Journal of Safe City

Online ISSN: 2676-556X

Journal Homepage: www.ispdrc.ir

Research Paper

Technological Analysis of the 12-Day Hybrid War by the U.S. and the Zionist Regime Against the Islamic Republic of Iran: From Strategy to Operational Structure

Mahnaz Mirza Ebrahim Tehrani [1]* gholamreza jalali farahani [2]

[1] Department of Environment, Faculty of Engineering, Islamic Azad University, North Tehran Branch

[2] Passive Defense Department, Faculty of Defense, National Defense University

Received: 15 September 2025 Received In revised form: 12 October 2025 Accepted: 23 Desember 2025 p.p: 294 –311

https://doi.org/10.22034/ispdrc.2025.2071066.1211

Extended Abstract

The 12-day war between the United States and the Zionist regime against the Islamic Republic of Iran can be considered a decisive turning point in the conceptual evolution of modern technology-based wars. Unlike conventional wars of the twentieth century that relied heavily on physical confrontations, territorial occupation, and traditional weapons systems, this conflict illustrated a new paradigm in which multiple layers of technology converge to form an integrated battlefield. This hybrid war represented a sophisticated combination of military and civilian instruments, physical and virtual domains, as well as hardware and software tools, thereby demonstrating that the boundary between traditional warfare and technologically enabled conflict has become increasingly blurred. The war underscored that power in the twenty-first century is no longer defined solely by tanks, missiles, and troops but by the ability to integrate cyber networks, artificial intelligence, electronic systems, and cognitive strategies into a coherent and coordinated campaign.

In this confrontation, advanced technologies were deployed in a phased and synergistic manner. Cyber operations targeted communication infrastructures, critical databases, and financial systems with the aim of creating disruption and uncertainty. Artificial intelligence tools enhanced surveillance, optimized decision-making, and facilitated autonomous functions in combat systems. Unmanned aerial vehicles, commonly referred to as drones,

played dual roles in intelligence gathering and precision strikes, minimizing the need for direct human presence in hostile zones. Electronic warfare disrupted radar, communication frequencies, and navigation systems, thereby undermining situational awareness and reducing the effectiveness of traditional defense mechanisms. Most significantly, cognitive operations aimed at shaping public perception, influencing morale, and destabilizing social cohesion revealed that modern warfare is as much about narratives and psychological impact as it is about physical destruction. The combined effect of these tools created multidimensional pressure on Iran's defense, economy, and society, highlighting the interconnectedness of various spheres of national security.

The purpose of the present article is to conduct a technological analysis of this war using the qualitative content analysis method within a descriptive-analytical framework. This methodology allows for an in-depth exploration of how technologies were deployed, the logic underlying their sequencing, and the effects they produced in different domains. The research data encompass official documents, field reports, media outputs, and expert assessments, all examined through a comparative approach and content interpretation. By analyzing both open-source intelligence and expert insights, the study reconstructs the technological architecture of the conflict and identifies the mechanisms through which superiority was sought and contested.

The findings indicate that technology-based warfare follows a purposeful and sequential logic. It typically commences with information gathering and precise surveillance of infrastructures. In the case of the 12-day war, the adversaries invested significant resources in reconnaissance, using satellites, drones, and cyber intrusions to map vulnerabilities and identify strategic choke points. Once a comprehensive situational picture was achieved, the conflict moved into the second phase, which consisted of cyber and electronic strikes aimed at weakening defense systems, interrupting logistics, and undermining economic stability. These operations did not operate in isolation but were synchronized with physical and cognitive measures, thereby amplifying their effectiveness. The final phase relied heavily on cognitive and psychological operations. Through targeted disinformation campaigns, manipulation of social media platforms, and symbolic military actions, the adversaries sought not only to consolidate battlefield achievements but also to project an image of dominance that could influence both domestic and international perceptions.

This war revealed several important insights into the nature of future conflicts. First, new technologies will not merely serve as auxiliary tools but will constitute the central elements of contemporary and forthcoming battlefields. Their integration allows for simultaneous engagement across multiple domains, effectively multiplying the reach and impact of military operations. Second, the distinction between civilian and military spheres becomes increasingly difficult to sustain. Attacks on financial systems, energy grids, and communication networks illustrate how societies as a whole, rather than just armed forces, become the targets of technologically enabled conflicts. Third, the role of cognition and perception has grown in prominence, suggesting that wars of the future will be judged not solely by territorial gains or casualty counts but by the ability to shape narratives, maintain legitimacy, and influence international opinion.

Understanding this emerging pattern is a strategic imperative. For states like Iran, which face technologically advanced adversaries, the lessons of the 12-day war underscore the urgency of redesigning national defense architecture to integrate cyber, electronic, and cognitive dimensions alongside traditional military capabilities. Enhancing the resilience of critical infrastructures, particularly in energy, communications, and finance, becomes central to national security. Equally important is the development of comprehensive strategies to build societal resilience, improve public awareness of cognitive manipulation, and strengthen long-term deterrence capacities.

In conclusion, the 12-day war exemplifies the trajectory of modern conflict, where technology is not an adjunct but the very foundation of warfare. By analyzing this case, the article contributes to the broader academic and strategic understanding of how wars are evolving in the twenty-first century and provides insights that are essential for policymakers, defense planners, and scholars concerned with the future of security.

Corresponding author (Email: tehrani.mah@gmail.com)

نشریه علمی شهـــر ایمـــن

شاپا الکترونیکی:2676-556X

Journal Homepage: www.ispdrc.ir

مقاله پژوهشی

تحلیل فناورانه جنگ ترکیبی ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران:

از راهبرد تا ساختار عملیاتی

مهناز میرزاابراهیم طهرانی*، غلامرضا جلالی فراهانی

[۱] گروه محیط زیست دانشکده فنی دانشگاه آزاد اسلامی واحد تهران شمال

[۲] گروه پدافند غیرعامل دانشکده دفاع دانشگاه عالی دفاع ملی

تاریخ ارسال: ۱٤۰٤/۰٦/۲٤ تاریخ بازنگری: ۱٤۰٤/۰۷/۲۰ تاریخ پذیرش: ۱٤۰٤/۱۰/۰۲ ص.ص ۳۱۱-۲۹٤

https://doi.org/10.22034/ispdrc.2025.2071066.1211

چکیده:

جنگ ۱۲ روزه آمریکا و رژیم صهیونیستی علیه جمهوری اسلامی ایران نقطه عطفی در تحول مفهومی جنگ‌های فناورمحور است. این جنگ ترکیبی، تلفیقی پیچیده از ابزارهای نظامی و غیرنظامی، فیزیکی و مجازی و همچنین سخت‌افزاری و نرم‌افزاری بود و نشان داد که مرز میان جنگ سنتی و جنگ فناورانه به‌طور چشمگیری کمرنگ شده است. فناوری‌های نوین مانند عملیات سایبری، هوش مصنوعی، پهپادهای هوشمند، جنگ الکترونیک و عملیات شناختی در قالب الگویی مرحله‌ای و هم‌افزا به‌کار گرفته شدند و بُعد فناورانه جنگ را به مؤلفه‌ای تعیین‌کننده در نتیجه نبرد تبدیل کردند . هدف مقاله، تحلیل فناورانه این جنگ با روش تحلیل کیفی محتوا و رویکرد توصیفی–تحلیلی است. یافته‌ها نشان می‌دهد که جنگ فناورمحور از منطق مرحله‌ای و هدفمند پیروی می‌کند؛ به گونه‌ای که ابتدا با رصد و جمع‌آوری داده‌ها آغاز شده، سپس از طریق حملات سایبری و شناختی توان دفاعی، روانی و اقتصادی کشور را هدف قرار داده و در نهایت با مهندسی روایت و عملیات ادراکی، نتایج را تثبیت کرده است. این الگو بیانگر آن است که فناوری نه صرفاً ابزار بلکه معماری میدان نبرد آینده است. تحلیل این روند می‌تواند به بازطراحی دکترین دفاع ملی، افزایش تاب‌آوری زیرساختی و ارتقای بازدارندگی فناورپایه جمهوری اسلامی ایران منجر شود.

کلیدواژه‌ها :جنگ ترکیبی، فناوری نظامی، جنگ شناختی، هوش مصنوعی، دکترین دفاعی ایران

*نویسنده مسئول Email: tehrani.mah@gmail.com

۱ .مقدمه

در دهه‌های اخیر، دگرگونی‌های عمیقی در منطق جنگ و نحوه اعمال قدرت در نظام بین‌الملل به‌وجود آمده است. دیگر میدان‌های نبرد صرفاً محدود به تقابل نیروهای نظامی در جغرافیای مشخص نیست، بلکه با گسترش فناوری‌های نوین، جنگ به حوزه‌هایی نظیر فضای سایبری، شناختی، اقتصادی، اطلاعاتی و حتی روانی نیز کشیده شده است .(Kello, 2017) در این میان، جنگ‌های ترکیبی فناورمحور به‌عنوان یکی از شاخص‌ترین اشکال جنگ مدرن، نمایانگر تلفیق چندلایه ابزارهای سخت و نرم، فیزیکی و مجازی، و دولت‌محور و غیردولتی هستند که به‌صورت هم‌زمان و هدفمند بر ساختارهای حیاتی کشور هدف تأثیر می‌گذارند.(Hoffman, 2007)

بیان مسئله از اینجا نشأت می‌گیرد که جمهوری اسلامی ایران، در تیرماه سال ۱۴۰۴، هدف حمله‌ای ۱۲ روزه قرار گرفت که تلفیقی از عملیات‌های نظامی دقیق، حملات سایبری مخرب، جنگ الکترونیک، عملیات روانی، پهپادی و اطلاعاتی بود. این عملیات، نه‌تنها در میدان نبرد نظامی بلکه در بستر زیرساخت‌های حیاتی، افکار عمومی، شبکه‌های اجتماعی و سامانه‌های مالی و اقتصادی کشور نیز گسترش یافت. ویژگی این جنگ در آن بود که با بهره‌گیری از فناوری‌های نوظهور مانند هوش مصنوعی، داده‌کاوی، پهپادهای تهاجمی، دیپ‌فیک و الگوریتم‌های تحلیل شناختی اجرا شد؛ به‌گونه‌ای که مرز میان جنگ و صلح، و میان حمله فیزیکی و تهاجم نرم به‌شدت تضعیف شد.(Singer & Brooking, 2018)

پرسش اصلی این پژوهش آن است که الگوی فناورانه جنگ ۱۲ روزه علیه ایران چگونه طراحی و اجرا شده و چه ابعاد، اهداف و پیامدهایی برای ساختار دفاعی کشور به همراه داشته است؟ بررسی ساختار این جنگ برای شناخت تهدیدات آینده، ارتقاء توان دفاعی ملی و توسعه دکترین مقابله فناورمحور ضروری است.

با توجه به فقدان پژوهش‌های جامع در خصوص ساختار فناورانه این نبرد خاص، این مقاله تلاش دارد با استفاده از رویکرد تحلیلی–توصیفی و روش تحلیل کیفی محتوا به بررسی دقیق ابعاد جنگ ترکیبی فناورمحور ۱۲ روزه بپردازد. در این مسیر، مقاله ابتدا مفاهیم نظری مربوط به جنگ ترکیبی فناورمحور را تشریح می‌کند، سپس با تحلیل داده‌های مستند، به بازشناسی مراحل پنج‌گانه جنگ، اهداف دشمن، ابعاد و ابزارهای به‌کار رفته، و نهایتاً پیامدهای راهبردی آن می‌پردازد.

نتایج این پژوهش می‌تواند در راستای تدوین سیاست‌های پدافند ملی، بازطراحی ساختارهای زیرساختی، ارتقاء آمادگی شناختی و مقابله با تهدیدات سایبری و اطلاعاتی مورد استفاده قرار گیرد. به‌ویژه آن‌که جنگ‌های آینده با سرعتی فزاینده به‌سوی ترکیب عملیات‌های فیزیکی و فناورانه در حرکت‌اند و ایران نیز یکی از اهداف اصلی این سناریوها در سطح منطقه‌ای و بین‌المللی تلقی می‌شود.(Rattray, 2022)

۲ .مبانی نظری پژوهش

پیشرفت‌های شتاب‌ناک فناورانه در دهه‌های اخیر، به‌ویژه در حوزه‌هایی مانند هوش مصنوعی، اینترنت اشیا، داده‌های کلان، پهپاد، شبکه‌های ارتباطی، واقعیت ترکیبی و فناوری‌های شناختی، موجب تحول بنیادین در ماهیت جنگ و درگیری‌های بین‌المللی شده است. در این راستا، مفهوم «جنگ ترکیبی فناورمحور (Technologically-Driven Hybrid Warfare) » به‌عنوان یکی از پیچیده‌ترین الگوهای نبرد مدرن، در ادبیات مطالعات امنیتی و نظامی ظهور یافته است.

۲.۱ .جنگ ترکیبی(Hybrid Warfare)

نخستین بار مفهوم جنگ ترکیبی توسط فرانک هافمن (۲۰۰۷) در قالب مدلی از درگیری‌های مدرن مطرح شد که در آن دشمنان از مجموعه‌ای از تاکتیک‌های متعارف، نامتقارن، اطلاعاتی، سایبری، رسانه‌ای و اقتصادی به‌صورت هم‌زمان استفاده می‌کنند تا ساختارهای حیاتی دولت‌ها را دچار اختلال نمایند. جنگ ترکیبی نه یک جنگ تمام‌عیار سنتی و نه صرفاً شورش یا عملیات سایبری، بلکه ترکیبی هوشمند از آن‌هاست که قابلیت انکارپذیری و پراکندگی جغرافیایی دارد(Hoffman, 2007; Bartles, 2016).

این نوع جنگ بر سه اصل استوار است:

۱. تلفیق ابزارها و روش‌ها
۲. مبهم‌سازی هویت مهاجم
۳. بهره‌گیری از فناوری‌های نوین

بررسی‌ها نشان می‌دهد اصول جنگ ۱۲ روزه عبارتند از:

۱. شناسایی دقیق و اشراف اطلاعتی فیزیکی
۲. جنگ شناختی و تحلیل انگاره‌های فروپاشی از درون
۳. درماندگی و فلج‌سازی راهبردی
۴. دیپلماسی آفنی مبتنی بر ایزوله‌سازی کشور و تنها کردن آن در جنگ
۵. تمرکز اطلاعات و شناخت عمیق از مراکز زیرساختی و فرماندهان
۶. تمرکز بر زنجیره خدمت و کنترل راهبردی آن
۷. تبدیل زنجیره تولید یا خدمات به راهبری حملات نظامی دشمن

۲.۲ .فناوری به‌عنوان پیشران جنگ‌های مدرن

جنگ نسل پنجم به عنوان مرحله‌ای نوین از تحول منازعات، نوعی جنگ ترکیبی و عمدتاً غیرکینتیک است که با اتکا به فناوری‌های پیشرفته، عملیات سایبری، جنگ شناختی و رسانه‌ای و بهره‌گیری از بازیگران دولتی و غیردولتی، بیش از آنکه بر میدان نبرد فیزیکی متمرکز باشد، بر تسلط بر ادراک، افکار عمومی و فرایندهای تصمیم‌گیری تمرکز دارد. این الگو با محو مرزهای سنتی میان جنگ و صلح، و با ایجاد بی‌ثباتی، فرسایش انسجام اجتماعی و تضعیف اقتدار سیاسی ـ امنیتی، به دنبال

تحقق اهداف راهبردی است، به گونه‌ای که ماهیت آن را می‌توان «جنگ ادراکات» و «منازعه مبتنی بر اطلاعات و روان جامعه» دانست (Wikipedia, 2024; Shahani, 2018; Qiao & Wang, 1999).

با ظهور جنگ‌های نسل پنجم(5GW) ، فناوری دیگر صرفاً ابزار پشتیبانی از جنگ نیست، بلکه خود به یک محیط جنگی تبدیل شده است. در جنگ‌های فناورمحور، تسلط بر داده‌ها، ادراکات و زیرساخت‌ها از طریق ابزارهایی مانند حملات سایبری، جنگال، پهپادهای هوشمند، هوش مصنوعی و عملیات روانی هدایت‌شده، نقشی تعیین‌کننده در شکست یا پیروزی دارد (Kello, 2017; Rid, 2020).

بررسی ادبیات جدید نشان می‌دهد که جنگ‌های فناورانه از ویژگی‌هایی همچون:

- کوتاه‌مدت بودن عملیات
- ناشناس بودن مهاجم
- تمرکز بر زیرساخت‌های حیاتی
- استفاده از دیپ‌فیک و تکنیک‌های شناختی
- به‌کارگیری ابزارهای غیرسنتی مانند رمزارز، شبکه‌های اجتماعی و حملات هدفمند برخوردار هستند (Kaspersen, 2016; Singer & Brooking, 2018).

۲.۳ .نظریه‌های مرتبط با جنگ فناورمحور

الف. نظریه جنگ نسل پنجم(5GW) :

جنگ نسل پنجم به‌مثابه یک نظریه تحول در منازعات بر این فرض استوار است که جنگ‌های معاصر دیگر صرفاً در میدان نبرد فیزیکی رخ نمی‌دهند، بلکه در «عرصه ادراکات، اطلاعات و فضاهای غیرملموس» جریان می‌یابند. نظریه‌پردازان این حوزه معتقدند که دشمنی در این نسل از جنگ‌ها الزاماً یک ارتش یا دولت مشخص نیست، بلکه می‌تواند مجموعه‌ای از بازیگران غیردولتی، شبکه‌های سایبری، گروه‌های اجتماعی یا حتی افراد توانمند (super-empowered individuals) باشد.

ویژگی‌های نظریه جنگ نسل پنجم شامل موارد زیر است:

- **غیرکینتیک بودن**: ابزار اصلی جنگ نه تسلیحات نظامی، بلکه رسانه، فناوری دیجیتال، حملات سایبری، هوش مصنوعی و جنگ شناختی است.
- **نبرد بر سر ادراک و آگاهی**: هدف، تغییر نگرش، باور و رفتار جامعه هدف از طریق اطلاعات غلط، پروپاگاندا و مهندسی افکار عمومی است.
- **ابهام در مرزها**: تمایز میان صلح و جنگ، و میان بازیگران دولتی و غیردولتی از بین می‌رود.

- **میدان نبرد همه‌جا**: جنگ محدود به جغرافیای خاص یا خط مقدم نیست، بلکه در فضای مجازی، رسانه‌ها، شبکه‌های اجتماعی و زیرساخت‌های حیاتی جریان دارد.
- **اهداف راهبردی غیرمستقیم**: به جای نابودی دشمن در میدان، تمرکز بر تضعیف انسجام اجتماعی، ایجاد بی‌ثباتی سیاسی و تردید در مشروعیت حاکمیت است.

بنابراین، نظریه جنگ نسل پنجم بر این ایده بنا شده است که در عصر اطلاعات، تسلط بر ذهن و ادراک جوامع مهم‌تر و مؤثرتر از تسلط بر زمین و سرزمین است .(Shahani, 2018; Wikipedia, 2024; Qiao & Wang, 1999)

در این نظریه، دشمن بدون آنکه در میدان نظامی حاضر شود، بر افکار عمومی، ساختارهای نرم‌افزاری و تصمیم‌سازی‌های کلان تأثیر می‌گذارد. جنگ‌های شناختی، رسانه‌ای و سایبری در این نسل از جنگ‌ها اولویت دارند.(Hammes, 2007)

ب. نظریه جنگ شناختی(Cognitive Warfare) :

جنگ شناختی شکلی از منازعه است که بر تسلط بر فرآیندهای ذهنی، ادراکی و تصمیم‌گیری **انسان** متمرکز است. در این نظریه، ذهن افراد به‌عنوان «میدان نبرد اصلی» تلقی می‌شود و بازیگران تلاش می‌کنند از طریق دستکاری در اطلاعات، احساسات، باورها و ادراکات، رفتار جمعی یا فردی را به‌گونه‌ای هدایت کنند که در راستای اهداف راهبردی آنان باشد (Lynn, 2020; NATO Innovation Hub, 2021).

- ریشه‌های نظری این رویکرد به جنگ روانی و عملیات اطلاعاتی بازمی‌گردد، اما جنگ شناختی فراتر از آنها عمل می‌کند.
- تمرکز آن نه‌فقط بر انتشار اطلاعات غلط یا پروپاگاندا، بلکه بر مدیریت نحوه پردازش اطلاعات توسط مغز انسان است.
- اساس نظریه این است که اگر بتوان بر شیوه تفکر، قضاوت و تصمیم‌گیری انسان مسلط شد، دیگر نیازی به استفاده مستقیم از زور نظامی نخواهد بود.

ویژگی‌های نظریه جنگ شناختی

- **انسان به‌عنوان سلاح و میدان نبرد**: فرد نه‌تنها هدف بلکه ابزار انتقال جنگ است (مثلاً از طریق بازنشر محتوا در شبکه‌های اجتماعی).
- **ترکیب روان‌شناسی، علوم شناختی و فناوری**: استفاده از داده‌کاوی، هوش مصنوعی، الگوریتم‌ها و شبکه‌های اجتماعی برای نفوذ در ذهن و رفتار.
- **پیچیدگی و پنهان‌بودن**: تشخیص منبع حمله دشوار است و پیامدها به‌تدریج و غیرمستقیم آشکار می‌شوند.
- **هدف راهبردی**: تضعیف انسجام اجتماعی، ایجاد تردید در مشروعیت سیاسی و برهم‌زدن اعتماد عمومی.

جایگاه نظری در تحول جنگ‌ها

- در چارچوب نظریه نسل‌های جنگ، جنگ شناختی را می‌توان زیربنای جنگ نسل پنجم دانست، زیرا بُعد اصلی ۵ GWکنترل ادراکات و ذهن‌هاست.
- ناتو نیز در گزارش (NATO Innovation Hub, 2021) «Cognitive Warfare» تأکید می‌کند که این نوع جنگ «شکل نهایی و پیشرفته جنگ‌های مدرن است» زیرا مستقیم‌ترین هدف آن «ذهن انسان» است.

این دیدگاه که از دهه ۲۰۱۰ توسط نهادهایی مانند ناتو و DARPA پیگیری شده است، بر تغییر باور، رفتار، و تصمیم افراد و جوامع از طریق فناوری تمرکز دارد. در این نوع جنگ، ذهن انسان به میدان نبرد تبدیل می‌شود و ابزارهایی چون هوش مصنوعی، تحلیل داده، دیپ‌فیک و شبکه‌های اجتماعی به‌کار گرفته می‌شوند.(Giordano, 2020)

ج. نظریه حاکمیت سایبری و جنگ نامرئی:

نظریه حاکمیت سایبری بر این اصل استوار است که هر کشور باید حق داشته باشد فضای سایبری خود را مطابق با قوانین و سیاست‌های ملی مدیریت و کنترل کند و مرزهای دیجیتال خود را حفظ نماید (Nye, 2010; Kremer & Nyarko, 2020). این نظریه به‌ویژه در مواجهه با تهدیدات سایبری و نفوذ اطلاعاتی اهمیت می‌یابد و بر استقلال ملی و امنیت زیرساخت‌های حیاتی تأکید دارد.

از سوی دیگر، نظریه جنگ نامرئی بیان می‌کند که بسیاری از منازعات مدرن، به‌ویژه در جنگ نسل پنجم و جنگ شناختی، بدون برخورد مستقیم نظامی و بدون شناسایی واضح بازیگران رخ می‌دهند و تمرکز آن‌ها بر تأثیرگذاری غیرمستقیم بر ذهن، تصمیم‌گیری و انسجام اجتماعی است .(Shaw & Duffy, 2018; NATO CCDCOE, 2021) این نوع جنگ معمولاً شامل حملات سایبری، پروپاگاندا و جنگ روانی است و مرز میان جنگ و صلح را محو می‌کند.

در این نظریه، فضای سایبری به‌عنوان عرصه جدیدی از رقابت‌های ژئوپلیتیکی تعریف می‌شود. بازیگران غیردولتی نیز می‌توانند با ابزارهای فناورانه به بازیگران مؤثر در جنگ تبدیل شوند.(Rattray, 2022)

با ادغام این نظریه،ها می‌توان جنگ ترکیبی فناورمحور علیه ایران را الگویی از «منازعه ادراکی فناورپایه» دانست که در آن تسلط بر اطلاعات، ذهن و زیرساخت سه ستون اصلی نبرد را تشکیل می‌دهند.

۲.۴ .پیشینه مطالعاتی

مروری بر ادبیات پژوهش‌های موجود نشان می‌دهد که طی سال‌های اخیر، تمرکز بر جنگ ترکیبی فناورمحور افزایش یافته است:

- **Clark (2021)**در مقاله‌ای در *RAND Corporation*تأکید می‌کند که آینده جنگ‌ها با ادغام فزاینده فضای فیزیکی و مجازی و تسلط اطلاعاتی تعریف خواهد شد.

- **Rattray (2022)**نشان می‌دهد که قابلیت‌های سایبری و الگوریتمی به‌عنوان ابزارهای کلیدی در تضعیف ساختارهای دفاعی کشورها به‌کار می‌روند.
- **Singer & Brooking (2018)**در اثر خود بر نقش رسانه‌های اجتماعی در جنگ‌افزارسازی اطلاعات تمرکز می‌کنند و نشان می‌دهند که جنگ‌های آینده دیگر نیازی به گلوله ندارند، بلکه اطلاعات و تصاویر کافی است.
- **Watts & Binnendijk (2023)**تحلیل دقیقی از جنگ ترکیبی روسیه در اوکراین ارائه داده و نشان می‌دهند چگونه ترکیب فناوری‌های نوین با عملیات شناختی باعث تضعیف جبهه مقاومت شده است.

با این وجود، همچنان شکاف‌هایی در بررسی نظام‌مند و بومی جنگ‌های فناورمحور در سطح منطقه‌ای، به‌ویژه در رابطه با جمهوری اسلامی ایران، وجود دارد. پژوهش حاضر در پی آن است که با پر کردن این خلأ، الگویی مفهومی و تحلیلی از ساختار جنگ ترکیبی فناورمحور علیه ایران ارائه دهد.

۳ .روش‌شناسی پژوهش

پژوهش حاضر با هدف تحلیل ساختار، اهداف، ابعاد و مراحل جنگ ترکیبی فناورمحور علیه جمهوری اسلامی ایران در جنگ ۱۲ روزه، به‌صورت توصیفی–تحلیلی و با رویکرد کیفی انجام شده است. نوع تحقیق در دسته کاربردی–توسعه‌ای قرار می‌گیرد؛ چراکه از یک سو به تبیین مفاهیم و الگوهای نظری می‌پردازد و از سوی دیگر درصدد ارائه مدلی تحلیلی برای استفاده در حوزه سیاست‌گذاری و راهبردهای دفاعی است.

این پژوهش با رویکرد کیفی و روش تحلیل مضمون براون و کلارک (2006) انجام شد. داده‌ها از منابع معتبر علمی، گزارش‌های امنیتی و اسناد رسمی (۲۰۲۴–۲۰۲۵) گردآوری شدند.

۳.۱ .روش گردآوری داده‌ها

برای گردآوری داده‌ها، از روش کتابخانه‌ای و اسنادی (Documentary Research Method) استفاده شده است. داده‌ها و اطلاعات اولیه از منابع زیر گردآوری شده‌اند:

- گزارش‌های تحلیلی مؤسسات بین‌المللی مانندRAND ، CSIS، IISS، NATO Strategic Communications Centre
- اسناد رسمی منتشرشده از سوی منابع خبری و نظامی غربی (از جمله *Breaking Defense*، *War on the Rocks*، *Times of Israel*)
- گزارش‌های فناوری و نظامی منتشرشده پس از جنگ ۱۲ روزه (در بازه زمانی تیر–مرداد ۱۴۰۴ / ژوئیه ۲۰۲۵)
- مقالات علمی معتبر از پایگاه‌هایی مانندScienceDirect ، JSTOR، Springerو Google Scholar
- اسناد راهبردی در حوزه جنگ ترکیبی، جنگ سایبری، عملیات شناختی و کاربرد فناوری در جنگ‌های مدرن

معیارهای انتخاب منابع شامل اعتبار علمی، استنادپذیری، تازگی داده‌ها و تطابق با موضوع تحقیق بوده است. علاوه بر این، برای تکمیل داده‌های بومی، از برخی تحلیل‌های رسمی منتشرشده توسط مراکز پژوهشی ایرانی در حوزه مطالعات امنیتی و فناوری استفاده شده است.

۳.۲ .ابزار و چارچوب تحلیل

مراحل تحلیل مورد استفاده در این پژوهش عبارتند از:

۱. مرور منابع و استخراج گزاره‌های کلیدی
۲. تولید کدهای اولیه
۳. گروه‌بندی و ترکیب کدها در مضامین مفهومی
٤. تفسیر و مدل‌سازی نهایی در سه سطح: توصیف، تجزیه، تفسیر

جدول ۱-نمونه کدگذاری متون

گزاره متنی	کد باز	مضمون محوری
نفوذ در سامانه های برق و فرماندهی	حمله زیرساختی سایبری	تضعیف بازدارندگی فناورانه
استفاده از دیپ فیک و مهندسی افکار عمومی	حمله شناختی دیجیتال	جنگ ادراک
اختلال در زنجیره تامین و خدمات	جنگ اقتصادی فناورانه	فرسایش تاب آوری ملی

از الگوی تحلیل کیفی محتوا بهره گرفته شده که برای تحلیل متون راهبردی، امنیتی و فناورانه مناسب است. به‌طور خاص، از رویکرد تحلیل مضمون استفاده شده است؛ بدین معنا که ابتدا متون مورد نظر مرور و کدگذاری شدند، سپس مضامین اصلی، الگوها و مفاهیم کلیدی استخراج و در نهایت دسته‌بندی موضوعی انجام شد.

چارچوب تحلیل پژوهش مبتنی بر سه سطح مفهومی است:

- **سطح اول (توصیف):** استخراج مفاهیم و گزاره‌های کلیدی از منابع (مانند نوع فناوری، اهداف حمله، ابزارها)
- **سطح دوم (تجزیه):** طبقه‌بندی یافته‌ها در قالب ابعاد جنگ ترکیبی (سایبری، نظامی، شناختی، اقتصادی و...)
- **سطح سوم (تفسیر):** تحلیل پیوندهای علّی، تعامل بین ابعاد و هدف راهبردی دشمن در یک مدل مرحله‌ای

۳.۳ .روش تجزیه و تحلیل داده‌ها

فرآیند تحلیل کیفی در این پژوهش بر اساس مراحل شش‌گانه تحلیل مضمون براون و کلارک (Braun & Clarke, 2006) انجام شده است:

۱. **آشنایی با داده‌ها:** مرور منابع و استخراج اطلاعات اولیه

۲. **تولید کدهای اولیه:**کدگذاری مفاهیم کلیدی مانند «حمله سایبری دقیق»، «اختلال در زنجیره تأمین»، «دیپ‌فیک»، «فاز بهره‌برداری»
۳. **جستجوی مضامین:** شناسایی مضمون‌هایی چون «فناوری در جنگ»، «مراحل اجرای جنگ ترکیبی»، «اهداف شناختی»
٤. **بازبینی مضامین:** بررسی ارتباط درونی مضامین و حذف یا ادغام مضامین ضعیف
٥. **نام‌گذاری مضامین:** تعریف روشن هر مضمون مانند «هدف‌گیری زیرساختی»، «فرسایش روانی»، «مهندسی ادراک»
٦. **تهیه گزارش نهایی:** ترکیب یافته‌ها در ساختار مقاله

۳.۴ .اعتبارسنجی و روایی یافته‌ها

برای اطمینان از اعتبار نتایج، از دو روش استفاده شده است:

- **اعتبار سنجی تطبیقی:**مقایسه یافته‌ها با گزارش‌های رسمی بین‌المللی و تحلیل‌های مشابه در حوزه جنگ ترکیبی (مانند مطالعات مربوط به جنگ اوکراین و جنگ اطلاعاتی علیه چین)
- **مثلث‌سازی منابع:** استفاده از منابع متنوع (رسانه‌ای، تحلیلی، علمی و راهبردی) برای افزایش جامعیت تحلیل و کاهش سوگیری

همچنین از نظرات چند کارشناس نظامی و فناور در قالب مشاوره غیررسمی برای بازبینی مضامین و صحت طبقه‌بندی‌ها بهره گرفته شده است.

۴ .تجزیه و تحلیل یافته‌ها

بر اساس تحلیل کیفی اسناد و منابع، الگوی جنگ ترکیبی فناورمحور علیه جمهوری اسلامی ایران در جنگ ۱۲ روزه، در قالب پنج مرحله اجرایی و در بستر شش بعد هم‌افزا شکل گرفته است. یافته‌ها حاکی از آن است که طراحی این جنگ بر پایه تسلط بر فناوری‌های نوین و بهره‌برداری از ظرفیت‌های شناختی، اطلاعاتی، سایبری، فضایی، اقتصادی و نظامی صورت گرفته است.

۴.۱ .اهداف راهبردی دشمن

بر اساس داده‌های استخراج‌شده، اهداف اصلی دشمن از اجرای این جنگ فناورمحور شامل موارد زیر است:

- ✓ تضعیف سامانه‌های دفاعی و بازدارندگی ایران: با حملات سایبری و پهپادی به سامانه‌های موشکی و پدافندی.
- ✓ اخلال در زیرساخت‌های حیاتی: حملات سایبری به شبکه‌های برق، آب، انرژی، حمل‌ونقل و بانک‌ها.
- ✓ فرسایش روانی و شناختی جامعه: از طریق عملیات دیپ‌فیک، اخبار جعلی، تحریک نارضایتی و ناامیدی.
- ✓ ایجاد اخلال در تصمیم‌سازی فرماندهی: با هدف نابودی انسجام تصمیم‌گیری در سطح نظامی و سیاسی.
- ✓ افزایش فشار بین‌المللی و تحمیل شرایط مذاکره: از طریق نمایش شکست داخلی و فشار رسانه‌ای خارجی.

۴.۲ .ابعاد فناورانه جنگ ترکیبی

تحلیل داده‌ها نشان می‌دهد که عملیات در شش بعد فناورانه هم‌زمان و با تعامل میان‌لایه‌ای اجرا شده‌اند:

جدول۲-ابعاد فناورانه جنگ ترکیبی(محقق ساخته)

بعد فناورانه	ابزارها و روش‌ها	اهداف کلیدی
سایبری	بدافزار، نفوذ بهSCADA ، حملاتDDoS	فلج‌سازی زیرساخت‌ها و سامانه‌های دفاعی
الکترونیک	GPS Spoofing، جنگال، EMP	اخلال در ناوبری، ارتباطات و رادار
پهپادی	پهپادهای انتحاری، ازدحامی، رادارگریز	تخریب دقیق مراکز حساس
فضایی	ماهواره‌هایELINT ، سنجش‌ازدور، داده‌کاوی فضایی	شناسایی تحرکات، تحلیل تصمیمات
شناختی و رسانه‌ای	دیپ‌فیک، عملیات اطلاعاتی، رسانه‌های اجتماعی	بی‌اعتمادسازی، جنگ روانی، آشوب نرم
اقتصادی	حمله به سامانه‌های بانکی، تحریم هدفمند	کاهش تاب‌آوری اقتصادی، نارضایتی عمومی

۴.۳ . مراحل اجرای جنگ ترکیبی فناورمحور

بر اساس الگوی استخراج‌شده، جنگ فناورمحور در پنج مرحله اصلی با ترتیب زیر اجرا شده است:

مرحله ۱: جمع‌آوری اطلاعات پیشرفته

نفوذ به سامانه‌های اطلاعاتی و امنیتی کشور، پایش فضایی و داده‌کاوی کلان با هوش مصنوعی برای شناسایی اهداف راهبردی و آسیب‌پذیری‌ها.

مرحله ۲: تخریب زیرساخت‌های حیاتی و حمبه به زنجیره تولید و خدمات راهبردی کشور

حملات سایبری و فیزیکی هم‌زمان به سامانه‌های حیاتی (برق، انرژی، شبکه بانکی، فرماندهی نظامی)، استفاده از پهپاد و جنگال برای فلج‌سازی سیستم دفاعی.

مرحله ۳: عملیات روانی و شناختی و رسانه‌محور

اجرای عملیات گسترده در فضای مجازی، انتشار اخبار جعلی، شایعات، دیپ‌فیک‌ها و پیام‌های هدایت‌شده برای تضعیف اراده ملی و تصمیم‌گیران.

مرحله ۴: ضربات ترکیبی سایبری–نظامی هدفمند

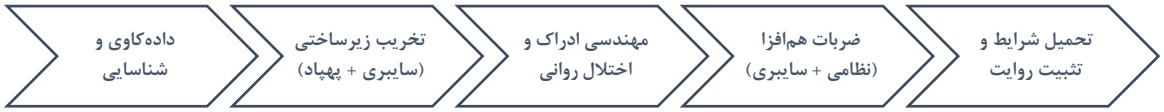
حملات دقیق و هم‌افزا به مراکز راهبردی با هماهنگی کامل میان حملات سایبری و عملیات فیزیکی، با هدف وارد کردن شوک نظامی و فلج‌سازی قابلیت پاسخ.

مرحله ۵: تثبیت و بهره‌برداری از نتایج

القای شکست به افکار عمومی، تحمیل فشار دیپلماتیک، مهندسی روایت شکست، بهره‌برداری اقتصادی از فروپاشی زیرساختی و اعتماد عمومی، القای ضرورت تغییر رفتار.

۴.۴ .تعامل بین فناوری و الگوی جنگ

از تحلیل مضامین برمی‌آید که فناوری صرفاً ابزار نیست، بلکه بستر راهبردی طراحی و اجرای جنگ محسوب می‌شود. مدل استخراج‌شده در تصویر زیر قابل نمایش است:



شکل ۱-مراحل اجرای جنگ ترکیبی فناورمحور(محقق ساخته)

۵ .بحث، جمع‌بندی و نتیجه‌گیری

۵.۱ .بحث

نتایج این پژوهش نشان داد که جنگ ترکیبی فناورمحور علیه جمهوری اسلامی ایران، از منظر طراحی، اجرا و بهره‌برداری، الگوی جدیدی از نبرد مدرن را به نمایش گذاشت. برخلاف جنگ‌های متعارف که بر نبردهای نظامی در جبهه‌های فیزیکی تمرکز دارند، در این جنگ دشمنان با استفاده از فناوری‌های نوین، فضای نبرد را به درون زیرساخت‌ها، فضای مجازی، ذهن شهروندان، تصمیم‌گیران و حتی نظام حکمرانی کشور گسترش دادند.

در جنگ ۱۲ روزه میان ایران و اسرائیل، استفاده از فناوری‌های پیشرفته در راستای اهداف دشمن، به‌ویژه در حوزه نفوذ سایبری و اطلاعاتی، نقش تعیین‌کننده‌ای ایفا کرد .رژیم صهیونیستی با بهره‌گیری از ابزارهای هوش مصنوعی و فناوری‌های نوین، توانست اطلاعات حساس نظامی و امنیتی ایران را از طریق شبکه‌های ارتباطی و دستگاه‌های دیجیتال استخراج کرده و در طراحی عملیات‌های خود به‌کار گیرد .این اقدامات نه‌تنها شامل جمع‌آوری داده‌های ارتباطی و موقعیت‌یابی تجهیزات نظامی بود، بلکه با استفاده از الگوریتم‌های پیشرفته، الگوهای رفتاری نیروهای ایرانی را تحلیل و پیش‌بینی می‌کردند .در این راستا، گروه‌های هکری وابسته به اسرائیل توانستند با نفوذ به سامانه‌های مالی و بانکی ایران، عملیات‌های سایبری پیچیده‌ای را اجرا

کنند که علاوه بر آسیب‌های مالی، تأثیرات روانی و اجتماعی گسترده‌ای نیز به همراه داشت .این نوع از جنگ، که ترکیبی از حملات سایبری، جاسوسی دیجیتال و جنگ شناختی است، نشان‌دهنده تحول در شیوه‌های جنگی و استفاده از فناوری‌های نوین در راستای اهداف راهبردی دشمن است.

یافته‌ها با نظریه‌های جنگ ترکیبی، جنگ نسل پنجم (5GW) و جنگ شناختی کاملاً همخوان است؛ به‌ویژه با دیدگاه هافمن (۲۰۰۷) درباره تلفیق روش‌های نظامی و غیربازنظامی، و دیدگاه گیوردانو (۲۰۲۰) درباره تبدیل ادراک انسانی به میدان نبرد. فناوری در این جنگ نه تنها تسهیل‌گر بلکه «معمار میدان نبرد» بود؛ به‌گونه‌ای که ابزارهایی چون هوش مصنوعی، حملات سایبری، دیپ‌فیک، پهپادهای هوشمند، داده‌کاوی و مهندسی روانی، در تمامی مراحل عملیات ایفای نقش کردند.

مقایسه این الگو با سایر جنگ‌های ترکیبی (مانند جنگ اوکراین–روسیه یا جنگ اطلاعاتی علیه ونزوئلا) نشان می‌دهد که در جنگ ۱۲ روزه علیه ایران، شدت تمرکز بر لایه شناختی و سایبری بیش از سایر موارد بوده و عملیات فیزیکی صرفاً در مرحله نهایی و با هماهنگی دقیق با سایر حوزه‌ها انجام شده است. همین امر، نشان‌دهنده حرکت مهاجمان از الگوی «جنگ سخت» به سمت «فشار فناورانه ترکیبی» برای تغییر رفتار سیاسی ایران است.

۵.۲ .جمع‌بندی

در این مقاله، جنگ ۱۲ روزه به‌مثابه یک مطالعه موردی پیشرفته در حوزه جنگ‌های ترکیبی فناورمحور تحلیل شد. نتایج نشان می‌دهد جنگ فناورمحور علیه ایران الگوی جدیدی از نبرد چندلایه است که می‌تواند دکترین دفاع ملی را متحول کند.

بر اساس یافته‌های پژوهش، می‌توان جمع‌بندی زیر را ارائه داد:

- فناوری نقش محوری در طراحی، اجرا و مدیریت جنگ ایفا کرده است و صرفاً ابزاری مکمل نبوده است.
- جنگ در پنج مرحله طراحی شده بود: جمع‌آوری داده، تخریب زیرساخت، عملیات شناختی، ضربات دقیق و تثبیت راهبردی.
- شش بعد فناورانه اصلی در این جنگ شناسایی شد: سایبری، الکترونیک، پهپادی، فضایی، شناختی و اقتصادی.
- اهداف دشمن شامل تضعیف بازدارندگی، ایجاد اختلال در زیرساخت‌ها، فرسایش روانی، القای ناتوانی و تحمیل شرایط سیاسی بوده است.
- تعامل هم‌زمان بین لایه‌های مختلف عملیات (فناورانه–نظامی–رسانه‌ای) موجب افزایش اثربخشی و کاهش امکان پاسخ از سوی کشور هدف شده است.

۵.۳ .پیشنهادهای راهبردی

با توجه به ساختار پیچیده و فناورمحور این جنگ، می‌توان راهکارهایی برای تقویت دفاع ملی و کاهش آسیب‌پذیری ارائه کرد:

۱. تدوین دکترین دفاع فناورپایه: شامل سیاست‌گذاری هماهنگ در حوزه‌های سایبری، فضایی، شناختی و زیرساختی
۲. توسعه زیرساخت‌های بومی اطلاعاتی و ارتباطی: برای مقابله با وابستگی به فناوری‌های غربی

۳. افزایش تاب‌آوری شناختی جامعه: از طریق سواد رسانه‌ای، تقویت اعتماد عمومی و مقاومت روانی
٤. ایجاد مرکز فرماندهی جنگ ترکیبی ملی: برای هماهنگی بین نهادهای نظامی، امنیتی، سایبری، اقتصادی و رسانه‌ای
٥. پایش لحظه‌ای تهدیدات فناورانه نوظهور: به‌ویژه در حوزه هوش مصنوعی، الگوریتم‌های نفوذ، سکوهای مجازی و فناوری‌های تحریف ادراک
٦. آماده‌سازی مدل مقابله مرحله‌ای با جنگ ترکیبی: بر پایه شبیه‌سازی، سناریونویسی و رزمایش‌های فناوری‌محور

این یافته‌ها به سیاست‌گذاران دفاعی کمک می‌کند تا مدل تصمیم‌سازی دکترین ایران را از دفاع فیزیکی صرف به دفاع شناختی–فناورانه ارتقا دهند.

۵.۴ محدودیت‌ها و مسیرهای آینده پژوهش

پژوهش حاضر با محدودیت‌های زیر مواجه بوده است:

- **دسترسی محدود به داده‌های واقعی امنیتی و نظامی** به‌دلیل ملاحظات طبقه‌بندی اطلاعات.
- **وابستگی نسبی به منابع ثانویه** و تحلیل‌های غیرمیدانی.
- **چالش در انجام مصاحبه با نخبگان نظامی و فناور.**

پیشنهاد می‌شود در پژوهش‌های آینده از روش‌های شبیه‌سازی، سناریونویسی و داده‌کاوی واقعی رزمایش‌ها استفاده شود تا دقت مدل‌سازی افزایش یابد.

منابع

1. **Hoffman, F. G.** (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.
2. **Kello, L.** (2017). *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.
3. **Singer, P. W., & Brooking, E. T.** (2018). *LikeWar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt.
4. **Giordano, J.** (2020). *Cognitive Warfare: The Future of Conflict*. NATO Innovation Hub.
5. **Hammes, T. X.** (2007). *War evolves into the fourth generation*. *Military Review*, 87(3), 14–23.
6. **Rattray, G. J.** (2022). *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.
7. **Clark, B.** (2021). *Mosaic Warfare: Exploiting the Power of the Network*. Santa Monica, CA: RAND Corporation.
8. **Watts, S., & Binnendijk, A.** (2023). *Hybrid Warfare in Ukraine: Lessons for the Future*. Santa Monica, CA: RAND Corporation.
9. **Rid, T.** (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.
10. **Kaspersen, A.** (2016). *The Future of War is Cyber*. World Economic Forum. Retrieved from: https://www.weforum.org/agenda/2016/04/the-future-of-war-is-cyber
11. **Breaking Defense.** (2025). *New missile defenses, EW tactics aided Israel during 12-day Iran conflict*. Retrieved from: https://breakingdefense.com/2025/07/new-

missile-defenses-ew-tactics-aided-israel-during-12-day-iran-conflict/

12. **Times of Israel.** (2025). *Israel's 12-day war with Iran was a test of technological dominance*. Retrieved from: https://www.timesofisrael.com/israels-12-day-war-with-iran-was-a-test-of-technological-dominance/

13. **The Daily Star.** (2025). *How AI shaped the Iran-Israel 12-day war*. Retrieved from: https://www.thedailystar.net/opinion/views/news/how-ai-shaped-the-iran-israel-12-day-war-3927726

14. **Gulf News.** (2025). *Iran-Israel war: The rise and risks of hybrid warfare*. Retrieved from: https://gulfnews.com/premium/opinion/iran-israel-war-the-rise-and-risks-of-hybrid-warfare-1.500176446

15. **War on the Rocks.** (2025). *Lessons Observed from the War Between Israel and Iran*. Retrieved from: https://warontherocks.com/2025/07/lessons-observed-from-the-war-between-israel-and-iran/