Military Science and Tactics
https://www.qjmst.ir/

Cognitive readiness components of cyber defense in the military field

Morteza Talebi [1]✉ | Hasan Mahjoub Eshratabadi [2] |Mosen Aghaee[3]

1. Corresponding Author. I.R.I Army Command and Staff University, Tehran, Iran.
E-mail: m.talebi@casu.ac.ir
2. Faculty of Management, University of Shahid Sattari, Tehran, Iran.
E-mail: hassanmahjub@ut.ac.ir
3. Faculty of Security, Supreme National Defense University, Tehran, Iran.
Email: aghaee@sndu.ac.ir

Article Info

Article type:

Research Article

Article history:

Received

24 December 2023

Received in revised form

22 January 2024

Accepted

25 January 2024

Published online

12 September 2024

Keywords:

cyber defense cognitive readiness system,

cognitive readiness,

defense readiness

ABSTRACT

Objective: Due to the speed, variety and volatility of cyber threats, it is not possible to provide training to cyber employees for every defense scenario. The current research was carried out with the aim of calculating the cognitive readiness components of cyber defense in the military field in order to adapt and effectively face cyber threats.

Methodology: This research is mixed in terms of its purpose, application and approach in data collection and analysis. In the qualitative part, meta-synthesis and content analysis method and to analyze quantitative data from descriptive statistics and to evaluate the fit of the conceptual model of the cyber defense cognitive readiness system, factor analysis method and SmartPLS software were used

Findings: The results of the qualitative part of the research showed that the concept of cognitive readiness of cyber defense includes two components of main executive functions and high-level cognitive functions with 11 sub-components; Memory, self-regulation, flexibility, decision making, problem solving, cognitive openness, metacognition, creativity, adaptability, critical thinking. The results of the confirmatory factor analysis in the quantitative section also showed that the components of cyber defense cognitive readiness have a factor load and a significant effect on the related structures, and the data obtained from this research fits well with the factor structure of this scale.

Conclusion: The most valuable skill or characteristic for the cyber defense workforce is the individual's cognitive preparation, which often allows him to transfer his learning from one system or scenario to another without the need for retraining. By counting the components of cognitive readiness and improving it, it is possible to learn how to adapt to the environment in each threat and cyber-attack scenario and to be much more agile and effective in facing the challenges that occur in response to the incident.

Cite this article: Talebi, Morteza, Mahjoub Eshratabadi, Hasan, Aghaee, Mosen**. (**2024). Cognitive readiness components of cyber defense in the military field. *Military science and tactics*, 20 (68), 39-68.
DOI: http//doi.org/10.22034/qjmst.2024.2018685.1994
Publisher: AJA Command and Staff University
DOI: 10.22034/qjmst.2024.2018685.1994

فصلنامه علمی علوم و فنون نظامی
https://www.qjmst.ir/
دانشگاه فرماندهی و ستاد آجا

مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی

مرتضی طالبی [۱] ✉ | حسن محجوب عشرت‌آبادی [۲] | محسن آقایی [۳]

۱. نویسنده مسئول، دانشکده فرماندهی و ستاد، دانشگاه فرماندهی و ستاد آجا، تهران، ایران، رایانامه: m.talebi@casu.ac.ir

۲. دانشکده مدیریت، دانشگاه هوایی شهید ستاری، تهران، ایران. رایانامه: hassanmahjub@ut.ac.ir

۳.دانشکده امنیت، دانشگاه عالی دفاع ملی، تهران، ایران. رایانامه: aghaee@sndu.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی
تاریخ دریافت:
۱۴۰۲/۱۰/۰۳
تاریخ بازنگری:
۱۴۰۲/۱۱/۰۲
تاریخ پذیرش:
۱۴۰۲/۱۱/۰۵
تاریخ انتشار:
۱۴۰۳/۰۶/۲۲

کلیدواژه‌ها: *آمادگی دفاعی، آمادگی شناختی، دفاع سایبری.*

چکیده

هدف: با توجه سرعت، تنوع و نوسان تهدیدات سایبری ، امکان ارائه آموزش به کارکنان سایبری برای هر سناریوی دفاعی، وجود ندارد. پژوهش حاضر با هدف احصاء مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی به منظور سازگاری و مواجهه موثر با تهدیدات سایبری انجام شده 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 ، برای تجزیه‌وتحلیل داده‌های کمی از آمار توصیفی و برای ارزیابی برازش مدل مفهومی آمادگی شناختی دفاع سایبری از روش تحلیل عاملی و نرم‌افزار اسمارت پی.ال.اس استفاده شده است.

یافته‌ها: نتایج بخش کیفی پژوهش نشان داد که مفهوم آمادگی شناختی دفاع سایبری شامل دو مؤلفه کارکردهای اصلی اجرایی و کارکردهای شناختی سطح بالا با ۱۱ زیرمؤلفه؛ حافظه، خودتنظیمی، انعطاف‌پذیری، تصمیم‌گیری، حل مسئله، گشودگی شناختی، فراشناخت، خلاقیت، انطباق‌پذیری، تفکر انتقادی است. نتایج تحلیل عاملی تأییدی دربخش کمی نیز نشان داد مؤلفه‌های آمادگی شناختی دفاع سایبری دارای بار عاملی و تأثیر معنی‌داری برسازه‌های مربوطه هستند و داده‌های حاصل از این پژوهش با ساختار عاملی این مقیاس برازش مناسبی دارد.

نتیجه‌گیری: با توجه سرعت، تنوع و نوسان تهدیدات سایبری ، امکان ارائه آموزش به کارکنان سایبری برای هر سناریوهای دفاعی، وجود ندارد. با احصاء مؤلفه‌های آمادگی شناختی و ارتقاء آن، می‌توان متناسب با محیط با اغلب سناریوهای تهدید و حمله سایبری سازگار شد و در مواجهه با چالش‌هایی که در واکنش به حادثه رخ می‌دهند، بسیار چابک‌تر و مؤثرتر بود.

استناد:طالبی، مرتضی؛ محجوب عشرت‌آبادی، حسن و آقایی، محسن. (۱۴۰۳). مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی. *علوم و فنون نظامی*، ۲۰ (۶۸)، ۶۸- ۳۹.

DOI: http//doi.org/10.22034/qjmst.2024.2018685.1994

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

DOI: 10.22034/qjmst.2024.2018685.1994

مقدمه

هدف غایی و نهایی تمام اشکال منازعات و جنگ‌ها تسلط بر ذهن و اخلال در فرایندهای شناختی مخاطب به‌منظور تحمیل اراده خود بر اوست و فضای سایبری یکی از بهترین و کم‌هزینه‌ترین روش‌ها برای نیل به این مقصود است. افزایش کاربرد و تکیه بر فناوری‌های سایبری در عملیات نظامی منجر به معرفی این فضا به‌عنوان عرصه 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 نموده است. این امر از طریق سرمایه‌گذاری در واحدهای دفاع سایبری، آموزش دفاع سایبری و به رسمیت شناختن فضای سایبری به‌عنوان عرصه عملیات (NATO, 2016b) مشخص می‌شود. بهره‌برداری از ویژگی‌ها و ظرفیت‌های عرصه فضای سایبری برای تأثیرگذاری بر عملکردهای شناختی کاربران است. این فضای به‌عنوان یک زیست‌بوم با ماهیت فناورانه - اجتماعی دارای ابعاد فناوری، انسان (مدافع، مهاجم و کاربر) و فرایندها است (Al Sabbagh, Kowalski & 2017). 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 عدم‌قطعیت در محیط‌های دفاعی مدرن مانند عرصه سایبری، به معنای تغییر نیازهای آتی نیروهای مسلح و ضرورت خلق شایستگی‌ها و قابلیت‌های دفاعی جدید است. از جمله‌ی این شایستگی‌ها می‌توان به آمادگی‌های شناختی[1]، همراه با تاب‌آوری[2]، در مواجهه و دفاع در برابر تهدیدات نوظهور خلق‌شده در این فضا اشاره نمود. 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 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 نموده و به او امکان می‌دهد اغلب بدون نیاز به

[1] Cognitive Readiness
[2] Resilience

آموزش مجدد، یادگیری خود را از یک سیستم یا سناریو به سیستم یا سناریوی دیگر انتقال دهد.

در حال حاضر حملات و تهدیدات 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 تصمیم‌گیرنده انسانی، از طریق بهره‌برداری از فرایندهای شناختی جهت مقابله با این تهدیدات، هنوز هم ناگزیر و ضروری هستند. با تأکید بر قابلیت استفاده از فناوری ها در دفاع سایبری، نیروی انسانی به عنوان ضعیف ترین حلقه در زنجیره امنیت شناخته می شوند. بنابراین ، انسان در زنجیره دفاع سایبری حلقه‌ای ضعیف با جذابیت بالا در معرض تهدیدات و حملات سایبری قرار می گیرد (Nobel,2018). عدم شناسایی و بهره‌گیری مناسب از عوامل توانمندساز و پیشران مانند فناوری‌ها و سیستم‌های سایبر - شناختی (یادگیری ماشین، داده‌کاوی، پردازش زبان طبیعی و ...) 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 در حوزه‌های نظامی 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 پیچیده رزم سایبری موجب بروز خطاها و سوگیری‌های شناختی و درنتیجه اخذ تصمیمات و اقدامات 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.

[1] Advanced Persistence Threats

نظر به موارد فوق هدف اصلی این پژوهش احصاء مولفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی هست که در بخش کیفی با فراترکیب و تحلیل محتوای ادبیات آمادگی شناختی به احصاء مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی پرداخته است و سپس اعتبارسنجی و برازش الگوی مفهومی آمادگی شناختی دفاع سایبری در حوزه نظامی را انجام داده است.

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری

در پژوهش حاضر، از الگوی منطق در طراحی نظام و فرایندهای مربوط به آن استفاده شده است. چراکه برای پیاده‌سازی کامل و موفق یک نظام جامع‌ومانع، لازم است که تفکر سیستمی و جامع‌نگر بر سازمان و محیط کار و فعالیت حاکم بوده و فرهنگ‌سازمانی با اصول و الزامات آن هماهنگی داشته و روحیه کارِگروهی و انعطاف‌پذیری در سازمان جاری و ساری باشد. نظام آمادگی شناختی دفاع سایبری در حوزه نظامی، به معنی تعیین اجزای اصلی مؤثر در آمادگی شناختی دفاع سایبری با تبیین کارکرد مستقل و وابسته هر یک از آن‌ها باهم برای فهم و جهت‌گیری سیستمی در ارتباط با نهادینه نمودن مؤلفه‌های آمادگی دفاع شناختی به‌منظور زمینه‌سازی و ایجاد چارچوب‌هایی برای انجام تکالیف فردی و سازمانی و هم‌افزایی بین آن‌ها هست. در این نظام با الگوگیری از الگوی منطق اگر آنگاه، عوامل محیطی (مشتمل بر پویایی، عدم قطعیت، پیچیدگی، ابهام و...) و تهدیدات و حملات سایبری (در حجم، تنوع و سرعت بالا) به‌عنوان ورودی نظام و اسناد بالادستی و عوامل توانمندساز (مشتمل بر دکترین، سازمان، آموزش، مدیریت منابع) به‌عنوان الزامات نظام برای رسیدن به اهداف کلان آمادگی شناختی دفاع سایبری در حوزه نظامی با رعایت اصول، ارزش‌ها و سیاست‌های مصوب یا ابلاغی تعیین و ارائه می‌گردد.

طبق تعریف ناتو، فضای سایبر، فراتر از شبکه اینترنت است و نه‌تنها شامل سخت‌افزار، نرم‌افزار و سامانه‌های اطلاعاتی، بلکه شامل افراد و تعاملات اجتماعی آن‌ها در داخل این شبکه‌ها نیز هست (مرکز دفاع سایبری ناتو، ۲۰۱۲).

فضای سایبری یک قلمرو جهانی در محیط اطلاعاتی است که از شبکه وابسته به هم از زیرساخت‌های فناوری اطلاعات شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های مربوط به آن‌ها تشکیل‌شده است. در دستورالعمل میدانی اقدامات سایبرالکترومغناطیس[1] ارتش ایالات متحده آمریکا (۲۰۱۴)، فضای سایبر، یک قلمرو

[1] FM 3-12

جهانی در محیط اطلاعاتی قلمداد شده است که مشتمل بر ابعاد فیزیکی، اطلاعاتی و شناختی به شرح زیر است:

- ≠ بعد فیزیکی: فضای سایبر یک شبکه ارتباطی گسترده جهانی متشکل از زیرساخت‌های ارتباطی و فناوری اطلاعات است.
- ≠ بعد اطلاعاتی: فضای سایبر یک منبع اطلاعاتی توزیع‌شده حاوی انواع و سطوح مختلف داده، اطلاعات و دانش، از خودی و غیرخودی است.
- ≠ بعد شناختی: فضای سایبر یک جامعه مجازی است که اعضای آن، قابلیت انجام فعالیت‌های اجتماعی، اقتصادی، سیاسی و فرهنگی را دارند.

لایه شناختی مهم‌ترین و درعین‌حال آسیب‌پذیرترین لایه در فضای سایبر است و دفاع از این فضا تنها با توجه به لایه‌های فیزیکی و شناختی، بدون در نظر گرفتن قابلیت‌ها و آمادگی‌های شناختی عنصر مدافع این فضا عملاً ناقص و محکوم‌به شکست است.

به‌طور ساده شناخت را می‌توان به‌عنوان فرایندها یا جریان‌هایی که به کمک آن‌ها یادگیری، یادآوری و تفکر صورت می‌پذیرد، تعریف کرد. 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. درواقع 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 ازجمله 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 حوزه‌ی شناختی مجموعه‌ای اصلی از فرآیندهای 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 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 (Raymond and et al, 2008). 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» ازآنچه قبلاً آموخته‌ایم یا می‌توانیم به خاطر بسپاریم استفاده می‌کنند. این واحدهای دانش شامل همه‌چیز از زبان، تجربیات، خاطرات، انتظارات و احساسات است (Diamond, 2013).

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[1] (۲۰۱۵) پیشنهاد می‌کنند که اپراتورهای 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 (غیرقابل پیش‌بینی‌بودن و نبود اطلاعات کافی)، پیچیدگی (تعاملات محیطی و وجود عوامل چندگانه) و ابهام محیطی (ناتوانی درک وقایع و ارزیابی درست محیط خارجی) است (Hagemann ,2016). مگبری[2] (۲۰۱۷) آمادگی شناختی را به‌عنوان شایستگی جدیدی در حوزه رهبری برای پذیرش و سازگاری با تغییرات غیرقابل‌پیش‌بینی و رویارویی با چالش‌های محیطی مطرح می‌کند.

واژه مخفف VUCA برای اولین بار در سال ۱۹۸۷، با تکیه‌بر نظریه‌های رهبری وارن بنیس[3] و برت نانوس[4] برای توصیف یا تأمل در مورد پویایی، عدم قطعیت، پیچیدگی و ابهام شرایط و موقعیت‌های عمومی استفاده شد (دانشگاه جنگ ارتش ایالات‌متحده،۲۰۱۸). دانشگاه جنگ ارتش ایالات‌متحده، مفهوم VUCA را برای توصیف دنیای چندقطبی پرنوسان، نامطمئن، پیچیده و مبهم که نتیجه پایان جنگ سرد تلقی می‌شود، معرفی کرد.

محیط‌های سایبری به‌سرعت و گاهی اوقات به‌شدت تغییر می‌کنند. دشمنان به‌طور مداوم تاکتیک‌های خود را تغییر می‌دهند و تکنیک‌های خود را تکامل می‌دهند 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

[1] Ben-Asher and Gonzalez
[2] Mgbere
[3] Bennis, Warren
[4] Nanus, Burt

نمی‌دانند. علاوه بر این، تاکتیک‌ها، تکنیک‌ها و فرایندهای مهاجمان سایبری ازنظر طراحی پیچیده هستند و توانایی تیم‌های دفاعی را برای شناسایی، بررسی و اصلاح هر مشکلی کاهش می‌دهند. عدم قطعیت زمانی است که اطلاعات مربوطه در دسترس نباشد و ناشناخته باشد و ابهام در جایی که اطلاعات مرتبط در دسترس است اما معنای کلی آن هنوز ناشناخته است (Bodenhausen & Peery, 2009). 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 حملات و تهدیدات سایبری هرروز پیچیده‌تر و هوشمندتر می‌شوند، ایجاد سطح آگاهی و آمادگی شناختی برای مواجهه در برابر آن‌ها بسیار مهم است.

پیشینه‌های پژوهش

آمادگی شناختی کمتر از یک دهه است که در علوم نظامی مطرح شده است (Morrison & Fletcher, 2002). 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 مدنظراست، ولی در علوم نظامی آمادگی شناختی به آمادگی ذهنی افراد در شرایط استرس‌زا و همچنین استفاده 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).

در ادبیات آمادگی شناختی، تعاریف و کاربردهای مختلفی به شرح ذیل اشاره شده است:

≠ آمادگی شناختی عبارت است از آمادگی ذهنی (ازجمله 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 (Morrison & Fletcher, 2002).

≠ آمادگی شناختی طیف وسیعی از جنبه‌های فکری، عاطفی و مهارتی روانی اجتماعی و اجرای موفقیت‌آمیز شرایط استرس‌زا، مبهم و غیرقابل‌پیش‌بینی در دو سطح فرد و گروه-کار است (Bolstad and et al, 2014). در این تعریف آمادگی شناختی در دو بعد فردی و گروه-کاری در ارتباط با موقعیت‌های نوظهور و چالش‌های پیش‌رو موردتوجه قرارگرفته است.

≠ دایر[1] و دیگران (۲۰۰۷) آمادگی شناختی را توانایی به انجام رساندن مأموریت‌ها با تصمیم‌گیری و اجرای تصمیم به شیوه 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.

≠ کوزنسو، فاتکین و پاتون[4] (۲۰۰۷) آمادگی شناختی را به معنای حداکثرسازی و بهبود عملکرد شناختی انسان تعریف و آن را به‌منزله عنصر اساسی برای عملکرد مؤثر افراد برای انجام فعالیت‌ها تعریف کردند.

≠ بیرمن، تورس، دومیترویچ، ولش و گست[5] (۲۰۰۹) آمادگی شناختی را در دو حوزه تعریف کردند: ۱) دانش دانشگاهی شامل کیفیت محتوای آموزشی و همچنین توانایی افراد در به دست آوردن اطلاعات جدید در محیط دانشگاه ۲) مهارت استدلال شناختی به‌عنوان مهارت کارکرد اجرایی[6] که اطلاعات لازم را برای استدلال و حل مسئله. این نوع مهارت بیانگر توانایی افراد برای حل مسائل، کنترل بازدارنده[7] و انعطاف‌پذیری شناختی[8] است.

≠ گریر[9] (۲۰۱۲) آمادگی شناختی را از سه منظر تعریف کرده است: ۱) آمادگی شناختی تاکتیکی: حالتی از چالاکی شناختی ذهنی برای اطمینان از سطح قابل‌قبول عملکرد در انجام مأموریت‌های واگذارشده. ۲) آمادگی شناختی عملیاتی: آمادگی ذهنی (ازجمله دانش، مهارت‌ها، توانایی‌ها، انگیزه و تمایلات فردی) که افراد به‌منظور عملکرد مناسب در محیط پیچیده و غیرقابل‌پیش‌بینی به آن‌ها نیاز دارند. ۳) آمادگی شناختی راهبردی: به

[1] Dyer
[2] Branscome & Grynovicki
[3] Mental acuity
[4] Cosenzo, Fatkin, & Patton
[5] Bierman,Torres, Domitrovich, Welsh, Gest
[6] Executive function (EF) skills
[7] Inhibitory control
[8] Cognitive flexibility
[9] Grier

معنـای قابلیت افراد در انجام وظایف شناختی محول شده در محیط پیچیده و غیرقابل‌پیش‌بینی است.

≠ آرچـی بالـد، فیبـو، آرچـی بالـد و دی فیبـو[1] (۲۰۱۳) معتقدنـد آمـادگی شـناختی از دو شایسـتگی دانـش و تخصـص و توانایی شناختی کلیدی تشکیل شده است که بـه افـراد در روبرو شدن با تغییرات غیرقابل‌پیش‌بینی کمک می‌کند.

≠ فلچر و ویند[2] (۲۰۱۴) آمـادگی شـناختی را توانـایی افـراد در ۱) حـذف ابهـام و تشـخیص الگوهـای در موقعیـت‌هـای نامطمئن، مبهم و پر هرج‌ومـرج ۲) شناسـایی و اولویـت‌بنـدی مسائل و فرصت‌های ارائه‌شده۳) ارائه پاسخ مؤثر بـه مشکلات و یا فرصت‌ها ۴) پیاده‌سـازی این پاسخ تعریف می‌کنند.

≠ پرز و بیکر[3] (۲۰۱۴) آمادگی شناختی را ترکیبی از تفاوت‌های فـردی و دانـش و تجربیـات آموخته‌شده و همچنین تعامل بین تخصص افراد و موقعیت‌های پیش رو تعریـف مـی‌کننـد. استرنبرگ[4] (۲۰۱۴) آمادگی شناختی را بر اساس توانایی چهارگانه خلاق، تحلیلی، عملی[5] و خردمحور[6] تعریف می‌کند.

سه ویژگی مشترک در این تعاریف دیـده مـی‌شـود: ۱) آمـادگی شـناختی مـی‌توانـد عملکـرد شناختی افراد را پـیش‌بینـی کنـد. ۲) آمـادگی شـناختی در موقعیـت‌هـای مـبهم، پیچیـده و غیرقابل‌پیش‌بینی معنا و مفهـوم پیـدا مـی‌کنـد. ۳) آمـادگی شـناختی حاصـل تعامـل فـرد و موقعیت‌های پیش‌رو است. اینکه چرا آمادگی شناختی در حـوزه نظـامی موردتوجـه قرارگرفتـه است، به دلیل پیچیده بودن و غیرقابل‌پیش‌بینی بودن محـیط نظـامی اسـت و اینکـه نیروهـای نظـامی ازنظـر ذهنـی، اجتمـاعی و عـاطفی بـرای فعالیـت در چنـین محیطـی آمـاده باشـند و عکس‌العمل مناسب نشان دهند.

با توجه به تعاریف آمادگی شناختی، می‌توانیم مفهوم عمومی آمادگی شناختی را به مؤلفـه‌هـای خاص‌تری کاهش دهیم. برخی محققین، از منظر یک دیدگاه جامع به آمادگی شناختی نگاه می کنند. برای مثال، آن‌هـا مفهـوم‌سـازی فلتچـر (۲۰۰۴) از آمـادگی شـناختی را اصـلاح‌کـرده و آمادگی شناختی را شامل این مؤلفه‌ها می‌دانند: انطباق‌پذیری[7]، ارتباط، خلاقیت، تفکر انتقـادی،

[1] Archibald, Filippo, Daniele; Archibald
[2] Fletcher, J. D. & Wind
[3] Baker
[4] Sternberg
[5] Practical
[6] wisdom
[7] Adaptability

تصمیم‌گیری، فراشناخت، طرح‌واره بازشناسی، حل مسئله، تاب‌آوری، آگاهی وضعیتی و مهارت های کار تیمی و [روابط] بین‌فردی ((Bolstad and, et al, 2014). بولستاد، اندزلی و کیواس[1](۲۰۱۴) نگاه جامعی به ۲۱ ویژگی‌ای دارند که آمادگی شناختی را تعریف می‌کند؛ 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 بعد اصلی مفهوم‌سازی می‌کند:

۱) دانش[3]، ۲) مهارت‌ها[4] و ۳) ویژگی‌ها[5] (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 (Jackson and et al, 2012). اصطلاح صفت، معمولاً به‌عنوان جایگزین اصطلاح شایستگی مورداستفاده قرار می‌گیرد. بااین‌حال، کلیم، هارتیگ و راش[6] (۲۰۰۸) دیدگاه دیگری نسبت به شایستگی دارند که اساساً بیانگر دیدگاه اروپایی است. همچنین صفت به‌صورت قابل‌معاوضه‌ای با اصطلاح نگرش نیز مورداستفاده قرار می‌گیرد. به نظر انیل صفات از اصطلاح نگرش، فراگیرتر هستند، بنابراین، حرف «A» در مدل «KSA» اشاره به صفات دارد.

انیل، پرز و بیکر (۲۰۱۴) بر مبنای این تلاش‌های پژوهشی که درگذشته انجام‌شده‌اند، مدل فلتچر را مورد تجدیدنظر قرار داده و مدل آمادگی شناختی اُنیل را برای آموزش و ارزیابی آمادگی شناختی، ایجاد کردند.

اپراتورهای سایبری نظامی نیز باید با در نظر گرفتن عوامل اجتماعی و عوامل فناورانه از سیستم اجتماعی - فنی آگاهی داشته باشند و آن را درک کنند (Coghlan and Miller, 2014). بخشی از این وظایف در کنار بار اطلاعات زیاد، منجر به این می‌شود که کار دفاع سایبری به‌عنوان ایمنی - حیاتی توصیف شود (Knox and et al 2018). کارکنان دفاع سایبری برای حرکت و مانور در ابعاد سایبری - فیزیکی و تاکتیکی - راهبردی به‌منظور درک محیط کار به توانایی‌های شناختی (D'Amico and et al, 2016) و چابکی شناختی دارند (Jøsok and et al, 2016). دفاع سایبری در محیط‌های نظامی نیز به دلیل قرار گرفتن در معرض حملات و تهدیدات با تنوع، سرعت و حجم بالای مستمر، پیچیده‌تر از محیط دفاعی و نظامی است و نیروی انسانی

[1] Bolstad, Endsley, and Cuevas
[2] O'Neil
[3] Knowledge
[4] Skills
[5] Attributes
[6] Klieme, Hartig, and Rauch

این حوزه نیز باید از دانش و مهارت‌های لازم برای مواجهه و مقابله با تهدیدات و حملات نوظهور و غیرقابل‌پیش‌بینی برخوردار باشند و همچنین عکس‌العمل مناسبی در قبال تغییر و تحولات محیطی نشان دهند. به‌ویژه این‌که فضای 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 (Buchler and et al, 2018). درواقع توجه به آمادگی شناختی دفاع سایبری این اطمینان را خواهد داد که نیروی انسانی آن ازنظر 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 نظامی این حوزه جدید هستند.

چارچوب فضای جنگ‌های هیبریدی (ترکیبی) نیز این نظریه را مطرح می‌کند که مهارت‌های فنی به‌تنهایی برای انجام عملیات کافی نیست (Buchler and et al, 2016). چارچوب فضای هیبریدی تصدیق می‌کند که محیط کار اپراتورهای سایبری نظامی 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[1] (Knox and et al, 2018) به کاربر سایبری اجازه می‌دهد در حین انجام وظایف سایبری در سطح تاکتیکی به تفکر استراتژیک بپردازد (جوسوک و همکاران،۲۰۱۶). گود و یگانه[2] (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 اپراتور سایبری برای تحرک شناختی با استفاده از توجه انعطاف‌پذیر و استراتژی‌های خودتنظیمی قبلاً به‌عنوان چابکی شناختی توصیف شده است (Knox and et al, 2018). لاتروپ[3] و همکاران (۲۰۱۶) پیشنهاد می‌کند که اپراتورهای سایبری برای انجام وظایف بر شایستگی‌هایی مانند معنابخشی به تجربیات[4]، تفکر خلاق، تجسم ذهنی[5] و سایر عملکردهای شناختی سطح بالا متکی هستند.

[1] Cognitive performance
[2] Good & yegane
[3] Lathrop
[4] Sense making
[5] ,Mental projection

ناکس و همکاران (۲۰۱۸) از 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 (Knox and et al, 2018). چارچوب فضایی ترکیبی نیز قبلاً برای ارزیابی چابکی شناختی اپراتور سایبری در طول یک تمرین دفاع سایبری استفاده شده است. با استفاده از چارچوب فضای ترکیبی، ناکس و همکاران (۲۰۱۷) چابکی شناختی را به‌عنوان یکی از شایستگی‌های مهم شناختی که می‌تواند عملکرد اپراتور سایبری را پشتیبانی کند، پیشنهاد کرد. آن‌ها چابکی شناختی را به‌عنوان «حرکات متمرکز شناختی» در فضای ترکیبی تعریف کردند و بعداً آن‌ها نمایش چابکی شناختی در فضای ترکیبی را با فراشناخت و عملکرد اپراتورهای سایبری مرتبط کردند (Knox and et al, 2017،،

مرور مبانی نظری و پیشینه مربوط به موضوع آمادگی شناختی و دفاع سایبری نشان می‌دهد که در سال‌های اخیر شاهد فعالیت‌های زیادی مبنی بر انتشار مقالات، کتاب‌های علمی و پژوهش‌های علمی در خصوص آمادگی شناختی بوده‌ایم. بااین‌حال علی‌رغم این‌که بر توسعه آمادگی شناختی و نقش آن در بهبود عملکرد تأکید شده است، اما همچنان یک الگوی جامع که دربرگیرنده جنبه‌های آمادگی شناختی متناسب با عرصه دفاع سایبری باشد، ارائه نشده است. برای مثال تعدادی از پژوهشگران بر آمادگی شناختی فردی، بر الگوی آمادگی شناختی با تأکید بر دانش، نگرش و مهارت‌ها و تعدادی دیگر برالگوی آمادگی شناختی گروه- کاری بر الگوی سه سطحی آمادگی شناختی و گروهی دیگر از محققین بر الگوی آمادگی شناختی گروه-کاری تأکید می‌کنند. در این الگوها ارتباط متقابل بین ابعاد و مؤلفه‌های آمادگی شناختی موردتوجه قرار نگرفته است؛ بنابراین الگوهای مطرح‌شده در این حوزه نگاه همه‌جانبه و کلی نسبت به آمادگی شناختی و به‌ویژه در عرصه دفاع سایبری به‌صورت نظام‌مند نداشتند. بااین‌حال می‌توان با بهره‌گیری از این منابع و تعمیم آن به فضای سایبری ابعاد آمادگی شناختی در دفاع سایبری (پیش‌بینی، نظارت، کشف، شناسایی، مجزاسازیِ، پاسخ، بازیابی و ارزیابی) را می‌توان به‌عنوان ترکیبی از توانمندی‌های اساسی؛ رفع ابهام در موقعیت‌های پرابهام و پیچیده، تشخیص الگوهای تهدیدات سایبری، اولویت‌بندی و تصمیم مؤثر و پیاده‌سازی تصمیم درک کرد.

روش‌شناسی پژوهش

با عنایت به موضوع تحقیق که درصدد احصاء مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی و ایجاد وفاق در فرایند تصمیم‌سازی و تصمیم‌گیری برای فرماندهان است ، بر

اساس هدف در زمره تحقیقات کاربردی قرار می‌گیرد. در این پژوهش آمادگی‌های شناختی دفاع سایبری در حوزه نظامی، توصیف و تحلیل و با دیدی اکتشافی، مؤلفه‌های آمادگی شناختی دفاع سایبری در حوزه نظامی کشور ج.ا.ا ارائه شده است و ازلحاظ رویکرد پژوهش، روش ترکیبی یا آمیخته از نوع اکتشافی متوالی است. در بخش کیفی پژوهش با استفاده از روش کیفی فراترکیب و تحلیل محتوا با کدگذاری باز، محوری و انتخابی، مؤلفه‌های تشکیل‌دهنده آمادگی شناختی دفاع سایبری با رویکرد زیست‌بومی به محیط دفاع سایبری شناسایی شد. در مرحله بعد بر اساس نظرات خبرگان، الگوی اولیه را تکمیل و اصلاح گردید. 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 بخش کمی پژوهش از شیوه توصیفی- تحلیلی استفاده گردید. پرسشنامه‌ای با ۳۴ سؤال در اختیار جامعه آماری بخش کمی پژوهش قرار گرفت. برای تجزیه‌وتحلیل داده‌های کمی از آمار توصیفی (فراوانی، میانگین و انحراف استاندارد) 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 شده است. جامعه آماری برای مشارکت در فرآیند مصاحبه، شامل خبرگان حوزه 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 یاد شده شناسایی و در فرآیند مصاحبه مشارکت داده شدند. در بخش فراترکیب مقالات و منابع پژوهشی مرتبط با آمادگی‌های شناختی و دفاع سایبری هستند که از ۹۰ مقاله اولیه مرتبط با عملیات سایبری، زیست‌بوم دفاع سایبری، علوم شناختی و آمادگی‌های شناختی با استفاده از چک‌لیست ارزیابی حیاتی[1] (CASP) تعداد ۵۳ مقاله برای ورود به مرحله‌ی بعدی یعنی، مرور تمام متن و تجزیه‌وتحلیل انتخاب شدند. همچنین جامعه آماری برای توزیع پرسشنامه در مرحله کمی پژوهش، از کارشناسان آشنا با فضای سایبر و علوم و فناوری‌های سایبر - شناختی در نیروهای مسلح ج.ا.ا که دارای مشخصات مدرک تحصیلی مرتبط حداقل کارشناسی، دارای فهم راهبردی و علمی از عرصه‌های دفاع سایبری و علوم شناختی، حداقل ۱۵ سال سابقه کار در حوزه دفاع سایبری و خدمت در رده‌های فرماندهی/ مدیریتی باشند استفاده گردید.

[1] Critical Appraisal Skills program (CASP)

به‌منظور برآورد حجم نمونه تحقیق با استفاده از فرمول کوکران برای جامعه نامعین، $z_{\alpha 2}$ در سطح خطای α=۰/۰۵ برابر با ۱/۹۶ و d یا خطای مجاز برابر با ۰/۰۵ در نظر گرفته شده است. به‌منظور تعیین انحراف استاندارد، از مطالعه آزمایشی استفاده شد. در مطالعه آزمایشی، پرسشنامه آمادگی شناختی دفاع سایبری میان ۳۰ نفر توزیع شد. با توجه به تحلیل آماره‌های مرکزی و پراکندگی، میانگین متغیر آمادگی شناختی ۳/۵۱، انحراف استاندارد ۰/۳۱۸ به دست آمد. با قرار دادن مقادیر محاسبه‌شده در فرمول کوکران، حداقل حجم نمونه موردنیاز تحقیق ۱۵۵ ≈۱۵۵/۳۹ محاسبه گردید.

روایی سؤالات مصاحبه به روش محتوایی و مبتنی بر نظر خبرگان تأیید گردیده 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 در مصاحبه بهره‌برداری شد. همچنین برای قابلیت تأیید در مرحله پایانی، طبقات به‌دست‌آمده به سه نفر از مشارکت‌کنندگان اولیه به‌منظور بازبینی و تأیید برگردانده شد و نکات پیشنهادی اعمال گردید. 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 گردید.

به‌منظور بررسی روایی محتوایی به شکل کمی، 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 گردید 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 نشان‌دهنده پایایی مناسب پرسش‌های طرح‌شده برای ارزیابی ابعاد، مؤلفه‌ها و زیرمؤلفه‌ها است.

تجزیه‌وتحلیل داده‌های پژوهش

برای تجزیه‌وتحلیل داده‌های بخش کیفی پژوهش از کدگذاری باز و محوری استفاده شد. در این پژوهش از روش کدگذاری باز که یکی از معروف‌ترین روش برای تحلیل داده‌های کیفی است، استفاده شد. کدگذاری باز به معنای فرایند خرد کردن، بررسی، مقایسه، مفهوم‌پردازی و

[1] Content Validity Ratio

طبقه‌بندی است. در این شکل از کدگذاری فرضیه‌های مقدماتی درباره شیوه‌های ممکن مرتبط کردن کدها در ابعاد مشخص مطرح می‌شود؛ و درنتیجه داده‌های مشابه گروه‌بندی و نام‌گذاری می‌شوند (نوری و مهر محمدی، ۱۳۹۰). در این پژوهش کدگذاری داده‌ها با خواندن مکرر متن در داخل خطوط و پاراگراف و یافتن یک درک کلی آغازشده است سپس متون کلمه به کلمه خوانده شده است تا کدها استخراج شوند. کدگذاری با نوشتن کدها در حاشیه متن داده‌ها صورت گرفته است. این فرایند به‌طور پیوسته از استخراج کدها تا نام‌گذاری آن‌ها تداوم یافته است. در این مرحله، کدگذاری بدون هیچ‌گونه محدودیتی ازلحاظ تعداد کدها صورت گرفته است در مرحله دوم عمل کدگذاری برای روی کدهای استخراج‌شده صورت گرفت. در این مرحله محقق با در نظر گرفتن مفهوم هر یک از کدها، آن‌ها را در یک مفهوم مشابه دسته‌بندی کرد تا مفاهیم پژوهش شکل داده شود. درنهایت برای به دست آوردن تصویری بهتر از کدها، جدول دوبعدی طراحی شد که در یک بعد آن نویسنده /نویسندگان مقالات به همراه سال و در یک بعد کدهای استخراج‌شده، نوشته شده است. درواقع با این کار فراوانی کدها در مقالات منتخب مشخص شد.

جدول (۱) اطلاعات منابع کلیدی منتخب

کد مقاله	پژوهشگر/ (سال)	کد مقاله	پژوهشگر/ (سال)	کد مقاله	پژوهشگر/ (سال)	کد مقاله	پژوهشگر/ (سال)
۱	Andrade 2019	۲	Archibald 2014	۳	Bierman 2009	۴	Bolstad 2006
۵	Branscome 2007	۶	Buchler 2018	۷	Buchler 2016	۸	Champion 2014
۹	Cosenzo2007	۱۰	D’Amico2005	۱۱	Dyer2007	۱۲	Efklides 2008
۱۳	Etter 2000	۱۴	Fletcher& Wind 2014	۱۵	Fletcher 2006	۱۶	Fletcher2004
۱۷	Grier2012	۱۸	Jackson 2012	۱۹	Jøsok 2016	۲۰	Klieme2008
۲۱	Knox & Lug 2017	۲۲	Knox, Jøsok 2018	۲۳	Lafond 2012	۲۴	Lathrop 2016
۲۵	Maymir 2015	۲۶	Mgbere 2017	۲۷	Morrison 2012	۲۸	Murray 2016
۲۹	Nuijten 2020	۳۰	O’Neil 2014	۳۱	Pitagorsky 2017	۳۲	Rebecca A. Grier. 2012
۳۳	Røislien, H. E.	۳۴	Tapscott, D.	۳۵	Tversky	۳۶	Christian&

Griffiths.2019		1974		2014		2015	
Kounev 2015	۴۰	Camara 2017	۳۹	Pinon. 2014	۳۸	Zager 2017	۳۷
Banks, 2001	۴۴	Andrade, Torres, 2018	۴۳	Thompson & McCreary 2006	۴۲	Lewis 2016	۴۱
سیف ۱۳۸۸	۴۸	سالاری و دیگران، ۱۳۹۹	۴۷	خرازی و دیگران ۱۳۹۳	۴۶	Good, Yeganeh 2012	۴۵
نصیری و الیاسی ۱۳۹۷	۵۲	عزتی و همکاران، ۱۳۹۸	۵۱	هلیلی،۱۳۹۷	۵۰	مهدی‌نژاد نوری، ۱۳۹۸	۴۹

منابع انتخاب‌شده شامل مقالات مروری، مقالات علمی- پژوهشی، پایان‌نامه و کتاب است. درنهایت برای به دست آوردن تصویری بهتر از کدها، جدول دوبعدی طراحی شد که در یک بعد آن نویسنده / نویسندگان مقالات به همراه سال و در یک بعد کدهای استخراج‌شده، نوشته شد. درواقع با این کار تصویری از فراوانی کدها در مقالات منتخب به دست آمد. 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. هدف عمده کدگذاری محوری مقایسه مفاهیم با یکدیگر و یافتن محورهای مشترک است. درواقع مقوله‌ها از طریق فرایند تحلیل و مقایسه مفاهیم بر مبنای شباهت‌ها و تفاوت‌ها میان آن‌ها خلق شد. این مرحله که کدگذاری محوری نامیده می‌شود، محقق مقولات و مفاهیم به‌دست‌آمده را باهم مقایسه می‌کند، ترکیب و ادغام می‌کند کدگذاری محوری را می‌توان عمل مرتب کردن، درآمیختن و سازمان‌دهی انبوهی از داده‌ها تعریف کرد (فراست خواه، ۱۳۹۶: ۱۷۰). در این مرحله سعی شد مفاهیم با یکدیگر مقایسه شوند تا شباهت‌ها و تفاوت‌هایشان مشخص شود تا زمینه برای شکل‌گیری مقوله‌ها فراهم شود.

در این مرحله کدهای به‌دست‌آمده پس از دسته‌بندی و همگن‌سازی به جامعه خبرگان پژوهش ارائه گردید. سرانجام و پس از اعمال اصلاحات لازم، در مرحله بعد به روش کمی 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 انجام گردید. بدین منظور داده‌های مربوط به ۱۵۵ آزمودنی، جمع‌آوری و تحلیل داده‌های گردآوری‌شده از طریق نرم‌افزار اسمارت. پی. ال. اس[1] انجام گردید.

[1] Smart PLS

یافته‌های بخش کیفی

با استفاده از مرور نظام‌مند پیشینه 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. حاصل واکاوی و تحلیل محتوای متون منابع منتخب، استخراج مجموعه نسبتاً گسترده‌ای از مفاهیم پایه مرتبط با ابعاد و مؤلفه‌های آمادگی شناختی دفاع سایبری بود که از این میان، برخی مفاهیم کم ارتباط کنار گذاشته شدند و مفاهیمی که با یکدیگر اشتراک معنایی و مضمونی داشتند نیز با یکدیگر ادغام شدند. درنهایت با بازبینی و پالایش مکرر مفاهیم استخراج‌شده، به مجموعهٔ منسجمی از مفاهیم شامل تعداد ۳۴ مفهوم پایه تقلیل یافته و ارائه شد. در گام دوم، مفاهیم پایه منتخب، بر اساس تناسب و نزدیکی معنایی و محتوایی و مبتنی بر ادبیات و مبانی نظری پژوهش، ذیل عنوان زیرمؤلفه‌های شناختی زیست‌بوم دفاع سایبری دسته‌بندی و ارائه شدند. حاصل این اقدام، تعیین تعداد ۱۱ مؤلفهٔ آمادگی شناختی دفاع سایبری شامل: خودتنظیمی، حافظه، انعطاف‌پذیری، تصمیم‌گیری، تفکر انتقادی، معنابخشی، انطباق‌پذیری، فراشناخت، حل مسئله، خلاقیت و گشودگی شناختی است.

در گام سوم، ضمن تحلیل ماهیت مفهومی پدیدهٔ آمادگی شناختی دفاع سایبری و با عنایت به معنای مفهومی مؤلفه‌ها، ابعاد دارای اشتراک معنایی و محتوایی با استناد به مبانی نظری و ادبیات پژوهش با یکدیگر ترکیب و در طبقاتی انتزاعی‌تر و کلی‌تر با عنوان مؤلفه‌های اصلی آمادگی شناختی دفاع سایبری دسته‌بندی و ارائه شدند. حاصل این طبقه‌بندی معرفی تعداد ۲ بعد اصلی شامل: کارکردهای اجرایی اصلی شناختی و کارکردهای شناختی سطح بالا در الگوی آمادگی شناختی دفاع سایبری جایابی شدند. درنهایت نیز تعداد ۳۴ شاخص برای الگوی آمادگی شناختی دفاع سایبری ارتش جمهوری اسلامی ایران احصاء گردید.

جدول شماره (۲) مؤلفه‌ها، زیرمؤلفه‌ها و مفاهیم پایه شناختی زیست‌بوم دفاع سایبری

مقوله	مؤلفه	زیرمولفه	مفاهیم پایه	منابع (کد)
مؤلفه‌های آمادگی شناختی دفاع سایبری	کارکردهای اجرایی اصلی شناختی	خود تنظیمی	توانایی کنترل سطح هیجان	۲۴,۲۲,۲۱
			توانایی حفظ انگیزه	۲۴,۲۲,۲۱
			حفظ توجه متمرکز بر روی گزینه‌ها	۲۴,۲۲,۲۱
		حافظه	توانایی سازمان‌دهی مفاهیم در ذهن	۴۲,۳۵,۴۸,۴۶,۱,۱۷
			معنایابی و ارتباط‌دهی مفاهیم در ذهن	۴۶,۱,۱۷
			توانایی بازیابی مفاهیم از ذهن	۴۲,۳۵,۴۸,
		انعطاف‌پذیری	ایجاد راه‌حل‌های جایگزین متعدد	۴,۲۲,۲۱,۳,۱
			در جابه‌جایی بین وظایف و ایده‌ها	۲۲,۲۱,۳,۱

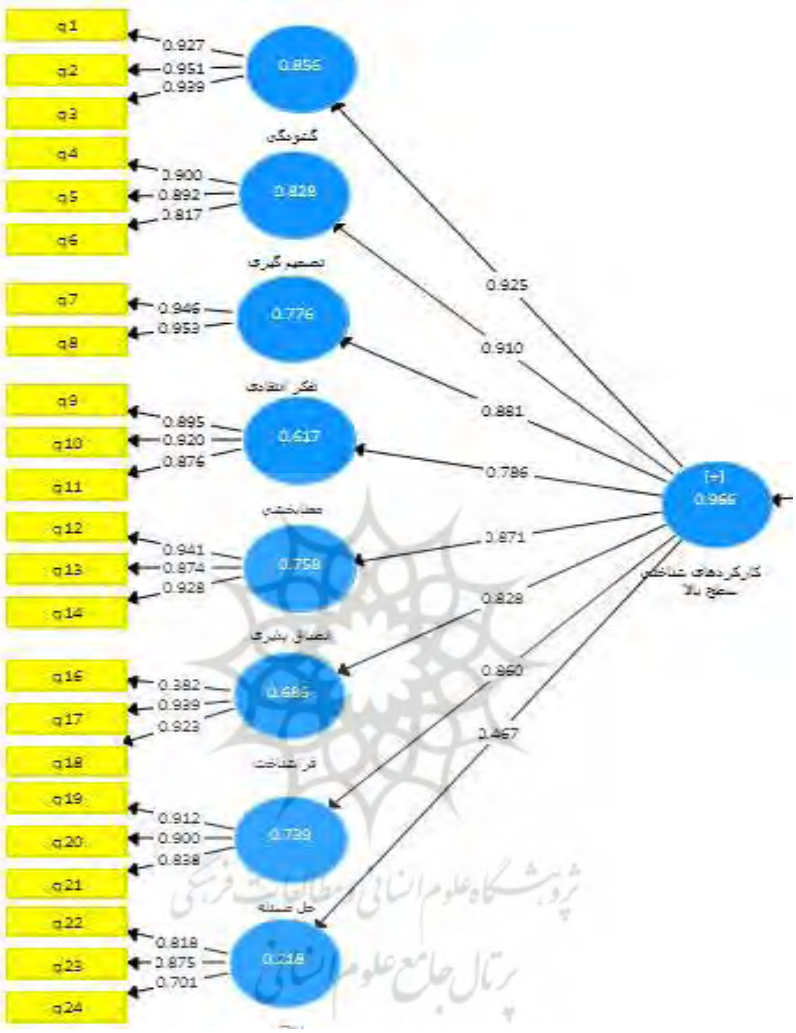
مقوله	مؤلفه	زیرمولفه	مفاهیم پایه	منابع (کد)
			غلبه بر پاسخ‌های خودکار یا پیش‌فرض	۲۱,۳,۱
		تصمیم‌گیری	تفکر شهودی و حس درونی	۱ و ۴۲ و ۲۳،۲۸
			کنترل خطاهای شناختی در قضاوت	,۱۱,۳۵
			پیش‌بینی پیامدهای رخدادها	۱۳,۴۳,۲۵,۱۱
		تفکر انتقادی	تطبیق دانش تخصصی با اقتضائات مسئله	۵۱ ,۲۸
			استفاده نوآورانه و هوشمندانه از امکانات	۵۱,۲۸
			ارائه روش‌های جدید	۵۱ ,۲۸
		معنابخشی	برقراری تعامل سازنده با محیط پیرامون	۲۴,۵۲ ,۳۱
			توانایی درک و تفسیر تجربیات	۵۲ ,۳۱
			ساخت مفاهیم ذهنی جدید از تجربیات	۲۴,۵۲
	کارکردهای شناختی سطح بالا	انطباق‌پذیری	سازگاری با شرایط محیطی	۴۴ ,۳۰
			یادگیری مداوم در موقعیت‌های متنوع	۴۴,۳۰
			تغییر در رفتار خود، متناسب با شرایط	۴۴,۳۰
		فراشناخت	نظارت و کنترل افکار خود	۱۲,۲۲,۲۱,۳۰,۴
			برنامه‌ریزی و تخصیص بهینه منابع	۲۴ ,۲۲,۲۱
			آگاهی از ماهیت، نوع و کیفیت وظایف	۲۱،۲۴,۳۰,۴
			کسب، حفظ و استفاده صحیح از دانسته‌ها	۲۲،۲۴,۲۱,۳۰
		حل مسئله	تجزیه‌وتحلیل پدیده‌ها و وقایع پیرامونی	۴۴،۲۳،۵۲،۳۰،۴،۳
			تولید و ارزیابی فرضیه درباره وقایع	۴۴,۵۲,۳۰,۴,۳
			تفسیر و قضاوت منطقی فرضیه‌ها	۵۲,۳۰,۴,۳
		خلاقیت	ارائه اندیشه‌های نو	۲۴,۴۴,۱۴
			حل خلاقانه مشکلات و مسائل پیش رو	۲۴,۴۴
		گشودگی شناختی	تمایل ذاتی به کسب دانش و تجربه بیشتر	۴۵،۲۳
			جذب و پذیرش ایده‌های بدیع و غیرمتعارف	۴۵،۲۴
			تخیل و تجسم در ارائه راه‌کارها	۲۳ ،۴۵،۲۴

یافته‌های بخش کمی

الگوی آمادگی شناختی دفاع سایبری یک مدل سلسله مراتبی است، بدین معنی که برای سنجش دقیق‌تر سازه اصلی آمادگی شناختی دفاع سایبری، دو سطح از سازه‌ها طراحی‌شده است. به‌منظور ارزیابی مدل، هر یک از مدل‌های اندازه به‌صورت جداگانه مورد ارزیابی قرار می‌گیرد.

در این تحقیق 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)[1] و واگرایی مدل (معیار فورنل و لارکر و معیار روایی یگانه – دوگانه) استفاده شده است.



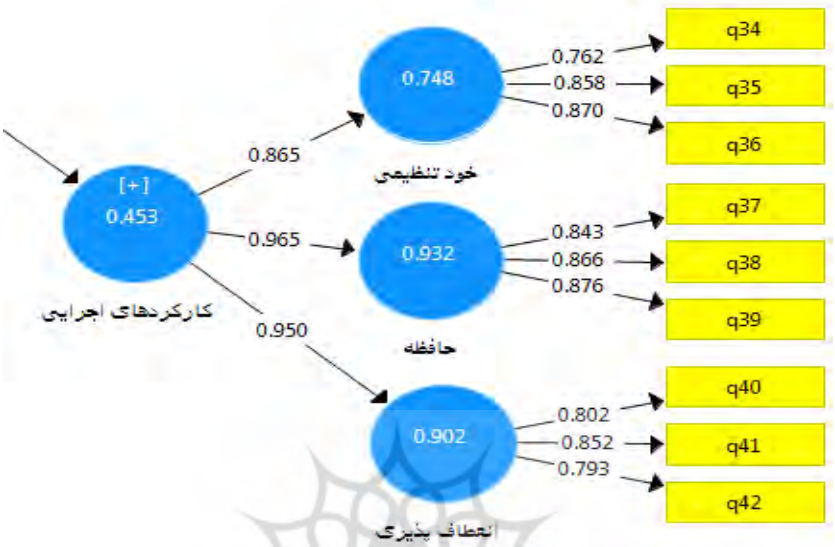
شکل (۱) ضرایب معناداری بارهای عاملی سازه و مؤلفه‌های کارکردهای شناختی سطح بالا

≠ برازش مدل‌های اندازه‌گیری

الف) ضرایب بارهای عاملی: 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

[1] Average Variance Extracted

است. میزان بار عاملی مؤلفه، سازه‌ها و شاخص‌ها بیشتر از مقدار قابل‌قبول ۰/۴ است. همچنین محاسبه ضرایب معناداری بارهای عاملی نشان می‌دهد که تمامی بارهای عاملی در سطح اطمینان ۹۵٪ معنادار است.



شکل (۲) ضرایب معناداری بارهای عاملی سازه و مؤلفه‌های کارکردهای اجرایی

ب) پایایی ترکیبی: پایایی ترکیبی مؤلفه و سازه‌ها بیشتر از مقدار ۰/۷ است که نشان‌دهنده پایایی ترکیبی مدل کارکردهای شناختی سطح بالا و کارکردهای اجرایی است.

≠ روایی همگرای مدل

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

≠ روایی واگرای مدل اندازه‌گیری

الف) 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 تائید کننده 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 کننده روایی همگرای مدل با معیار فورنل و لارکر است.

ب) روایی یگانه – دوگانه: مقادیر HTMT مربوط به سازه‌های مدل کارکردهای شناختی سطح بالا و کارکردهای اجرایی کمتر از مقدار ۰/۹ است که نشان‌دهنده روایی واگرای مدل است.

≠ **ارزیابی برازش مدل ساختاری**

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

الف) ضریب تعیین (R^2) : ضریب تعیین تمامی سازه‌ها و مؤلفه‌ها بیشتر از مقدار حداقلی ۰/۱۹ است.

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

ج) 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 ترسیم‌شده 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 نشان‌دهنده برازش قوی مدل است.

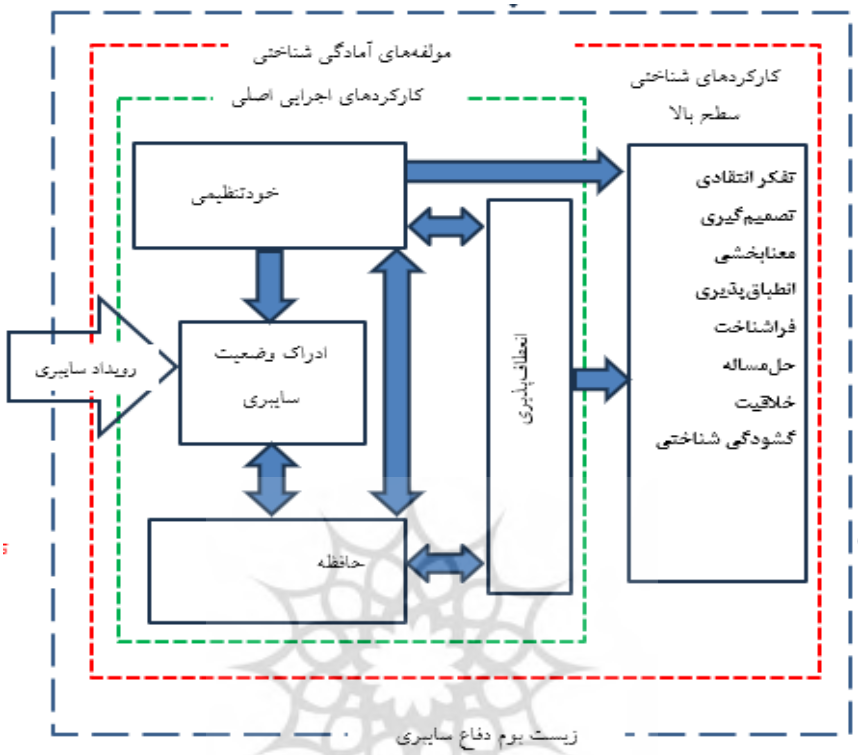
$$\mathbf{GOF} = \sqrt{0/733 \times 0/807} = 0/769$$

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

ج) شاخص تتای ریشه میانگین مربعات (RMS_theta) برای مدل، مقدار ۰/۱۱ محاسبه شد که با توجه به دامنه بحرانی کمتر از ۰/۱۲ نشان‌دهنده برازش مناسب مدل است. مبنای آن همبستگی بین متغیرهای خطا یا باقیمانده‌هاست. هر چه این همبستگی‌ها کوچک‌تر باشند شاخص RMS کوچک‌تر شده و مطلوب‌تر خواهد بود. کمترین مقدار و مناسب‌ترین مقدار شاخص RMS Theta صفر است.

[1] (SRMR) Standardized Root Mean Square Residual

شاخص برازش کلی مدل هم نشان می‌دهد که مدل کلی آمادگی شناختی دفاع سایبری از برازش قابل قبولی برخوردار است.



شکل (۳) مدل مفهومی آمادگی شناختی دفاع سایبری

مبنای یافته‌های این پژوهش مجموعه‌ای از مهارت‌ها و شایستگی‌های موردنیاز برای کارکنان دفاع سایبری در حوزه نظامی است که با عنوان مولفه‌های آمادگی شناختی دفاع سایبری نام‌گذاری شد. آمادگی شناختی در این پژوهش تأکید بر آمادگی ذهنی و مجموعه دانش، توانایی‌ها و مهارت‌هایی دارد که برای عملکرد مؤثر کارکنان دفاع سایبری در مواجهه با عوامل محیطی سایبری ضروری است. در این پژوهش آمادگی شناختی دفاع سایبری در دو حوزه کارکردهای شناختی سطح بالا و کارکردهای اصلی اجرایی با ۱۱ متغیر؛ حافظه، خودتنظیمی، انعطاف‌پذیری، تصمیم‌گیری، حل مسئله، گشودگی شناختی، فراشناخت، خلاقیت، انطباق‌پذیری، تفکر انتقادی و بررسی‌شده است. آمادگی شناختی در ادبیات پیشین پژوهش موردتوجه قرارگرفته است اما توجه به آن در دفاع سایبری به‌عنوان یک مفهوم جدید است که در این پژوهش شناسایی گردید. فرآیندهای شناختی در زیست‌بوم دفاع سایبری به کارکنان دفاع سایبری کمک می‌کند تا تعاملات خود را با محیط سایبری و دنیای درون هدایت،

برنامه‌ریزی، شروع، توقف، نظارت و اصلاح کنند. این مجموعه مانند یک تیم مدیریت یا «سیستم اجرایی» برای همه جنبه‌های شناخت و رفتار است. مهارت‌ها و شایستگی‌های شناختی کارکنان دفاع سایبری باعث انعطاف‌پذیری، هدفمندی و سازگاری آن‌ها در برابر عوامل محیطی سایبری می‌شود زیرا می‌تواند راهی برای تقویت تجربی عملکرد فردی کارکنان دفاع سایبری باشد.

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 می‌شوند که ازنظر کارایی می‌تواند شگفت‌انگیز باشد. بااین‌حال، در یک موقعیت بحرانی و غیرمنتظره، سوگیری[1] می‌تواند تفکر را محدود کند. برای دور زدن سوگیری، باید متفاوت فکر کرد که این امر مستلزم خودآگاهی و نحوه 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 در حوزه نظامی است که با عنوان آمادگی شناختی دفاع سایبری نام‌گذاری شد. آمادگی شناختی در این پژوهش تأکید بر آمادگی ذهنی و مجموعه دانش، توانایی‌ها و مهارت‌هایی دارد که برای عملکرد مؤثر کارکنان دفاع سایبری در مواجهه با عوامل محیطی سایبری ضروری است. در این پژوهش آمادگی شناختی دفاع سایبری در دو حوزه کارکردهای شناختی سطح بالا و کارکردهای اصلی اجرایی با ۱۱ متغیر؛ حافظه، خودتنظیمی، انعطاف‌پذیری، تصمیم‌گیری، حل مسئله، گشودگی شناختی، فراشناخت، خلاقیت، انطباق‌پذیری، تفکر انتقادی و بررسی‌شده است.

[1] Bias

فرآیندهای شناختی کارکردهای اجرایی در زیست‌بوم دفاع سایبری به کارکنان دفاع سایبری کمک می‌کند تا تعاملات خود را با محیط سایبری و دنیای درون هدایت، برنامه‌ریزی، شروع، توقف، نظارت و اصلاح کنند. 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 کاری، بازداری، انعطاف‌پذیری ذهنی، خودتنظیمی و همچنین شروع و نظارت بر عمل است (ریموند و همکاران، ۲۰۰۸). نتایج حاصل از بخش کیفی پژوهش کارکردهای اجرایی اصلی شناختی در سه مؤلفه خودتنظیمی (فرآیندهایی که ما را قادر می‌سازد سطوح بهینه برانگیختگی عاطفی، انگیزشی و شناختی را حفظ کنیم)، حافظه کاری (توانایی نگه‌داشتن اطلاعات در ذهن و کار ذهنی با آن است یا به‌عبارت‌دیگر، کار با اطلاعاتی که دیگر ازنظر ادراکی وجود ندارد) و انعطاف‌پذیری (توانایی تغییر دیدگاه‌ها یا رویکردها به یک مشکل، سازگاری انعطاف‌پذیر با خواسته‌ها، قوانین یا اولویت‌های جدید، جابه‌جایی بین وظایف و ایده‌ها بدون از دست دادن بینش نسبت به آنچه فکر می‌کنیم) موردتوجه قرارگرفته است. مهارت‌ها و شایستگی‌های کارکردهای اجرایی شناختی کارکنان دفاع سایبری باعث انعطاف‌پذیری، هدفمندی و سازگاری آن‌ها در برابر عوامل محیطی سایبری می‌شود. آن‌ها همواره درگیر موقعیت‌های پیچیده، پر ابهام، بدیع و چالش‌برانگیز هستند و این کارکردهای شناختی اصلی به آن‌ها کمک می‌کنند تا با استخراج «منابع» اضافی از یادگیری و حافظه قبلی، کارکردهای اجرایی درجه بالاتری (تصمیم‌گیری، حل مسئله، استدلال و ...) را ایجاد نمایند.

کارکردهای شناختی سطح بالا در هشت مؤلفه تصمیم‌گیری (توانایی بررسی برنامه‌های مختلف اقدام، ارزیابی تأثیر احتمالی هر یک، انتخاب یکی و تخصیص منابع برای آن.)، تفکر انتقادی (توانایی تطبیق دانش تخصصی با اقتضائات مسئله و استفاده نوآورانه و هوشمندانه از امکانات)، معنابخشی (برقراری تعامل سازنده با محیط پیرامون، درک و تفسیر تجربیات و ایجاد مفاهیم ذهنی جدید)، انطباق‌پذیری (توانایی تغییر کارکردی (شناختی، رفتاری و یا عاطفی) در پاسخ به تغییرات واقعی یا به‌درستی پیش‌بینی‌شده در شرایط احتمالی محیطی)، فراشناخت (توانایی نظارت، ارزیابی، تنظیم و تقویت فرایندهای شناختی شخص)، حل مسئله (توانایی تجزیه‌وتحلیل وضعیت فعلی، درک اهداف و ایجاد راهکار برای دستیابی به آن‌ها)، خلاقیت (توانایی ایجاد نظرات و راه‌حل‌هایی است که جدید، مناسب و باکیفیت) و گشودگی شناختی (تمایل ذاتی به کسب دانش و تجربه بیشتر و جذب و پذیرش ایده‌های بدیع و غیرمتعارف) موردبررسی قرار گرفته است. شاخص‌های برازش حاصل از تحلیل مسیر نیز نشان داد که داده‌های این پژوهش با

ساختار عاملی کارکردهای شناختی سطح بالا در آمادگی شناختی دفاع سایبری برازش مناسبی دارد. برابر متن پژوهش‌های پیشین نیز مؤید این نتایج هستند.

پیشنهادها

در این تحقیق سعی شد به‌صورت توأمان به هر دو مقوله آمادگی شناختی و سایبری با رویکرد زیست‌بومی و به‌طور هم‌زمان، نقش عوامل محیطی، فناوری‌ها و فناوری‌های سایبری و شناختی موردمطالعه قرار گیرد. باوجوداین، تعداد زیاد عوامل تشکیل‌دهنده نظام آمادگی شناختی دفاع سایبری مانع از آن شد که همه 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 تشکیل‌دهنده 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:

۱) مطالعه گسترده‌تر مؤلفه‌های شناختی تأثیرگذار بر فرایند دفاع سایبری در حوزه نظامی.
۲) مطالعه در خصوص تهیه اطلس شایستگی‌های شناختی کارکنان دفاع سایبری در سطوح مختلف فنی، تاکتیکی، عملیاتی و راهبردی
۳) دانشگاه‌های وابسته به نیروهای مسلح، ارائه راهبردها و برنامه‌های حفظ و ارتقاء آمادگی سایبری نیروهای مسلح را بر اساس نظام ارائه‌شده در این پژوهش را در دستور کار خود قرار دهند.

قدردانی

از تمامی عزیزانی که همکاری لازم را در انجام این پژوهش داشتند، تشکر و قدردانی می‌گردد.

منابع

≠ خرازی، کمال و تلخابی، محمود (۱۳۹۳). *مبانی آموزش‌وپرورش شناختی*، تهران: انتشارات سمت.

≠ 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، بوگر اسحاق و طالع پسند، سیاوش (۱۳۹۶). اثربخشی آموزش آمادگی شناختی بر مهارت تصمیم‌گیری و عملکرد تیراندازی با اثر تعدیل‌کنندگی اضطراب حالتی - رقابتی. *فصلنامه طب انتظامی ۷.*

≠ 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

≠ Bennis, Warren; Nanus, Burt. (1985). Leaders: Strategies for Taking Charge Biases and heuristics in strategic decision-making. *Journal of Business Venturing 12: 9*

≠ 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 Enginnering 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

≠ Cosenzo, K. A. Fatkin, L. T. & Patton, D. J (2007). Ready or not: Enhancing operational effectiveness through use of readiness measures. *Aviation, Space, and Environmental Medicine.* 78(5), B96–B106

≠ 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

≠ Etter, D. M. Foster, R. E. & Steele, T. P (2000). Cognitive readiness and advanced distributed learning. Crosstalk. *The Journal of Defense Software Engineering*, 13, 5-

≠ 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

≠ FM3-38, Cyber Electromagnetic Activities (2014). Headquarters Department of the Army Washington, DC, 12 February 2014

≠ 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. https://www.bing.com/ck/a

≠ 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. https://doi.org/10.1177/0956797611423545

≠ 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).*

≠ Klieme, Hartig, and Rauch (2008). The Concept of Competence in Educational Contexts, *Zeitschrift für Psychologie / Journal of Psychology*, 216, 60–72.

≠ 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.* doi: 10. 1080/08995605.2018.1478546

≠ 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 onHCI International 2017, (Cham: Springer International Publishing*), 330–338. doi: 10.1007/978-3-319-58750-9_46

≠ 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 battle against cybercrime.

≠ NATO (2016a). Cyber Defence Pledge. *Brussels: NATO*.

≠ NATO (2016b). Warsaw Summit Communiqué. *Brussels: NATO*.

≠ NOBLES, Calvin (2018). Botching Human Factors in Cybersecurity in Business Organizations, HOLISTICA 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, https://doi.org/10.1016/j.acn.2007.08.010

≠ 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

≠ 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*