مجله علمی «نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۴، فصل زمستان ۱۴۰۰؛ ص ۱ تا ۱۴

راهبردهای پدافند غیرعامل در حوزه محافظت از زیرساخت رسانه ملی

حسین نوروستا[1*] **ایمان سلطانی**[2]

کارشناسی ارشد مهندسی پدافند غیرعامل دانشگاه صنعتی مالک اشتر، تهران، ایران

همکار پژوهشی دانشگاه عالی دفاع و تحقیقات راهبردی، تهران، ایران

(دریافت۱۴۰۰/۰۴/۰۵، پذیرش:۱۴۰۰/۱۱/۰۹)

چکیده

سرمایه‌های رسانه‌ای علاوه بر عناصر نرم‌افزاری و سخت‌افزاری، شامل سرمایه‌ها و دارائی‌های فیزیکی و زیرساختی هستند. براین‌اساس به‌منظور مقابله با تهدیدات بر علیه این سرمایه ها و کاهش آسیب پذیری، نیاز به تدوین راهبردهای حفاظت از این زیرساخت‌ها با رویکرد دفاع غیرعامل است که در این پژوهش به‌عنوان هدف اصلی مطرح شده است. پژوهش حاضر از نوع توصیفی - تحلیلی و جمع‌آوری اطلاعات از طریق روش‌های اینترنتی، کتابخانه‌ای و میدانی و روش اصلی تحلیل اطلاعات گردآوری شده، روش SWOT می‌باشد و همچنین به‌منظور سنجش پرسش‌نامه‌ها از ضریب آلفای کرونباخ و آزمون‌های آماری بهره برده شده است. در این پژوهش پس از بررسی اسناد بالادستی و اخذ نظرات خبرگان، ۹۲ عامل محیطی مؤثر در محافظت از این زیرساخت شناسایی و در نرم افزار SPSS مورد ارزیابی قرار گرفته است. سپس ۲۱ راهبرد بر اساس مدل تدوین راهبرد دانشگاه عالی دفاع ملی تدوین گردید. از راهبردهای اولویت‌دار طبق نظر خبرگان می‌توان به برنامه‌ریزی جهت افزایش توان بازدارنده در تهدیدات سایبری، توسعه علمی، پژوهشی و آموزشی نیروی انسانی موردنیاز با استفاده از ظرفیت‌های موجود در کشور به‌منظور افزایش دانش تخصصی مرتبط، مصون‌سازی، استحکام‌بخشی زیرساخت‌های رسانه ملی در برابر تهدیدات سخت با استفاده از متخصصان داخلی، افزایش حمایت‌های مادی و معنوی از شرکت‌های دانش‌بنیان فعال در زمینه طرح‌های توسعه‌ای در حوزه ماهواره‌ای مرتبط با رسانه ملی، بومی‌سازی و به‌کارگیری دانش هوش مصنوعی به‌منظور ایجاد نظام رصد و پایش و هشدار حملات سایبری و کمک به مصون‌سازی زیرساخت رسانه ملی در برابر تهدیدات، خرید و مهندسی معکوس نمونه‌هایی از سامانه‌های نرم‌افزاری پیشرفته در حوزه رسانه ملی اشاره کرد.

کلیدواژه‌ها: پدافند غیرعامل، دارایی، رسانه ملی، امنیت ملی، SWOT.

Passive defense strategies in the field of national media infrastructure protection

H, Norousta
Master of Passive Defense Engineering Malek Ashtar University of Technology, Tehran, Iran

I, Soltani
Research Fellow, University of Defense and Strategic Research.Tehran. Iran

(Received: 2021/June/26; Accepted:2022/January/29)

Abstract

In addition to software and hardware components, media assets include physical and infrastructure assets and assets. Therefore, in order to deal with threats against these assets and reduce vulnerability, it is necessary to develop strategies to protect these infrastructures with a passive defense approach, which has been proposed as the main goal in this study. The present study is descriptive-analytical and data collection through Internet, library and field methods and the main method of data analysis is SWOT method and also Cronbach's alpha coefficient and statistical tests have been used to measure the questionnaires. In this study, after reviewing upstream documents and obtaining expert opinions, 92 environmental factors affecting the protection of this infrastructure have been identified and evaluated in SPSS software. Then 21 strategies were developed based on the strategy formulation model of the Higher National Defense University. According to experts, one of the priority strategies can be planned to increase the deterrent capability in cyber threats, scientific, research and training development of the required manpower using the existing capacities in the country to increase relevant specialized knowledge, hedge, strengthen national media infrastructure against severe threats. Using local experts, increasing material and moral support of knowledge-based companies active in the field of development projects in the field of satellites related to national media, localization and application of artificial intelligence knowledge to establish a monitoring system and cyber attacks and help protect national media infrastructure in Against threats, purchasing and reverse engineering, he cited examples of advanced software systems in the field of national media.

Keywords: Passive Defense, Asset, National Media, National Security, SWOT.

Corresponding Author E-mail: hossein.norosta@yahoo.com

۱. مقدمه

حضرت امام خامنه‌ای (دامت‌برکاته) در دیدار با رئیس‌جمهوری و اعضای هیات دولت در تاریخ ۱۳۹۱/۰۶/۰۲ فرموده‌اند: "رسانه‌ها خیلی نقش دارند در این‌که وحدت ایجاد کنند یا اختلاف ایجاد کنند. امروز با گسترش مراکز و پایگاه‌های اطلاع‌رسانی و خبری و اینترنتی، حرف از هر زبانی، از هر حنجره‌ای در بیاید، به گوش همه می‌رسد". در کنار توسعه رسانه‌های سمعی و بصری، حفاظت از زیرساخت‌های رسانه‌ای اهمیت زیادی دارد. فضای رسانه‌ای کشور، باید به‌صورت مداوم مورد رصد و پایش قرار گرفته و هرگونه تهدید، آسیب‌پذیری، مخاطره، تهاجم و حادثه سایبری و پیامد اعم از سایبری، فیزیکی و روانی، مورد شناسایی قرار گرفته و اقدام‌های مقابله‌ای برای کاهش و رفع آنها انجام پذیرد [۱]. از طرف دیگر، نقش و اهمیت حوزه‌های فنی و زیرساختی برای پیشبرد مأموریت‌های رسانه در تمامی سطوح، واضح و بدیهی است. در واقع، شرط لازم برای استقرار هر رسانه‌ای اعم از خصوصی یا عمومی تأمین زیرساخت‌های فنی است. بدون فناوری و زیرساخت مناسب، هیچ پیام و محتوایی قابلیت تولید، توزیع و انتشار نخواهد داشت و این مهم در مورد سازمان صداوسیما به دلیل تأمین زیرساخت‌های تحقق حوزهٔ پیام و مسئولیت یکتا و منحصربه‌فرد انتقال و انتشار که مطابق قانون اساسی کشور تنها در اختیار سازمان صداوسیما می‌باشد از اهمیت ویژه‌ای برخوردار است؛ بنابراین می‌توان گفت؛ تحقق و تجلیِ مفاهیم رسانه خدمت عمومی در سازمان‌های رسانه‌ای همچون سازمان صداوسیما تنها مبتنی بر حوزه‌های پیام و محتوایی نبوده و یکی از مهم‌ترین شروط لازم در این زمینه، توجه و تأکید بر ابعاد فنی و زیرساختی است [۲]. زیرساخت‌ها، سیستم‌های حساس و حیاتی کشور نیز هرکدام به نحوی با این فضا ارتباط دارند و بخش قابل‌توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و قسمت قابل‌توجهی از درآمدهای مادی و معنوی شهروندان نیز از این حوزه به دست می‌آید و یا تأثیر می‌پذیرد. به همین علت هرگونه بی‌ثباتی، ناامنی و چالش در این فضا می‌تواند بر روی بخش‌های مختلف جامعه اثرگذار و زندگی شهروندان را تحت‌تأثیر قرار دهد همچنین اقتصاد پایدار و توسعه جوامع، بدون برنامه‌ریزی راهبردی برای حفاظت و تأمین امنیت زیرساخت‌های حیاتی امکان‌پذیر نیست. زیرساخت‌های برق، گاز، آب و فاضلاب، نفت و پتروشیمی، ارتباطات و مخابرات، حمل‌ونقل، بانکداری و خدمات مالی، کشاورزی و تغذیه، سلامت و بهداشت عمومی و خدمات اضطراری از جمله زیرساخت‌های حیاتی هستند که نقش کلیدی در توسعه و پایداری جوامع امروز دارند. در سال‌های اخیر، به‌واسطه صدمات ناشی از تشدید حملات عامدانه، فجایع طبیعی و حوادث شدید آب‌وهوایی، مسئله حفاظت از زیرساخت‌های حیاتی اهمیتی دوچندان یافته است [۳].

اهمیت و ضرورت پژوهش حاضر در این می‌باشد که به‌منظور رسیدن به افزایش توان بازدارنده، کاهش آسیب‌پذیری، تداوم فعالیت‌های حیاتی در بحران‌ها و در برابر تهدیدات مختلف، تدوین راهبردهای پدافند غیرعامل در حوزه زیرساخت رسانه ملی در برابر تهدیدات به‌صورت متمرکز و در جهت رسیدن به اهداف عالی پدافند غیرعامل به علت وجود تهدیدات گسترده و متنوع از سوی دشمنان نظام اسلامی ایران ضرورت می‌یابد که با انجام این پژوهش، راهبردهای تخصصی در جهت محافظت از این زیرساخت‌ها استخراج خواهد شد. ازاین‌رو شناخت تهدیدات محتمل علیه رسانه ملی و قابلیت محافظت از آنان ناشی از تهدیدات متصور بر بخش‌های مختلف زیرساختی اهمیت و ضرورت می‌یابد، چراکه در صورت عدم پرداختن به این موضوع باعث باقی‌ماندن نقاط ضعف شده و از رغبت دشمن در تهاجم به آن کاسته نمی‌شود. با درنظرگرفتن مطالب فوق و باتوجه‌به سیاست‌های بین المللی جمهوری اسلامی ایران و حساسیت زیرساخت رسانه ملی که هدف آماج تهدیدات از سوی دشمنان قسم‌خورده انقلاب اسلامی است، هدف از انجام این پژوهش شناسایی و ارزیابی راهبردهایی از جنس پدافند غیرعامل در حوزه محافظت از زیرساخت‌های رسانه ملی می‌باشد.

پیشینه شناسی

- غلامرضا جلالی فراهانی و سعید علوی وفا در مقاله‌ای با عنوان طراحی و تدوین ارکان جهت‌ساز پدافند غیرعامل در رسانه ملی با کنکاش در مفاهیم پدافند غیرعامل و رسانه ملی، با بررسی تهدیدات و تهاجمات به رسانه ملی به تحلیل ابعاد ارکان جهت‌ساز پدافند غیرعامل رسانه ملی پرداخته است که در نهایت منجر به شناسایی ارزش‌های کلان ۴ گانه و اصول اساسی ۱۴ گانه پدافند غیرعامل رسانه ملی شناسایی شده و براین‌اساس چارچوب کلی ارکان جهت‌ساز پدافند غیرعامل در رسانه ملّی واکاوی و تدوین گردیده است [۴].
- آقایان عبدالعلی پورشاسب و احمدعلی نظری نژاد با پژوهشی با عنوان تدابیر و راهکارهای پدافند غیرعامل در حفاظت از زیرساخت‌های حیاتی جمهوری اسلامی ایران اقدام به ارائه تدابیر و راهکارهای پدافند غیرعامل در موضوع

ذکر شده نموده‌اند که در نتیجه این تحقیق ۶ زیرساخت حیاتی کشور با اولویت زیرساخت‌های حکومتی و زیرساخت‌ها اطلاع‌رسانی شناسایی و معرفی گردیده است و همچنین ۷ تهدید فراروی زیرساخت‌های حیاتی جمهوری اسلامی ایران با اولویت حملات هدفمند موشکی و ۹ راهکار اجرایی پدافند غیرعامل جهت حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات مرتبط ارائه گردیده است [۵].

- آقایان میر یوسفی و غفار پور در پژوهشی تحت عنوان راهبردهای نوین حفاظت از زیرساخت‌های حیاتی با بررسی و تحلیل راهبردهای اتخاذ شده در سطوح ملی، در راستای اهداف کمک به ایجاد درک بهتر تهدیدات و چالش‌های پیش‌روی سامانه‌های زیرساختی، لزوم تغییر نگرش نسبت به مفاهیم و راهبردهای نوین حفاظت از زیرساخت‌های حیاتی، بیان الزامات اولیه برای توسعه چارچوب‌ها و همچنین برنامه‌ریزی راهبردی تأمین امنیت زیرساخت‌های حیاتی تلاش کرده است. در این راستا، پس از بیان لزوم تغییر نگرش نسبت به مفهوم حفاظت زیرساخت‌های حیاتی به‌عنوان یکی از مهم‌ترین اهداف این تحقیق از بخش‌هایی مطالعات تطبیقی دررابطه‌با راهبردهای ملی حفاظت از زیرساخت‌های حیاتی از منظر دستورالعمل‌ها، راهبردها و سیاست‌های راهبردی برخی کشورها به‌صورت هدفمند طرح شد. در نهایت، الزامات اولیه دررابطه‌با راهبرد ملی حفاظت از زیرساخت‌های حیاتی، با شناسایی و تحلیل نقاط تمرکز، اولویت‌ها و چالش‌های راهبردی در این حوزه با رویکردی آینده‌پژوهانه ارائه شده است [۶].
- همچنین آقایان قدیر نظامی و عباس مهری در سال ۱۳۸۷ مقاله با عنوان نقش پدافند غیرعامل در امنیت کشور تدوین نموده‌اند که در آن پدافند غیرعامل و عوامل و مؤلفه‌های امنیت کشور مورد واکاوی قرار گرفته است و تأثیر متغیرهای مقاوم‌سازی و استحکامات، مکان‌یابی، استتار، فریب، ایجاد سامانه‌های هشداردهنده و تحرک و جابه‌جایی بر امنیت کشور به اثبات رسید و تأثیر متغیرهای پوشش، تفرقه و پراکندگی بر امنیت کشور معنی‌دار نبود و در انتها ضمن دسته‌بندی و اولویت‌بندی کردن آن اهمیت مؤلفه‌های تشکیل‌دهنده پدافند غیرعامل و امنیت تبیین و پیشنهادهای لازم به مسئولان کشور ارائه گردیده است [۷].
- آقایان واعظی نژاد و مقدس (۱۳۹۴)، در مقاله‌ای با موضوع راهبردهای امن‌سازی زیرساخت‌های حیاتی کشور در حوزه فناوری اطلاعات، با اشاره به مبانی زیرساخت‌های تأمین امنیت آن با مطالعه و بررسی کشور آمریکا، کشورهای عضو اتحادیه اروپا و راهبردهای حفاظت از زیرساخت‌های حیاتی کشور، انجام برخی اقدامات نظیر ارائه راهکارهای مدیریتی، سازمانی و فنی به جهت به‌حداقل‌رساندن آسیب‌پذیری‌های زیرساخت‌های فناوری اطلاعات پرداخته است [۸].
- آقای قدسی (۱۳۹۲)، در مقاله‌ای با عنوان تأثیر زیرساخت فضای تبادل اطلاعات بر امنیت جمهوری اسلامی ایران و ارائه راهبرد، به بررسی ابعاد اثرگذار این فضا پرداخته است و آسیب‌پذیری امنیت ملی کشور در برابر کارکردهای سیاسی فضای تبادل اطلاعات اولویت نخست قرار گرفته است. در پایان نیز در میان راهبردهای ارائه شده، تأسیس مرکز سیاست‌گذاری به‌منظور مدیریت یکپارچه بهره‌گیری از ظرفیت‌های جامعه و تقویت سرمایه اجتماعی در اولویت این راهبردها قرار گرفته است[۹].

۳- مفهوم‌شناسی

پدافند غیرعامل

عبارت است از مجموعه اقدامات غیر مسلحانه‌ای که باعث افزایش قدرت بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی می‌گردد[۱۰].

رسانه ملی

از منظر امام خمینی (رضوان‌الله تعالی علیه) سازمان صداوسیما (رسانه ملی) یک دانشگاه عمومی است (جلد ۵، صفحه ۲). این تعریف به‌تمامی کارکردهای سیاسی، اقتصادی، اجتماعی، فرهنگی و غیره قابل تعمیم است. از منظر امام خامنه‌ای (دامت‌برکاته) نیز صداوسیما متولی مدیریت افکارعمومی است (۱۳۷۵/۵/۹). در افق چشم‌انداز ۱۴۰۴ صداوسیمای جمهوری اسلامی ایران، رسانه ملی، سازمان رسانه‌ای اطلاق می‌شود که خود را متعلق به عموم مردم سرزمین و منطقه خود بداند و آگاهانه و برنامه‌ریزی‌شده، تأمین منافع، مصالح، امنیت، آرمان‌ها و ارزش‌های مشترک آحاد مردم را مبنای تصمیم‌گیری، موضع‌گیری، تولید، تأمین، پخش، توزیع و ارائه خدمات خود قرار دهد[۱۱].

آسیب‌پذیری

در حوزۀ مسائل مهندسی، آسیب‌پذیری، قابلیت میزان خسارتی است که در اثر در معرض قرارگیری در مقابل یک یا مجموعه‌ای از عوامل ایجاد خطر، سنجیده می‌شود. در واقع، آسیب‌پذیری

عبارت است از احتمال ایجاد خطر یا حمله موفقیت‌آمیز به یک جزء یا به‌عبارت‌دیگر کمیت مقاومت در مواجهه با یک تهدید که بین صفر تا صددرصد تغییر می‌کند[۱۲]. علاوه بر این، به عقیده تیمرمن، آسیب‌پذیری عبارت است از درجه‌ای که سیستم در شرایط خطرناک پس از وقوع حادثه، فعالیت اصلی خود را انجام ندهد. تیمرمن همچنین آسیب‌پذیری را به برگشت‌پذیری مرتبط و عنوان می‌کند که برگشت‌پذیری، ظرفیت سیستم به‌منظور جذب و بازآوری خود پس از رخداد یک سانحه خطرناک است[۱۳].

زیرساخت

زیرساخت‌های شامل سامانه‌هایی است که منابع وابسته به تمام عملکردهای جامعه را مهیا می‌سازند[۱۴]. شامل دارایی‌ها، سیستم‌ها و شبکه‌های فیزیکی یا مجازی هستند که تخریب یا ازمیان‌رفتن آن‌ها تأثیر ناتوان‌کننده‌ای بر امنیت کشور، تداوم فعالیت‌ها و یا هر ترکیبی از این عوامل داشته باشد[۱۵]. همچنین با ارائه کردن خدماتی که برای عملکرد جامعه ضروری هستند، ستون فقرات جامعه را تشکیل می‌دهند[۱۶].

امنیت ملی

در لغت حالت فراغت از هرگونه تهدید یا حمله و یا آمادگی برای رویارویی با هر تهدید و حمله را گویند. در اصطلاح سیاسی و حقوقی به‌صورت امنیت فردی، امنیت اجتماعی، امنیت ملی و بین‌المللی به کار برده می‌شود، یا ایجاد وضعیتی است که در آن منافع و ارزش‌های حیاتی کشور مورد تهدید جدی نباشد یا حالتی است که ملتی فارغ از تهدید ازدست‌دادن تمام یا بخشی از جمعیت دارایی یا خاک خود به سر برد[۱۷]. در جدول شماره ۱ ابعاد اقدامات ضد امنیت ملی آورده شده است.

جدول (۱). ابعاد اقدامات ضد امنیت ملی در رسانه‌های بیگانه[۱۸]

فرهنگی	تهاجم به اعتقادات
	ترویج الگوهای غلط
سیاسی و اجتماعی	شبهه سازی ضد نظام
	ترویج ناکارآمدی نظام و مسئولان کشور
	شبهه‌آفرینی سیاسی
	ایجاد رسانه‌های فارسی‌زبان معاند
رسانه	فضاسازی منفی ضد رسانه ملی
	ترویج شبکه‌های اجتماعی دگراندیشی

۴. روش تحقیق

پژوهش حاضر از نوع پژوهش توصیفی - تحلیلی می‌باشد که باتوجه‌به ماهیت آن، جمع‌آوری اطلاعات، اسناد بالادستی و مدارک

موردنیاز از طریق روش‌های اینترنتی، کتابخانه‌ای و میدانی می‌باشد. روش اصلی تحلیل داده‌های گردآوری شده، روش SWOT و به‌منظور سنجش پرسش‌نامه‌ها از ضریب آلفای کرونباخ و آزمون‌های آماری بهره برده شده است. به این منظور پرسش‌نامه اول برای اولویت‌بندی ۹۲ عامل محیطی اثرگذار (جداول شماره ۲ و ۳) توسط ۴۲ نفر از خبرگان پدافند غیرعامل تکمیل و پرسش‌نامه دوم با ۲۱ راهبرد توسط ۲۳ نفر از خبرگان در حوزه پدافند غیرعامل و رسانه و امنیت اطلاعات تکمیل شده است.

۵. نتایج و بحث

پس از بررسی عوامل محیطی بر اساس مطالعات میدانی، کتابخانه‌ای، مستندات موجود و درنظرگرفتن وضعیت فعلی کشور پرسش‌نامه اول طراحی و توزیع گردید. در این پرسش‌نامه از روش امتیازدهی طیف لیکرت استفاده شده است.

جدول (۲). ارزیابی محیط داخلی

ردیف	قوت‌ها	میانگین	اولویت	وزن	رتبه	امتیاز
S1	وجود متخصصین با توان علمی بالا در صنعت فاوا کشور	۴,۲۹	۳	۰,۰۲۲۸	۴	۰,۰۹۱۲
S2	همکاری و انگیزه دفاعی بالای نیروهای مسلح کشور	۴,۲۴	۵	۰,۰۲۲۶	۴	۰,۰۹۰۲
S3	امکان بهره‌گیری از تجربیات ارزشمند دفاع مقدس و سایر منازعات منطقه‌ای و جهانی به‌منظور کاهش آسیب‌پذیری زیرساخت‌ها	۴,۰۷	۹	۰,۰۲۱۷	۳	۰,۰۶۵۰
S4	انگیزه بالای مسئولان کشور نسبت به بومی‌سازی انواع فناوری‌ها در جهت کاهش وابستگی به بیگانگان	۳,۶۷	۱۶	۰,۰۱۹۵	۳	۰,۰۵۸۵
S5	تأکیدات رهبر معظم انقلاب اسلامی نسبت به تولید علم و خودکفایی در حوزه فناوری‌های نوین و عدم وابستگی به بیگانگان	۴,۲۱	۶	۰,۰۲۲۴	۴	۰,۰۸۹۷

S6	حمایت نسبی دولت از کسب‌وکارهای نوپا و استارت‌آپ در حوزه فضای تبادل اطلاعات و معافیت مالیاتی آنها	۳,۷۶	۱۵	۰,۰۲۰۰	۳	۰,۰۶۰۱
S7	وجود مراکز دانشگاهی، شرکت‌های دانش‌بنیان و نیروی جوان تحصیل‌کرده در خصوص ارائه راهکارهای نوین در حوزه فضای تبادل اطلاعات و رسانه ملی	۴,۰۵	۱۰	۰,۰۲۱۵	۳	۰,۰۶۴۶
S8	امکان استفاده از تجهیزات جدید و به‌کارگیری شیوه‌های نوین در مقابله با تهدیدات ضد زیرساخت رسانه ملی	۴	۱۱	۰,۰۲۱۳	۳	۰,۰۶۳۹
S9	دانش، بینش و حساسیت جامعه علمی کشور و قشر تحصیل‌کرده نسبت به حفاظت زیرساخت رسانه ملی	۳,۹۳	۸	۰,۰۲۱۹	۳	۰,۰۸۷۷
S10	انگیزه بالای مسئولان جهت بومی‌سازی فناوری‌های نوین و پیشرفته و حمایت مالی از شرکت‌های دانش‌بنیان به دلیل صرفه‌جویی ارزی	۳,۹۰	۱۳	۰,۰۲۰۸	۳	۰,۰۶۲۳
S11	امکان به‌کارگیری بخشی از اعتبارات صندوق توسعه ملی و صندوق ملی جهت توسعه تحقیقات حفاظت از زیرساخت رسانه ملی	۳,۹۳	۱۲	۰,۰۲۰۹	۳	۰,۰۶۲۷
S12	روحیه ملی و اعتقادی نسبتاً بالای مردم ایران در حمایت از رسانه ملی	۴,۳۱	۲	۰,۰۲۲۹	۴	۰,۰۹۱۷
S13	وجود فرهنگ و روحیه بالای مشارکت و همکاری برای رفع بحران‌ها در کشور	۴,۳۳	۱	۰,۰۲۳۱	۴	۰,۰۹۲۲
S14	توجه اسناد بالادستی کشور به حفاظت از زیرساخت‌های رسانه ملی	۳,۸۸	۱۴	۰,۰۲۰۷	۳	۰,۰۶۲۰
S15	قوانین تصویب شده در کمیسیون تنظیم مقررات ارتباطات در راستای حمایت از شبکه‌های تبادل اطلاعات و ارتباطات داخلی	۴,۲۶	۴	۰,۰۲۲۷	۴	۰,۰۹۰۷
S16	توانایی ایمن‌سازی نسبی مراکز حیاتی و حساس مرتبط با زیرساخت‌ها در مقابل تهدیدات زیست‌محیطی نظیر سیل و زلزله	۴,۱۷	۷	۰,۰۲۲۲	۴	۰,۰۸۸۷
ردیف	ضعف‌ها	میانگین	اولویت	وزن	رتبه	امتیاز
W1	آسیب‌پذیری بالای زیرساخت‌های رسانه ملی در اثر حملات موشکی و هوایی	۴,۱۴	۱۴	۰,۰۲۲۰	۱	۰,۰۲۲۰
W2	ضعف در تدوین برنامه‌هایی به‌منظور افزایش توجه و ارتقای آموزش‌های نیروهای مسلح نسبت به به‌کارگیری و رعایت اصول ایمنی و الزامات مقابله با تهدیدات در حوزه زیرساخت‌های رسانه ملی	۴,۵۰	۲	۰,۰۲۳۹	۲	۰,۰۴۷۹
W3	آسیب‌پذیر بودن زیرساخت‌های فیزیکی رسانه ملی در قبال انواع تهدیدات به دلیل نداشتن سیستم دفاع از خود	۴,۳۱	۵	۰,۰۲۲۹	۱	۰,۰۲۲۹
W4	ضعف در نظام توسعه سیستم‌عامل بومی و شبکه ملی اطلاعات به دلیل مسائل امنیتی	۳,۹۹	۲۰	۰,۰۲۱۲	۱	۰,۰۲۱۲
W5	عدم توجه کافی به نظارت و کنترل نامحسوس تردد افراد به زیرساخت‌های حساس مراکز داده سازمان صداوسیما	۴,۵۲	۱	۰,۰۲۴۱	۲	۰,۰۴۸۲
W6	فقدان برنامه‌ریزی دقیق، مدیریت یکپارچه، اصولی و علمی در راستای مدیریت بحران‌های احتمالی	۴,۱۰	۱۶	۰,۰۲۱۸	۱	۰,۰۲۱۸
W7	ضعف سازوکارهای اجرایی و عملیاتی جهت هماهنگی و همکاری نهادها و سازمان‌های مرتبط و موازی‌کاری سازمان‌ها و نهادهای متولی در حوزه حفاظت از زیرساخت‌های رسانه ملی	۳,۹۹	۲۱	۰,۰۲۱۲	۱	۰,۰۲۱۲
W8	عدم توجه به سرمایه‌گذاری مناسب در جهت آگاه‌سازی و جلب اعتماد مردم (اقناع کاربران) نسبت به شبکه‌های اطلاع‌رسانی داخلی	۴,۲۱	۱۱	۰,۰۲۲۴	۱	۰,۰۲۲۴

W9	نبود اراده جدی در اجرای راهبرد عملیاتی جهت کاهش وابستگی رسانه ملی به ماهواره‌های بیگانه	۴,۳۶	۳	۰,۰۲۳۲	۲	۰,۰۴۶۴
W10	بی‌توجهی به افزایش توانمندی سازمان‌های داخلی در شناسایی فوری اختلالات در زیرساخت‌های رسانه ملی	۴,۲۶	۸	۰,۰۲۲۷	۱	۰,۰۲۲۷
W11	ضعف در توسعه، استقلال و بومی‌سازی شبکه یکپارچه فناوری اطلاعات	۴,۲۹	۷	۰,۰۲۲۸	۱	۰,۰۲۲۸
W12	ضعف دانش بومی در جهت بهینه‌سازی و روزآمدسازی زیرساخت‌ها و فناوری‌های مرتبط با زیرساخت‌های رسانه ملی	۴,۳۳	۴	۰,۰۲۳۱	۲	۰,۰۴۶۱
W13	عدم توجه به رعایت الزامات پدافند غیرعامل در طراحی و ساخت زیرساخت‌های رسانه ملی	۴,۱۹	۱۲	۰,۰۲۲۳	۱	۰,۰۲۲۳
W14	ضعف در برنامه‌ریزی توسعه پردازشگرهای چندمنظوره	۳,۶۰	۲۷	۰,۰۱۹۱	۱	۰,۰۱۹۱
W15	ضعف در تولید تجهیزات اولیه مورداستفاده در مراکز داده (مانند سرورها، ذخیره‌سازها، سوئیچ‌ها و نظایر آن)	۳,۳۳	۲۸	۰,۰۱۷۷	۱	۰,۰۱۷۷
W16	عدم توسعه و روزآمدسازی آزمایشگاه‌ها و تجهیزات وابسته به رسانه ملی در جهت کاهش آسیب‌پذیری در برابر تهدیدات نوین	۳,۹۳	۲۳	۰,۰۲۰۹	۱	۰,۰۲۰۹
W17	ضعف برنامه‌ریزی در جهت افزایش دانش و توانمندی کارشناسان مجری طرح‌های کلان مرتبط با زیرساخت‌های رسانه‌ای	۳,۷۹	۲۶	۰,۰۲۰۱	۱	۰,۰۲۰۱
W18	عدم توجه کافی به حمایت نهادهای پولی و بانکی جهت انجام طرح‌های توسعه‌ای در زمینه فناوری اطلاعات و رسانه ملی	۴,۳۰	۶	۰,۰۲۲۹	۱	۰,۰۲۲۹
W19	ضعف در برنامه‌ریزی به‌منظور ایجاد و جذب سرمایه‌گذاری‌های کافی جهت بوی سازی تکنولوژی‌های نوین	۴,۱۷	۱۳	۰,۰۲۲۲	۱	۰,۰۲۲۲
W20	عدم توجه کافی به نیروهای نخبه و تحصیل‌کرده	۴,۲۵	۹	۰,۰۲۲۷	۱	۰,۰۲۲۷
W21	عدم راه‌اندازی زیرساخت بومی‌سازی شده در کشور	۳,۶۴		۰,۰۱۹۴	۱	۰,۰۱۹۴
W22	مدرک‌گرایی در بسیاری از دانشگاه‌های کشور	۳,۹۵	۲۲	۰,۰۲۱۰	۱	۰,۰۲۱۰
W23	افزایش حجم مهاجرت در میان افراد تحصیل‌کرده	۳,۸۱	۲۵	۰,۰۲۰۳	۱	۰,۰۲۰۳
W24	تمایل برخی متخصصان جوان و اساتید دانشگاهی جهت مهاجرت موقت یا دائمی از کشور	۴,۰۷	۱۷	۰,۰۲۱۷	۱	۰,۰۲۱۷
W25	ضعف قانونی در رسیدگی زودهنگام در بررسی تخلفات سایبر الکترونیک به‌ویژه در قبال زیرساخت‌های ارتباطی	۴,۲۴	۱۰	۰,۰۲۲۶	۱	۰,۰۲۲۶
W26	ضعف قانونی در حوزهٔ فضای تبادل اطلاعات کشور به‌منظور حفظ حریم‌های خصوصی و جلوگیری از خروج اطلاعات کشور	۴,۰۵	۱۸	۰,۰۲۱۵	۱	۰,۰۲۱۵
W27	وجود برخی قوانین ضعیف، دست‌وپاگیر، ناکارآمد یا مخرب در مسیر بومی‌سازی سریع و ارزان‌قیمت محصولات پراهمیت موردنیاز کشور در عرصهٔ زیرساخت‌های رسانه ملی	۴	۱۹	۰,۰۲۱۳	۱	۰,۰۲۱۳
W28	عدم انجام مطالعات زیست‌محیطی و شناسایی نقاط آسیب‌پذیر در مکان‌یابی زیرساخت‌ها	۴,۱۲	۱۵	۰,۰۲۱۹	۱	۰,۰۲۱۹
W29	فقدان طراحی و تولید انواع زیرساخت‌ها متناسب با ویژگی‌های طبیعی و اقلیمی کشور و مأموریت‌های مختلف	۳,۸۶	۲۴	۰,۰۲۰۵	۱	۰,۰۲۰۵
	مجموع			۱	-	۲,۰۱۷

جدول (۳). ارزیابی محیط خارجی

ردیف	فرصت‌ها	میانگین	اولویت	وزن	رتبه	امتیاز
O1	امکان همکاری دفاعی - رسانه‌ای با برخی کشورهای همسو و هم‌پیمان	۴,۳۷	۲	۰,۰۲۳۱	۴	۰,۰۹۲۷
O2	امکان همکاری با کشورهای دوست برای جمع‌آوری اطلاعات موردنیاز در جهت کاهش آسیب‌پذیری رسانه ملی	۴,۰۲	۱۵	۰,۰۲۱۷	۳	۰,۰۶۵۳
O3	امکان تأمین اطلاعات غیرنظامی دشمن از برخی شرکت‌های کامپیوتری غربی	۴,۰۵	۱۴	۰,۰۲۱۸	۳	۰,۰۶۵۶
O4	امکان نفوذ به پایگاه‌های اطلاعاتی مراکز علمی‌پژوهشی رسانه‌ای بیگانه	۴,۲۷	۳	۰,۰۲۳۱	۴	۰,۰۹۲۷
O5	امکان اثرگذاری بر افکارعمومی مردم در محیط دشمن	۳,۹۸	۱۷	۰,۰۲۱۵	۳	۰,۰۶۵۴
O6	امکان داده‌کاوی و تحلیل شبکه‌های اجتماعی به‌منظور پیداکردن افراد کلیدی دشمن و نقاط حساس آنها	۴,۱۷	۱۰	۰,۰۲۲۵	۴	۰,۰۹۰۱
O7	امکان الگوبرداری از کشورهای موفق و پیشرو در حوزه شبکه‌های رسانه‌ای	۳,۷۹	۱۹	۰,۰۲۰۴	۳	۰,۰۶۱۴
O8	امکان استفاده از الگوریتم‌های پردازشی در شبکه‌های اجتماعی کشورهای متخاصم به‌منظور یافتن نقاط ضعف آنها و استفاده در حوزه دیپلماسی و فرهنگی	۴,۱۹	۹	۰,۰۲۲۶	۴	۰,۰۹۰۶
O9	همکاری با کشورهای همسو جهت همکاری‌های فناورانه و ایجاد شبکه‌های اطلاع‌رسانی مشترک	۴	۱۶	۰,۰۲۱۶	۳	۰,۰۶۴۹
O10	امکان استفاده از علم، تجربه و ارتباطات دانشمندان، متخصصان و مهندسان ایرانی مقیم خارج کشور	۳,۹۷	۱۸	۰,۰۲۱۵	۳	۰,۰۶۴۵
O11	امکان حضور در همایش‌ها و کنفرانس‌های بین‌المللی در حوزه‌های رسانه‌ای و فرهنگی	۴,۰۵	۱۴	۰,۰۲۱۸	۳	۰,۰۶۵۶
O12	امکان خرید و مهندسی معکوس نمونه‌هایی از سامانه‌های ماهواره‌ای پیشرفته خارجی در جهت ارتقاء تجربیات داخلی	۴,۲۱	۶	۰,۰۲۲۷	۴	۰,۰۹۱۱
O13	امکان صادرات تکنولوژی‌های و خدمات بومی‌سازی شده به کشورهای همسو باهدف ارزآوری و جذب منابع خارجی	۴,۱۲	۱۲	۰,۰۲۲۲	۴	۰,۰۸۹۱
O14	امکان هدایت سرمایه‌گذاران بین‌المللی جهت سرمایه‌گذاری مشترک در حوزه رسانه ملی	۴,۲۴	۵	۰,۰۲۲۹	۴	۰,۰۹۱۷
O15	وجود انگیزه بالای اسلامی و وطن‌دوستی مسلمانان و ایرانیان مقیم خارج جهت توسعه همکاری‌های علمی‌پژوهشی با جمهوری اسلامی ایران	۴,۳۸	۱	۰,۰۲۳۶	۴	۰,۰۹۴۷
O16	امکان برقراری پیوند اجتماعی با مردم و جلوگیری از اختلافات قومیتی در میان آنها توسط شبکه‌های اطلاع‌رسانی و رسانه‌های خارجی	۴,۰۷	۱۳	۰,۰۲۲۰	۴	۰,۰۸۸۰
O17	امکان استفاده از تجربیات موفق کارآمد بین‌المللی در حوزه‌های قانونی و حقوقی	۴,۱۹	۷	۰,۰۲۲۶	۴	۰,۰۹۰۶
O18	امکان استفاده از تجربیات کشورهای پیشرفته و ساخت زیرساخت‌های فضای تبادل اطلاعات متناسب با ویژگی‌های اقلیمی متفاوت	۴,۱۴	۱۱	۰,۰۲۲۴	۴	۰,۰۸۹۶
O19	امکان دریافت منابع مالی مناسب از معاهده‌های بین‌المللی برای ارتقای زیرساخت‌های رسانه ملی در جهت حفاظت از محیط‌زیست	۴,۲۶	۴	۰,۰۲۳۰	۴	۰,۰۹۲۲
ردیف	تهدیدها	میانگین	اولویت	وزن	رتبه	امتیاز
T1	آسیب‌پذیری بالای زیرساخت‌ها و تخریب آنها براثر حملات تروریستی خرابکارانه از سوی دشمن	۳,۷۹	۱۹	۰,۰۲۰۴	۲	۰,۰۴۰۹
T2	توجه جدی دشمنان به رسانه ملی و به‌روز کردن سیستم‌های نوین و کارآمد	۳,۵۵	۲۱	۰,۰۱۹۱	۱	۰,۰۱۹۱
T3	امکان استفاده دشمن از پهپادهای هوشمند برای جاسوسی از فعالیت‌های توسعه‌ای زیرساخت کشور	۳,۳۱	۲۶	۰,۰۱۷۹	۱	۰,۰۱۷۹

T4	قابلیت استفاده دشمن از تجهیزات جنگی هوشمند بر علیه زیرساخت‌های رسانه ملی	۳,۹۰	۱۱	۰,۰۲۱۱	۲	۰,۰۴۴۲
T5	امکان بهره‌گیری دشمن از سامانه‌های مبتنی بر هوش مصنوعی	۴,۰۵	۴	۰,۰۲۱۸	۲	۰,۰۴۳۷
T6	امکان نفوذ عوامل بیگانه به مراکز حساس رسانه ملی	۴,۲۱	۱	۰,۰۲۲۷	۲	۰,۰۴۴۵
T7	تأسیس شبکه‌های ماهواره‌ای توسط گروه‌های معاند نظام اسلامی	۳,۸۳	۱۴	۰,۰۲۰۷	۱	۰,۰۲۰۷
T8	ناامنی‌های موجود در کشورهای همسایه که باعث نفوذ راحت‌تر نیروهای امنیتی دشمن به داخل کشور می‌شود	۳,۵۲	۲۳	۰,۰۱۹۰	۱	۰,۰۱۹۰
T9	امکان ایجاد دست‌کاری‌های تعمدی تجهیزات مورداستفاده در زیرساخت‌های سایبر الکترونیکی که از خارج از کشور تهیه می‌شوند	۳,۸۱	۱۶	۰,۰۲۰۶	۱	۰,۰۲۰۶
T10	امکان ساخت و توزیع ویروس‌های هوشمند در سامانه‌های نرم‌افزاری رسانه ملی توسط دشمن	۳,۵۴	۲۲	۰,۰۱۹۱	۱	۰,۰۱۹۱
T11	انگیزه گروه‌های معاند جهت انجام اقدامات تخریبی علیه رسانه ملی	۳,۸۶	۱۳	۰,۰۲۰۸	۱	۰,۰۲۰۸
T12	وجود شبکه‌های ماهواره‌ای ضدایرانی و القای ناکارآمدی نظام	۳,۹۴	۹	۰,۰۲۱۳	۲	۰,۰۴۲۷
T13	اعمال تحریم‌های بین‌المللی و در پی آن جلوگیری از دستیابی کشور به همکاری‌های مشاوره‌ای و فنی بین‌المللی	۳,۹۸	۷	۰,۰۲۱۵	۲	۰,۰۴۳۰
T14	امکان بهره‌گیری دشمنان از درز اطلاعات ناشی از ضعف‌ها در زیرساخت‌های رسانه ملی	۳,۷۰	۲۰	۰,۰۲۰۴	۱	۰,۰۲۰۴
T15	تحریم‌های موجود در حوزه فناوری اطلاعات	۴,۰۲	۵	۰,۰۲۱۷	۲	۰,۰۴۳۵
T16	قابلیت ایجاد اختلال در زیرساخت‌های رسانه ملی از طریق حمله در فضای سایبری	۳,۹۳	۱۰	۰,۰۲۱۲	۲	۰,۰۴۲۵
T17	امکان جذب و به‌کارگیری آشکار یا نامحسوس اساتید دانشگاهی توسط دشمن	۴,۱۲	۲	۰,۰۲۲۲	۲	۰,۰۴۴۵
T18	امکان ایجاد عملیات اختلال، فریب و تخریب در فضای تبادل اطلاعات	۳,۳۳	۲۵	۰,۰۱۸۰	۱	۰,۰۱۸۰
T19	سرعت بالای رشد فناوری‌های رسانه‌ای نوین دولت‌های متخاصم	۳,۸۸	۱۲	۰,۰۲۰۹	۱	۰,۰۲۰۹
T20	قابلیت نفوذ و حملهٔ بدافزارهای دشمن به زیرساخت‌های رسانه ملی	۴	۶	۰,۰۲۱۶	۲	۰,۰۴۳۲
T21	افزایش هزینه‌های توسعه زیرساخت‌های شبکه ملی اطلاعات در اثر تحریم‌ها	۴,۱۰	۳	۰,۰۲۲۱	۲	۰,۰۴۴۳
T22	وجود تحریم‌های تجاری	۳,۸۲	۱۵	۰,۰۲۰۷	۱	۰,۰۲۰۷
T23	وجود مشوق‌های خارجی که مانع از بازگشت نخبگان	۳,۲۰	۲۷	۰,۰۱۷۲	۱	۰,۰۱۷۲
T24	قابلیت دشمن در ایجاد جنگ روانی و نبرد نرم از طریق ابزارهای هوشمند، شبکه‌های اجتماعی، و پیداکردن علایق و نقاط ضعف عموم مردم	۳,۱۹	۲۸	۰,۰۲۰۶	۱	۰,۰۲۰۶
T25	قابلیت دشمن در گسترش تهاجم فرهنگی از طریق شبکه‌های ارتباطی و ماهواره‌ای به‌منظور تهدید و تغییر ارزش‌ها و باورهای مردم	۳,۸۱	۱۷	۰,۰۱۸۶	۱	۰,۰۱۸۶
T26	اعمال قانون‌های مختلف جهت تحریم مراکز علمی و پژوهشی	۳,۴۵	۲۴	۰,۰۲۱۶	۱	۰,۰۲۰۶
T27	احتمال نفوذ سازمان‌یافته دشمن به مراکز تصمیم‌گیری و قانون‌گذاری جهت تغییر دادن اولویت‌ها	۳,۸۰	۱۸	۰,۰۲۱۳	۲	۰,۰۴۲۷
T28	امکان استفاده دشمن از ضعف‌های طبیعی و اقلیمی کشور	۳,۹۵	۸	۰,۰۲۱۲	۲	۰,۰۴۲۵
	مجموع			۱	-	۲,۴۰۲

به‌منظور سنجش پایایی پرسش‌نامه از ضریب آلفای کرونباخ استفاده شده است. مقدار این ضریب در واقع میزان سازگاری درون پرسش‌نامه را نشان می‌دهد که برای این پرسش‌نامه ۰,۸۷ می‌باشد. همچنین به‌منظور بررسی وضعیت نرمال بودن متغیرهای تحقیق از آزمون کالموگروف اسمیرنوف استفاده خواهد شد. فرض این آزمون جهت بررسی به‌صورت زیر می‌باشد:

فرض صفر: متغیرهای تحقیق دارای توزیع نرمال می‌باشند.

- فرض مقابل: متغیرهای تحقیق دارای توزیع نرمال نمی‌باشند.

جدول (۴). آزمون کالموگروف اسمیرنوف

نام متغیر	میانگین	آماره Z	سطح معناداری
S	۶۹,۶	۰,۸۶۸	۰,۴۳
W	۱۱۷,۶	۰,۷۴۶	۰,۶۳
O	۷۸,۵	۱,۲۶	۰,۰۸
T	۱۰۶,۳	۰,۹۶۸	۰,۳۱

باتوجه‌به جدول شماره ۴ به دلیل اینکه مقدار سطح معناداری آزمون برای تمامی متغیرهای تحقیق بیشتر از ۰,۰۵ می‌باشد، بنابراین در سطح معناداری ۹۵ درصد می‌توان گفت تمامی متغیرهای تحقیق از توزیع نرمال پیروی می‌کنند. در این صورت باید از آزمون‌های پارامتریک برای بررسی داده‌های تحقیق استفاده کرد. بدین منظور از آزمون آنالیز واریانس استفاده شده است. ابتدا باید همگن بودن واریانس‌ها با آزمون لوین بررسی شود، جدول شماره ۵ نتایج این آزمون پارامتریک را نشان می‌دهد:

جدول (۵). نتایج آزمون لوین

نام متغیر	آماره لوین	سطح معناداری
S	۰,۲۵۹	۰,۸۵۵
W	۲,۳۳	۰,۰۸۹
O	۱,۰۰۸	۰,۴۰
T	۰,۳۲۶	۰,۸۰۶

باتوجه‌به جدول شماره ۵ چون سطح معناداری آزمون لوین برای همه متغیرها بیشتر از ۰,۰۵ شده است بنابراین دلیلی بر ناهمگنی واریانس‌ها وجود ندارد و می‌توان از آزمون آنالیز واریانس استفاده کرد. جدول شماره ۶ نتایج این آزمون را نشان می‌دهد.

جدول (۶). نتایج آنالیز واریانس

نام متغیر		F آماره	سطح معناداری
S	بین گروه‌ها	3.947	.015
W	بین گروه‌ها	3.829	.017
O	بین گروه‌ها	1.767	.170
T	بین گروه‌ها	.224	.879

باتوجه‌به جدول شماره ۶ ملاحظه می‌شود برای دو متغیر اول چون سطح معناداری کمتر از ۰,۰۵ شده است بنابراین اختلاف معناداری بین آنها وجود ندارد. بر اساس تحلیل و بررسی عوامل داخلی و محیط خارجی شناسایی شده، راهبردها بر اساس این ارزیابی عوامل محیطی و با استفاده از جلسه خبرگی احصاء گردیدند. اولویت‌بندی این راهبردها بر اساس QSPM به شرح جدول شماره ۷ می‌باشند:

جدول (۷). اولویت‌بندی راهبردها بر اساس QSPM

اولویت	راهبردها	میانگین
۱	برنامه‌ریزی جهت افزایش توان بازدارنده در تهدیدات سایبری و حملهٔ بدافزارهای دشمن به زیرساخت رسانه‌ای کشور	۴,۰۱
۲	توسعه علمی، پژوهشی و آموزشی نیروی انسانی موردنیاز با استفاده از ظرفیت‌های موجود در کشور به‌منظور افزایش دانش تخصصی مرتبط با رسانه ملی	۳,۹۳
۳	مصون‌سازی، استحکام‌بخشی زیرساخت‌های رسانه ملی در برابر تهدیدات سخت با استفاده از متخصصان داخلی و به‌کارگیری دستورالعمل‌های پدافند غیرعامل	۳,۸۵
۴	افزایش حمایت‌های مادی و معنوی از شرکت‌های دانش‌بنیان و نخبگان فعال در زمینه طرح‌های توسعه‌ای در حوزه ماهواره‌ای مرتبط با رسانه ملی	۳,۸۵
۵	بومی‌سازی و به‌کارگیری دانش هوش مصنوعی به‌منظور ایجاد نظام رصد و پایش و هشدار حملات سایبری و کمک به مصون‌سازی زیرساخت رسانه ملی در برابر تهدیدات	۳,۸۳
۶	خرید و مهندسی معکوس نمونه‌هایی از سامانه‌های نرم‌افزاری پیشرفته در حوزه رسانه ملی	۳,۷۹
۷	برگزاری مانورهای دوره‌ای منظم در زیرساخت رسانه ملی با بهره‌گیری از تجربیات منازعات منطقه‌ای و جهانی به‌منظور حفظ و افزایش آمادگی در برابر تهدیدات	۳,۷۱
۸	استفاده از تجربیات کشورهای پیشرفته جهت افزایش تأثیرگذاری رسانه ملی در بحران‌ها	۳,۷۰

۹	مقابله با درز اطلاعات مرتبط با ضعف‌ها در زیرساخت رسانه ملی	۳,۶۷
۱۰	برنامه‌ریزی جهت مقابله با قابلیت دشمن در ایجاد جنگ روانی و نبرد نرم از طریق ابزارهای هوشمند در شبکه‌های اجتماعی	۳,۶۲
۱۱	افزایش سرمایه‌گذاری جهت بومی‌سازی فناوری‌های نوین مرتبط با زیرساخت‌های رسانه ملی	۳,۶۰
۱۲	برنامه‌ریزی جهت عملیاتی‌سازی الزامات پدافند غیرعامل در جهت مقابله با استفاده دشمن از تجهیزات جنگی هوشمند به‌منظور اجرای عملیات‌های نظامی و حمله به زیرساخت‌های رسانه ملی کشور	۳,۵۷
۱۳	حذف و اصلاح قوانین ضعیف، دست‌وپاگیر، ناکارآمد یا مخرب در مسیر بومی‌سازی سریع و ارزان‌قیمت محصولات پراهمیت موردنیاز رسانه ملی	۳,۵۴
۱۴	کاهش ریسک تهدیدات مراکز حیاتی رسانه ملی به جهت افزایش توان بازدارنده در مقابل تهاجمات دشمن	۳,۵۱
۱۵	برنامه‌ریزی جهت مقابله با داده‌کاوی و تحلیل شبکه‌های اجتماعی توسط دشمن که باهدف پیداکردن افراد کلیدی داخلی و نقاط حساس کشور صورت می‌گیرد	۳,۴۴
۱۶	به‌روزرسانی قوانین آموزشی نظارتی در رسانه‌های کشور به جهت مقابله با تهدیدات نوین دشمن	۳,۴۴
۱۷	همکاری با کشورهای همسو جهت تأمین پراکنده تجهیزات موردنیاز در رسانه ملی به‌منظور کاهش خطر نفوذ از روش تعبیه حفره‌های امنیتی پنهانی	۳,۴۲
۱۸	برنامه‌ریزی و سازماندهی آزمایشگاه‌های تخصصی مرجع به‌منظور ارزیابی خطرات و آسیب‌پذیری‌ها جهت شناسایی فوری اختلالات در زیرساخت‌های رسانه ملی	۳,۴۰
۱۹	برنامه‌ریزی جهت استفاده از علم، تجربه و ارتباطات دانشمندان، متخصصان و مهندسان ایرانی مقیم خارج کشور	۳,۴۰
۲۰	برنامه‌ریزی جهت کاهش وابستگی رسانه ملی به ماهواره‌های بیگانه	۳,۲۹
۲۱	حمایت دولت و صداوسیما از کمک نوآورها به جهت آگاهی‌رسانی به جامعه از پیشرفت‌های کشور	۲,۹۵

به منظور بررسی وضعیت نرمال بودن متغیرهای پژوهش از آزمون کالموگروف اسمیرنوف استفاده شده است. فرض این آزمون جهت بررسی به‌صورت زیر می‌باشد:

- فرض صفر: متغیرهای تحقیق دارای توزیع نرمال می‌باشند.
- فرض مقابل: متغیرهای تحقیق دارای توزیع نرمال نمی‌باشند.

جدول (۸). آزمون کالموگروف اسمیرنوف

نام متغیر	میانگین	آماره Z	سطح معناداری
S	۱۴۰,۲	۰,۴۹۹	۰,۹۶
W	۱۴۰,۲	۰,۶۴۷	۰,۷۹
O	۱۴۰,۰۴	۰,۸۵۲	۰,۴۶
T	۱۴۰	۰,۴۵۴	۰,۹۸

باتوجه‌به جدول شماره ۸ چون مقدار سطح معناداری آزمون برای تمامی متغیرهای تحقیق بیشتر از ۰,۰۵ می‌باشد، بنابراین در سطح معناداری ۹۵ درصد می‌توان گفت تمامی متغیرهای تحقیق از توزیع نرمال پیروی می‌کنند. به این منظور از آزمون‌های پارامتریک برای بررسی داده‌ها استفاده خواهد شد. باتوجه‌به اینکه در این پژوهش هدف بررسی نتایج دو جامعه با هم است بنابراین از آزمون تی استفاده شده است. باتوجه‌به اینکه در این آزمون جوامع در دو حالت همگن بودن واریانس‌ها و عدم همگن بودن واریانس‌ها مورد بررسی قرار می‌گیرند، ابتدا باید با بررسی همگن بودن واریانس‌ها تصمیم گرفت نتایج مربوط به کدام حالت را در نظر گرفت. بدین منظور از آزمون لوین برای بررسی همگن بودن واریانس‌ها استفاده شده است.

جدول (۹). آزمون لوین

نام متغیر	آماره لوین	سطح معناداری
S	۲,۲	۰,۱۵
W	۰,۹۴	۰,۳۴
O	۳,۱	۰,۰۹
T	۰,۲۶	۰,۶۱

باتوجه‌به جدول شماره ۹ ملاحظه می‌شود که برای هر چهار متغیر سطح معناداری از ۰,۰۵ بیشتر شده است که در نتیجه می‌توان نتیجه گرفت واریانس‌ها همگن بوده و در نتایج آزمون T از حالت برابری واریانس‌ها باید استفاده کرد. جدول شماره ۱۰ نتایج این آزمون را نشان می‌دهد:

جدول (۱۰). نتایج آزمون T

نام متغیر	سطح معناداری
S	۰,۲۸
W	۰,۸۷
O	۰,۸۱
T	۰,۳۵

باتوجه‌به نتایج آزمون T ملاحظه می‌شود که برای تمامی

متغیرها مقدار سطح معناداری بیشتر از ۰،۰۵ شده است بنابراین می توان نتیجه گرفت در سطح اطمینان ۹۵ درصد بین دو گروه بررسی شده، به ازای هر چهار متغیر تفاوت معناداری وجود دارد. با بررسی و تحلیل نتایج پرسشنامه‌های دوگانه و همچنین اخذ نظرات خبرگان برای عملیاتی سازی راهبردهای ارائه شده، برنامه‌ریزی در توسعه موارد زیر ضروری می‌باشد.

الف- فناوری های اولویت دار

فناوری‌های مورد نیاز در جهت پایش، توسعه و بومی‌سازی افزارها، سامانه‌ها، تجهیزات لازم در جهت تحقق اهداف و مبانی پدافند غیرعامل در حفاظت از زیرساخت‌های رسانه ملی اعم از:

۱. سایبرالکترونیک
۲. مدیریت بحران
۳. مدیریت سوانح
۴. نانو تکنولوژی
۵. شبیه سازهای مجازی
۶. علوم نوین ارتباط از راه دور
۷. سنجش از راه دور و ... می‌باشند که این فناوری‌ها منظور تجهیز آزمایشگاه‌ها، پیش بینی و تحلیلگر وضعیت، تولید محصولات برای رقابت در بازارهای جهانی و ... مورد استفاده قرار می‌گیرند.

ب- علوم موردنیاز

۱. پدافند غیرعامل
۲. فناوری اطلاعات و ارتباطات
۳. علوم رایانه
۴. علوم رسانه‌ای
۵. مخابرات
۶. مکانیک
۷. معماری و عمران
۸. جغرافیا و Gis
۹. سنجش از راه دور
۱۰. مدیریت بحران و سوانح
۱۱. علوم پایه (فیزیک، ریاضی، شیمی و ....)

پ- نیروی انسانی، آموزش و تربیت و تعالی

۱. سران قوا
۲. هیات دولت
۳. نمایندگان مجلس متخصص و متعهد
۴. اساتید، متخصصان و کارشناسان حوزه دفاع
۵. کارشناسان و خبرگان پدافند غیرعامل
۶. مهندسان و کارشناسان علوم رایانه‌ای
۷. مهندسان فناوری اطلاعات و ارتباطات
۸. اساتید دانشگاه‌ها
۹. مدیران دستگاه‌های اجرایی کشور
۱۰. سرمایه‌گذارن و تولیدکنندگان در صنایع و شرکت‌های دانش بنیان
۱۱. کلیه کارشناسان علوم مرتبط با زیرساخت‌های رسانه ملی
۱۲. نیروی کار انسانی

ت- رهبری و مدیریت

ستاد کل نیروهای مسلح در کنار سازمان پدافند غیرعامل و وزارت‌خانه‌های دفاع و پشتیبانی نیروهای مسلح، اطلاعات، علوم و تحقیقات، ارتباطات و فناوری اطلاعات و خارجه به عنوان رهبری اجرای سیاست‌های نظام در حفاظت از زیرساخت‌های حیاتی کشور و سازمان‌های ذینفع مانند صدا و سیما و وزارت‌خانه‌ها مانند صمت، ارتباطات و فناوری ارتباطات در کنار مجلس شورای اسلامی به عنوان سیاست گذاران اصلی نقش مدیریت سند راهبردی تهیه شده را بر عهده دارد. این وظایف (رهبری و مدیریت) شامل موارد زیر می‌باشد:

۱. توسعه صادرات و واردات برنامه ریزی شده با کشورهای دوست و هم جهت به منظور افزایش سطح حفاظت از زیرساخت‌های مربوطه
۲. تقویت دیپلماسی دفاعی
۳. استفاده از نخبگان ایرانی تحصیل کرده و مقیم در خارج از کشور
۴. بازنگری در قوانین و دستور العمل‌ها و استانداردها مربوطه در زیرساخت‌های حیاتی کشور
۵. افزایش تعامل بین سازمانی در سطح اجرایی
۶. راهبری و هدایت پروژه‌های دانش بنیان و بنیادین و کاربردی در کشور

ث- سخت افزار

اجرای این پژوهش در کنار گستره نظارتی و راهبری حفاظت از زیرساخت رسانه ملی در بعد سازمانی ساختار نوینی در بخش سخت افزاری و نرم افزاری را بهبود و توسعه خواهد بخشید، از جمله سخت افزارها می‌توان به موارد زیر اشاره کرد:

۱. توسعه بانک‌های اطلاعاتی
۲. قطعات، ماژول‌ها و سامانه‌های مبتنی بر الکترونیک و توان پالسی
۳. توسعه تجهیزات شبکه‌های مجازی
۴. توسعه و بروزسازی بستر فیبر نوری مخابراتی و ارتباطی سازمان‌ها و صنایع و ...

۵. اینترنت و شبکه ملی اطلاعات
۶. سامانه‌ها و افزارهای رمز نگار و پنهان کننده
۷. سخت افزارهای بومی
۸. دانشگاه و مراکز آموزش عالی
۹. شرکت‌های دانش بنیان
۱۰. شرکت توسعه شبکه زیرساخت کشور

ج- سازمان دهی و شبکه سازی

به منظور سازماندهی و شبکه سازی، ستاد کل نیروهای مسلح در کنار سازمان پدافند غیرعامل و هیات دولت وظیفه سیاست گذاری اجرایی، راهبری، تحلیل و بررسی شاخص‌ها، به روز رسانی و ایجاد ارتباطات بین دستگاهی لازم اعم از دولتی و خصوصی را برای توسعه فناوری‌ها در حوزه حفاظت از زیرساخت رسانه ملی در چارچوب این سند را بر عهده خواهند داشت.

۱. شبکه کنترل کیفیت سامانه‌های مجازی بومی شده
۲. شبکه نظارت بر فعالیت شرکت‌های دانش بنیان
۳. شبکه نظارت حقوقی
۴. شبکه سیاست گذاری اجرایی در سطح کلان کشور
۵. شبکه جامع آگاهی رسانی به عموم مردم جامعه
۶. شبکه نفوذ به پایگاه‌های علمی و فنآوری دشمن
۷. شبکه نظارت بر توسعه و اجرایی شدن شبکه ملی اطلاعات
۸. شبکه بررسی تهدیدات نوین در حوزه‌های مرتبط با زیرساخت رسانه ملی

چ- الگوها

۱. الگوی هدفمند توسعه برنامه‌های توسعه‌ای در آموزش نیروهای انسانی مورد نیاز در حفاظت از زیرساخت‌ها
۲. مدیریت ریسک پایدار در جهت کاهش ریسک زیرساخت‌های حیاتی در برابر تهدیدات طبیعی و انسانی
۳. توسعه همکاری‌های علمی و پژوهشی منطقه‌ای با کشورهای غیرمتخاصم
۴. توسعه همکاری شرکت‌های خصوصی با سازمان‌ها و نهادهای دولتی و حاکمیتی به منظور دست یابی به علوم نوین
۵. شناسایی و پایش تهدیدات نوین و کمتر شناخته شده
۶. تدوین و تصویب همکاری‌های دو یا چندجانبه بین المللی در حوزه امنیت و ایمنی زیرساخت‌ها
۷. تدوین و تصویب سازوکارها و فرآیندهای عملیاتی در حوزه مقابله با تهدیدات سایبری و الکترومغناطیسی
۸. اقدامات لازم جهت صادرات محصولات بومی
۹. تدوین دستورالعمل‌های مکان یابی در شرایط مختلف سرزمینی
۱۰. تدوین، تصویب و عملیاتی سازی برنامه‌های فرهنگی و اجتماعی حوزه فضای رسانه‌ای
۱۱. بروزرسانی ساختار سلسله مراتبی مبتنی بر دانش روز و اهداف پدافند غیرعامل به منظور تعیین جایگاه جوامع و سازمان‌های علمی و تحقیقاتی در سیاست‌ها و طرح‌های کلان
۱۲. طراحی و اجرای سامانه پایش پیامرسان‌های خارجی

د- چارچوب نهادی

نگاشت نهادی یکی از ابزارهای مطالعه سیستم نوآوری می‌باشد. نگاشت نهادی چارچوبی است که با نمایی ساده و جامع وضعیت موجود سیستم نوآوری را نشان می‌دهد و با بررسی آن می‌توان نقایص موجود در اجزا و روابط میان اجزای سیستم را شناسایی و تحلیل نمود، سپس در جهت اصلاح این موارد برنامه‌ریزی‌های لازم را انجام داد. درواقع این نگاشت طرحی است که در نگاهی جامع همه بازیگران اصلی نظام علم، فناوری و نوآوری، جایگاه، تعاملات رسمی، اهداف، ابزارها و کارکردهای آنها را در سطح ملی نشان می‌دهد[۱۴]

۱) مجلس شورای اسلامی: مجلس و کمیسیون‌های مربوطه آن با سیاست‌گذاری، قانون‌گذاری، تصویب لوایح و پیگیری از بخش‌های اجرایی کشور فعالیت‌های تاثیرگذاری در حوزه‌ی رسانه دارند.
۲) هیئت دولت: با تصویب و تأیید لوایح پیشنهادی به مجلس، تصویب آیین‌نامه‌های دستگاه‌های اجرایی در حوزه‌ی رسانه می‌توان آنرا یکی از بخش‌های تاثیرگذار بشمار آورد.
۳) وزارت اطلاعات: وزارت اطلاعات مسئول خنثی سازی توطئه بیگانگان علیه منافع و منابع ملی کشور می‌باشد. این وزارت با رصد فعالیت بیگانگان در عرصه‌های مختلف نقشی مهم و سرنوشت ساز در عرصه حفاظت از زیرساخت‌ها را برعهده دارد.
۴) وزارت آموزش و پرورش: با توجه به این که افراد دوره طولانی از زندگی خود را در این نهادها می‌گذرانند آموزش روش‌ها، راهکارها و پژوهش در زمینه‌های پیشگیری و بالا بردن ضریب امنیت حرکت در این فضا راهبردی مؤثر در بالا بردن سطح آگاهی‌های عموم جامعه و افراد تحصیل کرده می‌باشد.
۵) وزارت دفاع و پشتیبانی نیروهای مسلح: وزارت دفاع از بدو تشکیل مسئول توسعه صنعت دفاعی کشور و حفاظت از سرمایه‌های داخلی کشور می‌باشد. این وزارت‌خانه با آموزش متخصصان و رصد فعالیت‌های بیگانگان و ... بر حسب وظیفه ذاتی خود نقش اساسی در حفاظت از زیرساخت‌های کشور را دارد.

۶) سازمان صدا و سیما جمهموری اسلامی ایران: این سازمان بر اساس رسالت خود و منویات امام خامنه‌ای و قانون اساسی نقش اطلاع رسانی و آموزش آحاد مردم و خط مقدم مقابله با تهاجم نرم دشمنان قرار دارد را بر عهده دارد.

۷) وزارت علوم و تحقیقات و فناوری: این وزارت نقش آموزش کارشناسان و مهندسان عرصه‌های مختلف را بر عهده دارد. علاوه بر این نقش عمده‌ای در پیشرفت اهداف کلان کشور بر عهده دارد.

۸) مجمع تشخیص مصلحت نظام: این مجمع نقش مشورتی در زمینه تدوین چشم‌اندازها و سیاست‌های کلان کشور برای رهبری ایفا می‌نماید. علاوه بر این، نقش نظارت، ارزیابی و هماهنگی برای اجرا و بررسی پیشرفت سیاست‌ها نیز بر عهده این مجمع است.

۹) سازمان پدافند غیرعامل: حوزه مسئولیتی این سازمان در برابر تهدیدات شامل: تهدیدات نظامی و تهدیدات سایبری ، زیستی (انسان،دام،کشاورزی،مواد غذایی و دارویی، آب، محیط زیست و منابع طبیعی)، پرتوی، شیمیایی و اقتصادی می‌باشد که سیاست‌گذاری، هدایت و برنامه ریزی مقابله با تهدیدات یاد شده در قرارگاه‌های (پدافند سایبری، پدافند زیستی، پدافند پرتوی، پدافند شیمیایی، پدافند اقتصادی و پدافند مردمی) تشکیلاتی سازمان پدافند غیرعامل کشور انجام می پذیرد، قرارگاه‌های یاد شده در سطوح استانی هم تشکیل شده و در حال فعالیت می‌باشند. مقابله با تهدیدات طبیعی (زلزله، سیل، آتشفشان، خشکسالی، سرما و...)که جزء حوادث طبیعی و غیر مترقبه می‌باشند.

۱۰) آحاد مردم جامعه (حال و آیندگان): مردم برای رفع نیازهای اقتصادی، اجتماعی، آموزشی و .. به فضای سایبری و رسانه‌ها احتیاج دارند. در حال حاضر با توجه به استفاده اکثر مردم ایران از فضای تبادل اطلاعات و ارتباطات و افزایش تقاضا، نیازهای آحاد جامعه باید تامین گردد، که طرح، لوایح، قانون و... زیادی برای رفع این دسته از نیازهای مردم تصویب شده است.

۴. نتیجه‌گیری

در این پژوهش پس از بررسی اسناد بالادستی و مبانی نظری و اخذ نظرات خبرگان و کارشناسان فنی، ۱۶ عامل قوت، ۲۹ عامل ضعف، ۱۹ عامل فرصت و ۲۸ عامل تهدید در محافظت از زیرساخت رسانه ملی شناسایی و تعیین گردیدند. سپس با اخذ نظرات خبرگان و تحلیل عوامل محیطی، راهبردهای محافظت از زیرساخت رسانه ملی با رویکرد پدافند غیرعامل تدوین و اولویت‌بندی گردیدند. از راهبردهای اولویت‌دار محافظت از زیرساخت رسانه ملی با رویکرد پدافند غیرعامل طبق نظر جامعه آماری و ارزیابی پرسش‌نامه دوم عبارت است از: " برنامه‌ریزی جهت افزایش توان بازدارنده در تهدیدات سایبری و حملهٔ بدافزارهای دشمن به زیرساخت رسانه‌ای کشور، توسعه علمی، پژوهشی و آموزشی نیروی انسانی موردنیاز با استفاده از ظرفیت‌های موجود در کشور به‌منظور افزایش دانش تخصصی مرتبط با رسانه ملی، مصون‌سازی، استحکام‌بخشی زیرساخت‌های رسانه ملی در برابر تهدیدات سخت با استفاده از متخصصان داخلی و به‌کارگیری دستورالعمل‌های پدافند غیرعامل، افزایش حمایت‌های مادی و معنوی از شرکت‌های دانش‌بنیان و نخبگان فعال در زمینه طرح‌های توسعه‌ای در حوزه ماهواره‌ای مرتبط با رسانه ملی، بومی‌سازی و به‌کارگیری دانش هوش مصنوعی به‌منظور ایجاد نظام رصد و پایش و هشدار حملات سایبری و کمک به مصون‌سازی زیرساخت رسانه ملی در برابر تهدیدات، خرید و مهندسی معکوس نمونه‌هایی از سامانه‌های نرم‌افزاری پیشرفته در حوزه رسانه ملی، برگزاری مانورهای دوره‌ای منظم در زیرساخت رسانه ملی با بهره‌گیری از تجربیات منازعات منطقه‌ای و جهانی به‌منظور حفظ و افزایش آمادگی در برابر تهدیدات ". همچنین ارزش‌ها و باورهای زیربنایی محافظت از این زیرساخت‌ها عبارت‌اند از: اعتقادات اسلامی، نفی ظلم و تعدی به آحاد جامعه، نفی اغواگری و رعایت حقوق همگان، ترویج سبک زندگی اسلامی و خانواده محوری، عمل کردن به قاعده نفی سبیل، ارتقای تفکر و عمل بسیجی می‌باشد.

ب - پیشنهادها

به‌منظور توسعه پژوهش حاضر با رویکرد پدافند غیرعامل موارد زیر پیشنهاد می‌شود:

۱. هر یک از تهدیدات یاد شده توسط گروهی از متخصصین و کارشناسان مرتبط بررسی شوند.
۲. اهمیت حفظ فضای وحدت و یکپارچگی ملی در مقابل دشمنان از منظر اسلام مورد تحلیل و بررسی قرار گیرد.
۳. اهمیت حفظ و استقلال رسانه ملی در مقابل دشمنان از منظر امامین انقلاب مورد تحلیل و بررسی قرار گیرد.
۴. بررسی تأثیر رعایت اصول و الزامات استتار، اختفاء و فریب در مقابله با تهدیدات ناشی حملات پهپادی.

۵. مطالعه و طبقه‌بندی انواع ویروس‌ها و تروجان‌ها نسبت به اهمیت و سابقه آنها در تهدید در زیرساخت‌ها.

۶. به‌منظور تهیه یک سند راهبردی جامع‌تر حفاظت و صیانت از سایر بخش‌های زیرساخت‌های رسانه ملی مانند مدیریت مصرف داده، اینترنت ملی با رویکرد پدافند غیرعامل مورد بررسی قرار گیرند.

۷. بررسی خلأهای فنی و فناورانه مدیریت مصرف و انتقال داده از داخل کشور به خارج کشور و بالعکس.

۸. باتوجه‌به وابستگی زیرساخت رسانه ملی به ماهواره‌های بین‌المللی، موضوع خودکفایی و کاهش وابستگی به ماهواره‌های بیگانه، مورد بررسی و ارزیابی قرار گیرد.

۹. ارزیابی و مدیریت ریسک و افزایش تاب‌آوری رسانه ملی به‌منظور پایایی رسانه ملی در بحران‌ها.

۵. مراجع

[1] G. Jalali Farahani and M. S. Beikpour, Development of the concept of deterrence theory in the country's cyberspace based on upstream documents and existing approaches, Journal of Electronic and Cyber Defense Research, 2021. (In Persian)

[2] Boroujerdi Alavi, Mahdokht, Rahmati, Mohammad Mehdi (1398). Compilation of Strategic Evaluation Indicators of Public Service Media in the Technical and Infrastructure of Radio and Television, Scientific Quarterly of Visual and Audio Media, Year 13, Issue 3. (In Persian)

[3] F. Petit, D. Verner, J. Phillips, and L. P. Lewis, "Critical Infrastructure Protection and Resilience Integrating Interdependencies," In Security by Design, A. J. Masys, Ed., Cham., Switzerland: Springer, 2018.

[4] Jalali Farahani, Gholamreza, Alavi Vafa, Saeed (1397). Designing and compiling the elements for creating passive defense in the national media, Strategic Defense Quarterly, Year 17, No. 78. (In Persian)

[5] Pourshasb, Abdul Ali, Nazari Nejad, Ahmad Ali (1399). Passive Defense Measures and Strategies in Protecting the Vital Infrastructure of the Islamic Republic of Iran, Strategic Defense Quarterly, Volume 18, Number 82. (In Persian

[6] Mir Yousefi, Seyed Mohsen, Ghaffarpour, Reza (1398). New Strategies for the Protection of Vital Infrastructure, Journal of Passive Defense, Third Year, No. 3. (In Persian)

[7] Nezami, Qadir, Mehri, Abbas (1387). The role of passive defense in national security, Strategic Attitude Monthly, Higher Defense University, No. 92. (In Persian)

[8] Vaezinejad, Mohammad Mehdi, Moqaddas (1394). Report on strategies for securing the country's vital infrastructure in the field of information technology. (In Persian)

[9] A. Ghodsi, The Impact of Cyberspace Infrastructure on the Security of the Islamic Republic of Iran and Strategy Presentation, Journal of Defense Strategy, Volume 11, Number: 44, 2013. (In Persian)

[10] General policies of the system in the field of passive defense - paragraph one, (2010), approved by the Expediency Council.

[11] Alavi Wafa, Saeed (1396). Challenges and Strategic Issues of National Media in Horizon 1404, Quarterly Journal of Communication Research, Twenty-Fourth Year, No. 1. (In Persian)

[12] RAMCAP Plus (۲۰۰۹). «All Hazard Risk and Resilience, Prioritizing Critical Infrastructure by Using the RAMCAP Plus SM Approach», ASME Innovative Innovative.

[13] Sinha, P. (2006). Disaster Vulnerabilities and Risks, Trends, Concepts, Classifications and Approaches. Indian: SBS Publishers & Distributers.

[14] Bradford J. Willke (September2007), A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events.

[۱۵] U.S.Department of homeland security. (September 2008). A guide to critical infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level, Washington.

[۱۶] Johansson, H. Hassel. An approach for modelling interdependent infrastructures in the context of vulnerability analysis, Reliability Engineering and system Safety 95(2010) 1335-1344.

[۱۷] Movahedinia, Jafar (۱۳۸۵). Theoretical and practical implications of passive defense. Tehran: Islamic Revolutionary Guard Corps, Joint Staff, Deputy of Education and Manpower, Center for Planning and Textbook Writing. (In Persian)

[۱۸] Report on the nature of cyber-electronic threats and how to passively defend against it (1396). Strategic View, Higher National Defense University, First Year, No. 50. (In Pe