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

Identifying and prioritizing emerging information-communication technological drivers effective in Iran's defense security 2035

Khalil Koulivand[1]| **Morteza Anooshe**[2]✉| **Mohammad Anisseh**[3]| **Aziz Nasirzade**[4]

1- PhD Student in Futures Studies, Imam Khomeini International University, Qazvin, Iran. Email: K.Koulivand@edu.ikiu.ac.ir
2- Assistant Professor of Industrial Management, Imam Khomeini International University, Qazvin, Iran. (Corresponding Author) Email: anoosheh@soc.ikiu.ac.ir
3- Assistant Professor of Industrial Management, Imam Khomeini International University, Qazvin, Iran. Email: m.anisseh@soc.ikiu.ac.ir
4- Associate Professor of Defense Management, Command and Staff University of the Islamic Republic of Iran Army, Tehran, Iran. Email: Iran.az.nasir1402@gmail.com

Article Info

Article type:
Research Article

Article history:
Received:
2025-9-27
Received in revised form:
2025-12-4
Accepted:
2025-12-19
Published online:
2026-5-22

Keywords:
Drivers, Emerging Information-Communication Technologies, Defense Security, Wilson Matrix, Metasynthesis.

ABSTRACT

Background and Objective: The rapid developments of emerging information and communication technologies have brought about profound transformations in the structure and function of national defense and security systems. Accordingly, the percies identification of key drivers influencing the defense security of the Islamic Republic of Iran by the horizon of 2035 is regarded as a strategic imperative for future-oriented policymaking and decision-making.

Methods: The present study is a longitudinal survey in terms of applied purpose, data collection in terms of mixed methods, and was conducted by focusing on qualitative futures research methods and quantitative data analysis methods using meta-synthesis of related studies and documents, Delphi, and interaction analysis using the Wilson matrix. The community of experts and experts participating in this study are 27 academic experts, managers, and senior experts in the defense and security fields.

Findings: Based on the meta-synthesis of the studies, 22 initial drivers were identified, and 11 final drivers were extracted by integrating their thematic and conceptual dimensions. The final categorization of these drivers into four structural groups: groups-key, interactive, dependent, and emerging-revealed that a considerable number of them exhibit nonlinear and overlapping characteristics, which must be taken into account in the design of future scenarios.

Conclusions: The findings indicate that emerging information and communication technologies, particularly those related to artificial intelligence, big data, virtual reality, cybersecurity, and fifth and sixthgeneration telecommunication infrastructures-will play a pivotal role in redefining the defense and security landscape of the country in the future.

Cite this article: Koulivand, Kh. Anooshe, M; Aniseh, M; and Nasirzadeh, A (2025). Identifying and prioritizing emerging information-communication technological drivers effective in Iran's defense security 2035. *Defensive Future Studies*, 11 (40),159-202.

DOI: https://doi.org/10.22034/dfsr.2025.2067124.1927

Publisher: IRI Military Command and Staff University

Extended abstract

INTRODUCTION

The rapid developments of emerging information and communication technologies over recent decades is regarded as one of the most significant factors in redefining traditional concepts of power, security, and defense within global political and military systems. These technologies have fundamentally transformed the nature of defense decision-making, command and control, and even deterrence strategies by reshaping the mechanisms of data collection, analysis, and transmission of data (Doicariu, 2023). Meanwhile, countries such as the Islamic Republic of Iran, facing complex, multi-level, and cognitive threats, require technological foresight more than ever to preserve information superiority and strengthen national security. Therefore, analyzing the driving forces of emerging information and communication technologies is a crucial prerequisite for formulating defense strategies and designing future scenarios for the 2035 horizon; an endeavor that can provide a scientific and forward-looking foundation for the nation's defense policy-making.

METHODOLOGY

The present study is designed with a specific purpose and employs a longitudinal survey with a mixed-methods approach to data collection. The research was conducted based on a forward-looking logic, combining document meta-synthesis, the Delphi method, and interaction analysis using the Wilson matrix. The statistical population consisted of 27 defense-security and ICT experts, each with at least five years of specialized experience in defense security future analysis, selected through purposive sampling. The content validity of the research instrument was verified through expert evaluation, and its reliability, big data, machine learning, and quantum computing.) and communication technologies (including 5G/6G, the Internet of Things, blockchain, and advanced satellite communications) were examined separately. The influential effective drivers of each category and their levels of uncertainty within the 2035 horizon were then measured and prioritized using specific indicators.

RESULT

The research findings derived from the meta-synthesis and fuzzy Delphi process provide a systematic understanding of the key drivers of emerging technologies shaping the defense security of the Islamic Republic of Iran through 2035. In the first phase, a systematic review of international scientific literature from 2015 to 2025, along with thematic analysis based on the seven-stage model of Sandelowski and Barroso, led to the identification of 22 initial drivers, organized into basic, organizing, and overarching themes. These drivers encompassed diverse areas such as artificial intelligence, the military Internet of Things, network-centric command, cybersecurity, quantum communications, virtual reality, big data, cognitive warfare, security biotechnology, and technological-geopolitical developments. Subsequently, through thematic synthesis and according to the criteria of functional alignment, technological commonality, and strategic convergence, 11 major mega-drivers were extracted from the conceptual integration of these themes. These macro-drivers represent the synergistic technological trends that are expected to shape the transformation of future defense architectures, including digital integration and network-centric command, the expansion of military artificial intelligence, the strategic use of big data, the evolution of cognitive warfare, and the development the evolution of next-generation communications infrastructures.

In the second phase, the findings from the meta-synthesis were validated through a two-round Delphi process involving experts in the futures studies. In this stage, the degree of influence and uncertainty of each driver within the 2035 horizon was assessed using a five-point Likert scale and the interquartile range (IQR) index. The results indicated a significant increase in expert consensus during the second round, leading to the identification of a set of key drivers with the highest levels of influence and importance. The final analysis, conducted using Wilson's interaction effects matrix, identified four main categories of drivers: interactive, key, dependent, and emerging. The findings revealed that the four drivers located in the interactive quadrant (such as military artificial intelligence and cognitive warfare) possess the greatest potential to generate paradigmatic and nonlinear transformations; three key drivers (including telecommunications infrastructure and network-based command) constitute the core of the future defense architecture. Two dependent drivers are more structural in nature, while two emerging drivers, although relatively less significant individually, may exert disruptive effects

on national security when combined with other technological trends. Overall, these findings offer a comprehensive perspective on the system of drivers shaping the future of Iran's defense security and establish a theoretical foundation for designing forward-looking scenarios and policies toward 2035.

DISCUSSION and CONCLUSIONS

The research findings indicate that emerging information and communication technologies, particularly military artificial intelligence, machine learning, big data, cybersecurity, and next-generation communication systems, will play a pivotal role in redefining the defense security paradigms of the Islamic Republic of Iran by the 2035 horizon. These technologies are expected to enhance the efficiency and agility of defense forces in complex and multidimensional environments by strengthening command intelligence, accelerating data-driven decision-making, and developing network-centric infrastructure. The results suggest that future security will increasingly rely on knowledge, information, and network capital rather than solely on hardware power capabilities. The Convergence of information and communication technologies with artificial intelligence, cognitive warfare, and digital command represents the most significant driver of transformation in the defense sector, profoundly affecting decision-making structure, training, and cybersecurity. Comparisons with domestic and international literature, including the studies of Movahedi-Sefat (2023), Azar and Moslemi (2024), Ahmadi et al. (2023), and RAND Institute reports, confirm the alignment of these findings with the global trend toward smart, forward-looking defense strategies. The primary contribution of this study lies in elucidating interactions between technologies and analyzing synergies across the information, communication, and cognitive domains, which may lead to a redistribution of power in future security environments. Despite limitations such as the lack of transparency of global trends and insufficient local data, the results are deemed highly generalizable for the Iranian defense system. Overall, this research provides a robust scientific foundation for formulating defense technology policies, designing future scenarios, and enhancing the nation’s strategic resilience against emerging technological threats.

ACKNOWLEDGEMENTS

Acknowledgments could be placed at the end of the text, but before the references.

REFERENCES

1. Ahmadi, A. Zargar, A. & Adami, A. (2023). Artificial Intelligence Technology and Change in the National Security of States. Defense Policy, 32(123),39-64, **[In Persian]**. (https://dor.isc.ac/dor)
2. Azar, D. and Moslemi, H. (2024). The pillars of the cyber power of the Islamic Republic of Iran Army. *Quarterly Journal of Interdisciplinary Studies on Strategic Knowledge*, *14*(56),131-111, **[In Persian]**. (https://smsnds.sndu.ac.ir/article_3084.html)
3. Doicariu, D. (2023). Emerging and disruptive technology trends in defense and security. *Journal of Defense Resources Management* (JoDRM), 14(2), 33-44. (https://www.ceeol.com/search/article-detail?id=1197967)
4. Movahhedi Sefat, M. Sepehri, M. Halili, K. and Farzaneh, A. (2023). Smart defense model based on Internet of Things technology. *Strategic Defense Studies*, *21*(92), 69-92, **[In Persian]**. (https://sds.sndu.ac.ir/article_2421.html)

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

شناسایی و اولویت‌بندی پیشران‌های فناورانه نوظهور اطلاعاتی – ارتباطی مؤثر در امنیت دفاعی ایران ۱۴۱۴

خلیل کولیوند[۱]، مرتضی انوشه[۲]✉، محمد انیسه[۳]، عزیز نصیرزاده[۴]

۱- دانشجوی دکترای آینده‌پژوهی، دانشگاه بین‌المللی امام خمینی (ره)، قزوین، ایران. رایانامه: K.Koulivand@edu.ikiu.ac.ir

۲- استادیار مدیریت صنعتی، دانشگاه بین‌المللی امام خمینی (ره)، قزوین، ایران. (نویسنده مسئول) رایانامه: anoosheh@soc.ikiu.ac.ir

۳- استادیار مدیریت صنعتی، دانشگاه بین‌المللی امام خمینی (ره)، قزوین، ایران. رایانامه: m.anisseh@soc.ikiu.ac.ir

۴- دانشیار مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: Iran.az.nasir۱۴۰۲@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:

تاریخ دریافت:
۱۴۰۴/۰۷/۰۵

تاریخ بازنگری:
۱۴۰۴/۰۹/۱۳

تاریخ پذیرش:
۱۴۰۳/۰۹/۲۸

تاریخ انتشار:
۱۴۰۵/۰۳/۰۱

کلیدواژه‌ها:
پیشران، فناوری‌های نوظهور اطلاعاتی-ارتباطی، امنیت دفاعی، ماتریس ویلسون، فراترکیب.

چکیده

زمینه و هدف: تحولات شتاب‌گیر فناوری‌های نوظهور اطلاعاتی–ارتباطی، ساختارها و عملکردهای امنیت دفاعی کشورها را با دگرگونی‌های عمیق مواجه کرده‌اند، از این‌رو شناخت دقیق پیشران‌های کلیدی و اثرگذار بر امنیت دفاعی جمهوری اسلامی ایران در افق ۱۴۱۴، ضرورتی راهبردی برای سیاست‌گذاری و تصمیم‌سازی آینده‌نگرانه محسوب می‌شود.

روش‌ها: پژوهش حاضر از نظر هدف کاربردی، از نظر گردآوری داده‌ها پیمایشی طولی و از نظر روش آمیخته است که با تمرکز بر روش‌های کیفی آینده‌پژوهی و روش‌های کمّی تحلیل داده‌ها با استفاده از روش‌های فراترکیب مطالعات و اسناد مرتبط، دلفی و تحلیل تأثیر متقابل با استفاده از ماتریس ویلسون انجام شد. جامعه خبرگی و صاحب‌نظران شرکت‌کننده در این پژوهش ۲۷ نفر از خبرگان دانشگاهی، مدیران و کارشناسان ارشد حوزه دفاعی و امنیتی هستند.

یافته‌ها: با توجه به فراترکیب مطالعات انجام شده، ۲۲ پیشران شناسایی شد که با تلفیق موضوعی و مفهومی در نهایت یازده پیشران نهایی استخراج شد. دسته‌بندی نهایی پیشران‌ها در چهار گروه ساختاری کلیدی، تعاملی، وابسته و نوظهور نشان داد که بخش قابل توجهی از پیشران‌ها ماهیت غیرخطی و متداخل داشته و لازم است در طراحی سناریوهای آینده مورد توجه قرار گیرند.

نتیجه‌گیری‌ها: نتایج نشان داد که فناوری‌های اطلاعاتی-ارتباطی نوظهور، به‌ویژه در پیوند با هوش مصنوعی، کلان‌داده، واقعیت مجازی، امنیت سایبری و زیرساخت‌های مخابراتی نسل پنجم و ششم، نقشی بنیادین در بازتعریف امنیت دفاعی کشور در آینده خواهند داشت.

استناد: کولیوند، خلیل؛ انو شه، مرت ضی؛ انی سه، محمد؛ و نـ صیرزاده، عزیز (۱۴۰۴). شنا سایی و اولویت‌بندی پی شران‌های نا شی از فناوری‌های نوظهور اطلاعاتی–ارتباطی مؤثر در امنیت دفاعی ایران ۱۴۱۴. *آینده‌پژوهی دفاعی*، ۱۱ (۴۰)، ۲۰۲-۱۵۹.
https://doi.org/10.22034/dfsr.2025.2067124.1927

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.

مقدمه

در دهه‌های اخیر، شتاب تحولات فناوری، به‌ویژه در حوزه فناوری‌های نوظهور اطلاعاتی-ارتباطی، موجب بازتعریف مفاهیم قدرت، تهدید و امنیت در نظام‌های دفاعی شده (چوری، ۱۴۰۲ و Patil et al, ۲۰۲۴) و تغییر در ابزارها و شیوه‌های جمع‌آوری، پردازش و انتقال داده‌ها، ظرفیت‌های تازه‌ای را در حوزه‌هایی چون فرماندهی و کنترل، جنگ سایبری، عملیات شناختی و تصمیم‌سازی امنیتی ایجاد کرده است (Doicariu, ۲۰۲۳). این شرایط سبب شده تا امنیت دفاعی کشورهایی مانند جمهوری اسلامی ایران که در معرض تهدیدات پیچیده ژئوپلیتیکی، سایبری و شناختی قرار دارند، بیش از پیش نیازمند نگاه آینده‌نگرانه و مبتنی بر رویکرد فناورانه باشند (موسوی شهیدی و همکاران، ۱۴۰۳)، از این رو، رویکرد آینده‌پژوهلنه در حوزه فناوری‌های نوظهور اطلاعاتی-ارتباطی نه‌تنها یک ضرورت علمی، بلکه یک الزام راهبردی است. این موضوع در افق ۱۴۱۴ بر اساس اسناد بالادستی از جمله سند چشم‌انداز جمهوری اسلامی ایران، نقشه جامع علمی کشور و سیاست‌های کلی دفاعی نمود بیشتری می‌یابد (سند جامع علم و فناوری در حوزه دفاعی و امنیتی جمهوری اسلامی ایران، مصوب جلسه ۸۳۷ مورخ ۱۳۹۹/۱۲/۰۵ شورای عالی انقلاب فرهنگی).

اهمیت این پژوهش نیز در این واقعیت نهفته است که نه تنها تحلیل روابط پویا بین فن‌آوری‌های نوظهور اطلاعاتی-ارتباطی و امنیتی-دفاعی را فراهم می‌کند، بلکه تلاش دارد تا پیشران‌های اصلی این حوزه مطالعاتی را شناسایی و زمینه طراحی سناریوهای امنیتی-دفاعی را میسر سازد تا مبنایی برای طراحی سناریوها و سیاست‌های دفاعی باشد. از این‌رو، هدف اصلی پژوهش شناسایی و اولویت‌بندی پیشران‌های فناورانه نوظهور اطلاعاتی – ارتباطی مؤثر در امنیت دفاعی ایران ۱۴۱۴ است. در همین راستا، پژوهش به دنبال پاسخ به این سؤال اصلی است که پیشران‌های فناورانه نوظهور اطلاعاتی – ارتباطی مؤثر در امنیت دفاعی ایران ۱۴۱۴ کدام‌اند و اولویت‌بندی آن‌ها چگونه است؟

مرور پیشینه و مبانی نظری

مرور پیشینه

تحولات پرشتاب و پیچیده فناوری‌های نوظهور اطلاعاتی-ارتباطی در دو دهه گذشته، بسترهای امنیتی و دفاعی را با چالش‌های جدید و ناشناخته مواجه کرده به‌گونه‌ای که این تحولات موجب شده پژوهشگران در حوزه مطالعات امنیتی و آینده‌پژوهی، توجه ویژه‌ای به پیامدهای مستقیم و غیرمستقیم فناوری‌های دیجیتال، هوش مصنوعی، داده‌های بزرگ، محاسبات کوانتومی، اینترنت اشیاء و سامانه‌های شناختی بر ساختارهای دفاعی داشته باشند (Popescu, ۲۰۲۱). در این راستا، بدنه‌ای از ادبیات علمی شکل گرفته که اگرچه تلاش دارند وجوه مختلف این مسئله را بررسی کنند، اما همچنان از حیث شناسایی پیشران‌های کلیدی و تأثیرگذار بر امنیت دفاعی در افق‌های بلندمدت، به‌ویژه در کشورهای در حال توسعه با مختصات ژئوپلیتیکی حساس مانند ایران، با کمبودهای اساسی مواجه‌اند.

در ادبیات داخلی، برخی مطالعات در حوزه تهدیدات سایبری، فناوری‌های نوین و مفاهیم جدید امنیتی انجام شده، در بخش رساله‌ها می‌توان به رساله موحدی صفت (۱۴۰۲) که با تمرکز بر فناوری‌های هوشمند به بازتعریف مفاهیم سنتی امنیت دفاعی پرداخته، اشاره نمود. در این رساله اهمیت داده‌کاوی، یادگیری ماشین و سامانه‌های هوشمند در تحولات آینده امنیتی مورد بررسی قرار می‌گیرد. قنواتی (۱۴۰۲) هم در رساله دکترای خود با رویکرد تدوین مدل بومی توسعه فناوری‌های نوظهور بر مبنای رویکرد نظام نوآوری فناورانه به توسعه فناوری نگاه دارد و با تطبیق وضعیت موجود فناوری در کشور و شناسایی روندهای آینده این فناوری‌ها در دنیا به ارائه سناریوهایی در جهت توسعه تولید افزایشی می‌پردازد.

در حوزه مقالات، تحقیقاتی مانند پژوهش آذر و مسلمی (۱۴۰۳) با محوریت ارکان جهت‌ساز راهبردی قدرت سایبری ارتش جمهوری اسلامی ایران، تأکید دارد که فناوری‌های نوظهور، قابلیت‌ها و توانمندی‌های جدیدی را در اختیار قرار داده و هم‌زمان محیط راهبردی را دچار تغییر نموده است. یا احمدی و همکاران (۱۴۰۲) در پژوهش خود با عنوان «فناوری هوش مصنوعی و تغییر در امنیت ملی دولت‌ها» بر این موضوع تأکید دارند که ظهور هوش مصنوعی و رویکردهای مرتبط با آن، تغییراتی را در تمام

ساحات بشری به وجود آورده و نظام بین‌الملل نیز از آن مستثنا نموده است. همچنین شریف‌زاده و همکارانش (۱۴۰۳) با بررسی آثار سیاست‌های توسعهٔ فناوری‌های نوظهور و هوش مصنوعی در گسترش راهبردهای سیاسی کلان با رویکرد سیاست‌های کلی نظام بر این موضوع صحه می‌گذارند که توسعهٔ فناوری‌های نوین، پیشران قدرتمند در تحولات دیپلماتیک و روابط سیاسی آیندهٔ جهان است. ضمن اینکه محمدی فاتح و ابراهیمی (۱۳۹۹) در پژوهشی که با رویکرد شناسایی به انجام رسیده معتقدند در چند سال اخیر یک نیاز جدی برای فهم اثرات فناوری‌های نوظهور اطلاعاتی با محوریت هوش مصنوعی و اینترنت اشیاء در سازمان‌ها بوجود آمده، هر چند که مساعدت نظری این پژوهش، شناسایی و طبقه‌بندی تعداد ۲۳ فناوری اطلاعاتی نوظهور در دو بُعد تملک فناوری و نوع کاربرد فناوری در بخش دفاعی است، اما عدم توجه به پیشران بودن، عدم قطعیت و تحولات پیچیده صحنه نبردهای آینده فقدانی اساسی برای آن تلقی می‌شود.

از سوی دیگر در سطح بین‌المللی، پژوهش‌های متعددی با محوریت پیامدهای فناوری‌های نوظهور بر ساختارهای امنیتی و جنگ‌های آینده انجام شده از جمله، پژوهش کاپا[1] (۲۰۲۴) با عنوان «نقش فناوری‌های اطلاعات شناختی در امنیت سایبری: سیستم‌های تشخیص تهدید و دفاع تطبیقی» که با تمرکز بر جنگ‌های شناختی با رویکرد فناوری‌های نوظهور، ادغام فناوری‌های اطلاعاتی-ارتباطی را با مبحث علوم اعصاب و رسانه‌های دیجیتال از دلایل اصلی پیچیده‌تر شدن تهدیدات نوظهور قلمداد می‌کند. دویکاریو[2] (۲۰۲۳) با تمرکز بر روندهای مرتبط با فناوری‌های نوظهور و مخرب در بخش دفاع و امنیت به ارائه توضیحاتی در خصوص تعریف فناوری‌های نوظهور و مخرب و همگرایی آن‌ها، روندهای جاری درزمینهٔ جنگ هیبریدی و همچنین امیدوارکننده‌ترین و مرتبط‌ترین فناوری‌هایی که می‌توانند در مقیاس وسیع اعمال شوند و بر حوزه‌های دفاع و امنیت تأثیرگذارند، پرداخته است. این پژوهش نیز در حد تعاریف مربوطه و روندهای حاکم بر فناوری‌های نوظهور در حوزه دفاع و امنیت بحث نموده و با محوریت اصلی پژوهش که پیشران‌ها هستند فاصله معنایی دارد.

1- Capa
2- Doicariu

در بخش اسناد و پروژه‌های تحقیقاتی اسنادی مانند گزارش شورای اطلاعات ملی آمریکا (ان آی سی)[1] تحت عنوان «روندهای جهانی ۲۰۴۰"[2] به بررسی روندهای جهانی در حوزه فناوری‌های نوظهور و چالش‌های امنیتی آن‌ها پرداخته است. این گزارش ماهیتی عمومی داشته و تمرکز آن به‌طور خاص بر کشورهای توسعه‌یافته است که به‌منظور ارائه سیاست‌های دفاعی از آن بهره می‌توان گرفت و در بررسی و شناسایی پیشران‌ها از آن استفاده نمود. آدیری و ابروشان[3] (۲۰۲۴) نیز به موضوع امنیت سایبری و جنگ‌های دیجیتال پرداخته و هشدار می‌دهند که در دنیای آینده، مرز میان صلح و جنگ با ورود فناوری‌های هوشمند، دچار ابهام و سردرگمی می‌شود. بیننديجک و همکاران[4] (۲۰۲۰) نیز در گزارش ارائه شده توسط موسسه رَند[5] با عنوان» رابطهای مغز و کامپیوتر (کاربردها و پیامدهای نظامی ایالات متحده)«به این موضوع اشاره دارند که ارتش‌های آینده ناگزیر از انطباق با الگوهای جدید تصمیم‌گیری مبتنی بر داده و اتوماسیون هستند». با توجه به آنچه در پیشینه مطرح شد و علی‌رغم وجود پژوهش‌هایی ارزشمند در حوزه فناوری، امنیت و دفاع، هنوز مطالعه‌ای جامع، بومی‌سازی‌شده و مبتنی بر آینده‌نگاری که به‌طور خاص بر شناسایی پیشران‌های تأثیرگذار فناوری‌های نوظهور اطلاعاتی-ارتباطی بر امنیت دفاعی متمرکز باشد، در دسترس نیست. از این‌رو، پژوهش حاضر با بهره‌گیری از رویکردی سیستمی و آینده‌نگرانه، تلاش دارد خلأ یادشده را پوشش دهد.

مبانی نظری

۱. فناوری ارتباطی و اطلاعاتی

فناوری‌های نوظهور اطلاعاتی و ارتباطی در دهه‌های اخیر تحولات بنیادین در حوزه‌های دفاعی و امنیت ملی ایجاد کرده‌اند. فناوری‌هایی همچون هوش مصنوعی و یادگیری ماشینی، کلان‌داده و تحلیل پیشرفته، اینترنت اشیاء دفاعی، شبکه‌های ارتباطی نسل پنجم و ششم، بلاک‌چین، واقعیت افزوده و مجازی، فناوری‌های شناختی و جنگ

1- National Intelligence Council
2- Global Trends 2040
3- Adeyeri & Abroshan
4- Binnendijk et al
5- RAND Corporation

سایبری ظرفیت‌های نوینی برای فرماندهی و کنترل، پایش صحنه نبرد، عملیات اطلاعاتی و تصمیم‌گیری راهبردی فراهم کرده‌اند (کولیوند، ۱۴۰۱). این فناوری‌ها نه تنها کارایی سامانه‌های دفاعی را افزایش داده، بلکه نحوه تعامل بین سامانه‌ها و تصمیم‌گیران را نیز دگرگون ساخته است. علاوه بر این، فناوری اطلاعات باعث ایجاد قابلیت‌های نوین در جمع‌آوری، پردازش و انتقال داده‌ها به صورت بلادرنگ شده و امکان تحلیل و پیش‌بینی روندهای تهدیدات و فرصت‌ها را فراهم می‌آورد (De Alwis et al, ۲۰۲۱).

۲. روندهای فناورانه نوظهور در حوزه اطلاعات و ارتباطات

پیش از آنکه به شناسایی و اولویت‌بندی پیشران‌ها پرداخته شود، ضروری است روندهای فناورانه نوظهور در عرصه اطلاعات و ارتباطات به‌عنوان بستر تحول‌آفرین در امنیت دفاعی بررسی شود. این روندها، چشم‌انداز آتی حوزه آی سی تی[1] را شکل داده و مبنایی برای انتخاب پیشران‌ها فراهم می‌آورند.

۲-۱. افزایش اتکاء سامانه‌های دفاعی به هوش مصنوعی و یادگیری ماشین

در سال‌های اخیر، اتکاء سامانه‌های دفاعی به هوش مصنوعی و یادگیری ماشین به یکی از روندهای کلیدی فناوری‌های نوظهور اطلاعاتی-ارتباطی تبدیل شده است. این روند با هدف تحلیل داده‌های حجیم، پیش‌بینی رفتار دشمن، طبقه‌بندی تهدیدها و پشتیبانی تصمیم‌گیری نظامی در حال گسترش است. همچنین، به‌کارگیری هوش مصنوعی در امنیت سایبری برای تشخیص نفوذ و مقابله با حملات پیشرفته، همراه با ادغام آن در چارچوب‌های زیروتراست[2] تا افق ۱۴۱۴ موجب تقویت ساختار دفاعی هوشمند کشورها خواهد شد (Bagawade, ۲۰۲۳).

۲-۲. گسترش ارتباطات تاکتیکی هوشمند در میدان نبرد

در میدان نبرد آینده، افزایش استفاده از ارتباطات تاکتیکی هوشمند برای ایجاد شبکه‌های پایدار، ایمن و کم‌تأخیر به‌سرعت در حال رشد است (کولیوند، ۱۴۰۱). از هوش مصنوعی در مدیریت خودکار شبکه‌های تاکتیکی شامل تخصیص بلند،

1- ICT
2- Zero Trust

خودترمیمی و هماهنگی چندعاملی، ظرفیت و تاب‌آوری ارتباطات را ارتقاء می‌دهد (Concha Salor & Monzon Baeza, ۲۰۲۳). این روند، با هدف کاهش آسیب‌پذیری در برابر اختلالات دشمن و بهبود خودسازگاری ارتباطات در محیط‌های جنگی تا افق ۱۴۱۴ به‌عنوان یکی از جهت‌گیری‌های اصلی تحول در سامانه‌های دفاعی شناخته می‌شود.

۲-۳. گسترش اینترنت اشیاء نظامی و شبکه‌سازی میدانی تجهیزات

در سال‌های اخیر، روند گسترش اینترنت اشیاء در حوزه نظامی موجب تحول در ساختارهای فرماندهی و کنترل شده است. تجهیزات میدانی مانند پهپادها، حسگرها، سامانه‌های پوشیدنی و ربات‌ها به‌صورت شبکه‌ای و هوشمند با یکدیگر ارتباط برقرار می‌کنند و آگاهی موقعیتی و هماهنگی عملیاتی را به‌طور چشمگیری افزایش می‌دهند (Oprisor, ۲۰۲۱). پیش‌بینی می‌شود تا افق ۱۴۱۴، یکپارچگی و خودکارسازی تبادل داده میان سامانه‌های نظامی با تکیه بر اینترنت اشیاء، یکی از روندهای اصلی در تحول نبردهای آینده و ارتقاء کارایی میدانی باشد.

۲-۴. گذار از رمزنگاری کلاسیک به امنیت کوانتومی در سامانه‌های دفاعی

در دهه گذشته، رشد سریع محاسبات کوانتومی چشم‌انداز امنیت سایبری را به‌طور بنیادین دگرگون کرده است. در حالی‌که تا چند سال پیش این فناوری در مرحله آزمایشگاهی بود، امروز توان آن برای شکستن الگوریتم‌های رمزنگاری متداول مانند آر اس ای[1] و ای سی سی[2] به نگرانی جدی بدل شده است (Subramani & Svn, ۲۰۲۵). هم‌زمان، روند توسعه و به‌کارگیری رمزنگاری کوانتومی و پروتکل‌های مقاوم در برابر حملات کوانتومی شتاب گرفته است. پیش‌بینی می‌شود تا افق ۱۴۱۴، گذار جهانی از رمزنگاری کلاسیک به امنیت کوانتومی به یکی از تحولات راهبردی در حفاظت از داده‌های دفاعی تبدیل شود.

۲-۵. گسترش سامانه‌های خودمختار و ربات‌های هوشمند در عملیات دفاعی

در دهه اخیر، روند افزایش به‌کارگیری سامانه‌های خودمختار و ربات‌های هوشمند در مأموریت‌های نظارتی و رزمی شتاب گرفته است. در ابتدا ربات‌ها بیشتر تحت کنترل

1-RSA
2- ECC

مستقیم انسان عمل می‌کردند، اما امروزه پهپادها و ربات‌های زمینی، دریایی و هوایی خودمختار به‌طور فزاینده‌ای قادر به تصمیم‌گیری و تطبیق با محیط هستند (Chen et al, ۲۰۲۲). شکل‌گیری رزمایش‌های کلان‌رباتیک و توسعه ربات‌های واکنشی[1] و اگزواسکلتون‌ها[2] رزمی روند جدیدی را رقم زده که تا افق ۱۴۱۴ می‌تواند به محور اصلی عملیات‌های خودکار و هماهنگ دفاعی تبدیل شود.

۲-۶. تکامل جنگ الکترونیک پیشرفته و کنترل هوشمند طیف رادیویی

در دهه گذشته، جنگ الکترونیک از ابزارهای اختلال و شنود سنتی به سمت سامانه‌های هوشمند کنترل طیف رادیویی تحول یافته است. این روند با هدف افزایش توان شناسایی، اختلال، پنهان‌سازی و مقابله الکترونیکی در حال گسترش است (Haigh & Andrusenko, ۲۰۲۱: ۱۶۷). در حال حاضر، سامانه‌های جنگ الکترونیک مبتنی بر هوش مصنوعی قابلیت واکنش بلادرنگ به تهدیدات فرکانسی و سازگاری خودکار با محیط طیفی را دارند. پیش‌بینی می‌شود تا افق ۱۴۱۴، کنترل هوشمند و یکپارچه طیف رادیویی به مؤلفه‌ای راهبردی در برتری اطلاعاتی و امنیت دفاعی کشورها تبدیل شود.

۲-۷. گذار از شبکه‌محوری به داده‌محوری در سامانه‌های دفاعی

در سال‌های اخیر، افزایش چشمگیر داده‌های تولیدشده توسط حسگرها، پهپادها و ماهواره‌ها موجب تغییر جهت از ساختارهای شبکه‌محور به معماری‌های داده‌محور در نظام‌های دفاعی شده است. در گذشته، تمرکز بر اتصال اجزاء بود؛ اما اکنون تحلیل کلان‌داده، همگن‌سازی و اشتراک ایمن داده‌ها در مرکز تصمیم‌گیری قرار گرفته است (Stocchero, ۲۰۲۳: ۱۲۱). پیش‌بینی می‌شود تا افق ۱۴۱۴، نبردهای آینده بیش از هر زمان بر تسلط اطلاعاتی و پردازش لحظه‌ای داده‌ها در لبه شبکه متکی باشند و داده به عنصر تعیین‌کننده قدرت دفاعی تبدیل شود.

۲-۸. همگرایی و گسترش فناوری‌های دوکاربردی در عرصه دفاعی

در گذشته، توسعه فناوری‌ها میان بخش‌های نظامی و غیرنظامی تفکیک‌شده بود؛ اما در سال‌های اخیر، روند همگرایی فناوری‌های دوکاربردی شتاب گرفته است. امروزه

1- Reactive Robots
2- Exoskeletons

فناوری‌های نوظهور گسترده و هم‌زمان در صنایع غیرنظامی و دفاعی به کار گرفته می‌شوند (Bozbaş, ۲۰۲۵). این هم‌افزایی موجب تسریع نوآوری، انتقال دانش و کاهش هزینه‌های توسعه در بخش دفاعی گردیده و تا افق ۱۴۱۴، فناوری‌های دوکاربردی به ستون اصلی تحول در صنایع دفاعی و امنیت ملی تبدیل می‌شوند.

۳. نظریه‌های مبنایی تحقیق

در این پژوهش برای تحلیل دقیق پیشران‌های ناشی از فناوری‌های نوظهور در حوزه امنیت دفاعی از سه نظریه زیر که توانایی تحلیل پویایی‌های پیچیده آینده را دارند بهره گرفته شده است:

۳-۱. آینده‌نگاری راهبردی[1]

آینده‌نگاری راهبردی، برخلاف رویکردهای سنتی پیش‌بینی، بر امکان‌پذیری شکل‌دهی به آینده به ویژه آینده‌های محتمل و ممکن بر پایه تحلیل‌های مبتنی بر عدم قطعیت و محیط پرتلاطم آینده تمرکز دارد (Schwartz, ۲۰۲۳). آینده نه‌تنها قابل شناخت، بلکه قابل ساخت نیز هست، به‌شرط آن‌که با نگاهی سیستمی، مشارکتی و چندپارادایمی به آن نگریسته شود؛ این امر نشان‌دهنده تلفیقی از روش‌های آینده‌نگری با روش‌های مدیریت راهبردی است (Slaughter, ۱۹۹۷). آینده‌نگاری راهبردی، به‌ویژه در حوزه امنیت دفاعی، می‌تواند دولت‌ها را از حالت انفعال خارج و به بازیگران فعال در شکل‌دهی به روندها تبدیل کند (Kunadt, ۲۰۲۵).

۳-۲. نظریه سامانه‌های پیچیده[2]

بر اساس نظریه سامانه‌های پیچیده، تعامل متغیرها، فناوری‌ها، بازیگران و محیط منجر به تولید ساختارهای غیرخطی، حلقه‌های بازخوردی و نتایج پیش‌بینی‌ناپذیر می‌شود. سامانه‌های پیچیده به بررسی نحوه ارتباط بین اجزا و رفتار جمعی آن‌ها، نحوه ارتباط و برهمکنش با محیط اطراف پرداخته و رفتارهای دسته‌جمعی و همگرا را به‌عنوان یک هدف اساسی مورد مطالعه قرار می‌دهد. این نظریه که توسط محققانی همچون میشل و

1- Strategic Foresight
2- Complex Systems Theory

نیومن[1] (۲۰۰۲) و استیون و کالینز[2] (۲۰۲۱) در حوزه امنیت توسعه یافته (Mitchell & Newman, ۲۰۰۲)، امکان تحلیل پویایی‌های امنیتی در بستر فناوری‌های نوظهور را فراهم می‌آورد (Stevens & Collins, ۲۰۲۱).

۴-۳. پیشران‌ها (نیروهای بزرگ تغییر)[3]

در تحلیل آینده، پیشران‌ها به‌عنوان نیروهای اصلی ایجاد تغییر، نقشی اساسی در شکل‌دهی به آینده ایفا می‌کنند (Minkkinen, ۲۰۲۰). پیشران‌ها که در آثار آینده‌پژوهانی مانند گلن و گوردون[4] (۲۰۰۳)، مینکینن[5] (۲۰۲۰)، شوارتز (۱۹۹۷) و بیشاپ و هاینز (۲۰۱۲) برجسته شده، بر شناسایی و تحلیل متقابل نیروهای کلان محیطی، فناورانه، اقتصادی، سیاسی و اجتماعی تأکید دارد که خود گونه‌ای از روندهای حاکم در این ابعاد هستند (Glenn & Gordon, ۲۰۰۳: ۴۳۱).

۵-۳. جایگاه پژوهش در توسعه نظریات آینده‌پژوهی دفاعی

پژوهش حاضر از دیدگاه نظری و کاربردی می‌تواند واجد سهمی مضاعف برای غنای ادبیات آینده‌پژوهی دفاعی قلمداد گردد. از منظر نظری، زمینه‌ساز بستری برای تحلیل تهدیدات نوظهور فناورانه در فضای فناوری‌های نوظهور اطلاعاتی-ارتباطی است. در واقع، این پژوهش بر این نکته تأکید دارد که تهدیدات آینده تنها به فناوری‌های دشمن وابسته نیست، بلکه به ناتوانی در پیش‌بینی و آمادگی ساختاری نیز بازمی‌گردد. نوآوری این پژوهش در سه بعد مفهومی (توسعه مفهوم «پیشران‌های امنیت‌برانداز فناورانه» که نه‌تنها تهدیدزا هستند، بلکه توان ساختارشکنی نهادهای دفاعی را دارند)؛ تحلیلی (بهره‌گیری از روش‌های ترکیبی دلفی و تحلیل اثر متقابل بر پایه ماتریس ویلسون[6] برای تحلیل روابط چندسطحی و پویای پیشران‌ها) و راهبردی (ارائه توصیه‌های سیاستی مبتنی بر توانمندسازی نظام دفاعی در برابر تهدیدات آینده متأثر از فناوری‌های نوظهور اطلاعاتی-ارتباطی) تعریف می‌گردد.

1- Mitchell & Newman
2-Stevens & Collins
3- Drivers (Major Forces of Change)
4- Glenn & Gordon
5- Minkkinen
6- Wilson

چارچوب نظری پژوهش

در این پژوهش تمرکز اصلی بر شناسایی و تبیین پیشران‌هایی است که می‌توانند در شکل‌دهی به آینده امنیت دفاعی نقش‌آفرینی کنند؛ بنابراین مدل مفهومی این تحقیق با هدف شناسایی و دسته‌بندی پیشران‌ها ارائه می‌شود و نه سنجش روابط علّی و آماری میان متغیرها. این چارچوب مفهومی نشان می‌دهد که پیشران‌های فناورانه می‌توانند به‌صورت مستقیم یا غیرمستقیم بر ابعاد سه‌گانه امنیت دفاعی اثرگذار بوده و مسیرهای آینده این حوزه را رقم بزنند.

روش‌شناسی

پژوهش حاضر از نظر هدف در دسته تحقیقات کاربردی، از نظر گردآوری داده‌ها پیمایشی طولی و از نظر روش آمیخته قلمداد می‌شود. از منطق پژوهش آینده‌نگر با تلفیق روش‌های فراترکیب مطالعات و اسناد مرتبط، دلفی و تحلیل تأثیر متقابل با استفاده از ماتریس ویلسون انجام شد. جامعه آماری پژوهش ۲۷ نفر خبره و صاحب‌نظر شامل اعضاء هیئت علمی دانشگاه‌ها، مدیران و کارشناسان ارشد در حوزه دفاعی-امنیتی با تجربه مستقیم در حوزه آی سی تی و آینده‌پژوهی با استفاده از نمونه‌گیری هدفمند است. معیار ورود به جامعه خبرگی داشتن حداقل پنج سال تجربه تخصصی در تحلیل آینده امنیت دفاعی و نیز آشنایی اولیه با مبانی آینده‌نگاری دفاعی است. برای سنجش روایی محتوایی ابزار تحقیق، پرسش‌نامه اولیه در اختیار چند نفر از متخصصان همان حوزه قرار گرفت و اصلاحات لازم براساس نظرات ایشان انجام شد. پایایی نیز از طریق ضریب هماهنگی بین پاسخ‌های خبرگان در طی مراحل مختلف فرایند دلفی محاسبه گردید. در این پژوهش، مفاهیم کلیدی به‌صورت شفاف تعریف شد. منظور از فناوری‌های نوظهور، دسته‌ای از فناوری‌هاست که هنوز در مرحله توسعه یا پذیرش گسترده قرار دارند اما قابلیت ایجاد تغییرات بنیادین در حوزه‌های دفاعی و امنیتی را دارند. این دسته فناوری‌ها معمولاً با سطح بالای عدم‌قطعیت و سرعت تحول سریع شناخته می‌شوند. در چارچوب این تحقیق، فناوری‌های نوظهور اطلاعاتی به آن دسته از فناوری‌ها اطلاق می‌شود که توانایی نوین در جمع‌آوری، پردازش، تحلیل و ذخیره‌سازی داده‌ها ایجاد می‌کنند؛ مانند هوش مصنوعی، کلان‌داده، یادگیری ماشینی و محاسبات کوانتومی. در مقابل، فناوری‌های نوظهور ارتباطی شامل فناوری‌هایی هستند که امکان

تبادل و انتقال سریع‌تر، ایمن‌تر و کارآمدتر داده‌ها و اطلاعات را فراهم می‌کنند؛ مانند شبکه‌های نسل پنجم و ششم (۶G/۵G)، اینترنت اشیاء، بلاک‌چین و ارتباطات ماهواره‌ای پیشرفته. در پرسش‌نامه دلفی، پیشران‌های فناورانه در دو دسته «اطلاعاتی» و «ارتباطی» تعریف و برای هر یک شاخص‌های سنجش میزان تأثیر بر امنیت دفاعی و سطح عدم‌قطعیت در افق ۱۴۱۴ تدوین گردید.

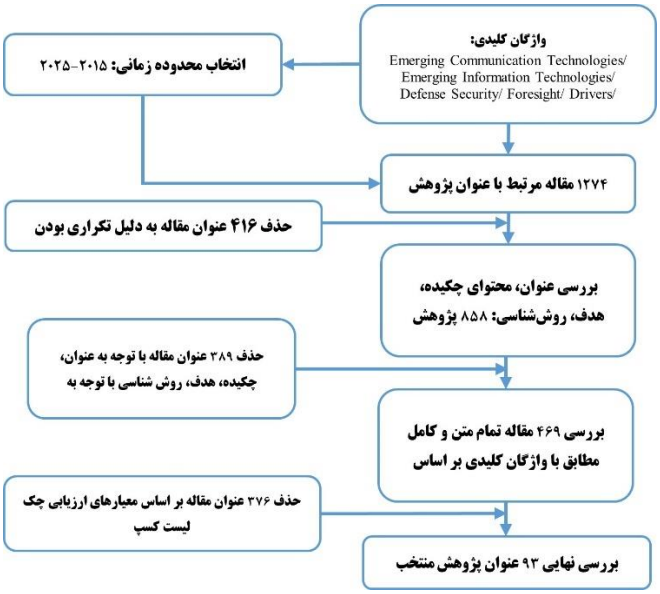
تجزیه و تحلیل یافته‌ها

همان‌گونه که در بخش روش‌شناسی مطرح شد، گام نخست این پژوهش با رویکرد فراترکیب به مرور سیستماتیک و مطالعات کتابخانه‌ای و اسنادی برای درک و شناختی عمیق پیرامون موضوع پژوهش می‌پردازد. طیف مطالعات شکل‌دهنده پژوهش را پایگاه‌های داده علمی و مجلات معتبر داخلی و خارجی با تراز بین‌المللی و کلیه مطالعات انجام شده در حوزه فناوری‌های نوظهور در بخش اطلاعاتی-ارتباطی تشکیل داد و بر اساس نمونه‌گیری هدفمند ملاک‌مدار، پژوهش‌های که بینش کامل‌تری نسبت به مفهوم کردند، انتخاب و جستجو تا مرحله‌ای ادامه یافت که پیشران‌های مربوطه، تکرار شدند. بازه زمانی انتخاب پژوهش‌های انجام شده از سال ۲۰۱۵ تا ۲۰۲۵ در نظر گرفته شد. بر این اساس اولین پژوهش در سال ۲۰۱۵ با عنوان (بررسی شبکه ۵G: معماری و فناوری‌های نوظهور توسط گوپتا و جوها[1]) شناسایی شد؛ این فرایند با محدود کردن پژوهش‌های موصوف به واژگان کلیدی خاصی همچون «فناوری‌های نوظهور ارتباطی»، «فناوری‌های نوظهور اطلاعاتی» و «امنیت دفاعی» با واژگان دیگری همانند آینده‌نگاری، پیشران، عدم قطعیت، عوامل کلیدی و موضوعاتی از این دست تا آخرین پژوهش در سال ۲۰۲۵ انجام شد. فرآیند فراترکیب انجام شده بهره‌گیری از الگوی هفت مرحله‌ای سندلوسکی و باروسو[2] بود. گام‌های روش مذکور تنظیم سؤال‌های پژوهش؛ بررسی نظام‌مند متون مورد نظر؛ جستجو و بررسی مقاله‌های مرتبط؛ استخراج اطلاعات مقالات و مستندات؛ تجزیه‌وتحلیل و ترکیب یافته‌های کیفی است. برای استخراج مضامین فراگیر[3] (پیشران‌ها) از روش ارائه شده توسط اترید-استرلینگ[4] بهره گرفته شد.

1- Gupta & Jha
2- Sandlowski and Barroso
3-Global Themes
4- Attride-Stirling

در این روش شبکه مضامین[1] از مقالات و پژوهش‌های مورد بررسی تشکیل و شبکه تم‌ها نیز توسط سه گونه اصلی کدها و مفاهیم از قبیل مضامین پایه[2]، مضامین سازمان‌دهنده[3] و مضامین فراگیر (پیشران شناسایی شده) تشکیل شد (کولیوند و همکاران، ۱۴۰۲). گام‌های پایانی روش هفت مرحله‌ای به بررسی پایایی و اعتبار داده‌ها می‌پردازد (طهرائی نصرآبادی و همکاران، ۱۴۰۲). پاسخ سه گام نخست مطرح شده برای فراترکیب در بخش‌های بیان مسئله، ادبیات نظری، پیشینه پژوهشی و روش‌شناسی ارائه شد.

فرآیند انجام شده در گام چهارم به صورت شکل (۱) قابل رویت است. مرحله ارزیابی و کنترل کیفیت فراترکیب بسیار حیاتی است که برای تحقق این امر از چک‌لیست ارائه شده توسط کسپ[4] که شامل ده سؤال اساسی و مهم استفاده شد (Frias-Goytia et al, ۲۰۲۴) تا در نهایت از بین ۹۳ پژوهش منتخب تعداد ۲۲ مضمون فراگیر (پیشران‌ها) به شرح جدول (۱) استخراج شود.



شکل ۱، مراحل طی شده برای جستجو و انتخاب پژوهش‌های منتخب (یافته‌های محققین)

1- Thematic Network
2-Basic Themes
3- Organizing Themes
4- CASP scale

جدول (۱)، فراترکیب مضامین بر پایه روش اترید-استرلینگ (یافته‌های محققین)

کد اختصاصی	مضامین پایه	مضامین سازمان‌دهنده
۱	رشد هوش مصنوعی و یادگیری ماشین در سیستم‌های نظامی	افزایش بهره‌برداری از هوش مصنوعی و یادگیری ماشین در سامانه‌های تصمیم‌گیر نظامی
	خودکارسازی تصمیم‌گیری در میدان نبرد	
	افزایش وابستگی به پلتفرم‌های مبتنی بر هوش مصنوعی ساخت قدرت‌های رقیب	
	به‌کارگیری هوش مصنوعی مولد در حوزه جنگ شناختی و فریب‌های راهبردی	
۲	توسعه اینترنت اشیاء نظامی	گسترش اینترنت اشیاء نظامی و اتصال تجهیزات به شبکه‌های متمرکز فرماندهی
	ظهور اینترنت تاکتیکی میدان جنگ	
۳	ادغام حسگرها، پهپادها و تجهیزات در یک شبکه هوشمند دفاعی	ظهور فرماندهی و کنترل شبکه‌محور با ادغام حسگرها، ربات‌ها و پهپادهای هوشمند
	افزایش کارایی و انعطاف‌پذیری سامانه‌های دفاعی	
	افزایش نفوذ سلاح‌های بدون سرنشین هوشمند در مأموریت‌های تهاجمی و شناسایی	
	کاربرد گسترده پهپادها در جمع‌آوری اطلاعات و حملات از طریق توسعه سیستم‌های بدون سرنشین هوشمند (پهپادها و ربات‌ها)	
۴	افزایش ریسک اقدامات غیرقابل کنترل و رشد سایبری و استقلال عملیات‌های نظامی با توسعه الگوریتم‌های خودتصمیم‌گیر در ربات‌ها و پهپادها	توسعه الگوریتم‌های خودتصمیم‌گیر و افزایش استقلال عملیات رباتیک و پهپادی
	قابلیت ترکیب داده‌های ماهواره‌ای، پهپادی، حسگرها و هوش مصنوعی برای حذف نقاط کور میدان نبرد	
۵	ظهور فناوری‌های ارتباطات کوانتومی و تحول در امنیت داده‌های حساس دفاعی	توسعه فناوری‌های کوانتومی و دگرگونی در امنیت تبادل اطلاعات نظامی
۶	تحول بنیادین در ساختار فرماندهی و کنترل با فناوری‌های نوین	دگرگونی ساختار فرماندهی و کنترل با استفاده از

کد اختصاصی	مضامین پایه	مضامین سازمان‌دهنده
		فناوری‌های شناختی و خودمختار
۷	افزایش وابستگی به زیرساخت‌های سایبری	افزایش آسیب‌پذیری زیرساخت‌های سایبری در برابر حملات ترکیبی و پیچیده
	نگرانی‌های ژئوپلیتیکی ناشی از بک‌دورها یا جاسوسی فناورانه	
	ضعف و ناکارآمدی در حکمرانی فناوری‌های نوظهور	
	تمرکز آسیب‌پذیری دفاعی به حملات سایبری	
۸	گسترش فناوری‌های واقعیت افزوده و مجازی در آموزش نظامی	گسترش کاربرد واقعیت افزوده و مجازی در آموزش، شبیه‌سازی و فرماندهی نظامی
۹	افزایش سرعت و امنیت انتقال داده در عملیات بر پایه گسترش شبکه‌های 5G و 6G در حوزه نظامی	تحول در سرعت، دقت و امنیت انتقال داده‌ها با بهره‌گیری از نسل پنجم و ششم مخابرات نظامی
	ایجاد شبکه‌های بلادرنگ برای تبادل اطلاعات بین نیروهای مختلف در میدان نبرد	
۱۰	بهبود پیش‌بینی تهدیدات و تصمیم‌سازی سریع با توجه به پیشرفت‌های گسترده در فناوری پردازش کلان‌داده	کاربرد کلان‌داده و تحلیل هوشمند برای پیش‌بینی تهدیدات و تصمیم‌سازی سریع‌تر
	تحول فزاینده در کنترل هوایی و عملیات اطلاعاتی و خرابکارانه	
	انباشت داده‌های کلان دشمن در طی زمان و ساخت مدل‌های رفتاری نیروها	
۱۱	ایجاد گسل‌های شناختی و سیاسی با افزایش شکاف دانشی و فناورانه میان نیروهای مسلح و جامعه مدنی	رشد جنگ‌های شناختی و کاربرد فناوری‌های نوین برای نفوذ روانی و کنترل ادراکات
۱۲	همگرایی فناوری‌های نوین در پلتفرم‌های دفاعی	افزایش پیچیدگی امنیتی ناشی از همگرایی فناوری‌های نوین در محیط عملیاتی
	افزایش پیچیدگی امنیتی و نقاط نفوذ جدید بر پایه ادغام فناوری‌های نوظهور	

کد اختصاصی	مضامین پایه	مضامین سازمان‌دهنده
۱۳	ایجاد تغییر گسترده در موازنه قدرت منطقه‌ای ناشی از دسترسی به فناوری‌های نوظهور	تغییر در موازنه قدرت منطقه‌ای براثر دسترسی نامتقارن به فناوری‌های نوظهور
	رقابت قدرت‌های بزرگ بر سر سلطه بر فناوری‌های سایبری و اطلاعاتی نوظهور	
۱۴	چالش‌های قانونی و بین‌المللی در استفاده از هوش مصنوعی در تسلیحات	افزایش ریسک تحریم فناورانه و وابستگی به پلتفرم‌های خارجی در حوزه دفاعی
	نفوذ الگوریتم‌های خارجی در سیستم‌های دفاعی از طریق تجهیزات غیرایمن	
۱۵	تضعیف روحیه و نفوذ روانی با توجه به رشد سریع فناوری‌های نوظهور جنگ شناختی	دگرگونی ساختار فرماندهی و کنترل با استفاده از فناوری‌های شناختی و خودمختار
	ظهور سلاح‌های شناختی و اطلاعاتی فراتر از تصور سنتی جنگ	
۱۶	پیشرفت فناوری تشخیص چهره و شناسایی زیستی در امنیت مرزی و پایش جمعیت	افزایش استفاده از فناوری‌های زیستی و بیومتریک در کنترل مرزی و امنیت داخلی
	بهبود کنترل و نظارت با تمرکز بر استفاده از داده‌های بیومتریک	
۱۷	افزایش سرعت تغییر فناوری نسبت به ظرفیت انطباق ساختارهای دفاعی	شتاب رشد فناوری نسبت به ظرفیت انطباق سازمان‌های دفاعی با تغییرات فناورانه
۱۸	وابستگی به پلتفرم‌های خارجی و خطر تحریم فناورانه	نفوذ الگوریتم‌های خارجی از طریق تجهیزات وارداتی و تهدیدات پنهان امنیتی
	عدم خودکفایی در تولید سخت‌افزارها و زیرساخت‌های ارتباطی حیاتی	
۱۹	توسعه شبکه‌های مغز به مغز و امکان نفوذ به تصمیمات فرماندهی	ظهور دوقلوهای دیجیتال نظامی و امکان شبیه‌سازی کامل صحنه نبرد در زمان واقعی
	دوقلوهای دیجیتال نظامی	
۲۰	شکاف زمانی خطرناک در پاسخ به تهدیدات فناورانه	به‌کارگیری هوش مصنوعی مولد در عملیات فریب، جنگ اطلاعاتی و تولید محتوای گمراه‌کننده
	به‌کارگیری گروه‌های پهپادی هماهنگ با تصمیم‌گیری مستقل گروهی از طریق هوش مصنوعی جمعی	
	تحریک‌پذیری جمعیت از طریق شبکه‌های اجتماعی	

کد اختصاصی	مضامین پایه	مضامین سازمان‌دهنده
۲۱	ظهور ابر پردازشگران نظامی با توان پردازشی و تحلیل هم‌زمان سناریوهای چندبعدی امنیتی	توسعه ابر پردازشگران نظامی برای تحلیل هم‌زمان سناریوهای چندبعدی امنیتی
	توسعه سلاح‌های خودمختار کشنده	
۲۲	افزایش توانمندی گروه‌های غیردولتی در دسترسی به فناوری‌های پیشرفته با تغییرات ایجادشده در الگوی امنیت و جنگ	افزایش توانایی گروه‌های غیردولتی در بهره‌برداری از فناوری‌های پیشرفته نظامی

پس از شناسایی و تحلیل اولیه پیشران‌ها، فرآیند کدگذاری محوری و مضامین‌یابی انجام شد. از آنجا که پیشران‌ها در طیف گسترده‌ای از حوزه‌های فناورانه، اطلاعاتی–امنیتی، سایبری، شناختی و ژئوپلیتیکی توزیع گردیده‌اند، به‌منظور افزایش انسجام و تحلیل موضوعی، در گام بعدی تلفیق مفهومی انجام شد.

در این مرحله، با اتکاء به روش تحلیل مضمون و شباهت‌های مفهومی، ساختاری و کارکردی، ۱۱ کلان پیشران به‌عنوان مضامین فراگیر از تلفیق ۲۲ پیشران اولیه شناسایی شد. فرآیند تلفیق مبتنی بر سه معیار اصلی هم‌راستایی کارکردی پیشران‌ها در زنجیره ارزش دفاعی–امنیتی، اشتراک فناوری مبنایی یا کاربردی میان پیشران‌ها و پیامدهای هم‌گرا در سطح راهبردی و عملیاتی هستند. نتیجه این فرایند به شرح جدول (۲) قابل‌رؤیت است.

جدول (۲)، کلان پیشران‌های شناسایی شده

کد پیشران	مضامین فراگیر	مضامین سازمان‌دهنده
Dr۱	به‌کارگیری فناوری‌های نوظهور اطلاعاتی – ارتباطی در همگرایی با هوش مصنوعی نظامی	• افزایش بهره‌برداری از هوش مصنوعی و یادگیری ماشین در سامانه‌های تصمیم‌گیر نظامی؛ • توسعه الگوریتم‌های خودتصمیم‌گیر و افزایش استقلال عملیات رباتیک و پهپادی؛ • به‌کارگیری هوش مصنوعی مولد در عملیات فریب، جنگ اطلاعاتی و تولید محتوای گمراه کننده.

کد پیشران	مضامین فراگیر	مضامین سازمان‌دهنده
Dr۲	توسعه یکپارچه‌سازی دیجیتالی و فرماندهی شبکه‌محور	• گسترش اینترنت اشیاء نظامی و اتصال تجهیزات به شبکه‌های متمرکز فرماندهی؛ • ظهور فرماندهی و کنترل شبکه‌محور با ادغام حسگرها، ربات‌ها و پهپادهای هوشمند؛ • دگرگونی ساختار فرماندهی و کنترل با استفاده از فناوری‌های شناختی و خودمختار.
Dr۳	تقویت نوآوری اطلاعاتی در امنیت سایبری نظامی	• توسعه فناوری‌های کوانتومی و دگرگونی در امنیت تبادل اطلاعات نظامی؛ • افزایش آسیب‌پذیری زیرساخت‌های سایبری در برابر حملات ترکیبی و پیچیده • نفوذ الگوریتم‌های خارجی از طریق تجهیزات وارداتی و تهدیدات پنهان امنیتی
Dr۴	توسعه و کاربرد متنوع شبیه‌سازها در جهت آموزش پیشرفته	• گسترش کاربرد واقعیت افزوده و مجازی در آموزش، شبیه‌سازی و فرماندهی نظامی؛ • ظهور دوقلوهای دیجیتال نظامی و امکان شبیه‌سازی کامل صحنه نبرد در زمان واقعی
Dr۵	پیشرفت زیرساخت‌های مخابراتی نظامی	• تحول در سرعت، دقت و امنیت انتقال داده‌ها با بهره‌گیری از نسل پنجم و ششم مخابرات نظامی
Dr۶	بهره‌گیری و استفاده از کلان‌داده و تحلیل هوشمند در همگرایی تحلیلی	• کاربرد کلان‌داده و تحلیل هوشمند برای پیش‌بینی تهدیدات و تصمیم‌سازی سریع‌تر؛ • توسعه ابر پردازشگران نظامی برای تحلیل هم‌زمان سناریوهای چندبعدی امنیتی
Dr۷	رشد مضاعف جنگ شناختی و نفوذ ادراکی فناوری محور در عملیات آینده	• رشد جنگ‌های شناختی و کاربرد فناوری‌های نوین برای نفوذ روانی و کنترل ادراکات؛ • به‌کارگیری هوش مصنوعی مولد در عملیات فریب
Dr۸	پیچیدگی و ابهام در محیط عملیاتی با	• افزایش پیچیدگی امنیتی ناشی از همگرایی فناوری‌های نوین در محیط عملیاتی؛

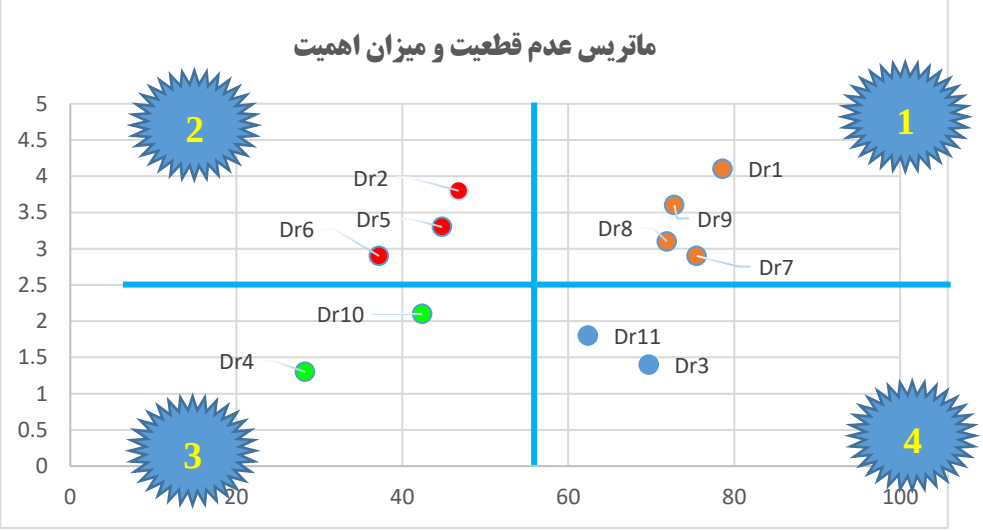
مضامین سازمان‌دهنده	مضامین فراگیر	کد پیشران
• شتاب رشد فناوری نسبت به ظرفیت انطباق سازمان‌های دفاعی با تغییرات فناورانه	همگرایی و تلفیق فناوری‌ها	
• تغییر در موازنه قدرت منطقه‌ای بر اثر دسترسی نامتقارن به فناوری‌های نوظهور؛ • افزایش ریسک تحریم فناورانه و وابستگی به پلتفرم‌های خارجی در حوزه دفاعی	تغییرات ژئوپلیتیکی فناورانه و تهدیدات ناشی از وابستگی فناورانه	Dr۹
• افزایش استفاده از فناوری‌های زیستی و بیومتریک در کنترل مرزی و امنیت داخلی	به‌کارگیری گسترده زیست‌فناوری‌های امنیتی	Dr۱۰
• افزایش توانایی گروه‌های غیردولتی در بهره‌برداری از فناوری‌های اطلاعاتی پیشرفته نظامی	دسترسی غیردولتی‌ها به فناوری اطلاعاتی نظامی	Dr۱۱

در گام بعد برای شناسایی و ارزیابی پیشران‌های کلیدی از روش دلفی استفاده شد. در این راستا از خبرگان و صاحب‌نظران خواسته شد تا میزان تأثیر هر پیشران بر امنیت دفاعی ایران را بر اساس طیف لیکرت پنج‌درجه‌ای (۱ = کمترین تأثیر تا ۵ = بیشترین تأثیر) ارزیابی نمایند. علاوه بر این، خبرگان میزان عدم‌قطعیت هر پیشران در افق ۱۴۱۴ را با اختصاص نمره‌ای بین صفر تا ۱۰۰ مشخص کردند؛ به‌گونه‌ای که نمره صفر بیانگر ثبات کامل پیشران و احتمال تغییر صفر درصد و نمره ۱۰۰ نشان‌دهنده احتمال تغییر قطعی آن در آینده بود. فرایند دلفی در دو مرحله متوالی انجام شد. در مرحله نخست، نظرات اولیه خبرگان جمع‌آوری و تحلیل شد. سپس نتایج مرحله اول در اختیار مشارکت‌کنندگان قرار گرفت تا در پرتو بازخوردهای گروهی، امکان بازنگری و تعدیل نظرات خود را داشته باشند. در مرحله دوم، پاسخ‌ها مجدداً گردآوری و از طریق روش‌های آماری توصیفی، درجه اجماع و همگرایی میان خبرگان مشخص شد. تکرار دومرحله‌ای این فرایند موجب افزایش روایی و پایایی نتایج شد و نهایتاً مجموعه‌ای از پیشران‌های کلیدی با اجماع خبرگان استخراج گردید. برای این منظور معیار موردقبول واقع شدن نظرات خبرگان و کارشناسان در مورد میزان عدم اطمینان IQR≤۳۰ و میزان تأثیر IQR≥۱/۲ مدنظر قرار گرفت (Sekaran, ۲۰۰۳: ۸۳) (جدول ۳).

جدول ۳، نتایج اجرای دو مرحله دلفی (یافته‌های محققین)

پیشران کلیدی	میزان عدم قطعیت						میزان تأثیر					
	مرحله اول			مرحله دوم			مرحله اول			مرحله دوم		
	IQR	Mean	SD	IQR	Mean	SD	IQR	Mean	SD	IQR	Mean	SD
Dr۱	۲۸	۷۱/۳	۲۲/۹	۳۰	۷۸/۶	۲۰/۷	۱/۵	۲/۸	۱	۱/۸	¼	۰/۸
Dr۲	۳۱	۴۶/۴	۲۰/۷	۲۹	۴۶/۸	۲۰/۷	۱	۳/۶	۱	۱/۹	۳/۸	۱
Dr۳	۳۴	۶۱/۳	۱۱/۷	۲۷	۶۹/۷	۱۱/۲	۱/۲	۳/۲	۰/۹	۱/۷	۱/۴	۰/۸
Dr۴	۳۹	۲۷/۹	۲۲/۲	۳۰	۲۸/۳	۲۱/۳	۱/۵	۴/۳	۱/۱	۱/۴	۱/۳	۱
Dr۵	۳۹	۴۱/۱	۱۸/۸	۳۰	۴۴/۸	۱۷/۶	۱	۳/۹	۰/۹	۱/۲	۳/۳	۰/۹
Dr۶	۳۶	۳۵/۵	۱۸/۴	۲۸	۳۷/۲	۱۶/۷	۱/۵	۳/۸	۱/۱	۱/۳	۲/۹	۰/۹
Dr۷	۲۸	۷۴/۷	۱۷/۹	۳۰	۷۵/۵	۱۶/۴	۱/۲	۳/۴	۱	۱/۹	۲/۹	۱
Dr۸	۳۴	۶۸	۱۷/۸	۳۰	۷۱/۹	۱۵/۷	۱/۵	۴	۰/۹	۱/۵	۳/۱	۰/۷
Dr۹	۳۳	۶۶/۸	۱۹/۶	۲۶	۷۲/۸	۱۹/۳	۰/۵	۳/۳	۰/۹	۱/۵	۳/۶	۰/۹
Dr۱۰	۳۲	۴۰/۴	۲۵/۵	۲۷	۴۲/۴	۲۵/۵	۱/۵	۴	۱	۱/۷	½	۰/۹
Dr۱۱	۳۶	۵۸	۱۷/۸	۲۸	۶۲/۴	۱۵/۷	۱/۵	۴	۰/۹	۱/۵	۱/۸	۰/۷

بر اساس جدول فوق با توجه معیار مورد قبول واقع شدن نظرات خبرگان و کارشناسان برای عدم قطعیت و میزان تأثیر در راند دوم دلفی به‌منظور تحلیل روابط متقابل و شناسایی پیشران‌هایی با بیشترین تأثیرگذاری و تأثیرپذیری، از ماتریس تحلیل اثرات متقابل ویلسون استفاده شد. جانمایی پیشران‌ها در شکل (۲) قابل مشاهده است.



شکل (۲)، جانمایی پیشران‌ها بر اساس ماتریس ویلسون (یافته‌های محققین)

در ماتریس ویلسون با چهار دسته پیشران تعاملی[1]، کلیدی[2]، وابسته[3] و نوظهور[4] مواجه هستیم. پیشران‌های تعاملی که در ربع اول ماتریس ویلسون قرار دارند، مولد اصلی سناریوهای غیرخطی، تحولات شگرف و تغییرات پارادایمی در آینده هستند. این پیشران‌ها در حالی از اهمیت و تأثیرگذاری بالایی برخوردارند که به‌دلیل نو بودن، سرعت تحولات فناورانه، عدم توافق بر چارچوب‌های حکمرانی و سطح بلوغ پایین، با عدم‌قطعیت بسیار بالایی همراه‌اند و در اولویت اول قرار می‌گیرند (Popper et al, ۲۰۰۸).

پیشران‌های کلیدی با اهمیت و تأثیرگذاری بالا و عدم‌قطعیت پایین در ربع دوم ماتریس، نشان می‌دهند که با اطمینان بالایی می‌توان انتظار داشت آینده امنیت دفاعی را به شکل بنیادین تحت تأثیر قرار می‌دهند. این پیشران‌ها به دلیل ماهیت تثبیت‌شده، گستره جهانی توسعه، نرخ رشد فناوری و وجود نمونه‌های عملیاتی، از درجه اطمینان بالایی برخوردار بوده و در عین حال به شدت تعیین‌کننده‌اند. این دسته از پیشران‌ها به نوعی نقش «ستون فقرات آینده دفاعی» را ایفا می‌کنند. بُعد راهبردی آن‌ها نه تنها در

1- Interactive Drivers
2- Key Drivers
3-Dependent
4- Critical Uncertainties

قابلیت فنی، بلکه در میزان تحول‌پذیری ساختارهای فرماندهی، آموزش، لجستیک و عملیات نظامی است. آن‌ها به صورت انباشتی و تدریجی، ساختارهای سنتی دفاعی را دگرگون کرده و به سمت یک نظم جدید مبتنی بر هوش، سرعت، دقت و کنترل بلادرنگ سوق داده و در رتبه دوم قرار می‌گیرند (Miles & Keenan, ۲۰۰۳).

ربع سوم ماتریس مذکور به پیشران‌های وابسته تعلق دارد که نشان‌دهنده وضعیت‌های ساختاری یا نهادی‌ای بوده و عمدتاً تابع عملکرد یا عدم‌عملکرد در سایر پیشران‌هاست و می‌توان آن‌ها را در رتبه سوم اولویت‌ها لحاظ نمود (Wilson et al, ۲۰۱۳).

و در ربع چهارم پیشران‌های نوظهور قرار دارند، اگرچه در نگاه نخست از اهمیت راهبردی کمتری برخوردارند، اما در بسترهای خاص و در ترکیب با سایر پیشران‌ها می‌توانند به عوامل اختلال‌آفرین، تسریع‌کننده یا حتی تشدیدکننده بحران‌های امنیتی تبدیل شوند (Wilson, ۲۰۰۴).

بر اساس آنچه مطرح شد چهار پیشران تعاملی در اولویت اول، سه پیشران کلیدی در اولویت دوم، دو پیشران وابسته در اولویت سوم و دو پیشران نوظهور در اولویت چهارم قرار گرفتند.

جدول (۴)، دسته‌بندی پیشران‌ها بر اساس جانمایی در ماتریس ویلسون (یافته‌های محققین)

رده پیشران	عنوان پیشران‌ها	فناوری‌های نوظهور مرتبط
تعاملی	به‌کارگیری فناوری‌های نوظهور اطلاعاتی – ارتباطی در همگرایی با هوش مصنوعی نظامی	***هوش مصنوعی و یادگیری ماشین*** برای تحلیل خودکار داده‌ها و تصمیم‌سازی هوشمند؛ ***محاسبات شناختی*** برای ایجاد سامانه‌های تصمیم‌یار نظامی؛ ***اینترنت اشیای نظامی*** جهت اتصال و یکپارچه‌سازی تجهیزات، حسگرها و سامانه‌های رزمی؛ ***شبکه‌های ارتباطی نسل پنجم و ششم (۵G و ۶G)*** برای انتقال سریع و امن داده‌های میدانی؛ ***رایانش لبه‌ای و هم‌محور*** برای پردازش محلی داده‌ها و کاهش وابستگی به مراکز داده مرکزی؛ ***یادگیری ماشین کوانتومی*** برای افزایش سرعت تحلیل‌های پیچیده در مقیاس راهبردی؛ ***رباتیک خودمختار و ازدحامی*** برای عملیات گروهی بدون فرمان مستقیم انسانی؛ ***واقعیت افزوده و واقعیت مجازی***

رده پیشران	عنوان پیشران‌ها	فناوری‌های نوظهور مرتبط
		برای آموزش و شبیه‌سازی‌های نظامی هوشمند؛ و ***تحلیل کلان‌داده‌ها*** برای استخراج الگوهای رفتاری و پیش‌بینی تهدیدات آینده.
	رشد مضاعف جنگ شناختی و نفوذ ادراکی در عملیات آینده	***فناوری‌های عصبی و رابط‌های مغز و رایانه*** برای تعامل مستقیم میان سامانه‌های دیجیتال و ذهن انسان، ***رلیانش عاطفی*** برای شناسایی و تحلیل احساسات نیروها و دشمنان، ***رسانه‌های مصنوعی و فناوری‌های جعل عمیق*** به‌منظور هدایت ادراک و تولید واقعیت‌های کاذب، ***عصب‌ارگونومی*** برای بهینه‌سازی عملکرد ذهنی در محیط‌های عملیاتی، ***همزیستی انسان و ماشین*** در تصمیم‌سازی‌های شناختی، ***واقعیت مجازی و واقعیت توسعه‌یافته*** برای آموزش و القای موقعیت‌های ادراکی شبیه‌سازی‌شده و در نهایت ***تحلیل داده‌های زیستی و عصبی*** جهت پیش‌بینی و کنترل واکنش‌های شناختی.
	پیچیدگی و ابهام در محیط عملیاتی با همگرایی فناوری‌ها	***فناوری‌های همگرای چنددامنه‌ای*** برای ادغام عرصه‌های زمینی، هوایی، دریایی، فضایی و سایبری، هوش مصنوعی و الگوریتم‌های تصمیم‌گیری خودکار برای تحلیل و واکنش بلادرنگ در شرایط پیچیده؛ ***سامانه‌های خودمختار و ازدحامی*** با قابلیت تعامل جمعی غیرقابل پیش‌بینی، محاسبات کوانتومی که با توان پردازشی و رمزنگاری پیشرفته خود ساختار اطمینان اطلاعاتی را دگرگون می‌کند، ***فضای سایبری هوشمند*** برای حملات و دفاع‌های چندلایه خودآموز، شبکه‌های ارتباطی نسل ششم (۶G) برای انتقال فوق‌سریع داده‌ها میان واحدهای رزمی، ***کلان‌داده‌ها و تحلیل پیش‌نگرانه*** برای درک و مدل‌سازی پویایی‌های نبرد، ***رایانش لبه‌ای و توزیع‌شده*** برای پردازش مستقل در نقاط مختلف شبکه، ***فناوری‌های فضا پایه و ماهواره‌ای نوظهور*** برای گسترش میدان عملیات به مدارهای فضایی و ***فناوری‌های شبیه‌سازی محیط‌های پیچیده*** جهت آموزش و تصمیم‌سازی در شرایط نامطمئن.
	تغییرات ژئوپلیتیکی	فناوری‌های زیرساختی کلیدی دیجیتال نظیر ***اینترنت اشیاء صنعتی***، زیرساخت‌های ابری بومی و شبکه‌های داده حاکمیتی،

رده پیشران	عنوان پیشران‌ها	فناوری‌های نوظهور مرتبط
	فناورانه و تهدیدات ناشی از وابستگی	فناوری‌های نیمه‌هادی پیشرفته و ریزتراشه‌ها، محاسبات کوانتومی و رمزنگاری کوانتومی ملی، هوش مصنوعی بومی و سامانه‌های تصمیم‌یار ملی، زنجیره‌بلوک برای ایجاد زنجیره‌های تأمین مقاوم و شفاف، ***فناوری‌های انرژی نو و ذخیره‌سازی هوشمند*** برای کاهش وابستگی به منابع متمرکز، ***فناوری‌های فضاپایه و ماهواره‌ای مستقل*** برای کنترل داده‌های جغرافیایی و ارتباطی، ***فناوری‌های سایبری و امنیت داده مستقل*** برای حفاظت از زیرساخت‌های حیاتی، زیست‌فناوری‌های ژئوپلیتیکی در حوزه امنیت زیستی و سلامت ملی و ***فناوری‌های تولید پیشرفته (چاپ سه‌بعدی و تولید افزایشی)*** برای خودکفایی صنعتی.
کلیدی	پیشرفت زیرساخت‌های مخابراتی نظامی	***فناوری نسل پنجم (5G) و ششم (6G) نظامی*** برای ایجاد ارتباطات فوق‌سریع و امن، ***شبکه‌های ارتباطی ماهواره‌ای کم‌مدار*** برای پوشش جهانی و پیوسته، فناوری‌های ارتباطات کوانتومی جهت ایجاد شبکه‌های غیرقابل نفوذ و رمزنگاری‌شده، ***رادیوهای شناختی*** برای استفاده هوشمند از طیف فرکانسی، ***شبکه‌های مش*** به‌منظور حفظ ارتباط در شرایط نبرد و تخریب زیرساخت، ***میکروماهواره‌ها و سامانه‌های ارتباطات تاکتیکی پهپادی*** برای ایجاد شبکه‌های متحرک، فناوری‌های لیزری و نوری در انتقال داده‌های حجیم، ***رایانش لبه‌ای*** برای پردازش بلادرنگ در میدان نبرد، سیستم‌های فرماندهی و کنترل یکپارچه و امنیت سایبری ارتباطی مبتنی بر هوش مصنوعی.
	بهره‌گیری و استفاده از کلان‌داده و تحلیل هوشمند در همگرایی تحلیلی	***فناوری‌های کلان‌داده*** برای جمع‌آوری و ذخیره‌سازی داده‌های عظیم از منابع مختلف، ***تحلیل پیش‌بین*** برای شناسایی روندها و تهدیدات آینده، ***هوش مصنوعی و یادگیری ماشین*** برای استخراج الگوهای پنهان از داده‌ها، ***یادگیری عمیق*** در تشخیص خودکار اهداف و رفتارها، ***رایانش لبری و لبه‌ای جهت پردازش توزیع‌شده‌ی داده‌ها در مقیاس وسیع***، ***پردازش زبان طبیعی*** برای تحلیل اطلاعات متنی و ارتباطی، ***تحلیل داده‌های چندوجهی*** برای ترکیب داده‌های متنی، تصویری و سیگنالی، ***فناوری‌های***

رده پیشران	عنوان پیشران‌ها	فناوری‌های نوظهور مرتبط
		مصورسازی هوشمند داده‌ها برای تصمیم‌سازی سریع‌تر، ***تحلیل شناختی در پشتیبانی تصمیمات نظامی و فناوری‌های امنیت داده و حاکمیت اطلاعات*** برای حفاظت از داده‌های حیاتی.
	توسعه یکپارچه‌سازی دیجیتالی و فرماندهی شبکه‌محور	***شبکه‌های ارتباطی امن و مقاوم*** برای تبادل داده‌های لحظه‌ای، ***سیستم‌های فرماندهی و کنترل یکپارچه*** برای هماهنگی تمام‌سویه نیروها، ***اینترنت اشیای نظامی*** برای اتصال حسگرها، سامانه‌ها و تجهیزات رزمی، ***هوش مصنوعی و یادگیری ماشین*** برای تصمیم‌گیری خودکار و تحلیل سریع داده‌ها، ***رایانش لبه‌ای و توزیع‌شده*** برای پردازش داده در نقاط میدانی، ***ربات‌های خودمختار و سامانه‌های ازدحامی*** برای عملیات هماهنگ و شبکه‌محور، ***فضای سایبری هوشمند*** برای دفاع و امنیت اطلاعاتی، ***کلان‌داده و تحلیل هوشمند*** برای پشتیبانی تصمیمات لحظه‌ای و ***شبیه‌سازی و تمرین دیجیتال*** برای آموزش فرماندهان و نیروها در محیط شبکه‌محور.
وابسته	توسعه و کاربرد شبیه‌سازها در جهت آموزش پیشرفته	***واقعیت مجازی و واقعیت افزوده*** برای ایجاد محیط‌های شبیه‌سازی‌شده کاملاً واقع‌گرایانه، ***واقعیت ترکیبی و واقعیت توسعه‌یافته*** برای تمرین سناریوهای پیچیده و تعامل با محیط‌های دیجیتال، ***شبیه‌سازی مبتنی بر هوش مصنوعی*** برای تولید سناریوهای پویا و پاسخ‌دهی خودکار، ***شبیه‌سازی چندعامل و ازدحامی*** برای آموزش در محیط‌های چندواحدی و تعاملات گروهی، ***رایانش ابری و توزیع‌شده*** جهت پردازش داده‌های شبیه‌سازی بزرگ و لحظه‌ای، ***کلان‌داده و تحلیل هوشمند*** برای بازخورد دقیق عملکرد و بهبود آموزش، ***شبیه‌سازی شبکه‌محور و فرماندهی دیجیتال*** برای تمرین تصمیم‌گیری در محیط‌های شبکه‌محور و ***یادگیری ماشین و تحلیل رفتار*** برای ارزیابی و بهبود مهارت‌های فردی و گروهی.
	به‌کارگیری گسترده	***مهندسی ژنتیک و ویرایش ژنومی*** برای مقابله با عوامل بیماری‌زا و تقویت ایمنی نیروها، ***زیست‌حسگرها و نانوحسگرهای زیستی***

رده پیشران	عنوان پیشران‌ها	فناوری‌های نوظهور مرتبط
	زیست‌فناوری‌ها ی امنیتی	برای پایش سلامت و شناسایی تهدیدات میدانی، ***زیست‌داروها و واکسن‌های پیشرفته*** برای پیشگیری و درمان تهدیدات زیستی، ***بیوانفورماتیک و تحلیل داده‌های زیستی*** برای شناسایی الگوها و پیش‌بینی تهدیدات، ***زیست‌فناوری‌های همگرای اطلاعاتی– ارتباطی*** جهت هم‌افزایی داده‌های زیستی با سامانه‌های اطلاعاتی، ***نانوفناوری زیستی*** برای تولید سامانه‌های پایش و دارورسانی دقیق، ***رسانه‌های مصنوعی زیستی*** برای طراحی و تولید عوامل زیستی کاربردی و ***اتوماسیون و رباتیک زیستی*** برای انجام عملیات میدانی و آزمایشگاهی در شرایط خطرناک.
نوظهور	دسترسی غیردولتی‌ها به فناوری اطلاعاتی نظامی	***فناوری‌های رمزنگاری پیشرفته و کوانتومی*** برای حفاظت از اطلاعات حساس، ***سامانه‌های کنترل دسترسی هوشمند*** برای مدیریت و محدودسازی ورود غیرمجاز، ***شبکه‌های ایمن و مقاوم در برابر نفوذ*** برای حفاظت از تبادل داده‌ها، ***سامانه‌های شناسایی و پایش تهدید سایبری*** برای شناسایی فعالیت‌های غیرمجاز، ***هوش مصنوعی و یادگیری ماشین در امنیت سایبری*** برای تحلیل رفتار کاربران و پیش‌بینی نفوذ، ***فناوری‌های بلاک‌چین و دفترکل توزیع‌شده*** برای ثبت امن تراکنش‌ها و تغییرناپذیری داده‌ها، ***امنیت شبکه‌های ابری و مجازی‌سازی شده*** برای محافظت از داده‌ها و منابع حیاتی و ***فناوری‌های تشخیص و احراز هویت بیومتریک و چندعاملی*** برای اطمینان از هویت کاربران مجاز.
	تقویت نوآوری اطلاعاتی در امنیت سایبری نظامی	***هوش مصنوعی و یادگیری ماشین در امنیت سایبری*** برای تشخیص و مقابله خودکار با تهدیدات، ***یادگیری عمیق و تحلیل رفتاری*** شناسایی نفوذهای پیچیده و پیش‌بینی رفتار مهاجمان، ***فناوری‌های رمزنگاری پیشرفته و کوانتومی*** برای حفاظت از داده‌ها و ارتباطات حساس، ***امنیت شبکه‌های ابری و توزیع‌شده*** برای مدیریت و حفاظت از منابع حیاتی، ***فناوری‌های شناسایی و پاسخ خودکار*** برای کاهش زمان واکنش به تهدیدات، ***بلاک‌چین و دفترکل توزیع‌شده*** برای اطمینان از یکپارچگی داده‌ها و شفافیت

ردهٔ پیشران	عنوان پیشران‌ها	فناوری‌های نوظهور مرتبط
		تراکنش‌ها، سیستم‌های مدیریت هوشمند آسیب‌پذیری‌ها و وصله‌گذاری خودکار و تحلیل پیش‌بینانه تهدیدات و شبیه‌سازی حملات سایبری.

با توجه به فراترکیب انجام شده و تحلیل سامانه‌ای پیشران‌ها و فناوری‌های نوظهور مرتبط، می‌توان روند تأثیر این فناوری‌ها و بلوغ پیشران‌ها را در بازه زمانی ده‌ساله (۱۴۰۴–۱۴۱۴) شناسایی نمود. نتایج نشان داد که هر یک از پیشران‌ها با سرعت و شدت متفاوتی در طول زمان رشد و اثرگذار هستند. از سوی دیگر همگرایی فناوری‌ها نقش کلیدی در تسریع بلوغ و تحقق توان عملیاتی هر پیشران دارد. در بازه اولیه (۱۴۰۴–۱۴۰۷)، تمرکز عمدتاً بر توسعه و پیاده‌سازی فناوری‌های پایه و آزمایشی است؛ در بازه میانی (۱۴۰۷–۱۴۱۰)، گسترش هم‌زمان سامانه‌ها و آغاز یکپارچه‌سازی فناوری‌ها، موجب افزایش اثرگذاری و بلوغ نسبی شده و در بازه پایانی (۱۴۱۰–۱۴۱۴)، فناوری‌ها به سطح بلوغ عملیاتی رسیده و پیشران‌ها با بیشترین توان خود بر محیط‌های عملیاتی و ساختار امنیت ملی و دفاعی تأثیر می‌گذارند. این موضوع نشان‌دهنده یک الگوی افزایشی و تسریع‌شونده در اثرگذاری فناوری‌های نوظهور است که تحت تأثیر عوامل کلان‌داده، هوش مصنوعی، شبکه‌محور شدن فرماندهی و یکپارچه‌سازی سامانه‌ها قرار دارد. بر این اساس در جدول (۵) روند زمانی تأثیر فناوری‌ها و بلوغ پیشران‌ها در طول ده سال را به تفکیک هر پیشران می‌توان مشاهده نمود.

جدول (۵)، روند زمانی تأثیر فناوری‌ها و بلوغ پیشران‌ها در بازه ده‌ساله (یافته‌های محققین)

ردی ف	پیشران	بازه ۱۴۰۴– ۱۴۰۷	بازه ۱۴۰۷– ۱۴۱۰	بازه ۱۴۱۰– ۱۴۱۴	روند کلی تأثیر
۱	به‌کارگیری فناوری‌های نوظهور اطلاعاتی – ارتباطی در همگرایی با	آغاز توسعه و پیاده‌سازی سامانه‌های هوشمند و	گسترش سامانه‌های ترکیبی هوش مصنوعی با	بلوغ فناوری‌های هوشمند و شبکه‌های همگرا؛ افزایش	تأثیر رو به افزایش و شتابان

ردی ف	پیشران	بازه ۱۴۰۴– ۱۴۰۷	بازه ۱۴۰۷– ۱۴۱۰	بازه ۱۴۱۰– ۱۴۱۴	روند کلی تأثیر
	هوش مصنوعی نظامی	شبکه‌های داده‌ای	ربات‌ها و پهپادها	اتوماسیون تصمیم‌گیری	
۲	رشد مضاعف جنگ شناختی و نفوذ ادراکی در عملیات آینده	استفاده محدود از تحلیل داده‌ها و حملات شناختی	افزایش حملات شناختی پیشرفته و نفوذ ادراکی هدفمند	بلوغ جنگ شناختی و یکپارچگی با سامانه‌های شبکه‌محور	تأثیر فزاینده و مستمر
۳	پیچیدگی و ابهام در محیط عملیاتی با همگرایی فناوری‌ها	آغاز همگرایی فناوری‌های زمینی، هوایی و سایبری	گسترش سامانه‌های خودمختار و ازدحامی؛ افزایش عدم قطعیت	محیط عملیاتی فوق‌پیچیده و غیرقابل پیش‌بینی	تأثیر پیوسته و صعودی
۴	تغییرات ژئوپلیتیکی فناورانه و تهدیدات ناشی از وابستگی	افزایش وابستگی به فناوری‌های کلیدی خارجی	ظهور بازیگران جدید و افزایش تهدیدات استراتژیک	تثبیت نقش فناوری در توزیع قدرت و امنیت ملی	تأثیر قابل توجه و رو به افزایش
۵	پیشرفت زیرساخت‌های مخابراتی نظامی	توسعه شبکه‌های 5G و سیستم‌های ارتباطی تاکتیکی	افزایش پهنای باند، امنیت و شبکه‌های ماهواره‌ای کم‌مدار	زیرساخت شبکه‌محور و مقاوم؛ تسهیل عملیات پیچیده	تأثیر فزاینده و تقویتی
۶	بهره‌گیری و استفاده از کلان‌داده و تحلیل هوشمند در همگرایی تحلیلی	شروع جمع‌آوری داده‌ها و تحلیل اولیه	توسعه هوش مصنوعی تحلیلی و پردازش بلادرنگ	بلوغ سامانه‌های پیش‌بین و تصمیم‌یار هوشمند	تأثیر رو به افزایش و تسریع‌شونده

ردی ف	پیشران	بازه ۱۴۰۴– ۱۴۰۷	بازه ۱۴۰۷– ۱۴۱۰	بازه ۱۴۱۰– ۱۴۱۴	روند کلی تأثیر
۷	توسعه یکپارچه‌سازی دیجیتالی و فرماندهی شبکه‌محور	آغاز پیاده‌سازی سامانه‌های شبکه‌محور محدود	گسترش شبکه‌های فرماندهی دیجیتال و یکپارچه	بلوغ فرماندهی شبکه‌محور و هماهنگی تمام‌سویه	تأثیر پایدار و تسهیل‌کننده
۸	توسعه و کاربرد شبیه‌سازها در جهت آموزش پیشرفته	شبیه‌سازی‌های مجازی و واقعیت افزوده اولیه	توسعه شبیه‌سازی‌های هوشمند و چندعامل	آموزش پیشرفته مبتنی بر شبیه‌سازی و تحلیل عملکرد نیروها	تأثیر افزایشی و پایدار
۹	به‌کارگیری گسترده زیست‌فناوری‌های امنیتی	تحقیق و توسعه زیست‌فناوری‌های بومی	پیاده‌سازی آزمایشی سامانه‌های زیستی و پایش تهدید	بلوغ زیست‌فناوری‌های امنیتی و دفاعی؛ خودکفایی	تأثیر صعودی و استراتژیک
۱۰	دسترسی غیردولتی‌ها به فناوری اطلاعاتی نظامی	محدودسازی و نظارت اولیه	افزایش کنترل و رصد دسترسی‌ها	ایجاد سامانه‌های امن، مقاوم و هوشمند برای جلوگیری از نفوذ	تأثیر تثبیتی و کنترلی
۱۱	تقویت نوآوری اطلاعاتی در امنیت سایبری نظامی	توسعه الگوریتم‌های اولیه و سامانه‌های پایش	گسترش هوش مصنوعی و تحلیل رفتاری پیشرفته	بلوغ نوآوری سایبری و سامانه‌های دفاعی هوشمند	تأثیر فزاینده و مستمر

یافته‌ها نشان می‌دهد پیشران‌های فناورانه نوظهور اطلاعاتی-ارتباطی نقش تعیین‌کننده‌ای در شکل‌دهی به امنیت دفاعی ایران در افق ۱۴۱۴ ایفا می‌کنند. تحلیل روند زمانی ده‌ساله نشان می‌دهد که این پیشران‌ها با شدت و سرعت متفاوت رشد و اثرگذاری دارند، اما همگی تحت تأثیر همگرایی فناوری‌های نوظهور، توسعه زیرساخت‌ها و یکپارچه‌سازی سامانه‌ها به بلوغ عملیاتی می‌رسند.

در مجموع، یافته‌ها تأکید می‌کنند که همگرایی فناوری‌ها و پیشران‌ها، یکپارچه‌سازی دیجیتالی و توسعه سامانه‌های هوشمند و شبکه‌محور، مسیر اصلی تحقق امنیت دفاعی پایدار در افق ۱۴۱۴ است. این روندها نه‌تنها امکان تصمیم‌گیری سریع و دقیق در محیط‌های پرابهام و پیچیده را فراهم می‌کنند، بلکه سطح آمادگی راهبردی و توان دفاعی ایران را در برابر تهدیدات داخلی و خارجی به‌طور قابل توجهی ارتقاء می‌دهند.

بحث و نتیجه‌گیری:

پژوهش حاضر با هدف شناسایی و تحلیل پیشران‌های ناشی از فناوری‌های نوظهور اطلاعاتی–ارتباطی و اثر آن‌ها بر امنیت دفاعی جمهوری اسلامی ایران در افق ۱۴۱۴ انجام شد. در گام نخست، ۲۲ پیشران فناورانه از طریق فراترکیب مطالعات داخلی و خارجی استخراج و با استفاده از روش دلفی و تحلیل ساختاری–عدم قطعیت، این پیشران‌ها در قالب ۱۱ کلان‌پیشران سازمان‌دهی شدند.

یافته‌ها نشان داد فناوری‌های نوظهور اطلاعاتی–ارتباطی، به‌ویژه هوش مصنوعی نظامی، یادگیری ماشینی، کلان‌داده و تحلیل هوشمند، امنیت سایبری، واقعیت‌های ترکیبی و زیرساخت‌های مخابراتی پیشرفته، بیشترین نقش را در بازتعریف امنیت دفاعی کشور در افق ده‌ساله ایفا می‌کنند. این نتایج تأکید می‌کنند که آینده امنیت دفاعی نه صرفاً بر توان سخت‌افزاری، بلکه بر توانمندی‌های نرم‌افزاری، شبکه‌ای و داده‌محور استوار است. پیشران‌هایی مانند به‌کارگیری فناوری‌های نوظهور اطلاعاتی–ارتباطی در همگرایی با هوش مصنوعی نظامی، بهره‌گیری از کلان‌داده و تحلیل هوشمند و توسعه یکپارچه‌سازی دیجیتالی و فرماندهی شبکه‌محور، بیشترین سرعت رشد و تأثیرگذاری را در دهه آینده داشته و به‌عنوان پیشران‌های کلیدی تحول دفاعی و امنیت ملی شناخته می‌شوند. این پیشران‌ها با تسریع اتوماسیون تصمیم‌گیری، هوشمندسازی سامانه‌ها و شبکه‌محور شدن فرماندهی، توان عملیاتی نیروهای مسلح را در محیط‌های پیچیده و پرابهام افزایش می‌دهند. ضمن اینکه پیشران‌هایی مانند رشد مضاعف جنگ شناختی و نفوذ ادراکی، پیچیدگی محیط عملیاتی با همگرایی فناوری‌ها و تغییرات ژئوپلیتیکی فناورانه و وابستگی‌ها، اثرات بلندمدت و پیوسته‌ای دارند و نشان‌دهنده ضرورت تحلیل شناختی، مدیریت عدم قطعیت و توجه به امنیت راهبردی هستند. این روندها بیانگر آن است که فناوری‌ها صرفاً ابزار پیشرفت نیستند، بلکه عامل بازتوزیع قدرت و تسلط راهبردی در

محیط دفاعی و امنیتی محسوب می‌شوند. همچنین پیشران‌های آموزش پیشرفته با شبیه‌سازها، به‌کارگیری زیست‌فناوری‌های امنیتی، دسترسی غیردولتی‌ها به فناوری‌های نظامی و تقویت نوآوری اطلاعاتی در امنیت سایبری نیز نشان‌دهنده نیاز به خودکفایی، نوآوری و مدیریت هوشمند تهدیدات هستند. بهره‌گیری مؤثر از این پیشران‌ها موجب کاهش ریسک عملیاتی، افزایش آمادگی نیروها و ارتقاء مقاومت سامانه‌ها در برابر تهدیدات پیچیده و چندبعدی خواهد شد.

مقایسه یافته‌های پژوهش حاضر با ادبیات موجود نشان می‌دهد نتایج این تحقیق با مطالعات داخلی و بین‌المللی همخوانی دارد. در سطح داخلی، رساله موحدی‌صفت (۱۴۰۲) بر اهمیت فناوری‌های هوشمند، داده‌کاوی و یادگیری ماشین در بازتعریف مفاهیم امنیت دفاعی تأکید دارد و نقش کلان‌داده و سامانه‌های هوشمند در تحولات آینده امنیتی را مورد بررسی قرار داده است. همچنین، قنواتی (۱۴۰۲) مبتنی بر رویکرد نظام نوآوری فناورانه، توسعه فناوری‌های نوظهور و شناسایی روندهای آینده را در بستر شرایط بومی تحلیل کرده است. پژوهش آذر و مسلمی (۱۴۰۳) نیز نشان می‌دهد که فناوری‌های نوظهور، توانمندی‌ها و قابلیت‌های جدیدی در حوزه قدرت سایبری ایجاد می‌کنند و محیط راهبردی را دچار تغییر نموده‌اند. پژوهش احمدی و همکاران (۱۴۰۲) بر تأثیر ظهور فناوری‌های نوظهور و هوش مصنوعی بر تغییرات امنیت ملی و مناسبات بین‌المللی تأکید دارد و شریف‌زاده و همکاران (۱۴۰۳) نقش فناوری‌های نوظهور و هوش مصنوعی را به‌عنوان پیشران‌های مهم در تحولات دیپلماتیک و روابط سیاسی آینده برجسته می‌کنند. در سطح بین‌المللی نیز، پژوهش کاپا (۲۰۲۴) با تمرکز بر فناوری‌های اطلاعات شناختی و جنگ‌های شناختی، ضرورت همگرایی فناوری‌های نوظهور اطلاعاتی-ارتباطی با علوم اعصاب و رسانه‌های دیجیتال را نشان داده است. دویکاریو (۲۰۲۳) به روندهای فناوری‌های نوظهور و مخرب در دفاع و امنیت پرداخته و همگرایی این فناوری‌ها با جنگ هیبریدی را تحلیل کرده است. آدیری و ابروشان (۲۰۲۴) بر ابهام مرز صلح و جنگ در دنیای آینده با ورود فناوری‌های هوشمند و خطرات ناشی از حملات زنجیره تأمین و تهدیدات سایبری تأکید دارند. همچنین، بیننديجک و همکاران (۲۰۲۰) در گزارش مؤسسه رند به ضرورت انطباق ارتش‌های آینده با تصمیم‌گیری مبتنی بر داده و اتوماسیون اشاره کرده‌اند.

یکی از مهم‌ترین نوآوری‌های تحقیق، شـــناخت تعاملات میان فناوری‌ها و همگرایی فناوری‌های اطلاعاتی–ارتباطی با حوزه‌هایی نظیر هوش مصـــنوعی نظامی، فرماندهی شبکه‌محور، جنگ شناختی و تحلیل هوشمند داده‌ها است که می‌تواند منجر به تحول مفهومی در الگوهای امنیت دفاعی کشـــور شـــود. این پیشـــران‌ها از قدرت تأثیرگذاری بالایی برخور بوده و ســـطح عدم قطعیت در تحقق آن‌ها نیز بالاســـت، از این رو تحلیل آن‌ها از منظر سناریوپردازی راهبردی و آینده‌نگری اهمیت ویژه‌ای دارد.

ســـطح تعمیم‌پذیری یافته‌ها برای نظام دفاعی جمهوری اســـلامی ایران بالا ارزیابی می‌شـــود، مشـــروط بر آنکه ویژگی‌های ســـاختاری، ظرفیت‌های فناورانه داخلی و الگوی تهدیدات منطقه‌ای در اجرای نتایج مدنظر قرار گیرد. علاوه بر این، یافته‌ها می‌توانند در توسعه چارچوب‌های ارزیابی تهدیدات فناورانه، تدوین برنامه‌های تحقیق و توسعه دفاعی و به‌روزرســـانی دکترین‌های نظامی کاربردی باشـــند. محدودیت‌های پژوهش شـــامل عدم شـــفافیت در برخی روندهای فناورانه جهانی، کمبود داده‌های بومی درباره فناوری‌های نوظهور نظامی و پیچیدگی در تعیین زمان‌بندی دقیق تحقق فناوری‌ها اســـت که بر پیش‌بینی‌پذیری سناریوهای آینده اثرگذار هستند.

در جمع‌بندی، یافته‌های پژوهش، پاسـخی علمی و دقیق به سـؤال اصـلی تحقیق درباره پیشـــران‌های تحول‌آفرین در امنیت دفاعی ایران در افق ۱۴۱۴ ارائه می‌دهند و مبنای تحلیلی محکمی برای ارتقاء هوشمندانه و آینده‌نگرانه توان دفاعی کشور در برابر تحولات سریع فناوری‌های نوظهور اطلاعاتی–ارتباطی فراهم می‌آورند.

توصیه‌های کلیدی برای سیاست‌گذاران دفاعی

۱- سرمایه‌گذاری هدفمند در حوزه فناوری نوظهور هوش مصنوعی نظامی و فرماندهی شبکه‌محور در راستای تقویت امنیت دفاعی

۲- ایجاد مراکز تحلیل داده پیش‌بین، مبتنی بر هوش مصـــنوعی برای پشـــتیبانی تصمیم‌سازی راهبردی

۳- تدوین نظام‌نامه کاهش وابســـتگی به تجهیزات و پلتفرم‌های خارجی در حوزه‌های حیاتی مانند ارتباطات، شبیه‌سازی و حسگرهای نظامی

۴- ایجاد واحد ویژه رصـــد فناوری‌های در دســـترس بازیگران غیردولتی به‌منظور شناسایی الگوهای استفاده و طراحی واکنش‌های متقارن و نامتقارن

تشکر و قدردانی

این مقاله بخشی از یافته‌های رساله دکتری با عنوان «پیامدسنجی فناوری‌های نوظهور نظامی-امنیتی و اطلاعاتی-ارتباطی بر امنیت دفاعی ایران ۱۴۱۴: سناریوها و راهبردها» است که در گروه آینده‌پژوهی دانشکده علوم اجتماعی دانشگاه بین‌المللی امام خمینی (ره) انجام شده است. نویسنده از راهنمایی‌ها و حمایت‌های استاد محترم راهنما و اساتید مشاور و نیز مشارکت متخصصان گران‌قدر در مراحل گردآوری داده‌ها و تحلیل آن‌ها صمیمانه قدردانی می‌نماید.

تضاد منافع:

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

منابع

منابع فارسی

- احمدی، علی. زرگر، افشین؛ و آدمی، علی. (۱۴۰۲). فناوری هوش مصنوعی و تغییر در امنیت ملی دولت‌ها. *سیاست دفاعی*، ۳۲(۱۲۳)، ۳۹-۶۴. (https://dor.isc.ac/dor/۲۰.۱۰۰۱.۱.۱۰۲۵۵۰۸۷.۱۴۰۲.۳۲.۱۲۳.۲.۰)
- آذر، داود و مسلمی، حسین. (۱۴۰۳). ارکان جهت‌ساز راهبردی قدرت سایبری ارتش جمهوری اسلامی ایران. *مطالعات بین رشته‌ای دانش راهبردی*، ۱۴(۵۶)، ۱۱۱-۱۳۱. (https://smsnds.sndu.ac.ir/article_۳۰۸۴.html)
- چوری، علی. (۱۴۰۲). چالش‌ها و فرصت‌های فناوری‌های نوظهور در مدیریت استراتژیک. *تکنولوژی در کارآفرینی و مدیریت استراتژیک*، ۲(۴)، ۱-۷. (https://doi.org/۱۰.۶۱۸۳۸/kman.jtesm.۲.۴.۱)
- سند جامع علم و فناوری در حوزه دفاعی و امنیتی جمهوری اسلامی ایران، مصوب جلسه ۸۳۷ مورخ ۱۳۹۹/۱۲/۰۵ شورای عالی انقلاب فرهنگی، مرکز پژوهش‌های مجلس شورای اسلامی. (https://rc.majlis.ir/fa/law/show/۱۶۵۱۱۷۷)

- شریف زاده، زهرا. میرکوشش، امیرهوشنگ و حسینی، محمد مهدی. (۱۴۰۳). بررسی آثار سیاست‌های توسعهٔ فناوری‌های نوین و هوش مصنوعی در گسترش راهبردهای سیاسی کلان با رویکرد سیاست‌های کلی نظام. سیاست‌های راهبردی و کلان، ۱۲(۴۵)، ۲۴-۴۷. (https://dor.isc.ac/dor/۲۰.۱۰۰۱.۱.۲۳۴۵۲۵۴۴.۱۴۰۳.۱۲.۴۵.۲.۳)
- قنواتی، فاطمه. (۱۳۹۲). *تدوین مدل بومی توسعه فناوری های نوظهور بر مبنای رویکرد نظام نوآوری فناورانه؛ مطالعه موردی ساخت افزایشی*، پایان‌نامه دکتری، دانشکده مدیریت، دانشگاه علم و صنعت ایران.(https://dor.isc.ac/dor/۲۰.۱۰۰۱.۱.۲۳۴۵۲۵۴۴.۱۴۰۳.۱۲.۴۵.۲.۳)
- کولیوند، خلیل. (۱۴۰۱). آینده‌نگاری سیگنال‌های ضعیف تغییر در پیشایند بازی جنگ ترکیبی روسیه علیه اوکراین. دوفصلنامه بازی جنگ، ۵(۱۱)، ۸۵-۱۰۶(https://doi.org/۱۰.۲۲۰۳۴/ijwg.۲۰۲۳.۳۸۷۳۶۵.۱۰۳۸)
- کولیوند، خلیل. (۱۴۰۱). واکاوی آینده‌پژوهلنه مؤلفه‌های الگوی مدیریت دانش نظامی در دفاع همه جانبه نبردهای آینده با رویکرد جنگ ترکیبی. فصلنامه مطالعات جنگ، ۴(۱۵)، ۵-۳۲. (https://doi.org/۱۰.۲۲۰۳۴/qjws.۲۰۲۳.۱۹۸۷۰۵۷.۱۱۰۷)
- کولیوند، خلیل. ستاری‌خواه علی و سپهری، محمد. (۱۴۰۲). سناریوهای فراروی جنگ ترکیبی اسرائیل علیه جمهوری اسلامی ایران در افق ۱۴۰۷. علوم و فنون نظامی، ۱۹(۶۶)، ۱۸۹-۲۱۸.(https://doi.org/۱۰.۲۲۰۳۴/qjmst.۲۰۲۴.۱۹۸۶۹۰۸.۱۸۳۱)
- گودرزی، غلامرضا و اجلالی، محمدمهدی. (۱۴۰۰). تحلیل روندهای آینده فناوری‌های دفاعی در افق ده‌ساله. آینده‌پژوهی دفاعی، ۶(۲۳)، ۳۷-۵۷.(https://doi.org/۱۰.۲۲۰۳۴/dfsr.۲۰۲۲.۵۳۰۷۷۷.۱۴۹۷)

- محمدی فاتح، اصغر و ابراهیمی، سید عباس. (۱۳۹۹). شناسایی و رتبه‌بندی فناوری‌های اطلاعاتی نوظهور در بخش دفاعی- نظامی. آینده‌پژوهی دفاعی، ۵(۱۷)، ۱۷۱-۱۴۳.(https://doi.org/۱۰.۲۲۰۳۴/dfsr.۲۰۲۰.۱۲۸۶۶۸.۱۳۹۵)
- موحدی صفت، محمدرضا. سپهری، محمد. هلیلی، خداداد؛ و فرزانه، عادل. (۱۴۰۲). مقاله پژوهشی: الگوی دفاع هوشمند مبتنی بر فناوری اینترنت اشیاء. مطالعات دفاعی استراتژیک، ۲۱(۹۲)، ۶۹-۹۲.(https://sds.sndu.ac.ir/article_۲۴۲۱.html)
- موسوی شهیدی، سید مهدی. وحدانی‌نیا، ولی‌اله و حسینی، سید ناصر. (۱۴۰۳). ایران در آستانه یک تقاطع ژئوپلیتیک: چالش‌های ناشی از سناریوی محتمل کریدور زنگزور. آینده‌پژوهی دفاعی، ۹(۳۵)، ۱-۲۵.(https://doi.org/۱۰.۲۲۰۳۴/dfsr.۲۰۲۵.۲۰۴۷۰۸۲.۱۸۵۶)
- نجات پور، مجید. فرخی، مرتضی. سجادی، محسن؛ و هادی پور، میثم. (۱۴۰۱). تحلیل جایگاه هوش مصنوعی در توسعه سازمان نظامی. مدیریت و پژوهش‌های دفاعی، ۲۱(۹۸)، ۱۶۴-۱۴۳.(https://dor.isc.ac/dor/۲۰.۱۰۰۱.۱.۲۰۰۸۶۱۲۱.۱۴۰۱.۲۱.۹۸.۱.۲)

منابع انگلیسی

- Adeyeri, A. & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*, *15*(11), 682.(https://doi.org/10.3390/info15110682)
- Ahmadi, A. Zargar, A. & Adami, A. (2023). Artificial Intelligence Technology and Change in the National Security of States. Defense Policy, 32(123), 39-64, **[In Persian]**. (https://dor.isc.ac/dor/20.1001.1.10255087.1402.32.123.2.0)
- Azar, D. and moslemi, H. (2024). The pillars of the cyber power of the Islamic Republic of Iran Army. *Quarterly Journal of Interdisciplinary Studies on Strategic Knowledge*, *14*(56), 131-111, **[In Persian]**. (https://smsnds.sndu.ac.ir/article_3084.html)
- Bagawade, J. A. (2023). New Emerging technology. *AG Volumes*, 85-94. (https://agvolumes.com)

- Binnendijk, A. Marler, T. & BARTELS M.E (2020), Brain Computer Interfaces, RAND's publications. ISBN: 978-1-9774-0523-4 (https://www.rand.org/content/dam/rand.pdf)
- Bozbaş, G. (2025). Dual-Use Technologies in Türkiye's Defense Sector. *Insight Turkey*, *27*(2), 199-220. (https://www.jstor.org/stable/48829612)
- Capa, K. A. (2024). The Role of Cognitive-Information Technologies in Cybersecurity: Threat Detection and Adaptive Defense Systems. *Вопросы безопасности*, (1), 61-70. (https://doi.org/10.25136/2409-7543.2024.1.69882)
- Chen, J. Sun, J. & Wang, G. (2022). From unmanned systems to autonomous intelligent systems. *Engineering*, *12*, 16-19. (https://doi.org/10.1016/j.eng.2021.10.007)
- Chouri, A. (2023). Challenges and Opportunities of Emerging Technologies in Strategic Management. *Journal of Technology in Entrepreneurship and Strategic Management (JTESM)*, 2(4), 1-7, **[In Persian]**. (doi: https://doi.org/10.61838/kman.jtesm.2.4.1)
- Comprehensive document on science and technology in the defense and security fields of the Islamic Republic of Iran, approved by the 837th session dated 05/12/2019 of the Supreme Council of the Cultural Revolution, *Research Center of the Islamic Consultative Assemb*, Tehran, Iran, **[in Persian]**. (https://rc.majlis.ir/fa/law/show/1651177)
- Concha Salor, L. & Monzon Baeza, V. (2023, October). Harnessing the potential of emerging technologies to break down barriers in tactical communications. In *Telecom* (Vol. 4, No. 4, pp. 709-731). MDPI. (https://doi.org/10.3390/telecom4040032)
- De Alwis, C. Kalla, A. Pham, Q. V. Kumar, P. Dev, K. Hwang, W. J. & Liyanage, M. (2021). Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. *IEEE Open Journal of the Communications Society*, *2*, 836-886. (https://doi.org/DOI:10.1109/OJCOMS.2021.3071496)
- Doicariu, D. (2023). Emerging and disruptive technology trends in defense and security. *Journal of Defense Resources Management (JoDRM)*, *14*(2), 33-44. (https://www.ceeol.com/search)
- Frias-Goytia, G. L. Lojo-Seoane, C. Mallo, S. C. Nieto-Vieites, A. Juncos-Rabadán, O. & Pereiro, A. X. (2024). A systematic review of quality of life (QoL) studies using the CASP scale in older adults. *Quality of Life Research*, 1-13. (https://link.springer.com/article/10.1007/s11136-024-03750-9)

- Ghanavati, F. (2013). Developing a Native Model for the Development of Emerging Technologies Based on the Technological Innovation System Approach; A Case Study of Additive Manufacturing, PhD Thesis, Faculty of Management, Iran University of Science and Technology, **[In Persian]**.
- Glenn, J. C. & Gordon, T. J. (2003). Futures research methodology. *The Washington*. (https://www.millennium-project.org/)
- Gudarzi, G. and Ejlali, M. M. (2022). Analysis of future trends in defense technologies over a ten-year horizon. *Defensive Future Studies*, *6*(23), 37-57, **[In Persian]**. (https://doi.org/doi:10.22034/dfsr.2022.530777.1497)
- Gupta, A. & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE access*, 3, 1206-1232. (https://doi.org/DOI:10.1109/ACCESS.2015.2461602)
- Haigh, K. & Andrusenko, J. (2021). *Cognitive electronic warfare: an artificial intelligence approach*. Artech House. (https://ieeexplore.ieee.metrics)
- Koulivand, Kh. (2023). Foresight the weak signals of change ahead of Russia's combined war game against Ukraine. *Iranian Journal of Wargaming*, 5(11), 85-106, **[In Persian]**. (https://doi.org/doi:10.22034/ijwg.2023.387365.1038)
- Koulivand, Kh. (2023). Futuristic analysis of the components of the military knowledge management model in the all-round defense of future battles with a combined warfare approach. *War Studies*, *4*(15), 5-32 **[In Persian]**. (https://doi.org/doi:10.22034/qjws.2023.1987057.1107)
- Koulivand, Kh. Satarikhah,A. and Sepehri,M. (2024). Scenarios for the Hybrid war of Israel against the Islamic Republic of Iran in the horizon of 2029. Military Science and Tactics, 19(66), 189-218, **[In Persian]**. (https://doi.org/doi:10.22034/qjmst.2024.1986908.1831)
- Kunadt, F. (2025). Combining Strategic Foresight and Strategic Communication: An Interdisciplinary Framework of Future-Oriented Communication in Times of Multiple Future Challenges. *International Journal of Strategic Communication*, 1-23. (https://doi.org/10.1080/1553118X.2025.2454676)
- Miles, I. & Keenan, M. (2003, February). Ten Years of Foresight in the UK. In *The Second International Conference On Technology Foresight–Tokyo* (pp. 27-28). (https://www.nistep.go.jp/IC/ic030227/pdf/p3-1.pdf)
- Minkkinen, M. (2020). Theories in futures studies: Examining the theory base of the futures field in light of survey results. *World Futures Review*, *12*(1), 12-25.(https://doi.org/10.1177/1946756719887717)

- Mitchell, M. & Newman, M. (2002). Complex systems theory and evolution. *Encyclopedia of evolution*, *1*, 1-5. (https://melaniemitchell.me/PapersContent.pdf)
- Mohammadi fateh, A. and Ebrahimi, S. A. (2020). An investigation and ranking of emerging information technologies in the defense sector. Defensive Future Studies, 5(17), 143-171, **[In Persian]**. (https://doi.org/doi:10.22034/dfsr.2020.128668.1395)
- Mousavi shahidi, M. vahdaninia, V. and Hosseini, S. N. (2025). Iran on the Brink of a Geopolitical Crossroads: Challenges Arising from the Probable Scenario of the Zangezur Corridor. *Defensive Future Studies*, *9*(35), 1-25, **[in Persian]**. (https://doi.org/doi:10.22034/dfsr.2025.2047082.1856)
- Movahhedi Sefat, M. Sepehri, M. Halili, K. and Farzaneh, A. (2023). Smart defense model based on Internet of Things technology. *Strategic Defense Studies*, *21*(92), 69-92, **[In Persian]**. (https://sds.sndu.ac.ir/article_2421.html)
- National Intelligence Council (NIC) (2021), Global Trends 2040, A Publication of the National Intelligence Council. (http://www.dni.gov/files/ODNI/documents.pdf)
- Nejatpour, M. Farrokhi, M. Sajadi, M. & Hadipour, M. (2023). The role of artificial intelligence in the development of autonomous military Equipment. *Defensive Researches and Management*, *21*(98), 164-143, **[In Persian]**. (https://doi.org/Dor:20.1001.1.20086121.1401.21.98.1.2)
- Oprisor, I. (2021). The Impact of Emerging and Disruptive Technologies on Security. Land Forces Academy Review, 26(4), 261-268. (https://doi.org/DOI:10.2478/raft-2021-0033)
- Patil, A. T. Vidhale, B. & Titarmare, A. (2024, May). Strategic innovations in defense systems: a comprehensive analysis of emerging technologies and future trends. In 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-7). (IEEE. https://doi.org/DOI:10.1109/ISCS61804.2024.10581013)
- Pink, S. (2022). *Emerging technologies/Life at the edge of the future*. Routledge. (https://doi.org/10.4324/9781003182528)
- Popescu, S. (2021, October). Emerging and Disruptive Technologies' Impact on the Military. In Romanian Military Thinking International Scientific Conference Proceedings (pp. 218-229). Centrul tehnic-editorial al armatei. (https://www.ceeol.com/search/chapter-detail?id=1004703)
- Popper, R. & Medina, J. (2008). 12. Foresight in Latin America. *In: Georghiou L, Harper JC, Keenan M, Miles I, Popper R (eds) The handbook of technology foresight: concepts and practice. Edward Elgar*

Publishing, Cheltenham, UK, Northampton, MA, USA, 256-286. (https://research.manchester.ac)

- Schwartz, P. (1997). *Art of the long view: planning for the future in an uncertain world*. John Wiley & Sons. (https://www.amazon.com/Art-Long)
- Schwarz, J. O. (2023). Strategic foresight: An emerging field. In *StrategicForesight* (pp.141-150).Routledge. (https://www.taylorfrancis.com/strategic-foresight)
- Schwarz, J. O. Wach, B. & Rohrbeck, R. (2023). How to anchor design thinking in the future: Empirical evidence on the usage of strategic foresight in design thinking projects. *Futures*, *149*, 103137. (https://doi.org/10.1016/j.futures.2023.103137)
- Sekaran, U. (2003). Research Methods for Business: A Skill Building Approach. New York: John Wiley & Sons.
- Sharifzadeh, Z. Mirkoushesh, A. H. and Hosseini, M. M. (2024). Examining the Impact of New Technology and Artificial Intelligence Development Policies on the Expansion of Macro-Political Strategies with a Focus on General Policies. *Quarterly Journal of The Macro and Strategic Policies*, *12*(45), 24-47, **[In Persian]**. (https://doi.org/doi:10.30507/jmsp.2023.388244.2555)
- Slaughter, R. A. (1997). Developing and applying strategic foresight. *ABNReport*, *5*(10),13-27. (https://www.academia.edu/slaughter_Strategic_Foresight.pdf)
- Stevens, A. L. & Collins, A. (2021). Multiple conceptual models of a complex system. In *Aptitude, learning, and instruction* (pp. 177-198). Routledge. (https://www.taylorfrancis.albert-stevens-allan-collins)
- Stocchero, J. M. (2023). A network centric architecture for military command and control systems. (http://hdl.handle.net/10183/264212)
- Subramani, S. M, S. A, K. & Svn, S. K. (2025). Review of security methods based on classical cryptography and quantum cryptography. *Cybernetics and Systems*, *56*(3), 302-320. (https://doi.org/10.1080/01969722.2023.2166261)
- Wilson, C. Grubler, A. Bauer, N. Krey, V. & Riahi, K. (2013). Future capacity growth of energy technologies: are scenarios consistent with historical evidence? *Climatic Change*, *118*(2), 381-395. (https://doi.org/10.1007/s10584-012-0618-y)
- Wilson, I. (2004). Technology foresight in an age of uncertainty. *International Journal of Foresight and Innovation Policy*, *1*(3-4),207-217.(https://doi.org/10.1504/IJFIP.2004.004960)