آحاد جامعه و تغییر بنیان‌های اعتقادی، اخلاقی و فرهنگی از طریق فضای سایبر
۱۶.مدیریت هوشمند انتشار و دسترسی به اطلاعات الکترونیکی در شبکه ملی اطلاعات
۱۷.ارتقاء سطح دانش کارشناسان و متخصصین داخلی
۱۸.جلوگیری از خروج ارز و دارایی‌های کشور به خارج از کشور

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 تمامی اجزاء و حوزه‌های کاربردی خدمات و محتوا، از سطح مطلوبی از امنیت برخوردار با شد. در غیر این صورت، ناامن بودن این شبکه، تهدیدات امنیتی را در سطوح مختلف کاربران، جامعه و دولت ایجاد خواهد نمود. شورای عالی فضای مجازی یک مدل چهارلایه‌ای برای فضای مجازی کشور ارائه داده است که در شکل (۱-۲) آمده است (مرکز ملی فضای مجازی، الف، ۱۳۹۶).



شکل (۱-۲): مدل چهارلایه‌ای فضای مجازی (مرکز ملی فضای مجازی، الف، ۱۳۹۶)

بر اساس این مدل لایه‌ای، شبکه ملی اطلاعات به‌عنوان بستر یا زیرساخت ارتباطی فضای مجازی کشور در نظر گرفته شده است. بر مبنای شکل (۱-۲) اجزای شبکه ملی اطلاعات علاوه بر زیرساخت‌های اطلاعاتی و ارتباطی، شامل بخش‌های مدیریت یکپارچه، کاربر، محتوا و دو پیوست فرهنگی و امنیتی نیز می‌باشد؛ بنابراین امن بودن شبکه ملی اطلاعات با امن بودن سه لایه دیگر فضای مجازی؛ یعنی خدمات، محتوا و کاربران نیز مرتبط است.

در این بخش امنیت شبکه ملی اطلاعات در چهار لایه زیرساخت، خدمات و محتوا مورد بررسی قرار گرفته و برای هر لایه، شاخص‌های امنیتی احصاء شده است. امنیت در لایه زیرساخت؛ شامل امن بودن اجزای این لایه؛ مانند تجهیزات ارتباطی، سوئیچینگ، مسیریاب، مراکز داده و تجهیزات امنیتی است. این مسئله پیش‌نیاز امنیت در لایه خدمات و محتواست. در لایه خدمات، امنیت خود خدمات، ارائه امنیت به‌عنوان خدمت، خدمات مربوط به احراز هویت و جامعیت و محرمانگی و همچنین امنیت مواردی، مانند سیستم‌عامل، منابع و بانک‌های اطلاعاتی، خدمات، پرتال‌ها، شبکه‌های اینترانتی و اختصاصی، پروتکل‌های ارتباطی، رابط‌ها[1] و میان‌افزارهای[2] لازم برای تعامل سیستم‌ها، نرم‌افزارها، پردازش‌ها و برنامه‌های کاربردی مطرح هستند.

در لایه محتوا نیز فرایندهای تولید، توزیع، مدیریت و بهره‌برداری از محتوا باید در یک بستر امن قرار گیرد. همچنین تبادل اطلاعات خارجی (دسترسی به شبکه جهانی اینترنت) باید به‌صورت حفاظت‌شده، قابل کنترل و تعاملی مد نظر قرار گیرد.

در لایه کاربران، امنیت؛ شامل اعتماد کاربران، آموزش و آگاهی‌بخشی و هشداردهی، حفاظت از حریم خصوصی، عدم افشای هویت، احراز هویت، مدیریت مجوزها و کنترل دسترسی، کنترل لاگ فعالیت‌ها، محرمانگی در اطلاعات و داده کاربران می‌باشد.

پس از جلسات خبرگی متعدد، ویژگی‌های امنیتی هرکدام از این سه لایه احصاء شد که این مسئله در جدول (۳-۲) نشان داده شده است.

---

۱. Application Programming Interface (API)

۲. Middleware

جدول (۱-۲): لایه‌های فضای مجازی و شاخص‌های امنیت شبکه ملی اطلاعات در هر لایه

لایه‌های فضای مجازی	شاخص‌های امنیتی شبکه ملی اطلاعات
لایه زیرساخت	مکانیسم‌های امنیتی، پروتکل‌های امنیتی، الگوریتم‌های رمزنگاری داخلی، امضای الکترونیکی و گواهی دیجیتال، استفاده از نرم‌افزارهای خاص در جاهای خاص، پنهان کردن ساختار شبکه، مدیریت پیکربندی، پنهان کردن و مدیریت IP ها، مدیریت کاربران و کنترل دسترسی آن‌ها، رصد و پایش (گرفتن گردش کار از اتصالات به سرورها و لاگ‌گیری)، داشتن نگاه فرایندی به امنیت، انجام مرتب تست‌های نفوذ، دسترسی به اینترنت به‌صورت تعاملی، مدیریت شده و حفاظت شده، دسترسی داخلی مستقل از اینترنت (پر سرعت، هزینه پایین، کیفیت بالا، مداوم، همگانی، فراگیر)، دسترسی از خارج از کشور به شبکه ملی اطلاعات به صورت حفاظت شده، خارج نشدن مسیریابی‌های مراکز داده داخلی، پایدار بودن (پایداری در زیرساخت شبکه) (عدم قطعی، دسترس‌پذیری، عدم مشکلات سخت‌افزاری و نرم‌افزاری، عدم لختی شبکه)، پایداری در المان‌های شبکه (مسیریابی/گره‌ها و لینک‌ها/پروتکل‌ها)، پایداری از نظر تخصیص پهنای باند (تناسب پهنای باند با حجم ترافیک)، پایداری در برابر حملات (عدم شناخت نقاط ضعف شبکه و توپولوژی شبکه توسط مهاجم)، پایداری اجرایی و استمرار کسب‌وکار
لایه خدمات	بومی بودن، امنیت خود خدمات، ارائه امنیت به‌عنوان خدمت، پشتیبانی از پروتکل‌های امنیتی، خدمات مربوط به احراز هویت و جامعیت و محرمانگی، پویایی و به‌روز بودن، توسعه‌پذیری، امنیت مربوط به سیستم‌عامل، منابع و بانک‌های اطلاعاتی، نرم‌افزارها، پرتال‌ها، شبکه‌های اینترانتی و اختصاصی، رابط‌ها[1] و میان‌افزارهای[2] لازم برای تعامل و سازگاری سیستم‌ها و امنیت پردازش‌ها و برنامه‌های کاربردی
لایه محتوا	تولید محتوا با رعایت ضوابط و در چارچوب قانون، ایجاد محیط امن اقتصادی در تولید محتوا برای افزایش سهم اقتصاد جهانی، رونق کسب‌وکار، کارآفرینی، تضمین امنیت داده و حریم خصوصی افراد، مدیریت و پایش محتوا برای جلوگیری از تضعیف مشروعیت و مقبولیت نظام اسلامی و مخل امنیت ملی، تولید محتوا در راستای انسجام بخشیدن به فضای فرهنگی کشور و ارتقاء تحمل، همزیستی مسالمت‌آمیز هویت‌های فرهیخته در درون یک جامعه، اعمال فیلترینگ بر محتوا، تنوع محتوای مورد نیاز با نگاه ایجابی به امنیت در توزیع و بهره‌برداری، جلوگیری از افشا و انتشار اسرار کشور، امن بودن داده‌های ارتباطی بین مراکز حساس و حیاتی و حفظ حریم خصوصی افراد
لایه کاربران	اعتماد کاربران، فرهنگ‌سازی امنیت توسط مراکز علمی و تحقیقاتی و مشاوره‌ای، آموزش و آگاهی‌بخشی و هشداردهی، همکاری با مراکز گوهر، حفاظت از حریم خصوصی، عدم افشای هویت، احراز هویت، مدیریت مجوزها و کنترل دسترسی، کنترل لاگ فعالیت‌ها، محرمانگی در

[1] Application Programming Interface (API)

[2] Middleware

	اطلاعات و داده کاربران، رعایت الزامات امنیتی و پیوست‌ها، گزارش رخدادهای امنیتی، مشارکت در پاسخ‌دهی به تهدیدات

امنیت در فضای سایبر همانند امنیت در فضای واقعی امری نسبی است که به‌صورت ایجابی و سلبی قابل انجام است. علاوه بر آن، در این فضا، امنیت بیش از آنکه جلوه‌های بیرونی و عینی داشته باشد، ماهیتی ذهنی و نامحسوس دارد. در بُعد عینی امنیت به‌مثابه فقدان تهدیدات تعبیر می شود؛ اما بسیاری از تهدیدات امنیتی فضای سایبر ممکن است در فضای واقعی نمود عینی نداشته و قابل اندازه‌گیری نباشند. این مسئله موجب می‌شود احساس امنیت کاذب در این فضا به وجود بیاید؛ بنابراین در مبحث امنیت در فضای سایبر باید تمامی جنبه‌های سلبی/ ایجابی و عینی/ذهنی آن را در نظر گرفت. امنیت در فضای مجازی تنها از طریق ایجاد محدودیت و برخورد سلبی با تهدیدات عینی حاصل نمی‌شود.

فضای سایبر تمامی ابعاد زندگی بشر، اعم از سیاسی، اقتصادی، اجتماعی، فرهنگی، دفاعی- امنیتی و حقوقی- قضایی را تحت تأثیر قرار داده است. همان‌طور که در فضای واقعی این ابعاد در سطوح فردی و اجتماعی نیازمند امنیت هستند؛ در فضای سایبری نیز باید این الزام محقق شود. امنیت فضای سایبر در امتداد امنیت ملی قرار می‌گیرد. چراکه در جمهوری اسلامی ایران، گفتمان امنیت ملی مبتنی بر ساختار ایدئولوژیک و واکنش در مقابل تهدیدات امنیتی علیه آن است. دستیابی به امنیت ملی پایدار به‌منزله حفظ ارزش‌های حیاتی بدون امنیتی کردن سراسر جامعه است (نصری، ۱۳۹۲).

در فضای سایبر مقابله با حملات سایبری، جنگ نرم، جنگ رسانه‌ای، جمع‌آوری و کنترل اطلاعات برای هدایت جنبش‌های سیاسی و اجتماعی معاند و برانداز، مواجهه با تبعات احساس امنیت ذهنی و کاذب فضای مجازی از چالش‌های جدی امنیتی در سطح کشور است؛ بنابراین مهم‌ترین فلسفه وجودی شکل‌گیری شبکه ملی اطلاعات را می‌توان در ایجاد امنیت و مدیریت فضای مجازی برای مواجهه با تهدیدات روزافزون دانست.

فرصت‌ها و تهدیدهای فضای مجازی

محیط در متون تخصصی مدیریت به پدیده‌های اطراف سازمان اطلاق می‌شود و شامل مجموعه جریان‌ها، شرایط، روندها، متغیرها، عوامل، رخدادها و اقداماتی است که بر عملکرد سازمان تأثیر می‌گذارند و یا تحت تأثیر عوامل اداره‌کننده سازمان قرار می‌گیرند. عواملی که تحت کنترل کامل مدیریت واقع می‌شوند، محیط داخلی و عواملی که تحت تأثیر مدیریت و عوامل و بازیگران متعدد قرار دارند محیط خارجی هستند(حسن بیگی، ۱۳۹۰: ۲۴۲).

فضای سایبر با تمامی ابعاد زندگی بشر ممزوج شده است. در این محیط پیچیده و پویا، عوامل و متغیرهای زیادی در کنش و تعامل با هم قرار گرفته‌اند. بسیاری از این عوامل با آنچه از آن‌ها در فضای واقعی تداعی می‌شود، فرق دارند؛ به‌طوری‌که میزان تأثیرگذاری آن‌ها بر پدیده‌های مختلف فضای مجازی نیز ممکن است نامحسوس یا غیر قابل پیش‌بینی باشد.

با انجام تجزیه‌وتحلیل محیطی،[1] عوامل محیطی اثرگذار و اثرپذیر در امنیت فضای مجازی، به دست می‌آید. در این تحقیق، محیط خارجی فضای مجازی کشور شامل کلیه عوامل و عناصر خارج از کنترل در نظر گرفته شده است؛ بنابراین باید توجه داشت که مرزهای محیط داخل و خارج برای فضای سایبر منطبق با مرزهای جغرافیایی نیست.

روش‌شناسی تحقیق

پژوهش حاضر از نظر هدف کاربردی و از نظر روش گردآوری داده‌ها توصیفی-کاربردی است. همچنین این پژوهش از نظر روش تجزیه‌وتحلیل داده‌ها، آمیخته (کمی و کیفی) است. در این پژوهش داده‌های کیفی از مطالعه اسناد و گزارش‌های مرتبط جمع‌آوری

---

1. Environment Analysis

شده و به‌منظور اعتبار سنجی و ارزیابی نتایج از پر سشنامه و تحلیل آماری ا ستفاده شده است.

جامعه آماری این تحقیق شامل مدیران راهبردی، پژوهشگران، متخصصان و اساتید در حوزه فضای سایبر است. از آنجا که در این تحقیق مدیریت فرصت‌ها و تهدیدهای فضای مجازی مورد توجه قرار گرفته، جامعه آماری محدود بوده و خبرگان مورد نظر باید تخصص و تجربه کافی در حوزه شناخت و مدیریت این موارد را داشته باشند.

در تحقیق حاضر از روش کتابخانه‌ای و میدانی (پرسشنامه) با توجه به محدودیت تعداد جامعه آماری حدود ۳۰۰ نفر بر اساس فرمول کوکران، ۹۶ نفر حجم نمونه انتخاب شده است. پر سشنامه محقق ساخته میان جامعه آماری توزیع و از پاسخ‌دهندگان خواسته شد تا میزان اهمیت هریک از شاخص‌ها را بر ا ساس طیف لیکرت از خیلی کم (۱) تا خیلی زیاد (۵) مشخص کنند.

تجزیه‌وتحلیل یافته‌های تحقیق

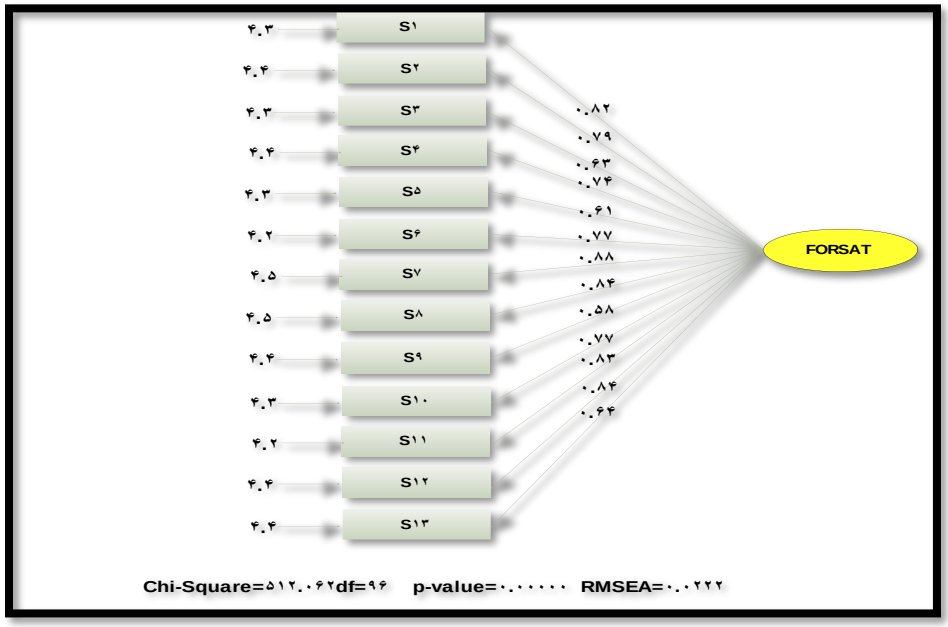
در محیط فضای مجازی با استفاده از روش اکتشافی و نظر خبرگان، تعداد ۲۲ گزاره فرصت و تعداد ۲۳ گزاره تهدید احصاء شد و پس از اخذ نظر خبرگان، تعداد ۱۳ فرصت و تعداد ۱۳ تهدید به‌عنوان شاخص به تأیید رسید و شاخص‌ها از طریق پرسشنامه محقق‌ساخته در دو وضعیت میزان تأثیرگذاری هر شاخص و میزان مدیریت آن توسط شبکه ملی اطلاعات، از طریق جامعه آماری به تعداد ۹۶ نفر پرسشنامه تکمیل شد و از طریق نرم‌افزار لیزرل و SPSS داده‌ها مورد تجزیه‌وتحلیل قرار گرفت که نتیجه به شرح زیر می‌باشد.

تحلیل میانگین بار عاملی میزان تأثیر فرصت‌ها و مدیریت آن توسط شبکه ملی اطلاعات، در جدول زیر درج شده است:

جدول (۱-۳): تحلیل آماری شاخص‌های فرصت با استفاده از آزمون رتبه‌ای فریدمن

ردیف	شاخص	میزان تأثیر این فرصت در فضای مجازی	میزان مدیریت این فرصت توسط شبکه ملی اطلاعات
1	وجود دانش بین‌المللی برای توسعه و تقویت امنیت در شبکه ملی اطلاعات	۷۶,۷	۹۱,۱
2	وجود تجهیزات و زیرساخت‌های اطلاعاتی و ارتباطی مناسب برای نشر و گسترش محتوای فرهنگی، هنری، آموزشی، سلامت و ...	۸۳,۵	۹۱,۱
3	وجود بازار کسب‌وکار الکترونیکی بین‌المللی برای ارائه محصولات و خدمات سایبری	۷۸,۳	۹۰,۱
4	وجود ابزارها و فناوری های مرتبط با ممانعت از نقض حریم خصوصی و جاسوسی اطلاعاتی	۷۸,۵	۸۹,۸
5	وجود دانش و فناوری های نوین داده کاوی و رصد و پایش اطلاعات	۸۱,۸	۸۹,۴
6	وجود فضای مناسب برای تبادل اطلاعات علمی میان دانشگاه‌ها و شرکت‌های دانش‌بنیان داخلی با خارج از کشور	۸۰	۸۹,۴
7	وجود کنوانسیون ها و مجامع قانونی بین‌المللی برای پیگیری مطالبات حقوقی ملت ایران	۸۳,۵	۸۹,۲
8	وجود مخاطبین خارج از کشور و تقاضا جهت پذیرش فرهنگ، ارزش‌های دینی و سبک زندگی ایرانی-اسلامی	۷۶,۷	۸۷,۶
9	وجود اطلاعات باارزش در داده های کلان تولیدشده توسط شبکه‌های اجتماعی داخلی و خارجی	۸۰,۲	۸۷,۶
10	وجود مجامع و انجمن های علمی در فضای مجازی جهت دسترسی به علوم و فناوری‌های نوظهور سایبری	۸۱,۸	۸۷,۲
11	دستیابی به کریدور ارتباطی منطقه‌ای	۷۸,۵	۸۷,۲
12	دسترسی به داده‌های جهانی برای تقویت پایگاه‌های داده بومی؛ مانند اطلس زمین‌شناسی و ...	۷۶,۷	۸۵,۹

ردیف	شاخص	میزان تأثیر این فرصت در فضای مجازی	میزان مدیریت این فرصت توسط شبکه ملی اطلاعات
13	وجود رسانه‌های متنوع سایبری برای ایجاد فضای گفتمان در زمینه تحکیم هویت دینی، مسئولیت‌های اجتماعی، فرهنگ خانواده و شکاف بین نسلی	۷۸,۳	۸۴,۳
	میانگین بار عاملی	79.5769231	88.4538462



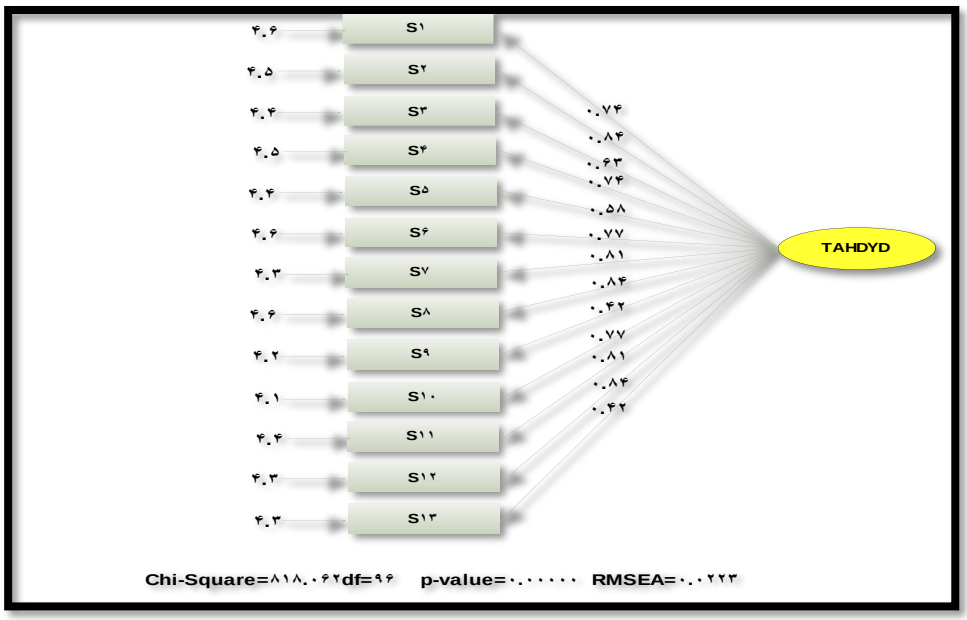
Normed Fit Index (NFI) =95%

شکل (۱-۳): تحلیل آماری شاخص‌های فرصت از نرم‌افزار لیزرل

تحلیل میانگین بار عاملی میزان تأثیر تهدیدها و مدیریت آن توسط شبکه ملی اطلاعات، در جدول زیر درج شده است:

جدول (۱-۴): تحلیل آماری شاخص‌های تهدید با استفاده از آزمون رتبه‌ای فریدمن

ردیف	شاخص	میزان تأثیر تهدید در فضای مجازی	میزان مدیریت تهدید توسط شبکه ملی اطلاعات
1	جاسوسی، افشای اطلاعات و نقض حریم خصوصی از طریق فضای سایبر توسط کشورهای بیگانه	۸۷,۷	۹۲,۹
2	احتمال قطع اینترنت و اعمال تحریم در برقراری ارتباط شبکه ملی اطلاعات با شبکه جهانی اینترنت	۷۳,۳	۹۲,۷
3	ایجاد اختلال و خرابکاری در تجهیزات زیرساخت های حیاتی با استفاده از فضای سایبر	۶۰	۹۱,۲
4	تحرکات دشمن در فضای سایبر به‌منظور براندازی نظام با ناکارآمد نشان دادن و تشکیل ائتلاف های جهانی علیه جمهوری اسلامی ایران	۷۹,۱	۹۰,۶
5	توان دشمن در سازمان‌دهی حملات و جنگ سایبری علیه جمهوری اسلامی ایران	۸۴,۵	۹۰,۶
6	استفاده دشمن از ظرفیت شبکه‌های اجتماعی در ایجاد معضلات اجتماعی و تهدید امنیت ملی	۷۸,۳	۸۸,۹
7	تلاش برای تغییر بنیان های اعتقادی، اخلاقی و فرهنگی در فضای مجازی	۷۹,۱	۸۶,۶
8	توانمندی رسانه‌های سایبری دشمن در ترویج پروپاگاندا، جنگ روانی و شایعه علیه حاکمیت	۷۸,۵	۸۶,۶
9	نفوذ و تأثیرگذاری فرهنگ غرب در فروپاشی بنیان خانواده	۷۹,۱	۸۶,۴
10	تبلیغات، عملیات روانی و نفوذ جریانی با استفاده از فضای سایبر	۸۳,۱	۸۵,۴
11	داده‌کاوی، ذائقه سنجی و رفتارشناسی و القای نیازهای کاذب و مصرف‌گرایی در جامعه	۸۰,۶	۸۴,۷
12	ترویج یأس و ناامیدی در بین آحاد جامعه و برهم زدن امنیت ذهنی	۶۴,۷	۸۳,۱
13	گسترش تفرقه و اختلافات قومی و مذهبی در فضای مجازی	۷۹,۱	۸۲,۹
	میانگین بار عاملی	**77.46923077**	**87.89230769**



Normed Fit Index (NFI) =95%

شکل (۱-۴): تحلیل آماری گویه‌های تهدید با استفاده از نرم‌افزار لیزرل

خروجی شاخص‌های برازش مدل معادلات ساختاری بالاتر از ۹۰ نشان می‌دهد که این مدل از برازش قابل قبولی برخوردار می‌باشد.

همان‌طور که در جداول تحلیل میزان تأثیر فرصت‌ها و تهدیدهای فوق مشاهده می‌شود، با توجه به میانگین بار عاملی میزان تأثیرگذاری شـــاخص‌ها، تمام شـــاخص‌ها در ابعاد فرصت‌ها و تهدیدها به تأیید رسیده و دارای اعتبار می‌باشند.

نتیجه‌گیری و پیشنهادها

بر اساس یافته‌های تحقیق در جدول شماره (۱-۳) و (۱-۴) و در پاسخ به سؤالات اصلی و فرعی تحقیق نتیجه گرفته می‌شود که شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدها نقش به‌سزایی دارد و میزان آن بسیار بالا، پراهمیت و به شرح زیر می‌باشد؛

۱. میانگین میزان مدیریت فرصت‌های فضای مجازی از طریق شبکه ملی اطلاعات در

مجموع ۸۸/۴۵ و میانگین میزان مدیریت تهدیدهای فضای مجازی از طریق شبکه ملی اطلاعات در مجموع ۸۷/۸۹ به دست آمده است؛ لذا نقش شبکه ملی اطلاعات در مدیریت فرصت‌ها بیشتر از مدیریت تهدیدها است و بر اساس میانگین به‌دست‌آمده، نقش بسیار بالایی در مدیریت فرصت‌ها و تهدیدها ایفا می‌نماید.

۲. در بخش مدیریت فرصت‌های فضای مجازی، شبکه ملی اطلاعات در سه شاخص؛ الف - وجود دانش بین‌المللی برای توسعه و تقویت امنیت در شبکه ملی اطلاعات، با میانگین بار عاملی ۹۱/۱؛ ب- وجود تجهیزات و زیرساخت‌های اطلاعاتی و ارتباطی مناسب برای نشر و گسترش محتوای فرهنگی، هنری، آموزشی، سلامت و ... با میانگین بار عاملی ۹۱/۱؛ ج- وجود بازار کسب‌وکار الکترونیکی بین‌المللی برای ارائه محصولات و خدمات سایبری، با میانگین بار عاملی ۹۰/۱؛ بیشترین نقش و همچنین وجود رسانه‌های متنوع سایبری برای ایجاد فضای گفتمان در زمینه تحکیم هویت دینی، مسئولیت‌های اجتماعی، فرهنگ خانواده و شکاف بین نسلی، با میانگین بار عاملی ۸۴/۳ کمترین امتیاز در مدیریت فرصت‌ها را دارد.

۳. در بخش مدیریت تهدیدهای فضای مجازی، شبکه ملی اطلاعات در سه شاخص؛ الف - جاسوسی، افشای اطلاعات و نقض حریم خصوصی از طریق فضای سایبر توسط کشورهای بیگانه، با میانگین بار عاملی ۹۲/۹؛ ب- احتمال قطع اینترنت و اعمال تحریم در برقراری ارتباط شبکه ملی اطلاعات با شبکه جهانی اینترنت، با میانگین بار عاملی ۹۲/۷؛ ج - ایجاد اختلال و خرابکاری در تجهیزات زیرساخت‌های حیاتی با استفاده از فضای سایبر، با میانگین بار عاملی ۹۱/۲؛ بیشترین نقش و همچنین گسترش تفرقه و اختلافات قومی و مذهبی در فضای مجازی، با میانگین بار عاملی ۸۲/۹، کمترین امتیاز را در مدیریت تهدیدها را دارد.

۴. با توجه نقش شبکه ملی اطلاعات در مدیریت فرصت‌های دانش بین‌المللی برای

توسعه و تقویت امنیت شبکه، گسترش محتوای فرهنگی، هنری، آموزشی و همچنین گسترش کسب‌وکار بین‌المللی و خدمات سایبری و از طرفی مدیریت مقابله با تهدیدهای جاسوسی، نقض حریم خصوصی، جلوگیری از قطع ارتباط و تحریم و جلوگیری از اختلال و خرابکاری در زیرساخت‌های کشور، وجود شبکه ملی اطلاعات بسیار ضروری و حائز اهمیت است.

منطبق با یافته‌های تحقیق و نتایج حاصله، موارد زیر پیشنهاد می‌گردد؛

۱. بر اساس تأکید و اوامر مقام معظم رهبری و همچنین نقش بسیار بالای شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدها، در راه‌اندازی و تکمیل سایر بخش‌های مختلف شبکه ملی اطلاعات تسریع شود.
۲. انتقال مراکز داده به داخل کشور و مدیریت یکپارچه در استفاده از فناوری‌های نوین داده‌کاوی، تجهیزات و مکانیزم‌های امنیتی بومی ازجمله محرمانگی، احراز هویت، کنترل دسترسی و... و مقابله با جرائم سایبری، در شبکه ملی اطلاعات به‌منظور پیشگیری از غفلت راهبردی، مقابله با تهدیدات و کاهش آسیب‌پذیری‌های فضای سایبر در راستای ناکارآمد ساختن اقدامات خصمانه دشمن.
۳. نسبت به بومی نمودن سامانه‌های امنیتی و زیر ساختی شبکه ملی اطلاعات جهت اجرای فیلترینگ هوشمند، نظارت و کنترل و مدیریت اطلاعات، حفظ حریم خصوصی و... در فضای مجازی اقدام شود.
۴. نسبت به ارتقاء مهارت و آمادگی کاربران شبکه ملی اطلاعات در برابر تهدیدات سایبری به‌منظور تأمین امنیت و حفظ اطلاعات و حفظ حریم خصوصی توسط متولیان امر و مجموعه‌های ارائه‌کننده سرویس و خدمات اقدام گردد.
۵. ضمانت اجرایی برای تحقق قوانین و مقررات در شبکه ملی اطلاعات پیش‌بینی و توسط متولیان امر پیگیری گردد.
۶. تدوین و اجرای پیوست‌های فرهنگی، امنیتی و آموزشی و حضور فعال و مؤثر در

معاهدات امنیت سایبری در عرصه جهانی، به‌منظور تأمین امنیت شبکه ملی اطلاعات، بازدارندگی در تهاجم سایبری، قطع اینترنت و اعمال تحریم‌های سایبری در راستای جلوگیری از تغییر بنیان‌های اعتقادی، اخلاقی و فرهنگی، تحکیم هویت ملی، استمرار سبک زندگی ایرانی- اسلامی و مقابله با جریان سلطه جهانی

۷. با ر صد مداوم شبکه ملی اطلاعات، تهدیدها و آ سیب‌پذیری‌های موجود در شبکه ملی اطلاعات شناسایی شود و نسبت به رفع آن‌ها اقدام گردد.

۸. اجرای فرمایشات مقام معظم رهبری، سیاست‌های ابلاغی نظام، الزامات قانونی و پدافند غیرعامل در زمینه ممنوعیت استفاده از محصولات خارجی و استفاده از محصولات بومی در شبکه ملی اطلاعات با بهره‌گیری از شرکت‌های دانش‌بنیان و نیروهای متخصص داخلی به‌منظور توسعه فناوری‌های نوین، صیانت از حریم خصوصی و جلوگیری از جاسوسی و افشای اطلاعات، به‌طور جدی در دستور کار متولیان امر قرار گیرد.

۹. در جهت تولید و به‌کارگیری محصولات خدمات‌پایه بومی؛ ازجمله سیستم‌عامل، موتور جستجو، پست الکترونیکی، پیام‌رسان‌های اجتماعی، در راستای توسعه کسب‌وکار الکترونیکی و ارائه خدمات امن، کم‌هزینه و فراگیر در شبکه ملی اطلاعات و حضور فعال و مؤثر در مجامع بین‌المللی، به‌منظور قطع وابستگی، افزایش اعتماد عمومی، خنثی‌سازی فعالیت‌های دشمن، کاهش معضلات اجتماعی و ارتقاء امنیت ملی و جلوگیری از رصد و تحلیل داده‌های کشورمان، اقدام شود.

فهرست منابع ومآخذ

الف. منابع فارسی

- امام خامنه‌ای (مدظله‌العالی)، پایگاه اطلاع‌رسانی دفتر حفظ و نشر آثار حضرت آیت‌الله‌العظمی سید علی خامنه‌ای (مدظله‌العالی) به آدرس: www.khamenei.ir
- بالایی حمید و ا سماعیلی، مح سن (۱۳۹۲)، الگوی راهبردی تأمین امنیت ملی جمهوری ا سلامی ایران در قوانین برنامه توسعه اقتصادی، سیاسی، فرهنگی، فصلنامه پژوهش‌های راهبردی سیاست، سال دوم، شماره پنجم.
- ح سن‌بیگی، ابراهیم (۱۳۹۰)، مدیریت راهبردی، تهران: انت شارات سازمان مطالعه و تدوین کتب علوم انسانی (سمت).
- ریاضی، عبدالمجید و ولیزاده، بهنام (۱۳۸۸)، شبکه ملی اینترنت: طرح تدوین جامعه فناوری اطلاعات کشور، تهران: انتشارات نیک‌پی.
- سایت دولت آ مر یکا و اروپا (۱۳۹۶)، به آدرس‌های https://www.gov.uk و https://www.enisa.europa.eu
- سند افتا (۱۳۸۶)، امنیت فضای تبادل اطلاعات کشور، معاونت فناوری اطلاعات ریاست جمهوری، دفتر امور زیربنایی فناوری اطلاعات.
- عجاج، نویهض و شیخی، حمیدرضا (مترجم) (۱۳۹۴)، پروتکل‌های دانشوران صهیون: برنامه عمل صهیونیسم جهانی، ناشر: بنیاد پژوهش‌های آستان قدس رضوی، چاپ هفتم.
- قرآن کریم، بقره ۱۹۴
- کرمی، جهانگیر (بهار ۱۳۸۰)، «تأثیر محیط امنیّتی منطقه‌ای بر سیاست‌های دفاعی دولت‌ها»، مجله سیاست دفاعی، شماره ۳۴.
- ماندل، رابرت (۱۳۷۸)، چهره متغیر امنیت ملی، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.
- مرادحا صل، نیلوفر (۱۳۹۱)، مجری پروژه تحقیقاتی. بازنگری مفاهیم شبکه ملی اطلاعات، مرکز تحقیقات مخابرات ایران، تهران.
- مرکز ملی فضای مجازی (الف ۱۳۹۶)، شبکه ملی اطلاعات، سایت Majazi.ir
- مرکز ملی فضای مجازی (ب ۱۳۹۶)، تاریخچه شبکه ملی اطلاعات، سایت Majazi.ir
- میررفیع، سید علی (۱۳۹۴)، راهبردهای پدافند غیرعامل زیرساخت‌های ارتباطی شبکه ملی اطلاعات کشور در برابر تهدیدات سایبری، رساله دکتری، دانشگاه عالی دفاع ملی.
- نامداریان، لیلا (۱۳۹۶)، ارائه الگویی برای تقویت اثرات اقتصادی شبکه ملی اطلاعات، نشریه پردازش و مدیریت اطلاعات، شماره ۱.

- نصـــری، قدیر (۱۳۹۲)، امنیت جامعه‌ای به‌مثابه هســـته حیاتی امنیت ملی پایدار، فصـــلنامه امنیت پژوهی، سال دوازدهم شماره ۴۳.
- واحدی، مرتضی و صنیعی، محمدحسین (۱۳۹۲)، امنیت ملی در فضای سایبر، پژوهشکده امنیت ملی و مطالعات راهبردی، دانشگاه عالی دفاع ملی.

ب. منابع انگلیسی

- Ben, Shenglin. and Bosc, Romain. (2017). "Digital Infrastructure Overcoming the digital divide in China and the European Union", Emerging Market Sustainability Dialogues, PP 1-55.
- Lindwall, (2017). Australian Medical Association -Productivity Commission, www.pc.gov.au.Implementation, World Bank Group Publication. pp 41-59.
- Shark Alan, R. (2015). Technology and Public Management, Rutledge Publisher, First edition, PP 1-426.
- Yoon, Jeongwon. (2016). Korean Digital Government Infrastructure Building and and Implementation", World Bank Group Publication. pp 41-59.