Supreme National Defense University Quarterly of Defense Strategy

https://ds.sndu.ac.ir E-ISSN: 2980-8464

Vol. 23, No. 3, Issue. 91, Autumn 2025 **Received:** 2025/05/01 **Accepted:** 2025/11/06

Research paper

# Identification and Prioritization of Security Strategies for the National Information Network of the Islamic Republic of Iran in Cyberspace

**Khodadad Halili**
Assistant Professor, Department of Cyber, Faculty of Computer and Cyber, Shahid Sattari Aeronautical University of Science and Technology.

## Abstract

The National Information Network (SHAMA) affords numerous advantages, including enhanced domestic access speeds, accelerated and simplified content and service delivery, reduced costs, the pervasive implementation of e-government, network autonomy from the internet under crisis conditions, and the effective management of security threats at both individual and national levels. Realizing these benefits necessitates the assurance of security and service continuity within this network. Concurrently, securing the cyberspace domain to safeguard virtual assets and protect national interests is a fundamental component of the nation's national security architecture and a paramount concern of the sovereign authority. Security within SHAMA constitutes a prerequisite for the network's efficacy and the bedrock for ensuring enduring stability in the nation's cyberspace. The principal objective of this article is to propose strategies for augmenting the security of SHAMA. This investigation is applied in purpose and descriptive-analytical in nature and method of data collection. Initially, an environmental analysis was conducted to identify strengths, weaknesses, opportunities, and threats, and through the application of the SWOT method, offensive, defensive, competitive, and conservative strategies were formulated. Subsequently, utilizing a researcher-designed questionnaire, the proposed strategies were evaluated by the statistical population, and the strategies were prioritized employing the TOPSIS technique. The findings of this research indicate that the implementation of security requirements within SHAMA will enhance its resilience against cyber crises, including internet disconnection, virtual embargoes, cyberattacks, espionage, and information disclosure, thereby playing a pivotal and prominent role in securing the nation's cyberspace.

**Keywords:** National Information Network (SHAMA), Cybersecurity, National Security, TOPSIS Technique.

فصلنامه راهبرد دفاعی

سال بیست و سوم، شماره سوم (پیاپی ۹۱)، پاییز ۱۴۰۴، صص. ۱۵۵-۱۸۶
تاریخ دریافت: ۱۴۰۴/۰۲/۱۱ ـ تاریخ پذیرش: ۱۴۰۴/۰۸/۱۵

مقام معظم رهبری : «ابزارهای تسهیل‌کننده، مثل رایانه‌ها و ارتباطات اینترنتی و فضای مجازی و سایبری هم که الان در اختیار شماست. اگر بتوانید این‌ها را یاد بگیرید، می توانید یک کلمه حرف درستِ خودتان را به هزاران مستمعی که شما آن‌ها را نمی‌شناسید، برسانید؛ این فرصت فوق‌العاده‌ای است»

مقاله پژوهشی

# شناسایی و رتبه‌بندی راهبردهای امنیت شبکه ملی اطلاعات جمهوری اسلامی ایران در فضای مجازی

**خداداد هلیلی**
استادیار گروه سایبر، دانشکده رایانه و سایبر دانشگاه شهید ستاری، تهران، ایران

## چکیده

شبکه ملی اطلاعات (شَما)، دارای مزایایی مانند افزایش سرعت دسترسی داخلی، تسریع و تسهیل در عرضه محتوا و خدمات، کاهش هزینه‌ها، فراگیر شدن دولت الکترونیک، استقلال شبکه از اینترنت در شرایط بحران و مدیریت تهدیدات امنیتی در سطوح فردی و ملی است. دستیابی به این مزایا مستلزم تضمین امنیت و پایداری خدمات در این شبکه است. از سوی دیگر، تأمین امنیت فضای مجازی به‌منظور حفاظت از سرمایه‌های مجازی و صیانت از منافع ملی، در راستای تحقق امنیت ملی کشور قرار دارد و از دغدغه‌های مهم حاکمیت به شمار می‌رود. امنیت در شَما، پیش‌نیاز کارآمدی این شبکه و زمینه‌ساز تأمین امنیت پایدار در فضای مجازی کشور است. هدف اصلی این مقاله، ارائه راهبردهایی برای ارتقای امنیت شَما است. این تحقیق از نظر هدف، کاربردی و از نظر ماهیت و روش گردآوری داده‌ها، توصیفی-تحلیلی است. در ابتدا، با تحلیل محیطی، نقاط قوت، ضعف، فرصت‌ها و تهدیدها شناسایی شد و با استفاده از روش سوآت، راهبردهای تهاجمی، تدافعی، رقابتی و محافظه‌کارانه استخراج گردید. در ادامه، با استفاده از پرسش‌نامه‌ی محقق‌ساخته، راهبردهای ارائه‌شده توسط جامعه آماری ارزیابی شده و با به‌کارگیری تکنیک تاپسیس، رتبه‌بندی راهبردها انجام گرفت. نتایج این تحقیق نشان می‌دهد که به‌کارگیری الزامات امنیتی در شَما موجب افزایش تاب‌آوری آن در برابر بحران‌های مجازی ازجمله قطع اینترنت، تحریم مجازی، حملات مجازی، جاسوسی و افشای اطلاعات خواهد شد و این مسئله در تأمین امنیت فضای مجازی کشور، نقشی کلیدی و برجسته ایفا می‌کند.

**کلیدواژه‌ها:** شبکه ملی اطلاعات (شَما)، امنیت مجازی، امنیت ملی، روش تاپسیس

## مقدمه

ایدهٔ ایجاد شبکه ملی اطلاعات (شَما) از سال ۱۳۸۴ مطرح شد و مطابق ماده ۴۶ برنامه پنجم توسعه، مقرر شد که تا سال ۱۳۹۴، میزان استفاده از این شبکه به ۶۰ درصد برسد. تشکیل شورای عالی فضای مجازی در اسفند ۱۳۹۰ و تأکید مقام معظم رهبری بر تسریع در راه‌اندازی شبکه ملی اطلاعات در بند ۵ حکم انتصاب اعضای شورا در شهریور ۱۳۹۴، نقطه عطفی در سیاست‌گذاری فضای مجازی و بیانگر اهمیت راهبردی این شبکه است؛ بااین‌حال، با وجود گذشت دو دهه و تغییرات ساختاری و مدیریتی دولت‌ها، این کلان‌پروژه ملی به‌طور کامل تحقق نیافته است.

فضای مجازی به دلیل قابلیت‌های گسترده جمع‌آوری اطلاعات و فعالیت‌های جاسوسی، چالش‌های امنیتی متعددی در ابعاد سیاسی، اقتصادی، فرهنگی و اجتماعی ایجاد کرده است. ازاین‌رو، امنیت فضای مجازی در برنامه‌ریزی‌های راهبردی بسیاری از کشورها مورد توجه ویژه قرار گرفته و سیاست‌گذاری، سازماندهی و سرمایه‌گذاری گسترده‌ای در این حوزه انجام شده است.

تأمین منافع ملی کشور مستلزم تحقق امنیت پایدار ملی است و امنیت فضای سایبر با صیانت از دستاوردها و ارزش‌های انقلاب اسلامی، نقشی حیاتی در این زمینه ایفا می‌کند. همچنین، براساس باورها و ارزش‌های اسلامی و گفتمان سلطه ناپذیری انقلاب اسلامی، مقابله با مستکبران و دشمنان نظام اسلامی در فضای سایبر، از طریق فراهم ساختن امنیت در این فضا امکان‌پذیر است. این مسئله نیازمند ایجاد زیرساختی امن برای مدیریت، کنترل و نظارت مستقل داخلی است. همچنین باید تعامل متوازن و هوشمندانه‌ای با اینترنت برقرار شود تا ضمن کاهش تهدیدات امنیتی، از فرصت‌های تاریخی و بی‌نظیر این فضا بهره‌برداری شود.

فلسفه راه‌اندازی شَما بر پایه کاهش وابستگی به شبکه جهانی اینترنت، بهره‌گیری هوشمندانه از فرصت‌های فضای مجازی، مقابله با تهدیدهای مجازی و فراهم‌سازی بستر امن برای ارائه خدمات بومی و کنترل‌شده در راستای تأمین امنیت ملی شکل گرفته است.

این اهداف راهبردی در طراحی معماری لایه‌ای شبکه نیز مورد توجه قرار گرفته تا زیرساختی مستقل، پایدار و قابل مدیریت برای کشور فراهم شود.[۱]

لزوم به‌کارگیری شَما برای تأمین امنیت فضای سایبر و حفاظت از سرمایه‌های سایبری، از دغدغه‌های مهم حاکمیت و مسئله‌ای راهبردی است که در این تحقیق مورد بررسی قرار گرفته است.

## ۱. کلیات

### ۱-۱. بیان مسئله

شَما با بسیاری از حوزه‌های کاربردی فضای سایبر ازجمله سیاست‌گذاری، قوانین و مقررات، خدمات الکترونیکی، اقتصاد دیجیتال، دانش و فناوری، سلامت و آموزش، ارتباطات امن، پدافند غیرعامل، دفاع مجازی و امنیت ملی مرتبط است. ازاین‌رو تعامل و تبادل اطلاعات میان بخش عمده‌ای از سازمان‌ها و نهادهای دولتی و خصوصی کشور و افراد جامعه در بستر این شبکه انجام می‌شود.

براساس مصوبات شورای عالی فضای مجازی، طراحی این شبکه بر پایه شش الزام اصلی شامل زیرساخت ارتباطی، استقلال از اینترنت جهانی همراه با دسترسی مدیریت شده به آن، ارائه خدمات با کیفیت، امنیت خدمات، ارتباطات پایدار میان نهادهای حیاتی و ظرفیت بالا همراه با مراکز داده داخلی، موردتوجه سیاست‌گذاران و متولیان راه‌اندازی قرار گرفته است.[۲] در این میان، امنیت جایگاهی محوری دارد؛ چراکه شبکه باید امکان رمزنگاری، امضای دیجیتال و ارتباطات امن را برای حفاظت از داده‌ها و صیانت از زیرساخت‌های حیاتی کشور در مواجهه با حملات مجازی را فراهم کند.

همان‌طور که امنیت پایدار در فضای واقعی پیش‌شرط تأمین منافع ملی است؛ امنیت فضای سایبر نیز نقش اساسی در صیانت از منافع ملی، حفاظت از سرمایه‌های مجازی و دستیابی به

---

۱. فصل پنجم گزارش پژوهشگاه ارتباطات و فناوری اطلاعات با عنوان معماری کلان شبکه ملی اطلاعات

۲. در جلسه پانزدهم (۱۳۹۲/۱۰/۰۳) الزامات شش‌گانه تصویب و در مصوبات جلسه سی و پنجم (۱۳۹۵/۹/۲۰) این الزامات تبیین شد. این مصوبات، مبنای طراحی، اجرا و ارزیابی این پروژه ملی قرار گرفته‌اند.

اهداف و آرمان‌های انقلاب اسلامی دارد. امروزه امنیت فضای سایبر وجه نوینی از امنیت ملی است که نیازمند توجه ویژه، برنامه‌ریزی راهبردی، سازمان‌دهی و سرمایه‌گذاری مناسب در تمامی حوزه‌های سیاسی، اقتصادی، اجتماعی، فرهنگی، دفاعی و حقوقی است.

مسئله اصلی شکل‌گیری این تحقیق واکاوی و تأکید بر اهمیت و ضرورت امنیت در شَما، بررسی سازوکارهای امنیتی موردنیاز برای امن بودن این شبکه، تحلیل چالش‌های امنیتی از طریق تحلیل محیطی و شناسایی و رتبه‌بندی راهبردهای امنیت شَما در فضای سایبر است.

## ۱-۲. اهمیت و ضرورت تحقیق

- ❖ موضوع شَما از مسائل راهبردی است که به دلیل نبود پژوهش‌های کافی و هدفمند، با دیدگاه‌ها و تفاسیر متفاوت در میان جامعه، محافل علمی و متولیان اجرایی مواجه شده است. بنابراین انجام این تحقیق گامی مؤثر در مفهوم‌شناسی مبانی نظری شَما و زمینه‌ساز دستیابی به درک مشترک و همگرایی میان ذی‌نفعان و سیاست‌گذاران است.
- ❖ تبیین اهمیت امنیت در شَما و مدل مفهومی ارائه‌شده در این تحقیق، چهارچوبی اولیه برای انجام پژوهش‌های علمی آینده و توسعه دانش در این حوزه است.
- ❖ راهبردهای ارائه‌شده در این تحقیق نیز می‌توانند مبنای سیاست‌گذاری و تدوین برنامه‌های اقدام در سطح راهبردی قرار گیرند.
- ❖ دستیابی به زیرساخت ارتباطی امن در قالب شَما، از دغدغه‌های اصلی حاکمیت است که در اسناد بالادستی مورد تأکید قرار گرفته و توجه ویژه به چالش‌ها و تهدیدهای فضای مجازی و نقش حیاتی این شبکه در مقابله با مخاطرات بالقوه و بالفعل مجازی، ضرورت انجام تحقیق در این زمینه را برجسته می‌سازد.
- ❖ نبود تحقیق جامع در این حوزه، می‌تواند منجر به کم‌توجهی و تأخیر در تحقق خواسته جدی مقام معظم رهبری درباره تسریع در راه‌اندازی شبکه ملی اطلاعات گردد.

- در صورت عدم انجام این تحقیق، بسیاری از ابهامات و انتظارات مانند الزامات امنیتی شَما، جایگاه امنیت در شبکه و ایجاد رویکرد امنیت‌محور در فضای سایبر بی‌پاسخ خواهد ماند که این وضعیت موجب کاهش اعتماد عمومی و استقبال محدود از شبکه خواهد شد.
- درحال‌حاضر توسعه فضای سایبر در جمهوری اسلامی ایران با مؤلفه‌های تثبیت‌کننده امنیت ملی هم‌سویی کامل ندارد. بی‌توجهی به مقوله امنیت و فقدان تحقیقات هدفمند در این حوزه، مانع از برآورد دقیق تهدیدهای امنیتی شده و غفلت راهبردی در حکمرانی مجازی و خدشه‌دار شدن امنیت ملی را به همراه خواهد داشت.

## ۱-۳. پیشینهٔ تحقیق

موضوع شَما در سال‌های اخیر در برخی پروژه‌های تحقیقاتی، رساله‌ها و مقالات علمی مورد توجه پژوهشگران قرار گرفته است. یکی از پژوهش‌های نسبتاً جامع در زمینه شَما، پروژه تحقیقاتی با عنوان «بازنگری مفاهیم شبکه ملی اطلاعات» است که توسط جمعی از کارشناسان پژوهشگاه ارتباطات و فناوری اطلاعات انجام شده است. در این طرح، ضمن مرور اسناد بالادستی، تعریف، چهارچوب‌ها، حوزه‌های مطرح، بازیگران و دست‌اندرکاران، مدل‌های مفهومی، معماری کلان و اجزای شبکه ملی اطلاعات به تفصیل مورد بررسی قرار گرفته است (جمعی از پژوهشگران، ۱۳۹۱).

میررفیع در رساله دکتری خود با عنوان «راهبردهای پدافند غیرعامل زیرساخت‌های ارتباطی شبکه ملی اطلاعات کشور در برابر تهدیدات سایبری»، پس از احصاء تهدیدات سایبری در حوزه زیرساخت ارتباطی شبکه ملی اطلاعات و ارزیابی و پیامدسنجی آن‌ها به ارائه راهبردهایی جهت مصون‌سازی، استحکام‌بخشی و به‌کارگیری ملاحظات، اصول و ضوابط پدافند غیرعامل در شبکه ملی اطلاعات پرداخته است (میررفیع، ۱۳۹۴). برخی از مقالات منتشرشده در مورد شبکه ملی اطلاعات و نکات مطرح شده در این مقالات در جدول زیر آمده است.

| نویسندگان | نکات مرتبط |
|---|---|
| هلیلی و همکاران(۱۳۹۳) | تأکید بر ضرورت تولید، ذخیره، نگهداری، جابه‌جایی، انتقال و حفاظت از اطلاعات ملی حساس و طبقه‌بندی‌شده در بستری امن و قابل اعتماد. |
| هاشمی و همایون (۱۳۹۶) | بررسی نقش محوری شبکه ملی اطلاعات در زمینه‌سازی و فراهم‌سازی بسترهای لازم برای پیشبرد سیاست‌های فرهنگی کشور در فضای مجازی. |
| همایون و هاشمی (۱۳۹۶) | تحلیل انتقادی از نحوه بازنمایی شبکه ملی اطلاعات در رسانه‌های برون‌مرزی به‌عنوان ابزاری برای محدودسازی آزادی اینترنت، نقض حریم خصوصی و سرکوب جریان‌های مخالف. |
| نامداریان (۱۳۹۸) | مطالعه آثار اقتصادی شبکه ملی اطلاعات ازجمله بهبود کارایی و بهره‌وری، کاهش هزینه‌ها و نوآوری. |
| نصرت‌آبادی (۱۳۹۸) | ارزیابی شبکه ملی اطلاعات در سه بُعد امنیتی، فناورانه و مدیریتی. |
| محمدی خانقاهی و رضایی(۱۳۹۸) | شناسایی چالش‌هایی همچون فقدان اجماع نظر در میان مسئولان و نهادهای متولی، تمرکز بیش از حد بر بُعد زیرساختی و توسعه نامتوازن، ضعف پیوست اجتماعی و غلبه رویکرد سیاسی. |
| رحمانی و همکاران(۱۳۹۹) | بررسی امنیت شبکه ملی اطلاعات به‌منظور مدیریت مستقل داخلی، عرضه محتوا و خدمات، ارتباطات امن، پرظرفیت و پایدار با تضمین کیفیت. |
| عبیری و همکاران (۱۳۹۹) | احصاء شاخص‌های بین‌المللی برای تقویت امنیت، توسعه زیرساخت‌های اطلاعاتی و ارتباطی و فراهم‌سازی بستر خدمات مجازی به‌عنوان فرصت‌های شبکه ملی اطلاعات؛ در مقابل، تهدیداتی مانند جاسوسی، افشای اطلاعات، نقض حریم خصوصی، قطع اینترنت، تحریم‌ها و خرابکاری در زیرساخت‌ها |
| مرتضوی (۱۴۰۲) | تأکید بر نقش شبکه ملی اطلاعات در تحقق دولت الکترونیک، سلامت و آموزش الکترونیک و تضمین استقلال و امنیت ملی در فضای سایبر |
| قهرمانی و مسلمی(۱۴۰۲) | تحلیل نقش شبکه ملی اطلاعات در جنگ‌های شناختی و ترکیبی به‌منظور خنثی‌سازی ناکارآمدی و تقویت اقتدار ملی |

شَما با فراهم‌سازی زیرساخت مستقل، امن و پایدار برای انتقال و پردازش داده، موجب تقویت مدیریت و کنترل داده‌ها توسط کشور (حاکمیت داده) می‌شود. این امر موجب رشد پلتفرم‌های بومی، کاهش وابستگی به خدمات خارجی، صرفه‌جویی ارزی و تقویت اقتصاد مقاومتی در فضای دیجیتال می‌شود. در حوزه جنگ شناختی نیز، شَما، با کنترل جریان محتوا،

مقابله با پیام‌های رسانه‌ای مخرب و بومی‌سازی بسترهای توزیع محتوا، به تقویت امنیت ذهنی کاربران (مصونیت در برابر تهدیدات اطلاعاتی و شناختی، مانند تحریف واقعیت‌ها یا القای ترس ) کمک می‌کند. همچنین با افزایش اعتماد عمومی و اجرای سازوکارهای احراز هویت و حفظ حریم خصوصی، تاب‌آوری جامعه در برابر تهدیدهای شناختی افزایش می‌یابد.

در بسیاری از کشورها استفاده از شبکه‌ای مشابه شَما، مورد توجه قرار گرفته است. به‌عنوان مثال در کشورِ کره جنوبی با ایجاد بستر فیبر نوری در تمام مناطق شهری و روستایی طرحی یکپارچه در راستای حاکمیت الکترونیک پیاده‌سازی شده است (یون، ۲۰۱۶: ۴۷). در ایالات متحده آمریکا نیز از سال ۲۰۱۵، پروژه‌ای با عنوان شبکه ملی پهن‌باند عمومی با هدف دسترسی ارزان و گسترده به اینترنت اجرا شده است (شارک، ۲۰۱۵). یکی از کشورهای پیشگام در این حوزه، استرالیا است که استفاده از خدمات پهن باند و پر سرعت را تحت عنوان شبکه پهن باند ملی (NBN) فراهم نموده است. (لیندوال، ۲۰۱۷). در کشور چین نیز استفاده از موتورهای جست‌وجو و پیام‌رسان‌های بومی، با هدف دستیابی به فناوری‌های بدیع، رقابت صنعتی و ایجاد شبکه‌ای بومی برای امنیت اطلاعات انجام شده است (بن و همکاران، ۲۰۱۷ : ۲۶).

مرور مطالعه تطبیقی در سطح بین‌المللی نشان می‌دهد که نوع، میزان اثرگذاری و سطوح تهدیدات، همچنین اهداف طراحی شبکه‌های ملی اطلاعات در هر کشور متفاوت است. درواقع، شبکه ملی اطلاعات ایران در راستای اهدافی مشابه با کشورهای پیشرو توسعه‌یافته است. مانند کره جنوبی، بر ایجاد زیرساخت یکپارچه برای حاکمیت الکترونیک، همچون آمریکا و استرالیا بر گسترش دسترسی پهن‌باند ارزان و پرسرعت و مشابه چین بر بومی‌سازی خدمات، استقلال اطلاعاتی و ارتقای امنیت مجازی تمرکز دارد. این شبکه ترکیبی از اهداف توسعه‌ای، امنیتی و حاکمیتی را دنبال می‌کند.

در اغلب تحقیقات منتشرشده خارجی، بُعد فناورانه و زیرساختی این شبکه‌ها مورد توجه قرار گرفته است. از سوی دیگر، در برخی پژوهش‌های داخلی نیز به‌طور ضمنی به چالش‌های

امنیتی ناشی از گسترش فضای مجازی اشاره شده، اما آثار و پیامدهای حملات مجازی بر امنیت مجازی و امنیت ملی به‌صورت عمیق تحلیل نشده‌اند. درهرحال، شَما به‌عنوان یک شبکه بومی، دارای مؤلفه‌ها و شاخص‌های خاص خود است که برای طراحی راهبردهای امنیتی اثربخش، نیازمند پژوهش‌های جامع‌تر و عمیق‌تری است؛ موضوعی که در این تحقیق به‌طور ویژه مورد توجه قرار گرفته است.

## ۱-۴. اهداف تحقیق

### ۱-۴-۱. هدف اصلی

احصای راهبردهای امنیت شبکه ملی اطلاعات در فضای سایبر و اولویت‌بندی آن‌ها براساس میزان اهمیت و اثربخشی

### ۱-۴-۲. اهداف فرعی

- ❖ شناسایی و تحلیل الزامات و سازوکارهای امنیتی شبکه ملی اطلاعات؛
- ❖ احصا و بررسی عوامل و متغیرهای مؤثر داخلی و خارجی بر امنیت فضای سایبر؛
- ❖ ارائه و اولویت‌بندی راهبردهای تأمین امنیت فضای سایبر از طریق شبکه ملی اطلاعات.

## ۱-۵. سؤال‌های تحقیق

### ۱-۵-۱. سؤال اصلی

راهبردهای امنیتی شبکه ملی اطلاعات در فضای سایبر کدام‌اند و این راهبردها چگونه می‌توانند براساس میزان اهمیت و اثربخشی، اولویت‌بندی شوند؟

### ۱-۵-۲. سؤال‌های فرعی

- ❖ اجزای الزامات و سازوکارهای کلیدی در تحقق امنیت شبکه ملی اطلاعات کدام‌اند؟
- ❖ مؤلفه‌ها و متغیرهای مؤثر داخلی و خارجی در امنیت فضای سایبر کدام‌اند؟

❖ از منظر راهبردی شبکه ملی اطلاعات چگونه می‌تواند در تقویت امنیت فضای مجازی کشور نقش‌آفرینی کند؟

## ۱-۶. روش تحقیق

پژوهش حاضر از نظر هدف، کاربردی است، از لحاظ روش گردآوری اطلاعات، به‌صورت توصیفی- تحلیلی انجام شده است. همچنین از نظر روش تجزیه‌وتحلیل داده‌ها، آمیخته (کمی و کیفی) محسوب می‌شود. در بخش کیفی، داده‌ها از طریق مطالعه کتابخانه‌ای و بررسی اسناد، گزارش‌ها و منابع معتبر داخلی و بین‌المللی گردآوری شده‌اند. برای اعتبارسنجی و ارزیابی یافته‌ها، از پرسشنامه تخصصی و تحلیل آماری داده‌های کمی استفاده شده است.

در این مقاله، به‌منظور تحلیل راهبردی، از الگوی سوآت، استفاده شده است. در این روش، ابتدا با بهره‌گیری از نظرات خبرگان و متخصصان حوزه مجازی، عوامل مؤثر به دو دسته عوامل داخلی (نقاط قوت، ضعف) و خارجی (تهدید و فرصت) تقسیم‌شده است. سپس با تشکیل ماتریس سوآت مطابق جدول (۱)، راهبردهای تهاجمی(SO)، محافظه‌کارانه (WO)، رقابتی (ST) و تدافعی (WT) شناسایی و تدوین شده‌اند (حسن بیگی،۱۳۹۰: ۳۵۱).

جدول ۱: استفاده از عوامل محیطی سوآت در راهبردها

| | | عوامل داخلی | |
|---|---|---|---|
| | | نقاط ضعف (W) | نقاط قوت (S) |
| عوامل خارجی | فرصت‌ها (O) | راهبردهای محافظه‌کارانه (WO) (بهره‌گیری از فرصت‌ها برای جبران یا رفع نقاط ضعف و تبدیل آن‌ها به قوت) | راهبردهای تهاجمی (SO) (بهره‌گیری از نقاط قوت برای استفاده حداکثری از فرصت‌ها) |
| | تهدیدها (T) | راهبردهای تدافعی (WT) (کاهش اثر تهدیدات با کاهش آسیب‌پذیری‌ها و نقاط ضعف) | راهبردهای رقابتی (ST) (حذف یا مقابله با تهدیدها با استفاده از نقاط قوت) |

پس از احصای راهبردها، پرسش‌نامه‌ای محقق ساخته بین خبرگان توزیع گردید. پس از جمع‌آوری نظر خبرگان از روش رتبه‌بندی عوامل مؤثر در تصمیم‌گیری‌های چند شاخصه و نرم‌افزار تاپسیس برای اولویت‌بندی استفاده شد. در اینجا گزینه‌ها شامل راهبردها و شاخص‌ها، عوامل محیطی در نظر گرفته شدند.

در تکنیک «تاپسیس»[1] «انتخاب برترین گزینه از طریق تشابه به راه‌حل ایدئال»، هر عامل انتخاب شده باید کمترین فاصله را با عامل ایدئال مثبت و بیشترین فاصله را با عامل ایدئال منفی داشته باشد. فاصله از عامل ایدئال به‌عنوان معیاری برای درجه‌بندی و اولویت‌بندی عوامل است (شانیان و همکاران، ۱۳۸۳).

با توجه به تمرکز این تحقیق بر راهبردهای حوزه امنیت شَما، جامعه آماری به‌صورت هدفمند و محدود انتخاب شده و شامل خبرگان دارای تخصص و تجربه کافی در حوزه‌های مدیریت راهبردی، امنیت شبکه و مباحث مرتبط با فضای مجازی است. در این پژوهش، انتخاب خبرگان با رعایت معیارهای تخصصی و سازمانی انجام شد تا اعتبار و قابلیت اتکای داده‌های جمع‌آوری‌شده تضمین شود. معیارهای اصلی انتخاب خبرگان عبارتند از: دارا بودن حداقل پنج سال سابقه کاری مرتبط با حوزه‌های امنیت فضای مجازی، مدیریت راهبردی و سیاست‌گذاری در فضای مجازی؛ داشتن مدرک تحصیلی دکتری؛ عضویت فعال در نهادهای تصمیم‌ساز و اجرایی، نظیر مراکز ملی فضای مجازی، سازمان فناوری اطلاعات ایران ، سازمان پدافند غیرعامل و مراکز تحقیقاتی دانشگاهی معتبر و همچنین برخورداری از تجربه مدیریتی، پژوهشی و آموزشی مرتبط با موضوع تحقیق. براساس فرمول کوکران برای تعیین حجم نمونه، با توجه به جامعه آماری حدود ۷۰ نفر(N =70)، سطح اطمینان ۹۵ درصد (Z =1.96)، برآورد فراوانی ویژگی مورد نظر (p =0.5) خطای نمونه‌گیری قابل قبول (d =0.05)، حجم نمونه ۱۸ نفر انتخاب شد. این تعداد به‌عنوان نمونه‌ای از جامعه آماری در نظر گرفته شده است که امکان انجام تحلیل‌های آماری معتبر را فراهم می‌کند. این رویکرد موجب گردید دیدگاه‌های ارائه شده از جنبه‌های علمی، تخصصی و اجرایی برخوردار بوده و منجر به افزایش اعتبار و تعمیم‌پذیری نتایج تحقیق شود. با توزیع

1. TOPSIS: Technique of Preference by Similarity to Ideal Solution

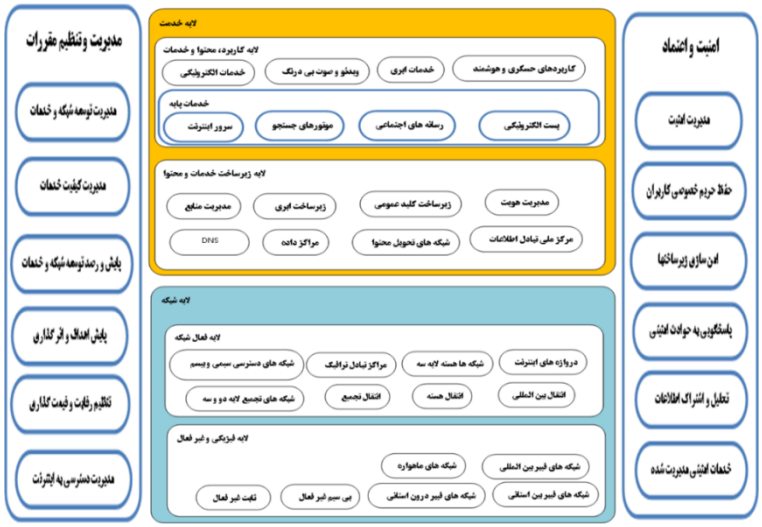
پرسش‌نامه محقق ساخته میان جامعه آماری، میزان اهمیت شاخص‌های احصا شده با استفاده از طیف لیکرت به‌دست آمده است.

## ۲. ادبیات و مبانی نظری تحقیق

### ۲-۱. معماری لایه‌ای و ویژگی‌های شبکه ملی اطلاعات

براساس تعریف مصوب شورای عالی فضای مجازی، شبکه ملی اطلاعات (شَما) به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای است مبتنی بر قراردادهای اینترنتی که از سوئیچ‌ها، مسیریاب‌ها و مراکز داده داخلی تشکیل شده و به‌گونه‌ای طراحی شده است که درخواست‌های دسترسی به اطلاعات ذخیره‌شده در مراکز داده داخلی، به هیچ‌وجه از طریق خارج کشور مسیریابی نشوند. همچنین، این شبکه امکان راه‌اندازی شبکه‌های اینترانت، خصوصی و امن داخلی را فراهم می‌سازد. از دیدگاه معماری، با توجه به تنوع فناوری‌های نوین، شَما، باید به‌گونه‌ای طراحی شود که با صرف حداقل هزینه و اعمال کمترین تغییرات، خدمات موردنیاز را به‌سرعت بتواند ارائه دهد؛ لذا برای تمایز بخش‌های مختلف، از معماری لایه‌ای استفاده می‌شود.

در منابع مختلف، مدل‌های مفهومی و لایه‌ای متنوعی برای شبکه ملی اطلاعات ارائه شده است. در همین راستا، در نشست خبرگان شورای عالی فضای مجازی در بهمن‌ماه ۱۳۹۴ یک مدل مرجع برای شبکه ملی اطلاعات در نظر گرفته شد. این مدل با هدف ایجاد انسجام، شفافیت وظایف و مرزبندی نقش‌ها در توسعه و بهره‌برداری از شبکه ملی اطلاعات، ارائه شده و از دو لایه افقی خدمت و زیرساخت شبکه و دو لایه عمودی مدیریت و تنظیم مقررات و امنیت و اعتماد تشکیل شده است. در شکل (۱) این مدل نشان داده شده است.




شکل ۱: مدل مرجع شبکه ملی اطلاعات

با توجه به مدل مرجع (شَما) و مرور مفاهیم و یافته‌های مطرح‌شده در پیشینه پژوهش، مهم‌ترین ویژگی‌های این شبکه به شرح زیر احصا شده است:

- ❖ برخورداری از زیرساخت مناسب برای ذخیره‌سازی، تعامل و اشتراک اطلاعات شبکه‌های رایانش ابری و ارائه خدمات الکترونیکی امن، سریع و کم‌هزینه؛
- ❖ قابلیت برقراری ارتباطات امن و پایدار میان دستگاه‌ها و مراکز حیاتی کشور برای دریافت خدمات چندرسانه‌ای از منابع داخلی؛
- ❖ ایجاد بستر مناسب برای توسعه خدمات بومی شامل شبکه‌های اجتماعی مجازی، سیستم‌عامل‌ها، موتورهای جستجو، پست الکترونیکی و دیگر پروژه‌های اقماری؛
- ❖ زمینه‌سازی برای سالم‌سازی فضای مجازی و ترویج ارزش‌های معنوی و عدالت اجتماعی از طریق ارائه خدمات مطمئن، ارزان و در دسترس برای کلیه کاربران؛
- ❖ ارتقای سطح امنیت ملی و صیانت از حریم خصوصی کاربران در فضای مجازی؛
- ❖ ویژگی‌های شَما در چهارچوب مدل چهارلایه‌ای مرجع عبارتند از: زیرساخت ارتباطی امن، پایدار و پرسرعت در لایه شبکه، خدمات بومی و مقرون‌به‌صرفه در

لایه خدمت، حفاظت از حریم خصوصی و امنیت ملی در لایه امنیت و سیاست‌گذاری و نظارت در لایه مدیریت و مقررات.

این تقسیم‌بندی، بیانگر جامعیت شَما در پوشش ابعاد فنی، خدماتی و حاکمیتی است.

## ۲-۲. نقش و جایگاه امنیت در شبکه ملی اطلاعات

امنیت همواره یکی از اصلی‌ترین دغدغه‌های بشر بوده و با وجود تحول در معنا و عوامل آن، همچنان مهم‌ترین کارویژه و فلسفه وجودی دولت‌ها محسوب می‌شود (ملکی و همکاران، ۱۴۰۲).

امنیت در فضای سایبر، همچون امنیت در جهان واقعی، مفهومی نسبی و چندوجهی با ماهیتی عمدتاً ذهنی است. بنابراین تحقق آن صرفاً با رویکرد برخورد سلبی با تهدیدات عینی حاصل نمی‌شود ، بلکه نیازمند ساختارهایی برای تقویت اعتماد، انسجام و تاب‌آوری در فضای مجازی است (عبیری و همکاران، ۱۳۹۹).

با توجه به اینکه فضای سایبر تمامی ابعاد زندگی بشر را تحت تأثیر قرار داده، تأمین امنیت در این فضا به اندازه فضای واقعی ضروری است. در جمهوری اسلامی ایران، امنیت مجازی در امتداد گفتمان امنیت ملی با رویکردی ایدئولوژیک تعریف می‌شود که هدف آن حفظ ارزش‌های حیاتی بدون امنیتی‌سازی جامعه است(نصری، ۱۳۹۲). بر این اساس، نقش و جایگاه امنیت در شَما، امری ضروری و واجد اهمیت راهبردی است. این شبکه برای ایفای نقش مؤثر در ساختار امنیت ملی باید از ویژگی‌ها و سازوکارهای لازم برای تأمین و حفظ امنیت برخوردار باشد.

پس از بررسی مدل‌های ارائه شده برای اجزاء معماری شَما و نیز امنیت شَما، مدل مفهومی شکل (۲) برای امنیت در این شبکه، پیشنهاد می‌شود. در این مدل مفهومی، شَما شامل چهار لایه اصلی است و برای هر لایه، سازوکارهای امنیتی مشخصی در قالب ده محور کلیدی تعریف شده است که به‌منظور تأمین جامع امنیت در سطوح مختلف این شبکه در نظر گرفته شده است. سازوکارهای امنیت در هر لایه عبارتند از:

- ❖ لایهٔ محتوا–خدمات و کاربردها: محرمانگی، یکپارچگی (صحت) و دسترس‌پذیری؛
- ❖ لایهٔ شبکه–زیرساخت اطلاعاتی و ارتباطی: رمزنگاری، امضای دیجیتال و مجازشناسی؛
- ❖ لایهٔ انسانی و اجتماعی (کاربران و ذی‌نفعان): احراز هویت و حریم خصوصی
- ❖ لایهٔ مدیریت و قوانین: عدم انکار و کنترل دسترسی


شکل ۲: مدل پیشنهادی امنیت در شبکه ملی اطلاعات (منبع: پژوهشگر)

امنیت شَما، حاصل تعامل زنجیروار چهار لایه است: لایه حاکمیتی وظیفه تدوین سیاست‌ها و مقررات را بر عهده دارد؛ لایه زیرساخت، این سیاست‌ها را با بهره‌گیری از ابزارهای فنی اجرا می‌کند؛ لایه خدمات و محتوا بر بستر این زیرساخت، خدمات امن ارائه می‌دهد؛ و لایه انسانی از طریق رفتار کاربران، احراز هویت و رعایت حریم خصوصی، نقشی کلیدی در حفظ یا تضعیف امنیت دارد.

مدل مفهومی پیشنهادی به‌گونه‌ای طراحی شده که سازوکارهای امنیتی در هر لایه، نقشی مکمل و وابسته به سایر لایه‌ها دارند و مجموعه این سازوکارها یک زنجیره امنیتی منسجم را تشکیل می‌دهند. در این مدل، هیچ‌یک از لایه‌ها به‌صورت مستقل، قادر به تضمین امنیت نیستند بلکه آنچه امنیت را پایدار و یکپارچه می‌سازد؛ هم‌پوشانی و تعامل میان سازوکارهاست. به همین دلیل، مدل به‌صورت زنجیروار طراحی شده تا نشان دهد که شکاف یا ضعف در هر یک از حلقه‌ها، می‌تواند کل امنیت شَما را با تهدید مواجه سازد.

## ۳. تجزیه‌وتحلیل یافته‌های تحقیق

با توجه به مبانی نظری تبیین‌شده در بخش‌های پیشین، امنیت مجازی به‌عنوان مفهومی چندبُعدی، متأثر از ساختارهای فناورانه، حکمرانی دیجیتال و تعاملات انسانی در سطوح مختلف مطرح می‌شود. در این راستا، شَما، به‌عنوان زیرساخت ارتباطی فضای سایبر کشور، نیازمند بهره‌گیری از تجهیزات امنیتی پیشرفته و پیاده‌سازی الزامات امنیتی برای تقویت اطمینان و اعتماد عمومی است. در این مقاله، بر پایه مدل مفهومی چهارلایه‌ای پیشنهادی و در نظر گرفتن فضای سایبر به‌مثابه محیط اثرگذار بر امنیت شَما متغیرها و عوامل مؤثر بر امنیت شَما از طریق مطالعات اکتشافی شناسایی شده و مورد تجزیه‌وتحلیل قرار می‌گیرند. در جدول (۲) فهرست این عوامل ارائه شده است.

جدول۲: عوامل و متغیرهای مؤثر در امنیت شبکه ملی اطلاعات

| لایه‌های شَما | عوامل و متغیرهای مؤثر در امنیت شَما |
|---|---|
| شبکه/ زیرساخت اطلاعاتی و ارتباطی | استفاده از سامانه‌های امنیتی بومی، توسعه زیرساخت‌های ارتباطی و اطلاعاتی ایمن، ایجاد ارتباطات پایدار، امن و فراگیر، بهره‌گیری از تجهیزات امنیتی پیشرفته، ارتقای امنیت در مراکز داده داخلی<br>شناسایی و مقابله با آسیب‌پذیری‌ها و حفره‌های امنیتی، به‌کارگیری سازوکارهای رمزنگاری و امضای دیجیتال، مدیریت تهدید ناشی از تحریم‌های مجازی، رفع محدودیت در دسترسی به فناوری‌های نوین |
| مدیریت و قوانین | تدوین و اجرای قوانین و مقررات جامع امنیت مجازی، توسعه خدمات الکترونیکی ایمن و قانون‌مند، تعامل مؤثر میان سازمان‌ها و نهادهای مسئول امنیت اطلاعات، مشارکت در پیمان‌ها و چهارچوب‌های امنیت مجازی منطقه‌ای و جهانی، سیاست‌گذاری و اعمال نظارت و مدیریت هوشمند محتوا، مقابله با جاسوسی و افشای غیرمجاز اطلاعات، پیشگیری و واکنش به حملات مجازی و خرابکاری‌های هکری، برخورد با جرائم سازمان‌یافته مجازی و پول‌شویی اطلاعاتی، مدیریت خسارات وارده به زیرساخت‌های ارتباطی، تقویت توان بازدارندگی و دفاع فعال در برابر تهدیداهای پیشرفته مجازی |
| محتوا/ خدمات و کاربردها | تولید و انتشار محتوای غنی علمی، پژوهشی و آموزشی، اعمال نظارت هوشمند و هدفمند بر محتوای شبکه، لحاظ پیوست‌های فرهنگی و امنیتی در خدمات دیجیتال، ارائه خدمات پایه امنیتی قابل‌دسترس و کارآمد، اجرای نظام فیلترینگ هوشمند و چندلایه، تقویت تاب‌آوری در برابر بحران‌ها و تهدیدات مجازی، تضمین |

| | |
|---|---|
| | ارتباطات امن و پایدار در خدمات کاربردی، مدیریت اختلال در ارائه خدمات الکترونیکی، برنامه‌ریزی برای مواقع قطع ارتباط با اینترنت جهانی، توجه به پدیده خودسانسوری در تعاملات کاربری |
| انسانی و اجتماعی (کاربران) | اهتمام مسئولان و سیاست‌گذاران به توسعه شبکه‌ای امن، تربیت و به‌کارگیری نیروی انسانی ماهر، متخصص و متعهد، ارتقای سطح آگاهی و آمادگی کاربران در حوزه امنیت مجازی، تقویت سواد رسانه‌ای و رفتار مسئولانه کاربران، اجرای سازوکارهای دقیق احراز هویت کاربران، حفاظت مؤثر از حریم خصوصی و داده‌های شخصی، تقویت امنیت ذهنی و روانی کاربران در فضای مجازی، میزان پذیرش عمومی شَما در میان اقشار مختلف جامعه، نگرانی‌های کاربران درباره نقض حریم خصوصی و امنیت اطلاعات، تأثیرات روانی و اجتماعی ناشی از محدودیت‌ها یا قطع احتمالی اینترنت، نگرش‌ها، رفتارها و تجارب کاربران در استفاده از خدمات بومی |

در این تحقیق پس از احصای عوامل مؤثر در امنیت شَما، مطابق جدول (۲)، مهم‌ترین عوامل محیط داخلی (قوت و ضعف) و عوامل محیط خارجی ( فرصت و تهدید) بدست آمده است. در مرحله بعد، بر مبنای جدول (۲) و استفاده از مبانی نظری پژوهش، مطالعات اسنادی کتابخانه‌ای و استفاده از نظرات خبرگان، راهبردهای SO، WO، ST و WT تدوین گردیده است. عوامل محیطی و راهبردهای احصا شده در جدول (۳) نشان داده شده است.

جدول۳: ماتریس راهبردهای امنیت در شبکه ملی اطلاعات

| نقاط قوت (S) | نقاط ضعف (W) | |
|---|---|---|
| S1- عنایت خاص مقام معظم رهبری، تأکیدات قانونی در اسناد بالادستی و اهتمام مسئولین نسبت به شَما<br>S2 - وجود نیروی انسانی ماهر، متخصص و کارآمد داخلی<br>S3 - وجود دانش بومی و منابع غنی علمی، فرهنگی، دینی، پژوهشی، آموزشی | W1- بومی نبودن تجهیزات امنیتی و مراکز داده داخلی<br>W2- آسیب‌پذیری‌ها و حفره‌های امنیتی در زیرساخت‌های حیاتی<br>W3- وابستگی تجهیزات امنیتی شَما به کشورهای صنعتی پیشرفته | عوامل داخلی |

| | | | |
|---|---|---|---|
| S4 - ظرفیت‌ها و توانمندی‌های صنایع و شرکت‌های دانش‌بنیان داخلی در تولید سامانه‌های امنیتی<br>S5- برنامه‌های آگاه‌سازی و کسب آمادگی کاربران در مورد مخاطرات امنیتی<br>S6- توانمندی‌های موجود داخلی در زمینه رصد، پایش و مدیریت اطلاعات<br>S7- توسعه مناسب زیرساخت‌های ارتباطی، اطلاعاتی و شبکه<br>S8- قابلیت‌های موجود در برقراری ارتباطات امن و محافظت‌شده بین سازمان‌ها و مراکز حیاتی کشور | W4- کیفیت پایین و ناکارآمدی پیوست‌های فرهنگی و امنیتی در جلب اعتماد کاربران<br>W5 - ضعف در تدوین قوانین و مقررات و بازدارندگی پایین قوانین مصوب<br>W6- عدم همکاری و هماهنگی مناسب میان سازمان‌های مرتبط با سیاست‌گذاری امنیت<br>W7- هزینه بالا و کیفیت پایین ارائه و دسترسی به خدمات پایه امنیتی<br>W8- پایین بودن سواد رسانه‌ای کاربران در مواجهه با ملاحظات امنیت مجازی | عوامل خارجی | |
| **راهبردهای SO** | **راهبردهای WO** | | فرصت‌ها (O) |
| (SO)1: تسریع در راه‌اندازی شَما، براساس خواسته مقام معظم رهبری و اسناد بالادستی، به‌منظور دستیابی به استقلال داخلی و تاب‌آوری در بحران‌های امنیتی فضای سایبر<br>(SO)2: افزایش تولید و تبادل محتوای غنی علمی، آموزشی فرهنگی و دینی در بستر شَما جهت فراهم نمودن حاکمیت داده و تأمین نیازهای مادی و معنوی جامعه | (WO)1: به‌کارگیری سازوکارهای رمزنگاری و امضای دیجیتال بومی در شَما، به‌منظور کاهش آسیب‌پذیری‌ها در زیرساخت‌های حیاتی کشور همراه با برنامه‌ریزی برای تأمین منابع مالی جهت غلبه بر چالش‌های فناورانه<br>(WO)2: بهره‌گیری از احراز هویت هوشمند در شَما، جهت حفاظت از حریم خصوصی، | O1- شکل‌گیری پیمان‌ها و معاهدات امنیت مجازی در سطح بین‌الملل<br>O2 - قابلیت‌های بازدارندگی و دفاع در حملات و تهاجم مجازی<br>O3 – حاکمیت داده به‌منظور ایجاد امنیت روانی و ذهنی<br>O4 – فناوری‌های داده‌کاوی، فیلترینگ هوشمند، نظارت و کنترل محتوا در فضای سایبر | |

| | | | |
|---|---|---|---|
| 3(SO): به‌کارگیری سامانه‌های امنیتی بومی در زیرساخت‌های شَما، به‌منظور اجرای فیلترینگ هوشمند، نظارت، کنترل و مدیریت اطلاعات و ارتقاء مشارکت در احراز هویت، حفاظت از حریم خصوصی و رفتار مسئولانه کاربران در فضای سایبر | کاهش جرائم مجازی و رعایت ملاحظات امنیتی از طریق فرهنگ‌سازی و هماهنگی فنی و حقوقی میان نهادهای ذی‌ربط | O5- تأمین امنیت خدمات از طریق سازوکارهای رمزنگاری و امضای دیجیتال بومی<br>O6- استقلال داخلی و تاب‌آوری در مدیریت بحران‌های مجازی<br>O7- تبادل اطلاعات امن، پایدار و فراگیر میان نهادهای دولتی، شرکت‌های خصوصی و کاربران<br>O8 - احراز هویت و حفاظت از حریم خصوصی کاربران | |
| **راهبردهای ST** | **راهبردهای WT** | T1- جاسوسی و افشای غیرمجاز اطلاعات در مراکز داده ملی<br>T2 - نفوذ، خرابکاری و اختلال در ارائه خدمات الکترونیکی<br>T3 - حملات مجازی هکرها و کشورهای متخاصم به سامانه‌های حیاتی و حساس<br>T4- صدمه و خسارت به زیرساخت‌های ارتباطی شَما،<br>T5- اقدام به قطع ارتباط شَما، با اینترنت<br>T6 - امکان تحریم مجازی و عدم دستیابی به فناوری‌های نوین | تهدیدها (T) |
| 1(ST): گسترش کمی و کیفی اقدامات آگاه‌سازی و جلب اعتماد کاربران نسبت به امنیت شَما، جهت افزایش آمادگی در برابر تهدیدات امنیتی و کسب امنیت روانی جامعه در صورت قطعی اینترنت<br>2(ST): توسعه سامانه‌های ارتباطی و اطلاعاتی امن و بومی در شَما، با در نظر گرفتن محدودیت‌های فناوری، موانع تأمین منابع و هزینه‌های اجرایی، جهت مقابله با حملات مجازی هکرها و کشورهای متخاصم به زیرساخت‌های حیاتی و حساس کشور | 1(WT): برنامه‌ریزی و سرمایه‌گذاری در زمینه بومی‌سازی تجهیزات امنیتی شَما، به‌منظور خنثی‌سازی جاسوسی، افشای اطلاعات و صدمه به زیرساخت‌های حیاتی براساس تحلیل محدودیت‌های دسترسی به فناوری‌های نوین ناشی از اثرات تحریم‌ها<br>2(WT): کاهش وابستگی به شبکه جهانی اینترنت از طریق راه‌اندازی تدریجی شَما، به‌منظور کسب آمادگی در برابر تهدید قطع اینترنت، تحریم مجازی و مدیریت پیامدهای اجتماعی-فرهنگی مانند خودسانسوری | | |

| | | | |
|---|---|---|---|
| | | T7- القای ناکارآمدی شَما در تأمین امنیت و برهم زدن امنیت ذهنی و روانی جامعه<br>T8- خودسانسوری و عدم دسترسی به محتوا و خدمات شَما از خارج از کشور | |

در ادامه به‌منظور ارزیابی و اولویت‌بندی راهبردهای احصا شده از تکنیک تاپسیس استفاده شده است. در این روش، مراحل زیر انجام شده است:

۱. ایجاد ماتریس تصمیم‌گیری: پس از احصای ۹ راهبرد جدول (۳)، پرسش‌نامه محقق ساخته‌ای برای بررسی میزان اثر راهبردها بر عوامل محیطی (ضعف، قوت، فرصت و تهدید) تهیه شد و پس از توزیع بین اساتید و خبرگان حوزه‌های مرتبط با فضای سایبر و متخصصان شَما، جمع‌آوری شد. با توجه به اینکه تعداد ۹ راهبرد انتخاب‌شده است؛ میزان تأثیر هر راهبرد با استفاده از روش میانگین حسابی نظرات همه خبرگان محاسبه شد که نتایج آن در جدول (۴) به‌عنوان ماتریس تصمیم‌گیری نشان داده شده است.

جدول۴: ماتریس تصمیم‌گیری(D)

| شاخص‌ها/ راهبردها | S | W | O | T |
|---|---|---|---|---|
| (SO)1 | ۵/۸۳۳۳ | ۵/۴۰۰۵ | ۶/۱۲۰۰ | ۵/۰۸۳۳ |
| (SO)2 | ۵/۶۶۶۷ | ۴/۳۴۳۳ | ۵/۳۲۳۳ | ۵/۵۴۱۷ |
| (SO)3 | ۵/۴۰۰۰ | ۵/۴۳۱۳ | ۶/۳۵۳۳ | ۵/۶۶۶۷ |
| (WO)1 | ۵/۶۶۶۷ | ۵/۲۳۳۳ | ۶/۰۸۰۰ | ۵/۱۲۵۰ |
| (WO)2 | ۵/۴۳۳۳ | ۵/۳۰۱۰ | ۵/۶۶۶۷ | ۵/۱۲۵۰ |
| (ST)1 | ۵/۱۶۶۷ | ۵/۰۳۳۳ | ۶/۰۳۰۰ | ۴/۹۵۸۳ |
| (ST)2 | ۵/۲۳۳۳ | ۶/۰۰۲۳ | ۵/۵۰۱۰ | ۵/۶۶۶۷ |
| (WT)1 | ۴/۸۶۶۷ | ۵/۲۰۰۰ | ۶/۵۰۹۰ | ۴/۶۶۶۷ |
| (WT)2 | ۵/۷۶۶۷ | ۵/۱۳۳۳ | ۴/۱۶۶۷ | ۵/۱۶۶۷ |

۲. به دست آوردن ماتریس بی‌مقیاس موزون: برای این کار ابتدا ماتریس نرمال با تقسیم هر درایه ماتریس بر جذر مجموع مربعات ستون متناظر آن به‌دست‌آمده است. سپس از روش آنتروپی شانون[1] برای وزن دهی به معیارها استفاده شده است. هرچه پراکندگی مقادیر یک شاخص در گزینه‌ها بیشتر (آنتروپی کمتر) باشد اهمیت آن شاخص در تصمیم‌گیری بیشتر است در این بخش مقادیر موزون بدست می‌آیند (مؤمنی، ۱۳۸۵). در جدول (۵) ماتریس نرمال و در جدول (۶) مقادیر وزن معیار آمده است.

جدول۵: ماتریس نرمال (N)

| | S | W | O | T |
|---|---|---|---|---|
| (SO)1 | ۰/۳۱۶۷ | ۰/۳۴۷۳ | ۰/۳۴۳۱ | ۰/۳۵۶۴ |
| (SO)2 | ۰/۳۴۵۳ | ۰/۳۰۸۷ | ۰/۲۷۵۴ | ۰/۳۴۶۲ |
| (SO)3 | ۰/۳۵۳۱ | ۰/۳۶۶۶ | ۰/۳۴۵۳ | ۰/۳۲۹۹ |
| (WO)1 | ۰/۳۱۹۳ | ۰/۳۴۷۳ | ۰/۳۳۲۵ | ۰/۳۴۶۲ |
| (WO)2 | ۰/۳۸۱۶ | ۰/۳۲۸۰ | ۰/۳۳۶۸ | ۰/۳۳۱۹ |
| (ST)1 | ۰/۳۰۸۹ | ۰/۳۴۷۳ | ۰/۳۱۹۸ | ۰/۳۱۵۶ |
| (ST)2 | ۰/۳۵۳۱ | ۰/۳۱۸۳ | ۰/۳۸۱۳ | ۰/۳۱۹۷ |
| (WT)1 | ۰/۲۹۰۸ | ۰/۳۷۶۲ | ۰/۳۳۰۴ | ۰/۲۹۷۳ |
| (WT)2 | ۰/۳۲۱۹ | ۰/۲۴۱۲ | ۰/۳۲۶۲ | ۰/۲۵۲۳ |

جدول ۶: مقادیر محاسبه‌شده وزن معیار

| ردیف | معیارها | مقدار آنتروپی(Ej) | مقدار عدم اطمینان(dj) | وزن معیار(Wj) |
|---|---|---|---|---|
| ۱ | S | ۰/۹۵۲۹ | ۰/۰۴۷۱ | ۰/۲۴۸۸ |
| ۲ | W | ۰/۹۵۱۳ | ۰/۰۴۸۷ | ۰/۲۵۷۳ |
| ۳ | O | ۰/۹۵۲۹ | ۰/۰۴۷۱ | ۰/۲۴۸۸ |
| ۴ | T | ۰/۹۵۳۶ | ۰/۲۴۸۸ | ۰/۲۴۵۱ |

برای به‌دست‌آمده آوردن ماتریس بی‌مقیاس موزون (V)، ماتریس بی‌مقیاس شده (ماتریس نرمال) را در مقادیر وزن معیار به‌دست‌آمده ، ضرب می‌کنیم ( $V = w_j \times N$). برای این کار هر

1. Shannon entropy

ستون ماتریس N در یکی از مقادیر وزن معیار متناظر ضرب می‌شود. جدول (۷) ماتریس بی‌مقیاس موزون را نشان می‌دهد.

جدول ۷: ماتریس بی‌مقیاس موزون (V)

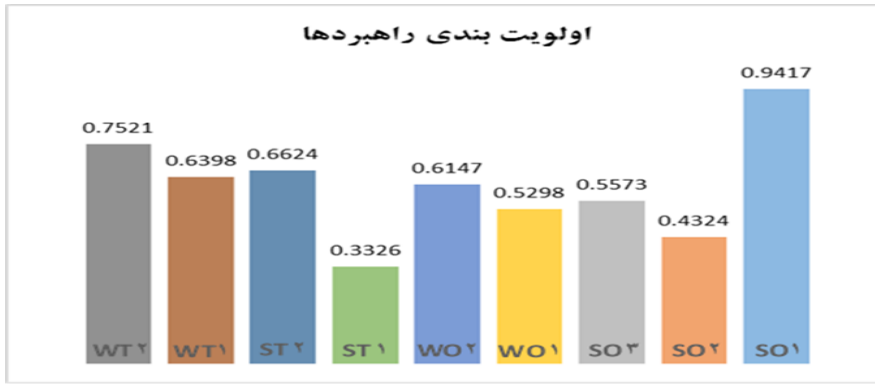
| | S | W | O | T |
|---|---|---|---|---|
| (SO)1 | ۰/۰۷۹ | ۰/۰۹۰ | ۰/۰۸۵ | ۰/۰۸۸ |
| (SO)2 | ۰/۰۸۶ | ۰/۰۸۰ | ۰/۰۶۹ | ۰/۰۸۵ |
| (SO)3 | ۰/۰۸۸ | ۰/۰۹۵ | ۰/۰۸۶ | ۰/۰۸۱ |
| (WO)1 | ۰/۰۸۰ | ۰/۰۸۹ | ۰/۰۸۳ | ۰/۰۸۵ |
| (WO)2 | ۰/۰۹۵ | ۰/۰۸۴ | ۰/۰۸۴ | ۰/۰۸۱ |
| (ST)1 | ۰/۰۷۷ | ۰/۰۸۹ | ۰/۰۷۹ | ۰/۰۷۸ |
| (ST)2 | ۰/۰۸۷ | ۰/۰۸۲ | ۰/۰۹۵ | ۰/۰۷۹ |
| (WT)1 | ۰/۰۷۳ | ۰/۰۹۹ | ۰/۰۸۲ | ۰/۰۷۳ |
| (WT)2 | ۰/۰۸۰ | ۰/۰۶۲ | ۰/۰۸۱ | ۰/۰۸۷ |

۳. تعیین عامل ایدئال مثبت و ایدئال منفی: در این مرحله باید گزینه‌های که از نظر پاسخ‌دهندگان به‌عنوان مهم‌ترین عامل و کم‌اهمیت‌ترین عوامل مشخص شده‌اند، شناسایی شوند. در این مرحله باید گزینه‌های که از نظر پاسخ‌دهندگان به‌عنوان مهم‌ترین عامل و کم‌اهمیت‌ترین عوامل مشخص شده‌اند، شناسایی شوند. به عبارتی برای شاخص‌های مثبت، ایدئال مثبت بزرگ‌ترین مقدار v و ایدئال منفی کوچک‌ترین مقدار v است، هم‌چنین برای شاخص‌های منفی، ایدئال مثبت کوچک‌ترین مقدار v و ایدئال منفی بزرگ‌ترین مقدار v است. در نهایت محاسبه میزان نزدیکی هرکدام از عوامل به عامل ایدئال مثبت و ایدئال منفی انجام می‌شود و براساس آن می‌توان رتبه‌بندی راهبردها را انجام داد.خلاصه نتایج این محاسبات در جدول (۸) و شکل (۴) نشان داده شده است.

جدول ۸ : رتبه‌بندی راهبردها

| گزینه‌ها | فاصله تا ایدئال مثبت | فاصله تا ایدئال منفی | CL | رتبه |
|---|---|---|---|---|
| (SO)1 | ۰/۰۱۷۷ | ۰/۲۸۵۲ | ۰/۹۴۱۷ | ۱ |

| گزینه‌ها | فاصله تا ایدئال مثبت | فاصله تا ایدئال منفی | CL | رتبه |
|---|---|---|---|---|
| (SO)2 | ۰/۰۳۲۹ | ۰/۰۲۵۱ | ۰/۴۳۲۴ | ۸ |
| (SO)3 | ۰/۰۲۹۷ | ۰/۰۳۷۴ | ۰/۵۵۷۳ | ۶ |
| (WO)1 | ۰/۰۲۶۸ | ۰/۰۳۰۱ | ۰/۵۲۹۸ | ۷ |
| (WO)2 | ۰/۰۲۱۲ | ۰/۰۳۳۸ | ۰/۶۱۴۷ | ۵ |
| (ST)1 | ۰/۰۴۰۲ | ۰/۰۲۰۰ | ۰/۳۳۲۶ | ۹ |
| (ST)2 | ۰/۰۱۸۸ | ۰/۰۳۶۹ | ۰/۶۶۲۴ | ۳ |
| (WT)1 | ۰/۰۲۰۲ | ۰/۰۳۵۸ | ۰/۶۳۹۸ | ۴ |
| (WT)2 | ۰/۰۱۳۴ | ۰/۰۴۰۶ | ۰/۷۵۲۱ | ۲ |




شکل۴: اولویت‌بندی راهبردهای احصا شد

### ۳-۱. فرایند عملیاتی پیاده‌سازی راهبردهای امنیت شبکه ملی اطلاعات

برای اثربخشی راهبردهای احصاءشده در حوزه امنیت شَما، صرف تدوین راهبرد کافی نیست؛ بلکه باید سازوکاری عملیاتی برای پیاده‌سازی، ارزیابی و به‌روزرسانی آن‌ها طراحی شود. چهارچوب عملیاتی پیشنهادی در این پژوهش، با هدف تبدیل راهبردهای کلان به اقدامات اجرایی و قابل سنجش، تدوین شده است. در ادامه، فرایند عملیاتی پیشنهادی در چهار گام کلان برای اجرای راهبردهای نه‌گانه در حوزه شَما، ارائه می‌شود:

**گام اول: آماده‌سازی و تحلیل وضعیت** : در این مرحله، ابتدا نهادهای ذی‌ربط شناسایی می‌شوند و وضعیت موجود شَما، از منظر زیرساختی، نهادی، قانونی و امنیتی بررسی می‌گردد. همچنین، نقاط قوت و ضعف موجود تحلیل شده و منابع موردنیاز برای اجرای هر راهبرد (اعم از انسانی، مالی، فنی) تخمین زده می‌شود.

**گام دوم: برنامه‌ریزی اجرایی**: با توجه به راهبردهای احصاءشده، برای هرکدام برنامه اجرایی مشخصی تدوین می‌شود. این برنامه شامل اقدامات کلیدی، جدول زمان‌بندی، مسئولیت دستگاه‌ها و نهادهای اجرایی و شاخص‌های سنجش پیشرفت است. هماهنگی نهادی و مشارکت دستگاه‌های مرتبط در این مرحله اهمیت دارد.

**گام سوم: اجرا و نهادینه‌سازی**: در این گام، اقدامات برنامه‌ریزی‌شده در سطح ملی و مرحله‌بندی‌شده اجرا می‌گردد. اجرای پایلوت‌ها در حوزه‌هایی مانند فیلترینگ هوشمند، سامانه‌های رمزنگاری بومی و احراز هویت دیجیتال پیشنهاد می‌شود. همچنین، استفاده از ظرفیت شرکت‌های دانش‌بنیان و مراکز علمی کشور در طراحی و توسعه زیرساخت‌های بومی تقویت می‌گردد.

**گام چهارم: ارزیابی و بهبود مستمر**: اجرای هر راهبرد به‌صورت دوره‌ای مورد ارزیابی قرار می‌گیرد و پیشرفت آن با استفاده از شاخص‌های عملکرد سنجیده می‌شود. این ارزیابی توسط نهادی ناظر و مستقل صورت گرفته و بازخوردها برای اصلاح و ارتقاء مستمر راهبردها به کار گرفته می‌شود. شفاف‌سازی عملکرد برای افزایش اعتماد عمومی نیز در این مرحله اهمیت دارد.

## ۴. نتیجه‌گیری و پیشنهاد

براساس نتایج حاصل از رتبه‌بندی راهبردها، از دیدگاه پاسخ‌دهندگان، استقلال و تاب‌آوری شَما، در بحران‌های مجازی بالاترین امتیاز را دارد این مسئله لزوم تسریع در راه‌اندازی این شبکه البته به‌صورت واقعی (و نه نمایشی) را نشان می‌دهد. چراکه این شبکه با تغییر دولت‌ها، همواره در معرض رویکردهای متفاوت قرار گرفته و علیرغم صرف هزینه‌های زیاد، کارایی مورد انتظار و الزامات وضع‌شده برای آن محقق نشده است.

میزان درک مشترک، نگرش، اراده و انگیزه سیاست‌گذاران و نهادهای حاکمیتی، در مواجهه با چالش‌های فضای سایبر مانند حریم خصوصی، خلأهای قانونی، مسائل فرهنگی، سواد دیجیتال و اقتصاد مجازی، تأثیر زیادی در اولویت‌بخشی به راه‌اندازی و امنیت این شبکه دارد. این مسئله خواسته جدی مقام معظم رهبری نیز هست. معظم له در بند پنجم از حکم انتصاب اعضای دوره دوم شورای عالی فضای مجازی در شهریور ۱۳۹۴ مطالبه «تسریع در راه‌اندازی شَما، پس از تصویب طرح آن در شورای عالی و نظارت مستمر و مؤثر مرکز ملی بر مراحل راه‌اندازی و بهره‌برداری از آن» را به‌طور صریح اعلام فرمودند. همچنین براساس دکترین مجازی جمهوری اسلامی ایران و اسناد بالادستی و سیاست‌های ابلاغی دستیابی به قدرت مجازی در تراز جهانی، مستلزم فراهم ساختن امکان حاکمیت بر زیرساخت‌های قابل کنترل در فضای سایبر از طریق راه‌اندازی شَما، میسر می‌شود (هلیلی و همکاران، ۱۳۹۷).

در این تحقیق، راهبردهای اهمیت شَما، در کاهش وابستگی به شبکه جهانی اینترنت و کسب آمادگی در برابر تهدید قطع اینترنت، تحریم مجازی و خودسانسوری و به‌کارگیری سامانه‌های ارتباطی و اطلاعاتی امن و بومی به‌منظور مقابله با حملات مجازی هکرها و کشورهای متخاصم به زیرساخت‌های حیاتی و حساس کشور در رتبه‌های دوم و سوم قرارگرفته‌اند.

استقلال شَما و بومی‌سازی تجهیزات و سامانه‌های امنیتی این شبکه، امکان پیشگیری، خنثی‌سازی و مقابله با تهدیدات عینی و ذهنی را فراهم می‌سازد و این مسئله ارتقاء امنیت ملی کشور را در پی خواهد داشت. بااین‌حال، امنیت و استقلال شبکه نباید به معنای ایزوله شدن از جامعه جهانی، خودتحریمی و خودسانسوری در توزیع محتوای داخلی باشد. پیش‌بینی اقدامات جبرانی جهت مواجهه با اعمال محدودیت‌های فناورانه و تحریم‌های مجازی، از نکات مهمی است که در تحقق شَما، باید مدنظر قرار گیرد.

شَما، نقش مهمی در خنثی‌سازی، جاسوسی، افشای اطلاعات و صدمه به زیرساخت‌های حیاتی دارد و درصورتی‌که از سامانه‌های احراز هویت هوشمند در آن استفاده شود می‌تواند

ضمن ارتقای اعتماد کاربران، موجب حفاظت از حریم خصوصی، کاهش جرائم مجازی و رعایت ملاحظات امنیتی توسط کاربران شود. بومی بودن سامانه‌های امنیتی در زیرساخت این شبکه امکان اجرای فیلترینگ هوشمند محتوا (استفاده از فناوری‌هایی مانند یادگیری ماشین و پردازش زبان طبیعی، به‌جای مسدودسازی کلی سایت‌ها و هدف قرار دادن محتوای نامناسب یا مغایر با ارزش‌های فرهنگی و امنیتی)، نظارت و کنترل و مدیریت اطلاعات را در فضای سایبر فراهم می‌سازد.

این شبکه، بستر مناسبی برای افزایش تولید و تبادل محتوای غنی علمی، آموزشی، فرهنگی و دینی است و در صورت تحقق این مهم، ضمن دارا بودن حاکمیت داده، نیازهای مادی و معنوی کاربران در فضای سایبر تأمین می‌شود و این مسئله امنیت ذهنی و روانی جامعه را افزایش می‌دهد. در نهایت، یکی از کلیدی‌ترین عوامل در امنیت پایدار این شبکه، افزایش آگاهی و مهارت کاربران در مواجهه با تهدیدهای مجازی است. این موضوع مستلزم برنامه‌ریزی دقیق، سرمایه‌گذاری در آموزش و گسترش اقدامات آگاه‌سازی هدفمند در سطح ملی است.

با توجه به یافته‌های این پژوهش، راهبردهای احصاء شده می‌توانند مبنای تحقیقات تکمیلی و سیاست‌گذاری‌های هدفمند در حوزه امنیت شَما، قرار گیرند. در این راستا، پیشنهادات پژوهشی و اجرایی این تحقیق به‌صورت زیر ارائه می‌شود:

پیشنهادهای پژوهشی: هر یک از راهبردهای نه‌گانه احصاءشده می‌توانند به‌صورت تخصصی از جنبه‌های اجرایی، فنی، اقتصادی، حقوقی و اجتماعی مورد تحلیل قرار گیرند. پژوهش‌های آینده می‌توانند با استفاده از روش‌های مدل‌سازی سناریو، مسیرهای مختلف تحقق شَما را شبیه‌سازی و ارزیابی کنند. همچنین، مطالعه تطبیقی اقدامات سایر کشورها می‌تواند به استخراج تجارب موفق بین‌المللی در توسعه شبکه‌های ملی اطلاعات کمک کند. علاوه بر این، تحلیل نگرش‌ها، اعتماد و آمادگی کاربران و جامعه نسبت به شَما از منظر روان‌شناختی و فرهنگی می‌تواند در کاهش شکاف بین سیاست‌گذاران و جامعه مؤثر باشد.

پیشنهادهای اجرایی: شورای عالی فضای مجازی به‌عنوان نهاد عالی سیاست‌گذاری فضای سایبر، باید نقشه راهی مدون برای ارتقاء امنیت شَما تدوین کند که شامل زمان‌بندی، تقسیم وظایف و شاخص‌های عملیاتی باشد. سازمان‌های مسئول باید زمینه مشارکت فعال شرکت‌های دانش‌بنیان داخلی را در توسعه تجهیزات بومی، فناوری‌های رمزنگاری و سامانه‌های احراز هویت فراهم کنند. همچنین، باید توازن لازم بین امنیت شبکه و جریان آزاد اطلاعات حفظ شود تا اعتماد عمومی تقویت گردد. طراحی سازوکارهای پایش مستمر و ارزیابی دوره‌ای اثربخشی اقدامات و دریافت بازخورد منظم از کاربران و ذی‌نفعان نیز بخشی از فرآیند اجرایی باشد.

## فهرست منابع


- امام خامنه‌ای، پایگاه اطلاع‌رسانی دفتر حفظ و نشر آثار امام خامنه‌ای مدظله‌العالی به آدرس: www.khamenei.ir
- جمعی از پژوهشگران (۱۳۹۱). ***پروژه تحقیقاتی با عنوان: بازنگری مفاهیم شبکه ملی اطلاعات***. مرکز تحقیقات مخابرات ایران. تهران.
- حسن بیگی، ابراهیم (۱۳۹۰). ***مدیریت راهبردی***. انتشارات سازمان مطالعه و تدوین کتب علوم انسانی (سمت)، تهران.
- رحمانی، علیرضا؛ احمدی، علیرضا؛ کاظمی، محسن؛ آقایی، محسن (۱۳۹۹). ***شناسایی و رتبه‌بندی عوامل مؤثر بر شبکه ملی امن اطلاعات جمهوری اسلامی ایران***. امنیت ملی. ۱۰ (۳۸)
- شانیان، علی؛ سعدی نژاد، سهیل؛ داداش زاده، محمد (۱۳۸۳). ***کاربرد تکنیک‌های تصمیم‌گیری چند معیارها در انتخاب راهبرد مناسب جهت اجرای پروژه فناوری اطلاعات***. نشریه مدیریت ساز. شماره ۱۵. صص ۱۰۲ تا ۱۱۶
- عبیری، داود؛ یزدانی، رحیم؛ هلیلی، خداداد؛ ثقفی، کامیار (۱۳۹۹). ***تبیین نقش شبکه ملی اطلاعات در مدیریت فرصت‌ها و تهدیدهای فضای مجازی کشور***. امنیت ملی. ۱۰ (۳۷).
- قهرمانی، علی؛ مسلمی، نوشین (۱۴۰۲). ***نقش شبکه ملی اطلاعات در مواجهه با جنگ شناختی- رسانه‌ای از منظر اندیشه دفاعی امام خامنه‌ای***. مدیریت دانش اسلامی. ۵(۹).
- محمدی خانقاهی، محسن؛ رضایی، صفیه (۱۳۹۸). ***آسیب‌شناسی مدیریت فضای مجازی در جمهوری اسلامی ایران با تأکید بر شبکه ملی اطلاعات***. مطالعات اسلامی آسیب‌های اجتماعی. ۱ (۱).
- مرتضوی شاهرودی، محمدعلی (۱۴۰۲). ***جایگاه شبکه ملی اطلاعات در ایران براساس حقوق بین‌المللی ارتباطات***. دومین کنفرانس ملی فضای سایبر. دانشگاه تهران.
- ملکی، عباس؛ قادری، سیدرضا؛ صفرنژاد، حسین (۱۴۰۲). ***نقش رسانه ملی در ارتقای احساس امنیت نظامی جمهوری اسلامی ایران***. فصلنامه راهبرد دفاعی ، ۲۱ (۸۴).
- مؤمنی، منصور (۱۳۸۵). ***مباحث نوین تحقیق در عملیات***. دانشگاه تهران.

- 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 (۱۳۹۸). ***ارائه الگویی برای تقویت اثرات اقتصادی شبکه ملی اطلاعات***. پژوهش‌نامه پردازش و مدیریت اطلاعات. ۳۳ (۱).
- نصرت‌آبادی، جمشید؛ مؤمنه، محسن؛ یاقوت پور، محمدحسین؛ مهدی نژاد نوری، محمد (۱۳۹۸). ***ارائه الگوی راهبردی ارزیابی شبکه ملی اطلاعات***. امنیت ملی. ۹(۳۳).
- نصری، قدیر (۱۳۹۲). ***امنیت جامعه‌ای به‌مثابه هسته حیاتی امنیت ملی پایدار***. فصلنامه امنیت پژوهی، سال دوازدهم شماره ۴۳
- هاشمی، محمدساجد؛ همایون محمدهادی (۱۳۹۶). ***جایگاه شبکه ملی اطلاعات در سپهر سیاست فرهنگی جمهوری اسلامی ایران***. مطالعات راهبردی سیاست‌گذاری عمومی. ۷ (۲۳).
- همایون، محمدهادی؛ هاشمی، محمدساجد (۱۳۹۶). ***بازنمایی شبکه ملی اطلاعات در رسانه‌های برون‌مرزی***. مطالعات رسانه‌های نوین. ۳ (۹).
- هلیلی، خداداد؛ عبیری، داوود؛ ولوی، محمدرضا (۱۳۹۳). ***نقش و جایگاه شبکه ملی اطلاعات در امنیت سامانه‌های C4I***، هشتمین کنفرانس ملی فرماندهی و کنترل ایران
- هلیلی، خداداد؛ ولوی، محمدرضا؛ موحدی صفت، محمدرضا (۱۳۹۷). ***شناسایی عوامل و مؤلفه‌های اثرگذار بر تدوین رهنامه قدرت مجازی ج.ا.ایران مبتنی بر سیاست‌های ابلاغی و اسناد بالادستی***. فصلنامه راهبرد دفاعی ، ۱۶ (۳).

## References


- 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.