Quarterly Journal Defensive Future Studies
IRI Military Command and Staff University
www.dfsr.ir
Online ISSN: 2645-7172
Print ISSN: 2588-428x

Cyber protection strategies for the command and control network of the I R I Army

Habibaleh Sayari[1]✉ **Kiumars Aria**[2]

1. Professor of Military Strategic Management, Supreme National Defense University, Tehran, Iran. Email: h.sayari@sndu.ac.ir
2. PhD Student in Defense Management, Army Command and Staff University, Tehran, Iran Email: kiumarsradinanil@gmail.com

Article Info

Article type:
Research Article

Article history:
Received
2025-11-26
Received in revised form:
2026-4-16
Accepted:
2026-5-5
Published online:
2026-5-22

Keywords:
Strategy, cyber protection, Command and Control, Future Threats

ABSTRACT

Background and Objective: The unknown nature of future cyber threats, along with the rapid growth of emerging technologies and the intertwining of the command and control network with cyberspace, has created major vulnerabilities in the future in the cyber environment.

Methodology: Given that the results of this research are useful in improving and perfecting the behaviors, methods, and tools used by the army's command and control network cyber assets, the type of research is an applied article and its implementation method is descriptive, analytical, and with a mixed approach.

Findings: After analyzing the data obtained from the environment, internal environmental factors (10 strengths, 14 weaknesses)and external environmental factors (6 opportunities,8 threats)were identified and the corresponding strategies were calculated using a paired matrix table.

Conclusion: Applying three cybersecurity strategies (using a separate and secure communication infrastructure, changing the approach from technological dependence to independence, and changing the approach to implementing a comprehensive, integrated, exclusive network instead of its multiplexing) can protect command and control network from unknown vulnerabilities.

Cite this article: Sayari, H. & Aria, K. (2026). Cyber protection strategies for the command and control network of the I R I Army. (e736468). *Defensive Future Studies*, *11*(40), 325-359.

DOI: https://doi.org/10.22034/dfsr.2026.2079746.1982

Publisher: IRI Military Command and Staff University

Extended Abstract

Background and Objective:

Cybersecurity is the process of increasing security and minimizing cyber risks through proactive, objective measures to prevent, detect, and respond to threats posed by domestic and foreign actors, including governments and mercenaries, spies and cyber terrorists, organized cyber criminals, and so on. (Yazdani Chaharborj, 2019: 75)

The concern was that focusing only on the aforementioned categories may lead to mental persuasion; in reality, a serious threat may exist, but it remains beyond our superficial view and may disrupt the normal situation in the future. However, as long as the mind does not perceive it, it does not understand the threat correctly, and practically no damage is achieved in terms of security, and it brings a false sense of security. Therefore, the objective issue of cyber protection should be prioritized so that, if the mind of the perpetrator creates a false sense of "no threat" in the future, and with the practical technical measures foreseen, major damage can be prevented. In this research, identifying cyber protection strategies for command and control was considered the main goal. The importance of this research can be considered to help respond appropriately to some of the future cyber threats, develop theoretical foundations for the pathology of command and control cyber networks, and move in the right and safe direction to prevent protection failure and strategic surprise. Because the failure to implement this research may reduce the functions of the command and control network in the future and create uncertainty about the health of the networks, it was necessary to conduct this research.

In the background of this research, there are guidelines and manuals extracted from research related to cybersecurity by technology-rich countries or international institutions at the global level, but with the specific conditions of our country in its dependence on those countries in terms of equipment and technology, adherence to the implementation of the provisions of these documents is not enough to create the security of cyber assets. Given that cyber protection precedes cyber security and that tangible and objective cyber protection measures can cover the negligence caused by the margin of subjective security in the illusion of cyber security, it was necessary to examine the discussion of cyber protection on a case-by-case basis in the field of command and control. Therefore, by determining the overall goal of "Cyber Protection Strategies for the Command and Control Network," this research was conducted, and its results were scientifically presented in the form of cyber protection strategies so that, by implementing these strategies step by step over the next ten years, the command and control network will

be protected from the harm of unknown future vulnerabilities and negligence caused by the halo of false subjective cyber security.

Methodology:

The present study is an applied research that employs a descriptive–analytical research method with a mixed-methods approach. In the qualitative section, qualitative analysis methods and expertise assessment were used to document cybersecurity knowledge, and the axes of this documentation were examined by referring to upstream documents, documents, and strategic security measures of different countries, and concepts were extracted. Then, using the expertise assessment method, the theoretical framework and models related to the research variables were studied, and important and influential issues on cybersecurity were examined. In the quantitative part, after the dimensions and components of cyber security were identified, a researcher-made questionnaire consisting of 4 dimensions, 22 components, and 65 initial items (but ultimately 14 components and 39 items were confirmed) was designed as a five-option Likert scale, and after carrying out the validity and reliability stages (determining the validity and reliability of the questionnaire questions using Cronbach's alpha coefficient), it was distributed to 59 people, considering the limitations of the statistical population: 1- faculty of defense universities, 2- specialists and those with scientific influence in the cyber field, 3- experience in the field of command and control, and the sampling results were analyzed in the form of a complete census and using quantitative methods, descriptive statistics, and SPSS software. To achieve validity, first by studying texts, doctoral theses, research reports, strategic documents, reference models, and after taking advantage of the opinions of respected professors, obtaining the opinions of experts and interviewing experts to the point of theoretical saturation, the dimensions and components of cyber security were extracted and taken into account and approved in the development of the initial questionnaire and the final adjustment. In order to ensure the reliability of the documents, the data obtained from various sources were matched with each other and with the opinions of the interviewed experts, so that their convergence with the theoretical framework was matched and the validity of the sources was confirmed. For the reliability of the questionnaire, the Cronbach's alpha coefficient of the Likert scale questionnaire was calculated using SPSS software. The results of this calculation were all greater than 0.6, indicating the stability of the items. In the strategy census using the SWOT analysis model, first, in the form of a questionnaire, the internal factor evaluation (IFE) and external factor evaluation (EFE) tables were formed; the current and desired position was determined; and the strategy was adapted.

Findings:

Following the analysis, 10 strengths and 14 weaknesses were identified from the internal environmental factors, while 6 opportunities and 8 threats were identified from the external environmental factors. Also, using statistical data from the questionnaire and inferential statistics techniques, and examining the average rank and T-test, the impact of the dimensions (prevention, detection, response and incident management), along with the components and 39 related indicators that were identified equally in the cybersecurity of the command and control network, was summarized.

According to the numbers that were calculated for the current and desired status in the internal and external factors assessment tables.The current situation is in the defensive quadrant, and the desired situation is in the offensive quadrant. The current situation shows that there are more weaknesses than threats in the cybersecurity category of the command and control network. This means that the vulnerabilities of the command and control network have the ability to absorb threats. The current state of the art is not in a favorable condition and must be strengthened. Therefore, the command and control network must abandon the past approach to achieve the desired state of cyber protection. The desired state was also more focused on opportunities, and the forces did not have a high weight. In the current situation, the desired state shows that the forces do not have the ability to hunt for opportunities. Therefore, if we want to reach the desired point and improve the cyber protection of the command and control network to improve and reach the ideal point, the forces must be strengthened. At the same time, in addition to repelling future cyber threats, special attention must be paid to using opportunities.

Conclusion:

Based on the current state matrix of cyber security of the command and control network and the analysis of the status of these factors, as well as the expected desired state for achieving cyber security of the command and control network and staying safe from unknown future vulnerabilities, after identifying fifteen general strategies, three main strategies were summarized with attractiveness scores as follows:

1 Using a separate, independent, and secure communication infrastructure from public telecommunications for the command and control network

2 Changing the approach from technological dependence to independence

3 Changing the approach to implementing a comprehensive, integrated, exclusive network instead of a multitude of island networks and equipment with different brands.

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: ۲۳۸۸-۲۲۸X شاپای الکترونیکی: ۷۱۷۲-۲۶۴۵ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد آجا

راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش جمهوری اسلامی ایران

حبیب‌الله سیاری[۱] ✉ کیومرث آریا[۲]

۱. استاد مدیریت راهبردی نظامی، دانشگاه عالی دفاع ملی، تهران، ایران. (نویسنده مسئول)، رایانامه: h.sayari@sndu.ac.ir

۲. دانشجوی دکتری تخصصی مدیریت دفاعی دانشگاه فرماندهی و ستاد ارتش، تهران، ایران. رایانامه: kiumarsradinanil@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:
تاریخ دریافت:
۱۴۰۴/۰۹/۰۵
تاریخ بازنگری:
۱۴۰۵/۰۱/۳۰
تاریخ پذیرش:
۱۴۰۵/۰۲/۱۵
تاریخ انتشار:
۱۴۰۵/۰۳/۰۱

کلیدواژه‌ها:
راهبرد، حفاظت سایبری، فرماندهی و کنترل، تهدیدهای آینده

چکیده

زمینه و هدف: ناشناخته بودن تهدیدهای سایبری آینده به‌موازات رشد سریع فناورهای نوظهور و همچنین درهم‌تنیدگی شبکه فرماندهی و کنترل با فضای سایبری، آسیب‌پذیری‌های عمده‌ای را در آینده، در محیط سایبری متصوّر نموده است، ازاین‌رو هدف این تحقیق، ارائه راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش جهت جلوگیری از چنین آسیب‌پذیرها در آینده است.

روش‌شناسی: نوع پژوهش مقاله، کاربردی و روش اجرای آن توصیفی، تحلیلی و با رویکرد آمیخته است. از نظرات تعداد ۱۳ نفر از جامعه خبرگان و برای رتبه‌بندی متغیرها، کشف جذابیت راهبردها و وضعیت فعلی و مطلوب به تعداد ۵۹ نفر پرسش‌نامه توزیع و با استفاده از روش SWOT و تشکیل ماتریس برنامه‌ریزی استراتژیک کمّی (QSPM) راهبردهای مناسب ارائه شدند.

یافته‌ها: پس از تجزیه‌وتحلیل داده‌های حاصل از محیط‌شناسی، عوامل محیط داخلی (۱۰ قوّت،۱۴ ضعف) و عوامل محیط خارجی (۶ فرصت، ۸ تهدید) شناسایی و راهبردهای متناظر، با استفاده از جدول ماتریس زوجی احصاء شدند.

نتیجه‌گیری: به‌کارگیری سه راهبرد حفاظت سایبری (استفاده از زیرساخت ارتباطی مجزا و امن، تغییر رویکرد وابستگی فناورانه به استقلال، تغییر رویکرد به پیاده‌سازی شبکه جامع یکپارچه انحصاری به‌جای تعدّد آن) می‌تواند شبکه فرماندهی و کنترل ارتش را از گزند آسیب‌پذیری‌های ناشناخته مصون نگه دارد.

استناد: سیاری، ح.، و آریا، ک. (۱۴۰۵). راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش جمهوری اسلامی ایران. آینده‌پژوهی دفاعی، ۱۱(۴۰)، ۳۲۵-۳۵۹.

DOI: https://doi.org/10.22034/dfsr.2026.2079746.1982

CC BY NC ND

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.

مقدمه

پیشرفت و توسعه سریع فناوری اطلاعات و ارتباطات، حوزه فرماندهی و کنترل که با فضای سایبری درهم‌تنیده را دچار تغییروتحول اساسی نموده و تأثیر آن را در توان رزمی، در اولویت قرار داده است. (مسلمی و آذر،۱۴۰۱: ۲۲)

اختلال در تبادل اطلاعات سامانه فرماندهی و کنترل، خسارت و آسیب‌های جبران‌ناپذیری را به همراه دارد؛ بنابراین جلوگیری از این خسارت مستلزم انجام اقدامات پیش‌بینی شده در محیط سایبری است که نتیجه آن دسترسی امن و پایدار به اطلاعات و اِعمال فرایند مطلوب عملیات است. (البرزنیا،۱۴۰۲: ۱۱۵)

حفاظت سایبری افزایش امنیت و حداقّل رساندن مخاطرات سایبری با انجام اقدامات عینی پیشگیری، تشخیص و واکنش جهت مقابله با تهدیدهایی است که از سوی بازیگران داخلی و خارجی از جمله دولت‌ها و مزدوران، جاسوسان و تروریست‌های سایبری، مجرمین سازمان‌یافته سایبری و غیره ناشی می‌گردند. (یزدانی‌چهاربرج،۱۳۹۹: ۷۵)

از سالیان گذشته در کشور به‌ویژه در ارتش مفاهیمی همچون امنیت، دفاع و پدافند سایبری شکل‌گرفته و به آن پرداخته شده است لیکن موضوع حفاظت سایبری که انجام تمهیدات پیشگیرانه جهت مصون‌سازی در برابر تهدیدهای ناشناخته احتمالی در آینده است به‌دقت موردتوجه واقع نشده است. می‌توان گفت در مقوله‌های امنیت، دفاع و پدافند سایبری منتظر حمله‌ای هستیم تا اقدامی انجام پذیرد و دغدغه این بود که توّجه صرف به مقوله‌های ذکر شده قبلی، ممکن است اقناع ذهنی به همراه داشته باشد و باتوجه‌به توانمندی بالای دشمن در حوزه سایبری ممکن است تهدید جدّی وجود داشته باشد و این تهدید از دید سطح نگر ما مخفی بماند و در آینده باعث به‌هم‌ریختگی وضعیت عادّی گردد؛ ولی تا زمانی که ذهن آن را حس نکند آن تهدید را به‌درستی درک نکرده و عملاً خدشه‌ای در احساس ما به امنیت رخ نداده و حس کاذب وجود امنیت شکل می‌گیرد، بنابراین مسئله حفاظت سایبری که اقدامی سخت‌گیرانه به شیوه اتخاذ تمهیدات سایبری در برابر کنشگری نامشخص در برابر تهدیدات ناشناخته است باید در اولویت قرار گیرد تا اگر ذهن مرتکب حس کاذب «نبود تهدید» در آینده شد با اقدامات پیش‌بینی شده، به‌صورت سیستمی جلوی آسیب عمده به دارایی سایبری گرفته شود.

در این پژوهش توجه به مقوله فیزیکی حفاظت سایبری به‌منظور بی‌اثر نمودن حس کاذب "نبود تهدید" به‌عنوان دغدغه اصلی مطرح و در نتیجه شناسایی راهبردهای حفاظت سایبری فرماندهی و کنترل ارتش به‌عنوان هدف اصلی مدنظر قرار دارد، در اهمیت این پژوهش می‌توان کمک به پاسخگویی به بخشی از تهدیدها و آسیب‌پذیرهای سایبری آینده و تدوین مبانی نظری آن، حرکت در مسیر صحیح و مطمئن برای پیشگیری از شکست حفاظتی و فریب راهبردی را می‌توان خاطرنشان کرد. همچنین تداوم ابهام در کارکردهای مطمئن به شبکه فرماندهی و کنترل از ضرورت انجام این پژوهش بود.

در پیشینه‌های پژوهش در سطح جهانی دستورالعمل‌ها و شیوه‌نامه‌های برآمده از تحقیقات حوزه امنیت سایبری توسط کشورهای صاحب فناوری و یا نهادهای بین‌المللی انجام شده ولی با شرایط خاص کشورمان (واردکننده تجهیزات و فناوری‌های سایبری از سایر کشورها)، پایبندی به اجرای مفاد این اسناد در ایجاد مصونیت دارایی‌های سایبری کافی نیست.

در سطح کشور در موضوع حفاظت سایبری فرماندهی و کنترل، پژوهش قابل استنادی یافت نشد و هر پژوهشی انجام شده به مقوله امنیت و دفاع سایبری پرداخته است که مستلزم پذیرش ضربه اولیه سایبری برای اقدام منفعلانه است و در این راستا فقط رحیم یزدانی‌چهاربرج در قالب رساله دکتری تخصصی با عنوان الگوی راهبردی حفاظت سایبری در سال ۱۳۹۹ در دانشگاه عالی دفاع ملّی به موضوع حفاظت سایبری زیرساخت حیاتی خدمات عمومی کشوری باهدف بی‌اثر نمودن ضربه اولیه سایبری پرداخته است؛ ولی آن‌هم در محتوا به‌گونه‌ای حملات و ضربات غیرفعال و خاموش را پذیرفته است؛ بنابراین این رساله به همراه سایر پژوهش‌ها بیشتر به حوزه عمومی امنیت سایبری نظر داشته و به حفاظت سایبری شبکه فرماندهی و کنترل ارتش توجّهی نداشته است.

باتوجه‌به اینکه حفاظت سایبری مقدم بر امنیت سایبری است و اقدامات فیزیکی و عینی حفاظت سایبری می‌تواند غفلت ناشی از حاشیه امنیت ذهنی در توهّم امنیت سایبری را پوشش دهد لازم بود بحث حفاظت سایبری به‌صورت موردی در حوزه فرماندهی و کنترل ارتش بررسی گردد بنابراین نتایج این پژوهش در قالب راهبردهای حفاظت سایبری ارتش ارائه شد تا با اجرای گام‌به‌گام این راهبردها و الزامات و اقدامات عملیاتی آن در دوره کوتاه‌مدت، شبکه فرماندهی و کنترل ارتش از گزند آسیب‌پذیری‌های ناشناخته آینده و غفلت ناشی از هاله امنیت سایبری ذهنی کاذب آن، در امان بماند.

مرور پیشینه و مبانی نظری

مرور پیشینه

جدول (۱) پیشینه پژوهش

ردیف	کشور	سال	پژوهشگر	عنوان	روش‌شناسی
۱	ایران	۱۳۹۹	رحیم یزدانی‌چهاربرج	الگوی راهبردی حفاظت سایبری زیرساخت‌های حیاتی کشوری	آمیخته، تحلیل کیفی
۲	هلند	۲۰۲۲	شرکت ASML هلند	امنیت سایبری سامانه کنترل جاسازی با رویکرد صنعتی	همبستگی، توصیفی
۳	نروژ	۲۰۲۰	مارتین گیلجه جاتون	بررسی امنیت سایبری در زیرساخت‌های حیاتی هوایی	کیفی، موردی
۴	یونان	۲۰۲۳	کوسماس پیپیروس	مدل بهبود ارزیابی حملات در زیرساخت سایبری حیاتی	تحلیلی - توصیفی
۵	آمریکا	۲۰۲۱	گروه امنیت سایبری ریاست‌جمهوری	سند راهبردی امنیت سایبری دارایی‌های سایبری ملّی	تحلیلی - توصیفی
۶	اتحادیه اروپا	۲۰۲۰	مرکز خبرگی امنیت شبکه اتحادیه اروپا	افق ۲۰۳۰، ابزارها و ادوات امنیت سایبری	تحلیلی - توصیفی
۷	اتحادیه جهانی	۲۰۲۲	کمیسیون ارتباطات در اتحادیه جهانی	مدل وظیفه‌ای چهارمرحله‌ای محافظت از دارایی سایبری	تحلیلی کیفی، موردی

در تحقیقات و اسناد اشاره شده جدول بالا، علی‌رغم پرداختن به برخی متغیرهای مرتبط با موضوع پژوهش، هیچ‌کدام از آن‌ها به‌صورت جامع به مقوله حفاظت سایبری شبکه فرماندهی و کنترل نپرداخته‌اند و محتوای آن‌ها مرتبط با امنیت سایبری کشورهای صاحب فناوری و یا نهادهای بین‌المللی بوده و قابلیت بهره‌برداری و تعمیم آن‌ها با شرایط خاص کشورمان (وابستگی تجهیزاتی و فناورانه به آن کشورها) را ندارند همچنین ویژگی ممتاز شبکه فرماندهی و کنترل به‌ویژه در حوزه دفاعی ضرورت توجّه جدّی به آن را فراتر از مقوله عمومی تأکید دارد تا با ارائه راهبرد پیش‌گیرانه بومی از آسیب‌پذیری محتمل ناشی از غفلت ذهنی در هاله وجود امنیت سایبری خودداری گردد.

در الگوی راهبردی ردیف یکم پیشینه، ۴ بُعد، ۱۸ مؤلفه و ۱۳۱ زیرمؤلفه زیرساخت کشوری مطرح شده‌اند که این متغیرها با مقوله شبکه فرماندهی و کنترل هم راستا نیستند لیکن در بررسی کلی محیط داخلی و خارجی سایبری این مقاله استفاده شدند.

در پیشینه ردیف دوم، تاب‌آوری دارایی‌های سایبری حیاتی به چرخه عامِ واکنش به حوادث شامل اقدامات پاسخ به حوادث، فعالیت‌های بازیابی و پس از حادثه و همچنین اثربخشی تاب‌آوری به توانایی زیرساخت اطلاعاتی حیاتی برای پیش‌بینی، جذب، پذیرش و سرعت بازیابی موکول شده که این رویکرد در شبکه فرماندهی و کنترل که عملاً هر گونه حادثه سایبری جزئی ماهیت مأموریتی آن را سلب می‌کند قابل‌پذیرش نمی‌کند لیکن از نتایج آن، جهت شناسایی نقاط ضعف محیط سایبری استفاده شده است.

ردیف سوم پیشینه، عوامل افزایش‌دهنده مخاطره آسیب‌پذیری‌های فناوری اطلاعات هوایی، افزایش دیجیتالی‌شدن و افزایش خودکارسازی در هواپیماهای مدرن، افزایش میزان و پیچیدگی نرم‌افزارهای بکار رفته، افزایش ارتباطات بین دستگاه و زیرسیستم‌ها، افزایش تعداد رابط‌های ارتباطی با دنیای بیرون از طریق ادغام سامانه گزارش‌گیری و ارتباطات هواپیمایی با سامانه‌های فناوری پایه را مورد بررسی قرار داده است. این پژوهش به‌صورت موردی به صنعت هوایی پرداخته و هر چند که امکان الگوبرداری جزئی از آن برای شبکه فرماندهی و کنترل فراهم است لیکن قابلیت بهره‌برداری جامع آن در این مقاله نیست.

در پیشینه ردیف چهارم در مدل‌سازی امنیت سایبری، رعایت سیزده اصل قابلیت جذب، سازماندهی مجدد، قابلیت اطمینان و رسیدن به عملکرد قابل‌قبول، حرکت به سمت اصلاح، افزایش ظرفیت‌های محلی، قابلیت تعامل، افزونگی فیزیکی، افزونگی عملکردی، دفاع لایه‌ای، دخالت نیروی انسانی، کاهش پیچیدگی، کاهش تعاملات پنهانی مطرح شده‌اند که بیانگر پذیرش نفوذ به شبکه است درحالی‌که ویژگی حفاظت سایبری شبکه فرماندهی و کنترل ضرورت سلب هرگونه نفوذ و دوری از هر گونه حمله سایبری را تأکید دارد.

در پیشینه ردیف پنجم طرح «حفاظت از زیرساخت‌های ملّی آمریکا» شامل الزامات طرح «امن‌سازی و تاب‌آوری زیرساخت‌های حیاتی» است در این طرح مشارکت همه ذی‌نفعان زیرساخت حیاتی در همه سطوح دولتی و صنعت تأکید شده و نهاد فدرالی به‌عنوان نهاد متولّی مسئول توسعه و پیاده‌سازی مفاهیم «حفاظت از زیرساخت‌های ملی آمریکا» بر اساس ویژگی‌های خاص هر زیرساخت شده است. سند «حفاظت از زیرساخت‌های ملّی آمریکا» به‌عنوان سند راهنمای سیاست‌گذاری، مثالی از همکاری بین مالکان و کاربرهای فدرالی، دولتی، محلی، نهادهای منطقه‌ای، سازمان‌های غیرانتفاعی و مؤسسات دانشگاهی است درحالی‌که ویژگی‌های شبکه فرماندهی و کنترل از بابت رعایت اصل محرمانگی و

حیطه‌بندی اطلاعات مانع مشارکت همگانی در تحقّق امنیت سایبری بوده و در آن سند مفهوم حفاظت سایبری شبکه فرماندهی و کنترل مغفول مانده است.

در پیشینه ردیف ششم، آژانس امنیت اطلاعات و شبکه اتحادیه اروپا، ۹ اقدام اساسی را موردتوجه قرار داده است: تنظیم چشم‌انداز، دامنه، اهداف و اولویت‌ها/ ایجاد و تبعیت از رویکرد ملی ارزیابی مخاطرات/ شناسایی و مشارکت ذی‌نفعان/ ایجاد سازوکارهای تبادل اطلاعات رخدادهای امنیتی/ سازمان‌دهی رزمایش‌های سایبری و شناسایی آسیب‌پذیری‌ها و افزایش همکاری‌ها/ ایجاد سازوکار گزارش‌دهی/ تحقیق‌وتوسعه در فرایندهای امنیتی / ایجاد سازوکار مشارکت عمومی و خصوصی / ارزیابی اقدامات.

اقدامات بالا دستورالعمل کلی است که در آن جزئیات مغفول مانده و ضرورت دارد با استفاده از محتوای کلی آن که به شناسایی محیط داخلی و خارجی کمک می‌کند به تدوین راهبرد حفاظت سایبری شبکه فرماندهی و کنترل ارتش پرداخت.

در پیشینه ردیف هفتم، اتحادیه بین‌المللی ارتباطات مدل چهارمرحله‌ای حفاظت از زیرساخت‌های سایبری شامل پیشگیری، تشخیص، واکنش، مدیریت بحران را مطرح نموده و باتوجه‌به ماهیت شبکه فرماندهی و کنترل که بایستی همواره موضوع تهدیدات ناشناخته در آینده پیش‌بینی گردد مدل ارائه شده هر چند صرفاً به‌عنوان نظریه مختار برای تعیین ویژگی حفاظت سایبری شبکه فرماندهی و کنترل در چارچوب نظری این مقاله استفاده شده امّا در مسیر تدوین راهبردهای حفاظت سایبری در محیط پیچیده شبکه فرماندهی و کنترل، شناسایی عوامل خارجی و تهدیدهای ناشناخته آینده، به آن افزوده شده است.

مبانی نظری

ازآنجایی‌که حفاظت سایبری یک موضوع چالشی است؛ لذا رویکرد دولت‌ها متفاوت بوده و از حالت کاملاً حاکمیتی تا حداقل دخالت حاکمیتی متغیر است لکن اقدامات بین‌المللی در موضوع حفاظت سایبری در راستای ارائه مدل، تعیین اصول و چارچوب‌ها قابل‌توجه است به‌طوری که اتحادیه بین‌المللی ارتباطات مدل چهارمرحله‌ای ارائه کرده است که شامل مراحل پیشگیری و هشدار، تشخیص، واکنش و مدیریت بحران هست. درحالی‌که اتحادیه اروپا هم مدل پنج‌مرحله‌ای (آمادگی، تشخیص، مقابله، همکاری بین‌المللی، توسعه معیارهای شناختی) و هم چارچوبی را با هشت محور (امنیت جامع سیستمی، مدیریت

مخاطرات و تحلیل آسیب‌پذیری، پیشگیری و تشخیص، پاسخ به حوادث و بازیابی، بقاپذیری سامانه‌ها، مباحث حقوقی و نظارتی و سیاست‌گذاری، تحقیق‌وتوسعه بنیادی، مسائل غیرفنی) ارائه کرده است. اجلاس جهانی جامعه اطلاعاتی مجموعه اصول و برنامه عملی در زمینه افزایش محرمانگی، حفاظت از جامعیت داده و شبکه تدوین کرده است. همچنین سازمان همکاری و توسعه اقتصادی، خطوط راهنمایی برای امنیت سامانه‌ها و شبکه‌های اطلاعاتی و نهایتاً کشورهای عضو «گروه هشت» اصول نه‌گانه (داشتن شبکه‌های هشدار، ارتقای سطح آگاهی، شناسایی وابستگی بین زیرساخت‌های ارتباطی، ارتقای مشارکت هیئت حاکمه، داشتن شبکه‌های ارتباطی برای شرایط بحران، اطمینان از وجود سیاست‌های دسترسی به داده، وجود قوانین نظارتی کافی، تسهیل ردیابی حملات و تبادل تجربیات، انجام رزمایش‌ها و تمرینات، مشارکت در همکاری‌های بین‌المللی) ارائه کرده‌اند. بر اساس مطالعه اصول، خطوط راهنما و فرایندهای مذکور می‌توان کلیدواژه‌های مرتبط با حفاظت سایبری را در اسناد موردمطالعه، مطابق با جدول زیر در نظر گرفته و مدل، رویکرد و اقدامات بین‌المللی آن‌ها را تشریح نمود.

جدول (۲) کلیدواژه‌های موردتأکید در اسناد کشورها و سازمان‌های مطرح در حوزه سایبری

مرجع	کلیدواژه‌های موردتأکید
آمریکا	محافظت عملی از دارایی‌های سایبری در قبال آسیب‌پذیری‌ها و حملات از طریق پیشگیری، هشدار به‌موقع، تشخیص، واکنش، مدیریت بحران (Paik et al. 2021:35)
آلمان	پیشگیری، واکنش عملی مؤثر در صورت وقوع حادثه در حوزه فناوری اطلاعات، تاب‌آوری از طریق تقویت امنیت حوزه فناوری اطلاعات (Kaska & Trinberg, 2022: 38)
روسیه	تشخیص، پیشگیری و حذف اثرات حملات سایبری (Tadviser,2022)
استرالیا	ارزیابی، تشخیص، کاهش مخاطرات زیرساخت‌های سایبری، ارزیابی دارائی‌های سایبری، شناسایی تهدیدها، ارزیابی سلامت دارائی‌ها، اتخاذ واکنش مناسب در برابر مخاطرات مرتبط با دسترس‌پذیری و محرمانگی دارائی‌ها Segura Serrano,2023,3
کره جنوبی	اقدامات عملی پیشگیرانه، واکنشی توسط دولت و بخش خصوصی در زیرساخت‌های سایبری حیاتی (Kim,2020:15)
سازمان همکاری و توسعه اقتصادی	افزایش عینی سطح امنیت در شبکه‌ها و سامانه‌های اطلاعاتی، داشتن راهبرد مدیریت مخاطرات و پیاده‌سازی مکانیزم‌های مربوطه، ایجاد تیم‌های پاسخ به حوادث امنیتی، راه‌اندازی سازوکار تبادل اطلاعات(Vasileios Mavroeidis,2020,36)
اتحادیه جهانی مخابرات	مدل چهارمرحله‌ای حفاظت سایبری شامل مراحل عملی پیشگیری و هشدار اولیه، تشخیص، واکنش، مدیریت حوادث است. (Kauspadiene et al.2020: 112)

مدل‌ها

به‌منظور برداشتن گام به سمت یک واحدسازمانی مؤثر و کارآمد، اتحادیه بین‌المللی ارتباطات، مدل چهار مرحله حفاظت سایبری را مطرح نموده که شامل پیشگیری و هشدار، تشخیص، واکنش و مدیریت بحران به شرح زیر است. (Kauspadiene et al,2017: 112)

پیشگیری و هشدار: گرچه می‌توان گفت که هر چهار مرحله دارای ویژگی پیشگیرانه است لکن هدف از هشدار، ارتقای آمادگی عمومی و آماده‌سازی برای کاهش نقض امنیت اطلاعات و کاهش آسیب‌پذیری‌ها است.

تشخیص: لازم است واحدهای حفاظت از زیرساخت‌های شبکه‌ای با گروه‌های واکنش سریع و کارشناسان فنی و بخش خصوصی همکاری کنند. در بحث کشف، باید به محدودنشدن حمله به مرزهای جغرافیایی و همچنین باید به تحلیل‌های اجتماعی و غیرفنی توجّه کرد.

واکنش: واکنش شامل شناسایی عوامل اختلال و برطرف ساختن آن عوامل است که می‌توان به آمادگی شبانه‌روزی، تشخیص به‌موقع، تسریع در اقدام، پیگرد قانونی و تعقیب مهاجمان، محدودنشدن به اقدامات فنی، همکاری با متولیان پاسخگو در دو سطح داخلی و خارجی، تهیه مستندات و ثبت وقایع از الزامات واکنش به هنگام، اشاره کرد.

مدیریت شرایط اضطرار: مدیریت بحران بخشی از حفاظت سایبری است. به‌منظور حداقل‌سازی اثرات هرگونه اختلال در سطح سازمان و در سطح حاکمیت، بایستی حفاظت از زیرساخت‌های سایبری در ساختار کلان مدیریت بحران جای گیرد تا توانایی ارائه مشاوره به سازمان‌ها و دولت را داشته باشد.

به‌منظور تعیین چارچوب حفاظت سایبری در سطح اتحادیه اروپا، مدلی مطرح شده است که این مدل شامل ۸ محور زیر است. (Luiijf, 2019: 2)

امنیت جامع سیستمی، مدیریت مخاطرات و تحلیل آسیب‌پذیری، پیشگیری و تشخیص، پاسخ به حوادث و بازیابی، بقاپذیری سامانه‌ها، مباحث حقوقی و سیاست‌گذاری، تحقیق‌وتوسعه بنیادی، مسائل غیرفنی که به حفاظت سایبری مرتبط است.

علاوه بر مدل اتحادیه بین‌المللی ارتباطات و چارچوب اتحادیه اروپا، آقای الیسفان و همکارش در رساله دکتری، مدل «مشاوره‌ای، هشداردهی امنیتی اجتماع‌محور» ارائه کرده است (Mouton and Ellefsen,2019: 3). در این مدل ساختار موردنیاز حفاظت سایبری را در دو گروه بایستی لحاظ کرد که یکی از آن گروه‌ها با «تیم پاسخ به حوادث امنیتی رایانه‌ای» پشتیبانی می‌شود و دیگری با ساختار اجتماع‌محور؛ یعنی ساختار حفاظت سایبری باید از راهبرد دوعاملی پیروی کند تا هر دو گروه را به طور موازی پشتیبانی کند.

رویکردها

رویکرد در زمینه حفاظت سایبری به‌ویژه در سطح کلان آن در کشورها متفاوت بوده و می‌تواند یکی از حالت‌های زیر باشد. (Min,2018: 15)

- ✓ کاملاً حاکمیتی (حفاظت کامل حاکمیتی از دارائی زیرساخت‌های سایبری)
- ✓ اجباری کردن استانداردهای امنیت سایبری در معماری
- ✓ استانداردسازی، نظارت و اجرای امنیت در زیرساخت‌ها توسط بخش خصوصی
- ✓ حفاظت سایبری توسط انجمن‌های صنفی
- ✓ اجرای حفاظت سایبری با بخش خصوصی و تصدیق با کارفرما
- ✓ تشویق، روان‌سازی و ایجاد چارچوب قانونی توسط کارفرما و حداقل دخالت

اقدامات بین‌المللی

در اجلاس بین‌المللی جنگ و امنیت سایبری، فعالیت نهادهای بین‌المللی برای بهبود سیاست‌ها و مدیریت حفاظت و امنیت سایبری به شرح جدول (۳) مشروحه زیر جمع‌بندی و ارائه شده‌اند که هرکدام از آن‌ها، دارای موضوع و الزامات خاصی هستند که می‌توانند به‌عنوان چارچوب نظری در تدوین مدل مفهومی استفاده شوند. (Satola et al,2017:318)

جدول (۳) موضوعات و الزامات موردتأکید نهادهای بین‌المللی

نهادها	موضوعات مرتبط با حفاظت سایبری
اجلاس جهانی جامعه اطلاعاتی	اصول و برنامه عملی در زمینه نظارت قانونی و محیط سیاست‌گذاری جهت حداکثرسازی مزایا، تصریح در ارتقای فرهنگ جهانی امنیت سایبری باهدف افزایش محرمانگی، حفاظت از جامعیت داده و شبکه را تدوین و ارائه نموده و تهدیدات فناوری اطلاعات و ارتباطات و دیگر موضوعات امنیت شبکه و امنیت اطلاعات را موردتوجه قرار داده است.
انجمن تیم‌های پاسخ به حوادث امنیتی	نهاد بین‌المللی فنی فعال در تهیه استانداردهاست که با تیم‌های پاسخ به حوادث رایانه‌ای همکاری می‌کند و زمینه اشتراک‌گذاری اطلاعات بین تیم‌های پاسخ به حوادث رایانه‌ای و دیگر سازمان‌های پاسخ‌دهی به حوادث را آماده می‌کند و انباره‌ای از اطلاعات لازم برای حفاظت سایبری را دارا بوده و ارائه داده است.
سازمان همکاری و توسعه اقتصادی	ارائه‌دهنده «خطوط راهنمای برای امنیت سامانه‌ها و شبکه‌های اطلاعاتی» جهت فرهنگ‌سازی امنیت است.

کشورهای عضو گروه هشت	اصول نه‌گانه‌ای را ارائه داده که شامل: داشتن شبکه‌های هشدار، ارتقای سطح آگاهی، شناسایی وابستگی بین زیرساخت‌های سایبری، ارتقای مشارکت بین سهام‌داران عمومی و خصوصی، داشتن شبکه‌های ارتباطی برای شرایط بحران، اطمینان داشتن از وجود سیاست‌های دسترسی به داده به‌عنوان الزام، وجود قوانین کافی در تعقیب حملات، تسهیل ردیابی حملات و تبادل تجربیات، انجام رزمایش‌ها، مشارکت در همکاری‌های بین‌المللی
اتحادیه اروپا	طرح عملی را بر پایه ۵ مرحله آمادگی و پیشگیری، تشخیص و واکنش، مقابله و بازیابی، تقویت همکاری بین‌المللی در زمینه اصول و دستورالعمل‌های تاب‌آوری، توسعه معیارهای شناختی ارائه کرده است.
سازمان بین‌المللی استاندارد	پوشش‌دهنده استانداردهایی است که مرتبط با زیرساخت اطلاعات و سامانه‌های ارتباطی و فناوری اطلاعات است.
انجمن حکمرانی اینترنت	مدل جذابی را برای مشاوره‌های حفاظتی و انجمن بین‌المللی برای گفتمان‌های وسیع حول حفاظت از زیرساخت‌های حیاتی ارائه داده است.

حفاظت سایبری از زیرساخت‌های حیاتی یک موضوع مرتبط با امنیت ملی است به این معنا که شکست یا نابودی زیرساخت‌های حیاتی، تأثیر جدی بر امنیت، اقتصاد و رفاه شهروندان می‌گذارد و حتی به دلیل همبستگی جهانی، تأثیر جهانی دارد. (Luiijf, 2016:5) جوامع به‌شدّت به عملکرد زیرساخت‌های حیاتی مانند شبکه‌های ارتباطی و سامانه‌های فرماندهی و کنترل وابسته هستند و عملکرد آن زیرساخت‌ها به عملکرد زیرساخت‌های سایبری بستگی دارند. زیرساخت‌های اطلاعاتی حیاتی به‌عنوان یکی از بخش‌های کلیدی جامعه، جهت داشتن عملکرد مداوم و قابل‌اعتماد، متّکی به طیف گسترده‌ای از شبکه‌ها و سامانه‌های کنترلی نرم‌افزار و سخت‌افزار پایه ملّی هستند. (Rajaonah, 2017: 109).

این شبکه‌ها حلقه اتصال زیرساخت‌های سایبری حیاتی بوده و آن‌ها را به هم متصل و وابسته می‌کنند؛ لذا حفاظت سایبری از آن‌ها به دلیل منافع عمومی و امنیت ملّی و سازمانی مبحث کلان و راهبردی است. در سطح جهانی هم حفاظت از زیرساخت‌های اطلاعاتی حیاتی به‌عنوان بخش مهمی از امنیت ملی در کشورهای مختلف است. (ENISA,2015: 81) با این رویکرد، بازیگران اصلی حفاظت سایبری از زیرساخت‌های حیاتی در سطوح بین‌المللی، ملی، سازمانی، قانونی، فنی، بازیگران امنیتی هستند. (Rajaonah, 2017: 109) در کشور خودمان ایران، در اسناد بالادستی به‌ضرورت انکارناپذیر توجّه جدّی به موضوع حفاظت سایبری پرداخته که متغیرهای آن‌ها قابل‌استفاده در شبکه فرماندهی و کنترل است.

چارچوب نظری پژوهش

باتوجه‌به مطالب اشاره شده بالا، به‌منظور تعیین چارچوب حفاظت سایبری در این مقاله، مدل اتحادیه جهانی ارتباطات شامل چهار مرحله (پیشگیری، تشخیص، واکنش، مدیریت حوادث)، **به‌عنوان نظریه مختار** جهت شناسایی ویژگی‌های حفاظت سایبری تعیین گردید و روش SWOT که موردتأکید گروه مؤلفین دافوس آجا نیز است در طراحی جهت تدوین راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش تعیین شده است.



مدل مفهومی

مطابق نظر خبرگان و مبانی نظری، در تدوین راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش، تأثیر ضعف و قوّت بر هر یک از ویژگی‌های حفاظت سایبری شامل اقدامات پیشگیری، تشخیص، واکنش و مدیریت حوادث، در ترکیب با تأثیر فرصت و تهدید بر هر یک از موارد خاص محیط سایبری ارتش شامل سیاسی، اجتماعی و فرهنگی، قانونی و نظارت، علوم و فناوری، حملات و آسیب‌پذیری‌ها و بازیگران تهدید باید مورد بررسی قرار گیرد تا بتوان بر اساس مدل تحلیل SWOT وضعیت‌های موجود و مطلوب ارتش را شناسایی نمود؛ بنابراین مدل مفهومی مقاله، از روش اکتشافی به شرح شکل (۱) احصاء شده است.

شکل (۱) مدل مفهومی پژوهش

رویکرد هیئت حاکمه	سیاسی	فرصت	راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش	ضعف	پیشگیری	سخت‌افزار و نرم‌افزار		
جایگاه اجتماعی سازمان		تهدید				آموزش و فرهنگ‌سازی		
فرهنگ‌سازمانی	اجتماعی، فرهنگی	فرصت		قوّت		پیاده‌سازی امن معماری		
آگاهی عمومی و فنی						نظارت و پایش		
انگیزه کارکنان						هشدار		
آموزش		تهدید		ضعف	تشخیص	پایشگری		
نگرش مدیران						کنترل نفوذ		
قوانین و مقررات	قانون و نظارت	فرصت		قوّت		رفتار کاربران		
استانداردهای امنیتی					واکنش	تحلیل تهدیدات		
نهادهای نظارتی		تهدید		ضعف		اسکن آسیب‌پذیری‌ها		
رشد فناوری‌ها	علوم و فناوری	فرصت				بررسی لاگ‌ها		
تغییر فناوری‌ها						تمرین حملات		
تأخیر دریافت فناوری‌ها		تهدید		قوّت		شناسایی و ارزیابی حادثه		
نفوذ اطلاعاتی	حملات و آسیب‌پذیری‌ها	فرصت				مهار		
بدافزارها						بازیابی		
باج‌افزارها						فعالیت پس از حادثه		
فیشینگ		تهدید		ضعف	مدیریت حوادث	برنامه‌ریزی و آمادگی		
اشباع سرویس						شناسایی و ثبت		
زنجیره تأمین						ارزیابی و تحلیل		
تهدید خودی	بازیگران	فرصت		قوّت		هماهنگی واکنش		
						مستندسازی		
تهدید خارجی		تهدید				بهبود		
						کنترل ریسک		

روش‌شناسی

باتوجه‌به اینکه حاصل پژوهش در بهبود و به کمال رساندن رفتارها، روش‌ها و ابزارهای مورداستفاده دارایی‌های سایبری شبکه فرماندهی و کنترل ارتش کاربرد دارد نوع مقاله کاربردی و روش اجرای آن توصیفی، تحلیلی و با رویکرد آمیخته است.

به علّت محدودیت شرایط خبرگی ۱ مقام عالی‌رتبه حوزه دفاعی ۲ متخصص در حوزه سایبری ۳ سابقه اشتغال عملی به مدّت دو دهه در حوزه پژوهش که تعداد ۱۳ خبره بودند و همچنین محدودیت جامعه آماری ۱ هیئت‌علمی دانشگاه‌های دفاعی ۲ متخصّص و دارای اثر علمی در حوزه سایبری ۳ سابقه فعالیت در حوزه فرماندهی و کنترل، تعداد ۵۹ نفر صاحب‌نظر شناسایی شدند؛ بنابراین نمونه‌گیری به‌صورت تمام شمار انجام شد.
در بخش کیفی به‌منظور استخراج مؤلفه‌ها و شاخص‌های مفهومی از داده‌های حاصل از مصاحبه‌ها، منابع و اسناد علمی، از روش تحلیل مضمون استفاده شد. انتخاب این رویکرد بر اساس ماهیت داده‌ها و هدف پژوهش صورت گرفت، فرایند تحلیل داده‌های کیفی با پیروی از گام‌های پیشنهادی براون و کلارک شامل آشنایی با داده‌ها، کدگذاری اولیه، شکل‌گیری مضامین اولیه، بازنگری و پالایش مضامین، تعریف و نام‌گذاری مضامین نهایی و در نهایت تبدیل مضامین به مؤلفه‌ها و شاخص‌ها انجام شد و فرایند استخراج، دسته‌بندی، مقایسه، پالایش و ترکیب استقرایی و قیاسی به‌گونه‌ای انجام شد که مسیر تبدیل از واحد معنایی خُرد (کد) تا مفهوم کلان (مقوله/مؤلفه) به‌صورت تلفیقی، متمرکز بر شباهت معنایی و تکرار پالایشی طی گردد. در راستای کدگذاری اولیه، ابتدا تمامی متن‌های حاصل از مصاحبه‌ها و اسناد، به‌صورت دقیق و بند به بند مورد بازخوانی قرار گرفتند و گزاره‌ها، عبارات کلیدی و مفاهیم مرتبط با عنوان مقاله، شناسایی و با برچسب‌های اولیه (کدها) مشخص شدند. سپس به‌منظور شکل‌گیری مضامین اولیه، کدهای اولیه از تمام منابع، جمع‌آوری و مورد مقایسه قرار گرفتند. در این مرحله دنبال همپوشانی معنایی و ارتباط مفهومی بین کدها بودیم و کدهایی که پیرامون یک ایده یا مفهوم مشترک شکل‌گرفته بودند، در قالب مضامین اولیه دسته‌بندی شدند. در پایان به‌منظور بازنگری، پالایش و تعریف مقولات نهایی، مجدداً مورد ارزیابی دقیق قرار گرفتند. مضامین اولیه، با درنظرگرفتن پیشینه نظری تحقیق و همچنین داده‌های خام، پالایش شده و ذیل مفاهیم کلان‌تر سازماندهی شدند تا به مقولات سطح بالا تبدیل گردند. این فرایند تکرارشونده و چندوجهی، باعث شد که مقولات نهایی، نه‌تنها از داده‌ها به دست آیند؛ بلکه نماینده‌ی پیچیدگی و ابعاد مختلف راهبردهای ارائه شده این مقاله بر اساس شواهد موجود در مصاحبه‌ها و منابع علمی باشند.

در بخش کمّی، پس از شناسایی ابعاد و مؤلفه‌های حفاظت سایبری، پرسش‌نامه به‌صورت طیف لیکرت پنج‌گزینه‌ای طراحی و به جامعه آماری توزیع شد. سپس نتایج نمونه‌گیری به‌وسیله روش‌های کمّی، آمار توصیفی و نرم‌افزار SPSS مورد تجزیه‌وتحلیل قرار گرفتند. برای بالابردن روایی پرسش‌نامه، ابتدا پرسش‌نامه در میان منتخب جامعه آماری توزیع و در طول تکمیل پرسش‌نامه نظرات اصلاحی از آنان اخذ و سپس سؤال‌هایی که اهداف تحقیق را برآورده نمی‌کردند اصلاح و یا حذف شدند. به‌منظور پایابودن اسناد و مدارک، داده‌های حاصل از منابع گوناگون، با یکدیگر و با نظرات صاحب‌نظران مصاحبه‌شونده، مطابقت داده شد. برای پایایی مصاحبه، سؤالات مصاحبه در زمان‌های مختلف ارائه شد تا با مقایسه پاسخ‌های دریافتی با پاسخ‌های پیشین به پایایی دست‌یافت، برای پایایی پرسش‌نامه، پایایی پرسش‌نامه از طریق اجرای آزمون اعتبارسنجی توسط نرم‌افزار SPSS و سنجش ضریب آلفای کرونباخ ارزیابی که مقدار ضریب آلفای کرونباخ به‌دست‌آمده بیشتر از ۰/۷۵ بود و گویه‌های پرسش‌نامه از قابلیت اطمینان لازم برخوردار بود. برای روایی همگرایی در ترکیب اسناد، مصاحبه و پرسش‌نامه از نرم‌افزار لیزرل کمک گرفته شد؛ چون میزان میانگین واریانس استخراج شده عدد ۰٫۶ بزرگ‌تر از ۰٫۵ است و پایایی مرکب عدد ۰٫۸بزرگ‌تر از ۰٫۷محاسبه شده روایی همگرایی در ترکیب آن‌ها وجود داشت. بر اساس مدل تحلیل نقاط قوّت، ضعف و فرصت‌ها و تهدیدات (SWOT)، ابتدا در قالب پرسش‌نامه جدول ارزیابی عوامل داخلی(IFE) و جدول ارزیابی عوامل خارجی(EFE) تشکیل و موقعیت فعلی و مطلوب تعیین و تطبیق راهبرد انجام شد. سپس با تشکیل ماتریس برنامه‌ریزی استراتژیک کمّی (QSPM) و دریافت امتیاز جذابیت نسبی راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل و تجمیع گزاره‌ها برای مبنای عناصر تدوین راهبرد (اهداف، وسیله و روش) راهبردهای اولویت‌دار تدوین و ارائه گردیدند.

در پایان از نظرات تأییدی تعداد ۳ نفر از اساتید دانشگاهی حوزه سایبری با رتبه استاد تمام برای اعتبارسنجی نهایی نتایج این پژوهش استفاده شده است.

تجزیه‌وتحلیل یافته‌ها

تجزیه‌وتحلیل آماری داده‌های جمعیت‌شناختی

در این پژوهش جهت شناسایی جامعه آماری ۴ پرسش در خصوص میـزان تحصیـلات، میـزان آشنـایی پاسخ‌دهندگان با موضوع پژوهش، سابقه کار در حوزه موضوع پژوهش و رده مسئـولیتی پاسخ‌دهندگان مطرح شد که گویه‌های جمعیت‌شناختی آن پس از جمع‌آوری با استفاده از فنون آمار توصیفی مانند فراوانی، درصد فراوانی، فراوانی تجمعی و نمودار هیستوگرام تجزیه‌وتحلیل گردید و نتایج حاصل به شرح جدول زیر است.

جدول (۴) توزیع فراوانی جامعه نمونه آماری

توزیع فراوانی میـزان تحصیـلات	**تحصیلات**	**فراوانی**	**درصد فراوانی**	**درصد فراوانی تجمعی**
	کارشناسـی	۵	۸/۴	۸/۴
	کارشناسی‌ارشد	۴۴	۷۴/۵	۸۲/۹
	دکتـری	۱۰	۱۷/۱	۱۰۰
	جمـع کل	۵۹	۱۰۰	
آمار توصیـفی میـزان آشنـایی پاسخ‌دهندگان با موضوع پژوهش	**میزان به درصد**	**فراوانی**	**درصد فراوانی**	**درصد فراوانی تجمعی**
	۶۰٪	۰	۰	۰
	۸۰٪	۸	۱۴/۵	۱۴/۵
	۱۰۰٪	۵۱	۸۵/۵	۱۰۰
	جمـع کل	۵۹	۱۰۰	
آمار توصیفـی سابقه کار در حوزه موضوع پژوهش پاسخ‌دهندگان	**سال سابقه خدمت**	**فراوانی**	**درصد فراوانی**	**فراوانی تجمعی**
	۱۵-۱۱	۴	۷	۷
	۲۰-۱۶	۱۹	۳۳	۴۰
	۲۵-۲۱	۱۸	۳۰	۷۰
	بیش از ۲۵ سال	۱۸	۳۰	۱۰۰
	جمـع کل	۵۹	۱۰۰	
توزیع فراوانی رده مسئـولیتی پاسخ‌دهندگان	**تحصیلات**	**فراوانی**	**درصد فراوانی**	**درصد فراوانی تجمعی**

	عضـو هیئت‌علمی	۱۷	۲۸/۹	۲۸/۹
	مدیریتـی	۴۰	۶۷/۸	۹۶/۷
	کارشنـاس فنی	۲	۳/۳	۱۰۰
	جمـع کل	۵۹	۱۰۰	

تجزیه‌وتحلیل سایر داده‌ها و ارائه یافته‌های پژوهش

در جدول زیر مؤلفه‌هایی که موردتأیید قرار گرفته‌اند لحاظ و سایر ابعاد مدل مفهومی این مقاله که موردتأیید واقع نشده‌اند از جدول حذف شدند در واقع مدل مفهومی شامل ۴ بعد، ۲۲ مؤلفه و ۶۵ گویه اولیه بود؛ ولی در نهایت ۱۴ مؤلفه و ۳۹ گویه تأیید شدند.

جدول (۵) میانگین تأثیرگذاری ابعاد، مؤلفه و شاخص‌های مرتبط

ابعاد	رتبه میانگین	مؤلفه	رتبه میانگین	شاخص	رتبه میانگین
پیشگیری	۲/۷۶	سخت‌افزار و نرم‌افزار	۲/۷۱	به‌روزرسانی امنیتی سیستم‌ها	۸/۰۶
				استفاده از تجهیزات امن شبکه	۸/۰۲
				تنظیمات امنیتی صحیح	۷/۵۲
		پیاده‌سازی امن معماری	۲/۹۵	ساده‌سازی تجهیزات شبکه	۸/۰۲
				ایزوله‌سازی شبکه‌های عملیاتی	۷/۹۲
				پیاده‌سازی احراز هویت	۷/۷۲
		نظارت و پایش	۲/۸۶	ابزارهای نظارتی	۸/۰۲
				جمع‌آوری و تحلیل لاگ‌ها	۷/۹۲
		هشدار	۲/۵۵	ابزارهای هوشمند هشدار	۷/۲۵
				هوشمندسازی شناسایی	۷/۹۵
تشخیص	۲/۴۲	پایشگری	۲/۵۲	پایشگری ترافیک شبکه	۶/۹۶
				پایشگری سیستم‌ها	۶/۸۲
				پایشگری لاگ‌ها	۶/۷۵
				پایشگری رفتار کاربران	۷/۰۵
		کنترل نفوذ	۲/۶۱	شبکه‌ای	۷/۳۲
				میزبانی	۷/۲۶
		اسکن آسیب‌پذیری‌ها	۲/۸۰	اسکن شبکه	۷/۶۷
				شناسایی آسیب‌پذیرها	۸/۱۵
واکنش	۲/۳۵		۲/۹۵	اعتبارسنجی هشدارها	۶/۵۳

		شناسایی و ارزیابی حادثه		ارزیابی آسیب	۶/۷۶
				اولویت‌بندی	۶/۵۲
		مهار	۲/۹۵	جداسازی دستگاه‌های آلوده	۷/۴۳
				مسدودسازی ترافیک مخرب	۷/۶۵
				تغییر رمزهای عبور	۷/۳۴
				جداسازی دستگاه‌های آلوده	۷/۵۲
		بازیابی	۲/۷۵	حذف بدافزارها	۷/۸۵
				پاک‌سازی سیستم‌ها	۷/۶۵
				بازیابی داده‌ها	۶/۴۳
				بازگردانی سیستم‌ها	۶/۶۵
		فعالیت پس از حادثه	۲/۶۰	بهبود فرایندها و سیاست‌ها	۶/۴۶
				جلوگیری از تکرار	۶/۹۵
مدیریت حوادث	۲/۵۲	برنامه‌ریزی و آمادگی	۲/۶۵	تشکیل تیم مدیریت حوادث	۸/۲۵
				توسعه سیاست‌ها و رویه‌ها	۷/۶۳
				شناسایی الگوها	۷/۶۵
		هماهنگی واکنش	۲/۷۲	فعال‌سازی تیم واکنش	۸/۲۲
				تخصیص منابع	۷/۵۴
				هماهنگی و مدیریت بحران	۶/۹۷
		کنترل ریسک	۲/۶۵	شناسایی ریسک‌ها	۸/۱۵
				کاهش ریسک‌ها	۸/۰۶

باتوجه‌به تفاوت میانگین و با مقدار متوسط، همه میانگین‌ها با مقدار متوسط حداکثر بیش از یک واحد تفاوت دارند؛ بنابراین میانگین تمام مؤلفه‌ها در محدوده زیاد و به بالا قرار گرفته و در فاصله اطمینان قرار گرفته و قابل‌تعمیم هستند.

گویه‌های جدول ارزیابی عوامل داخلی و خارجی با استفاده از روش‌های تحلیل کیفی و مستندسازی دانش حفاظت سایبری در قالب پرسش‌نامه در اختیار جامعه آماری داده شد تا با تخصیص ضریب اهمیت، فعلی و مطلوب متغیر بین اعداد ۱ تا ۷ برای هر عامل در مسیر ارزیابی تدوین راهبرد حفاظت سایبری شبکه فرماندهی و کنترل ارتش قرار گرفته و نمرات تخصیص‌یافته موزون شدند. در پایان پس از پردازش موقعیت فعلی و وضعیت مطلوب حفاظت سایبری شبکه فرماندهی و کنترل، احصاء و تعیین شده است.

جدول (۶) جدول ارزیابی عوامل داخلی و خارجی و نمرات موزون

ر	عوامل	ضریب اهمیت	وزن	ضریب وضعیت فعلی	نرمالیزه وضعیت فعلی	ضریب وضعیت مطلوب	نرمالیزه وضعیت مطلوب
جدول ارزیابی عوامل داخلی(IFE) (قوّت و ضعف)							
S1	استفاده از ارتباطات مستقل	۴/۵۰۲	۰/۰۳۲	۳/۳	۰/۱۰	۴	۰/۱۳
S2	جداسازی شبکه‌های عملیاتی	۴/۳۴۵	۰/۰۳۱	۳/۰	۰/۰۹	۴	۰/۱۲
S3	آزمایشگاه‌های ارزیابی امنیتی	۳/۸۲۶	۰/۰۲۷	۳/۶	۰/۱۰	۴	۰/۱۱
S4	بومی‌سازی رویکردها	۴/۲۴۵	۰/۰۳۰	۳/۶	۰/۱۱	۴	۰/۱۲
S5	انگیزه کارآمدی کارکنان	۴/۲۷۳	۰/۰۳۰	۳/۵	۰/۱۱	۴	۰/۱۲
S6	زمینه دانشی در دانشگاه‌ها	۳/۵۲۷	۰/۰۲۵	۳/۵	۰/۰۹	۴	۰/۱۰
S7	رعایت اصل حیطه‌بندی ف ک	۴/۳۸۵	۰/۰۳۱	۳/۶	۰/۱۱	۴	۰/۱۲
S8	اصل طبقه‌بندی ساختار ف ک	۴/۴۵۱	۰/۰۳۱	۳/۸	۰/۱۲	۴	۰/۱۳
S9	رعایت الزامات رصد سایبری	۴/۳۱۵	۰/۰۳۰	۳/۶	۰/۱۱	۴	۰/۱۲
S10	به‌کارگیری کارکنان متخصّص	۳/۷۱۶	۰/۰۲۶	۳/۰	۰/۰۸	۴	۰/۱۰
W1	وابستگی به زیرساخت کشوری	۴/۳۵۵	۰/۰۳۱	۱/۵	۰/۰۵	۲	۰/۰۶
W2	پیچیدگی تنوع تجهیزات	۳/۹۰۴	۰/۰۲۸	۱/۸	۰/۰۵	۲	۰/۰۶
W3	ضعف در پایش و پایشگری	۳/۹۲۳	۰/۰۲۸	۱/۸	۰/۰۵	۲	۰/۰۶
W4	به‌روزرسانی دیرهنگام	۳/۶۷۰	۰/۰۲۶	۰/۵	۰/۰۱	۲	۰/۰۵
W5	پروتکل‌های	۴/۳۱۱	۰/۰۳۰	۰/۵	۰/۰۲	۲	۰/۰۶

	غیربومی						
W6	کافی‌نبودن استانداردها	۴/۳۳۰	۰/۰۳۱	۱/۰	۰/۰۳	۲	۰/۰۶
W7	رویکرد بازیابی پس از حادثه	۴/۴۴۷	۰/۰۳۱	۱/۸	۰/۰۶	۲	۰/۰۶
W8	وجود تجهیزات ناایمن غیربومی	۴/۹۷۰	۰/۰۳۵	۱/۵	۰/۰۵	۲	۰/۰۷
W9	تلفیق کامل پروتکل سامانه‌ها	۴/۱۸۷	۰/۰۳۰	۱/۴	۰/۰۴	۲	۰/۰۶
W10	تأثیرپذیری از آسیب‌های	۳/۶۰۳	۰/۰۲۵	۰/۵	۰/۰۱	۲	۰/۰۵
W11	ضعف در مقوله تاب‌آوری	۴/۲۵۵	۰/۰۳۰	۰/۵	۰/۰۲	۲	۰/۰۶
W12	ضعف دانشی مدیریت تخصصی	۳/۳۵۹	۰/۰۳۱	۱/۰	۰/۰۳	۲	۰/۰۶
W13	ضعف نظارت دقیق به نفوذ	۴/۳۸۴	۰/۰۳۱	۱/۰	۰/۰۳	۲	۰/۰۶
W14	تأثیر تهدیدات ترکیبی فناوری‌های نوین و پیشرفته	۴/۴۱۷	۰/۰۳۱	۰/۵	۰/۰۲	۲	۰/۰۶
جمع		***۱۴۱/۷۹۱***	***۱/۰۰۰***		***۱/۷۵***		***۲/۵۸***
جدول ارزیابی عوامل خارجی(EFE) (فرصت‌ها و تهدیدها)							
O1	انعقاد پیمان‌های دفاع سایبری	۴/۱۶۶	۰/۰۶	۳/۰	۰/۱۸	۴	۰/۲۴
O2	توسعهٔ همکاری مراکز علمی	۴/۲۴۶	۰/۰۶	۳/۳	۰/۲۰	۴	۰/۲۴
O3	ظرفیت کشورهای هم‌سو	۴/۴۸۴	۰/۰۶	۳/۰	۰/۱۹	۴	۰/۲۶
O4	پیاده‌سازی تجهیزات بومی	۴/۳۴۷	۰/۰۶	۳/۶	۰/۲۲	۴	۰/۲۵
O5	تعاملات کشوری و لشکری	۳/۷۰۳	۰/۰۵	۳/۰	۰/۱۶	۴	۰/۲۱
O6	آگاهی و تعهد کاربران	۴/۹۲۵	۰/۰۷	۳/۰	۰/۲۱	۴	۰/۲۸

T1	تهدیدات ناشی از وابستگی	۴/۷۳۳	۰/۰۷	۱/۰	۰/۰۷	۲	۰/۱۴
T2	تهدیدات ناپایداری زیرساخت	۳/۹۲۹	۰/۰۶	۱/۵	۰/۰۸	۲	۰/۱۱
T3	تحریم سامانه‌ها امنیت سایبری	۴/۰۴۳	۰/۰۶	۱/۰	۰/۰۶	۲	۰/۱۲
T4	تغییرات در فناوری‌های نوین	۴/۹۴۱	۰/۰۷	۱/۱	۰/۰۸	۲	۰/۱۴
T5	ناشناختگی تهدیدات آینده	۴/۵۴۴	۰/۰۷	۱/۵	۰/۱۰	۲	۰/۱۳
T6	افزایش قدرت بازیگران سایبری	۳/۲۳۶	۰/۰۴	۱/۵	۰/۰۳	۲	۰/۱۱
T7	تجارب کشورهای همسو	۴/۳۷۲	۰/۰۶	۱/۰	۰/۰۶	۲	۰/۱۳
T8	ظهور تهدیدهای ترکیبی	۴/۵۵۹	۰/۰۷	۱/۵	۰/۱۰	۲	۰/۱۳
جمع کل		***۶۹/۸۷۶***	***۱/۰۱***		***۲/۰۴***		***۲/۸۸***

تعیین موقعیت و اقدام راهبردی

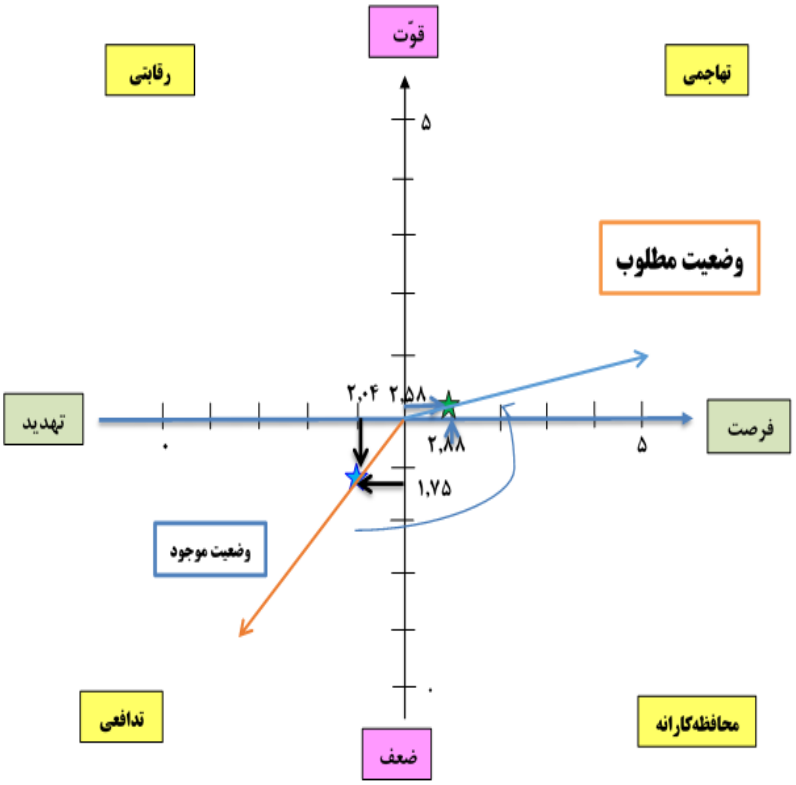
باتوجه‌به اعدادی که برای وضعیت فعلی و مطلوب در جداول ارزیابی عوامل داخلی و خارجی احصاء شد. موقعیت موجود و مطلوب به شرح نمودار بیانگر مطالب زیر است:

الف) وضعیت موجود در ربع تدافعی و وضعیت مطلوب در ربع تهاجمی قرار دارد.

ب) وضعیت موجود نشان می‌دهد که ضعف بیش‌تر از تهدیدات در مقوله حفاظت سایبری مطرح است. این بدان معنا است که آسیب‌پذیری‌های شبکه فرماندهی و کنترل، قابلیت جذب تهدید را در صورت عدم اجرای اقدامات حفاظت سایبری را دارد.

ج) محور **Y** نشان می‌دهد قوّت‌های وضعیت موجود در شرایط مساعدی قرار ندارد و بایستی برای رسیدن به حفاظت سایبری تقویت گردند.

د) وضعیت مطلوب بیشتر معطوف به فرصت‌ها بوده و قوّت‌ها از وزن بالایی برخوردار نیستند؛ لذا در شرایط فعلی اگر بخواهیم به نقطه مطلوب حفاظت سایبری برسیم، باید قوّت‌ها تقویت شوند.



مرحله تطبیق (تدوین راهبرد)

باتوجه‌به چهار دسته راهبُرد ماتریس سوات (شامل راهبُردهای WT,WO,ST,SO) و نظر به منطقه قرارگرفتن در ماتریس داخلی و خارجی، آن دسته از گزاره‌ها جهت ارزیابی و انتخاب در ماتریس برنامه‌ریزی استراتژیک کمّی (QSPM) و دریافت امتیاز جذابیت نسبی راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل انتخاب می‌شوند که در منطقه تعیین‌شده ماتریس داخلی و خارجی باشند. در انتها از تجمیع گزاره‌ها برای مبنای عناصر تدوین راهبرد (اهداف، وسیله و روش) راهبردهای اولویت‌دار تدوین گردیدند. لازم به ذکر است که در هیچ‌کدام از پژوهش‌های پیشین، گزاره‌هایی که بتوان از آن‌ها در تدوین راهبرد حفاظت سایبری شبکه فرماندهی و کنترل استفاده کرد یافت نشد.

جدول (۷) ماتریس زوجی برای احصاء راهبردها

(IFE) (EFE)	نقاط قوّت S- نقاط قوت را فهرست کنید	نقاط ضعف W نقاط ضعف را فهرست کنید
فرصت‌ها – O فرصت‌ها را فهرست کنید	راهبُردهای SO با بهره جستن از قوّت‌ها درصدد بهره‌برداری از فرصت‌ها برآیید	راهبُردهای WO با بهره جستن از فرصت‌ها نقاط ضعف را از بین ببرید.
تهدیدات -T تهدیدات را فهرست کنید	راهبُردهای ST برای احتراز از تهدیدات از نقاط قوّت استفاده کنید	راهبُردهای WT نقاط ضعف را کاهش دهید و از تهدیدات پرهیز کنید

تعیین راهبردهای اصلی و الزامات اجرایی کوتاه‌مدت آن

برای تحقّق حفاظت سایبری شبکه فرماندهی و کنترل ارتش به‌منظور درامان‌ماندن از گزند آسیب‌پذیری‌های ناشناخته آینده، پانزده راهبرد تهاجمی کلی در یک دوره ده‌ساله، شناسایی و پیشنهاد شد که پس از جمع‌بندی بررسی‌های راهبردهای پانزده‌گانه، جامعه آماری سه راهبرد اصلی زیر را دارای قابلیت عملیاتی به همراه الزامات اجرایی کوتاه‌مدت آن تشخیص دادند که به‌منظور اولویت‌بندی بر اساس منطقه تهاجمی در نواحی راهبُرد SWOT، امتیاز جذابیت کسب شده آن‌ها مطابق جدول ۸ احصاء و ارائه می‌گردند.

۱) استفاده از زیرساخت ارتباطی مجزا از مخابرات عمومی، مستقل و امن (به‌منظور تأمین هدف استقلال زیرساخت ارتباطی ارتش، خدمات ارتباطی دریافتی از مخابرات کشوری به‌جای دریافت به‌صورت پهنای باند با ابزار فیبر نوری تاریک پیاده‌سازی گردد).

۲) تغییر رویکرد وابستگی فناورانه به استقلال با ابزار جداسازی سوئیچ‌های ارتباطات پیاده‌سازی شده از سایر سوئیچ‌های خدمات عمومی.

۳) تغییر رویکرد به پیاده‌سازی شبکه جامع یکپارچه انحصاری به‌جای تعدّد شبکه‌های جزیره‌ای و تجهیزات با نشان‌های مختلف

جدول (۸) تعیین امتیاز جذابیت نسبی راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل

			راهبرد (۱)		راهبرد (۲)		راهبرد (۳)	
ر	عوامل	ضریب اهمیت	رتبه	نمره	رتبه	نمره	رتبه	نمره

S1	استفاده از ارتباطات مستقل	۰/۰۴۲	۲	۰/۰۶۴	۲	۰/۰۶۴	۲	۰/۰۶۴
S2	جداسازی شبکه‌های عملیاتی	۰/۰۴۱	۴	۱/۲۴	۲	/۰۶۲	۲	۰/۰۶۲
S3	آزمایشگاه‌های ارزیابی امنیتی	۰/۰۳۷	۳	۰/۰۸۱	۲	۰/۰۵۴	۲	۰/۰۵۴
S4	بومی‌سازی رویکردها	۰/۰۴۰	۳	۰/۰۹	۲	۰/۰۶	۲	۰/۰۶
S5	انگیزه کارآمدی کارکنان	۰/۰۴۰	۲	۰/۰۶	۲	۰/۰۶	۴	۰/۱۲
S6	زمینه دانشی در دانشگاه‌ها	۰/۰۴۵	۲	۰/۰۵	۲	۰/۰۵	۳	۰/۰۷۵
S7	رعایت اصل حیطه‌بندی ف ک	۰/۰۴۱	۲	۰/۰۶۲	۲	۰/۰۶۲	۴	۰/۱۲۴
S8	اصل طبقه‌بندی ساختار ف ک	۰/۰۴۱	۲	۰/۰۶۲	۲	۰/۰۶۲	۴	۰/۱۲۴
S9	رعایت الزامات رصد سایبری	۰/۰۴۰	۲	۰/۰۶	۲	۰/۰۶	۴	۰/۱۲
S10	به‌کارگیری نیروی انسانی متخصّص	۰/۰۴۶	۲	۰/۰۵۲	۲	۰/۰۵۲	۳	۰/۰۷۸
W1	وابستگی به زیرساخت کشوری	۰/۰۵۱	۳	۰/۰۹۳	۲	۰/۰۶۲	۲	۰/۰۶۲
W2	پیچیدگی به علّت تنوع تجهیزات	۰/۰۳۸	۴	۰/۱۱۲	۲	۰/۰۵۶	۲	۰/۰۵۶
W3	ضعف در پایش و پایشگری	۰/۰۳۶	۴	۰/۱۰۴	۲	۰/۰۵۲	۲	۰/۰۵۲
W4	به‌روزرسانی دیرهنگام سیستم‌ها	۰/۰۲۸	۲	۰/۰۵۶	۲	۰/۰۵۶	۲	۰/۰۵۶
W5	استفاده از پروتکل‌های غیربومی	۰/۰۳۵	۴	۰/۱۲	۲	۰/۰۶	۲	۰/۰۶
W6	کافی‌نبودن استانداردهای امنیتی	۰/۰۳۶	۴	۰/۱۰۴	۲	۰/۰۵۲	۲	۰/۰۵۲
W7	نبود رویکرد بازیابی پس از حادثه	۰/۰۳۵	۴	۰/۱۲	۲	۰/۰۶	۲	۰/۰۶
W8	وجود تجهیزات ناایمن غیربومی	۰/۰۴۰	۴	۰/۱۲	۲	۰/۰۶	۲	۰/۰۶

W9	عدم تلفیق کامل پروتکل سامانه‌ها	۰/۰۴۱	۴	۰/۱۲۴	۲	۰/۰۶۲	۲	۰/۰۶۲
W10	تأثیرپذیری از آسیب‌های فاوایی	۰/۰۴۲	۴	۰/۱۲۸	۲	۰/۰۶۴	۲	۰/۰۶۴
W11	ضعف در مقوله تاب‌آوری	۰/۰۴۱	۴	۰/۱۲۴	۲	۰/۰۶۲	۲	۰/۰۶۲
W12	ضعف دانش مدیریت تخصصی	۰/۰۴۵	۲	۰/۰۷	۲	۰/۰۷	۲	۰/۰۷
W13	ضعف نظارت دقیق به نفوذ	۰/۰۴۰	۲	۰/۰۶	۲	۰/۰۶	۴	۰/۱۲
W14	تأثیرپذیری از تهدیدات ترکیبی	۰/۰۴۵	۲	۰/۰۵	۲	۰/۰۵	۴	۰/۱
	جمع	***Σ=۱***		***۴/۰۳۶***		***۲/۳۲۷***		***۲/۷۰۷***
O1	انعقاد پیمان‌های دفاع سایبری	۰/۰۸	۲	۰/۱۲	۴	۰/۲۴	۲	۰/۱۲
O2	توسعهٔ همکاری مراکز علمی	۰/۰۷	۴	۰/۲۴	۲	۰/۱۲	۲	۰/۱۲
O3	ظرفیت کشورهای هم‌سو	۰/۰۷	۴	۰/۲۴	۴	۰/۲۴	۲	۰/۱۲
O4	امکان پیاده‌سازی تجهیزات بومی	۰/۰۸	۴	۰/۲۴	۲	۰/۱۲	۲	۰/۱۲
O5	تعاملات سازنده کشوری و لشکری	۰/۰۷	۴	۰/۲	۲	۰/۱	۲	۰/۱
O6	زمینه ارتقای آگاهی و تعهد کاربران	۰/۰۸	۴	۰/۲۸	۲	۰/۱۴	۲	۰/۱۴
T1	تهدیدات ناشی از وابستگی	۰/۰۹	۲	۰/۱۴	۴	۰/۲۸	۲	۰/۱۴
T2	تهدیدات کیفیت ناپایدار زیرساخت	۰/۰۹	۴	۰/۲۸	۴	۰/۲۸	۲	۰/۱۴
T3	تحریم سامانه‌های امنیت سایبری	۰/۰۷	۳	۰/۱۸	۴	۰/۲۴	۲	۰/۱۲
T4	سرعت تغییرات در فناوری‌های نوین	۰/۰۸	۴	۰/۲۴	۳	۰/۱۸	۲	۰/۱۲
T5	ناشناختگی تهدیدات آینده سایبری	۰/۰۸	۲	۰/۱۴	۴	۰/۲۸	۲	۰/۱۴

T6	افزایش قدرت بازیگران سایبری	۰/۰۸	۴	۰/۲۸	۳	۰/۲۱	۲	۰/۱۴
T7	تجارب کشورهای همسو	۰/۰۵	۴	۰/۱۶	۲	۰/۰۸	۲	۰/۰۸
T8	ظهور تهدیدهای سایبری ترکیبی	۰/۰۸	۲	۰/۱۲	۲	۰/۱۲	۳	۰/۱۲
جمع		$\Sigma = 1$		۳/۲۴		۳/۱۳		۲/۲۴
مجموع نمره‌های جذابیت		$\boldsymbol{\Sigma = 2}$		***۷/۲۷۶***		***۵/۴۵۷***		***۴/۹۴۷***

اولویت‌بندی راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش

با احصاء مجموع امتیاز جذابیت کسب شده برای هر یک از اولویت‌ها، اولویت‌بندی به شرح زیر برای راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش احصاء شده است.

جدول (۹) راهبردهای حفاظت سایبری شبکه فرماندهی و کنترل ارتش بر اساس اولویت

ردیف	اولویت	راهبردها	امتیاز
۱	۱	استفاده از زیرساخت ارتباطی مجزا از مخابرات عمومی، مستقل و امن شبکه	۷/۲۷۶
۲	۲	تغییر رویکرد وابستگی فناورانه به استقلال با ابزار جداسازی سوئیچ‌های ارتباطات پیاده‌سازی شده از سایر سوئیچ‌های خدمات عمومی	۵/۴۵۷
۳	۳	تغییر رویکرد به پیاده‌سازی شبکه جامع یکپارچه انحصاری به‌جای تعدد شبکه‌های جزیره‌ای و تجهیزات با نشان‌های مختلف	۴/۹۴۷

بحث و نتیجه‌گیری:

یافته‌های این پژوهش، در مقایسه با مطالعات پیشین، تمایزات و نوآوری‌های کلیدی به شرح زیر را در زمینه حفاظت سایبری شبکه‌های فرماندهی و کنترل نشان می‌دهد.

عدم جامعیت و قابلیت انطباق مطالعات پیشین: برخلاف تحقیقات و اسناد اشاره‌شده در مرور پیشینه مانند ردیف ۱، ۳ و ۵ که عمدتاً بر امنیت سایبری کشورهای پیشرفته یا نهادهای بین‌المللی تمرکز دارند و فاقد قابلیت انطباق با شرایط بومی (وابستگی‌های فناورانه و تجهیزاتی) هستند، این مطالعه به‌طور مشخص بر بومی‌سازی راهبرد حفاظت سایبری برای شبکه فرماندهی و کنترل ارتش تمرکز کرده است. ماهیت دفاعی و حیاتی

این شبکه، نیازمند رویکردی پیشگیرانه و متمایز از مقوله امنیت سایبری عمومی است تا از آسیب‌پذیری‌های ناشی از «غفلت ذهنی» یا وابستگی‌های خارجی جلوگیری شود.

ارتباط متغیرها با حفاظت سایبری شبکه فرماندهی و کنترل: الگوی راهبردی ردیف اول پیشینه، هم‌راستا با نیازهای شبکه فرماندهی و کنترل نیستند. بااین‌حال، از چارچوب کلی آن برای تحلیل محیط داخلی و خارجی حفاظت سایبری استفاده شده است.

تفاوت در پذیرش تهدید و نفوذ: مدل‌سازی امنیت سایبری در پیشینه ردیف چهارم که بر اصولی مانند «قابلیت جذب» و «پذیرش نفوذ» تأکید دارد، با ویژگی «حفاظت سایبری» در شبکه فرماندهی و کنترل در تضاد است. شبکه فرماندهی و کنترل نیازمند سلب هرگونه نفوذ و دوری از هرگونه حمله سایبری است، نه صرفاً مدیریت آن.

محدودیت برون‌سپاری در شبکه فرماندهی و کنترل: طرح «حفاظت از زیرساخت‌های ملّی آمریکا» بر مشارکت گسترده ذی‌نفعان (دولتی، صنعتی، دانشگاهی) تأکید دارد. این رویکرد در شبکه فرماندهی و کنترل ارتش به دلیل اصل محرمانگی و حیطه‌بندی اطلاعات، امکان‌پذیر نبوده و مفهوم حفاظت سایبری این شبکه، در آن سند مغفول مانده است.

تکمیل راهبردهای کلی: اقدامات نُه‌گانه آژانس امنیت اطلاعات اتحادیه اروپا (ردیف ششم)، دستورالعمل‌های کلی ارائه داده که فاقد جزئیات اجرایی لازم برای تدوین راهبرد حفاظت سایبری شبکه فرماندهی و کنترل است. این پژوهش با الهام از محتوای کلی آن (شناسایی محیط داخلی و خارجی)، به تدوین راهبردهای مشخص‌تر پرداخته است.

نوآوری در مدل‌سازی حفاظت سایبری: این مطالعه با افزودن تمرکز بر شناسایی عوامل خارجی مختص محیط سایبری ارتش، راهبردهای حفاظت سایبری را در محیط پیچیده فرماندهی و کنترل بررسی و آن را فراتر از یک مدل نظری صرف مانند مدل چهارمرحله‌ای اتحادیه بین‌المللی ارتباطات، به سمت عملیاتی‌شدن سوق داده است.

برخلاف مطالعات پیشین که عمدتاً به تحلیل آسیب‌پذیری‌ها مدل‌های عمومی امنیت سایبری پرداخته‌اند و فاقد کاربرد مستقیم در زمینه شبکه‌های فرماندهی و کنترل نظامی بودند، این پژوهش با بهره‌گیری از ابعاد چهارگانه اتحادیه جهانی مخابرات و تلفیق آن با نیازهای خاص شبکه فرماندهی و کنترل ارتش، یک شکاف دانشی کلیدی را پر می‌کند. یافته‌های این تحقیق نشان می‌دهند که ضعف ذاتی در زیرساخت ارتباطی و نه صرفاً

شدّت تهدیدات، عامل اصلی ریسک در شبکه فرماندهی و کنترل ارتش است. این تمرکز بر آسیب‌پذیری به‌جای تهدید، یک تفاوت پارادایمی نسبت به رویکردهای گذشته است که عمدتاً بر دفع تهدیدات شناخته شده متمرکز بودند، درحالی‌که اولویت‌های راهبردی ما بر تقویت ظرفیت درونی شبکه در برابر تهدیدات ناشناخته آینده تأکید دارد.

برابر یافته‌های پژوهش، در شرایط فعلی اگر بخواهیم به نقطه مطلوب حفاظت سایبری برسیم، باید قوّت‌ها تقویت شوند؛ بنابراین اگر بخواهیم به نقطه آرمانی رسیده و حفاظت سایبری شبکه فرماندهی و کنترل ارتش را ارتقا دهیم باید هم‌زمان علاوه بر دفع تهدیدات سایبری آینده به استفاده از فرصت‌ها توجه ویژه داشت و در این راستا جهت جلوگیری از آسیب‌پذیری تهدیدهای ناشناخته آینده، دستیابی به راهبردهای زیر احصاء و اولویت‌بندی شده‌اند که اقدامات کوتاه‌مدت آن‌ها در ادامه برای اجرا تأکید شده‌اند.

اولویت اول: استفاده از زیرساخت ارتباطی مجزا از مخابرات عمومی، مستقل و امن شبکه

اولویت دوم: تغییر رویکرد وابستگی فناورانه به استقلال با ابزار جداسازی سوئیچ‌های ارتباطات پیاده‌سازی شده از سایر سوئیچ‌های خدمات عمومی

اولویت سوم: تغییر رویکرد به پیاده‌سازی شبکه جامع یکپارچه انحصاری به‌جای تعدّد شبکه‌های جزیره‌ای و تجهیزات با نشان‌های مختلف،

اقدام عملیاتی اول: تدوین برنامه فنی و تخصیص بودجه (ظرف ۳ سال) برای گام اول مهاجرت ترافیک حیاتی شبکه فرماندهی و کنترل به مسیر ارتباطی مبتنی بر فیبر نوری اختصاصی و یا لینک‌های رادیویی امن که کاملاً از شبکه مخابرات عمومی تفکیک شده‌اند.

اقدام عملیاتی دوم: انجام یک ممیزی امنیتی تفصیلی از تمامی سوئیچ‌های موجود (ظرف یک سال) و اجرای جداسازی فیزیکی/منطقی سوئیچ‌های شبکه از سوئیچ‌های عمومی در تمامی نقاط بحرانی (تکمیل گام حذف وابستگی در مناطق کم‌خطر ظرف دو سال).

اقدام عملیاتی سوم: تشکیل کارگروه استانداردسازی (ظرف یک سال) و تعریف یک پلتفرم تجهیزات استاندارد و یکپارچه برای شبکه فرماندهی و کنترل و تهیه یک برنامه پنج‌ساله (با گام‌های اجرایی سالانه) برای جایگزینی تدریجی تجهیزات جزیره‌ای فعلی.

پیشنهادها

پیشنهاد می‌گردد:

۱- از مجموعه مخابرات کشوری، موارد زیر را پیگیری و به نتیجه برسد.

الف- دریافت خدمات ارتباطی از طریق فیبر نوری تاریک.
ب- جداسازی سوئیچ‌های ارتباطات پیاده‌سازی سازمانی از سوئیچ‌های خدمات عمومی.
۲- باتوجه‌به وابستگی زیرساخت تجهیزاتی سایبری در اکثر سازمان‌ها و نهادها به تجهیزات غیربومی، تسریع در بازنگری در نگرش‌ها به‌منظور گذر از تعدّد تجهیزات وارداتی و رعایت اصل سادگی و رفع پیچیدگی با اتّکا به تجهیزات بومی پیشنهاد می‌شود.
۳- مبادی پژوهشی، کیفیت اجرای الزامات حفاظت سایبری از جمله نیروی انسانی متبحّر، زیرساخت فنی، منابع بودجه‌ای و... را به‌صورت پژوهش مجزا بررسی نماید.
۴- جهت رفع حس کاذب امنیت ذهنی، آسیب‌پذیری‌های احتمالی شبکه فرماندهی و کنترل شناسایی و ضرورت اقدام حفاظت سایبری را به‌عنوان وظیفه همگانی تبیین و تشریح گردد.
۵- با بهره‌گیری از ظرفیت‌های دانشی سازمان‌ها، دانشگاه‌ها و مراکز علمی کشور، نسبت به ارتقای مقوله حفاظت سایبری شبکه فرماندهی و کنترل، اقدام گردد.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱- جداسازی شبکه فرماندهی و کنترل از مخابرات عمومی کشوری
۲- فرهنگ‌سازی فرماندهان و مدیران در خصوص عواقب خطرناک توهّم امنیت سایبری
۳- بررسی عینی نقصان حفاظت سایبری شبکه‌ها به‌جای تکیه ذهنی به امنیت سایبری
۴- جلوگیری از تعدّد دارایی سایبری به‌منظور رعایت اصل سادگی و عدم پیچیدگی سایبری

تشکر و قدردانی:
از همه اساتید و عزیزانی که با مشاوره خود، پژوهشگر را یاری نمودند تشکر و قدردانی دارم.

تضاد منافع:
بدین‌وسیله نویسندگان این مقاله تصریح دارند که هیچ‌گونه تضاد منافع در انجام این پژوهش وجود ندارد.

منابع:

الف- منابع فارسی

- آذر، داوود. مسلمی، حسین و پرتوی، محمدتقی (۱۴۰۱)، راهبردهای قدرت سایبری ارتش جمهوری اسلامی ایران، فصلنامه آینده پژوهی دفاعی، دوره ۷، شماره ۲۷، زمستان ۱۴۰۱، صفحه ۶۳-۸۲. (https://doi.org/۱۰.۲۲۰۳۴/dfsr.۲۰۲۳.۱۹۸۳۴۴۹.۱۶۶۷)
- افتخاری، اصغر (۱۴۰۲)، ساختار قدرت نرم. رساله دکتری، دانشگاه علامه طباطبایی.
- البرزنیا، حمیدرضا (۱۴۰۲)، ارتقای سامانه فرماندهی و کنترل، چاپ سوم، تهران، انتشارات جهاد دانشگاهی.(https://civilica.com/doc/۱۴۲۴۰۴۷)
- ایجابی، ابراهیم. حافظزاده، مهران. نامداری، نوید و کریمیان، رضا (۱۴۰۴)، سناریوی محتمل تهدیدهای نظامی رژیم صهیونیستی علیه ایران، فصلنامه آینده پژوهی دفاعی، دوره ۱۰، شماره ۳۶، بهار ۱۴۰۴، صفحه ۱۶۷-۲۰۳ (https://doi.org/۱۰.۲۲۰۳۴/dfsr.۲۰۲۴.۲۰۴۷۱۲۶.۱۸۵۸)
- جلالی، غلامرضا (۱۴۰۲)، اصول و مبانی پدافند سایبری، چاپ دوم، تهران، انتشارات نبوی. (https://www.gisoom.com/book/۱۹۷۶۳۵۸)
- گروه مؤلفین دافوس آجا (۱۴۰۳)، مدیریت راهبردی و فرایند تدوین راهبرد، چاپ دوم، تهران، انتشارات دانشگاه فرماندهی و ستاد ارتش.
- محمدزهرایی، سپهر. موحدی صفت، محمدرضا، نوروزانی، شهرام و بیگدلی، وحید (۱۴۰۴)، اجزاء سامانه بازی جنگ راهبردی سایبری نیروهای مسلح ایران، فصلنامه علمی علوم و فنون نظامی، دوره ۲۱، شماره ۷۳، پاییز ۱۴۰۴، صفحه ۴۱-۷۵ (https://doi.org/۱۰.۲۲۰۳۴/qjmst.۲۰۲۵.۲۰۲۰۳۵۱.۲۰۰۴)
- نصرت‌آبادی، جمشید، (۱۳۹۸)، ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح ج.ا.ا، رساله دکتری تخصصی دانشگاه دفاع ملّی.
- یزدانی‌چهاربرج، رحیم (۱۳۹۸)، الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران، رساله دکتری تخصصی، دانشگاه عالی دفاع ملی.

ب– منابع انگلیسی

- Adrian Venables, Siraj Ahmed Shaikh and James Shuttleworth, (2021), A MODEL FOR - Cyber Space Operation Air Force Doctrine Document.
- Alborznia, H. (2023). *Improving the command and control system* (3rd ed.). University Jihad Publications. https://civilica.com/doc/1424047 [in Persian]
- Azar, D., Moslemi, H., & Partovi, M. T. (2023). Cyber power strategies of the Army of the Islamic Republic of Iran. *Defense Future Studies Quarterly*, *7*(27), 63–82. https://doi.org/10.22034/dfsr.2023.1983449.1667 [in Persian]
- DAFOUS AJA Authors Group. (2024). *Strategic management and the strategy formulation process* (2nd ed.). Army Command and Staff University Press. [in Persian]
- Eftekhari, A. (2023). *The structure of soft power* (Doctoral dissertation, Allameh Tabataba'i University). [in Persian]
- Eric Luiijf, (2021), "Towards a European Research Agenda for CIIP: Results from the CI2RCO Project", Springer Berlin Heidelberg, PP 1-12.
- Euisun Paik, Heung Youl Youm, (2021), " Knowledge Sharing Series Cybersecurity", APCICT Publication, PP 1-108.
- Geluvaraj B. P. M. Satwik and T. A. Ashok Kumar, (2020), "The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace", International Conference on Computer Networks,p738.(https:// d-9783030455408-9783030455415.html)
- Ijabi, E., Hafezzadeh, M., Namdari, N., & Karimian, R. (2025). Probable scenario of Israeli military threats against Iran. *Defense Future Studies Quarterly*, *10*(36), 167–203. https://doi.org/10.22034/dfsr.2024.2047126.1858 [in Persian]
- ITU Cybersecurity Team (2022), Global Cybersecurity Index (GCI),Telecommunication Development Bureau.(https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx)
- Jalali, G. (2023). *Principles and foundations of cyber defense* (2nd ed.). Nabavi Publications. https://www.gisoom.com/book/1976358 [in Persian]
- Jc jansen van vuuren, (2021), "Building Blocks for National Cyberpower" Boston University of the United States.
- Kim Hyung Jong, (June 2020),Understanding of Korean Critical Information Infrastructure Protection,Seoul Women University Report.
- Mohammadzahraei, S., Movahedi Sefat, M. R., Norouzani, S., & Bigdeli, V. (2025). Components of the strategic cyber war-gaming system of the Iranian Armed Forces. *Journal of Military Science and Technology*, *21*(73), 41–75. https://doi.org/10.22034/qjmst.2025.2020351.2004 [in Persian]
- NIST, (2020), " NIST Cloud Computing Security Reference Architecture - NIST Special Publication 500-299", 1-204.
- Nosratabadi, J. (2019). *Presenting a strategic model for evaluating the cyber power of the Armed Forces of the Islamic Republic of Iran* (Doctoral dissertation, National Defense University). [in Persian]

- Satola, T. Mądziel, M. & Wójtowicz, S. (2017). Cybersecurity in Local Government Units in Poland – Problems and Recommendations. In: Proceedings of the 12th International Conference on Cyber Warfare and Security (ICCWS 2017), pp. 318–326.
- Serkim Hyung Jong, (June 2024),Understanding of Korean Critical Information Infrastructure Protection,Seoul Women University Report.
- Sgantzos Konstantinos, Grigg Ian, (2020), "Artificial Intelligence Implementations on the Blockchain. Use Cases and Future Applications.
- -U.S. Cyber Command, (2021), Organizing For Cyberspace Operations, Committee On Armed.(https://www.cybercom.mil)
- Velasquez, (2021), "A Comprehensive Instrument for Identifying Critical Information Infrastructure Services", TARTU UNIVERSITY, pp 1-56.
- Yazdani Chaharborj, R. (2019). *A strategic model for cyber protection of critical information infrastructure of the Islamic Republic of Iran* (Doctoral dissertation, Supreme National Defense University). [in Persian]

پ – وبگاه‌ها

- Source: IEEE-USA. Available at http://www.ieeeusa.org/policy/positions/infoinfrastructure.html tions/infoinfrastructure.html
- http://tadviser.com/index.php/Article:Law_On_security_of_critical_information_infrastructure_of_the_Russian_Federation