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

The ecosystem of cyber defense cognitive readiness

Morteza Talebi [1]✉ | **Hasan Mahjoub Eshratabadi** [2]

1. Assistant Professor of Strategic Management, IRI Military Command and Staff University, Tehran, Iran. (Corresponding Author). E-mail: m.talebi@casu.ac.ir
2. Associate Professor of Higher Education, Shahid Satari University, Tehran, Iran. E-mail: hassanmahjub@ut.ac.ir

Article Info

Article type:
Research Article

Article history:
Received:
2024-10-10
Received in revised form:
2024-11-15
Accepted:
2024-11-18
Published online:
2024-11-21

Keywords:
Cyberspace, cyber defense, defense readiness, cognitive readiness, cyber defense cognitive readiness system

ABSTRACT

Background and Objective: In an increasingly complex defense landscape, particularly in the cyber domain, the armed forces must adapt to meet new challenges. This research aims to define the cognitive readiness ecosystem essential for cyber defense, highlighting the key components and influencing factors involved.
Methodology: This study employs a mixed-methods approach, combining qualitative and quantitative strategies. Meta-composition and content analysis were used for qualitative data, while descriptive statistics and factor analysis, aided by SmartPLS software, focused on validating the conceptual model.
Findings: Our analysis shows that cognitive readiness in cyber defense includes dimensions such as personnel readiness, cyber technologies, and cognitive processes, influenced by various factors. Confirmatory factor analysis revealed significant relationships between these dimensions and their constructs, confirming that our data aligns with the proposed factor structure.
Conclusion: Cyber defense readiness is a cohesive ecosystem consisting of processes, technologies, and environmental factors. By identifying the cognitive readiness needed for effective cyber defense, we enable personnel to transfer their knowledge across different scenarios, minimizing retraining needs and enhancing overall operational efficiency. This approach strengthens our future defense capabilities.

Cite this article: Talebi, M , & Mahjub, H. (2024). The ecosystem of cyber defense cognitive readiness. Defensive Future Studies, 9(34), 147- 182.

DOI: 10.22034/dfsr.2024.2043105.1838

Publisher: IRI Military Command and Staff University

Extended Abstract

Introduction:
The increasing usefulness and reliance on cyber systems for military operations, the expansion of conflicts to this space, and the use of technologies in this area in the form of cyber weapons to threaten countries in the form of cyber warfare have revealed the need to develop and expand the concepts of cyber defense readiness as a strategy to prevent and reduce damage to the national interests of countries. This space, as an ecosystem with a technological-social nature, has the dimensions of technology, humans (defender, attacker, and user), and processes[1]. Defending such a space also requires a systems approach that, in addition to its physical, informational, and cognitive layers, includes technological, process, and other components and factors that affect it. By identifying the cognitive limitations of human agents in the face of cyber threats and attacks, this approach identifies the cognitive readiness required for cyber defense and allows them to transfer their learning from one system or scenario to another, often without the need for retraining.[2]

Methodology:
This research, based on its objective is applied, employs a descriptive and analytical method, and in terms of its approach, it is a mixed-methods study of the sequential exploratory type. In the qualitative part of the research, the factors affecting the cognitive readiness of cyber defense and its constituent components were identified using a qualitative method of meta-synthesis and content analysis with open, axial, and selective coding. In the next stage, the initial model was completed and modified based on the opinions of experts. The validation of the designed model was obtained using a researcher-made questionnaire by holding focus group sessions in the presence of experts. The sample size, calculated using Cochran's formula for an undefined population, was 155. A questionnaire with 63 questions was provided to the statistical community of the quantitative section of the research. For the analysis of quantitative data, descriptive statistics were used, and for evaluating the fit of the conceptual model of the cybersecurity cognitive preparedness system, structural equation

modeling, factor analysis (first and second order), and the Smart PLS software were employed.

Findings:

After combining similar codes, subcomponents and components were identified and grouped together to form concepts, and categories were created from the combination of similar concepts. As a result of coding, removing duplicate codes, and final data summarization, 63 codes, 4 concepts (dimensions) including cybercognitive technologies, cybercognitive processes, cognitive readiness components and factors affecting cyber defense cognitive readiness, and 9 main components including artificial intelligence technology, data mining technology, immersive technology, cybercognitive situational awareness, cyber self-awareness, main cognitive executive functions, high-level cognitive functions, perception of environmental factors and enabling resources with relevant subcomponents were identified and extracted. Finally, by inviting experts again and forming focus groups during two stages, experts confirmed the overall work, proposed corrective points of view, and the final validation of the conceptual model was carried out.

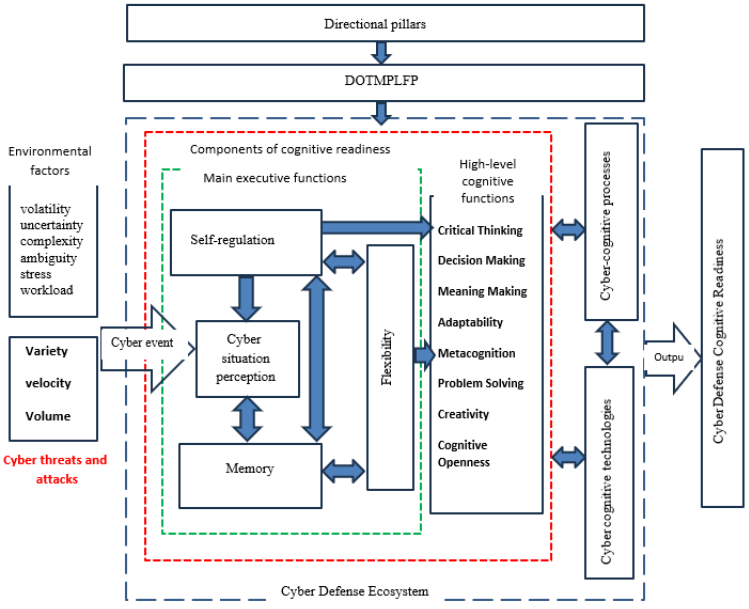


Figure 1. Conceptual model of cyber defense cognitive readiness ecosystem

It is a hierarchical model, to more accurately measure the main structure of cyber defense cognitive readiness, two levels of structures have been designed. For model fitting in structural equation modeling, measurement model fitting, structural model fitting, and general model fitting have been used.

To fit the measurement model, the reliability criteria of the indicator (combined reliability and factor loading coefficients), convergent validity (shared variance root), and model divergence (Fornell and Larker criterion) were used.

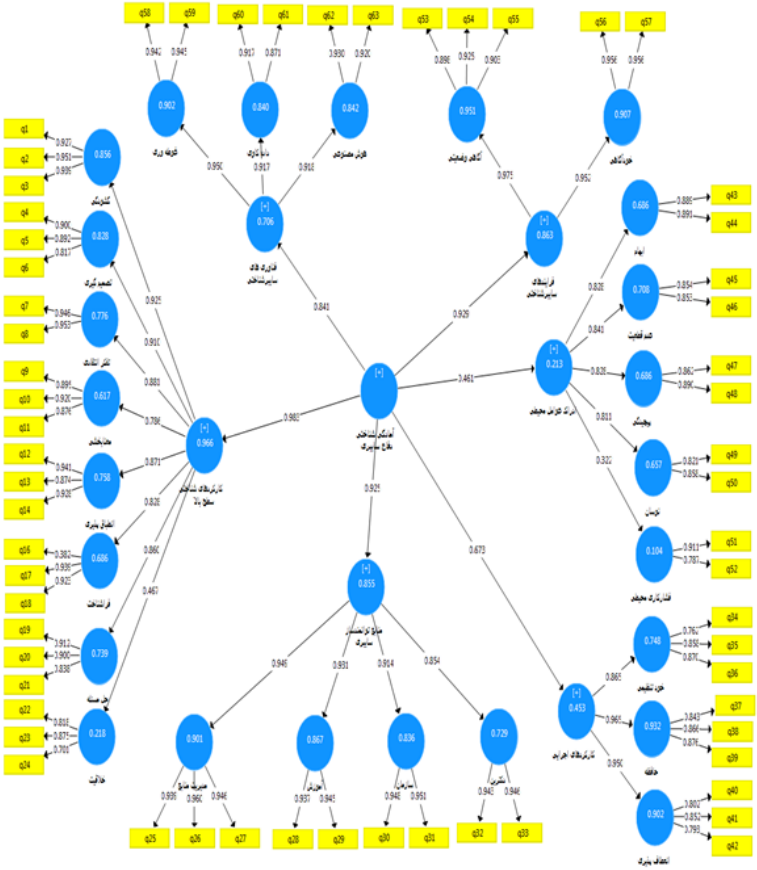


Figure 2. Model of constructs, components, and indicators of the cyber defense cognitive readiness ecosystem

Since the research model is hierarchical, the factor loadings of the questions, constructs, and components must also be calculated.

Calculating the significance coefficients of the factor loadings shows that all factor loadings are significant at the 95% confidence level.

- Composite Reliability:

The composite reliability of the components and constructs is greater than 0.7.

- Convergent Validity of the Model:

The Average Variance Extracted (AVE) for all constructs is greater than 0.5.

- Discriminant Validity of the Measurement Model:

Fornell and Larker criterion: The square root of the shared variance of all constructs in the higher-level cognitive functions and executive functions (matrix diagonal values) is greater than the correlation of each construct with other constructs (matrix cell values), confirming the convergent validity of the model using the Fornell and Larker criteria.

- Structural model fit assessment

The structural part of the model indicators (Q2 criterion and Red variability) also shows that the relationships between the latent constructs are correctly mapped.

- Overall model fit assessment

According to the above, the overall model fit indices (GOF and SRMR criteria) also show that the overall cyber defense cognitive readiness model has an acceptable fit.

Discussion and Conclusion

The most valuable skill or characteristic of a cybersecurity workforce is cognitive readiness, enabling individuals to transfer their learning from one system or scenario to another, often without requiring retraining. In this research, cognitive readiness emphasizes mental preparedness and the set of knowledge, abilities, and skills necessary for effective performance by cyber defense personnel when confronting cyber environmental factors.

Analysis of the findings reveals that the cyber defense readiness system is a cognitive ecosystem comprised of processes, technologies, cognitive readiness components, and environmental factors influencing it, forming a socio-technical ecosystem with components including

input, process, output, feedback, environmental factors, and consequences. The final model obtained indicates that in cyber defense operations, adopting a purely technological approach without considering the knowledge, skills and qualifications of cyber defense personnel is doomed to failure.

In this research, effective cyber defense requires addressing dimensions such as; the cognitive readiness of cyber defense personnel, cyber technologies (to reduce cognitive load and improve cognitive skills), cyber cognitive processes (such as situational awareness and self-awareness), environmental factors, and enabling resources. This approach has attempted to identify the cognitive readiness required for cyber defense by identifying the cognitive limitations of human factors when facing cyber threats and attacks.

Given the importance of the cognitive aspects of cyber defense users, technologies, and cyber-cognitive technologies, the following suggestions are offered for future research in this area:

• Employing emerging technologies such as artificial intelligence, immersive technologies, and big data to reduce cognitive load and enhance the cognitive preparedness components of cyber defense personnel

• In the strategic programs for improving the cyber readiness of the Islamic Republic of Iran's armed forces, the cyber defense ecosystem approach of this research and the empowerment and enhancement of cognitive competencies alongside technical competencies should be considered

References:

1. Al Sabbagh, B. & Kowalski (2017). Socio-Technical SIEM (ST-SIEM): Towards Bridging the Gap in Security Incident Response. International Journal of Systems and Society (IJSS). 4. 8-21. 10.4018/IJSS.2017070102. DOI:10.4018/978-1-7998-7705-9.ch009
2. Talebi, Morteza; Mahjoob Eshratabadi, Hassan and Aghaei, Mohsen (1403). Cognitive readiness components of cyber defense in the military domain. Quarterly Journal of Military Sciences and Technologies, Volume 20, Number 68, 1403, Pages 68-39. 10.22034/qjmst.2024.2018685.1994

فصلنامه علمی آینده‌پژوهی دفاعی
شاپای چاپی: ۲۵۸۸-۲۲۸X شاپای الکترونیکی: ۲۶۴۵-۷۱۷۲ http://www.dfsr.ir/
دانشگاه فرماندهی و ستاد آجا

زیست‌بوم آمادگی شناختی دفاع سایبری

مرتضی طالبی[۱] ✉ | حسن محجوب عشرت‌آبادی[۲]

۱. استادیار مدیریت راهبردی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. (نویسنده مسئول) رایانامه: m.talebi@casu.ac.ir

۲. دانشیار آموزش عالی، دانشگاه شهید ستاری، تهران، ایران. رایانامه: hassanmahjub@ut.ac.ir

اطلاعات مقاله

نوع مقاله:
پژوهشی

تاریخچه مقاله:

تاریخ دریافت:
۱۴۰۳/۰۷/۱۹

تاریخ بازنگری:
۱۴۰۳/۰۸/۲۵

تاریخ پذیرش:
۱۴۰۳/۰۸/۲۸

تاریخ انتشار:
۱۴۰۳/۰۹/۰۱

کلیدواژه‌ها:
فضای سایبر، دفاع سایبری، آمادگی دفاعی، آمادگی شناختی، نظام آمادگی شناختی دفاع سایبر

چکیده

زمینه و هدف: پیچیدگی و عدم قطعیت در محیط‌های دفاعی مدرن مانند عرصه سایبری به معنای تغییر نیازهای آتی نیروهای مسلح و ضرورت خلق شایستگی‌ها و قابلیت‌های دفاعی جدید است. پژوهش حاضر با هدف تعریف زیست‌بوم آمادگی شناختی دفاع سایبری، مؤلفه‌های آمادگی شناختی موردنیاز محیط دفاع سایبری و عوامل مؤثر بر آن را در قالب یک زیست‌بوم مطرح کرده است.

روش‌شناسی: این پژوهش از حیث هدف، کاربردی و رویکرد آن در جمع‌آوری و تجزیه‌وتحلیل داده‌ها آمیخته است. در بخش کیفی از روش فراترکیب و تحلیل محتوا و برای تجزیه‌وتحلیل داده‌های کمّی از آمار توصیفی و برای ارزیابی برازش مدل مفهومی از روش تحلیل - عاملی و نرم‌افزار اسمارت پی.ال.اس استفاده شده است.

یافته‌ها: نتایج بخش کیفی پژوهش نشان داد که آمادگی شناختی دفاع سایبری، دارای ابعاد آمادگی شناختی کارکنان، فناوری‌های سایبری، فرایندهای سایبر شناختی و عوامل مؤثر هستند. نتایج تحلیل عاملی تأییدی نشان داد مؤلفه‌های آمادگی شناختی دفاع سایبری و عوامل مؤثر بر آن دارای بار عاملی و تأثیر معنی‌داری بر سازه‌های مربوطه است وداده‌های حاصل از این پژوهش با ساختار عاملی این مقیاس، برازش مناسبی دارد.

نتیجه‌گیری: آمادگی دفاع سایبری، زیست‌بومی متشکل از فرایندها، فناوری‌ها، مؤلفه‌های آمادگی شناختی و عوامل محیطی مؤثر بر آن در قالب یک زیست‌بوم فنی – اجتماعی با اجزا: درون‌داد، فرایند، برون‌داد، بازخور، عوامل محیطی و پیامدها است. شناسایی آمادگی‌های شناختی موردنیاز برای دفاع سایبری این امکان را می‌دهد که کارکنان اغلب بدون نیاز به آموزش مجدد، یادگیری خود را از یک سیستم یا سناریو به سیستم یا سناریوی دیگر انتقال دهند.

استناد: طالبی، مرتضی و محجوب عشرت‌آبادی، حسن. (۱۴۰۳). زیست‌بوم آمادگی شناختی دفاع سایبری. آینده‌پژوهی دفاعی، ۹ (۳۴)، ۱۴۷- ۱۸۲.

DOI: 10.22034/dfsr.2024.2043105.1838

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

هدف غایی و نهایی تمام اشکال منازعات و جنگ‌ها تسلط بر ذهن و اخلال در فرایندهای شناختی مخاطب به‌منظور تحمیل ارادهٔ خود بر اوست و فضای سایبری یکی از بهترین و کم‌هزینه‌ترین روش‌ها برای نیل به این مقصود است. بخش قابل‌توجهی از جنگ‌های بین کشورها در سالیان اخیر به جنگ‌های سایبری و فناورانه تغییر شکل داده است (حسین‌زاده و همکاران، ۱۴۰۳). افزایش کاربرد و تکیه بر فناوری‌های سایبری در عملیات نظامی منجر به معرفی این فضا به‌عنوان عرصهٔ پنجم نبرد بعد از زمین، دریا، هوا و فضا شده است. افزایش سودمندی و اتکا به سامانه‌های سایبری برای انجام عملیات نظامی، گسترش منازعات به این فضا و استفاده از فناوری‌های این حوزه در قالب تسلیحات سایبری برای تهدید کشورها به شکل جنگ سایبری، لزوم توسعه و گسترش مفاهیم آمادگی دفاع سایبری را به‌عنوان راهبردی جهت جلوگیری و کاهش خسارت وارده به منافع ملی کشورها، آشکار کرده است. این امر از طریق سرمایه‌گذاری در واحدهای دفاع سایبری، آموزش دفاع سایبری و به رسمیت شناختن فضای سایبری به‌عنوان عرصه عملیات (ناتو، ۲۰۱۶) مشخص می‌شود. این فضا به‌عنوان زیست‌بومی با ماهیت فناورانه - اجتماعی دارای ابعاد فناوری، انسان (مدافع، مهاجم و کاربر) و فرایندها است (الصباغ و کوالسکی[1]، ۲۰۱۷) . دفاع از چنین فضایی نیز نیازمند رویکرد سیستمی است که علاوه بر لایه‌های فیزیکی و اطلاعاتی و شناختی آن جنبه‌های فناورانه، فرایندی و سایر اجزاء و عوامل تأثیرگذار بر آن را نیز در برگیرد.

پویایی و پیچیدگی همراه با ابهام و عدم قطعیت در عرصهٔ سایبری، به معنای تغییر نیازهای آتی نیروهای مسلح و ضرورت خلق شایستگی‌ها و قابلیت‌های دفاعی جدید است. از جملهٔ این شایستگی‌ها می‌توان به آمادگی‌های شناختی[2]، همراه با تاب‌آوری[3] در مواجهه و دفاع برابر تهدیدات نوظهور خلق‌شده در این فضا اشاره کرد. آمادگی شناختی معطوف به آمادگی ذهنی افراد است که دانش، مهارت و توانایی لازم را در برخورد با محیط‌های آشوبناک، غیرقابل‌پیش‌بینی و پیچیدهٔ عملیات سایبری و همچنین

1. Kowalski & Al Sabbagh
2. Cognitive Readiness
3. Resilience

عکس‌العمل آن‌ها را موردتوجه قرار می‌دهد. این رویکرد با شناسایی محدودیت‌های شناختی عوامل انسانی در مواجهه با تهدیدات و حملات سایبری، نسبت به شناسایی آمادگی‌های شناختی موردنیاز برای دفاع سایبری اقدام کرده و به او این امکان را می‌دهد که اغلب بدون نیاز به آموزش مجدد، یادگیری خود را از یک سیستم یا سناریو به سیستم یا سناریوی دیگر انتقال دهد (طالبی و همکاران، ۱۴۰۳).

در حال حاضر حمله‌ها و تهدیدهای پیشرفته پایدار هوشمند[1] به نقاط ضعف و آسیب‌پذیری‌ها، بیشتر به بخش کاربران تمرکز دارد و علی‌رغم ورود سامانه‌های خودکار و هوشمند، توجه به شایستگی‌های تحلیلی تصمیم‌گیرندهٔ انسانی از طریق بهره‌برداری از فرایندهای شناختی جهت مقابله با این تهدیدها، هنوز هم ناگزیر و ضروری است. انسان با محدودیت‌های شناختی خود، ضعیف‌ترین و درعین‌حال مؤثرترین حلقهٔ زنجیره امنیت و دفاع سایبری است. عدم شناسایی و بهره‌گیری مناسب و نظام‌مند از عوامل توانمندساز و پیشران مانند فناوری‌ها و سامانه‌های سایبر - شناختی (یادگیری ماشین، داده‌کاوی، پردازش زبان طبیعی و ...) برای داده‌کاوی و استخراج اطلاعات، کارکنان و تحلیلگران عملیات دفاع سایبری را علی‌رغم دسترسی به انبوه اطلاعات با فقر دانش در تصمیم‌گیری روبرو کرده است.

از سوی دیگر عوامل مختلف فردی، محیطی و سازمانی مانند فشار کاری و استرس بالا، میزان بالای هشدارهای کاذب، تجربه پایین، وظایف بدون ساختار، منابع نامشخص اطلاعات و عدم وجود معیارهای عملکردی مناسب، رفتار و فرایندهای ذهنی کاربران، تحلیلگران و تصمیم‌گیرندگان دفاع سایبری را به‌شدت تحت تأثیر قرار داده است. مواجهه با این وضعیت از دانش و مهارت‌های شناختی کاربران، تحلیلگران و تصمیم‌گیرندگان دفاع سایبری فراتر رفته است. بدون بهره‌گیری مناسب از فرایندهای شناختی استاندارد به‌عنوان حلقه اتصال فناوری و عامل انسانی در زیست‌بوم دفاع سایبری، امکان ایجاد هماهنگی و هم‌افزایی مقدور نیست.

با توجه به مطالب فوق به دلیل عدم شناسایی، حفظ و تقویت نظام‌مند آمادگی‌های شناختی (دانش، مهارت، توانایی و نگرش) موردنیاز فرد برای ایجاد و حفظ کارایی و اثربخشی شایسته در محیط‌های عملیاتی پیچیدهٔ رزم سایبری، موجب بروز خطاها و

1. Advanced Persistence Threats

سوگیری‌های شناختی و درنتیجه اخذ تصمیم‌ها و اقدام‌های نامناسب دفاع سایبری شده است. دفاع اثربخش در این فضا فقط با اتکا به رویکردهای متداول فناور محور که غالباً به امنیت و دفاع لایه‌های اطلاعاتی و فیزیکی پرداخته و از مهم‌ترین و درعین‌حال آسیب‌پذیرترین لایه، یعنی لایه شناختی غافل است، مقدور نیست.

نظر به موارد فوق هدف اصلی این پژوهش تدوین زیست‌بوم آمادگی شناختی دفاع سایبری هست که بر اساس روش تحقیق کیفی (فراترکیب) با تحلیل محتوای ادبیات آمادگی شناختی به ارائهٔ زیست‌بوم آمادگی شناختی دفاع سایبری پرداخته است و سپس اعتبارسنجی و برازش الگوی مفهومی آمادگی شناختی دفاع سایبری را انجام داده است. منظور از زیست‌بوم آمادگی شناختی دفاع سایبری در این پژوهش آمادگی بر اساس پرسشنامه‌ای است که مبتنی بر آمادگی شناختی کارکنان دفاع سایبری، فناوری‌ها و فرایندهای سایبر شناختی به‌دست‌آمده در بخش کیفی تحقیق ساخته شده است و نمره حاصل از آن به‌عنوان زیست‌بوم آمادگی شناختی دفاع سـایبری محاسبه می‌شود.

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

طبق تعریف ناتو، فضای سایبر، فراتر از شبکهٔ اینترنت است و نه‌تنها شامل سخت‌افزار، نرم‌افزار و سامانه‌های اطلاعاتی، بلکه شامل افراد و تعاملات اجتماعی آن‌ها در داخل این شبکه‌ها نیز هست (کلیمبورگ[1]، ۲۰۱۲). فضای سایبری یک قلمرو جهانی در محیط اطلاعاتی است که از شبکهٔ وابسته به هم از زیرساخت‌های فناوری اطلاعات شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های مربوط به آن‌ها تشکیل‌شده است. محیط اطلاعاتی مجموعه‌ای از افراد، سازمان‌ها و سامانه‌هایی است که اطلاعات را جمع‌آوری، پردازش، انتشار یا عمل می‌کنند. ازآنجایی‌که همه عملیات سایبری نیاز به ایجاد، پردازش، ذخیره‌سازی و یا انتقال اطلاعات دارند، فضای سایبری به‌طور کامل در محیط اطلاعات قرار دارد. محیط اطلاعاتی به ابعاد فیزیکی، اطلاعاتی و شناختی تقسیم می‌شود و شامل بسیاری از انواع اطلاعات غیر در فضای مجازی می‌شود. (نشریه

1. Klimburg

مشترک عملیات سایبری آمریکا[1]، ۲۰۱۸: ۲۷).

با تأکید بر قابلیت استفاده از فناوری‌ها در دفاع سایبری، نیروی انسانی به‌عنوان ضعیف‌ترین حلقه در زنجیرهٔ امنیت شناخته می‌شود؛ بنابراین انسان در زنجیره دفاع سایبری حلقه‌ای ضعیف با جذابیت بالا در معرض تهدیدات و حملات سایبری قرار می‌گیرد (نوبل، ۲۰۱۸). دفاع از این فضا تنها با توجه به لایه‌های فیزیکی و اطلاعاتی، بدون در نظر گرفتن قابلیت‌ها و آمادگی‌های شناختی عنصر مدافع این فضا عملاً ناقص و محکوم به شکست است.

به‌طور ساده شناخت را می‌توان به‌عنوان فرایندها یا جریان‌هایی تعریف کرد که به کمک آن‌ها یادگیری، یادآوری و تفکر صورت می‌پذیرد. به‌طور دقیق‌تر شناخت به فرایندهای درونی ذهن و راه‌هایی که ما به‌وسیله آن‌ها اطلاعات را موردتوجه قرار می‌دهیم، آن‌ها را درک می‌کنیم، به رمز درمی‌آوریم، در حافظه ذخیره می‌کنیم و مورداستفاده قرار می‌دهیم، گفته می‌شود (سیف، ۱۳۸۸). بر اساس تعریف دیگر شناخت، نظامی از باورهاست که افراد برای ادراک، ساخت و معنابخشی به جهان اطرافشان و تصمیم‌گیری دربارهٔ اقداماتشان از آن بهره می‌گیرند. همچنین، شناخت را مجموعه‌ای از دانش‌ها و باورها و فعالیت‌های ذهنی متمرکز بر اکتساب و پردازش اطلاعات تعریف می‌کنند. در واقع تمرکز اصلی شناخت بر درک و فهم فرایندهای فکری و ذهنی انسان است. روان‌شناسی شناختی با توجه به یافته‌های علوم اعصاب شناختی، کارکردهای شناختی انسان از جمله ادراک، توجه، هوشیاری، یادگیری، حافظه، یادآوری، استدلال، تصمیم‌گیری، هوش و خلاقیت را موردمطالعه قرار می‌دهد. روان‌شناسی شناختی به مطالعه فرایندهایی می‌پردازد که پدیدآورنده رفتارهای پیچیده انسانی‌اند (خرازی و تلخابی، ۱۳۹۳).

در حوزهٔ شناختی مجموعه‌ای اصلی از فرایندهای شناختی به نام کارکردهای اجرایی (کنترل شناختی) نهفته است که به ما کمک می‌کند تا تعاملات خود را با دنیای بیرون و دنیای درون هدایت، برنامه‌ریزی، شروع، توقف، نظارت و اصلاح کنیم. این مجموعه مانند یک تیم مدیریت یا «سیستم اجرایی» برای همه جنبه‌های شناخت و رفتار است. «عملکردهای اجرایی» یک اصطلاح چتر برای عملکردهایی مانند برنامه‌ریزی، حافظه

1. JP 3-12

کاری، بازداری، انعطاف‌پذیری ذهنی، خودتنظیمی و همچنین شروع و نظارت بر عمل است. کارکردهای اجرایی کارکردهای شناختی انعطاف‌پذیر، هدفمند و سازگار هستند. آن‌ها معمولاً بیشتر درگیر موقعیت‌های بدیع و چالش‌برانگیز هستند (ریموند[1] و دیگران، ۲۰۰۸). این کارکردهای شناختی اصلی (کارکردهای اجرایی) به ما کمک می‌کنند تا با استخراج «منابع» اضافی از یادگیری و حافظه قبلی‌مان، کارکردهای اجرایی درجه بالاتری (تصمیم‌گیری، حل مسئله، استدلال و ...) بسازیم؛ بنابراین کارکردهای اجرایی مرتبه بالاتر ترکیبی از کارکردهای اجرایی اصلی هستند که از واحدهای «دانش» از آنچه قبلاً آموخته‌ایم یا می‌توانیم به خاطر بسپاریم، استفاده می‌کنند. این واحدهای دانش شامل همه‌چیز از زبان، تجربیات، خاطرات، انتظارات و احساسات است (دیموند[2]، ۲۰۱۳).

یکی از مهم‌ترین دلایل توجه به آمادگی شناختی در محیط‌های نظامی و دفاع سایبری، سرعت تغییر و تحول بسیار بالا در این محیط‌ها است. بن اشر و گونزالز[3] (۲۰۱۵) پیشنهاد می‌کنند که کاربران سایبری به دانش نظری به‌روز، تجربه عملی و آموزش نحوه «یادگیری سریع و سازگاری با محیط‌های جدید و پویا» نیاز دارند. محیط سازمان‌ها تحت تأثیر چهار عامل بی‌ثباتی (سرعت و پویایی تغییر)، عدم قطعیت (غیرقابل‌پیش‌بینی بودن و نبود اطلاعات کافی)، پیچیدگی (تعاملات محیطی و وجود عوامل چندگانه) و ابهام محیطی (ناتوانی درک وقایع و ارزیابی درست محیط خارجی) است (هاگمن، ۲۰۱۶). مگبری[4] (۲۰۱۷) آمادگی شناختی را به‌عنوان شایستگی جدیدی در حوزه رهبری برای پذیرش و سازگاری با تغییرات غیرقابل‌پیش‌بینی و رویارویی با چالش‌های محیطی مطرح می‌کند.

محیط‌های سایبری نیز به‌سرعت و گاهی اوقات به‌شدت تغییر می‌کنند. دشمنان به‌طور مداوم تاکتیک‌های خود را تغییر می‌دهند و تکنیک‌های خود را کامل و یک چشم‌انداز تهدید سایبری پویا ایجاد می‌کنند. در دفاع سایبری علی‌رغم اقدامات امنیتی لایه‌ای و سرمایه‌گذاری زیرساختی قابل‌توجه، تیم‌های امنیتی همچنان نگران چیزهایی هستند که نمی‌دانند. علاوه بر این، تاکتیک‌ها، تکنیک‌ها و فرایندهای مهاجمان سایبری از نظر

1. Raymond
2. Diamond
3. Ben-Asher and Gonzalez
4. Mgbere

طراحی پیچیده هستند و توانایی تیم‌های دفاعی را برای شناسایی، بررسی و اصلاح هر مشکلی کاهش می‌دهند (طالبی و همکاران، ۱۴۰۳). عدم قطعیت زمانی است که اطلاعات مربوطه در دسترس نباشد و ناشناخته باشد و ابهام در جایی است که اطلاعات مرتبط در دسترس است اما معنای کلی آن هنوز ناشناخته است (بودنهازن و پری، ۲۰۰۹). ابهام در محیط امنیتی - دفاعی سایبری بسیار زیاد است. داشتن بینش فوری، روشن و تجویزی نسبت به رویدادهای امنیتی دشوار است. مقادیر بسیار زیاد داده‌های رویداد و هشدار تجزیه گزارش‌ها را به‌سرعت یا به‌اندازه کافی غیرممکن می‌کند. تیم‌های سایبری اغلب باید تلاش کنند تا رویدادها را از سراسر زیرساخت به‌صورت دستی مرتبط کنند تا زمینه را برای پاسخ خود ترکیب کنند. وقتی تیم‌ها به‌طور مداوم در سطح بالایی از هوشیاری کار می‌کنند، پتانسیل بیشتری برای خستگی، اشتباه خواندن و خطا وجود دارد. ازآنجایی‌که حمله‌ها و تهدیدهای سایبری هر روز پیچیده‌تر و هوشمندتر می‌شوند، ایجاد سطح آگاهی و آمادگی شناختی برای مواجهه در برابر آن‌ها بسیار مهم است.

یکی دیگر از عوامل مؤثر در آمادگی شناختی منابع و توانمندسازها برای حفظ و ارتقای آن در سطح ملی و سازمانی است که بدون آن‌ها آمادگی دفاعی سایبری معنا و مفهوم پیدا نمی‌کند. بر اساس تعریفی که اولین بار توسط مرکز آموزش و دکترین ارتش ایالات‌متحده امریکا صورت گرفت، مؤلفه‌های توانمندساز شامل هفت عنصر کلیدی دکترین، سازمان‌دهی، آموزش، تجهیزات، نیروی انسانی، رهبری و منابع و امکانات هستند که به مدل مرجع «سامانه توسعهٔ یکپارچه توانمندی‌ها» یا به‌اختصار به (DOTMPLF[1]) مشهور هستند. این مدل با انجام تغییراتی در سایر سازمان‌های نظامی و غیرنظامی مورداستفاده قرار می‌گیرد. البته این مؤلفه‌ها در حوزهٔ عملیات دفاع سایبری به‌واسطه شرایط و پیچیدگی‌های حاکم بر این فضا که در بخش‌های قبلی به آن اشاره شد، نیازمند بازنگری و توسعه است. چراکه به‌واسطه ویژگی‌ها این فضا و چالش‌های اجرای عملیات سایبری از قبیل آسیب‌پذیری، هماهنگی و مسائل قانونی، ضرورت دارد که برخی از این منابع توانمندساز به این مؤلفه‌ها افزوده شود.

پیشینه‌های پژوهش

1. Doctrine, Organization, Training, Materiel, Personal, Logistic, Facility

آمادگی شناختی کمتر از سی سال است که در علوم نظامی مطرح شده است. این اصطلاح پیش‌ازاین در روان‌شناسی تحولی و آموزشی بیان شده بود، ولی اهداف استفاده از آن در علوم نظامی متفاوت است چراکه در روان‌شناسی تحولی و آموزشی عموماً بلوغ شناختی فرد برای فعالیت‌های متناسب با سن مدنظر است، ولی در علوم نظامی آمادگی شناختی به آمادگی ذهنی افراد در شرایط استرس‌زا و همچنین استفادهٔ بهینه از ابزارها و فناوری‌های موجود به بهترین شکل کمک می‌کند (ناجی، ۱۳۹۶). اهمیت آمادگی شناختی ازاین‌جهت است که موفقیت در عملیات نظامی علاوه بر آمادگی جسمانی، به آمادگی شناختی هر فرد نیز بستگی دارد. پژوهش‌ها نشان می‌دهند که ۸۰ درصد از خطای نظامی ناشی از خطای انسانی است و یا استرس طولانی‌مدت به افراد منجر به آسیب زدن به آن‌ها می‌شود. همچنین ۱۰ تا ۵۰ درصد تلفات عملیات به علت مسائل روان‌شناختی است که می‌توان با آمادگی شناختی با آن مقابله کرد (ناجی، ۱۳۹۶). طالبی و همکاران(۱۴۰۳) در پژوهشی به کارکردهای شناختی سطح بالا و کارکردهای اصلی اجرایی در دفاع سایبری پرداخته‌اند. در ادبیات آمادگی شناختی، تعاریف و کاربردهای مختلفی به شرح ذیل اشاره شده است:

- آمادگی شناختی عبارت است از آمادگی ذهنی (از جمله مهارت‌ها، دانش، توانایی‌ها، انگیزه‌ها و تمایلات شخصی) که یک فرد به‌منظور ایجاد و حفظ عملکرد مناسب در محیط پیچیده و غیرقابل‌پیش‌بینی به آن نیاز دارد (موریسون و فلچر، ۲۰۰۲).
- دایر[1] و دیگران (۲۰۰۷) آمادگی شناختی را توانایی به انجام رساندن مأموریت‌ها با تصمیم‌گیری و اجرای تصمیم به شیوهٔ مؤثر، کارآمد و به‌روز در محیط در حال تغییر و پیچیده تعریف می‌کنند.
- برانسکوم و گرینوسکی[2] (۲۰۰۷) آمادگی شناختی را حالت بهبودیافته‌ای از چالاکی ذهنی[3] افراد در برخورد با تقاضای شناختی در موقعیت‌ها تعریف می‌کنند.
- گریر[4] (۲۰۱۲) آمادگی شناختی را از سه منظر تعریف کرده است: ۱) آمادگی شناختی

1. Dyer
2. Branscome & Grynovicki
3. Mental acuity
4. Grier

تاکتیکی: حالتی از چالاکی شـناختی ذهنی برای اطمینان از سطح قابل‌قبول عملکـرد در انجـام مأموریـت‌هـای واگذارشـده. ۲) آمـادگی شناختی عملیاتی: آمادگی ذهنی (از جمله دانش، مهارت‌ها، توانایی‌ها، انگیزه و تمایلات فردی) که افراد به‌منظور عملکرد مناسب در محیط پیچیده و غیرقابل‌پیش‌بینی به آن‌ها نیاز دارند. ۳) آمـادگی شـناختی راهبردی: بـه معنـای قابلیت افراد در انجام وظایف شناختی محول شده در محیط پیچیده و غیرقابل‌پیش‌بینی است.

- آرچی بالد، و همکاران[1] (۲۰۱۳) معتقدند آمادگی شناختی از دو شایسـتگی دانـش و تخصـص و توانایی شناختی کلیدی تشکیل شده است که به افراد در روبرو شدن با تغییرات غیرقابل‌پیش‌بینی کمک می‌کنند.
- فلچر و ویند[2] (۲۰۱۴) آمادگی شناختی را توانایی افراد در ۱) حذف ابهام و تشخیص الگوهـا در موقعیـت‌هـای نامطمئن، مبهم و پر هرج‌ومرج، ۲) شناسایی و اولویت‌بندی مسائل و فرصت‌های ارائه‌شده، ۳) ارائهٔ پاسخ مؤثر بـه مشکلات و یا فرصت‌ها و ۴) پیاده‌سازی این پاسخ تعریف می‌کنند.
- پرز و بیکر[3] (۲۰۱۴) آمادگی شناختی را ترکیبی از تفاوت‌های فردی و دانش و تجربیات آموخته‌شده و همچنین تعامل بین تخصص افراد و موقعیت‌های پیش رو تعریف می‌کنند. استرنبرگ[4] (۲۰۱۴) آمادگی شناختی را بر اساس توانایی چهارگانه خلاق، تحلیلی، عملی و خردمحور تعریف می‌کند.

با توجه به تعاریف آمادگی شناختی، می‌توانیم مفهوم عمومی آمادگی شناختی را به مؤلفه‌های خاص‌تری کاهش دهیم. برخی محققین، از منظر یک دیدگاه جامع به آمادگی شناختی نگاه می‌کنند. برای مثال، آن‌ها مفهوم‌سازی فلتچر (۲۰۰۴) از آمادگی شناختی را اصلاح‌کرده و آمادگی شناختی را شامل این مؤلفه‌ها می‌دانند: انطباق‌پذیری، ارتباط، خلاقیت، تفکر انتقادی، تصمیم‌گیری، فراشناخت، طرح‌واره بازشناسی، حل مسئله،

1. Archibald, et al
2. Fletcher, J. D. & Wind
3. Baker
4. Sternberg

تاب‌آوری، آگاهی وضعیتی و مهارت‌های کار تیمی و [روابط] بین فردی (بولستاد و دیگران، ۲۰۱۴). بولستاد، اندزلی و کیواس[1](۲۰۱۴) نگاه جامعی به ۲۱ ویژگی‌ای دارند که آمادگی شناختی را تعریف می‌کنند؛ برای مثال، ویژگی‌هایی از قبیل شیوهٔ رفتاری، منابع شناختی، انسجام، اشتراک در اهداف، مدیریت تعارض، تصمیم‌گیری، هیجان، خستگی و انعطاف‌پذیری. مدل اُنیل[2]، آمادگی شناختی را در قالب سه بُعد اصلی مفهوم‌سازی می‌کند:

۱) دانش، ۲) مهارت‌ها و ۳) ویژگی‌ها[3] (KSA). در این چهارچوب، دانش حوزه‌ای خاص است، مهارت‌ها حوزهٔ خاص یا مستقل هستند و صفات، نسبتاً حوزه‌ای مستقل هستند. صفات، ویژگی‌هایی هستند که کاربردی هستند اما آموزش آن‌ها سخت است (جکسون[4] و دیگران، ۲۰۱۲). اصطلاح صفت، معمولاً به‌عنوان جایگزین اصطلاح شایستگی مورداستفاده قرار می‌گیرد.

کاربران سایبری نیز باید با در نظر گرفتن عوامل اجتماعی و عوامل فناورانه از سیستم اجتماعی - فنی آگاهی داشته باشند و آن را درک کنند (کوگلان و میلر[5]، ۲۰۱۴). بخشی از این وظایف در کنار بار اطلاعات زیاد، منجر به این می‌شود که کار دفاع سایبری به‌عنوان ایمنی - حیاتی توصیف شود (ناکس[6] و دیگران، ۲۰۱۸). کارکنان دفاع سایبری برای حرکت و مانور در ابعاد سایبری - فیزیکی و تاکتیکی - راهبردی به‌منظور درک محیط کار به توانایی‌های شناختی (دامیکو[7] و دیگران، ۲۰۱۶) و چابکی شناختی نیاز دارند (جوسوک[8] و دیگران، ۲۰۱۶). دفاع سایبری نیز به دلیل قرار گرفتن در معرض حمله‌ها و تهدیدها با تنوع، سرعت و حجم بالای مستمر، پیچیده‌تر از محیط دفاعی و نظامی است و نیروی انسانی این حوزه نیز باید از دانش و مهارت‌های لازم برای مواجهه و مقابله با تهدیدها و حمله‌های نوظهور و غیرقابل‌پیش‌بینی برخوردار باشند و همچنین عکس‌العمل مناسبی در قبال تغییر و تحولات محیطی نشان دهند. به‌ویژه این‌که فضای

1. Bolstad, Endsley, and Cuevas
2. O'Neil
3. Knowledge, Skill and Ability or Attitude
4. Jackson
5. Coghlan and Miller
6. Knox
7. D'Amico
8. Jøsok

سایبری و دفاع از آن تحت تأثیر چهار عامل بی‌ثباتی، عدم قطعیت، پیچیدگی و ابهام محیطی قرار دارد. درحالی‌که شایستگی فنی سایبری برای فعالیت در حوزه سایبری بسیار مهم است، مهارت‌های نرم و شایستگی‌های شناختی توجه بیشتری را به خود جلب کرده است (باچلر[1] و دیگران، ۲۰۱۸). در واقع توجه به آمادگی شناختی دفاع سایبری این اطمینان را خواهد داد که نیروی انسانی آن از نظر ذهنی برای انجام مأموریت‌ها و فعالیت‌ها آماده است و به آن‌ها برای رویارویی با چالش‌های محیطی و همچنین موقعیت‌های غیرقابل‌پیش‌بینی کمک می‌کند. بااین‌حال، وظایف کاربران سایبری، الزامات شایستگی و عملکرد، مفاهیم بی‌نظمی هستند که فاقد تعریف و دستورالعمل‌های مشخص برای پشتیبانی از جذب، گزینش، آموزش و تربیت کارکنان این حوزه جدید است.

چارچوب فضای جنگ‌های هیبریدی (ترکیبی) نیز این نظریه را مطرح می‌کند که مهارت‌های فنی به‌تنهایی برای انجام عملیات کافی نیست (باچلر و دیگران، ۲۰۱۶). چارچوب فضای هیبریدی تصدیق می‌کند که محیط کار کاربران سایبری علاوه بر اینکه تحت تأثیر عواملی مانند: کار گروهی، رهبری، سلسله‌مراتب، ارتباطات و غیره است، تحت تأثیر ویژگی‌های نامشهود زمینه و اطلاعات دیجیتالی نیز قرار می‌گیرد. درنتیجه تغییر نیازها از آمادگی جسمانی به سمت کارایی و یا عملکرد شناختی[2] (ناکس و دیگران، ۲۰۱۸) به کاربر سایبری اجازه می‌دهد در حین انجام وظایف سایبری در سطح تاکتیکی به تفکر استراتژیک بپردازد (جوسوک و همکاران،۲۰۱۶). گود و یگانه[3] (۲۰۱۲) چابکی شناختی کاربران سایبری را به‌عنوان ساختاری متشکل از سه جزء انعطاف‌پذیری شناختی، گشودگی (پذیرا بودن) شناختی و توجه متمرکز توصیف می‌کند. مطابق با این تعریف، قابلیت کاربران سایبری برای تحرک شناختی با استفاده از توجه انعطاف‌پذیر و استراتژی‌های خودتنظیمی قبلاً به‌عنوان چابکی شناختی توصیف شده است (ناکس و دیگران، ۲۰۱۸). لاتروپ[4] و همکاران (۲۰۱۶) پیشنهاد می‌کنند که کاربران سایبری برای انجام وظایف بر شایستگی‌هایی مانند معنابخشی به تجربیات[5]، تفکر خلاق، تجسم ذهنی و سایر عملکردهای شناختی سطح بالا متکی هستند. ناکس و همکاران (۲۰۱۸) از

1. Buchler
2. Cognitive performance
3. Good & yegane
4. Lathrop
5. Sense making

چارچوب فضای (ترکیبی) هیبریدی برای توصیف اینکه افراد برای مانور در فضای ترکیبی باید از توانایی‌های شناختی متفاوتی استفاده کنند، بهره گرفته‌اند. به‌عنوان‌مثال می‌توان به دیدگاه اجتماعی - شناختی، شناخت محیطی، تاب‌آوری شناختی، شناخت کلان، فراشناخت و خودتنظیمی اشاره کرد (ناکس و دیگران، ۲۰۱۸). با استفاده از چارچوب فضای ترکیبی، ناکس و همکاران (۲۰۱۷) چابکی شناختی را به‌عنوان یکی از شایستگی‌های مهم شناختی پیشنهاد کرد که می‌تواند عملکرد کاربران سایبری را پشتیبانی کند. آن‌ها چابکی شناختی را به‌عنوان «حرکات متمرکز شناختی» در فضای ترکیبی با فراشناخت و عملکرد کاربران سایبری مرتبط کردند (ناکس و دیگران، ۲۰۱۷). مرور مبانی نظری و پیشینهٔ مربوط به موضوع آمادگی شناختی و دفاع سایبری نشان می‌دهد علی‌رغم این‌که بر توسعهٔ آمادگی شناختی و نقش آن در بهبود عملکرد تأکید شده است، اما همچنان یک الگوی جامع ارائه نشده است که در برگیرندهٔ جنبه‌های آمادگی شناختی متناسب با عرصهٔ دفاع سایبری باشد. بااین‌حال می‌توان با بهره‌گیری از این منابع و تعمیم آن به فضای سایبری ابعاد آمادگی شناختی در دفاع را به‌عنوان ترکیبی از توانمندی‌های اساسی، رفع ابهام در موقعیت‌های پر ابهام و پیچیده، تشخیص الگوهای تهدیدهای سایبری، اولویت‌بندی و تصمیم مؤثر و پیاده‌سازی تصمیم درک کرد.

روش‌شناسی پژوهش

با عنایت به موضوع تحقیق که درصدد طراحی و اعتبارسنجی نظام آمادگی شناختی دفاع سایبری و ایجاد وفاق در فرایند تصمیم‌سازی و تصمیم‌گیری برای فرماندهان است و بر اساس هدف در زمرهٔ تحقیقات کاربردی قرار می‌گیرد. در این پژوهش آمادگی‌های شناختی دفاع سایبری، توصیف و تحلیل و با دیدی اکتشافی، ارائه شده است و از لحاظ رویکرد پژوهش، روش ترکیبی یا آمیخته از نوع اکتشافی متوالی مورد استفاده گرفته است. در بخش کیفی پژوهش با استفاده از روش کیفی فراترکیب و تحلیل محتوا با کدگذاری باز، محوری و انتخابی عوامل مؤثر بر آمادگی شناختی دفاع سایبری و همچنین مؤلفه‌های تشکیل‌دهندهٔ آن با رویکرد زیست‌بومی به محیط دفاع سایبری شناسایی شد. در مرحله بعد بر اساس نظرات خبرگان، الگوی اولیه تکمیل و اصلاح شد. اعتباریابی الگوی طراحی‌شده با استفاده از پرسشنامه محقق ساخته در طیف لیکرت و با برگزاری

جلسات گروه کانونی با حضور متخصصان و خبرگان اخذ گردید.
در مرحله دوم پژوهش از روش تحقیق کمّی از شیوه توصیفی- تحلیلی استفاده شد. پرسشنامه با ۶۳ سؤال در اختیار جامعه آماری بخش کمّی پژوهش قرار گرفت. جامعه آماری برای مشارکت در فرایند مصاحبه، شامل خبرگان حوزهٔ دفاع سایبری و علوم شناختی هستند که دارای ویژگی‌هایی چون سابقه خدمتی بالای ۱۵ سال، مدرک تحصیلی مرتبط دکتری، مسئولیت در سطوح عالی فرماندهی و مدیریتی مرتبط با سایبر در نیروهای مسلح جمهوری اسلامی ایران باشند. نمونه‌گیری برای انتخاب خبرگان با رویکرد هدفمند قضاوتی تا سرحد اشباع نظری داده‌ها انجام و تعداد ۸ نفر از خبرگان مبتنی بر معیارهای یادشده شناسایی و در فرایند مصاحبه مشارکت داده شدند. در بخش فراترکیب مقالات و منابع پژوهشی مرتبط با آمادگی‌های شناختی و دفاع سایبری هستند که از ۱۴۰ مقالهٔ اولیهٔ مرتبط با عملیات سایبری، زیست‌بوم دفاع سایبری، علوم شناختی و آمادگی‌های شناختی با استفاده از چک‌لیست ارزیابی حیاتی[1] (CASP) تعداد ۹۰ مقاله برای ورود به مرحلهٔ بعدی یعنی، مرور تمام متن و تجزیه‌وتحلیل انتخاب شدند. همچنین جامعهٔ آماری برای توزیع پرسشنامه در مرحلهٔ کمّی پژوهش، از کارشناسان آشنا با فضای سایبر و علوم و فناوری‌های سایبر - شناختی در نیروهای مسلح ج.ا.ا استفاده شد که دارای مشخصات مدرک تحصیلی مرتبط حداقل کارشناسی، دارای فهم راهبردی و علمی از عرصه‌های دفاع سایبری و علوم شناختی، حداقل ۱۵ سال سابقهٔ کار در حوزهٔ دفاع سایبری و خدمت در رده‌های فرماندهی/ مدیریتی باشند.
به‌منظور برآورد حجم نمونهٔ تحقیق با استفاده از فرمول کوکران برای جامعهٔ نامعیّن، حداقل حجم نمونه موردنیاز تحقیق ۱۵۵ ≃ ۱۵۵/۳۹ محاسبه شد. برای تجزیه‌وتحلیل داده‌های کمّی از آمار توصیفی و برای ارزیابی برازش مدل مفهومی نظام آمادگی شناختی دفاع سایبری از روش تحلیل عاملی (مرتبه اول و دوم) و نرم‌افزار اسمارت پی.ال.اس. استفاده شد.
روایی سؤالات مصاحبه به روش محتوایی و مبتنی بر نظر خبرگان تأیید شده است. همچنین برای اطمینان از روایی نتایج مصاحبه و تحلیل محتوا از معیار مقبولیت و قابلیت تأیید استفاده شد. جهت افزایش مقبولیت از روش‌های بازنگری توسط شرکت‌کنندگان

1. Critical Appraisal Skills program (CASP)

در مصاحبه بهره‌برداری شد. همچنین برای قابلیت تأیید در مرحلهٔ پایانی، طبقات به‌دست‌آمده به سه نفر از مشارکت‌کنندگان اولیه به‌منظور بازبینی و تأیید برگردانده شد و نکات پیشنهادی اعمال شد. برای افزایش سطح پایایی سؤالات مصاحبه نیز تلاش گردید که سؤالات بدون هیچ‌گونه ابهامی طراحی شوند و از تعداد سه نفر از مصاحبه‌شوندگان در دو بازه زمانی مختلف سؤالات پرسیده شد و روشن گردید که مصاحبه‌شوندگان درک یکسانی از سؤالات در زمان‌های مختلف دارند. درعین‌حال، پایایی روند کدگذاری عبارت‌های بیانی مصاحبه نیز به روش کدگذاری مجدد انجام شد.

به‌منظور بررسی روایی محتوایی به شکل کمّی از ضریب نسبی روایی محتوا[1] (CVR) استفاده شد. بر اساس تعداد متخصصانی که سؤالات را مورد ارزیابی قرار دادند، مقدار CVR بزرگ‌تر از ۰/۷ بود که نشان‌دهنده روایی سؤالات پرسش‌نامه بود. همچنین برای بررسی اعتبار و پایایی پرسش‌نامه تهیه‌شده، پرسش‌نامه‌ها بین جامعه آماری توزیع شد و اطلاعات به‌دست‌آمده از طریق آزمون آماری (پایایی ترکیبی) مورد تجزیه‌وتحلیل قرار گرفت. مطابق نتایج به‌دست‌آمده مقدار پایایی ترکیبی همه مؤلفه‌ها و سازه‌های پرسش‌نامه بیش از ۰/۷ هست که نشان‌دهندهٔ پایایی مناسب پرسش‌های طرح‌شده برای ارزیابی ابعاد، مؤلفه‌ها و زیر مؤلفه‌ها است.

برای تجزیه‌وتحلیل داده‌های بخش کیفی پژوهش از کدگذاری باز و محوری استفاده شد. در نهایت برای به دست آوردن تصویری بهتر از کدها، جدول دوبُعدی طراحی شد که در یک بُعد آن نویسنده / نویسندگان مقالات به همراه سال و در یک بُعد کدهای استخراج‌شده، نوشته شده است. در واقع با این کار فراوانی کدها در مقالات منتخب مشخص شد. منابع انتخاب‌شده شامل مقالات مروری، مقالات علمی - پژوهشی، پایان‌نامه و کتاب است. (جدول ۱).

جدول ۱. نمونه اطلاعات منابع کلیدی منتخب

کد مقاله	پژوهشگر/ پژوهشگران (سال)	کد مقاله	پژوهشگر/ پژوهشگران (سال)	کد مقاله	پژوهشگر/ پژوهشگران (سال)	کد مقاله	پژوهشگر/ پژوهشگران (سال)
۱	Andrade 2019	۲	Archibald 2014	۳	Absar 2010	۴	Andrade 2018

1. Content Validity Ratio

در گام بعدی برای کدگذاری محوری، پژوهشگر ابتدا تمام عوامل استخراج‌شده از مطالعات را کد در نظر گرفت و سپس با در نظر گرفتن مفهوم هر یک از کدها آن‌ها را در یک مفهوم مشابه دسته‌بندی کرد (فراست‌خواه، ۱۳۹۶: ۱۷۰). در این مرحله سعی شد مفاهیم با یکدیگر مقایسه شوند تا شباهت‌ها و تفاوت‌هایشان مشخص شود و زمینه برای شکل‌گیری مقوله‌ها فراهم شود. سپس کدهای به‌دست‌آمده پس از دسته‌بندی و همگن‌سازی به جامعهٔ خبرگان پژوهش ارائه شد. سرانجام و پس از اعمال اصلاحات لازم، در مرحله بعد به روش کمّی و از طریق پیمایش با استفاده از ابزار پرسش‌نامه محقق ساخته، الگوی آمادگی شناختی دفاع سایبری و همچنین بررسی روابط بین آن‌ها به کمک روش‌های مدل‌سازی معادلات ساختاری و از طریق نرم‌افزار اسمارت. پی. ال. اس انجام شد.

تجزیه‌وتحلیل داده‌ها

هدف اصلی پژوهش حاضر ارائهٔ ابعاد، مؤلفه‌ها و شاخص‌های آمادگی شناختی دفاع سایبری در زیست‌بوم شناختی دفاع سایبری است. برای این منظور با استفاده از مرور نظام‌مند پیشینهٔ پژوهش و کاربست روش فراترکیب، محتوای دستاوردهای کیفی منابع علمی منتخب به روش تحلیل استقرائی خط به خط واکاوی و اطلاعات و داده‌های موردنیاز گردآوری شد. در نهایت با بازبینی و پالایش مکرر مفاهیم استخراج‌شده به مجموعهٔ منسجمی از مفاهیم، شامل ۷۳ کد تقلیل یافته و ارائه شد. در مرحلهٔ بعد کد شناسایی شد و پس از ترکیب کدهای مشابه زیر مؤلفه‌ها و مؤلفه‌ها شناسایی و در کنار هم قرار داده شدند تا مفاهیم پیدا شد و از تلفیق مفاهیم مشابه مقوله‌ها به وجود آمدند. در مرحله بعد با استفاده از مصاحبه با خبرگان و صاحب‌نظرانی که با موضوع موردمطالعه ارتباط نزدیکی داشتند، خواسته شد نظرات خود را در خصوص احصاء ابعاد، مؤلفه‌ها، عوامل توانمندساز و تأثیرگذار بر نظام آمادگی شناختی دفاع سایبری مطرح کنند بدون این‌که الگوی اولیه به آن‌ها عرضه شود. به‌منظور احصاء اجزاء اصلی و روابط فی‌مابین نظام و همچنین اعتبارسنجی مدل مفهومی، نظرات خبرگان الگوی اولیه تکمیل و اصلاح شد. نهایتاً با دعوت مجدد از خبرگان و تشکیل گروه‌های کانونی در طی دو مرحله

صاحب‌نظران و خبرگان ضمن تأیید کلیت کار نقطه نظرات اصلاحی را مطرح نمودند و اعتبار یابی نهایی الگوی مفهومی انجام گردید.

در این مرحله سعی شد نظر متخصصان و خبرگان تا جایی اعمال شود که داده‌های گردآوری‌شده و پیشینه موضوع و نظرات سایر صاحب‌نظران اجازه می‌داد. در نتیجه کدگذاری و حذف کدهای تکراری و تلخیص نهایی داده‌ها تعداد ۶۳ کد شناسایی گردید و سپس از ترکیب کدهای مشابه زیر مؤلفه‌ها و مؤلفه‌ها شناسایی و در کنار هم قرار داده شدند تا مفاهیم پیدا شد و از تلفیق مفاهیم مشابه مقوله‌ها به وجود آمدند. در پایان ۴ مفهوم (بُعد) شامل فناوری‌های سایبر شناختی، فرایندهای سایبر شناختی، مؤلفه‌های آمادگی شناختی و عوامل مؤثر بر آمادگی شناختی دفاع سایبری و ۹ مؤلفه اصلی شامل فناوری هوش مصنوعی، فناوری داده‌کاوی، فناوری غوطه‌وری، آگاهی وضعیتی سایبر شناختی، خودآگاهی سایبری، کارکردهای اجرایی اصلی شناختی، کارکردهای شناختی سطح بالا، ادراک عوامل محیطی و منابع توانمندساز با زیر مؤلفه‌های مربوطه شناسایی و استخراج گردید.

جدول ۲. نمونه‌ای از کدگذاری باز و محوری نهایی و استخراج مقوله، مفاهیم، مؤلفه‌ها

مقوله	مفهوم	مؤلفه	زیر مؤلفه	کد	منابع
زیست‌بوم شناختی دفاع سایبری و عوامل مؤثر	فناوری‌های سایبر شناختی	هوش مصنوعی	پردازش زبان طبیعی	درک تیمی انسان و ماشین	۱،۶۱، ۱۴، ۶۱، ۲۲، ۲۳،
			یادگیری ماشین	یادگیری توزیع‌شده پیشرفته	
		داده‌کاوی	ادغام اطلاعات و تجزیه‌وتحلیل	یکپارچگی داده‌ها در حجم، تنوع و سرعت‌بالا	۴ ،۱ ،۲۳،۱۷ ۶،۶۹ ،۶ ،۱۴ ،۲۷
			تفسیر اطلاعات و استخراج دانش دقیق	شناسایی بلادرنگ نقاط قوت و ضعف	
		غوطه‌وری	واقعیت مجازی R	محیط‌های آموزش مجازی برای ارتقاء شناختی کارکنان	۱۷ ۶ ،۹۰،۱،

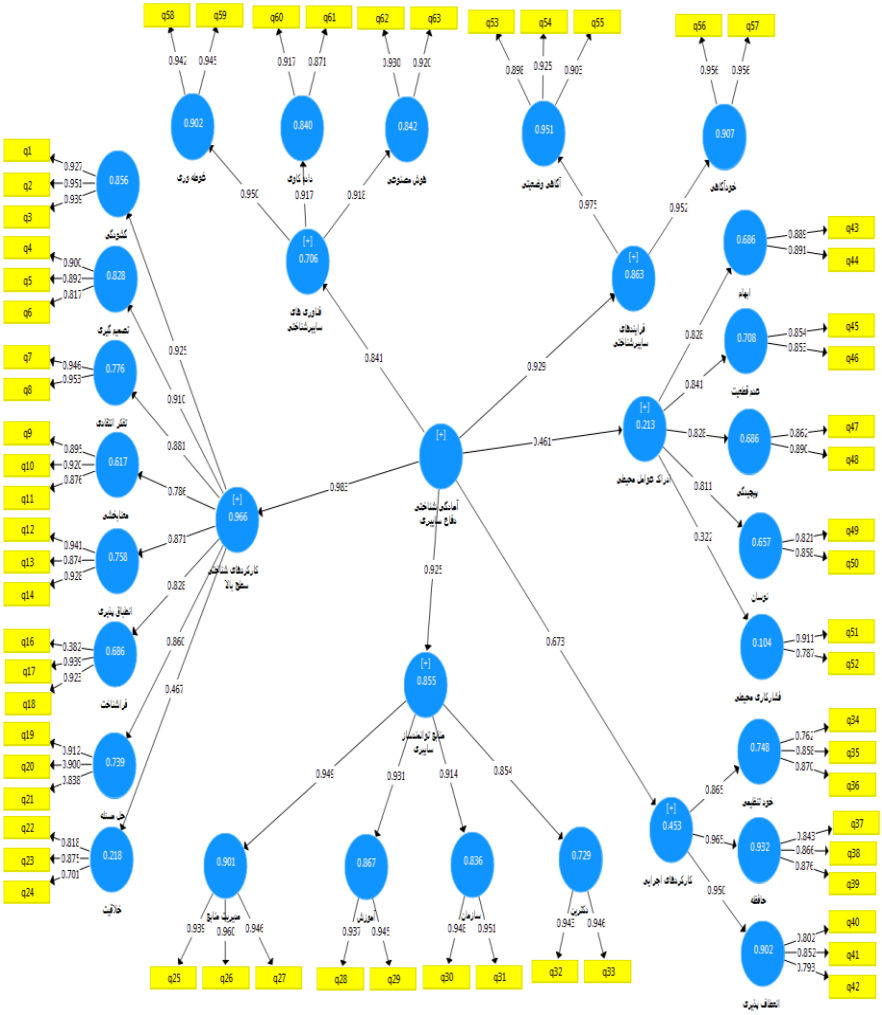
مقوله	مفهوم	مؤلفه	زیر مؤلفه	کد	منابع
			واقعیت افزوده	تجربه شناختی مبتنی بر شرایط محیطی	
			قابلیت پیش‌بینی	پیش‌بینی تأثیر تغییرات پویا	

در بخش تحلیل کمّی با توجه به این‌که الگوی آمادگی شناختی دفاع سایبری یک مدل سلسله مراتبی است، برای سنجش دقیق‌تر سازهٔ اصلی آمادگی شناختی دفاع سایبری، دو سطح از سازه‌ها طراحی‌شده است. برای برازش مدل در مدل‌سازی معادلات ساختاری از برازش مدل‌های اندازه‌گیری، برازش مدل ساختاری و برازش مدل کلی استفاده شده است.

برای برازش مدل اندازه‌گیری از معیارهای پایایی شاخص (پایایی ترکیبی و ضرایب بارهای عاملی)، روایی همگرا (جذر واریانس اشتراکی) و واگرایی مدل (معیار فورنل و لارکر) استفاده شده است.

- برازش مدل‌های اندازه‌گیری
- پایایی شاخص

الف) ضرایب بارهای عاملی



شکل ۲. مدل سازه‌ها، مؤلفه‌ها و شاخص‌های زیست‌بوم آمادگی شناختی دفاع سایبری

ازآنجاکه مدل پژوهش از نوع مدل سلسله مراتبی است باید علاوه بر بار عاملی سؤال‌ها، میزان بار عاملی سازه و مؤلفه‌ها هم محاسبه شود. اگرچه در خروجی نرم‌افزار، روابط بین سازه و مؤلفه را با عنوان ضرایب مسیر گزارش می‌کند، اما معادل با بار عاملی است. میزان بار عاملی مؤلفه، سازه‌ها و شاخص‌ها بیشتر از مقدار قابل‌قبول ۰/۴ است. محاسبه ضرایب معناداری بارهای عاملی نشان می‌دهد که تمامی بارهای عاملی در سطح اطمینان ۹۵٪ معنادار است.

جدول ۳. نمونه‌ای از ضرایب بارهای عاملی سازه‌ها و مؤلفه‌ها (فناوری‌های سایبر شناختی)

مؤلفه > سازه			سازه > سؤال	
مؤلفه	سازه	بار عاملی	سؤال پرسشنامه	بار عاملی
فناوری‌های سایبر شناختی ۰/۸۴۱ (۳۲/۲۱)	غوطه‌وری	۰/۹۵۰	Q58	۰/۹۴۲
			Q59	۰/۹۴۵
	داده‌کاوی	۰/۹۱۷	Q60	۰/۹۱۷
			Q61	۰/۸۷۱
	هوش مصنوعی	۰/۹۱۸	Q62	۰/۹۳۰
			Q63	۰/۹۲۰

ب) پایایی ترکیبی

پایایی ترکیبی مؤلفه و سازه‌ها بیشتر از مقدار ۰/۷ است. پایایی ترکیبی مدل در سازه کارکردهای شناختی سطح بالا در جدول ۴ نشان داده شده است.

جدول ۴. نمونه‌ای از پایایی ترکیبی سازه و مؤلفه‌ها (کارکردهای شناختی سطح بالا)

مؤلفه	CR (>0/7?)	سازه	CR (>0/7?)
کارکردهای شناختی سطح بالا	۰/۹۶۰	گشودگی	۰/۹۵۷
		تصمیم‌گیری	۰/۹۰۴
		تفکر انتقادی	۰/۹۴۹
		معنابخشی	۰/۹۲۵
		انطباق‌پذیری	۰/۹۳۹
		فراشناخت	۰/۹۱۹
		حل مسئله	۰/۹۱۵
		خلاقیت	۰/۹۴۲

- روایی شاخص

الف. روایی همگرای مدل

برای سنجش روایی همگرا از معیار جذر واریانس اشتراکی (AVE) استفاده می‌شود. مقدار AVE بالاتر از ۰/۵ نشان‌دهندهٔ روایی همگرای مدل کارکردهای شناختی سطح بالا و کارکردهای اجرایی است. شاخص AVE برای تمام سازه‌ها بیشتر از مقدار ۰/۵ است.

ب. روایی واگرای مدل اندازه‌گیری

معیار فورنل و لارکر: جذر واریانس اشتراکی تمامی سازه‌های مدل کارکردهای شناختی سطح بالا و کارکردهای اجرایی (مقادیر قطر ماتریس) بیشتر از همبستگی هر سازه با سایر سازه‌ها است (مقادیر سلول‌های ماتریس) که تائیدکنندهٔ روایی همگرای مدل با معیار فورنل و لارکر است. جذر واریانس اشتراکی تمامی سازه‌ها (مقادیر قطر ماتریس) بیشتر از همبستگی هر سازه با سایر سازه‌ها است (مقادیر سلول‌های ماتریس) که تائید کنندهٔ روایی همگرای مدل با معیار فورنل و لارکر است.

- ارزیابی برازش مدل ساختاری

به‌منظور ارزیابی بخش ساختاری مدل شاخص تغییرپذیری (Red)، شاخص Q^2 گزارش شده است.

الف) تغییرپذیری سازه‌های درون‌زا: تمامی سازه‌ها دارای مقادیر Red بیشتر از حداقل مقدار معیار تغییرپذیری ۰/۰۹۵ هستند. معیار تغییرپذیری برای کل مدل بیشتر از مقدار بحرانی ۰/۰۹۵ است که نشان‌دهندهٔ برازش مناسب مدل بر اساس این معیار است.

جدول ۵. تغییرپذیری سازه‌های درون‌زای آمادگی شناختی دفاع سایبری

	communality	R^2	Redundancy
فناوری‌های سایبر شناختی	۰/۸۴۸	۰/۷۰۶	۰/۵۹۸
هوش مصنوعی	۰/۸۵۶	۰/۸۴۲	۰/۷۲۰
داده‌کاوی	۰/۸۰۰	۰/۸۴۰	۰/۶۷۲
غوطه‌وری	۰/۸۹۰	۰/۹۰۲	۰/۸۰۲
کارکردهای شناختی سطح بالا	۰/۷۷۹	۰/۹۶۶	۰/۷۷۵
گشودگی	۰/۸۸۲	۰/۸۵۶	۰/۷۵۴
تصمیم‌گیری	۰/۷۵۸	۰/۸۲۸	۰/۶۲۸
تفکر انتقادی	۰/۹۰۱	۰/۷۷۶	۰/۶۹۹
معنابخشی	۰/۸۰۵	۰/۶۱۷	۰/۴۹۶
انطباق‌پذیری	۰/۸۳۷	۰/۷۵۸	۰/۶۳۴
فراشناخت	۰/۶۲۷	۰/۶۸۶	۰/۴۳۰
حل مسئله	۰/۷۸۱	۰/۷۳۹	۰/۵۷۷

	communality	R^2	Redundancy
خلاقیت	۰/۶۴۲	۰/۲۱۸	۰/۱۳۹
فرایندهای سایبر شناختی	۰/۹۶۳	۰/۸۶۳	۰/۸۳۱
آگاهی وضعیتی	۰/۹۷۵	۰/۹۵۱	۰/۹۲۷
خودآگاهی	۰/۹۵۲	۰/۹۰۷	۰/۸۶۳
ادراک عوامل محیطی	۰/۷۴۴	۰/۲۱۳	۰/۱۵۸
ابهام	۰/۷۹۲	۰/۶۸۶	۰/۵۴۳
عدم قطعیت	۰/۷۲۸	۰/۷۰۸	۰/۵۱۵
پیچیدگی	۰/۷۶۸	۰/۶۸۶	۰/۵۲۶
نوسان	۰/۷۰۵	۰/۶۵۷	۰/۴۶۳
فشار کاری محیطی	۰/۷۲۵	۰/۱۰۴	۰/۰۷۵
کارکردهای اجرایی	۰/۷۰	۰/۴۵۳	۰/۳۱۷
خودتنظیمی	۰/۶۹۱	۰/۷۴۸	۰/۵۱۶
حافظه	۰/۷۴۳	۰/۹۳۲	۰/۶۹۲
انعطاف‌پذیری	۰/۶۶۶	۰/۹۰۲	۰/۶۰۰
منابع توانمندساز سایبری	۰/۸۹۴	۰/۸۵۵	۰/۷۶۴
مدیریت منابع	۰/۸۹۹	۰/۹۰۱	۰/۸۰۹
آموزش	۰/۸۸۶	۰/۸۶۷	۰/۷۶۸
سازمان	۰/۹۰۱	۰/۸۳۶	۰/۷۵۳
دکترین	۰/۸۹۱	۰/۷۲۹	۰/۶۴۹
			Red= 0/603

همان‌طور که در جدول (۵) گزارش شده است، تمامی سازه‌ها به‌جز فشار کاری محیطی دارای مقادیر Red بیشتر از حداقل مقدار معیار تغییرپذیری ۰/۰۹۵ هستند. معیار تغییرپذیری برای کل مدل بیشتر از مقدار بحرانی ۰/۰۹۵ است که نشان‌دهندهٔ برازش مناسب مدل بر اساس این معیار است.

ب) معیار Q^2: برای تمامی سازه‌های درون‌زای مدل بیشتر از مقدار مطلوب ۰/۱۵ است که رابطه‌مند بودن پیش‌بینی سازه‌های مدل را نشان می‌دهد.

شاخص‌های بخش ساختاری مدل هم نشان می‌دهد که روابط میان سازه‌های پنهان به‌درستی ترسیم شده است.

- ارزیابی برازش کلی مدل

الف) معیار GOF: معیار برازش نکویی یکی از معیارهای ارزیابی برازش کلی مدل است. مقدار GOF مدل ۰/۷۶۹ محاسبه شد که نشان‌دهندهٔ برازش قوی مدل است.

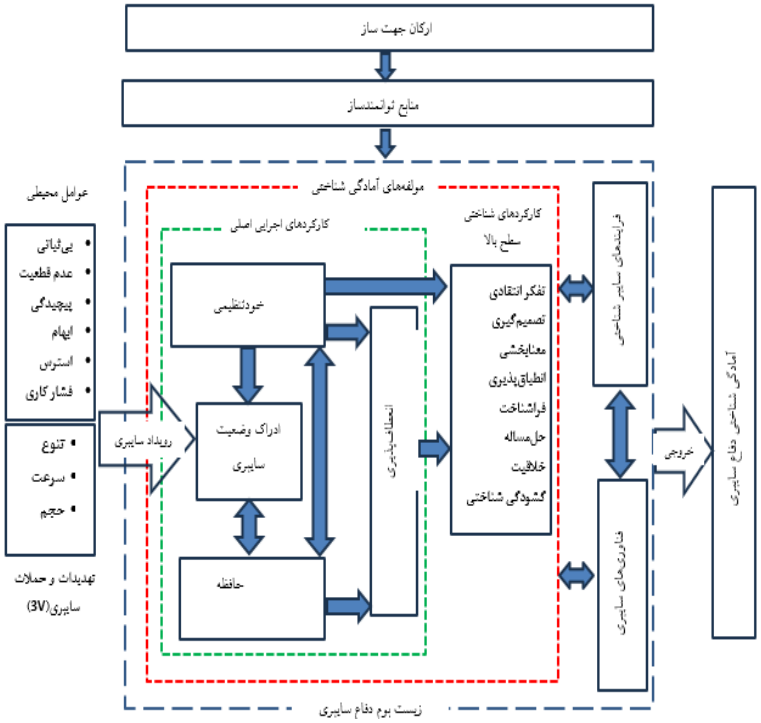
جدول ۶. معیار برازش نکویی

	Communality(AVE)	R^2
فناوری‌های سایبر شناختی	۰/۸۴۸	۰/۷۰۶
هوش مصنوعی	۰/۸۵۶	۰/۸۴۲
داده‌کاوی	۰/۸۰۰	۰/۸۴۰
غوطه‌وری	۰/۸۹۰	۰/۹۰۲
کارکردهای شناختی سطح بالا	۰/۷۷۹	۰/۹۶۶
گشودگی	۰/۸۸۲	۰/۸۵۶
تصمیم‌گیری	۰/۷۵۸	۰/۸۲۸
تفکر انتقادی	۰/۹۰۱	۰/۷۷۶
معنابخشی	۰/۸۰۵	۰/۶۱۷
انطباق‌پذیری	۰/۸۳۷	۰/۷۵۸
فراشناخت	۰/۶۲۷	۰/۶۸۶
حل مسئله	۰/۷۸۱	۰/۷۳۹
خلاقیت	۰/۶۴۲	۰/۲۱۸
فرایندهای سایبرشناختی	۰/۹۶۳	۰/۸۶۳
آگاهی وضعیتی	۰/۹۷۵	۰/۹۵۱
خودآگاهی	۰/۹۵۲	۰/۹۰۷
ادراک عوامل محیطی	۰/۷۴۴	۰/۲۱۳
ابهام	۰/۷۹۲	۰/۶۸۶
عدم قطعیت	۰/۷۲۸	۰/۷۰۸
پیچیدگی	۰/۷۶۸	۰/۶۸۶
نوسان	۰/۷۰۵	۰/۶۵۷
فشار کاری محیطی	۰/۷۲۵	۰/۱۰۴
کارکردهای اجرایی	۰/۷۰	۰/۴۵۳
خودتنظیمی	۰/۶۹۱	۰/۷۴۸
حافظه	۰/۷۴۳	۰/۹۳۲
انعطاف‌پذیری	۰/۶۶۶	۰/۹۰۲
منابع توانمندساز سایبری	۰/۸۹۴	۰/۸۵۵

	Communality(AVE)	R^2
مدیریت منابع	۰/۸۹۹	۰/۹۰۱
آموزش	۰/۸۸۶	۰/۸۶۷
سازمان	۰/۹۰۱	۰/۸۳۶
دکترین	۰/۸۹۱	۰/۷۲۹
	M=۰/۸۰۷	M=۰/۷۳۳
$GOF = \sqrt{0/733 \times 0/807} = 0/769$		

ب) جذر میانگین مربعات باقیمانده استاندارد[1](SRMR) برای مدل مقدار ۰/۰۹ محاسبه شد که با توجه به دامنهٔ بحرانی کمتر از ۰/۱۰ یا ۰/۰۸ نشان‌دهندهٔ برازش مناسب مدل است.

با توجه به مطالب فوق، شاخص‌های برازش کلی مدل هم نشان می‌دهد که مدل کلی آمادگی شناختی دفاع سایبری از برازش قابل قبولی برخوردار است.



شکل ۱. الگوی مفهومی زیست‌بوم آمادگی شناختی دفاع سایبری

1 (SRMR) Standardized Root Mean Square Residual

نتیجه‌گیری و پیشنهادها

با توجه به این‌که ماهیت تهدیدات سایبری بسیار سریع و متنوع و دائماً در حال تغییر است، بنابراین نمی‌توان برای هر سناریوی دفاعی، آموزش‌هایی را به کارکنان سایبری ارائه داد. با آمادگی شناختی، می‌توان آموخت که در هر سناریوی تهدید و حمله سازگار شد و در مواجهه با چالش‌هایی که در واکنش به حادثه رخ می‌دهند، بسیار چابک‌تر و مؤثرتر بود. یادگیری با حجم زیادی از دانش آغاز می‌شود و مستلزم افزودن مداوم مهارت‌ها، اطلاعات و تجربه‌های جدید به آن پایه است. همان‌طور که فرایند یادگیری اتفاق می‌افتد، مهارت بهبود می‌یابد، الگوهای تفکر توسعه‌یافته و خودکار می‌شود که ازنظر کارایی می‌تواند شگفت‌انگیز باشد. بااین‌حال، در یک موقعیت بحرانی و غیرمنتظره، سوگیری می‌تواند تفکر را محدود کند. برای دور زدن سوگیری، باید متفاوت فکر کرد که این امر مستلزم خودآگاهی و نحوهٔ درک محیط است تا تشخیص دهیم که چه زمانی الگوهای تفکر خودکار وارد می‌شوند. ارزشمندترین مهارت یا ویژگی برای نیروی کار دفاع سایبری، آمادگی شناختی فرد است که به او امکان می‌دهد اغلب بدون نیاز به آموزش مجدد، یادگیری خود را از یک سیستم یا سناریو به سیستم یا سناریوی دیگر انتقال دهد. مبنای یافته‌های این پژوهش مجموعه‌ای از مهارت‌ها و شایستگی‌های موردنیاز برای کارکنان دفاع سایبری است که با عنوان آمادگی شناختی دفاع سایبری نام‌گذاری شد. آمادگی شناختی در این پژوهش تأکید بر آمادگی ذهنی و مجموعهٔ دانش، توانایی‌ها و مهارت‌هایی دارد که برای عملکرد مؤثر کارکنان دفاع سایبری در مواجهه با عوامل محیطی سایبری ضروری است.

تحلیل یافته‌های به‌دست‌آمده از انجام مصاحبه‌ها با خبرگان علمی و اجرایی در تائید ادبیات موجود در این زمینه نشان می‌دهد که نظام آمادگی دفاع سایبری، زیست‌بومی شناختی متشکل از فرایندها، فناوری‌ها، مؤلفه‌های آمادگی شناختی و عوامل محیطی مؤثر بر آن در قالب یک زیست‌بوم فنی - اجتماعی با اجزاء؛ درونداد، فرایند، برونداد، بازخور، عوامل محیطی و پیامدها است. مدل نهایی حاصل‌شده بیانگر این است که در عملیات دفاع سایبری اتخاذ رویکرد صرفاً فناورانه و بدون در نظر گرفتن دانش مهارت و صلاحیت‌های کارکنان دفاع سایبری محکوم به شکست است.

در این تحقیق دفاع سایبری اثربخش مستلزم پرداختن به ابعادی مانند آمادگی‌های

شناختی کارکنان دفاع سایبری، فناوری‌های سایبری (جهت کاهش بار شناختی و ارتقاء مهارت‌های شناختی)، فرایندهای سایبر شناختی (مانند آگاهی وضعیتی و خودآگاهی)، عوامل محیطی و منابع توانمندساز است. این رویکرد با شناسایی محدودیت‌های شناختی عوامل انسانی در مواجهه با تهدیدها و حمله‌های سایبری، نسبت به شناسایی آمادگی‌های شناختی موردنیاز برای دفاع سایبری اقدام کرده است.

باوجود پیشینه و مبانی نظری گسترده در زمینه آمادگی‌های شناختی و آمادگی سایبری این پدیده‌ها هنوز به‌خوبی شناخته نشده‌اند. در این تحقیق سعی شد به‌صورت توأمان به هر دو مقولهٔ آمادگی شناختی و سایبری با رویکرد زیست‌بومی و به‌طور هم‌زمان، نقش عوامل محیطی، فناوری‌ها و فناوری‌های سایبری و شناختی موردمطالعه قرار گیرد. بااین‌وجود، تعداد زیاد عوامل تشکیل‌دهندهٔ نظام آمادگی شناختی دفاع سایبری مانع از آن شد که همهٔ ابعاد مربوط به هر یک از این عوامل به‌طور کامل بررسی و تحلیل شوند. ازاین‌رو پیشنهاد می‌شود در پژوهش‌های بعدی که در این زمینه انجام می‌شوند، تأثیر هر یک از عوامل تشکیل‌دهندهٔ این نظام به‌طور عمیق‌تر و گسترده‌تر موردمطالعه قرار گیرند. با توجه به اهمیت جنبه‌های شناختی کاربران دفاع سایبری، فناوری‌ها و فناوری‌های سایبری و شناختی پیشنهادهای زیر برای پژوهش‌های آتی در این زمینه ارائه می‌شوند:

- مطالعهٔ جامع و گسترده‌تر تأثیر منابع توانمندساز و عوامل محیطی بر زیست‌بوم دفاع سایبری،
- به‌کارگیری فناوری‌های نوظهور مثل هوش مصنوعی، غوطه‌وری و کلان داده‌ها به‌منظور کاهش بار شناختی و ارتقاء مؤلفه‌های آمادگی شناختی کارکنان دفاع سایبری،
- در برنامه‌های راهبردی ارتقاء آمادگی سایبری نیروهای مسلح ج.ا.ا، رویکرد زیست‌بومی دفاع سایبری این پژوهش و توانمندسازی و ارتقای سطح شایستگی‌های شناختی در کنار شایستگی‌های فنی موردتوجه قرار گیرد.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱. ایجاد نظام آمادگی دفاع سایبری، به عنوان زیست‌بومی شناختی متشکل از فرآیندها، فناوری‌ها، مؤلفه‌های آمادگی شناختی و عوامل محیطی مؤثر بر آن،

۲. توجه به قابلیت‌ها و آمادگی‌های شناختی عنصر مدافع لایه شناختی به

عنوان مهم‌ترین و درعین‌حال آسیب‌پذیرترین لایه در فضای سایبر،
۳. پرداختن به دفاع سایبری اثربخش شامل ابعاد آمادگی‌های شناختی کارکنان دفاع سایبری، فناوری‌های سایبری (جهت کاهش بار شناختی و ارتقاء مهارت‌های شناختی)، فرایندهای سایبر شناختی (مانند آگاهی وضعیتی و خودآگاهی)، عوامل محیطی و منابع توانمندساز است.

قدردانی

از استادان و مصاحبه‌کنندگانی که در این پژوهش به ما یاری رساندند، سپاسگزاریم.

تضاد منافع:

نویسندگان تصریح می‌دارند هیچ‌گونه تضاد منافعی درخصوص پژوهش حاضر وجودندارد.

منابع

- حسین‌زاده، جواد؛ احمدی، فرید و کلبخانی، هاشم (۱۴۰۳). ارائه یک مدل جامع برای سنجش آمادگی کشورها در مواجهه با انقلاب صنعتی چهارم. فصلنامه آینده‌پژوهی دفاعی، دوره ۹، شماره ۳۲، شماره پیاپی ۳۲، خرداد ۱۴۰۳، صفحه ۱۵۹-۱۸۸
- خرازی، کمال و تلخابی، محمود (۱۳۹۳). مبانی آموزش‌وپرورش شناختی، تهران: انتشارات سمت.
- طالبی، مرتضی؛ محجوب عشرت‌آبادی، حسن و آقایی، محسن (۱۴۰۳). مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی. فصلنامه علوم و فنون نظامی، دوره ۲۰، شماره ۶۸ شهریور ۱۴۰۳، صفحه ۶۸-۳۹
- سیف، علی‌اکبر (۱۳۸۸). روانشناسی پرورشی نوین، تهران: انتشارات آگاه.
- فراستخواه مقصود (۱۳۹۶). روش تحقیق کیفی در علوم اجتماعی با تأکید بر نظریه بر پایه (گراندد تئوری)، تهران: انتشارات آگاه.
- ناجی، احمدعلی؛ رحیمیان، اسحاق و طالع پسند، سیاوش. (۱۳۹۶). اثربخشی آموزش آمادگی شناختی بر مهارت تصمیم‌گیری و عملکرد تیراندازی با اثر تعدیل‌کنندگی اضطراب حالتی - رقابتی. فصلنامه علمی پژوهشی طب انتظامی، دوره: ۷، شماره:۱.

- Al Sabbagh, B. & Kowalski (2017). Socio-Technical SIEM (ST-SIEM): Towards Bridging the Gap in Security Incident Response. International Journal of Systems and Society (IJSS). 4. 8-21. 10.4018/IJSS.2017070102.
- Archibald, R. F, Ivano;Di Filippo, Daniele; Archibald, Shane (2014).Unlocking a project team's high-performance potential using cognitive readiness: A research study report and call to action. PM World Journal,2(11), 1-46.
- Ben-Asher, N. and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Comput. Human Behav. 48, 51–61. doi: 10.1016/j.chb.2015.01.039
- Bodenhausen, Galen V. Peery, Destiny. (2009). "Social Categorization and Stereotyping In vivo: The VUCA Challenge". Social and Personality Psychology Compass. 3 (2): 133–151. doi:10.1111/j.1751-9004.2009.00167.x. ISSN 1751-9004.
- Bolstad, C. A. Cuevas, H. M. Babbitt, B. A. Semple, C. A. & Vestewig, R. E (2006). Predicting cognitive readiness of military health teams. Paper presented at the International Ergonomics Association 16th World Congress, Maastricht, Netherlands
- Bolstad Cheryl A, E. M. R. and Cuevas Haydee M. (2014). A theoretically based approach to cognitive readiness and situation awareness assessment In H. F. O'Neil, Perez, Ray S, Baker, Eva L (Ed.), Teaching and Measuring Cognitive Readiness (pp. 161-179).
- Branscome, T. A. & Grynovicki, J. O (2007). An investigation of factors affecting multi-task performance in an immersive environment (ARL-TR-4325). Aberdeen Proving Ground, MD: U.S. Army Research Laboratory, Human Research and Engineering Directorate
- Buchler, N. Fitzhugh, S. M. Marusich, L. R. Ungvarsky, D. M. Lebiere, C.and Gonzalez, C. (2016). Mission command in the age of network-enabled operations: social network analysis of information sharing and situation awareness. Front. Psychol. 7:937. doi: 10.3389/fpsyg.2016.00937
- Buchler, N. La Fleur, C. G. Hoffman, B. Rajivan, P.Marusich, L. and Lightner, L (2018). Cyber teaming and role specialization in a cyber security defense competition. Front. Psychol. 9:2133. doi: 10.3389/fpsyg.2018.02133
- Coghlan, D. and Brydon-Miller, M. (2014). The SAGE Encyclopedia of Action Research. London: Sage Publications, Ltd. doi: 10.4135/9781446294406

- D'Amico, A. Whitley, K. Tesone, D. O'Brien, B. & Roth, E (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49(3), 229–233. https://doi.org/10.1177/154193120504900304
- Diamond A. (2013). Executive functions. Annual review of psychology, 64, 135–168. https://doi.org/10.1146/annurev-psych-113011-143750
- Department Of Defense. (2018). JP 3-12, Cyberspace Operation, Washington, DoD
- Dyer, J. L, Centric, J. H, &Wampler, R. L. (2007). A case for decentralized training (Research Report 1866). Arlington, VA: U.S. Army Research Institute. (2007). A case for decentralized training. Retrieved on October 25. 2008
- Fletcher, J. D. & Wind, A. P. (2014). The evolving definition of cognitive readiness for military operations. In Teaching and measuring cognitive readiness (pp. 25-52). Springer, Boston, MA
- Fletcher, J. D. (2004). Cognitive readiness: Preparing for the unexpected (D-3601). Alexandria, VA: Institute for Defense Analyses.
- Frostakhah Maqsood (2016). Qualitative research method in social sciences with emphasis on grounded theory (grounded theory), Tehran: Aghat Publications[in Persian]
- Good, D. Yeganeh, B (2012).Cognitive agility: adapting to real-time decision-making at work. Organization Development Practition. 44, 13–17.
- Grier, R.A. (2012). Military cognitive readiness at the operational and strategic levels: A theoretical model for measurement development. Journal of Cognitive Engineering and Decision Making.
- Hagemann Bonnie, B. S (2016), Research on trends in executive development: A benchmark report.
- Hosseinzadeh, Javad, Ahmadi, Farid and Kalbkhani, Hashem (2024). Providing a comprehensive model to measure countries' readiness in facing the fourth industrial revolution. Quarterly Journal of Defense Studies, Volume 9, Number 32, Serial Number 32, Khordad 1403, Pages 159-188[in Persian]
- Jackson, Thoemmes,Jonkmann, Lüdtke and Trautwein(2012).Military Training and Personality Trait Development: Does the Military Make the

Man, or Does the Man Make the Military? Psychological Science, 23 (3), 270–277.
- Joint Chiefs of Staff, (2018), "Joint Publication 3-12: Cyberspace Operations",
- Jøsok, Ø, Knox, B. Helkala, K. Lugo, R. Sutterlin, S. and Ward, P (2016).“Exploring the hybrid space theoretical framework applying cognitive science in military cyberspace operations, Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience (pp. 178-188).
- Kharazi, Kamal and Talkhabi, Mahmoud (2013). Basics of Cognitive Education, Tehran: Samit Publications.
- Knox, B. J. Jøsok, Ø, Helkala, K. Khooshabeh, P. Ødegaard, T. Lugo, R. G. et al (2018). Socio-technical communication: the hybrid space and the OLB model for science-based cyber education. Mil. Psychol. 30, 350–359.
- Knox, B. J. Lugo, R. G. Jøsok, Ø, Helkala, K. and Sütterlin, S. (2017). “Towards a cognitive agility index: the role of metacognition in human-computer interaction,” in Proceedings of the Conference on HCI International 2017, (Cham: Springer International Publishing), 330–338.
- Lathrop, S. D. Trent, S. and Hoffman, R. (2016). “Applying human factors research towards cyberspace operations: a practitioner’s perspective. In Advances in Human Factors in Cybersecurity, ed. D. Nicholson. Cham: Springer International Publishing. 2016, Volume 501 ISBN: 978-3-319-41931-2
- Mgbere.A (2017). Enhancing cognitive readiness: Instruction and assessment.paper presented at the 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Ukraine.
- Morrison, J. E. & Fletcher, J. D. (2002). Cognitive readiness. Alexandria, VA: Institute for Defense Analyses.Studies Institute, U.S. Army War College.
- Murray. S (2016). Human skills are essential in the battle against cybercrime.
- NATO (2016a). Cyber Defence Pledge. Brussels: NATO.
- NATO (2016b). Warsaw Summit Communiqué. Brussels: NATO.
- Naji Ahmad Ali, Rahimian, Boger Ishaq and Tal Pasand, Siavash. (1396). The effectiveness of cognitive preparation training on decision-making

skills and shooting performance with the moderating effect of state-competitive anxiety. Police Medicine Quarterly 7[in persian]

- NOBLES,Calvin(2018). Botching Human Factors in Cybersecurity in BusinessOrganizations, HOLISTIC Vol 9, Issue 3, 2018, pp. 71-88, DOI: 10.2478/hjbpa-2018-0024
- O'Neil, Pere,& Baker (2014). Teaching and Measuring Cognitive Readiness. Springer Science+Business Media New York.DOI 10.1007/978-1-4614-7579-8_1,
- Perez, R. S. & Baker, E. L. (2014). Teaching and measuring cognitive readiness. H. F. O'Neil (Ed). New York, NY: Springer
- Raymond C.K. Chan, David Shum, Timothea Toulopoulou, Eric Y.H. Chen(2008). Assessment of executive functions: Review of instruments and identification of critical issues, Archives of Clinical Neuropsychology, Volume 23, Issue 2, March 2008, Pages 201–216.
- Seif, Ali Akbar (2008). Modern Educational Psychology, Tehran: Aghat Publications[in Persian]
- Sternberg, Robert J. (2014). A model for instruction and assessment of cognitive readiness. In R. S. P. Harold F. O'Neil, Eva L. Baker (Ed.), Teaching and Measuring Cognitive Readiness (pp. 315-361): Springer Publishing Company.
- Talebi, Morteza, Mahjoub Eshratabadi, Hassan and Aghaei, Mohsen (2024). Components of cognitive readiness of cyber defense in the military field. Military Sciences and Techniques Quarterly, Volume 20, Number 68 ،September 2024, pages 68-39[in Persian]
- Tversky, Amos. Kahneman,Daniel (1974). Judgment under Uncertainty: Heuristics and Biases، Science, New Series, Vol. 185, No. 4157. (Sep. 27, 1974), pp. 1124-1131
- U.S. Army Heritage and Education Center. (2018). "Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)? USAHEC Ask Us a Question. The United States Army War College.