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

Resilience in future cyber command and control

Mohammad Ghasemi Tadavani[1] | Sajad Alimohammadi[2]✉
Mohammad Haji ali akbari[3]

1. Instructor of Cyber and Electronic Warfare, IRI Military Command and Staff University, Tehran, Iran. E-mail: m.ghasemi@casu.ac.ir
2. Instructor of Cyber and Electronic Warfare, IRI Military Command and Staff University, Tehran, Iran. (Corresponding Author) E-mail: s.alimohammadi33@casu.ac.ir
3. Instructor of Crisis Management, IRI Military Command and Staff University, Tehran, Iran. E-mail: M.hajaliakbari@casu.ac.ir

Article Info

Article type:
Research Article

Article history:
Received:
2024-11-19
Received in revised form: 2025-1-2
Accepted;
2025-1-4
Published online:
2025-2-19

Keywords:
command and control,
adaptive resilience,
Responsive response

ABSTRACT

Background and Aim: This research aims to provide resilience features for future cyber command and control (C2).

Methodology: The research employs a descriptive method combining qualitative and quantitative approaches. In the qualitative phase, data were collected through a review of relevant and credible documents as well as interviews with experts knowledgeable about the subject. This data was analyzed using TI Atlas software and the content analysis method. The indicators were evaluated across two dimensions: adaptive resilience and resilient responsiveness. Indicators with a Content Validity Index (CVI) greater than 0.79 were considered validated. In the quantitative phase, these indicators were ranked using SPSS software and the Friedman test to determine the priority of features necessary for achieving resilience in future cyber C2.

Findings: Resilience in future cyber C2 is categorized into two dimensions: adaptive resilience and resilient intelligence. A total of 54 indicators were identified across these two dimensions: adaptive resilience (including accurate prediction and effective resistance) and resilient response (including effective response and rapid repair and recovery).

Conclusion: To achieve accurate forecasting and maintain the integrity of cyber resources, it is essential to utilize automated systems and artificial intelligence. Key actions include threat monitoring, fostering cyber mobility, avoiding reliance on a single system, and promoting diversity among systems to enhance adaptive resilience. Regarding a resilient response, it is crucial to isolate vulnerable resources, ensure operational continuity, analyze incidents, and distribute responsibilities effectively. Additionally, rapid repair and recovery through fallback, rebuilding, or replacement strategies, along with the application of survivability engineering, are vital for addressing cyber incidents.

Cite this article: Ghasemi Tadavani, M. Ali Mohammadi, S. and Haji Ali Akbari, M. (2025). Resilience in future cyber command and control. Defensive Future Studies, 9(35), 27- 60.

DOI: 10.22034/dfsr.2025.2046026.1852

Publisher: IRI Military Command and Staff University

Extended Abstract

INTRODUCTION

The rapid adoption of information technologies such as electronics and telecommunications infrastructure has transformed the operational environment of military forces and created cyberspace as a global arena for information exchange (U.S. Department of Defense, 2014:63). Due to its emerging capabilities, cyberspace has become a significant enabler of military power for nations and has paved the way to achieving superior power through advanced cyber technologies. Despite its extensive capabilities, this space has also introduced new threats and crises due to its specific characteristics, such as ease of access (Ghasemi et al, 2023).

Command and control in cyberspace present numerous challenges due to the uniqueness of this environment and its differences from physical domains. Traditional structures are ineffective in this space, and the ease of access to information has increased the potential for infiltration and disruption by adversaries (U.S. Joint Chiefs of Staff, 2016: 49-50). Cyber resilience is proposed as a solution to counter these threats, ensuring the ability of systems to carry out missions even under conditions of enemy infiltration. This research aims to identify the characteristics of resilience in cyber command and control for the future battlefield (US Department of Homeland Security, 2018: 8-10; Thomas H, Hedgecock, 2021).

METHODOLOGY

This research was applied and conducted with a mixed-methods approach. Data collection was carried out using both library and field methods. In the library method, data were extracted and classified from credible sources such as books, scientific articles, journals, and websites related to cyber command and control. In the field method, six specialists with over twenty years of experience in the cyber domain and command and control were interviewed. For the quantitative method, the statistical population included 146 experts with at least 15

years of experience in ICT and cyber defense, from which 106 individuals were randomly selected using Cochran's formula.

In the qualitative approach, content analysis of documents and interviews was performed using Atlas. Ti software. This analysis involved identifying both hidden and explicit messages, comparing data, and discovering internal relationships among them. To confirm the validity of the tools, the indicators of the questionnaire were examined by calculating the Content Validity Index (CVI), resulting in the selection of 54 final indicators from an initial 61, all with a score exceeding 0.79. In the quantitative analysis, data were collected using a Likert scale and analyzed with SPSS software. Cronbach's alpha of 0.924 indicated the reliability of the questionnaire, and the ranking of indicators was conducted using the Friedman test.

RESULTS

Research has shown that cyber resilience in command and control encompasses four main dimensions: accurate forecasting, effective resistance, efficient response, and rapid recovery and restoration. These dimensions were derived through content analysis of documents, interviews with experts, and data analysis. Accurate forecasting involves the use of artificial intelligence to analyze and predict cyber threats and enhance automated and intelligent systems. Effective resistance focuses on strengthening infrastructures, employing advanced security techniques, and creating diversity within command-and-control systems. These findings underscore the importance of planning and defensive strategies in countering cyber-attacks.

Based on statistical analyses, indicators related to the dimensions of cyber resilience were ranked. Inaccurate forecasting, indicators such as assessing the status of cyber resources and utilizing autonomous systems received high rankings. Ineffective resistance, indicators like risk management, and the use of advanced equipment scored the highest. In the dimension of efficient response, indicators such as preparedness for crisis management and rapid response to threats were prominent. Additionally, in rapid recovery and restoration, indicators

such as system reconstruction and the use of survival engineering were emphasized.

The conceptual model of the research presented the dimensions and components of cyber resilience for command and control in cyberspace. This model demonstrated that enhancing forecasting, improving resistance, increasing responsiveness, and accelerating system recovery can significantly improve cybersecurity. These findings are applicable in designing cyber defense strategies, particularly in military command and control centers. This model can be utilized to assess the state of cyber resilience in organizations and provide appropriate solutions to address future threats.

DISCUSSION AND CONCLUSIONS

Resilience in future cyber command and control is the outcome of two dimensions: adaptive resilience and resilient responsiveness. The most critical factor for achieving accurate forecasting is the ability to assess the current status of cyber resources in real time. This is facilitated by the automation and autonomy of systems enhanced by nonlinear machine intelligence, which enables automated analysis through artificial intelligence. On the other hand, to establish effective resistance, the most important actions include monitoring and situational awareness of threats, creating mobility capabilities for cyber assets, avoiding reliance on a single command-and-control system, and establishing redundancy and diversity within the command-and-control systems. Therefore, accurate forecasting is achieved, and based on that, effective resistance is implemented; thus, adaptive resilience in cyber command and control is established. However, completing the resilience of cyber command and control requires the existence of resilient responsiveness. The most important characteristics of the effective response component in this dimension include the separation of vulnerable resources, maintaining continuity of cyber operations, analyzing reported incidents, and distributing responsibilities in the face of cyber incidents. Another component of this dimension is the rapid recovery and restoration from cyber incidents, which necessitates

the use of a restoration strategy. Depending on the extent and type of damage, one of the strategies of return, reconstruction, or replacement is selected. The application of the survival engineering principle with a balanced proactive strategy and an optimized reactive strategy ranks next in importance in this field.

REFERENCES

- Ghasemi, M. Azar, D. and Sajjadi Asil, V. (2019). Model for evaluating the cyber offensive power of the Islamic Republic of Iran Army. Military Sciences and Technologies, 35-61, 19. (64). [in Persian]
- U.S. Department of Defense. (2014). Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. Retrieved from: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, 63.
- U.S. Joint Chiefs of Staff. (2016). Cross Domain Synergy in Joint Operations Planner's Guide, (Washington, DC: U.S. Joint Chiefs of Staff), 49-50.
- US Department of Homeland Security. (2018). Cyber Resilience and Response, Public-Private Analytic Exchange Program, PP 8-10

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: X ۲۵۸۸-۴۲۸ شاپای الکترونیکی: ۲۶۴۵-۷۱۷۲ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد آجا

تاب‌آوری در فرماندهی و کنترل سایبری آینده

محمد قاسمی تادوانی[۱] | سجاد علی محمدی[۲]✉ | محمد حاجی علی اکبری[۳]

۱. مربی جنگال و سایبر، دانشگاه فرماندهی و ستاد ارتش، تهران، ایران. رایانامه: m.ghasemi@casu.ac.ir
۲. مربی جنگال و سایبر، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: s.alimohammadi33@casu.ac.ir
۳. مربی مدیریت بحران، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: M.hajaliakbari@casu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخچه مقاله:
تاریخ دریافت:
۱۴۰۳/۰۸/۲۹
تاریخ بازنگری:
۱۴۰۳/۱۰/۱۳
تاریخ پذیرش:
۱۴۰۳/۱۰/۱۵
تاریخ انتشار:
۱۴۰۳/۱۲/۰۱

کلیدواژه‌ها:
فرماندهی‌وکنترل، تاب‌آوری تطبیقی، پاسخگویی تاب‌آور

چکیده

زمینه و هدف: این پژوهش با هدف ارائه ویژگی‌های تاب‌آوری در فرماندهی و کنترل سایبری آینده انجام شده است.

روش: روش تحقیق توصیفی با رویکرد کیفی و کمّی است. در بخش کیفی داده‌ها با بررسی اسناد و مدارک مرتبط و معتبر و مصاحبه با خبرگان آشنا به موضوع جمع‌آوری شد. این داده‌ها به کمک نرم‌افزار اطلس. تی.آی و به روش تحلیل مضمون بررسی شدند. شاخص در دو بُعد تاب‌آوری تطبیقی و پاسخگویی تاب‌آور احصا شد. شاخص‌هایی که دارای CVI بیش از ۰/۷۹ بودند تأیید شدند. در بخش کمّی این شاخص‌ها با استفاده از نرم‌افزار SPSS و محاسبه آزمون فریدمن رتبه‌بندی شدند و برای دستیابی به تاب‌آوری در فرماندهی و کنترل سایبری آینده اولویت ویژگی‌ها مشخص شد.

یافته‌ها: تاب‌آوری در فرماندهی و کنترل سایبری آینده به دو بُعد تاب‌آوری تطبیقی و پاسخگویی تاب‌آور تقسیم می‌شود. ۵۴ شاخص در دو بعد تاب‌آوری تطبیقی (شامل پیش‌بینی صحیح و مقاومت اثربخش) و بُعد پاسخگویی تاب‌آور (شامل واکنش مؤثر و ترمیم و بازیابی سریع) احصا شد.

نتیجه‌گیری: برای دستیابی به پیش‌بینی صحیح و به‌روزرسانی وضعیت منابع سایبری، استفاده از سامانه‌های خودکار و هوش مصنوعی ضروری است. اقداماتی مانند نظارت بر تهدیدها، ایجاد قابلیت تحرک سایبری، عدم وابستگی به یک سیستم واحد و ایجاد تنوع در سامانه‌ها، باعث تقویت تاب‌آوری تطبیقی می‌شود. در بعد پاسخگویی تاب‌آور، جداسازی منابع آسیب‌پذیر، حفظ تداوم عملیات، تحلیل رویدادها و تقسیم مسئولیت‌ها اهمیت دارد. همچنین، ترمیم و بازیابی سریع با استفاده از راهبردهای بازگشت، بازسازی یا جایگزینی و بهره‌گیری از مهندسی بقا برای مقابله با رخدادهای سایبری ضروری است.

استناد: قاسمی تادوانی، محمد؛ علی محمدی، سجاد و حاجی علی‌اکبری، محمد. (۱۴۰۳). تاب‌آوری در فرماندهی و کنترل سایبری آینده. آینده‌پژوهی دفاعی، ۹(۳۵)، ۲۷- ۶۰.

DOI: 10.22034/dfsr.2025.2046026.1852

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

محیطی که نیروهای نظامی در آن فعالیت می‌کنند با توسعه سریع و پذیرش فناوری‌های اطلاعاتی مانند الکترونیک، زیرساخت‌های مخابراتی تغییر کرده است. استفاده از این فناوری‌ها باعث ایجاد محیطی به نام فضای سایبری شده است (U.S. Department of Defense, 2014:63). فضای سایبر یک محیط جهانی برای تبادل پویای اطلاعات است که بر همه جنبه‌های زندگی تأثیر می‌گذارد. در دوران معاصر، جهت‌گیری اولویت‌های راهبردی کشورها، برای نیل به قدرت فائقه، به سمت بهره‌برداری از فضای سایبر تغییریافته و فناوری‌های پیشرفته سایبری، زمینه‌ساز تجدید بنای قدرت ملی در قالب قدرت سایبری شده است. از سویی دیگر، فناوری‌های اطلاعاتی نوظهور، قابلیت‌ها و توانمندی‌های جدیدی را در اختیار قرار داده که محیط عملیاتی را تغییر داده‌اند و فضای سایبری را به‌عنوان یک توانمندساز و تسهیل‌کننده با تأثیر به‌سزا در قدرت نظامی کشورها مطرح کرده‌اند. همچنین ویژگی‌های این فضا احتمال وجود دشمن در آن را بالا می‌برد و زمینه بروز بحران‌ها را افزایش می‌دهد (قاسمی و همکاران، ۱۴۰۲: ۲۱).

فرماندهی و کنترل، اعمال اقتدار و هدایت توسط یک فرمانده بر قوای تعیین‌شده و وابسته، برای انجام‌دادن کامل مأموریت است (Department of Defense, 2018; XXii). تلاش‌ها برای تطبیق روش‌های فرماندهی و کنترل از حوزه‌های فیزیکی به حوزه سایبری وجود داشته و در حال تکمیل‌شدن است. استفاده از ساختارهای سنتی فرماندهی و کنترل نظامی در این حوزه به دلیل منحصربه‌فرد بودن فضای سایبری و متفاوت‌بودن از سایر حوزه‌ها منجر به مشکلات متعددی می‌شود؛ زیرا کنترل و نظارت بر فضای سایبر به دلیل سهولت دسترسی، دشوار است و به دشمنان نیز اجازه می‌دهد تا به‌راحتی به این اطلاعات دسترسی داشته باشند و قادرند عملیات مراکز مهم، حساس و حیاتی را از هر مکانی مختل کنند (U.S. Joint Chiefs of Staff, 2016: 49-50).

تاب‌آوری سایبری برای سامانه‌هایی ضروری و مهم است که از امنیت ملی و خدمات دولتی و زیرساخت‌های حیاتی پشتیبانی می‌کنند. تاب‌آوری سایبری آن ویژگی سامانهٔ است که اطمینان می‌دهد، حتی در هنگام حمله سایبری، سیستم به انجام وظایف اصلی مأموریت خود ادامه می‌دهد. نکته کلیدی که تاب‌آوری سایبری را از امنیت سایبری متمایز می‌کند این است که تاب‌آوری سایبری حتی پس از نفوذ دشمن به محیط امنیتی شبکه و به خطر

انداختن دارایی‌های سایبری، همچنان به عملکرد خود ادامه می‌دهد (Department of US Homeland Security, 2018: 8-10). انجام کامل مأموریت نیازمند یک فرماندهی و کنترل تاب‌آور سایبری است که با فرض حضور دشمن در این فضا و به‌صورت تاب‌آور تعریف و اجرا شود (Thomas H, Hedgecock, 2021:339).

اکنون فرماندهی و کنترل تاب‌آور در فضای سایبری به نحوی از این مفهوم در فضای فیزیکی توسعه یافته است درحالی‌که فضای سایبری به میزان زیادی متفاوت از محیط فیزیکی (زمین، هوا، دریا و فضا) است. فضای سایبری به‌واسطهٔ دلایل مختلفی از قبیل سهولت دسترسی، پیچیدگی شبکه‌ها و نرم‌افزارها، عدم توجه امنیتی در طراحی شبکه و توسعه نرم‌افزارها و نیز فعالیت‌های کاربران، آسیب‌پذیر است. آسیب‌پذیری‌های شبکه اطلاعاتی و تأثیرات ایجادشده در فضای سایبری، می‌تواند تأثیر گسترده‌ای در تمام حوزه‌های فیزیکی داشته باشد؛ در این شرایط، تنها فرماندهی و کنترل سایبری تاب‌آور قادر به هدایت و اجرای عملیات برای انجام مأموریت است و این پژوهش در پی یافتن ویژگی‌های تاب‌آوری در یک فرماندهی و کنترل سایبری متناسب با صحنه نبرد آینده است.

مرور پیشینه و مبانی نظری

مبانی نظری

فرماندهی و کنترل در فضای سایبری

وزارت دفاع ایالات متحده فضای سایبری را این‌گونه تعریف می‌کند: «حوزه جهانی در محیط اطلاعاتی متشکل از شبکه‌های وابسته به هم زیرساخت‌های فناوری اطلاعات و داده‌های موجود در آن، از جمله اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده‌ها و کنترل‌کننده‌های تعبیه‌شده» (U.S. Department of Defense, 2014:63)، پس می‌توان گفت فضای سایبری ورای مرزهای جغرافیایی و ژئوپلیتیک گسترده شده و با زیرساخت‌های حیاتی، فعالیت‌های دفاعی، اقتصادی، بازرگانی و حاکمیت ملی یکپارچه شده است. برتری در حوزه‌های فیزیکی (زمین، دریا، هوا و فضا) در بخش‌های زیادی به برتری در فضای سایبری وابسته است. فضای سایبری می‌تواند به‌عنوان یک واسط برای اجرای فعالیت‌ها و قابلیت‌های اطلاعاتی باشد (قاسمی و همکاران، ۱۴۰۳: ۱۸). از زمان اعلام فضای سایبری به‌عنوان حوزه‌ای عملیاتی، تلاش‌ها در جهت ایجاد ساختار فرماندهی

و کنترل برای عملیات فضای سایبری، برگرفته از دکترین سنتی نظامی فرماندهی و کنترل بوده است تا دستیابی به وحدت تلاش در حوزه فضای سایبری جهانی و با عملیات نظامی در حوزه‌های فیزیکی (زمین، دریا، هوا و فضا) ممکن شود (Pomerleau, 2018:2). دکترین‌های سنتی برای انجام عملیات در دنیای فیزیکی بسیار مؤثر بوده و مجموعه وسیعی از دکترین‌های فرماندهی و کنترل را برای عملیات در حوزهٔ فیزیکی ایجاد کرده است (Perkins et al. 2018:55). بااین‌حال، تلاش‌ها خود برای تطبیق روش‌های فرماندهی و کنترل از حوزه‌های فیزیکی (زمین، دریا، هوا و فضا) به حوزه سایبری ادامه دارد. فضای سایبر، محیط عملیاتی بسیار متفاوتی را نسبت به حوزه‌های فیزیکی ارائه می‌دهد (Stone, S. 2016:5).

ویژگی‌های زمان و مکانی فضای سایبری به‌طرز قابل‌توجهی با حوزه فیزیکی متفاوت است. برای موفقیت، عملیات نظامی در فضای سایبری به روش‌های جدید و چابک‌تر و تاب‌آورتر فرماندهی و کنترل نیاز دارد (Stone, S. 2016:11). به دلیل اینکه عملیات فضای سایبری باید با هماهنگی عملیات نظامی در زمین، دریا، هوا و فضا انجام شود، نمی‌توان به‌طور کامل دکترین موجود فرماندهی و کنترل را کنار گذاشت اما استفاده از ساختارهای سنتی فرماندهی و کنترل نظامی در حوزه فضای سایبری به دلیل منحصربه‌فرد بودن فضای سایبری از سایر حوزه‌ها، منجر به مشکلات متعددی می‌شود (U.S. Joint Chiefs of Staff, 2016: 49-50). این فضای گسترده نیازمند فرماندهی و کنترل سایبری مناسب است. فرماندهی شامل اقتدار و مسئولیت استفاده از منابع برای انجام کامل مأموریت تعیین شده است. کنترل در ذات فرماندهی است؛ کنترل برای فرماندهان به معنی آزادی عمل، اعمال اقتدار، هدایت عملیات از هر نقطه و همگام‌سازی اقدامات در منطقه عملیاتی است. عملیات فضای سایبری به وحدت فرماندهی و وحدت تلاش نیاز دارند، همچنین ایجاد روابط فرماندهی سایبری برای اطمینان از به‌کارگیری به‌موقع و مؤثر نیروها حیاتی است، اما ماهیت پیچیده عملیات فضای سایبری، جایی که نیروهای فضای سایبری بتوانند به‌صورت هم‌زمان اقدامات را در سطح جهانی و در صحنه نبرد یا سطح منطقه عملیات فراهم کنند به ایجاد چارچوب فرماندهی و کنترل پویا و تاب‌آوری نیاز دارد تا بتواند به تغییرهای مداوم، تهدیدهای نوپدید و ناشناخته تطبیق یابد (U.S. Department of Defense, 2018: IV-11).

بحث‌های مربوط به فرماندهی و کنترل تاب‌آور سایبری با تغییرات مداوم در محیط تهدید، محیط عملیاتی و محیط فنی همراه است. این تغییرات می‌توانند به طرق مختلف با هم تعامل داشته باشند و باعث افزایش پیچیدگی و کاهش شفافیت سامانه‌ها، خدمات، زیرساخت‌ها و زیست‌بوم‌ها شوند. (US Department of Homeland Security, 2018:6). فرماندهی و کنترل تاب‌آور در فضای سایبری با توانایی انطباق و پاسخگویی مؤثر به چالش‌های منحصربه‌فرد ناشی از این حوزهٔ عملیاتی مشخص می‌شود. تاب‌آوری تطبیقی شامل مؤلفه‌های پیش‌بینی صحیح و مقاومت اثربخش و پاسخگویی تاب‌آور شامل مؤلفه‌های واکنش مؤثر و ترمیم و بازیابی سریع است (قاسمی و همکاران، ۱۴۰۳: ۸۳).

تاب‌آوری تطبیقی

تاب‌آوری در فضای سایبری به توانایی سازمان‌های نظامی برای تنظیم سریع رویکردهای فرماندهی و کنترل خود با توجه به ماهیت پویا و پیچیده محیط سایبری اشاره دارد. تاب‌آوری از سویی به سازمان‌های نظامی اجازه می‌دهد با پیش‌بینی صحیح، راهبردها و تاکتیک‌های خود را به‌سرعت اصلاح کنند و اطمینان حاصل کنند که می‌توانند به تهدیدها و فرصت‌ها به‌موقع پاسخ دهند؛ از سوی دیگر، تاب‌آوری در فضای سایبری به معنای وجود یک مقاومت با توانایی محوری و تنظیم سریع راهبردهای عملیاتی برای حفظ اثربخشی در یک محیط به‌سرعت در حال تحول و غیرقابل‌پیش‌بینی است که برای دستیابی به اهداف نظامی در این حوزه بسیار مهم است (قاسمی و همکاران، ۱۴۰۱: ۹۶). تاب‌آوری تطبیقی، توانایی سازمان‌های نظامی در فضای سایبری، برای تنظیم سریع رویکردهای فرماندهی و کنترل خود با توجه به ماهیت پویا و پیچیده محیط سایبری است.

پیش‌بینی صحیح

رفتار یک سامانه به داده‌های ارائه‌شده بستگی دارد، اما نمی‌توان پیش‌بینی کرد که در آینده چه داده‌هایی به سیستم ارائه می‌شود تا بتوان اقدامات را برای همه ترکیب‌های احتمالی داده‌ها آماده یا پیش‌بینی کرد (Tammet, 2021:37). انتظار می‌رود که تاب‌آوری سایبری با افزایش غیرخطی هوش ماشینی در طول زمان، ارتقا یابد. قابلیت‌های یادگیری ماشینی این امکان را فراهم می‌کند که بتوان اقدامات دشمن را در مرحله‌ای به‌اندازه کافی زودتر پیش‌بینی کرد تا اقدامات پیشگیرانه نیمه یا کاملاً خودکار را انجام دهند (Thomas

et al, 2021:332). در یک سیستم خودکار و خودمختار بیشتر احتمالاتی توصیف می‌شود که عامل انسانی، توانایی پیش‌بینی دقیق آن و گام‌هایی را ندارد که سیستم باید برای انجام وظیفهٔ محولهٔ خود انجام دهد (Tammet, 2021:17). آپروزی و همکاران (۲۰۱۸) در مقاله خود با عنوان «در مورد اثربخشی ماشین و یادگیری عمیق برای امنیت سایبری» بیان می‌کند که در سال‌های اخیر علاقه زیادی به استفاده از یادگیری ماشین برای شبیه‌سازی رفتار یک تحلیلگر انسانی در هنگام مشاهده هشدارها وجود داشته است. چندین حوزه دفاع سایبری وجود دارد که تجزیه‌وتحلیل خودکار بهتر از زبان طبیعی به آن‌ها کمک قابل‌توجهی خواهد کرد. پرند پیر و همکاران (۲۰۱۸) در مقاله خود با عنوان «مبانی و کاربردهای هوش مصنوعی برای تشخیص حمله روز صفر و چندمرحله‌ای» بیان می‌کند که یکی از این موارد اسکن خودکار بازارهای جرائم سایبری و انجمن‌های تبادل اطلاعات است. مورد دیگر تشخیص هرزنامه و فیشینگ است؛ چون انتظار می‌رود که به دلیل پیشرفت سریع تولید متن مبتنی بر هوش مصنوعی، میزان حمله‌های فیشینگ هوشمند به‌طور قابل‌توجهی افزایش یابد، بنابراین به اقدامات متقابل کافی نیاز دارد. شاید ساده‌ترین و درنتیجه رایج‌ترین فناوری هوش مصنوعی که در پیش‌بینی سایبری استفاده می‌شود، تشخیص بیرونی یا ناهنجاری مانند تشخیص الگوهای غیرمعمول جدید است.

مجموعهٔ دیگری از ابزارها بر استفاده از الگوریتم‌های چندجانبه مناسب و تضمین‌شده برای حفظ حریم خصوصی یا اجزای محاسباتی با اعتماد بالا در یک ریزپردازنده متمرکز است. تاکنون داده‌های اطلاعات تهدید مبادله شده بیشتر بر توصیف‌های کوتاه به زبان طبیعی متکی بوده و با داده‌های ساختاریافته تقویت شده است؛ بنابراین تفسیر داده‌های مبادله شده منحصراً توسط تحلیلگران انسانی انجام شده است. از آنجایی‌که سامانه‌ها و شیوه‌های دفاع سایبری به‌کار گرفته‌شده توسط سازمان‌های مختلف به‌طرز قابل‌توجهی متفاوت است، تبدیل این داده‌ها به دانش ساختاری قابل‌پردازش توسط ماشین واقع‌بینانه نیست. این امر می‌تواند به‌طور تدریجی توسط سامانه‌های هوش مصنوعی تغییر کند و در تبدیل داده‌های اطلاعات سایبری کمک کند و اقدامی انجام دهد (Thomas et al, 2021:329). آپروزی و همکاران (۲۰۱۸) در مقاله خود با عنوان «در مورد اثربخشی ماشین و یادگیری عمیق برای امنیت سایبری» بیان می‌کند که یکی دیگر از کاربردهای مهم و واقع‌بینانه، توسعه سامانه‌های تبادل اطلاعات سایبری مستقل است. ارتباط مستمر فرماندهان و ستاد با متخصصان دفاع سایبری سازمان‌های مختلف، مبادله اطلاعات تازه

در مورد تهدیدها و حمله‌های جدید یکی از بخش‌های مهم و عملاً حیاتی فرایند پیش‌بینی تاب‌آوری سایبری است. تحقیقات فعلی نشان می‌دهد سیستمی که از یک منبع انسانی می‌آموزد، نیازمند به‌روز کردن منظم است؛ چون عملکرد سیستم در چند ماه به دلیل تغییر در الگوهای ترافیک شبکه و انواع جدید حمله‌ها به‌شکل قابل‌توجهی کاهش می‌یابد.

مقاومت اثربخش

مقاومت به‌صورت سنتی حالت جلوگیری و ایجاد سد در برابر خطر یا تأثیر اولیه آن است. مؤلفه مقاومت در تاب‌آوری بر تأمین حفاظت متمرکز شده است که از طریق تأمین قدرت یا حفاظت برای ایستادگی در برابر خطرها یا برخورد اولیه با آن ایجاد می‌شود (تقی‌پور، ۱۳۹۷: ۱۸۶). تاب‌آوری سایبری مبتنی بر این است که دشمنان می‌توانند حضور پنهانی در سامانه‌ها ایجاد و حفظ کنند؛ تکنیک‌هایی که برای مقاومت انجام می‌شود شامل حفاظت هماهنگ، فریب، تنوع، عدم تداوم، همسویی مجدد، افزونگی، یکپارچگی اثبات‌شده و غیرقابل پیش‌بینی، روش‌های تقسیم‌بندی، عملکرد توزیع‌شده، تقسیم‌بندی از پیش تعریف‌شده، محدودیت استفاده مبتنی بر ویژگی و رویکردهای مدیریت خصوصی مبتنی بر اعتماد است. سایر تکنیک‌ها و رویکردها می‌توانند پاسخ خودکار به نشانگرهای شناسایی‌شده از ناملایمات احتمالی یا مشکوک یا هشدار شرایط نامطلوب احتمالی آینده ارائه دهند. این‌ها شامل تکنیک پاسخ تطبیقی و جابه‌جایی عملکردی حسگرها، جابه‌جایی عملکردی منابع سایبری، تحرک دارایی‌ها، امتیازات پویا و رویکردهای تقسیم‌بندی و جداسازی پویا است (ROSS et al, 2021: 14).

توانایی مقاومت سایبری نیاز به رویکردی چندوجهی دارد تا به کمک آن تأثیر حمله به حداقل برسد:

- از حفاظت تا قربانی کردن: فناوری‌ها امروزه این امکان را فراهم می‌آورند که بخش‌هایی از اطلاعات یا عملیات را به نفع حفاظت از شبکه بزرگ‌تر قربانی کنیم.
- تغییر وضعیت از حالت ایمن به ایمن نسبت به خرابی: امنیت سایبری آینده باید هوشمندتر و همچنین قوی‌تر، با رویکرد انعطاف‌پذیری نرم باشد (Van Kessel, 2017: 25).

برای اطمینان از مقاومت سایبری باید از عناصر کلیدی مقاومت سایبری استفاده شود:

- راهبرد مدیریت خطرها: امنیت سایبری مستلزم یک ذهنیت بهبود مستمر و تلاش آگاهانه برای اطمینان از وجود کنترل‌های امنیت سایبری در یک سازمان است.

• سیاست‌ها و رویه‌ها: سیاست‌ها و رویه‌های یک سازمان، راهبردهای سایبری آن را به واکنش‌ها و رفتارهای معنادار تبدیل می‌کند.

• دفاع فنی: دفاع فنی با به‌روزرسانی مداوم و سایر کنترل‌های حفاظتی اغلب نشان‌دهندهٔ اولین خط دفاعی سازمان در برابر تهدیدهای سایبری است.

• نظارت و آگاهی از موقعیت: درصورتی‌که یک حمله با موفقیت به شبکه نفوذ کند، تمرکز بر روی قابلیت‌های کارآگاهی سازمان معطوف می‌شود تا مشخص شود مهاجم چگونه موفق شده و چه دارایی‌هایی به خطر افتاده است.

• آگاهی کارمندان: آموزش و آگاهی برای ایجاد فرهنگ ریسک سایبری مناسب که رفتارهای صحیح را هدایت می‌کند، بسیار مهم است (MacKinnon et al, 2018: 28-29).

یک سامانه که به‌درستی مقاومت‌سازی شده است، در برابر مهاجمی که به آن نفوذ کرده یا به آن آسیب رسانده است، مقاومت بیشتری خواهد داشت. این به‌عنوان به‌طور معمول «دفاع در عمق» نامیده می‌شود، می‌توان با پیچیده‌کردن و تنوع، با هدف قرار دادن سیستم در برابر اقدامات یک عامل مخرب مقاومت کرد. تنوع در اجزای سیستم و ساخت آن‌ها مستلزم آن است که مهاجم چندین راهبرد حمله را تدوین کند یا به‌اندازه کافی خوش‌شانس باشد که راهبرد خود را با مؤلفه ارائه‌شده به آن‌ها تطبیق دهد. راهبردهای دفاع متحرک در فضای سایبری با افزایش تنوع سیستم طراحی می‌شوند. ماژولار بودن در یک سیستم امکان پیکربندی مجدد و جایگزینی اجزا را بدون نیاز به تغییر در رابط بین آن‌ها فراهم می‌کند؛ بنابراین تنوع بیشتری را ممکن می‌سازد (Kott et al, 2018: 5).

پاسخگویی تاب‌آور

آدام اس مورگان و استیو دبلیو استون[1] (۲۰۱۹) در پژوهشی با عنوان فرماندهی و کنترل عملیات فضای سایبری - فراخوانی برای پژوهش بیان کرده است که پاسخگویی تاب‌آور در فضای سایبری به توانایی سازمان‌های نظامی برای تطبیق سریع راهبردهای فرماندهی و کنترل خود در واکنش به چالش‌های منحصربه‌فرد و پویا به وجود آمده در محیط سایبری اشاره دارد. واکنش‌های مؤثر نیازمند ساختار ترکیبی از مدل‌های فرماندهی و کنترل است که امکان تصمیم‌گیری و اقدام سریع در سطوح مختلف عملیات نظامی را

---

[1]. Adam S. Morgan, Steve W. Stone

فراهم می‌کند. علاوه بر این، واکنش مؤثر برای تاب‌آوری در فضای سایبری مستلزم درک ویژگی‌های منحصربه‌فرد دامنه، مانند ماهیت ساخت بشر، پیچیدگی «زمین» آن و دسترسی جهانی به عملیات سایبری است. این درک، فرماندهان نظامی را قادر می‌سازد تا تصمیم‌های آگاهانه بگیرند و اقداماتی را هماهنگ کنند که بتواند به‌طور مؤثر به تهدیدها واکنش نشان داده و درعین‌حال به اهداف راهبردی دست یابد. از طرفی، پاسخگویی تاب‌آور به انعطاف‌پذیری برای ترمیم و بازیابی سریع و مؤثر سامانه‌ها و عملیات پس از یک حادثه یا حمله سایبری اشاره دارد.

واکنش مؤثر

واکنش مؤثر در حوادث سایبری مستلزم وحدت تلاش بین قسمت‌های مختلف است؛ زیرا ماهیت فضای سایبری ایجاب می‌کند که افراد، سازمان‌ها و دولت همگی در واکنش به حوادث ایفای نقش کنند. همچنین در انجام فعالیت‌های واکنش به حوادث سایبری، رعایت اصول زیر لازم است:

- تقسیم مسئولیت‌ها
- پاسخ متناسب با خطر
- احترام به نهادهای آسیب‌دیده
- وحدت تلاش

در واکنش به هر حادثه سایبری، باید سازمانِ در معرض خطر در سه خط تلاش، هم‌زمان وظایف خود را انجام دهد: پاسخ به تهدید، پاسخ دارایی و پشتیبانی اطلاعاتی؛ در ادامه یک نهاد متأثر باید تلاش‌های مختلفی را برای مدیریت تأثیر یک رویداد سایبری انجام دهد که ممکن است شامل حفظ تداوم عملیاتی باشد (PRESIDENTIAL POLICY DIRECTIVE, 2016: 3). سازمان‌ها نیاز به آمادگی برای مقابله با اختلال، پاسخگویی به حوادث و مدیریت بحران دارند. آن‌ها همچنین نیاز به حفظ ادله دیجیتال برای بررسی رخنه سایبری دارند که اگر مهاجمین شناسایی شدند، سازمان علیه آن‌ها اقدام کند. در پایان آن‌ها همچنین نیاز به آمادگی برای برگرداندن سازمان به مأموریت‌های معمول در سریع‌ترین زمان ممکن دارند. یادگیری از آنچه اتفاق افتاده است و سازگاری و سازمان‌دهی مجدد سازمان، کمک به بهبود تاب‌آوری است (نصرت‌آبادی و همکاران، ۱۳۹۷: ۱۷۳-۱۹۸).

یک نکته مهم در واکنش به تهدیدها چابکی است؛ در زمینه پاسخ به تهدیدهای سایبری، چابکی به معنای داشتن توانایی پاسخ مؤثر با استفاده به‌موقع از فرصت‌های ناشی از تغییرات محیط است. چابکی سیستم، فرایندهای عملیاتی را قادر می‌سازد تا فناوری‌های جدید را ترکیب کنند و با قابلیت‌های در حال تغییر دشمن سازگار شوند. با فعال‌کردن پاسخ به تغییرات در هر وضعیت سیستم، می‌توان احتمال آسیب ناشی از سوءنیت، خطا یا شکست و میزان آسیب را کاهش داد؛ این اعمال شامل رفتارهایی برای محدودکردن مجموعه‌ای از منابع یا عناصر سیستم است که می‌تواند تحت تأثیر رفتار یک عنصر سیستم باشد. مهار را می‌توان به‌طور پیش‌فرض و متناوب از طریق تقسیم‌بندی به دست آورد یا علاوه بر این، پاسخ تطبیقی و ایزوله پویا را در پاسخ به رفتار مشکوک اعمال کرد و فعالیت‌های بعدی را در آنجا منحرف کرد (ROSS et al, 2021: 130).

ترمیم و بازیابی سریع

فرماندهان باید تحت شرایط نامطمئن آماده انجام عملیات در فضای سایبری باشند. آن‌ها می‌توانند با استفاده از اقدامات کاهش تهدید، خطرات ناشی از آن را مدیریت کنند. اقدام‌های بازیابی پس از ضربه انجام می‌شود و شامل اقدام‌هایی برای انجام مأموریت خود و اطمینان از قابلیت اطمینان داده‌های مهم است (U.S. Department of Defense, 2018: IV-11). به عبارتی سامانه‌های مقاوم در برابر سایبر می‌توانند حداقل عملکرد ضروری را بازیابی کنند (ROSS et al, 2021: 18). البته افزایش توانایی بازیابی سریع از حوادث مانع از توانایی دشمن در مکان‌یابی، حذف یا خراب‌کردن دارایی‌های مأموریت نمی‌شود؛ ولی باعث می‌شود که دشمن زمان و تلاش بیشتری را برای یافتن دارایی‌های مهم سازمان صرف کند درنتیجه احتمال آشکارشدن زودهنگام حضور، اقدامات دشمن افزایش می‌یابد (ROSS et al, 2021: 99). آدام اس مورگان و استیو دبلیو استون (۲۰۱۹) در پژوهشی با عنوان «فرماندهی و کنترل عملیات فضای سایبری - فراخوانی برای پژوهش» بیان کرده است که در زمینه عملیات فضای سایبری، ترمیم و بازیابی نه‌تنها مستلزم بازگرداندن سامانه‌ها به حالت قبلی است، بلکه همچنین تطبیق و بهبود دفاع برای جلوگیری از حوادث آینده را شامل می‌شود.

فرایند سامانه‌های عملیاتی سازمان در ترمیم به شرح زیر است:

- توسعه توانایی اطلاع و گزارش در صورت نفوذ به شبکه یا سیستم.

• به طرز مطلوبی عملکرد را تنزل داده یا مکانیسم‌های جایگزین برای ادامه حیاتی‌ترین وظایف مأموریت در نظر گرفته شود.

• سرانجام سیستم به حالت مورد اعتماد بازگردانده شود (DEPARTMENT OF DEFENSE, 2015: 62).

اهداف مؤلفه ترمیم و بازیابی، توانایی واکنش و بازیابی مؤثر و سریع در برابر حوادث مخرب است. کارایی این مؤلفه با تکمیل تلاش‌ها برای طراحی، آماده‌سازی و مانور در پیشرفت حوادث مشخص می‌شود (تقی‌پور، ۱۳۹۷: ۱۸۸). برای نیل به این اهداف لازم است اقدام‌هایی انجام شود؛ یک اقدام، فعال کردن ترمیم و بازیابی شامل فعالیت‌های واکنشی، به‌منظور تسهیل بازسازی و بازیابی نهادی است که دچار حادثه سایبری شده است که بازگشت به ادامه عملیات در اسرع وقت را تنظیم می‌کند (PRESIDENTIAL POLICY DIRECTIVE, 2016: 2). عامل مهم دیگر تقویت توانایی در پاسخ به فعالیت‌های غیرمجاز و دفاع از اطلاعات در برابر تهدیدهای سایبری پیچیده و چابک و بهبود سریع از حوادث سایبری است؛ اجزای فناوری سایبری باید این توانایی را داشته باشند که بدون دخالت انسان به‌صورت خودکار یا بدون هیچ‌گونه پیکربندی مجدد، خود را بازیابی و ترمیم کنند (Department of Defense Instruction, 2019: 32). به‌علاوه، سازمان باید روش‌هایی را برای نگهداری و تکثیر نسخه‌های قابل‌اعتماد از نرم‌افزارهای عملیاتی توسعه دهد و اطمینان لازم را به‌دست آورد که تغییرهای موردنظر تنها در نسخه طلایی ایجاد شده است. ابزارهای کنونی به مقدار قابل‌توجهی از تعامل انسان نیاز دارند؛ ولی سازمان باید به توسعه ابزارهایی با سطوح بالای اتوماسیون برای این عملکرد بپردازد (DEPARTMENT OF DEFENSE, 2015: 62).

«مهندسی بقا[1]» زیرمجموعه‌ای از مهندسی سامانه‌ها است که با به حداقل رساندن تأثیر اختلالات محیطی بر عملکرد سیستم مرتبط است. در زمینه مهندسی امنیت سامانه‌ها، هدف کنترل است که در مورد تمام انواع دارایی‌ها و پیامدهای مربوط به ضرر اعمال می‌شود؛ مشکل اصلی در طراحی سیستم است. راه‌حل این مشکل‌ها از طریق یک راهبرد فعال متعادل و یک راهبرد واکنشی بهینه‌شده است که محدود به پیشگیری نیست (قاسمی و همکاران، ۱۴۰۱: ۷۶). راهبردهای ترمیم شامل بازگشت (تکرار حالت قبلی که

---

[1]. Survival Engineering

شناخته‌شده است)، بازسازی (تکرار عملکردهای مهم و حمایتی در سطح قابل‌قبول با استفاده از منابع سیستم موجود) و جایگزینی (جایگزینی سیستم آسیب‌دیده، عناصر مشکوک سیستم یا انتخاب‌شده با عناصر جدید یا عناصر سیستم موجود برای انجام وظایف مختلف، به‌منظور انجام عملکردهای مهم و پشتیبانی، احتمالاً به روش‌های مختلف) است (ROSS et al, 2021: 102).

پیشینه‌های پژوهش

آدام اس مورگان و استیو دبلیو استون[1] (۲۰۱۹) در پژوهشی با عنوان «فرماندهی و کنترل عملیات فضای سایبری - فراخوانی برای پژوهش» بیان کرده است که از سال ۲۰۱۱ وزارت دفاع ایالات متحده فضای سایبری را به عرصه‌های جنگ اضافه کرد. فرماندهی و نیروی سایبری متعاقباً به‌منظور دستیابی به اهداف در فضای سایبری تشکیل شد. از آن زمان، ساختارهای فرماندهی و کنترل چندگانه برای عملیات فضای سایبری، مشتق شده از فرماندهی و کنترل نظامی سنتی، برای دستیابی به وحدت تلاش در سراسر عرصه فضای سایبری جهانی و با عملیات نظامی در عرصه‌های فیزیکی (زمین، دریا، هوا و فضا) پیاده‌سازی و تکامل‌یافته است. در این تحقیق عواملی که فضای سایبری را از سایر حوزه‌های عملیاتی متمایز می‌کند و چالش‌هایی که این تفاوت‌ها بر ساختارهای فرماندهی و کنترل موجود تحمیل می‌کنند، شرح داده شده است. همچنین روش‌های تطبیق فرماندهی و کنترل حوزه‌های فیزیکی با حوزه سایبری بیان‌شده است. آزمایش برای درک، ارزیابی و در نهایت به‌کارگیری مدل‌های جدید فرماندهی و کنترل بیان‌شده است. در ادامه دسته‌ای از آزمایش‌های فضای سایبری را برای رسیدگی به این چالش‌ها و شبیه‌سازی و اصلاح ساختارهای فرماندهی و کنترل فضای سایبری پیشنهاد کرده است. نتیجهٔ این تحقیق پیاده‌سازی مؤثرتر فرماندهی و کنترل سایبری، با پشتیبانی از عملیات چند دامنه، به‌عنوان ترکیبی از مدل‌های هماهنگ، مشارکتی و لبه، در فضاهای مختلف تصمیم‌گیری بوده است.

تقی‌پور (۱۳۹۷) در تحقیقی با عنوان طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران بیان می‌کند که به‌منظور کاهش حداکثری اثر هرگونه تهاجم سایبری، لازم

---

[1]. Adam S. Morgan, Steve W. Stone

است سامانه‌های پدافند غیرعامل سایبر در حوزه‌های مختلف زیرساخت‌های فناورانه، اقتصادی، اجتماعی، فرهنگی و نظامی مورد توجه قرار گیرند. در صورت بروز حمله سایبری، بنا به مقتضیات محیط‌های داخلی و خارجی و نیز محیط‌های روانی و عملیاتی لازم است سلاح و جنگ‌افزار لازم به‌منظور پاسخ‌های مؤثر به‌عنوان پدافند عامل فراهم شود. بُعد برگشت‌پذیری در مرحله پس از حمله سایبری، ناظر بر حفظ خودآگاهی، حفاظت و بازیابی کارکردهای سیستم در کمترین بازه زمانی ممکن است. این بعد در ارتباط با مؤلفه مقاومت در برابر آسیب و اختلال و نیز مؤلفه قابلیت اطمینان است که موجب شناخت حد آستانه تحمل و کاهش هزینه‌های مقابله و افزایش حداکثر بهره‌وری در موقعیت بحران می‌شود. مؤلفه افزونگی نیاز ناظر بر نیروهای انسانی، سخت‌افزار و نرم‌افزارها است که در طراحی الگوی سایبری باید موردتوجه جدی قرار گیرد. مؤلفه پاسخ و ارزیابی نیز برای حفاظت از زیرساخت‌ها، کاهش اثرات بحران، بازگشت به حالت عادی، بازسازی، ترمیم و توان‌بخشی است که ارتقا این شاخص‌ها مستلزم هوشمندسازی کلیت و اجزای سیستم واحد سیاسی و نیز در نظر گرفتن تکثر و جایگزینی کارکردی برای اجزا است تا در صورت ازکارافتادن یک جزء یا مرکزیت، کلیت سیستم به حیات خود ادامه دهد.

نصرت‌آبادی (۱۳۹۸) در پژوهشی با عنوان «ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران»، عوامل مؤثر برای ارزیابی نیروهای مسلح را در سه بُعد آفند سایبری، پدافند سایبری و تاب‌آوری سایبری تقسیم‌بندی کرده است که در بُعد تاب‌آوری سایبری شاخص‌های هوش تهدید سایبری، برآورد خطرات احتمالی، طرح آمادگی مقابله با اختلال، کاهش وابستگی زیرساخت، افزونگی، مسیرهای ارتباطی چندگانه، ساختار دفاعی لایه به لایه، تغییر ساختار از سلسله مراتبی به شبکه‌ای، افزایش نقاط تبادل اینترنتی، اقدامات کنترلی، بازیابی منابع اطلاعات، نحوه کنش و واکنش، حفظ ادله دیجیتال، زمان بازگشت، سازمان‌دهی مجدد، بازمعماری، طراحی ویژگی‌های عملیاتی مناسب را برای ارزیابی مناسب معرفی می‌کند.

در تحقیق‌هایی که در پیشینه پژوهش از آن‌ها نام برده شد از جنبهٔ قدرت سایبری، دفاع سایبری و تهدیدمحور به موضوع تاب‌آوری سایبری پرداخته شده است، در تحقیق حاضر تاب‌آوری فرماندهی و کنترل سایبری مدنظر قرار گرفته است.

روش‌شناسی

این پژوهش از نوع کاربردی است و با رویکرد آمیخته انجام‌شده است. روش جمع‌آوری داده‌ها در این پژوهش، کتابخانه‌ای و میدانی بوده است. در روش کتابخانه‌ای با استفاده از ابزار بررسی اسناد و مدارک داده‌های پژوهش از منابع ورودی مختلف و معتبر مانند کتب، مقالات، نشریات علمی، سایت‌های معتبر و مرتبط با حوزه فرماندهی و کنترل سایبری جمع‌آوری شد. داده‌های جمع‌آوری‌شده طبقه‌بندی و مرتب شدند. در روش میدانی، جامعه خبرگی برای مصاحبه، تعداد شش نفر از صاحب‌نظران حوزه سایبری و فرماندهی و کنترل بودند که به موضوع تحقیق آشنایی کامل داشته و حداقل بیست سال سابقه فعالیت در حوزه سایبری و فرماندهی و کنترل داشته و دارای مدرک کارشناسی ارشد و بالاتر بودند؛ مصاحبه‌ها توسط چند مصاحبه‌شونده و در زمان‌های مختلف انجام شد. در روش کمّی از کارشناسان حوزهٔ فرماندهی و کنترل سایبری استفاده شد که حداقل دارای ۱۵ سال سابقه فعالیت در مراکز فاوا یا مراکز دفاع سایبری بودند و به موضوع تحقیق آگاهی کامل داشتند که تعداد افراد جامعه با اعمال ضریبی ۱۴۶ نفر بود. با استفاده از فرمول کوکران و به‌صورت تصادفی ۱۰۶ نفر به‌عنوان جامعه نمونه انتخاب شدند.

در رویکرد کیفی، برای تجزیه‌وتحلیل محتوای اسناد و مدارک و نظرات صاحب‌نظران پژوهشگر با استفاده از نرم‌افزار اطلس تی.آی به تحلیل مضمون و آشکار کردن پیام‌های نهفته در بررسی متن اسناد و مدارک و مصاحبه پرداخته است. محقق با استفاده از نرم‌افزار اطلس تی.آی به تحلیل روابط و مقایسه داده‌های حاصل از مصاحبه و اسناد و مدارک پرداخت تا بتواند تقاطع و تباین آن‌ها را بیابد. فرایند بررسی محتوای آشکار و پنهان داده‌های به‌دست‌آمده از گفته‌ها و نوشته‌ها انجام شد. هدف این فرایند کشف ارتباط درونی اجزا و عناصر تشکیل‌دهندهٔ داده‌ها، دست‌یابی به هدف تحقیق است. فرایند تحلیل داده‌ها به‌صورت استقرایی شامل شناسایی گفته‌های اساسی، کلیدی و دسته‌بندی آن‌ها برحسب مقوله‌ها است. محقق با شناسایی و پاک‌سازی نوشته‌ها، نکات اساسی موجود در داده‌ها را شناسایی کرده است سپس با قضاوت و تصمیم‌گیری در مورد داده‌ها و استخراج شاخص‌های نهایی، مؤلفه‌ها و ابعاد تحقیق را مشخص و مدل مفهومی تحقیق را ارائه کرده است. از محاسبه CVI برای تأیید روایی شاخص‌های استفاده‌شده در پرسش‌نامه استفاده شد، از ۶۱ شاخص اولیه تعداد ۵۴ شاخص دارای امتیاز بیش از ۰/۷۹ بودند و به‌عنوان

شاخص‌های پرسش‌نامه مورد استفاده قرار گرفتند. در تحلیل کمّی با استفاده از طیف لیکرت پنج‌گزینه‌ای (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) شاخص‌ها به بوته آزمایش گذاشته شد و نظرات کارشناسان با استفاده از پرسش‌نامه در قالب داده‌های کمّی جمع‌آوری شد، جهت تحلیل کمی از نرم‌افزار SPSS استفاده شد؛ آلفای کرونباخ محاسبه‌شده برای پرسش‌نامه برابر ۰/۹۲۴ است که پایایی پرسش‌نامه را نشان می‌دهد. درنهایت از آزمون فریدمن برای ارزیابی و رتبه‌بندی شاخص‌ها استفاده شد.

تجزیه‌وتحلیل یافته‌ها

تحلیل کیفی

با کمک نرم‌افزار اطلس تی‌آی داده‌های جمع‌آوری‌شده از اسناد و مدارک و مصاحبه‌ها مورد بررسی قرار گرفت، از مقوله‌ها و روایت‌ها با کدگذاری باز، مفاهیم استخراج شد. پس از آن مقوله‌ها، کدگذاری محوری شده و مؤلفه‌های تحقیق در چهار عنوان ۱. پیش‌بینی صحیح، ۲. مقاومت اثربخش، ۳. واکنش مؤثر، ۴. ترمیم و بازیابی سریع احصا شد.

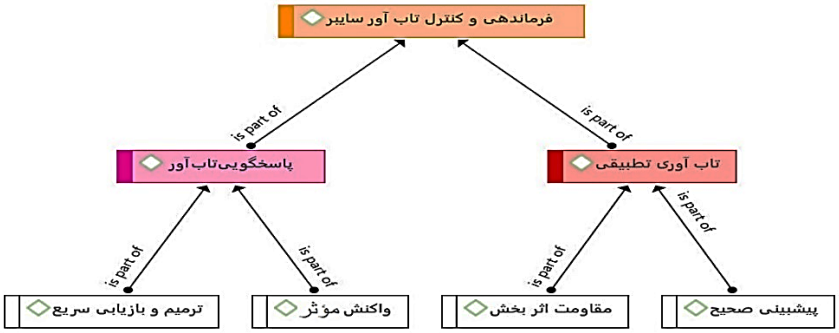
جدول نرمالیزه تقاطع شاخص‌های مؤلفه‌ها با اسناد و مصاحبه‌ها برحسب تعداد کد و روایت‌های بیان‌شده در جدول ۱ ارائه شده است.

جدول ۱. تقاطع شاخص‌های مؤلفه‌ها با اسناد و مصاحبه‌ها برحسب تعداد کد و روایت‌های بیان‌شده (نرمالیزه شده)

	ادبیات تحقیق Gr=64	مصاحبه۱ Gr=31	مصاحبه۲ Gr=5	مصاحبه۳ Gr=3	مصاحبه۴ Gr=7	مصاحبه۵ Gr=4	مصاحبه۶ Gr=3	جمع
پیش‌بینی صحیح ;Gr=23 GS=17	۱۲	۸	۱۲	۴۱	۲۰	۱۵	۲۰	۱۲۹
مقاومت اثربخش ;Gr=44 GS=23	۲۰	۳۵	۲۴	۰	۱۰	۱۵	۴۱	۱۴۶
واکنش مؤثر ;Gr=26 GS=11	۱۴	۱۴	۱۲	۲۰	۲۰	۱۵	۰	۹۶

ترمیم و بازیابی سریع ;Gr=20 GS=10	۱۵	۴	۱۲	۰	۱۰	۱۵	۰	۵۷
جمع	۶۱	۶۱	۶۱	۶۱	۶۱	۶۱	۶۱	۴۲۷

با کدگذاری انتخابی دو مؤلفه پیش‌بینی صحیح و مقاومت اثربخش در بُعد تاب‌آوری تطبیقی و دو بعد واکنش مؤثر، ترمیم و بازیابی سریع در بُعد پاسخگویی تاب‌آور قرار گرفتند.



نمودار ۱. ابعاد و مؤلفه‌ها

شاخص‌ها، مؤلفه‌ها و ابعاد اولیه احصا شده مطابق جدول ۲ است.

جدول ۲. ابعاد، مؤلفه‌ها و شاخص‌های اولیه

ردیف	متغیر	ابعاد	مؤلفه	شاخص	کد
۱	فرماندهی و کنترل تاب‌آوری سایبری	تاب‌آوری تطبیقی	پیش‌بینی صحیح (P)	پیش‌بینی صحیح و ارتقا با افزایش غیرخطی هوش ماشینی	P1
۲				توسعه سامانه‌های تبادل اطلاعات سایبری جهت تبادل اطلاعات بروز	P2
۳				واقع‌گرایانه بودن اقدامات سایبری صحیح	P3
۴				استفاده از سیستم تشخیص نفوذ	P4
۵				استفاده از الگوریتم‌های چندجانبه برای حفظ حریم خصوصی	P5
۶				نظارت بر شبکه	P6
۷				نظارت بر فعالیت کاربران و فعالیت تأمین‌کنندگان	P7

ردیف	متغیر	ابعاد	مؤلفه	شاخص	کد
۸				نظارت بر محیط فیزیکی	P8
۹				استفاده از سیستم خودکار و خودمختار در پیش‌بینی صحیح	P9
۱۰				برآورد به‌روز آخرین وضعیت منابع سایبری	P10
۱۱				پیش‌بینی صحیح با محاسبات کوانتومی	P11
۱۲				تأثیرات زیاد یادگیری ماشین	P12
۱۳				میزان پیچیدگی معماری شبکه، معماری امنیتی شبکه و طراحی لایه‌های امنیتی متنوع در میزان بحران	P13
۱۴				تجزیه‌وتحلیل خودکار با هوش مصنوعی صحیح	P14
۱۵				تدوین طرح‌های الزامات امنیتی جهت ایمن‌سازی محصولات	P15
۱۶				شناسایی آسیب‌های احتمالی	P16
۱۷			مقاومت اثربخش (M)	محدودیت در استفاده و دسترسی در سیستم فرماندهی و کنترل	M1
۱۸				ایجاد تنوع در سامانه‌های فرماندهی و کنترل	M2
۱۹				تعیین راهبرد مدیریت خطرات	M3
۲۰				توسعه و به‌کارگیری حفاظت‌های مناسب به‌منظور اطمینان از استمرار ارائه خدمات زیرساخت	M4
۲۱				عدم تداوم استفاده از یک سیستم به‌تنهایی در فرماندهی و کنترل	M5
۲۲				استفاده از تجهیزات به‌روز در راستای دفاع فنی	M6
۲۳				استفاده از تکنیک‌های فریب در جهت گمراه کردن دشمن	M7
۲۴				استفاده از رمز کننده‌های بومی	M8
۲۵				عملکرد توزیع‌شده در سیستم فرماندهی و کنترل	M9
۲۶				مهاجرت به سیستم‌عامل‌های بومی متن‌باز	M10
۲۷				ایجاد قابلیت تحرک در دارایی‌های سایبری	M11
۲۸				کاهش وابستگی زیرساختی	M12
۲۹				مشخص کردن سیاست‌ها و رویه‌های سایبری سازمان	M13
۳۰				نظارت و آگاهی از موقعیت تهدید	M14
۳۱				ایجاد افزونگی در سیستم فرماندهی و کنترل	M15

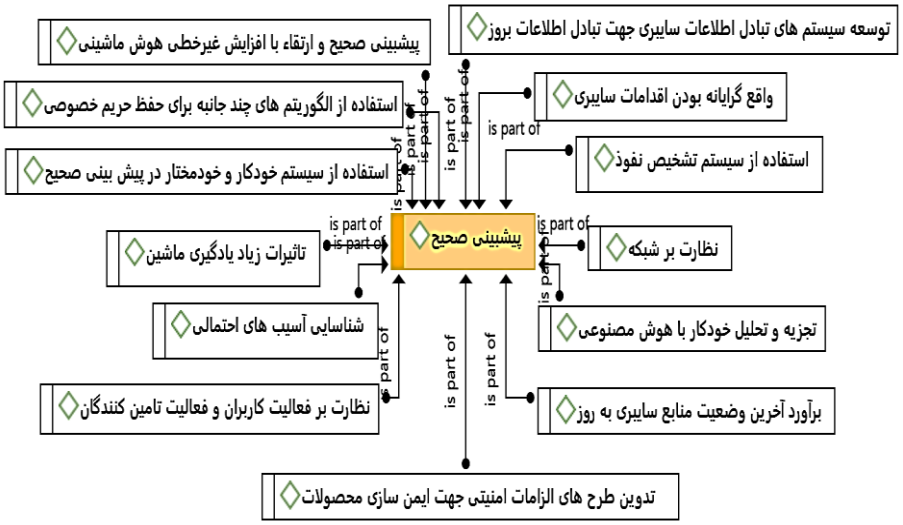
ردیف	متغیر	ابعاد	مؤلفه	شاخص	کد
۳۲				حفاظت هماهنگ چندلایه	M16
۳۳				تقسیم‌بندی و جداسازی پویا در سامانه‌های سایبری	M17
۳۴				ایجاد آگاهی و آموزش ریسک سایبری در کارمندان	M18
۳۵				ایجاد سامانه‌های پاسخ خودکار به شرایط نامطلوب احتمالی یا مشکوک	M19
۳۶				رویکرد حفاظت یا قربانی کردن اطلاعات برای حفظ شبکه بزرگ‌تر	M20
۳۷				افزایش موانع در مقابل حمله دشمن در راستای افزایش هزینه‌های او	M21
۳۸				تغییر تنظیمات سامانه‌ها بر اساس اطلاعات به‌دست‌آمده از تهدیدات	M22
۳۹		پاسخگویی تاب‌آور	واکنش مؤثر (V)	چابکی و پاسخ مؤثر و به‌موقع	V1
۴۰				یادگیری، سازگاری و سازمان‌دهی مجدد سازمان	V2
۴۱				ایجاد وحدت تلاش در برابر حوادث سایبری	V3
۴۲				آمادگی برای مقابله با اختلال، پاسخگویی به حوادث و مدیریت بحران	V4
۴۳				جداسازی منابع آسیب‌پذیر	V5
۴۴				تقسیم مسئولیت‌ها در برابر حوادث سایبری	V6
۴۵				پاسخ مناسب به خطرات سایبری	V7
۴۶				پشتیبانی مناسب اطلاعاتی در واکنش مؤثر	V8
۴۷				ایجاد سامانه‌های اس.او.سی[1] و سرت[2] در سازمان	V9
۴۸				موقعیت جغرافیایی، محیطی و وضعیت دشمن باعث پیچیدگی در واکنش مؤثر می‌شود	V10
۴۹				حفظ تداوم عملیات سایبری	V11
۵۰				تجزیه‌وتحلیل رویدادهای گزارش‌شده	V12
۵۱			ترمیم و بازیابی	افزایش توانایی سریع در واکنش و بازیابی مؤثر سیستم و ارزیابی دقیق تأثیر واکنش	T1

۱. مرکز عملیات امنیت (Security Operations Center)

۲. تیم پاسخگویی به رخدادهای امنیتی کامپیوتر (CERT) مخفف Computer Emergency Response Teams.

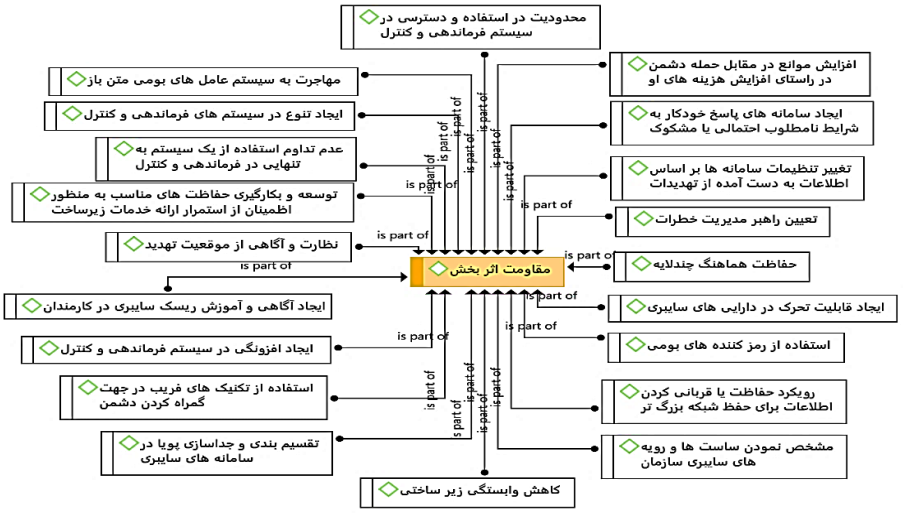
ردیف	متغیر	ابعاد	مؤلفه	شاخص	کد
۵۲				استفاده از راهبرد ترمیم (بازگشت، بازسازی و جایگزینی)	T2
۵۳				ایجاد سیستم موازی برای سامانه	T3
۵۴				نگهداری و تکثیر نسخه‌های قابل‌اعتماد از نرم‌افزارهای عملیاتی	T4
۵۵				اقدامات منجر به کاهش تنش	T5
۵۶				جلوگیری از انتشار حمله سایبری به سایر قسمت‌ها	T6
۵۷				سامانه‌های مقاوم در برابر حملات سایبری	T7
۵۸				قرنطینه بخش‌های آلوده	T8
۵۹				استفاده از اصل مهندسی بقا با راهبرد فعال متعادل و راهبرد واکنشی بهینه‌شده	T9
۶۰				افزایش توانایی بازیابی سریع سیستم با روش‌های متداول مانند گرفتن پشتیبانی از سیستم	T10
۶۱				توانایی اطلاع‌رسانی و گزارش در صورت نفوذ	T11

برای تعیین روایی محتوایی شاخص‌های به‌دست‌آمده، تعداد ۱۰ نفر از صاحب‌نظران و خبرگان حوزهٔ فرماندهی و کنترل سایبری انتخاب شدند و پس از توضیح اهداف آزمون برای آنان، تعاریف عملیاتی مربوط به سؤالات بیان شد. از محاسبه ضریب روایی محتوایی استفاده شد. صاحب‌نظران میزان مرتبط بودن هر شاخص را با طیف چهارگزینه‌ای (۱. غیر مرتبط ۲. نیاز به بازبینی اساسی ۳. مرتبط اما نیاز به بازبینی ۴. کاملاً مرتبط) مشخص کردند. شاخص‌هایی که حاصل تقسیم تعداد انتخاب‌های گزینه ۳ و ۴ توسط خبرگان بر کل خبرگان از ۰/۷۹ بیشتر بودند، قابل‌قبول محسوب شدند؛ لذا از ۶۱ شاخص اولیه ۷ شاخص حذف شد و ۵۴ شاخص تأیید شد. از مؤلفه پیش‌بینی صحیح شاخص‌های P8 ، P11و P13 حذف شدند و شاخص‌های برگزیده برابر نمودار ۲ است.



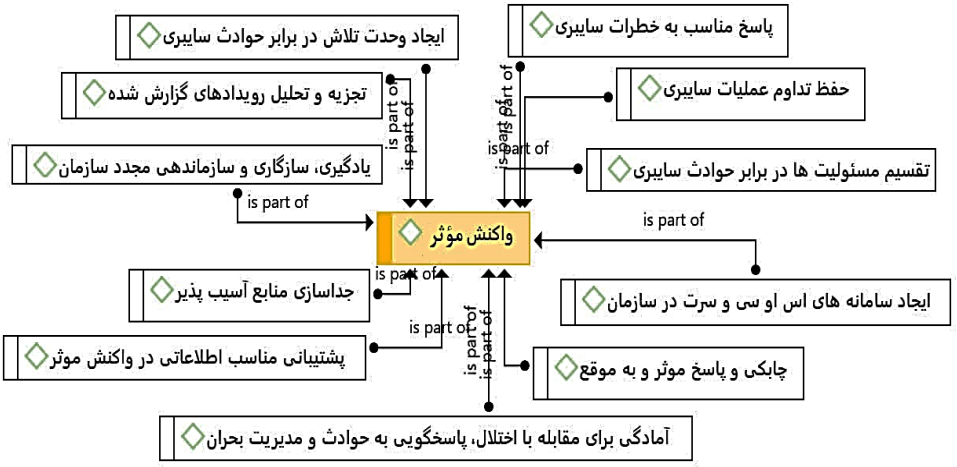
نمودار ۲. شاخص‌های برگزیده پیش‌بینی صحیح

در مؤلفه مقاومت اثربخش شاخص‌های M6 و M9 حذف شدند و شاخص‌های برگزیده برابر نمودار ۳ است.



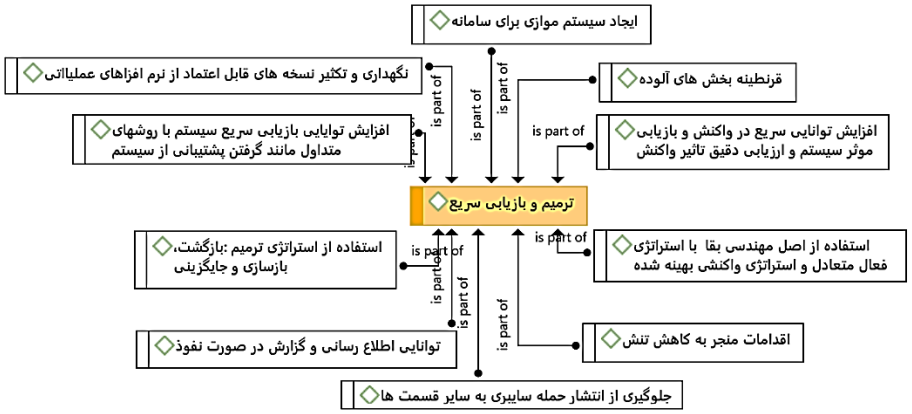
نمودار ۳. شاخص‌های مقاومت اثربخش

در واکنش مؤثر شاخص V10 طبق نظر صاحب‌نظران دارای مقدار کمتر ۰/۷۹ بوده؛ لذا حذف شدند و شاخص‌های برگزیده برابر نمودار ۴ است.



نمودار ۴. شاخص‌های برگزیده واکنش مؤثر

و در ترمیم و بازیابی سریع T7 دارای CVI کمتر از ۰/۷۹ بود و حذف شد و شاخص‌های برگزیده برابر نمودار ۵ است.



نمودار ۵. شاخص‌های ترمیم و بازیابی سریع

اهمیت شاخص‌ها با استفاده از پرسش‌نامه با طیف لیکرت پنج‌گزینه‌ای (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) توسط جامعه نمونه ارزیابی شد؛ سپس با کمک نرم‌افزار SPSS با استفاده از آزمون فریدمن شاخص‌ها رتبه‌بندی شدند.

تاب‌آوری تطبیقی در مجموع با ۳۳ شاخص مربوط به دو مؤلفه پیش‌بینی صحیح و مقاومت اثربخش مورد ارزیابی جامعهٔ نمونه قرار گرفت که در مؤلفه پیش‌بینی صحیح نتایج رتبه‌بندی ۱۳ شاخص آن برابر جدول ۳ است.

جدول ۳. رتبه‌بندی شاخص‌های پیش‌بینی صحیح بر اساس آزمون فریدمن

ردیف	شاخص	رتبه میانگین
۱	برآورد به‌روز آخرین وضعیت منابع سایبری	۹/۳۰
۲	استفاده از سیستم خودکار و خودمختار در پیش‌بینی صحیح	۸/۸۱
۳	پیش‌بینی صحیح و ارتقا با افزایش غیرخطی هوش ماشینی	۸/۰۸
۴	تجزیه‌وتحلیل خودکار با هوش مصنوعی صحیح	۷/۹۰
۵	نظارت بر شبکه	۷/۸۳
۶	توسعه سامانه‌های تبادل اطلاعات سایبری جهت تبادل اطلاعات به‌روز	۷/۷۶
۷	استفاده از سیستم تشخیص نفوذ	۷/۶۲
۸	نظارت بر فعالیت کاربران و فعالیت تأمین‌کنندگان	۶/۸۳
۹	استفاده از الگوریتم‌های چندجانبه برای حفظ حریم خصوصی	۶/۴۳
۱۰	تدوین طرح‌های الزامات امنیتی جهت ایمن‌سازی محصولات	۵/۸۷
۱۱	واقع‌گرایانه بودن اقدامات سایبری صحیح	۵/۵۲
۱۲	شناسایی آسیب‌های احتمالی	۴/۹۴
۱۳	تأثیرات زیاد یادگیری ماشین	۴/۱۱

در مؤلفه مقاومت اثربخش بر اساس آزمون فریدمن نتایج رتبه‌بندی شاخص‌های آن مطابق جدول ۴ است.

جدول ۴. رتبه‌بندی شاخص‌های مقاومت اثربخش بر اساس آزمون فریدمن

ردیف	شاخص	رتبه میانگین
۱	نظارت و آگاهی از موقعیت تهدید	۱۲/۸۸
۲	ایجاد قابلیت تحرک در دارایی‌های سایبری	۱۲/۸۶
۳	عدم تداوم استفاده از سامانه‌ای به‌تنهایی در فرماندهی و کنترل	۱۲/۷۰
۴	ایجاد افزونگی در سامانه فرماندهی و کنترل	۱۲/۵۶
۵	ایجاد تنوع در سامانه‌های فرماندهی و کنترل	۱۲/۲۵
۶	رویکرد حفاظت یا قربانی کردن اطلاعات برای حفظ شبکه بزرگ‌تر	۱۱/۹۵
۷	مشخص کردن سیاست‌ها و رویه‌های سایبری سازمان	۱۱/۶۳
۸	محدودیت در استفاده و دسترسی در سامانه فرماندهی و کنترل	۱۱/۴۵
۹	کاهش وابستگی زیرساختی	۱۰/۹۳
۱۰	افزایش موانع در مقابل حمله دشمن در راستای افزایش هزینه‌های او	۱۰/۴۹
۱۱	حفاظت هماهنگ چندلایه	۱۰/۴۸
۱۲	مهاجرت به سیستم‌عامل‌های بومی متن‌باز	۱۰/۴۷

۱۳	تعیین راهبرد مدیریت خطرات	۹/۹۵
۱۴	استفاده از تکنیک‌های فریب در جهت گمراه کردن دشمن	۹/۷۲
۱۵	ایجاد آگاهی و آموزش ریسک سایبری در کارمندان	۹/٤۷
۱۶	استفاده از رمزکننده‌های بومی	۹/۲۱
۱۷	تقسیم‌بندی و جداسازی پویا در سامانه‌های سایبری	۸/۸۳
۱۸	توسعه و به‌کارگیری حفاظت‌های مناسب به‌منظور اطمینان از استمرار ارائه خدمات زیرساخت	۸/۸۲
۱۹	ایجاد سامانه‌های پاسخ خودکار به شرایط نامطلوب احتمالی یا مشکوک	۷/٦٦
۲۰	تغییر تنظیمات سامانه‌ها بر اساس اطلاعات به‌دست‌آمده از تهدیدات	۵/٦۹

پاسخگویی تاب‌آور در مجموع با ۲۱ شاخص مربوط به دو مؤلفه واکنش مؤثر و ترمیم و بازیابی سریع مورد ارزیابی جامعه نمونه قرار گرفت که در مؤلفه واکنش مؤثر رتبه‌بندی شاخص‌های آن برابر جدول ۵ است.

جدول ۵. رتبه‌بندی شاخص‌های واکنش مؤثر بر اساس آزمون فریدمن

ردیف	شاخص	رتبه میانگین
۱	جداسازی منابع آسیب‌پذیر	۷/٤۲
۲	حفظ تداوم عملیات سایبری	۷/۲۹
۳	تجزیه‌وتحلیل رویدادهای گزارش‌شده	۷/۰۵
۴	تقسیم مسئولیت‌ها در برابر حوادث سایبری	۷/۰۱
۵	چابکی و پاسخ مؤثر و به‌موقع	٦/۹۷
۶	آمادگی برای مقابله با اختلال، پاسخگویی به حوادث و مدیریت بحران	٦/۹۷
۷	ایجاد وحدت تلاش در برابر حوادث سایبری	۵/۱۳
۸	ایجاد سامانه‌های اس.او. سی و سرت در سازمان	٤/۹٦
۹	یادگیری، سازگاری و سازمان‌دهی مجدد سازمان	٤/۵۹
۱۰	پاسخ مناسب به خطرات سایبری	٤/٤۰
۱۱	پشتیبانی مناسب اطلاعاتی در واکنش مؤثر	٤/۲۰

در مؤلفه ترمیم و بازیابی سریع بر اساس آزمون فریدمن نتایج رتبه‌بندی شاخص‌های آن مطابق جدول ۶ است.

جدول ۶. رتبه‌بندی شاخص‌های ترمیم و بازیابی سریع بر اساس آزمون فریدمن

ردیف	شاخص	رتبه میانگین
۱	استفاده از راهبرد ترمیم (بازگشت، بازسازی و جایگزینی)	۷/۰۱
۲	استفاده از اصل مهندسی بقا با راهبرد فعال متعادل و راهبرد واکنشی بهینه‌شده	٦/۸۷
۳	توانایی اطلاع‌رسانی و گزارش در صورت نفوذ	٦/۷۵
۴	نگهداری و تکثیر نسخه‌های قابل‌اعتماد از نرم‌افزارهای عملیاتی	٦/٤٦
۵	ایجاد سامانه موازی برای سامانه	۵/٦۹
۶	افزایش توانایی بازیابی سریع سامانه با روش‌های متداول مانند گرفتن پشتیبانی از سامانه	۵/۳۳
۷	قرنطینه بخش‌های آلوده	٤/۷٦
۸	جلوگیری از انتشار حمله سایبری به سایر قسمت‌ها	٤/٤۲
۹	افزایش توانایی سریع در واکنش و بازیابی مؤثر سامانه و ارزیابی دقیق تأثیر واکنش	٤/۳۰
۱۰	اقدامات منجر به کاهش تنش	۳/٤۱

بحث و نتیجه‌گیری

تاب‌آوری در فرماندهی و کنترل سایبری آینده، برآیند دو بُعد تاب‌آوری تطبیقی و پاسخگویی تاب‌آور است. مهم‌ترین عوامل برای دستیابی به پیش‌بینی صحیح، توانایی برآورد به‌روز آخرین وضعیت منابع سایبری است؛ این امر با استفاده از خودکاری و خودمختاری سامانه‌هایی تسهیل شده است که با افزایش غیرخطی هوش ماشینی ارتقا یافته‌اند و امکان تجزیه‌وتحلیل خودکار با هوش مصنوعی را دارند. از طرف دیگر برای ایجاد مقاومت اثربخش مهم‌ترین اقدام‌های نظارت و آگاهی از موقعیت تهدید، ایجاد قابلیت تحرک در دارایی‌های سایبری، عدم تداوم استفاده از یک سامانهٔ فرماندهی و کنترل به‌تنهایی و ایجاد افزونگی و تنوع در سامانه فرماندهی و کنترل است؛ لذا پیش‌بینی صحیح حاصل‌شده و بر مبنای آن مقاومت اثربخش انجام می‌شود و تاب‌آوری تطبیقی در فرماندهی و کنترل سایبری ایجاد می‌گردد، اما تکمیل تاب‌آوری فرماندهی و کنترل سایبری، مستلزم وجود پاسخگویی تاب‌آور است.

مهم‌ترین ویژگی‌های مؤلفه واکنش مؤثر در این بُعد، جداسازی منابع آسیب‌پذیر، حفظ تداوم عملیات سایبری، تجزیه‌وتحلیل رویدادهای گزارش‌شده و تقسیم مسئولیت‌ها در برابر حوادث سایبری است.

مؤلفه دیگر این بعد ترمیم و بازیابی سریع از رخداد سایبری است که این موضوع مستلزم استفاده از راهبرد ترمیم است که با توجه به میزان و نوع خسارت یکی از راهبرهای بازگشت، بازسازی و جایگزینی انتخاب می‌شود. استفاده از اصل مهندسی بقا با راهبرد فعال متعادل و راهبرد واکنشی بهینه‌شده در رتبه بعدی اهمیت این حوزه قرار دارد.

پیشنهادهای زیر برای تاب‌آوری در فرماندهی و کنترل سایبری آینده بر پایه دو بُعد تاب‌آوری تطبیقی و پاسخگویی تاب‌آور ارائه می‌شود:

۱- توسعهٔ هوش مصنوعی و یادگیری ماشین: سرمایه‌گذاری در تحقیق و توسعه هوش مصنوعی و یادگیری ماشین برای بهبود توانایی سیستم‌ها در پیش‌بینی تهدیدات، تجزیه‌وتحلیل خودکار داده‌ها و اتخاذ تصمیمات سریع‌تر و دقیق‌تر.

۲- خودکارسازی و خودمختاری سیستم‌ها: افزایش سطح خودکارسازی و خودمختاری در سیستم‌های فرماندهی و کنترل برای کاهش دخالت انسان و تسریع در پاسخ به تهدیدات.

۳- ایجاد تنوع و افزونگی در سیستم‌ها: طراحی و پیاده‌سازی سیستم‌های فرماندهی و کنترل با معماری‌های متنوع و افزونه برای کاهش آسیب‌پذیری در برابر حملات متمرکز.

توسعه قابلیت‌های تحرک در دارایی‌های سایبری: افزایش قابلیت تحرک داده‌ها و خدمات برای جلوگیری از تمرکز در یک نقطه و کاهش ریسک از دست رفتن اطلاعات.

۴- ایجاد سیستم‌های نظارت و آگاهی از موقعیت تهدید پیشرفته: توسعه سیستم‌های نظارت مداوم بر محیط سایبری برای شناسایی زودهنگام تهدیدات و پاسخگویی سریع.

۵-تقویت زیرساخت‌های ارتباطی: سرمایه‌گذاری در زیرساخت‌های ارتباطی امن و پایدار برای اطمینان از تداوم عملیات در شرایط بحرانی.

۶- آموزش و ارتقای آگاهی کارکنان: برگزاری دوره‌های آموزشی مستمر برای ارتقای آگاهی کارکنان در زمینه امنیت سایبری و توانمندسازی آن‌ها برای مقابله با تهدیدات.

ایجاد برنامه‌های بازیابی سریع و جامع: تدوین برنامه‌های بازیابی سریع و جامع برای بازگرداندن سیستم‌ها به حالت عادی پس از وقوع حادثه سایبری.

توجه به نکات زیر برای اجرای مؤثر این پیشنهادها ضروری است:

۱- تخصیص بودجه کافی: اختصاص بودجه کافی برای اجرای پروژه‌های مرتبط با افزایش تاب‌آوری در حوزه فرماندهی و کنترل سایبری.

۲- به‌روزرسانی مداوم تهدیدات: به‌روزرسانی مداوم اطلاعات در مورد تهدیدات سایبری و تطبیق راهکارهای دفاعی با تهدیدات جدید.

با اجرای این پیشنهادها، می‌توان به سطح بالاتری از تاب‌آوری در فرماندهی و کنترل سایبری دست یافت و از سیستم‌ها در برابر حملات سایبری محافظت کرد.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱- توسعهٔ هوش مصنوعی و یادگیری ماشین
۲- خودکارسازی و خودمختاری سیستم‌ها
۳- ایجاد تنوع و افزونگی در سیستم‌ها
۴- توسعه قابلیت‌های تحرک در دارایی‌های سایبری
۵- ایجاد سیستم‌های نظارت و آگاهی از موقعیت تهدید پیشرفته
۶- تقویت زیرساخت‌های ارتباطی
۷- آموزش و ارتقای آگاهی کارکنان
۸- ایجاد برنامه‌های بازیابی سریع و جامع

قدردانی

از کلیه اندیشمندان و پژوهشگرانی که در خلال تحقیق خالصانه دیدگاه‌ها و نقطه نظرات علمی و کارشناسی خود را ارائه کردند، تشکر و قدردانی می‌شود.

تضاد منافع

بدین‌وسیله نویسندگان تصریح می‌نمایند که هیچ‌گونه تضاد منافعی در خصوص پژوهش حاضر وجود ندارد.

منابع فارسی و انگلیسی

- تقی‌پور، رضا. (۱۳۹۷). طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، سال هشتم، شماره سی‌ام، ۱۸۲-۲۰۲.

قاسمی، محمد. آذر، داود و سجادی اصیل، وحید. (۱۴۰۲). الگوی ارزیابی قدرت آفند سایبری ارتش جمهوری اسلامی ایران، علوم و فنون نظامی، ۱۹(۶۴)، ۳۵-۶۱.

قاسمی، محمد، محمدزهرایی، سپهر و خاکپور فریبرز. (۱۴۰۳). کلیات جنگ سایبری (مبتنی بر C4I)، چاپ دوم، تهران: انتشارات دافوس آجا.

- نصرت آبادی, جمشید , لشکریان, حمیدرضا , مردانی, محمد و موحدی صفت, محمدرضا. (۱۳۹۸). مقاله پژوهشی:ارائه الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران. امنیت ملی۹(۳۱)؛ ۱۷۳-۱۹۸.

- Adam S. Morgan, Steve W. Stone, 2019, Command and Control for Cyberspace Operations - A Call for Research, Military Cyber Affairs, Vol. 4, Iss. 1, Art. 4, DOI: https://doi.org/10.5038/2378-0789.4.1.1051
- Apruzzese, Giovanni and others, (2018), 'On the Effectiveness of Machine and Deep Learning for Cyber Security' in Tomáš Minárik, Raik Jakschis and Lauri Lindström (eds), 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects (NATO CCDCOE). https://doi.org/10.23919/CYCON.2018.8405026
- Department of Defense Instruction, (2019) Cybersecurity, NO 8500.01, Incorporating Change 1. URL: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf
- Department Of Defense, (2015), Task Force Report: Resilient Military Systems And The Advanced Cyber Threat, Office Of The Secretary Of Defense 3140 Defense Pentagon Washington, DC. https://defenseinnovationmarketplace.dtic.mil/wpcontent/uploads/2018/04/Resilient_Military_Systems_Cyber_Threat.pdf
- Department of Defense, 2018, Joint Publication 3-0, P; XXii. https://www.moore.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/JP%203-0.pdf
- Ghasemi, Mohammad, Azar, Davoud and Sajjadi Asil, Vahid. (2019). Model for evaluating the cyber offensive power of the Islamic Republic of Iran Army. Military Sciences and Technologies, 35-61, 19.(٦٤). [in persian]. https://doi.org/10.22034/qjmst.2023.550347.1678
- Ghasemi, Mohammad, Mohammad Zahraei, Sepehr and Khakpour Fariborz, (2020), Generalities of Cyber Warfare (Based on C4I), Second Edition, Dafoos AJA Publications, Tehran. Iran. [in persian]
- Kott, Alexander, and others, (2018), Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153, US

Army Research Laboratory, ARL-SR-0396. https://doi.org/10.48550/arXiv.1804.07651

- MacKinnon, Marc, Fernandes, Mark, 2018, Take the lead on cyber risk How to move from now to next-level security, Deloitte, UK. www2.deloitte.com
- Nosratabadi, Jamshid, Lashkarian, Hamid Reza, Mardani Shahr Babak, Mohammad and Movahedi Sefat, Mohammad Reza. (2018). Presenting a model for evaluating the cyber power of the Islamic Republic of Iran Army, National Security Quarterly, National Defense University, 173-198. [in persian]. DOI; https://dor.isc.ac/dor/20.1001.1.33292538.1398.9.31.7.1
- Parend, Pierre, and others, (2018), Foundations and Applications of Artificial Intelligence for Zero-Day and Multi-Step Attack Detection, 4 EURASIP Journal on Information Security. DOI:10.1186/s13635-018-0074-y
- Perkins, D. G. & Holmes, J. M. 2018. "Multi-Domain Battle, Converging Concepts Toward a Joint Solution", in Joint Forces Quarterly, 88, (1st Quarter 2018): 54-57, 55. URL: https://jis-eurasipjournals.springeropen.com/counter/pdf/10.1186/s13635-018-0074-y.pdf
- Pomerleau, M. (2018, March). Cyber Command granted new, expanded authorities. C4ISRNet. https://www.c4isrnet.com/dod/cybercom/2018/02/28/cyber-command-granted-new-and-expanded-authorities/
- The White House. (2016, July 26). Presidential Policy Directive -- United States Cyber Incident Coordination. Whitehouse.gov; Whitehouse. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Ross, R. Pillitteri, V. Graubart, R. Bodeau, D. & McQuaid, R. (2019). Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1
- Stone, S. 2016. "Factors related to agility in allocating decision-making rights for cyberspace operations." Doctoral dissertation, Robert Morris University. URL: https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/54da5be5e4b0e9d26e577151/1423596517506/096.pdf
- Taghipour, Reza, (2018), Designing a conceptual model of the cyber defense model of the Islamic Republic of Iran, National Security Quarterly, Year 8, Issue 30, 182-202. [in persian]. URL: https://ns.sndu.ac.ir/article_349_8f9a149f221098a0ef97f71f6e9aa523.pdf
- Tammet, Tanel, (2021) Autonomous Cyber Defence Capabilities, Autonomous Cyber Capabilities under International Law, NATO CCDCOE Publications, Chapter 3. URL: https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf
- Thomas H, Hedgecock, Daniel A, and Pendergrass, J. Aaron, (2021) The State of Cyber Resilience: Now and in the Future, Johns Hopkins APL Technical Digest, Volume 35, No 4. URL: https://www.jhuapl.edu/Content/techdigest/pdf/V35-N04/35-04-Llanso.pdf
- Joint Chiefs of Staff. (2016, January 14). Cross-domain synergy: Overview. United States Department of Defense. URL:

https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230

- U.S. Department of Defense. 2014. Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. URL: http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf
- US Department of Homeland Security, 2018, Cyber Resilience and Response, Public-Private Analytic Exchange Program, PP 8-10. https://www.dhs.gov/publication/aep-overview-and-documents
- Van Kessel, Paul, (2017), Path to cyber resilience: Sense, resist, react, EY's 19th Global Information Security Survey. https://www.swisstreasurer.ch/wp-content/uploads/2015/11/GISS_2016_Report_Final.pdf