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

Cognitive Threats to Intelligence Organizations in the Cognitive War Paradigm (Case Study of a Military Intelligence Organization)

Hassan Mahjoub[1]✉ | **Morteza Talebi** [2] | **Saeed Shakouri** [3]

Associate Professor of Higher Education, Shahid Satari University, Tehran, Iran.Email: hassanmahjub@ut.ac.ir

Assistant Professor of Strategic Management, IRI Military Command and Staff University, Tehran, Iran. Email: m.talebi@casu.ac.ir

Researcher in the Field of Cognitive Sciences . I.R.I Military command and staff university.Tehran, Iran. Email: saeed.shakori@mail.um.ac.ir

Article Info

Article type:
Research Article

Article history:
Received:
2025-7-15
Received in revised form:
2026-2-1
Accepted:
2026-2-2
Published onlin:
2026-5-22

Keywords:
Cognitive threat, intelligence organization, process, technology, and cognitive security

ABSTRACT

Background and Objective: This research was conducted with the aim of identifying and analyzing cognitive threats in a military intelligence organization and designing effective mechanisms to counter these threats.

Methods: The research method is qualitative content analysis. For data collection, a standard open-ended questionnaire designed by the research team was used. The participants were 11 serving commanders and intelligence officers. The collected data were analyzed using the three-stage coding model of Strauss and Corbin.

Findings: The findings indicate that the studied organization faces cognitive threats at three levels: individual level (cognitive biases, impulsive decision-making style, weak cognitive resilience, cognitive fatigue, weak team cognition, etc.), technology-driven cognitive threats (cognitive assessment and monitoring technologies, cognitive intervention and control technologies, simulation and artificial intelligence technologies, metadata and big data analysis technologies), and process-driven cognitive threats (anti-creativity organizational culture, information overload, lack of timely access to information, work pressure, deceptive information, traditional intelligence methods, etc).

Conclusion: Cognitive intelligence operations are not possible without organizational cognitive development, cognitive empowerment, training and skill development, and capability-building collaboration and interaction.

Cite this article: MAHJUB,H , Talebi,M and Shakori,S . (2026). Cognitive Threats to Intelligence Organizations in the Cognitive War Paradigm (Case Study of a Military Intelligence Organization). (e735732). *Defensive Future Studies*, *11*(40), 289-324.

DOI: https://doi.org/10.22034/dfsr.2026.2065922.1922

Publisher: IRI Military Command and Staff University

Extended Abstract

Introduction

The evolving character of contemporary warfare has increasingly shifted from conventional kinetic engagements toward non-kinetic, multidimensional, and cognitively driven forms of conflict. Within this transformation, cognitive threats have emerged as a critical component of hybrid warfare, targeting the cognitive processes of individuals, organizations, and societies. Unlike traditional military threats, cognitive threats aim to influence perception, interpretation, judgment, and decision-making through information manipulation, psychological pressure, and technologically mediated influence. As a result, the cognitive domain has become a decisive arena in national security and defense. In defense and cybersecurity environments, cognitive threats are amplified by the rapid expansion of digital platforms, algorithmic information flows, and data-driven decision-making systems. These developments have increased both the scale and sophistication of influence operations, disinformation campaigns, and psychological manipulation. Consequently, military and security institutions are increasingly exposed to cognitive vulnerabilities that can undermine strategic judgment, operational effectiveness, and organizational resilience. This study addresses this emerging challenge by examining cognitive threats within the broader paradigm of cognitive warfare and by conceptualizing an integrated framework of cognitive readiness as a foundational element of effective cognitive defense.

Methodology

The study employs a qualitative, descriptive–analytical research design grounded in an interdisciplinary approach. Data were collected through a systematic review of academic literature, strategic doctrines, policy documents, and authoritative national and international reports related to cognitive warfare, hybrid threats, cyber defense, and cognitive security. Particular attention was given to defense-oriented studies and empirical research addressing cognitive vulnerabilities in military and security organizations.

The analytical process was conducted through thematic and conceptual analysis, allowing for the identification and categorization of recurring patterns, dimensions, and mechanisms of cognitive threats. Comparative

analysis was also applied to examine how cognitive threats manifest across military, cyber, and information domains. This methodological approach enables both theoretical integration and contextual adaptation, facilitating the development of a comprehensive and operationally relevant understanding of cognitive readiness within defense systems.

RESULT

The findings reveal that cognitive threats operate through a complex interaction of informational, psychological, technological, and organizational mechanisms. These threats exploit cognitive biases, information overload, uncertainty, and emotional stimuli to distort perception and weaken analytical judgment. In cyber-enabled environments, cognitive threats are further intensified through algorithmic amplification, rapid dissemination of disinformation, and the blending of authentic and deceptive data. The study identifies cognitive readiness as a multidimensional construct encompassing individual cognitive capacities, organizational processes, technological infrastructures, and strategic culture. Key components of cognitive readiness include cognitive literacy, critical thinking skills, resilience to psychological pressure, effective information filtering mechanisms, and adaptive decision-support systems. The findings also emphasize that cognitive threats do not act in isolation; rather, they form feedback loops that reinforce cognitive fatigue, misperception, and decision-making errors at both individual and institutional levels.

DISCUSSION and CONCLUSIONS

The discussion highlights the limitations of traditional defense paradigms in addressing cognitively driven threats. Conventional security approaches, primarily focused on physical assets and kinetic capabilities, fail to capture the subtle, persistent, and cumulative nature of cognitive influence operations. Cognitive threats are characterized by ambiguity, deniability, and long-term impact, making them particularly challenging to detect and counter. From a strategic perspective, cognitive defense should be understood as an ecosystem rather than a discrete capability. This ecosystem integrates human cognition, organizational design, technological tools, and policy frameworks into a coherent defensive architecture. The study argues that cognitive readiness enhances not only

operational effectiveness but also strategic adaptability and institutional learning. Furthermore, the integration of cognitive defense within cyber defense strategies is essential, as cyberspace has become the primary conduit for cognitive influence and manipulation. This study underscores the growing strategic significance of cognitive threats in contemporary security environments and highlights the necessity of developing comprehensive cognitive defense frameworks. By conceptualizing cognitive readiness as a foundational element of cognitive defense, the research contributes to both theoretical advancement and practical policy formulation. Strengthening cognitive readiness enables defense and security institutions to anticipate, absorb, and respond effectively to cognitively driven threats. In conclusion, cognitive defense should be regarded as a long-term, adaptive process that requires sustained investment in human capital, organizational reform, and technological innovation. Future research should focus on operationalizing cognitive readiness indicators, developing assessment metrics, and examining the dual role of emerging technologies as both enablers of cognitive threats and tools for cognitive resilience.

REFERENCES

Buchanan, V. & Cooke, N. J. (2015). The cognitive science of intelligence analysis. *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting*, 826–830. (https://doi.org/10.1177/1541931215591179)

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

تهدیدات شناختی سازمان‌های اطلاعاتی در پارادایم شناختی جنگ (مطالعه موردی یک سازمان اطلاعاتی نظامی)

حسن محجوب [۱] ✉ | مرتضی طالبی [۲] | سعید شکوری [۳] |

۱. استادیار مدیریت آموزش عالی، دانشگاه هوایی شهید ستاری، تهران، ایران. ایمیل hassanmahjub@ut.ac.ir
۲. استادیار مدیریت راهبردی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. ایمیل: m.talebi@casu.ac.ir
۳. پژوهشگر حوزه علوم شناختی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. محقق حوزه علوم شناختی saeed.shakori@mail.um.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله
تاریخ دریافت:
۱۴۰۴/۰۴/۲۴
تاریخ بازنگری:
۱۴۰۴/۱۱/۱۲
تاریخ پذیرش:
۱۴۰۴/۱۱/۱۳
تاریخ انتشار:
۱۴۰۵/۰۳/۰۱

کلیدواژه‌ها:
تهدید شناختی، سازمان اطلاعاتی، فرایند، فناوری، امنیت شناختی

چکیده

زمینه و هدف: این پژوهش با هدف شناسایی و تحلیل تهدیدات شناختی در یک سازمان اطلاعاتی نظامی و طراحی سازوکارهای مقابله اثربخش با این تهدیدات، انجام شده است.

روش‌ها: روش انجام پژوهش، تحلیل محتوای کیفی است. به‌منظور گردآوری داده‌ها، از پرسشنامه باز پاسخ استاندارد که توسط تیم تحقیقاتی طراحی گردیده استفاده شده است. مشارکت‌کنندگان ۱۱ تن از فرماندهان و افسران اطلاعاتی مشغول به خدمت بودند. داده‌های گردآوری‌شده با استفاده از الگوی کدگذاری سه مرحله‌ای اشتراوس و کوربین مورد تحلیل قرار گرفت.

یافته‌ها: یافته‌ها نشان می‌دهد سازمان موردمطالعه با تهدیدات شناختی در سه سطح فردی (سوگیری‌های شناختی، سبک تصمیم‌گیری تکانشی، تاب‌آوری شناختی ضعیف، خستگی شناختی، شناخت تیمی ضعیف و غیره)، تهدیدات شناختی فناوری محور (فناوری‌های ارزیابی و نظارت شناختی، فناوری‌های مداخله و کنترل شناختی، فناوری‌های شبیه‌سازی و هوش مصنوعی، فناوری‌های تحلیل فرادادهها و کلان داده‌ها)، تهدیدات شناختی فرایندمحور (فرهنگ‌سازمانی ضد خلاقیت، اضافه‌بار اطلاعاتی، عدم دسترسی به‌موقع به اطلاعات، فشار کاری، اطلاعات فریب‌دهنده، روش‌های سنتی اطلاعاتی و غیره) مواجه است.

نتیجه‌گیری: عملیات اطلاعاتی شناختی بدون توسعه شناختی سازمان، توانمندسازی شناختی، آموزش و مهارت‌آموزی، همکاری و تعامل قابلیت‌ساز امکان‌پذیر نیست.

استناد: محجوب، حسن؛ طالبی، مرتضی؛ شکوری، سعید. (۱۴۰۵). تهدیدات شناختی سازمان‌های اطلاعات در پارادایم شناختی جنگ (مطالعه موردی: یک سازمان اطلاعاتی نظامی). آینده‌پژوهی دفاعی، ۱۱(۴۰)، ۳۲۴-۲۸۹.
DOI: https://doi.org/10.22034/dfsr.2026.2065922.1922

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

تحولات شتابان در فناوری‌های نوین، به‌ویژه در حوزه‌های هوش مصنوعی، علوم شناختی، سامانه‌های داده‌محور و شبکه‌های پیچیده ارتباطی، منطق سنتی جنگ و امنیت را با چالش‌های بنیادین مواجه ساخته است. این تحولات نه‌تنها ابزارها و روش‌های نبرد، بلکه شیوه فهم، تفسیر و تصمیم‌گیری درباره جنگ را دگرگون کرده‌اند. در چنین بستری، مفهوم «پارادایم شناختی جنگ» به‌مثابه چارچوبی نوین برای تبیین ماهیت منازعات معاصر مطرح می‌شود؛ پارادایمی که در آن، شناخت انسان و ماشین به کانون اصلی رقابت راهبردی تبدیل شده است.

در چارچوب نظری توماس کوهن، پارادایم‌ها مجموعه‌ای از مفروضات، زبان مفهومی، مسائل مشروع و روش‌های حل مسئله‌اند که فهم یک حوزه علمی یا عملی را سامان می‌دهند. از منظر کوهن، زمانی که ناهنجاری‌های انباشته‌شده دیگر در چارچوب پارادایم مسلط قابل توضیح نباشند، یک «انقلاب پارادایمی» رخ می‌دهد و چارچوبی نو جایگزین می‌شود. این منطق، صرفاً به علوم طبیعی محدود نیست، بلکه در حوزه‌های اجتماعی و نظامی نیز کاربرد دارد. در عرصه جنگ، ناتوانی پارادایم‌های صنعتی و حتی اطلاعاتی در تبیین پدیده‌هایی چون غلبه بازیگران کوچک، اثرگذاری عملیات غیرسینتیکی، فروپاشی بازدارندگی کلاسیک و نقش تعیین‌کننده ادراک و روایت، نشانه‌های آشکار یک بحران پارادایمی است.

پارادایم صنعتی جنگ، بر انهدام فیزیکی، جرم نیرو و توان آتش استوار بود. با گذار به پارادایم اطلاعاتی، دسترسی به داده و برتری اطلاعاتی به عامل کلیدی قدرت تبدیل شد. بااین‌حال، پارادایم شناختی جنگ یک گام بنیادین فراتر می‌رود: در این چارچوب، داده و اطلاعات تنها مواد خام‌اند و ارزش راهبردی واقعی در توان پردازش، تفسیر و تصمیم‌گیری نهفته است. به‌بیان‌دیگر، «سلاح» دیگر صرفاً سخت‌افزار نظامی نیست، بلکه شامل الگوریتم‌ها، مدل‌های شناختی، معماری‌های انسان–ماشین و اکوسیستم‌های تصمیم‌یار می‌شود.

در پارادایم شناختی، هر عرصه نبرد (زمین، دریا، هوا، فضا و سایبر) به‌طور هم‌زمان دارای سه بعد فیزیکی، اطلاعاتی و شناختی است. بعد شناختی، لایه‌ای فراگیر و مسلط است که ادراک، معنا، هیجان، قضاوت و اراده کنشگران (نظامی و غیرنظامی، انسانی و

غیرانسانی) را شکل می‌دهد. از این منظر، جنگ شناختی صرفاً به معنای عملیات روانی یا جنگ اطلاعاتی پیشرفته نیست، بلکه به مجموعه‌ای از اقدامات نظام‌مند اطلاق می‌شود که هدف آن‌ها ایجاد، تغییر یا تخریب الگوهای ادراک و تصمیم‌گیری دشمن و هم‌زمان، حفاظت و تقویت تاب‌آوری شناختی خودی است.

پیشرفت‌های علوم شناختی، به‌ویژه در حوزه سوگیری‌های شناختی، پردازش دوگانه ذهن، بار شناختی و تصمیم‌گیری در شرایط عدم قطعیت، بنیان نظری این پارادایم را تقویت کرده‌اند. نظریه پردازش دوگانه دانیل کانمن (تمایز میان تفکر سریع، شهودی و مبتنی بر سوگیری و تفکر کند، تحلیلی و پرهزینه) نشان می‌دهد که بخش قابل‌توجهی از تصمیم‌های انسانی در شرایط فشار، ابهام و زمان محدود، مستعد خطای سیستمی هستند. پارادایم شناختی جنگ دقیقاً بر بهره‌برداری هدفمند از این آسیب‌پذیری‌های شناختی استوار است؛ آسیب‌پذیری‌هایی که با تحلیل کلان‌داده‌های رفتاری و بهره‌گیری از هوش مصنوعی، قابل‌شناسایی، پیش‌بینی و دست‌کاری می‌شوند.

در این چارچوب، هدف راهبردی دیگر صرفاً انهدام توان رزمی دشمن نیست، بلکه اختلال در چرخه‌های ادراک و تصمیم‌گیری اوست. فشرده‌سازی چرخه OODA(مشاهده، جهت‌یابی، تصمیم، اقدام) برای خودی و هم‌زمان، تحمیل تأخیر، اغتشاش و خطای شناختی به دشمن، به مرکز ثقل رقابت بدل می‌شود. برتری راهبردی نه در سرعت شلیک، بلکه در سرعت معناسازی و تصمیم‌سازی تعریف می‌گردد.

پارادایم شناختی جنگ همچنین ماهیتی ذاتاً اکوسیستمی دارد. این پارادایم حاصل برهم‌کنش هم‌زمان فناوری‌های دیجیتال، سامانه‌های هوشمند، رسانه‌ها، ساختارهای اجتماعی، فرهنگ، هویت و نهادهای حکمرانی است. در چنین اکوسیستمی، بازیگران دولتی و غیردولتی، انسانی و ماشینی، از طریق شبکه‌های چندلایه و حلقه‌های بازخورد تطبیقی به یکدیگر متصل‌اند. پیامد این وضعیت، افزایش پیچیدگی، عدم قطعیت و غیرخطی بودن منازعات است؛ وضعیتی که رویکردهای سنتی، خطی و سلاح‌محور قادر به مدیریت آن نیستند.

در سطح راهبردی، پارادایم شناختی جنگ منطق بازدارندگی را نیز بازتعریف می‌کند. بازدارندگی دیگر صرفاً مبتنی بر تهدید به نابودی فیزیکی نیست، بلکه شامل بازدارندگی شناختی می‌شود؛ یعنی توان یک نظام سیاسی- اجتماعی برای حفظ انسجام ادراکی،

اعتماد عمومی و ثبات تصمیم‌گیری در برابر عملیات دست‌کاری شناختی. ازاین‌رو، مفاهیمی چون «امنیت شناختی» و «تاب‌آوری شناختی» به‌تدریج در کنار امنیت سایبری و فیزیکی مطرح می‌شوند.

در نهایت، پارادایم شناختی جنگ یک تحول تدریجی اما عمیق کوهنی است که نه‌تنها ابزارها و تاکتیک‌ها، بلکه دکترین‌ها، ساختار نیروها، نظام آموزش، حکمرانی دفاعی و چارچوب‌های حقوقی و اخلاقی را دستخوش بازاندیشی می‌سازد. این پارادایم نشان می‌دهد که در منازعات آینده، پیروزی بیش از آنکه حاصل انهدام دشمن باشد، نتیجه برتری در فهم، تفسیر و هدایت ذهن‌ها خواهد بود.

مرور مطالعات داخلی و خارجی نشان می‌دهد که بیشتر پژوهش‌های پیشین صرفاً به «تعریف نظری جنگ شناختی» یا «تحلیل فناوری‌های شناختی» پرداخته‌اند و کمتر به تبیین اثرات تهدیدات شناختی بر سازمان‌های اطلاعاتی نظامی توجه کرده‌اند. به‌ویژه در سطح ملی، پژوهش‌های اندکی به تحلیل سطوح سه‌گانه تهدیدات شناختی (فردی، فناورانه، فرایندی) و پیامدهای آن‌ها بر عملکرد سازمان‌های اطلاعاتی پرداخته‌اند. این شکاف علمی، ضرورت انجام پژوهشی را نشان می‌دهد که با رویکردی نظام‌مند و مبتنی بر تحلیل محتوای کیفی، به شناسایی مؤلفه‌ها و الگوهای تهدید شناختی در یک سازمان اطلاعاتی نظامی بپردازد.

با توجه به موارد بالا «شناسایی و تحلیل تهدیدات شناختی مؤثر بر عملکرد سازمان‌های اطلاعاتی (موردمطالعه یک سازمان اطلاعاتی نظامی) به‌منظور طراحی معماری شناختی مقابله اثربخش با آن‌ها» به‌عنوان هدف اصلی و؛

۱. شناسایی ابعاد و مؤلفه‌های تهدیدات شناختی فردمحور؛
۲. تبیین تهدیدات شناختی فناوری‌محور در فرایندهای اطلاعاتی؛
۳. تحلیل تهدیدات شناختی فرایندمحور در ساختار و عملکرد سازمان اطلاعاتی؛
٤. بررسی نقش متقابل این سه سطح تهدید بر کارکرد کلی سازمان اطلاعاتی

به‌عنوان اهداف فرعی پژوهش هستند.

مبانی نظری و پیشینه تحقیق

تحلیل اطلاعاتی در سازمان‌های امنیتی و دفاعی مدرن، فراتر از جمع‌آوری صرف داده، به‌عنوان نوعی شناخت مرتبه بالا[1] تعریف می‌شود که از عملکردهای اجرایی دولت نظیر برنامه‌ریزی، تصمیم‌گیری و سیاست‌گذاری پشتیبانی می‌کند (ماندل و ایروین[2]،۲۰۲۴). مک‌نیس و همکاران[3] (۲۰۱۵) معتقدند که این فرآیند بر لبه «پهنای باند شناختی» تحلیل‌گران حرکت می‌کند. پژوهش‌های مبتنی بر تحلیل وظایف شناختی[4] نشان می‌دهند که محیط کار تحلیل‌گران با سه چالش بنیادین روبروست: فشار زمان خردکننده، حجم عظیم و متناقض داده‌ها و ضرورت قضاوت‌های دشوار انسانی درباره اعتبار و اطمینان به منابع (هاچینز[5] و همکاران،۲۰۰۷). به باور هاچینز و همکاران (۲۰۰۷)، قضاوت در مورد وزن‌دهی به قطعات داده در شرایطی که «فریب» یک اصل در داده‌های دشمن است، تحلیل را به یکی از دشوارترین فعالیت‌های ذهنی تبدیل می‌کند.

در نیم قرن گذشته، پارادایم غالب برای بهبود کیفیت تحلیل بر کاهش سوگیری‌های شناختی از طریق تکنیک‌های تحلیلی ساختاریافته[6] استوار بوده است (ماندل و ایروین،۲۰۲۴). تکنیک‌هایی نظیر تحلیل فرضیات رقیب[7] با هدف برون‌سپاری فرآیند استدلال از ذهن به فرم‌های خارجی (مانند ماتریس‌ها) طراحی شدند تا از سوگیری تائید جلوگیری کنند (ماندل و ایروین،۲۰۲۴). بااین‌حال، مطالعات اخیر شکاف‌های جدی در این رویکرد شناسایی کرده‌اند. ماندل و ایروین (۲۰۲۴) با نقد این تکنیک‌ها بیان می‌کنند که تکنیک‌های تحلیلی ساختاریافته اغلب پدیده «نوفه[8]» یا تنوع تصادفی در قضاوت‌ها را نادیده می‌گیرند و ممکن است به‌جای کاهش سوگیری، با تجزیه مراحل تحلیل، پتانسیل تولید خطا را افزایش دهند. کائونونن[9] (۲۰۱۹) نیز در مطالعه میدانی خود در

1 -Higher-order cognition
2 -Mandel & Irwin
3 -McNeese
4 -Cognitive Task Analysis (CTA)
5 -Hutchins
6 -Structured Analytical Techniques (SATs)
7 -Analysis Competing Hypotheses (ACH)
8 -Noise
9 -Kaunonen

سطح تاکتیکی نیروی زمینی دریافت که تحلیل‌گران حتی هنگام استفاده از این تکنیک‌ها، آن‌ها را در سطحی بسیار ابتدایی و صرفاً برای اثبات فرضیات قبلی خود به کار می‌برند که نشان‌دهنده ناکارآمدی آموزش‌های سنتی است. شناسایی سوگیری‌های غالب در محیط‌های عملیاتی مطالعات تجربی و آزمایش‌های شبیه‌سازی‌شده، تصویری دقیق از سوگیری‌هایی که منجر به شکست اطلاعاتی می‌شوند ارائه می‌دهند. کائونون (۲۰۱۹) در پژوهش خود، سوگیری تائید[1] و تفکر گروهی را به‌عنوان شایع‌ترین خطاها در تیم‌های تحلیلی شناسایی کرد. علاوه بر این، سوگیری‌هایی نظیر تصویرسازی آینه‌ای[2] (فرض بر اینکه دشمن طبق منطق ما عمل می‌کند) و اثر لنگر انداختن[3] (اتکای بیش‌ازحد به اولین اطلاعات دریافتی) به‌طور مکرر در فرآیندهای تحلیلی مشاهده‌شده‌اند که منجر به نادیده گرفتن شواهد متناقض و برآوردهای غلط از نیات دشمن می‌شود (هاچینز و همکاران،۲۰۰۷؛ کائونون، ۲۰۱۹).

برخلاف این تصور که ابزارهای مدرن فناوری اطلاعات باعث حذف سوگیری می‌شوند، زاناسی و روینی[4] (۲۰۱۸) استدلال می‌کنند که این ابزارها می‌توانند منجر به سوگیری‌های القایی توسط فناوری اطلاعات شوند (زاناسی و روینی،۲۰۱۸). همچنین، ابهام در واژگان در نرم‌افزارهای استخراج متن[5] می‌تواند منجر به خطاهای تفسیری و دسته‌بندی غلط اسناد شود.

بهینه‌سازی و ارتقای انسانی ادبیات اخیر پژوهش در حال عبور از رویکردهای صرفاً آموزشی به سمت متدهای پیشرفته‌تر است. زاناسی و روینی (۲۰۱۸) استفاده از بازی‌های جدی[6] نظیر پروژه‌های «لیلا» و «سیریوس[7]» را به‌عنوان راهکاری نوین برای آموزش تحلیل‌گران در محیطی بدون ریسک جهت شناسایی و مدیریت سوگیری‌های ناخودآگاه پیشنهاد می‌دهند. در مقابل، ماندل و ایروین (۲۰۲۴) دو مسیر جدید را معرفی می‌کنند؛

1 -Confirmation Bias
2 -Mirror Imaging
3 -Anchoring Effect
4 -Zanasi & Ruini
5 -Text Mining
6 -Serious Games
7 -LEILA & Sirius

بهینه‌سازی آماری:[1] استفاده از روش‌های ریاضی پساتحلیلی مانند کالیبراسیون مجدد و تجمیع وزنی قضاوت‌ها بر اساس عملکرد گذشته تحلیل‌گران. به‌طورکلی 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 (طالبی و محجوب، ۱۴۰۳).

ارتقای توانمندی‌های انسانی[2]: بهینه‌سازی شناخت از طریق علوم زیستی، شامل مدیریت علمی خواب، ورزش، تغذیه و استفاده از ترکیبات نوتروپیک برای تقویت حافظه و تمرکز تحلیل‌گران در مواجهه با حجم عظیم داده‌ها. در نهایت، مک‌نیس و همکاران (۲۰۱۵) بر ضرورت استفاده از رویکرد «آزمایشگاه زنده»[3] تأکید دارند که در آن شناخت تحلیل‌گر در محیطی مطالعه می‌شود که ترکیبی از مشاهده میدانی واقعی و آزمایش‌های کنترل‌شده آزمایشگاهی است تا اعتبار نتایج در دنیای واقعی تضمین شود

پژوهش‌های داخلی و خارجی درباره تهدیدات شناختی هنوز در مراحل ابتدایی است، اما روند تحولات نشان می‌دهد که این حوزه به‌سرعت به یکی از محورهای اصلی مطالعات امنیتی و اطلاعاتی تبدیل شده است. در ادامه مهم‌ترین پژوهش‌های مرتبط مرور و تحلیل می‌شوند:

جدول (۱) پیشینه تحقیق

پژوهشگر	عنوان و سال پژوهش	هدف تحقیق	روش تحقیق	یافته‌های کلیدی	ارتباط با پژوهش حاضر
جوردانو، جی؛ و دیولیس، دی.	تهدیدات عصبی-شناختی در عملیات نظامی و اطلاعاتی (۲۰۲۲)	بررسی تهدیدات عصب‌شناختی و پیامدهای فناوری‌های شناختی در عملیات اطلاعاتی	تحلیل اسنادی – مرور تحلیلی علوم اعصاب نظامی	تشریح تهدیدات عصب‌شناختی و ارائه راهبردهای دفاع شناختی	تبیین بعد فناورانه تهدیدات شناختی

1 -Statistical Optimization
2 -Human Augmentation
3 -Living Lab

لیندل، م.	تاب‌آوری شناختی در سازمان‌های اطلاعاتی (۲۰۲۳)	بررسی عوامل مؤثر بر خستگی شناختی و کاهش دقت تحلیلی افسران اطلاعاتی	پژوهش میدانی – داده‌های تجربی از سازمان اطلاعاتی غربی	نشان دادن نقش فشار ذهنی و بار شناختی در خطای تصمیم‌گیری	پایه تجربی سطح فردمحور
کوالسکی و جیانینی	هوش مصنوعی و دستکاری شناختی در زمینه‌های امنیتی (۲۰۲۰)	تحلیل نقش هوش مصنوعی در مداخله شناختی و تولید داده‌های فریب‌دهنده	مرور ادبیات – تحلیل نمونه‌های امنیتی	تشریح سوگیری الگوریتمی و آسیب‌پذیری تحلیلگران	تقویت سطح فناوری‌محور تهدیدات شناختی
محجوب عشرت‌آباد ی	عرصه شناختی جنگ و تهدیدات نوین در امنیت ملی ایران (۱۴۰۰)	بومی‌سازی مفهوم جنگ شناختی در ایران	تحلیل نظری – بررسی اسناد امنیت ملی	ارائه خوانش بومی از جنگ شناختی و اثر آن بر ساختار دفاعی	مبنای داخلی چارچوب نظری
رضایی و نادری	تحلیل تهدیدات شناختی در نظام تصمیم‌سازی امنیت ملی (۱۴۰۱)	شناسایی اختلالات شناختی تصمیم‌گیران در بحران‌ها	مطالعه کیفی – تحلیل مصاحبه‌ها و اسناد	عوامل شناختی مؤثر بر خطای تحلیلی تصمیم‌سازان	تطبیق‌پذیر با حوزه تصمیم‌سازی اطلاعاتی
رستمی و همکاران	پدافند شناختی و تهدیدات ترکیبی در فضای اطلاعاتی ایران (۱۴۰۲)	ارائه الزامات طراحی معماری پدافند شناختی	روش ترکیبی – تحلیل محتوا و اسناد	تبیین ضرورت پدافند شناختی در سطوح ملی و سازمانی	تقویت مبانی مقابله شناختی
فتحی و مظفری	تحلیل تطبیقی تهدیدات شناختی در سازمان‌های	مقایسه اثر فناوری‌های شناختی در سازمان‌های	مقایسه تطبیقی – تحلیل نظری	نشان دادن اثرگذاری دو حوزه نظامی و رسانه‌ای؛ پیشنهاد	پشتیبان بخش نتیجه‌گیری

	نظامی و رسانه‌ای (۱۴۰۲)	اطلاعاتی و رسانه‌ای		مدل دفاع شناختی بومی	
آنس کاونون	سوگیری‌های شناختی در تحلیل اطلاعات - ۲۰۱۹	بررسی ظهور سوگیری‌های شناختی و تأثیر آن‌ها بر فرآیند تحلیل اطلاعات در سطح تاکتیکی در تیم‌های اطلاعاتی نظامی	مطالعه موردی چندگانه با استفاده از روش‌های ترکیبی	سوگیری تأییدی، تفکر گروهی بسیار مکرر بود و ارزیابی آن توسط تحلیلگران دشوار؛ سایر سوگیری‌ها با فراوانی کمتر مشاهده شدند؛	مستقیماً به بررسی سوگیری‌های شناختی به‌عنوان یکی از تهدیدات شناختی در فرآیند تحلیل اطلاعات در سازمان‌های اطلاعاتی نظامی می‌پردازد،
ناتان جی. مکنتیس، وریکا مکانان، نانسی جی. کوک	علم شناختی هوش و تحلیل آن، ۲۰۱۵	ارائه چالش‌های شناختی متعددی که بر کار تحلیلگران اطلاعات تأثیر دارد	مروری بر ادبیات تحقیقات عوامل انسانی در تحلیل اطلاعات با استفاده از تحلیل وظیفه شناختی	چالش‌های کلیدی شامل فشار زمانی، سرریز اطلاعات، کمبود تخصص، ابزارهای ناکافی، آموزش ناکافی، کمبود بازخورد، رقابت بر سر دانش	بررسی چالش‌های شناختی در تحلیل اطلاعات در سازمان‌های اطلاعاتی که مستقیماً با تهدیدات شناختی در پارادایم جنگ شناختی مرتبط است.
آ. زاناسی و اف.روینی	سوگیری‌های شناختی ناشی از فناوری اطلاعات در هوش تحلیل:	بررسی رابطه بین سوگیری‌های شناختی و تحلیل کلان‌داده در حوزه اطلاعات	تحلیل کیفی	ابزارهای تحلیل کلان‌داده می‌توانند الگوهای پنهان را کشف کنند و برخی سوگیری‌ها را کاهش دهند، اما در دست کاربران بی‌تجربه ممکن است سوگیری‌ها را تسهیل کنند.	بررسی سوگیری‌های شناختی ناشی از فناوری اطلاعات در تحلیل اطلاعات که به‌عنوان یکی از تهدیدات شناختی در سازمان‌های اطلاعاتی نظامی در پارادایم جنگ شناختی مرتبط است.

پیشینه مطالعاتی مرتبط با تهدیدات شناختی در حوزه‌های امنیتی، اطلاعاتی و نظامی طی دهه اخیر رشد قابل‌توجهی داشته است. بااین‌حال، هنوز «تهدیدات شناختی در سازمان‌های اطلاعاتی نظامی ایران» به‌صورت نظام‌مند و سه‌سطحی (فردی، فناوری‌محور، فرآیند محور) بررسی نشده است. بر همین اساس، پیشینه حاضر بر اساس همین سه محور اصلی دسته‌بندی شده است تا انسجام محتوایی برقرار گردد و زمینه برای استخراج چارچوب نظری پژوهش فراهم شود.

بر اساس بررسی این منابع، سه نکته اساسی استخراج می‌شود:

۱) جهانی بودن موضوع: پژوهش‌های خارجی عمدتاً به تبیین نظریه‌های جنگ شناختی و تهدیدات عصب‌شناختی پرداخته‌اند و تمرکز اصلی آن‌ها بر فناوری‌های مغزی و داده‌ای است.

۲) شکاف بومی: پژوهش‌های داخلی اگرچه به مفهوم جنگ شناختی اشاره کرده‌اند، اما هنوز مطالعه‌ای جامع درباره تهدیدات شناختی سازمان‌های اطلاعاتی نظامی ایران وجود ندارد.

۳) نیاز به مدل‌سازی: در هیچ‌یک از مطالعات مرور شده، چارچوبی تلفیقی شامل سطوح سه‌گانه فردی، فناورانه و فرایندی برای تحلیل تهدیدات شناختی ارائه نشده است.

بنابراین، پژوهش حاضر با تمرکز بر سازمان اطلاعاتی نظامی، در پی آن است که با بهره‌گیری از یافته‌های فوق، مدلی بومی برای شناسایی، تحلیل و طبقه‌بندی تهدیدات شناختی ارائه کند و شکاف نظری و تجربی موجود را پوشش دهد.

برای رفع شکاف‌های موجود، پژوهش حاضر نوآوری‌های زیر را ارائه می‌دهد:

۱) طراحی مدل بومی سه‌سطحی تهدیدات شناختی در سازمان اطلاعاتی ارتش ایران.

۲) استخراج تهدیدات واقعی از طریق تحلیل محتوای کیفی داده‌های میدانی.

۳) ترکیب پیشینه‌های نظامی، امنیتی، شناختی و فناوری.

۴) ارائه چارچوب نظری منسجم برای فهم تهدیدات شناختی در ساختارهای اطلاعاتی.

این نوآوری‌ها پژوهش را از مطالعات مشابه متمایز می‌سازد.

مبانی نظری

ظهور مفهوم «جنگ شناختی» در ادبیات نظامی و اطلاعاتی، محصول هم‌گرایی علوم شناختی، علوم اعصاب، هوش مصنوعی، علوم رفتاری و فناوری‌های اطلاعاتی است. در

این چارچوب، تهدید شناختی به‌عنوان یکی از مهم‌ترین اشکال جدید تهدیدات ترکیبی[1] شناخته می‌شود که هدف آن دست‌کاری در فرایندهای شناختی انسان و سازمان است (دوکلوزل، ۲۰۲۱).

از دیدگاه ناتو (۲۰۲۳) جنگ شناختی، فراتر از عملیات روانی و اطلاعاتی است، زیرا به‌طور مستقیم ساختارهای ذهنی و الگوهای تصمیم‌گیری فرد یا سازمان را هدف قرار می‌دهد. این جنگ نه‌تنها به دنبال تغییر باورها، بلکه به دنبال تغییر شیوه تفکر و پردازش اطلاعات است. در چنین شرایطی، هر سازمانی که بر مبنای داده و تحلیل تصمیم می‌گیرد، ازجمله سازمان‌های اطلاعاتی، در معرض تهدیدات شناختی قرار دارد. این تهدیدات ممکن است از طریق فناوری، محیط سازمانی یا حتی ویژگی‌های فردی نیروهای اطلاعاتی بروز یابد. سازمان اطلاعاتی در ذات خود یک سامانه شناختی جمعی است؛ زیرا مأموریت آن گردآوری، پردازش، تفسیر و به‌کارگیری داده‌ها برای تصمیم‌سازی‌های راهبردی است. در چنین سامانه‌ای، «شناخت» نه‌تنها در سطح فردی (تحلیلگر یا افسر اطلاعاتی)، بلکه در سطح ساختاری و فناورانه نیز اهمیت دارد. بر اساس دیدگاه مارکوویچ (۲۰۱۹)، کارایی سازمان اطلاعاتی به میزان «هم‌ترازی شناختی» میان انسان، فناوری و فرایندها بستگی دارد. هرگونه عدم توازن در این سه بُعد، منجر به بروز تهدیدات شناختی خواهد شد. به‌عبارت‌دیگر، اگر نیروی انسانی دچار سوگیری شناختی، سامانه‌های اطلاعاتی دچار آلودگی داده‌ای، یا فرایندهای تصمیم‌گیری دچار ابهام و فشار زمانی شوند، احتمال وقوع خطاهای تحلیلی و تصمیم‌گیری اشتباه افزایش می‌یابد. این خطاها، جوهره تهدیدات شناختی در سازمان‌های اطلاعاتی را شکل می‌دهند.

استفاده از داده‌های رفتاری و تحلیل‌های تجربی دربارهٔ شناخت انسان، قابلیت مطالعهٔ جنبه‌های کارکردی و ساختاری مغز، به‌طور هم‌زمان را فراهم آورده است (گالوتی[2]، ۲۰۰۸). جنگ شناختی با استفاده از ابزارهای روان‌شناختی، فناوری‌محور، اطلاعاتی و ادراکی، مستقیماً بر چرخه تحلیل و تصمیم‌سازی نیروهای نظامی اثر می‌گذارد. ناتو در سند «جنگ شناختی ۲۰۲۱» تأکید می‌کند که آینده جنگ‌ها بیش از هر زمان دیگر «مبتنی بر ذهن انسان» خواهد بود و سازمان‌های اطلاعاتی بیشترین حساسیت را در برابر این تهدیدات دارند.

1 -Hybrid Threats
2 -Galotti

جوردانو و دی‌الیوت (۲۰۲۲) جنگ شناختی را «تلاش سازمان‌یافته برای اثرگذاری بر ساختارهای ادراکی و عصب‌شناختی تحلیلگران» تعریف می‌کنند؛ به‌طوری‌که قدرت تحلیل، قضاوت و تصمیم‌گیری آن‌ها به‌صورت هدفمند مختل شود. این تعریف به‌طور مستقیم به موضوع پژوهش حاضر مرتبط است.

علم مغز نظامی مبتنی بر تئوری‌ها و فناوری‌های پزشکی نظامی، پزشکی پایه، پزشکی نظامی، زیست‌شناسی، فیزیک، علم کامپیوتر، علوم نظامی و چندین رشته علمی دیگر است. علم مغز نظامی؛ تغییرات بنیادی را در مفهوم مبارزه، روش‌ها و سبک مبارزه به وجود آورده و درواقع با بازتعریف میدان جنگ یک کل جدید با عنوان جنگ مغز به وجود آورده است (جین، هو و وانگ[1]، ۲۰۱۸).

مطالعات نشان داده است که فضای محیطی (وایتورث و سیکولو[2]، ۲۰۱۶)، میدان‌های مغناطیسی و الکتریکی (هو و فو[3]، ۲۰۱۵) می‌توانند بر عملکرد سیستم عصبی و مغز تأثیر بگذراند و عملکرد شناختی آن را دچار اختلال کند.

محافظت از آسیب مغزی (جین، هو و وانگ[4]، ۲۰۱۸) و اطمینان از وضعیت کارکردی مغز، یکی از عوامل تعیین‌کننده در میدان جنگ است باید به خستگی مغزی و تصمیمات مغزی افراد کلیدی که در پست‌های مهم هستند نظارت مداوم داشته باشیم (بیگلر[5]، ۲۰۱۶)؛

چگونگی ایجاد اثرات مخرب به بخش‌های حساس بافت مغز به‌وسیله سلاح‌های صوتی (چان، هو و ریان[6]، ۲۰۱۶)، سلاح‌های لیزری، سلاح‌های انفجاری قوی (اکستانس[7]، ۲۰۱۵)، سلاح‌های الکترومغناطیسی؛ (ولف[8] و همکاران، ۲۰۰۹). سلاح‌های تداخل در امواج مغزی و سلاح‌های فرو صوت برای ایجاد تداخل در بافت‌های مغزی و جنون، طراحی و توسعه داده خواهد شد (کمیته تحقیقات ملی آمریکا، ۲۰۰۸). استراتژی اختلال در مغز،

1 -Jin, Hou, Wang
2- Whitworth, Ciccolo
3 -Jin, Hou, Fu
4 -Jin, Hou, Wang
5 -Bigler
6 -Chan, Ho, Ryan
7- Extance
8 -Wolf

می‌تواند بر ذهنیت، تفکر اثربخش، تصمیم‌گیری و سایر فرایندهای ذهنی تأثیر بگذارد و سبک مبارزه کاملاً جدید با عنوان جنگ مغز را به وجود بیاورد (ایوانی و هاگ[1]، ۲۰۱۶). علائم مزمن ناشی از آسیب مغزی مانند اختلال استرس پس از سانحه، هنوز از مسائل دشوار درزمینهٔ ترمیم مغز هستند (اوکی[2]، ۲۰۱۶).

در سطح دوم از تهدیدات شناختی، ما با تهدیدات شناختی مواجه هستیم که بر اساس یافته‌های روانشناسی شناختی در حوزه‌های کارکردها و فرایندهای شناختی طراحی و اجرا می‌شوند. عاملان جنگ شناختی از مطالعات شناختی در کارکردهای شناختی مانند توجه، حافظه، ادراک، تصمیم‌گیری، آگاهی، به‌منظور آسیب زدن به کارکردهای شناختی انسان استفاده می‌کنند. اگرچه این سطح از تهدیدات شناختی، نسبت به سطح عصب-شناختی، ضریب تأثیر کمتر و خطای بیشتری دارند، اما نیاز به منابع مالی و انسانی کمتر، ابزارهای فناورانه کمتر و ریسک اجرایی کمتر، باعث تمایل بیشتر کشورها به طراحی و اجرای این سطح از تهدیدات شده است. یکی از منابع مهم مورداستفاده در تهدیدات روان‌شناختی، استفاده از مطالعات گسترده در حوزه خطاها و انحرافات سیستماتیک شناخت انسان است. تیم‌های جنگ شناختی دشمن، معمولاً در طراحی و اجرای پیام‌های شناختی، از این سوگیری‌های شناختی برای تأثیرگذاری استفاده می‌کنند.

سوگیری شناختی، انحراف سیستماتیک (غیر تصادفی، قابل پیش‌بینی، مشخص و معین) از عقلانیت در قضاوت و تصمیم‌گیری است. این انحرافات از هنجارهای عقلانی و منطقی، سیستماتیک هستند، یعنی افراد بارها و بارها در یک مسئله شکست می‌خورند دوباره آن را تکرار می‌کنند. معلوم می‌شود که افراد به روش قابل پیش‌بینی غیرمنطقی هستند (آریلی[3]، ۲۰۰۸).

پدیده معروف توهم مولر – لیر[4] نشان می‌دهد که چگونه اطلاعات نامرتبط می‌تواند سیستم ادراکی ما را فریب بدهد. این خطاهای سیستماتیک در حافظه، توجه و سایر کارکردهای شناختی هم وجود دارد (هوی و پورویس[5]، ۲۰۰۵). سوگیری‌های شناختی

1 -Ivany, Hoge
2 -Okie
3 -Ariely
4 -Muller-Lyer illusion
5 -Howe and Purves

در سطح گروهی فاجعه‌بار است، چون سیستماتیک است و همه افراد آن را مرتکب می‌شوند (تصادفی نیست که یک گروه انجام بدهند و یک گروه انجام ندهند) و کسی نیست که آن را لغو کند؛ مانند زمانی که تصمیمات جمعی بحران‌های اقتصادی را رقم می‌زند (آریلی[1]، ۲۰۰۹).

انسان‌ها برآیندی از ابعاد زیستی، اطلاعاتی، روان‌شناختی، اجتماعی و فنی (بیش از مجموع ابعاد) هستند. بسیاری ماهیت انسان را متشکل از سه جنبه در نظر می‌گیرند: انسان به‌عنوان موجود «بیولوژیکی»، انسان به‌عنوان موجود «روان‌شناختی» و انسان به‌عنوان موجود «اجتماعی» که همگی در متن جهان بیرونی ظهور می‌یابد. یکی از دغدغه‌های اقتصاددانان، سیاست‌مداران، تاجران و استراتژیست‌های نظامی این است که چگونه از پتانسیل علوم شناختی در جهت تحقق اهداف استثماری اجتماعی بهره ببرند. به دلیل همین اهداف استثماری بود که اصطلاح جنگ شناختی به فضای اجتماعی و فرهنگی و در شرایط عادی جامعه هم کشیده شد.

تکنولوژیست‌های ناتو، معتقدند هدف جنگ شناختی، هم نیروهای نظامی است و هم کل جامعه. این نکته تأمل‌برانگیز است که نه‌تنها جامعهٔ دشمن که جامعهٔ خودی هم به‌عنوان دشمن می‌تواند در نظر گرفته شود. تهدید بالقوه، شهروندان هستند که ممکن است به‌عنوان «ستون ششم» یا «عناصر خفته»[2] ایفای نقش کنند (سازمان بین‌المللی استراتژی‌های سیاسی و اقتصادی[3]، ۲۰۲۱).

زروباول بر این باور است که علوم شناختی باید در موضع معرفت‌شناسی خود در مطالعهٔ چیستی شناخت تجدیدنظر کنند؛ یعنی در عوض آنکه کنش اندیشه‌ورزی را امری کاملاً فردی یا انسانی در نظر بگیرند، باید آن را کنشی اجتماعی در نظر گرفت. ما به‌عنوان فرد یا انسان نیست که به شناخت جهان اطراف خود دست می‌یابیم، بلکه فهم ما از پدیده‌های اطرافمان تا حد زیادی محصول این واقعیت است که ما موجوداتی اجتماعی هستیم شناخت جمعی چیزی بیش از حاصل جمع شناخت‌های فردی است و غالباً ساختاری متفاوت از آن‌ها دارد. به‌بیان‌دیگر، ما چیزها را تنها از طریق حواس تجربه نمی‌کنیم، بلکه

1 -Ariely
2- sleeping cells
3-Institute of International Political and Economic Strategies

به‌طور غیرشخصی از طریق عضویت ذهنی‌مان در جوامع فکری مختلف نیز تجربه می‌کنیم (زروباول[1]، ۲۰۱۹).

با بررسی پژوهش‌های پیشین و مبانی نظری مرتبط با موضوع جنگ شناختی و تهدیدات شناختی، نکات کلیدی مرتبط با ساختار و ماهیت این تهدیدات آشکار می‌شود. به‌ویژه در مطالعات نظامی، شناسایی سطوح مختلف تهدیدات شناختی برای طراحی راهبردهای مؤثر پدافند شناختی اهمیت فراوانی دارد. درنتیجه، بر اساس ادبیات نظری جمع‌آوری‌شده و یافته‌های پژوهش حاضر، طبقه‌بندی مبسوطی از این تهدیدات در سه سطح فردمحور، فناوری‌محور و فرآیندمحور ارائه می‌گردد.

تهدیدات شناختی فردمحور

تهدیدات شناختی فردمحور مرتبط با ادراک، حافظه، توجه، سوگیری‌ها، خستگی ذهنی و فرآیندهای ذهنی تحلیلگران اطلاعاتی هستند. مهم‌ترین عوامل فردمحور عبارت‌اند از:

- خستگی ذهنی و اضافه‌بار شناختی. لیندل (۲۰۲۳).
- سوگیری‌های شناختی همچون سوگیری تأییدی، دسترس‌پذیری و لنگرگیری
- اختلالات ناشی از فشار مأموریتی و استرس عملیاتی. هاگ (۲۰۰۸).
- ضعف در پردازش داده‌های پیچیده اطلاعاتی
- کاهش دقت قضاوت در شرایط تنش

جوردانو (۲۰۲۲) بیان می‌کند که در محیط‌های اطلاعاتی، ذهن انسان «بزرگ‌ترین نقطه‌ضعف» در برابر حملات شناختی است.

تهدیدات شناختی فناوری‌محور

این سطح شامل تهدیداتی است که از طریق فناوری و سامانه‌های اطلاعاتی بر ادراک و تحلیل نیروهای اطلاعاتی اثر می‌گذارند:

- سوگیری الگوریتمی ناشی از داده‌های ناقص یا جهت‌دار
- داده‌های فریب‌دهنده در عملیات شناختی دشمن
- تحریف اطلاعات در پردازش کلان‌داده‌ها
- مداخلات شناختی مبتنی بر هوش مصنوعی کوالسکی و جیوانی (۲۰۲۰).

1 -Zerubavel

- فناوری‌های NBIC (نانوفناوری، زیست‌فناوری، اطلاعات و علوم شناختی). روکو و بیانبریج (۲۰۰۳).

ناتو (۲۰۲۱) میان «تهدید شناختی فناورانه» و «تهدید اطلاعاتی» تفاوت قائل می‌شود و اولی را بسیار خطرناک‌تر می‌داند، زیرا مستقیماً ادراک تحلیلگر را هدف می‌گیرد.

تهدیدات شناختی فرآیند محور

این سطح شامل تهدیداتی است که ناشی از ساختار، فرهنگ سازمانی، فرایند تحلیل اطلاعات و جریان اطلاعات در سازمان هستند:

- سلسله‌مراتب سخت و چندلایه در ساختار اطلاعاتی
- انسداد اطلاعاتی و ناکارآمدی جریان داده‌ها. وزارت دفاع ایالات‌متحده (۲۰۲۳).
- نبود چرخه بازخورد تحلیلی هور و فرسون (۲۰۲۳).
- ضعف در نظام غربالگری و تأیید تحلیل‌ها
- رویه‌های تحلیلی غیرمنعطف
- فرهنگ سازمانی محافظه‌کار و محدودکننده تحلیل

این سطح یکی از مهم‌ترین سطوح تهدیدات شناختی در سازمان‌های اطلاعاتی نظامی محسوب می‌شود، زیرا ضعف ساختاری می‌تواند حتی تحلیلگر توانمند را ناکارآمد کند.

روش‌شناسی

روش انجام پژوهش، تحلیل محتوا است. تحلیل محتوا روشی برای مطالعه عینی، منظم و سیستماتیک فراورده‌های ارتباطی (محتوای آشکار ارتباطی) جهت رسیدن به تفسیر است. جامعه پژوهش، فرماندهان و افسران اطلاعاتی مشغول به خدمت در سازمان‌های اطلاعاتی نظامی بودند. به‌منظور انتخاب مشارکت‌کنندگان از روش انتخاب هدفمند و منطق اشباع نظری استفاده شده است. بر این اساس افرادی انتخاب شدند که اطلاعات و تجربه کافی در خصوص تهدیدات شناختی سازمان موردمطالعه داشته باشند. بر اساس منطق اشباع نظری، گردآوری داده‌های کیفی تا جایی ادامه یافت که پاسخ‌های مشارکت‌کنندگان تکراری بود و مضامین جدیدی برای نظام کدگذاری به همراه نداشت. با توجه به اینکه در تعداد ۱۱ مصاحبه مورد به اشباع نظری دست‌یافتیم، با حجم نمونه ۱۱ تن، کفایت نمونه‌گیری احراز شد. در این پژوهش به‌منظور جمع‌آوری اطلاعات و

داده‌ها از روش‌های گردآوری داده‌ها و اطلاعات اسنادی/ کتابخانه‌ای و میدانی استفاده‌شده است. همچنین ابزارهای مورداستفاده در این پژوهش شامل پرسشنامه باز پاسخ است که توسط تیم تحقیقاتی طراحی‌شده است. تحلیل داده‌های کیفی با استفاده از الگوی کدگذاری سه مرحله‌ای اشتراوس و کوربین[1] (۱۴۰۱) انجام شده است. به‌منظور احراز قابلیت اطمینان (معادل با روایی و پایایی در روش کمی) تحلیل محتوا از شاخص‌های تأییدپذیری (عینیت تحلیل محتوا از طریق استناد به گزاره‌های عینی)، انتقال‌پذیری (توصیف دقیق میدان پژوهش)، اتکاپذیری (توصیف دقیق گام‌های تحلیل) استفاده شده است.

برای تحلیل داده‌ها از نرم‌افزار مکس‌کیودا[2] استفاده شد است که در آن امکان تحلیل انواع داده‌های متنی وجود دارد. این نرم‌افزار امکان انجام کدگذاری سه‌مرحله‌ای (باز، محوری و انتخابی) را فراهم کرد و به پژوهشگر اجازه داد بخش‌های مختلف مصاحبه‌ها را در قالب کدها، طبقات و تم‌ها دسته‌بندی کند. به‌منظور افزایش تأییدپذیری یافته‌ها، فرایند تحلیل داده‌ها به‌صورت قدم‌به‌قدم مستندسازی شد و کلیه کدها و طبقات در نرم‌افزار مکس‌کیودا ثبت گردید. همچنین، مجموعه‌ای از بازبینی‌های بیرونی توسط یک پژوهشگر مستقل صورت گرفت تا مطمئن شود کدگذاری‌ها و تفاسیر پژوهشگر از داده‌ها با متن مصاحبه‌ها همخوانی دارد. علاوه بر این، از روش بازنگری مشارکت‌کنندگان برای تأیید صحت برداشت‌ها استفاده شد و خلاصه تحلیل‌ها برای برخی از مشارکت‌کنندگان ارسال و بازخورد آن‌ها دریافت گردید. برای تأمین اتکاپذیری، بخشی از داده‌ها توسط دو کدگذار مستقل تحلیل شد. میزان توافق بین کدگذاران با استفاده از فرمول توافق درون‌ذهنی و در نرم‌افزار مکس‌کیودا محاسبه شد و مقدار آن ۸۱ درصد به دست آمد که بالاتر از حداقل قابل‌قبول (۷۰ درصد) است. اختلاف‌ها نیز در چند جلسه هم‌اندیشی بررسی و رفع شدند. این فرایند باعث بالا رفتن ثبات و قابل‌اعتماد بودن نتایج شد. برای افزایش انتقال‌پذیری، توصیف غنی از زمینه پژوهش، مشخصات مشارکت‌کنندگان، موقعیت سازمانی و فرآیند گردآوری داده‌ها ارائه شد تا خوانندگان بتوانند تشخیص دهند که نتایج این مطالعه تا چه حد قابلیت استفاده در شرایط مشابه در سایر یگان‌های اطلاعاتی نظامی را دارد. انتخاب مشارکت‌کنندگان نیز به‌صورت هدفمند و بر اساس بیشترین آگاهی صورت گرفت

1- Strauss and Corbin
2- MAXQDA

تا دامنه متنوعی از تجربیات پوشش داده شود. برای افزایش اعتبار یافته‌ها، از روش مثلث‌سازی منابع استفاده شد؛ بدین‌صورت که داده‌های مصاحبه، اسناد سازمانی و گزارش‌های رسمی به‌طور هم‌زمان بررسی و مقایسه شد. همچنین مطابقت مستمر داده‌ها با چارچوب نظری و بازبینی مداوم توسط پژوهشگران اعمال شد.

تجزیه‌وتحلیل یافته‌ها

در یافته‌های حاصل از تحلیل ۱۱ مصاحبه نیمه ساختاریافته نشان می‌دهد که تهدیدات شناختی در سازمان اطلاعاتی نظامی موردمطالعه در سه سطح اصلی فردمحور، فناوری‌محور و فرایندمحور بروز می‌یابند. در این بخش، داده‌ها به‌صورت سازمان‌یافته، همراه با ارجاع به جداول و نمونه اظهارات مشارکت‌کنندگان، ارائه شده است.

تهدیدات شناختی فردمحور

مطابق جدول (۲)، تهدیدات فردمحور شامل دو بعد اصلی «سبک‌ها و ویژگی‌ها» و «ضعف‌ها و کمبودها» است.

جدول (۲) کدگذاری مفاهیم تهدیدات شناختی فرد محور

مقوله‌ها		کدهای مفهومی	مصاحبه شونده	نمونه گزاره‌های کلامی
سبک‌ها و ویژگی‌ها	سوگیری های شناختی	سوگیری قالب‌بندی/ سوگیری هیجان محور/ پردازش ذهنی خودکار/ جهت‌گیری ذهنی/	۱-۸-۷-۶-۵-۲-۳-	طریقه ارائه اطلاعات یا همان قالب‌بندی می‌تواند باعث شود تا افسران اطلاعاتی گرایش بیشتری روی آن خبر یا موضوع خاص داشته باشند (م.۶).
	سبک تصمیم گیری تکانشی	تصمیم‌گیری سریع و بدون تأمل/ عجله در تحلیل/ واکنش‌های هیجانی/ سرعت عمل در تصمیم‌گیری	۸-۷-۲-۵-۱-۳-	تصمیم‌گیری سریع اما بدون تأمل کردن فقط سرعت عمل در پاسخگویی را به همراه خواهد داشت اما درنهایت خروجی و برآیند کار فاقد پختگی و ارزش اطلاعاتی مطلوب خواهد بود (م.۳).
	توانایی ضعیف مشارکت و کار تیمی	توانایی ضعیف کار تیمی/ عدم همکاری و مشارکت تیمی/ استرس کار تیمی/ توانایی کار فردی/	۵-۴-۱-۲	انجام هرگونه عملیات اطلاعاتی بایستی به‌صورت تیمی و گروهی انجام شود و یک فرد به‌تنهایی قادر نیست در تمامی ابعاد و زمینه‌های اطلاعاتی و عملیاتی به نتیجه دلخواه برسد. (م.۵).

مقوله‌ها		کدهای مفهومی	مصاحبه شونده	نمونه گزاره‌های کلامی
	قطعیت-گرایی	ناتوانی در تصمیم‌گیری عدم قطعیت/ عدم تحمل ابهام/ قطعیت گرایی/ دوری از موقعیت‌های نامتعین/	۶-۱-۷- ۲-۳	اگرچه این تفکر وجود دارد که عدم قطعیت باعث خطا در تحلیل‌ها می‌شود اما در عصر عدم قطعیت بعضی وقت‌ها کشف الگوهای احتمالی در داده‌ها و اطلاعات بسیار سخت است و خب همه ابتدا احساس ابهام را دارند. (م.۷).
	تفکر غیر تحلیلی	تحلیل‌های سطحی/ اتکا به شواهد محدود/ توجه صرف به الگوهای آشکار/ ضعف در تحلیل ارتباطی داده‌ها و اطلاعات/	۷-۳-۲	معمولاً یک افسر اطلاعاتی توانایی تحلیلی زیادی باید داشته باشد، اما باید این را در نظر گرفت که به دلیل قدیمی بودن سامانه اطلاعاتی، اطلاعات بعضاً به‌صورت خام یا طبقه‌بندی و فیلتر نشده در اختیار ما قرار می‌گیرد و اگر افسر تفکر تحلیلی قوی نداشته باشد باعث گمراهی او خواهد شد (م.۷).
ضعف‌ها و کمبودها	تاب‌آوری شناختی	دوری از موقعیت‌های پراسترس/ تحلیل‌های ناقص و تکمیل‌نشده/ عدم تحمل ابهام/	۷-۶-۴	حتی در شرایطی اطلاعات زیاد یا بمباران اطلاعاتی افسران باعث اجتناب آن‌ها می‌شود و احساس می‌کنید که نمی‌توانید این کار را جمع کنید. (م.۷).
	سرعت پردازش ذهنی	سرعت‌پایین حل مسئله/ سرعت‌پایین تحلیل و استنتاج/ سرعت‌پایین تصمیم‌گیری/	۶-۱	اما بعضی از افسران در شرایط با محدودیت زمانی دچار استرس شده یا نمی‌توانند با سرعت مناسب گزارش را آماده کنند در این افراد همیشه عجله باعث می‌شود احتمال خطا افزایش یابد و قطعاً در پیش‌بینی ما را دچار خطا خواهد کرد (م.۶).
	انعطاف پذیری ذهنی	تک بعد نگری/ تصمیم-گیری یک‌سویه/ رویه‌ها و روش‌های تکراری/ تحلیل سطحی و تک‌بعدی/ ضعف در انتقال سریع بین تکالیف/	۱-۳-۶-۲-۵	در حوزه رصد و پردازش لازم است ذهن، پویا فعال و چندبعدی، باشد چنانچه یک افسر یا کارشناس فاقد انعطاف‌پذیری لازم در فرآیندها، باشد قطعاً نتایج به‌دست‌آمده تک‌بعدی خواهد بود که این مهم می‌تواند باعث صدمات جدی به مأموریت سازمان گردد (م.۱).
	دانش اطلاعاتی	عدم اشراف به اخبار و اطلاعات/ عدم شناخت درست مسئله/ عدم استفاده از چارچوب‌ها و روش‌های استاندارد/ عدم شناخت نسبت به	۱-۸-۷-۵-۶-۳	از راه‌های مهمی که می‌توان بر آسیب خطای تحلیل غلبه کرد می‌شود به استفاده از منابع معتبر اطلاعاتی، بهره‌گیری از منابع متعدد و گوناگون تقاطع گیری لحظه‌ای کاهش حجم اطلاعات، استفاده از شیوه‌ها و ابزارهای مختلف جمع‌آوری اطلاعات دروی از فضای رسانه‌ای

مقوله‌ها		کدهای مفهومی	مصاحبه شونده	نمونه گزاره‌های کلامی
		تهدیدات جدید/ عدم تقاطع اخبار/		هیجانی و... اشاره نمود که به سطح دانش اطلاعاتی افسر بستگی دارد (م.۱).
	خستگی شناختی	کاهش کارایی ذهنی/ افزایش خطاهای بررسی و تحلیل/ کاهش تمرکز و دقت/ ضعف در قدرت تفکر ذهنی	۳-۵-۲-	این حجم از اطلاعات تأثیر زیادی بر خود افسر یا کارشناس اطلاعات می‌گذارد و او را با یک خستگی روانی و ذهنی مواجه می‌سازد. زمانی که ذهن شما خسته می‌شود، کارایی ذهن شما برای تحلیل و سایر کارهای اطلاعاتی به‌شدت کاهش می‌یابد (م.۵).
	تمرکز ذهنی	بی‌انضباطی ذهنی/ فشار دغدغه‌های فردی/ منحرف شدن مسیر فکری/ تمرکز در زمان کم/	۳-۱-۲	بعضی وقت‌ها شما با انبوهی از اطلاعات مواجه هستید و حس می‌کنید در میان آن‌ها سردرگم هستید؛ و اگر تمرکز ذهنی کافی نداشته باشید به‌راحتی از مسیر منحرف می‌شوید (م.۲).
	ابتکار و خلاقیت	روش‌ها و تکنیک‌های قدیمی/ بی‌علاقگی به راه‌حل‌های جدید/ رویه-های تحلیلی سنتی/ پذیرا نبودن/ استرس خلاقیت/	۷-۴-۸	خلاقیت، هم در بخش گردآوری اطلاعات، هم در بخش تجزیه‌وتحلیل اطلاعات باعث نتایج جدیدی می‌شود؛ اما چون هم مشوق‌های خلاقیت وجود ندارد و هم ارائه راهکارهای خلاقانه ریسک بالایی برای افراد ممکن است داشته باشد و حمایت سازمانی ممکن است انجام نشود (م. ۸).
	یادگیری از خطا	عدم خطاپذیری و اصلاح‌گری/ بی‌توجهی به خطاهای گذشته/ تأمل نکردن در خصوص بازخوردهای دریافتی/ تکرار مداوم اشتباهات/	۳-۸-۱-۵-۲	خطاهایی که پس از تجربه تشخیص داده‌شده‌اند خود بهترین الگو و منبع اطلاعاتی به شمار می‌آیند. درک و فهم یک اشتباه و خطا در زمان و مکان مناسب خود از الطاف بزرگی است که یک کارشناس می‌تواند از تجربه آن‌ها درس بگیرد (م.۱).
	شناخت تیمی	ترجیح فعالیت فردی/ ضعف در تشکیل کارگروه‌های مشترک/ عدم علاقه سازمانی به کارگروهی/ تک‌بعدی عمل کردن/	۱-۸-۳	ازیک‌طرف افراد علاقه‌ای به کار گروهی ندارند و از طرفی هم محدودیت منابع انسانی و تخصص‌ها این مهم را با مشکل مواجه می‌سازد و ساختار سازمانی به‌گونه‌ای است که تشکیل کارگروه‌های مشترک متشکل از بخش‌های مختلف بسیار دشوار است (م.۸).

۲- تهدیدات شناختی سازمان اطلاعاتی نظامی موردمطالعه در سطح فناوری‌ها (تهدیدات شناختی فناوری محور) شامل چه ابعاد و مؤلفه‌هایی است؟

جدول (۳) کدگذاری مفاهیم تهدیدات شناختی فناوری محور

مقوله‌ها	کدهای مفهومی	مصاحبه شونده	نمونه گزاره‌های کلامی
ارزیابی و نظارت شناختی	مدل‌سازی شناختی/ تحلیل روایت‌ها و فرا روایت‌ها/ تحلیل گفتمان اجتماعی/ فناوری‌های تصویربرداری عصبی عمیق/ داده‌های نرم‌افزارهای ارزیابی/ کلان داده‌های رفتاری/ پلتفرم‌های عمومی/ جنبش‌های و جریان‌های جمعی/ کلان داده‌های فضای مجازی/ رسانه‌های اجتماعی	۹-۱۰-۱۱	رشد علوم و فناوری‌های شناختی این امکان را برای دولت‌ها فراهم ساخته تا بتوانند در سطح کلان و خیلی جزئی بسیاری از الگوهای شناختی را در سطح فردی و جمعی را ارزیابی و نظارت کنند. به‌عنوان‌مثال مدل‌سازی شناختی بر اساس تحلیل کلان داده‌ها این امکان را فراهم می‌کند تا بتوانند الگوهای شناختی را شناسایی کرده و به رفتارهای فردی و جمعی جهت بدهند. یک سامانه اطلاعاتی موفق باید بتوانند این تهدیدات شناختی که می‌توان گفت در سطح نظارت و ارزیابی است را شناسایی و تحلیل کند (م.۹).
مداخله و کنترل شناختی	خلق روایت/ جریان سازی/ اقناع‌سازی/ توانمندسازی شناختی/ فریب شناختی/بازتوانی شناختی/ تحریک مغزی/ داروهای شناختی/ ایمپلنت‌های مغزی/ رابط‌های بی‌سیم مغز-رایانه/ رابط‌های دوسویه تعاملی مغز-رایانه/	۹-۱۰	کشورهای پیشرو در علوم نظام و سازمان‌های معروفی مانند ناتو، بودجه بسیار زیادی را در ابزارها و فناوری‌های مداخله و کنترل شناختی اختصاص داده‌اند و برنامه‌های تحقیقاتی زیادی را در این زمینه تعریف کرده‌اند. به کمک ایمپلنت‌های مغزی و رابط‌های بسیم مغز-رایانه سربازان آینده که در جنگ حضور دارند به لحاظ قابلیت‌ها بسیار متفاوت با سربازان عادی هستند که می‌تواند صحنه نبرد را متفاوت کند (م.۱۰).
شبیه‌سازی و هوش مصنوعی	محاسبات شناختی/ سلاح‌ها و مهمات هوشمند/ تحلیل کلان داده‌ها/ سیستم فرماندهی‌وکنترل هوشمند/ شبکه‌های عصبی مصنوعی/ مدل‌سازی محاسبات شناختی/ ربات‌های هوشمند/ یادگیری ماشین/	۹-۱۰-۱۱	فناوری‌های مانند محاسبات شناختی، امکان الگوبرداری از فرایندها و کارکردهای شناختی انسان و پیاده‌سازی آن‌ها در ماشین‌ها و رایانه‌ها را فراهم کرده است (م.۱۱). سیستم فرماندهی‌وکنترل هوشمند که می‌توانند به‌صورت خودکار به سامانه تسلیحاتی وصل شده و اطلاعات دریافتی را تحلیل و پردازش کند، سطح عمیقی از منازعات شناختی در آینده را نشان می‌دهد (م.۱۰).

مطابق جدول (۳)، تهدیدات فناوری‌محور شامل سه مقوله اصلی «ارزیابی و نظارت شناختی»، «مداخله و کنترل شناختی» و «شبیه‌سازی و هوش مصنوعی» است. این مقولات شامل عناصر مهمی مانند تحلیل کلان‌داده‌ها، مدل‌سازی شناختی، فناوری‌های تصویربرداری، اقناع‌سازی شناختی، داروهای شناختی، رابط‌های مغز–رایانه، محاسبات شناختی و سیستم فرماندهی- کنترل هوشمند هستند.

۳- تهدیدات شناختی سازمان اطلاعاتی نظامی موردمطالعه در سطح فرایندهای سازمانی (تهدیدات شناختی فرایندمحور) شامل چه ابعاد و مؤلفه‌هایی است؟
مطابق جدول (۴)، تهدیدات فرایندی در سازمان اطلاعاتی شامل مقولات «منابع تهدید»، «پیامدها» و «شرایط تقویت‌کننده» هستند. مهم‌ترین مؤلفه‌ها شامل فرهنگ سازمانی ضد خلاقیت، ساختار سلسله‌مراتبی سخت، ضعف در فناوری‌های تحلیل، اتکا به روش‌های سنتی، اضافه‌بار اطلاعاتی، اطلاعات فریب‌دهنده، دسترسی محدود به اطلاعات، فشار کاری و شرایط عدم قطعیت است.

جدول (۴) کدگذاری مفاهیم تهدیدات شناختی فرایند محور

مقوله‌ها		کدهای مفهومی	مصاحبه‌شونده	نمونه گزاره‌های کلامی
منابع تهدید	فرهنگ‌سازمانی ضد خلاقیت	برخورد با اقدامات متهورانه/ ترس از بازخورد منفی/ فعالیت گروهی ضعیف/ ترس ارائه نظر/ عدم خلاقیت در گردآوری اطلاعات/ عدم خلاقیت تحلیل داده‌ها/ نبود مشوق‌های خلاقیت/ ریسک ادراک‌شده بالای خلاقیت/	۸-۷-۵	خلاقیت، هم در بخش گردآوری اطلاعات، هم در بخش تجزیه‌وتحلیل اطلاعات باعث نتایج جدیدی می‌شود؛ اما چون هم مشوق‌های خلاقیت وجود ندارد و هم ارائه راهکارهای خلاقانه ریسک بالایی برای افراد ممکن است داشته باشد و حمایت سازمانی ممکن است انجام نشود (م.۸).
	ساختار سازمانی سلسله مراتبی	عدم تناسب ساختار سازمانی با گستره صحنه عملیاتی/ تأخیر در ابلاغ مأموریتی دستور دهی/ تأثیر سلایق فردی/ کاهش سرعت گردش اطلاعات/ محدودیت دسترسی/	۸-۵-۳	بخش‌های معاونت تناسبی با گستردگی صحنه اطلاعات ندارند (ازنظر نفرات و تجهیزات) روش‌های اطلاعاتی به‌روز نبوده، از استانداردهای جهانی بسیار فاصله دارد و عموماً. (م. ۸).

مقوله‌ها		کدهای مفهومی	مصاحبه‌شونده	نمونه گزاره‌های کلامی
	ضعف در فناوری‌های نوین گردآوری و تحلیل داده‌ها	عدم استفاده از هوش مصنوعی/ ضعف در فناوری-های جدید/ ضعف در تشخیص اطلاعات غلط/ یادگیری ماشین/ ناتوانی در تشکیل پایگاه‌های کلان داده/ عدم به‌کارگیری تصمیم‌یارها/ محدودیت در تحلیل کلان داده‌ها و فراداده‌ها/ عدم دسترسی به اطلاعات رمزگذاری شده/ گسترش فضای وب و عدم دسترسی/	۸-۷-۶-۵-۳-۲-۱-	با توجه به پیشرفت گسترده و مداوم علم و فناوری و ارتقاء توانمندی‌های سازمان‌های امنیتی و سرویس‌های اطلاعاتی حریف جمع‌آوری اخبار و اطلاعات از دشمن در حوزه‌های مختلف پیچیده شده و نیازمند پیشرفت و فعالیت دستگاه‌های اطلاعاتی خودی بر اساس فنّاوری‌های روز و شرایط حاکم در کشورهای مختلف هست (۵).
	روش‌های سنتی اطلاعاتی	به‌روز نبودن روش‌های اطلاعاتی/ اتکا به روش‌های سنتی/ استفاده از شیوه‌ها و شگردهای قدیمی/ عدم تغییرات ساختارمند در سامانه‌ها/ فرسودگی زیرساخت‌ها/ تبعیت مطلق از ساختارهای سنتی/	۵-۸-۱-۶-۴	سامانه‌های جمع‌آوری و تحلیل اطلاعات در چارچوب طرح-های کوتاه‌مدت، میان‌مدت و بلندمدت باید نوسازی شود. روش‌های اطلاعاتی به‌روز نبوده، از استانداردهای جهانی بسیار فاصله دارد (م.۸).
	اضافه‌بار اطلاعاتی	انتشار حداکثری اطلاعات/ تعدد منابع خبری/ فیلتر ضعیف اطلاعات/ ارائه حجم عظیمی از اطلاعات غیرکاربردی/ حجم زیاد اطلاعات/ بمباران اطلاعاتی/ عدم کاهش حجم اطلاعات ورودی/ پایین آمدن راندمان کار/ اطلاعات گسترده و مبهم/	۵-۱-۳-۶-۴-۷-۸	رویکرد افشا و انتشار حداکثری اطلاعات که امروزه بر مجامع مختلف در جهان حاکم است حجم عظیمی از خبرها را حد منابع آشکار به جریان می‌اندازد لذا این منابع به شرطی که تحلیل‌گر ابزار و فناوری لازم داشته باشد (م.۸).
	اطلاعات فریب‌دهنده	فریب و جعل اطلاعات/ اتکا به منابع آشکار/ اطلاعات غلط و منحرف‌کننده/ غافلگیری/ تحمیل هزینه/	۱-۷-۵-۴	دریافت اطلاعات غلط و یا منحرف‌کننده از سوی سرویس‌های بیگانه به‌منظور، غافلگیری تحمیل هزینه و با

مقوله‌ها		کدهای مفهومی	مصاحبه‌شونده	نمونه گزاره‌های کلامی
		فریب هدفمند رسانه‌ای/ انحراف سامانه اطلاعاتی/ مسموم سازی و مشغول سازی سامانه/ اطلاعات اشتباه و غلط/ وجود منابع کاذب و گسترده داده‌ای/ اطلاعات دست‌کاری و مهندسی‌شده/		دست‌یابی به شیوه و شگردها خودی در مواجه با این‌گونه اطلاعات صورت می‌گیرد لذا به‌منظور خنثی‌سازی این مهم بایستی راستی آزمایی و چک ضد جاسوسی پیرامون عوامل و منابع اخبار و اطلاعات همواره در دستور کار باشد (م.۵).
	عدم دسترسی به‌موقع به اطلاعات	بخش‌بندی غیرضروری داده-ها/ تأخیر در دسترسی به اطلاعات پنهان/ طولانی شدن روند جمع‌آوری و تحلیل/ ساختاری سلسله مراتبی/ طبقه‌بندی بیش‌ازحد اطلاعات/ طولانی شدن اقدامات ارجحیت دار/	۸-۱-۶-۵-۳-۲	طولانی شدن روند گردش اطلاعات ممکن است زمان را برای انجام اقدامات ارجحیت دار از دست بدهیم. این امر تنها یک مانع به شمار می‌آید که دسترسی را به تأخیر می‌اندازد (م.۸).
	شرایط عدم قطعیت	ابهام و عدم قطعیت/ گستردگی و پیچیدگی عصر اطلاعات/ گسترش عملیات نامتقارن اطلاعات/ شرایط و موقعیت مبهم/ محیط گنگ پیچیده مدرن/	۸-۱	بروز این امر عادی و یکی از پیش‌آمده‌ای روزمره در روند کار تحلیل‌گر به شمار می‌آید، چراکه تمامی اطلاعات به‌گونه‌ای ابهام دارند و نمی‌توان به قطع صحت آن‌ها را تأثیر نمود. (م.۸).
	فشار کاری	عدم واگذاری وظایف به سامانه‌ها/ گستردگی کارها/ تخصصی نبودن وظایف/ موازی کاری/ فقدان افسران متخصص شناختی/ حجم زیاد کار/ محدودیت زمانی/ پراکندگی وظایف و کارها/ فشار کاری/	۸-۵-۱-۲	اما متأسفانه بخش اعظم کار اطلاعاتی را که سامانه‌ها باید انجام بدهند ما بر عهده منابع انسانی گذاشتیم که باعث خستگی ذهنی، فرسودگی ذهنی پیش از موقع، خطا در تحلیل‌های اطلاعاتی و غیره شده است (م.۷).
پیامدها	خطای نتیجه‌گیری	کیفیت پایین خروجی/ تحلیل اشتباه/ ارائه گزارش ناقص/ نتیجه‌گیری ناقص/ خطای استدلال/ خطا در	۳-۸-۵	سرعت و گستردگی کار در خوش‌بینانه‌ترین حالت موجب ارائه گزارش ناقص می‌گردد در حالت‌های بدتر گزارش اشتباه

مقوله‌ها		کدهای مفهومی	مصاحبه‌شونده	نمونه گزاره‌های کلامی
		تحلیل‌های اطلاعاتی/ نتیجه‌گیری‌های سطحی/ تحلیل‌های نادقیق/		و گمراه شدن دریافت‌کننده گزارش نتیجه چنین وضعیتی خواهد بود (م.۸).
	اختلال در تمرکز	اضطراب کاری/ مشغول سازی ذهنی/ سردرگمی ذهنی/ حواس‌پرتی/ ناتوانی در تفکر عمیق/ پریشانی ذهنی/	۷-۴-۸	مواجه با حجم انبوهی از اطلاعات می‌تواند موجب بروز اضافه قبا اطلاعاتی شود که تمرکز ذهنی افسران اطلاعاتی را به‌هم‌ریخته و دچار سردرگمی خواهد کرد (م.۷).
	خستگی شناختی	تحلیل تدریجی انرژی ذهنی/ اتلاف انرژی ذهنی/ خستگی ذهنی/ فرسودگی ذهنی پیش از موقع/ خستگی افسران اطلاعاتی/ فشار فکری	۷-۶-۸	همان‌طور که گفتم شما در اوایل فرایند شاید انرژی کافی داشته باشید اما به‌تدریج این انرژی تحلیل می‌رود و درواقع حجم عظیم اطلاعات باعث تحلیل ذهنی می‌شود و کم‌کم قدرت تصمیم‌گیری ضعیف شده و خستگی را افزایش می‌دهد (م.۷).
	خطای تصمیم-گیری	گمراه شدن دریافت‌کننده اطلاعات/ تصمیم‌گیری یک‌سویه/ تصمیم‌گیری با ریسک بالا/ تضعیف قدرت تصمیم‌گیری/ تصمیم‌گیری هیجانی/ کانالیزه شدن ذهن کارشناس/	۷-۸-۳-۱	سرعت و گستردگی کار در خوش‌بینانه‌ترین حالت موجب ارائه گزارش ناقص می‌گردد در حالت‌های بدتر گزارش اشتباه و گمراه شدن دریافت‌کننده گزارش نتیجه چنین وضعیتی خواهد بود (م.۸).

یافته‌های سه سطح نشان می‌دهد که:

- سطح فردی شامل ضعف‌ها و سبک‌های ذهنی است که بر تحلیل اطلاعات اثر مستقیم دارند؛
- سطح فناوری شامل تهدیدات ناشی از ابزارها، داده‌ها و سیستم‌های نوین است؛
- سطح فرایندی شامل تهدیدات ناشی از ساختار، فرهنگ و جریان اطلاعات در سازمان است.

این داده‌ها نشان می‌دهد که سه سطح تهدیدات نه‌تنها مستقل نیستند، بلکه بر یکدیگر اثر متقابل دارند.

بحث و نتیجه‌گیری

یافته‌های این پژوهش نشان داد که تهدیدات شناختی در سه سطح فردی، فناوری‌محور و فرایندی بروز می‌یابند و این سه سطح دارای اثرات متقابل‌اند؛ بنابراین تحلیل آن‌ها باید در چارچوب نظام شناختی سازمان اطلاعاتی نظامی انجام شود.

تهدیدات فردمحور شامل سوگیری‌های ذهنی، سبک تصمیم‌گیری تکانشی، خستگی شناختی، تمرکز ضعیف و عدم انعطاف‌پذیری ذهنی است. این الگو کاملاً با نظریه‌های کانمن (۲۰۱۱)، آریلی (۲۰۱۲) و مدل‌های تصمیم‌گیری تحت فشار مطابقت دارد. چرایی بروز این تهدیدات شامل؛ فشار زمانی عملیات اطلاعاتی، اضافه‌بار اطلاعاتی، ساختار سازمانی سلسله‌مراتبی و نبود سازوکارهای یادگیری شناختی هستند.

این ضعف‌ها باعث کاهش دقت تحلیل، اختلال در تشخیص الگوهای پنهان و افزایش خطای پیش‌بینی می‌شود. این روند در ادبیات جنگ شناختی به‌عنوان «ناپایداری شناختی تحلیلگر» شناخته می‌شود.

فناوری‌های نوین مانند هوش مصنوعی، تحلیل کلان‌داده‌ها، رابط‌های مغز–رایانه و مدل‌های محاسبات شناختی علاوه بر ایجاد فرصت، تهدیدات عمیقی را نیز به وجود می‌آورند. این تهدیدات با ادبیات «جنگ شناختی نسل ششم ناتو»، گزارش‌های فرانسوا دوکلوزل (۲۰۲۱) و پژوهش‌های اخیر درباره «ایمپلنت‌های شناختی» همخوان است. چرایی بروز تهدیدات فناوری‌محور شامل؛ وابستگی شناختی بیش‌ازحد به خروجی الگوریتم‌ها، نبود پایگاه داده پاک‌سازی‌شده، ضعف آگاهی کارکنان از خطرات شناختی فناوری و امکان فریب شناختی از طریق داده‌های آلوده هستند.

نتیجه این فرایند، کاهش استقلال تحلیلگر و شکل‌گیری «گسست شناختی انسان–ماشین» است؛ پدیده‌ای که در پژوهش‌های اخیر ناتو به‌عنوان خطر اصلی جنگ شناختی دهه آینده معرفی شده است. تهدیدات فرایندی شامل ساختار سلسله‌مراتبی، روش‌های سنتی تحلیل اطلاعات، نبود سامانه‌های هوشمند، اضافه‌بار اطلاعاتی، ضعف فیلتر اطلاعات و فشار کاری است. این یافته‌ها با نظریه «خطای فرایندی» در سازمان‌های اطلاعاتی و ادبیات «تفکر سازمانی در شرایط عدم قطعیت» مطابقت دارد. چرایی تهدیدات فرایندی

را می‌توان عدم نوسازی روش‌ها شکاف میان فناوری‌های نوین و رویه‌های سنتی، نبود پایگاه داده یکپارچه، فاصله میان بخش‌های عملیاتی و تحلیلی و نبود چرخه بازخورد یادگیرنده در نظر گرفت. این تهدیدات موجب شکل‌گیری «فرسایش شناختی سازمانی» می‌شود؛ یعنی سازمان به‌تدریج توانایی تحلیل عمیق و تصمیم‌سازی هوشمند را از دست می‌دهد. تحلیل بین‌سطحی نیز نشان داد که ضعف فردی، استفاده ناصحیح از فناوری را افزایش می‌دهد؛ نقص فناوری، سوگیری شناختی تحلیلگر را تشدید می‌کند و ناکارآمدی فرایندی، خستگی و خطای فردی را تقویت می‌کند. این تعاملات باعث ایجاد چرخه «بازخورد منفی شناختی» می‌شود که در ادبیات نظامی به‌عنوان خطر اصلی «شکست اطلاعاتی» شناخته می‌شود.

این نتایج با الگوی «مثلث شناختی انسان–فناوری–فرایند» که توسط کوچک‌سازی فرماندهی ناتو ارائه شده است، همخوان است.

این پژوهش نشان داد که تهدیدات شناختی در یک سازمان اطلاعاتی نظامی، پدیده‌ای چندسطحی، مرتبط و پویا هستند و نمی‌توان آن‌ها را به‌صورت مجزا مدیریت کرد. سه سطح تهدیدات شامل فردمحور، فناوری‌محور و فرایندمحور نه‌تنها مستقل عمل نمی‌کنند، بلکه در یک چرخه تقویت‌کننده منفی قرار دارند. مهم‌ترین پیامدهای کلیدی پژوهش شامل:

- تهدیدات فردی منجر به افزایش خطای تحلیل، کاهش دقت ارزیابی تهدیدات و ضعف در تصمیم‌گیری می‌شوند.
- تهدیدات فناوری‌محور می‌توانند شناخت انسان را منحرف کرده و موجب گسست شناختی انسان–ماشین شوند.
- تهدیدات فرایندی زمینه اصلی فرسایش شناختی سازمانی و کاهش سرعت تصمیم‌سازی در شرایط بحرانی هستند.
- تعامل این سه سطح، خطر «شکست اطلاعاتی» در سازمان را تشدید می‌کند.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱. گنجاندن مفهوم پدافند شناختی در اسناد بالادستی دفاعی کشور: ضرورت دارد در اسناد امنیت ملی و راهبرد دفاعی، بخش مستقلی به امنیت و پدافند شناختی اختصاص یابد.

۲. تأسیس «مرکز ملی دفاع شناختی» در ساختار پدافند غیرعامل: این مرکز می‌تواند با مأموریت هماهنگی میان نهادهای نظامی، اطلاعاتی، علمی و فناوری برای مقابله با تهدیدات شناختی فعالیت کند.
۳. توسعه همکاری‌های میان‌رشته‌ای بین علوم شناختی و امنیتی: برگزاری دوره‌ها و پروژه‌های مشترک میان دانشگاه‌های نیروهای مسلح
۴. ایجاد نظام ملی رصد تهدیدات شناختی: برای شناسایی زودهنگام روندهای فریب ادراکی، حملات شناختی و جنگ رسانه‌ای علیه ساختار دفاعی کشور.
۵. حمایت از تولید دانش بومی در حوزه شناخت دفاعی: اختصاص بودجه پژوهشی به پروژه‌های آینده‌پژوهی دفاع شناختی، تحلیل داده‌های مغزی و طراحی فناوری‌های ضد فریب شناختی.

تشکر و قدردانی

نویسندگان این مقاله از تمامی افرادی که در تهیه و انتشار این مقاله به‌ویژه سردبیر محترم نشریه و داوران این مقاله مؤثر بوده‌اند قدردانی می‌نمایند.

تعارض منافع:

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

منابع و مأخذ

- رضایی، محمد و نادری، امیر. (۱۴۰۱). *تحلیل تهدیدات شناختی در نظام تصمیم‌سازی امنیت ملی*. فصلنامه مطالعات راهبردی امنیت، ۱۴ (۲)، ۱۲۰–۱۴۵.
- رستمی، سعید؛ فلاح‌پور، مهدی و جلالی، حسن. (۱۴۰۲). *پدافند شناختی و تهدیدات ترکیبی در فضای اطلاعاتی ایران*. فصلنامه پدافند غیرعامل، ۱۱ (۳)، ۸۰–۱۰۲.
- فتحی، علی و مظفری، محمد. (۱۴۰۲). *تحلیل تطبیقی تهدیدات شناختی در سازمان‌های نظامی و رسانه‌ای*. فصلنامه آینده‌پژوهی دفاعی، ۵ (۱)، ۵۵–۷۸.
- کاظمی، احمد و نصراللهی، رضا. (۱۴۰۱). *چالش‌های شناختی در تصمیم‌سازی نظامی: رویکردی میان‌رشته‌ای*. مجله دفاع ملی، ۱۸ (۲)، ۹۵–۱۱۸.

- طالبی, مرتضی و محجوب عشرت آبادی, حسن. (۱۴۰۳). زیست‌بوم آمادگی شناختی دفاع سایبری. *آینده‌پژوهی دفاعی*, ۹(۳۴), ۱۴۷-۱۸۲. doi: (۱۰.۲۲۰۳۴/dfsr.۲۰۲۴.۲۰۴۳۱۰۵.۱۸۳۸)
- محجوب عشرت‌آبادی، حسن. (۱۴۰۰). *عرصه شناختی جنگ و تهدیدات نوین در امنیت ملی ایران*. فصلنامه راهبرد دفاعی، ۲۱ (۴)، ۴۵–۶۸.
- مؤسسه مطالعات راهبردی دفاعی. (۱۳۹۹). *گزارش پژوهشی: تهدیدات شناختی در جنگ‌های نوین*. تهران: معاونت پژوهش‌های دفاعی.
- وزارت دفاع و پشتیبانی نیروهای مسلح. (۱۴۰۲). *چارچوب نظری پدافند شناختی در جمهوری اسلامی ایران*. تهران: اداره کل آینده‌پژوهی دفاعی.
- Bigler, E. D. (2016). Systems biology, neuroimaging, neuropsychology, neuroconnectivity and traumatic brain injury. *Frontiers in Systems Neuroscience, 10*(55). (https://doi.org/10.3389/fnsys.2016.00055)
- Buchanan, V. & Cooke, N. J. (2015). The cognitive science of intelligence analysis. *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting*, 826–830. (https://doi.org/10.1177/1541931215591179)
- Carrubba, S. Frilot, C. Chesson, A. L. Jr. et al. (2010). Numerical analysis of recurrence plots to detect effect of environmental-strength magnetic fields on human brain electrical activity. *Medical Engineering & Physics, 32*(8), 898–907. (https://doi.org/10.1016/j.medengphy.2010.06.006)
- Chairman of the Joint Chiefs of Staff. (2017). *Joint planning* (Joint Publication 5-0). Washington, DC: Chairman of the Joint Chiefs of Staff.
- Chan, P. Ho, K. & Ryan, A. F. (2016). Impulse noise injury model. *Military Medicine, 181*(Suppl 5), 59–69. (https://doi.org/10.7205/MILMED-D-15)
- Du Cluzel, F. (2020). *Cognitive Warfare 2020*. Innovation Hub, June–November 2020.
- Du Cluzel, F. (2021). Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries. *Monthly Review Online*. Retrieved October 13, 2021, from (https://mronline.org/2021/10/13/behind-natos-cognitive-warfare-battle-for-your-brain-waged-by-western-militaries)
- Esser, S. K. Merolla, P. A. Arthur, J. V. et al. (2016). Convolutional networks for fast, energy-efficient neuromorphic computing.

Proceedings of the National Academy of Sciences of the United States of America, 113(41), 11441–11446. (https://doi.org/10.1073/pnas.1604850113)

- Extance, A. (2015). Military technology: Laser weapons get real. *Nature, 521*, 408–410. (https://doi.org/10.1038/521408a)
- Fathi, A. & Mozaffari, M. (2023). *A comparative analysis of cognitive threats in military and media organizations*. Defensive Futures Studies Quarterly, **5**(1), 55–78.(IN PERSIAN)
- Frégnac, Y. & Laurent, G. (2014). Neuroscience: Where is the brain in the human brain project? *Nature, 513*, 27–29. (https://doi.org/10.1038/513027a)
- Hargrove, L. J. Young, A. J. Simon, A. M. et al. (2015). Intuitive control of a powered prosthetic leg during ambulation: A randomized clinical trial. *JAMA, 313*(22), 2244–2252. (https://doi.org/10.1001/jama.2015.4527)
- Hutchins, S. G. Pirolli, P. L. & Card, S. K. (2007). What makes intelligence analysis difficult? A cognitive task analysis of intelligence analysts. Naval Postgraduate School, Monterey, CA.
- Heuer, R. J. & Pherson, R. H. (2023). *Structured analytic techniques for intelligence analysis* (3rd ed). CQ Press.
- Hoge, C. W. McGurk, D. Thomas, J. L. et al. (2008). Mild traumatic brain injury in U.S. soldiers returning from Iraq. *New England Journal of Medicine, 358*(5), 453–463. (https://doi.org/10.1056/NEJMoa072972)
- Ivany, C. G. & Hoge, C. W. (2016). Suicide attempts in the U.S. Army. *JAMA Psychiatry, 73*(2), 176. (https://doi.org/10.1001/jamapsychiatry.2015.2363)
- Jin, H. Hou, L. J. & Fu, X. B. (2015). Medical rescue of naval combat: Challenges and future. *Military Medical Research, 2*(21). (https://doi.org/10.1186/s40779-015-0048-z)
- Jung, Y. Kwak, J. H. Kang, H. et al. (2015). Mechanical and electrical characterization of piezoelectric artificial cochlear device and biocompatible packaging. *Sensors (Basel), 15*(8), 18851–18864. (https://doi.org/10.3390/s150818851)
- Kania, E. (2019). Minds at war: China's pursuit of military advantage through cognitive science and biotechnology. *PRISM, 3*, 83–101.

- Kazemi, A. & Nasrollahi, R. (2022). *Cognitive challenges in military decision-making: An interdisciplinary approach*. National Defense Journal, **18**(2), 95–118.(IN PERSIAN)
- Ljungqvist, J. Zetterberg, H. Mitsis, M. et al. (2017). Serum neurofilament light protein as a marker for diffuse axonal injury: Results from a case series study. *Journal of Neurotrauma, 34*(6), 1124–1127. (https://doi.org/10.1089/neu.2016.4496)
- Kaunonen, A. (2019). *Cognitive biases within intelligence analysis - A case study within selected teams in the tactical level of the land component* (Master's thesis). Finnish National Defense University, Helsinki.
- Mandel, D. R. & Irwin, D. (2024). Beyond bias minimization: Improving intelligence with optimization and human augmentation. *International Journal of Intelligence and CounterIntelligence, *37*(2), 649–665. (https://doi.org/10.1080/08850607.2023.2253120)
- Mahjoob Eshratabadi, H. (2021). *The cognitive domain of warfare and emerging threats in Iran's national security*. Defensive Strategy Quarterly, **21**(4), 45–68.(IN PERSIAN)
- Merolla, P. A. Arthur, J. V. Alvarez-Icaza, R. et al. (2014). Artificial brains: A million spiking-neuron integrated circuit with a scalable communication network and interface. *Science, 345*(6197), 668–673. (https://doi.org/10.1126/science.1254642)
- Ministry of Defense and Armed Forces Logistics. (2023). *The theoretical framework of cognitive defense in the Islamic Republic of Iran*. Tehran: General Directorate of Defense Futures Studies.(IN PERSIAN)
- National Research Council (US) Committee. (2008). *Military and intelligence methodology for emergent neurophysiological and cognitive/neural research in the next two decades*. Washington, DC: National Academies Press.
- NASA. (2020). *Explore moon to Mars*. Retrieved February 2, 2020, from (https://www.nasa.gov/topics/moon-to-mars/lunar-gateway)
- Norton, B. (2021). Behind NATO's 'cognitive warfare': 'Battle for your brain' waged by Western militaries. Retrieved October 13, 2021, from (https://mronline.org/2021/10/13/behind-natos-cognitive-warfare)

- Rezaei, M. & Naderi, A. (2022). *Analysis of cognitive threats in the national security decision-making system*. Strategic Security Studies Quarterly, 14(2), 120–145.(IN PERSIAN)
- Rostami, S. Fallahpour, M. & Jalali, H. (2023). *Cognitive defense and hybrid threats in Iran's information space*. Passive Defense Quarterly, **11**(3), 80–102.(IN PERSIAN)
- Roco, M. C. & Bainbridge, W. S. (2003). *Converging technologies for improving human performance: Nanotechnology, biotechnology, information technology, and cognitive science (NBIC)*. Washington, DC: National Science Foundation.
- Strategic Defense Studies Institute. (2020). *Research report: Cognitive threats in modern warfare*. Tehran: Deputy for Defense Research.(IN PERSIAN)
- Talebi, M. & Mahjoob Eshratabadi, H. (2024). *The ecosystem of cognitive readiness in cyber defense*. Defensive Futures Studies, **9**(34), 147–182. https://doi.org/10.22034/dfsr.2024.2043105.1838(IN PERSIAN)
- U.S. Department of Defense. (2023). *Joint publication 2-0: Joint intelligence*. Washington, DC: Office of the Chairman of the Joint Chiefs of Staff.
- U.S. Space Force. (2019). *Fact sheet*. Retrieved February 2, 2020, from (https://www.spaceforce.mil/About-Us/Fact-Sheet)
- Zanasi, A. & Ruini, F. (2018). IT-induced cognitive biases in intelligence analysis: Big data analytics and serious games. *International Journal of Safety and Security Engineering*, *8*(3), 438–450.(https://doi.org/10.2495/SAFE-V8-N3-438-450)