

The Role of AI-Enabled Cyber Units in Changing Military Equations: Lessons From the Russo–Ukrainian War for Security in the Middle East

Mehdi Abbaszadeh
Fathabadi * 

Faculty Member, Department of Political
Science, Faculty of Law and Theolog, Shahid
Bahonar University of Kerman, Kerman, Iran

Mosayyeb Rostami
Khanmakani 

LLM, Diplomacy and International
Organizations, Department of Political Science,
Faculty of Law and Theology, Shahid Bahonar
University of Kerman, Kerman, Iran

Introduction

Digital transformation in the military domain has rapidly reshaped the nature of warfare and power. In this context, artificial intelligence (AI), as one of the most consequential emerging technologies, has ushered in a new wave of the revolution in military affairs. This transformation extends beyond the enhancement of weapons systems; it has also produced a paradigm shift in the speed of decision-making, models of command and control, and the concept of deterrence. Against this backdrop, the Russo–Ukrainian War, as the first major interstate conflict to unfold in the emerging age of AI, provides a vital

* Corresponding Author: abbaszadeh@uk.ac.ir

How to Cite: Abbaszadeh Fathabadi, M & Rostami Khanmakani, M, (2026), “The Role of AI-Enabled Cyber Units in Changing Military Equations: Lessons From the Russo–Ukrainian War for Security in the Middle East”, *Political Strategic Studies*, Vol. 15 (58), 155-246. Doi: [10.22054/qpss.2026.89724.3713](https://doi.org/10.22054/qpss.2026.89724.3713)

and increasingly well-documented case for analyzing the role of cyber units in integrating the physical, cyber, and cognitive dimensions of warfare. AI-enabled cyber units, supported by algorithmic learning and automated analytical capabilities, have not only enhanced and partially automated offensive and defensive operations but have also transformed the capacity for real-time strategic decision-making.

The present study aimed to examine the operational, organizational, and discursive nexus surrounding the use of AI-enabled cyber units in the Russo–Ukrainian War, exploring the implications of the lessons derived from this experience for Middle Eastern security. It tried to answer the following questions: What role do AI-enabled cyber units play in reshaping the military balance in the Russo–Ukrainian War? And what tangible implications do the strategic lessons derived from this conflict have for exacerbating or containing the security dilemma in the Middle East?

Literature Review

The existing literature on AI-enabled cyber warfare has focused predominantly on its hardware and technical dimensions, while failing to fully account for the multifaceted nature of the phenomenon. This dominant approach tends to overlook two crucial dimensions: (1) the significance of organizational and decentralized adaptations on the battlefield, and (2) the role of intangible, discursive, and narrative dimensions in conflicts occurring in the information age.

The literature can be broadly divided into two main streams. The first comprises studies that focus on the geopolitical competition among major powers, particularly the United States and China, over control of the global data-driven architecture and the implications of AI for the distribution of power. Examples include “A New Approach to Power Based on Artificial Intelligence: A Case Study of US–China Competition From 2010 to 2023” (Torki, 2024) and “The US–Sino Competition in the Field of Artificial Intelligence: From

Technonationalism to Technogeopolitics” (Pirmohammadi et al., 2024). These studies primarily examine AI and data as emerging sources of geopolitical power and strategic competition.

The second stream consists of studies examining hybrid warfare, cyber warfare, and transformations in the discursive dimensions of conflict. A notable example is the article titled “The Role of Artificial Intelligence Technology in Transforming the Nature of War: Based on the Study of Strategic Documents of the Zionist Regime” (Mohammadi-Monfared & Taghipour-Javi, 2025). This body of research examines the Russo–Ukrainian War as the first major conflict to unfold in the emerging age of AI, as well as the military strategies of the Zionist regime, with particular attention to the multifaceted dimensions of hybrid and cyber warfare. Despite the significance of previous research findings, a critical review of the literature reveals an important analytical gap regarding the operational–comparative link between the evolution of warfare and its implications for regional security.

Materials and Methods

This study employed a comparative case study approach. First, a content analysis of the documents at the strategic–operational level was conducted to draw key lessons from the experience of the Russo–Ukrainian War. These lessons were then applied to the competitive dynamics, vulnerable infrastructures, and technological capabilities of key Middle Eastern actors to identify potential future scenarios and threats. Moreover, the theoretical framework of cognitive realism—a synthesis of neoclassical realism and structuralism—was used to analyze material–semantic synergies in cyber-information operations. The analysis specifically focused on its analytical lens on the case of AI-enabled cyber units in the Russo–Ukrainian War.

Results and Discussion

The Russo–Ukrainian War clearly demonstrated that warfare is shifting from a mass model based on the concentration of forces and equipment toward a network- and data-driven structure, in which military superiority is increasingly a function of the speed of data collection and processing, the connectivity of information nodes, and the ability to immediately operationalize information, rather than simply the accumulation of resources. One of the most prominent consequences of this transformation is the significant shortening of the identification–decision–action cycle. Cyber units, electronic warfare operations, and AI-based signal and information analysis tools played a decisive role in supporting battlefield operations during the Russo–Ukrainian War. These capabilities were not only effective in identifying and disrupting enemy systems but were also used to coordinate diverse sources of information—including drones, satellites, and human intelligence—to produce a common operational picture. One of the defining dimensions of the Russo–Ukrainian War is the expansion of the battlefield into the cyber and information domains, where AI, as a strategic accelerator, has proven effective at both the level of offensive and defensive operations and the level of narrative warfare.

As the first large-scale field experiment combining AI with hybrid warfare, the Russo–Ukrainian War has provided a clear picture of the future of international security. The lessons of this war have profound implications, both at the theoretical level—by intensifying the security dilemma and redefining norms—and at the practical level—by highlighting the importance of organizational flexibility and material–semantic synergy. The Middle East is historically characterized by the nature of adversarial regimes, the strong presence of non-state actors, and arms races. The region is thus particularly susceptible to the reproduction and even intensification of these patterns. From this

perspective, the Ukrainian experience is not merely a case study but also a strategic warning for the future security of the Middle East. In comparative terms, the pattern of technological competition in the Middle East can be analyzed at three levels: (1) the centralized authoritarian model (Iran and Saudi Arabia), (2) the decentralized and networked technological model (Israel and the UAE), and (3) the intermediate model (Turkey). The most successful actors in the future will be those capable of combining technological innovation with organizational adaptability and intelligent narrative construction. Generally, the emerging threats to the Middle East in the age of AI have three main characteristics: (1) accelerated decision-making and intensified preemptive responses, (2) the expansion of the battlefield to civilian infrastructure, and (3) the increasing blurring of the distinction between war and peace. Together, these three trends provide a clear picture of a post-AI Middle East.

Conclusion

This study analyzed the strategic role of AI-enabled cyber units in transforming military equations, drawing strategic lessons from the experience of the Russo–Ukrainian War for the security of the Middle East. According to the findings, innovative strategic superiority depends on combining technological innovation with institutional adaptability and intelligent narrative construction. The emergence of AI in cyberspace is not merely a technological transformation but a revolution in military affairs that has simultaneously transformed the material (hardware competition) and semantic (narrative warfare) dimensions of hybrid warfare.

Applying the lessons of Ukraine to the Middle Eastern security environment suggests that the region has entered a new phase of technological competition that could lead to the Ukrainization of security, or the internal erosion of states. Competition among key actors such as Iran, Israel, and Turkey in developing AI-based

decision-making systems is shortening decision-making cycles and increasing the likelihood of preemptive action and miscalculation. The growing reliance of states on digital infrastructure makes them increasingly attractive targets for AI-driven cyberattacks, while cognitive warfare poses a direct threat to social cohesion and state legitimacy. Overall, this research suggested that the future of Middle Eastern security would lie not in absolute military power, but in states' ability to intelligently manage the interaction among technology, organization, and identity narratives in the age of algorithms.

Keywords: Artificial Intelligence, Cyber Units, Military Equations, Russo–Ukrainian War, The Middle East

تحلیل نقش یگان‌های سایبری مجهز به هوش مصنوعی در تغییر معادلات نظامی: مطالعه موردی جنگ اوکراین و درس‌های آن برای امنیت خاورمیانه

عضو هیئت علمی، گروه علوم سیاسی، دانشکده حقوق و الهیات،
دانشگاه شهید باهنر کرمان، کرمان، ایران

مهدی عباس‌زاده فتح‌آبادی *  ID

دانش آموخته کارشناسی ارشد دیپلماسی و سازمان‌های بین‌المللی،
دانشکده حقوق و الهیات، دانشگاه شهید باهنر کرمان، کرمان، ایران

مصیب رستمی خانمکانی  ID

چکیده

هوش مصنوعی موجی تازه از «انقلاب در امور نظامی» رقم زده است. این پژوهش تلاشی است برای بازاندیشی مفهوم قدرت در عصر الگوریتم‌ها و درک پیامدهای ژئوپلیتیکی ظهور جنگ‌های هوشمند. هدف پژوهش حاضر تحلیل نقش یگان‌های سایبری مجهز به هوش مصنوعی در تغییر معادلات نظامی بر اساس مطالعه موردی جنگ اوکراین است. همچنین اینکه این مسئله چه درس‌های راهبردی برای امنیت خاورمیانه می‌تواند داشته باشد؟ یافته‌های پژوهش بر اساس یک چارچوب تحلیلی تلفیقی از رئالیسم نئوکلاسیک و سازه‌نگاری نشان می‌دهد که ظهور هوش مصنوعی در فضای سایبری، ابعاد مادی (رقابت سخت‌افزاری) و معنایی (جنگ روایت‌ها) در جنگ‌های ترکیبی را دگرگون ساخته است. هوش مصنوعی به‌عنوان یک «تسریع‌کننده راهبردی» با فشردن چرخه شناسایی - تصمیم‌گیری - عمل، فرصت پاسخ‌دهی دولت‌ها را کاهش داده و معمای امنیت را در فضای سایبری تشدید کرده است. موفقیت نسبی اوکراین در دفاع سایبری ناشی از انعطاف‌پذیری سازمانی، مدل غیرمتمرکز فرماندهی و ادغام سریع ظرفیت‌های بخش خصوصی و داوطلبان بود. تطبیق درس‌های اوکراین با محیط امنیتی خاورمیانه نشان می‌دهد که منطقه وارد فاز جدیدی از رقابت فناورانه شده است که می‌تواند به «اوکراینی‌سازی امنیتی» دولت‌ها منجر شود. بر اساس یافته‌های پژوهش، برتری راهبردی نوآورانه در گرو تلفیق نوآوری فناورانه با انعطاف‌پذیری نهادی و مدیریت هوشمندانه روایت‌ها است.

واژگان کلیدی: هوش مصنوعی، یگان‌های سایبری، معادلات نظامی، جنگ اوکراین، خاورمیانه.

مقدمه

تحول دیجیتال در عرصه نظامی، مفهوم جنگ و قدرت را به سرعت دگرگون ساخته است. در این میان، هوش مصنوعی به عنوان یکی از فناوری‌های کلیدی، موجی تازه از «انقلاب در امور نظامی»^۱ را رقم زده است. تسلط دولت‌ها بر هوش مصنوعی، اثربخشی استراتژیک آینده آن‌ها در امور نظامی و همچنین عملکرد آن‌ها، رقابت و توانایی بازدارندگی در مقابل دشمنان را تعیین می‌کند (دهقانی فیروزآبادی و چهرآزاد، ۱۴۰۲: ۲۲۵). این دگرگونی، فراتر از ارتقای تسلیحات، یک تغییر پارادایمی در سرعت تصمیم‌گیری، الگوی فرماندهی و مفهوم بازدارندگی ایجاد کرده است. جنگ اوکراین در این بستر به مثابه نخستین منازعه بزرگ دولتی در عصر هوش مصنوعی، یک بستر مستند و حیاتی برای تحلیل نقش یگان‌های سایبری در پیوند زدن جبهه‌های فیزیکی، سایبری و شناختی فراهم آورده است. یگان‌های سایبری مجهز به هوش مصنوعی با تکیه بر خودیادگیری الگوریتمی نه تنها عملیات تهاجمی و دفاعی را خودکار کرده‌اند؛ بلکه توانایی تصمیم‌گیری راهبردی را در زمان واقعی متحول ساخته‌اند.

ادبیات موجود در این تحلیل سایبری مبتنی بر هوش مصنوعی عمدتاً بر ابعاد سخت‌افزاری و تکنیکی متمرکز بوده و از تبیین کامل ابعاد چندوجهی این پدیده ناکارآمد مانده است. این رویکرد غالب، دو بعد حیاتی را نادیده می‌گیرد: اهمیت سازگاری‌های سازمانی و غیرمتمرکز در میدان نبرد و نقش ابعاد غیرمادی، گفتمانی و روایتی در منازعات عصر اطلاعات. این مقاله برای پر کردن این خلأ، استدلال می‌کند که برتری راهبردی نوین نه تنها به قدرت پردازش مشروط است؛ بلکه به انعطاف‌پذیری نهادی و توانایی استفاده از هوش مصنوعی در جنگ روایت‌ها و هویت‌ها نیز مستلزم است. ساختارهای غیرمتمرکز سایبری، ظرفیت دولت‌ها برای مدیریت هم‌زمان جبهه فیزیکی و تولید سریع روایت‌های پشتیبان را تقویت می‌کنند. پرسش اصلی پژوهش این است که نقش یگان‌های سایبری مجهز به هوش مصنوعی در تغییر معادلات نظامی جنگ اوکراین چیست؟ و این درس‌های راهبردی چه پیامدهای ملموسی برای تشدید یا مهار معمای امنیت در خاورمیانه دارند؟

1. Revolution in Military Affairs (RMA)

سهم نوآورانه این مقاله در ادبیات امنیت سایبری، ارائه یک چارچوب تحلیلی تلفیقی است. این مقاله با ترکیب واقع‌گرایی نئوکلاسیک (که تحلیل را در سطح واحد - سطحی ظرفیت‌های دولتی) و تعامل آن با ساختار نظام بین‌الملل متمرکز می‌کند) و سازه‌انگاری (برای فهم ابعاد غیرمادی و هویتی)، یک لنز تحلیلی جامع برای درک هوش مصنوعی به‌عنوان عامل هم‌زمان رقابت مادی و بازتولید هویتی ارائه می‌دهد. نویسندگان به منظور تقویت جنبه کاربردی پژوهش، بین دو موضوع تغییر معادلات نظامی ناشی از به‌کارگیری یگان‌های سایبری مجهز به هوش مصنوعی در جنگ اوکراین و پیامدهای امنیتی این مسئله برای منطقه خاورمیانه و ایران پیوند ایجاد کرده‌اند. بر این اساس، نتیجه‌گیری این مقاله نه تنها یک سهم نظری جدید ارائه می‌دهد، بلکه یک هشدار راهبردی حیاتی و توصیه‌های سیاستی مشخص برای مدیریت رقابت هوش مصنوعی در خاورمیانه فراهم می‌آورد. این پژوهش تلاشی است برای بازاندیشی مفهوم قدرت در عصر الگوریتم‌ها و درک پیامدهای ژئوپلیتیکی ظهور جنگ‌های هوشمند.

پیشینه تحقیق

پیشینه پژوهش درباره امنیت سایبری، جنگ‌های نوین و تأثیر هوش مصنوعی بر معادلات نظامی، در یک دهه اخیر از رویکردهای صرفاً فنی فاصله گرفته و وارد مرحله جدیدی شده است. پژوهش‌های اولیه که عمدتاً بر ابعاد سخت‌افزاری و ظرفیت‌های تکنولوژیک متمرکز بودند، در تبیین ابعاد چندوجهی و سازمانی - گفتمانی دگرگونی پدیده جنگ و پیامدهای آن برای امنیت بین‌الملل و منطقه‌ای، دچار کاستی هستند. این مقاله با هدف پر کردن خلأ تحلیلی در پیوند عملیاتی، سازمانی و گفتمانی میان یگان‌های سایبری مجهز به هوش مصنوعی در یک منازعه واقعی (جنگ اوکراین) و تبیین درس‌های آن برای امنیت خاورمیانه، ادبیات موجود را در دو جریان اصلی زیر واکاوی می‌کند تا زمینه‌ساز تبیین چارچوب نظری «رنالیسم شناختی» و سهم نوآورانه خود گردد.

دسته اول پژوهش‌هایی هستند که بر رقابت ژئوپلیتیک قدرت‌های بزرگ (به‌ویژه آمریکا و چین) بر سر کنترل معماری داده‌محور جهانی و تأثیر هوش مصنوعی بر توزیع قدرت تمرکز دارند. به‌عنوان مثال عباس‌زاده و رستمی (۱۴۰۴) در مقاله «ابعاد مادی و

غیرمادی ژئوپلیتیک نوین هوش مصنوعی: پویایی‌های رقابت آمریکا و چین»، ژئوپلیتیک هوش مصنوعی را فراتر از نبرد بر سر پردازنده‌ها، یک منازعه بنیادین بر سر ترسیم نظم نوظهور داده‌محور تلقی می‌کنند. این آثار با چارچوب‌های تلفیقی نشان می‌دهند که چگونه رویکردهای واگرایانه در سیاست صنعتی و حکمرانی (بعد مادی) که ریشه در تصورات آرمانی فنی - اجتماعی ملی (بعد غیرمادی) دارند، مبنای رقابت ژئوپلیتیکی میان قدرت‌ها را شکل می‌دهند. پیرمحمدی و همکاران (۱۴۰۴) در مقاله‌ای با عنوان «رقابت آمریکا و چین در حوزه هوش مصنوعی؛ از ملی‌گرایی فنی تا جغرافیای سیاسی فنی» بحث می‌کنند که چگونه تلاش‌ها و اقدام‌های آمریکا و چین برای رهبری عرصه فناوری، ملاحظات راهبردی آن‌ها در تمامی حوزه‌ها را تحت تأثیر قرار داده است. رهبران چین، هوش مصنوعی را فرصتی برای مقابله با سلطه نظامی و فناوری آمریکا و کسب برتری راهبردی می‌دانند. در نقطه مقابل نیز توانمندی‌های فناوری رو به رشد چین عامل اصلی تلاش‌های ایالات متحده برای ایجاد بلوکی از اقتصادهای رقومی (دیجیتال) در راستای موازنه‌سازی قدرت فزاینده چین است. همچنین هادی ترکی (۱۴۰۳) در مقاله «رهیافت جدید قدرت مبتنی بر هوش مصنوعی (مطالعه موردی رقابت آمریکا و چین از ۲۰۱۰ تا ۲۰۲۳)» بحث می‌کند که رقابت سخت آمریکا و چین در عرصه هوش مصنوعی بر حوزه‌های نظامی، دفاعی و اقتصادی متمرکز بوده و در عرصه نرم نیز تلاش و رقابت برای نشان دادن رهبری مناسب در سطح جهان برای کسب اعتبار و مشروعیت بین‌المللی در دهه‌های آینده است.

دسته دوم آثاری هستند که بر جنگ‌های ترکیبی، سایبر و دگرگونی گفتمانی متمرکز هستند. این جریان پژوهشی، تمرکز خود را بر جنگ اوکراین به عنوان نخستین منازعه بزرگ در عصر هوش مصنوعی و راهبردهای نظامی رژیم صهیونیستی معطوف کرده و ابعاد چندوجهی جنگ‌های ترکیبی/هیبریدی و سایبری را بررسی می‌کند. شکوهی و کریمی (۱۴۰۲) در مقاله «جنگ هیبریدی روسیه در منازعه ۲۰۲۲ اوکراین»، به واکاوی ابعاد و تأثیر جنگ هیبریدی روسیه علیه اوکراین پرداخته‌اند. یافته‌ها بر استفاده روسیه از تاکتیک‌های جنگ رسانه‌ای، حملات سایبری و حملات هدفمند به زیرساخت‌های کلیدی

تأکید دارند که اهمیت همگرایی جبهه‌های فیزیکی و سایبری را آشکار می‌سازد. در همین زمینه نوروزی و همکاران (۱۴۰۱) در مقاله «واکاوی جنگ روسیه و اوکراین از منظر امنیت هستی‌شناختی» بر ابعاد غیرمادی و گفتمانی منازعات تمرکز دارند و نشان می‌دهند که چگونه ایده‌ها، هویت‌ها و روایت‌ها می‌توانند محرک یک اقدام نظامی باشند و نیز در سطحی مرتبط، مقاله محمدی منفرد و تقی‌پور جاوی (۱۴۰۳) به طور مستقیم به بررسی تأثیر هوش مصنوعی بر ماهیت جنگ کلاوزیوتسی (خشونت، شانس و سیاسی بودن) با استفاده از مطالعه اسناد راهبردی رژیم صهیونیستی پرداخته و نشان داده‌اند که هوش مصنوعی می‌تواند تمامی ابعاد ماهیت جنگ را بازتعریف کند.

بررسی انتقادی ادبیات نشان می‌دهد که علی‌رغم پژوهش‌های عمیق در سطوح ژئوپلیتیک (دسته اول) و دگرگونی ماهیت جنگ و تبیین نحوه تعامل و هم‌افزایی ابعاد مادی و گفتمانی (دسته دوم)، در خصوص تحول پدیده جنگ و پیامدهای آن برای امنیت منطقه‌ای، شکاف‌های تحلیلی در خصوص پیوند عملیاتی - مقایسه‌ای وجود دارد. فقدان پژوهش نظام‌مندی که به طور مستقیم، درس‌های عملیاتی استفاده از یگان‌های سایبری مجهز به هوش مصنوعی در جنگ اوکراین را استخراج کرده و سپس آن را به عنوان یک نقشه راه سازمانی برای تحلیل الزامات امنیت خاورمیانه (سطح سازمانی بازیگران منطقه‌ای) به کار گیرد احساس می‌شود. همچنین خلأ در سنتز نظری نیز مشاهده می‌شود: عدم توانایی پژوهش‌ها در تلفیق ابعاد مادی - سازمانی (واقع‌گرایی نئوکلاسیک / ظرفیت دولتی) و گفتمانی - ادراکی (سازه‌انگاری / هویت و روایت) به صورت هم‌زمان و در چارچوب هم‌افزایی مادی - معنایی، ضرورت پژوهش در این حوزه را ایجاب می‌کند.

سهم نوآورانه این مقاله، پر کردن این خلأ عملیاتی و سنتز نظری است. این پژوهش نه تنها از چارچوب نظری «رنالیسم شناختی» (تلفیق واقع‌گرایی نئوکلاسیک و سازه‌انگاری) برای تحلیل هم‌افزایی مادی - معنایی در عملیات‌های سایبری - اطلاعاتی بهره می‌برد، بلکه به طور خاص، لنز تحلیلی خود را بر مطالعه موردی یگان‌های سایبری مجهز به هوش مصنوعی در جنگ اوکراین متمرکز می‌کند.

روش پژوهش

در این پژوهش برای گردآوری اطلاعات از منابع کتابخانه‌ای شامل کتاب، مقاله، اسناد و سایت‌های معتبر استفاده شده و برای تجزیه و تحلیل از روش تحلیل محتوا استفاده می‌شود. همچنین این پژوهش از روش مطالعه موردی تطبیقی بهره می‌برد. در ابتدا با استفاده از تحلیل محتوای اسنادی و با تمرکز بر سطح راهبردی - عملیاتی، درس‌های کلیدی از تجربه جنگ اوکراین استخراج می‌شوند. سپس این درس‌ها بر پویایی‌های رقابتی، زیرساخت‌های آسیب‌پذیر و توانمندی‌های فناورانه بازیگران کلیدی خاورمیانه تطبیق داده می‌شوند تا سناریوهای آینده و تهدیدات پیش رو مشخص گردند.

چارچوب نظری

چارچوب نظری پژوهش بر مبنای تلفیق دو نظریه واقع‌گرایی نئوکلاسیک و سازه‌انگاری در جهت هم‌افزایی ابعاد تحلیلی مختلف در موضوع مورد بحث می‌باشد که به آن‌ها پرداخته می‌شود.

الف- واقع‌گرایی نئوکلاسیک و معمای امنیت در فضای سایبر

واقع‌گرایی نئوکلاسیک در دهه‌های اخیر به‌عنوان یکی از جریان‌های مهم در روابط بین‌الملل ظهور کرده و کوشیده است تا کاستی‌های واقع‌گرایی ساختاری والتز را جبران کند. این رویکرد ضمن پذیرش اهمیت ساختار بین‌المللی، بر نقش متغیرهای «واحد - سطحی» مانند ادراک رهبران، ظرفیت‌های نهادی و فشارهای سیاسی داخلی در تبدیل فشارهای بیرونی به سیاست‌های مشخص تأکید دارد (Lobell et al., 2009: 1-5). بنابراین، سیاست خارجی دولت‌ها نه صرفاً برآیند فشارهای ساختاری، بلکه محصولی از تعامل این فشارها با ادراکات و توانایی‌های داخلی است (Kozub-Karkut, 2019: 203).

این رویکرد در حوزه سایبری اهمیت مضاعف می‌یابد؛ زیرا فضای سایبری ویژگی‌هایی دارد که معمای امنیت را تشدید می‌کند: هزینه پایین ورود، ناشناس بودن عاملان، دشواری در انتساب حملات و توانایی بازیگران کوچک برای ایجاد تهدید علیه

قدرت‌های بزرگ (Nye, 2010: 2). در این میان، هوش مصنوعی یک «تسریع‌کننده» است. الگوریتم‌های یادگیری ماشینی می‌توانند به صورت خودکار آسیب‌پذیری‌ها را شناسایی کرده، زمان حمله را به حداقل برسانند و چرخه تصمیم‌گیری - اقدام را تسریع کنند (میراحمدی و امیدی، ۱۴۰۳: ۲۸۷). نتیجه این است که فرصت پاسخ‌دهی برای دولت‌ها به شدت کاهش یافته و وسوسه حمله پیش‌دستانه افزایش پیدا می‌کند؛ زیرا هر طرف نگران است که تأخیر، به معنای ازدست‌دادن برتری باشد. این شتاب بخشی ناشی از هوش مصنوعی، همان چیزی است که نئو کلاسیک‌ها به عنوان «تشدید معمای امنیت» تعبیر می‌کنند (Meibauer et al., 2021: 270-272). از منظر تجربی نیز تحلیل‌های اخیر نشان می‌دهد که رئالیسم نئو کلاسیک ابزار مناسبی برای توضیح رقابت‌های سایبری است. میبائر و همکاران نیز نشان داده‌اند که پذیرش متغیرهای مداخله‌گر مانند افکار عمومی، روایت‌های فرهنگی و ظرفیت‌های استخراج منابع، رئالیسم نئو کلاسیک را به چارچوب مسلط واقع‌گرایان در تحلیل سیاست خارجی بدل ساخته است (Meibauer et al., 2021: 270-272). در نتیجه می‌توان گفت هوش مصنوعی با کاهش زمان تصمیم‌گیری، افزایش پیچیدگی حملات و فراهم کردن امکان استفاده مؤثر از منابع برای بازیگران کوچک‌تر، به طور مستقیم شدت معمای امنیت سایبری را افزایش می‌دهد.

ب- سازه‌انگاری و جنگ هویت‌ها و روایت‌ها

سازه‌انگاری برخلاف رویکردهای واقع‌گرایانه بر نقش هنجارها، ایده‌ها و هویت‌ها در شکل‌دهی به سیاست جهانی تأکید می‌کند. الکساندر ونت در اثر مهم خود «نظریه اجتماعی سیاست بین‌الملل» بیان می‌کند که نظام بین‌الملل بیش از آنکه یک ساختار مادی باشد، یک «ساختار اجتماعی» است که بر مبنای ایده‌ها و برداشت‌های مشترک بنا شده است. او سه فرهنگ آنارشی-هابزی، لاکي و کانتی-را معرفی می‌کند که بر اساس نوع رابطه میان دولت‌ها (دشمن، رقیب یا دوست) شکل می‌گیرند (Wendt, 1999: 246-300).

در فضای سایبری، این نگاه سازه‌انگارانه اهمیت ویژه دارد؛ چرا که جنگ‌ها در این حوزه نه تنها در سطح سخت‌افزاری، بلکه در سطح معنایی و هویتی رخ می‌دهند. عملیات‌های روانی، تولید اخبار جعلی و بهره‌گیری از فناوری‌هایی مانند «دپ‌فیک»

ابزارهایی هستند که می‌توانند ادراک عمومی را تغییر داده و هویت‌های جمعی را تضعیف کنند (Valeriano & Maness, 2015: 45). به بیان دیگر در جنگ سایبری، نبرد بر سر «معنا» و «روایت» همان قدر مهم است که نبرد بر سر زیرساخت‌ها. مثال بارز این موضوع در جنگ اوکراین مشهود است. روسیه در کنار حملات سایبری و نظامی سخت‌افزاری، روایت‌های متعددی برای مشروعیت‌بخشی به اقدامات خود تولید کرد. در مقابل، اوکراین با بهره‌گیری از شبکه‌های اجتماعی و روایت‌های هویتی توانست خود را به عنوان «مدافع دموکراسی» معرفی کند و حمایت جهانی را جلب نماید. این نشان می‌دهد که جنگ هویتی و روایت‌ها چگونه می‌تواند پیامدهای راهبردی داشته باشد.

هوش مصنوعی این فرایند را تشدید می‌کند. الگوریتم‌های تولید محتوا قادرند انبوهی از پیام‌های تفرقه‌افکن یا ملی‌گرایانه را به صورت هدفمند به مخاطبان مختلف عرضه کنند و هویت‌های مشترک را متزلزل سازند. این امر می‌تواند انسجام داخلی کشورها را از درون تضعیف کرده و حتی بدون حمله فیزیکی، بی‌ثباتی سیاسی ایجاد کند. علاوه بر این، استفاده از سامانه‌های خودمختار برای تولید محتوای جعلی و دیپ‌فیک، چالش‌های جدیدی را در برابر هنجارهای بین‌المللی مطرح می‌سازد. آیا استفاده از این ابزارها مشروع است؟ آیا می‌توان مرزی میان «قدرت نرم مشروع» و «دست‌کاری مخرب» ترسیم کرد؟ این پرسش‌ها نشان می‌دهد که با ظهور هوش مصنوعی، هنجارهای پیشین درباره رفتار مجاز در فضای سایبری در حال بازتعریف است.

پ- پیوند نظری: هم‌افزایی معمای امنیت (واقع‌گرایی) و جنگ روایت‌ها (سازه‌انگاری)

پیوند میان رویکرد رئالیسم نئوکلاسیک و سازه‌انگاران در حوزه هوش مصنوعی ما را به مفهوم «انقلاب در امور نظامی» نوین می‌رساند. هوش مصنوعی در واقع به عنوان یک محرک پارادایمی، این دو نیروی متضاد (مادی و معنایی) را به طور هم‌زمان فعال می‌کند و از این رهگذر، «انقلاب در امور نظامی» جدید شکل می‌گیرد: در بعد مادی، هوش

مصنوعی چرخه شناسایی - تصمیم‌گیری - عمل^۱ را سرعت می‌بخشد، کارایی تسلیحات هوشمند را افزایش می‌دهد و امکان حملات سایبری پیچیده‌تر و کم‌هزینه‌تر را فراهم می‌سازد. این امر معمای امنیت سایبری (دیدگاه نئو کلاسیک) را تشدید کرده و دولت‌ها را برای حفظ موازنه قدرت وادار به اقدام پیش‌دستانه می‌کند و در بعد معنایی، همین فناوری می‌تواند روایت‌ها را شکل دهد، دیپ‌فیک تولید کند و با دست‌کاری اطلاعات، اعتماد عمومی را از بین ببرد. این همان جنگ روایت‌ها و هویت‌ها (دیدگاه سازه‌انگاران) است که به تضعیف مشروعیت دولت‌ها در طول منازعه کمک می‌کند.

این دو بعد اغلب هم‌زمان عمل می‌کنند. برای نمونه یک حمله سایبری به زیرساخت (بعد مادی) اگر با موجی از اخبار جعلی درباره ناتوانی دولت همراه شود (بعد معنایی)، هم‌افزایی مادی - معنایی رخ می‌دهد. این هم‌افزایی، ویژگی بارز جنگ‌های ترکیبی در عصر هوش مصنوعی و همان «انقلاب در امور نظامی» نوین است. بدین ترتیب هوش مصنوعی به مثابه یک «مضاعف‌کننده قدرت» نه تنها معمای امنیت را تشدید می‌کند، بلکه امکان جنگ‌های ترکیبی در مقیاسی بی‌سابقه را نیز فراهم می‌سازد (Nye, 2014: 9).

نوآوری اصلی این پژوهش در ارائه چارچوبی تلفیقی است که شکاف میان متغیرهای مادی و غیرمادی قدرت را در تحلیل تحول امنیتی ناشی از هوش مصنوعی پر می‌کند. در حالی که رئالیسم نئو کلاسیک بر «ظرفیت سازمانی دولت‌ها» و «ادراک نخبگان تصمیم‌گیر» در تبیین رفتار امنیتی تمرکز دارد (Ripsman et al., 2016)، سازه‌انگاری بر قدرت هنجارها، روایت‌ها و بازنمایی اجتماعی فناوری تأکید می‌کند (Wendt, 1999). این پژوهش استدلال می‌کند که تحولات امنیتی مرتبط با هوش مصنوعی در جنگ اوکراین و خاورمیانه را نمی‌توان صرفاً با یکی از این دو چارچوب توضیح داد؛ بلکه باید هر دو سطح مادی - سازمانی و گفتمانی - ادراکی را به صورت هم‌زمان در نظر گرفت. بدین ترتیب، این پژوهش نوعی رئالیسم شناختی^۲ را پیشنهاد می‌کند که تعامل میان ادراک نخبگان، ظرفیت‌های فناورانه و هنجارهای بین‌الذهانی را در قالبی واحد تلفیق می‌کند -

1. Observe-Orient-Decide-Act (OODA Loop)

2. Cognitive Realism

تمایزی که آن را از سایر رویکردهای تجمیعی مانند رئالیسم - لیبرالیسم یا سازه‌انگاری - لیبرالیسم متمایز می‌سازد.

چارچوب نظری این پژوهش با تلفیق واقع‌گرایی نئوکلاسیک و سازه‌انگاری، تحلیلی جامع از نقش یگان‌های سایبری مجهز به هوش مصنوعی در جنگ‌های معاصر ارائه می‌دهد. از یک‌سو واقع‌گرایی نئوکلاسیک نشان می‌دهد که فشارهای ساختاری و ظرفیت‌های داخلی چگونه سیاست‌های سایبری را شکل می‌دهند و معمای امنیت را تشدید می‌کنند. از سوی دیگر سازه‌انگاری بر جنگ روایت‌ها، هویت‌ها و بازتعریف هنجارهای بین‌المللی در عصر هوش مصنوعی تأکید دارد. نهایتاً مفهوم انقلاب در امور نظامی با میانجی‌گری هوش مصنوعی این دو سطح را به هم پیوند می‌دهد و تصویری چندبعدی از جنگ‌های ترکیبی ارائه می‌کند؛ جنگ‌هایی که نه تنها زیرساخت‌ها، بلکه ذهن و هویت جوامع را نیز هدف قرار می‌دهند.

یافته‌های پژوهش

در این قسمت از مقاله ابتدا تحولات میدانی جنگ اوکراین و موضوع یگان‌های سایبری برای تحلیل تغییرات در شیوه جنگ‌های امروزی با کاربرد هوش مصنوعی مورد بررسی قرار می‌گیرد و سپس تطبیق بحث در مورد خاورمیانه و تشدید معمای امنیت سایبری در این منطقه صورت می‌گیرد. همچنین پیشنهادهای سیاستی در این زمینه برای تقویت سیاست‌ها و راهبردها در حوزه نظامی و امنیتی در جهت تامین منافع ملی مطرح می‌گردد.

جنگ اوکراین: تحلیل میدانی یک تحول در حال وقوع

جنگ اوکراین به طور آشکار نشان داد که نبردها از الگوی «توده‌ای» مبتنی بر تراکم نیرو و تجهیزات به سمت یک ساختار شبکه‌ای - داده‌محور در حال گذار هستند؛ ساختاری که در آن برتری نظامی بیش از آنکه صرفاً محصول انباشت منابع باشد، تابع سرعت گردآوری و پردازش داده، اتصال گره‌های اطلاعاتی و توانایی به‌کارگیری فوری اطلاعات است. یکی از پیامدهای برجسته این تغییر، کوتاه‌سازی چشمگیر چرخه شناسایی -

تصمیم‌گیری - عمل است. سامانه‌های خودکار تشخیص هدف^۱ و ابزارهای پردازش بلادرننگ تصاویر پهپادی/ ماهواره‌ای با کمک الگوریتم‌های یادگیری ماشینی، بخش قابل توجهی از بار شناختی فرماندهی را کاهش داده و امکان واکنش‌های سریع‌تری را فراهم آوردند (Slusher et al., 2025: 27). این تحول به‌ویژه در فاز «جهت‌گیری»^۲ محسوس بوده است؛ جایی که تبدیل داده خام به اطلاعات عملیاتی با تأخیر کم، به تغییرات تاکتیکی فوری می‌انجامد.

اوکراین و تجربه یگان‌های سایبری در عملیات جنگ الکترونیک

یگان‌های سایبری و عملیات جنگ الکترونیک^۳ و ابزارهای تحلیل اطلاعات سیگنالی^۴ مبتنی بر هوش مصنوعی در جنگ اوکراین نقش تعیین‌کننده‌ای در پشتیبانی از عملیات میدانی داشتند. این نهادها نه تنها در شناسایی و اختلال سیستم‌های دشمن مؤثر بودند، بلکه در هماهنگ‌سازی تأمین‌کننده‌های اطلاعات (پهپاد، ماهواره، منابع انسانی) برای تولید یک تصویر عملیاتی مشترک به کار گرفته شدند. با این حال تحقیقات میدانی نشان می‌دهد که هماهنگی میان یگان‌های سایبری داوطلب و ساختارهای رسمی ارتش همیشه بدون تنش نبوده و ضعف در «قابلیت همکاری» گاه موجب تأخیر یا تضاد اطلاعاتی شده است (Grzegorzewski et al., 2022: 32).

اوکراین با توسعه دکرین پهپادمحور و شبکه‌سازی گسترده (استفاده از گره‌های پهپادی/حسگر)^۵ توانست تصویر مشترک عملیاتی را در سطوح پایین‌تری در اختیار واحدها قرار دهد و این امر کارایی رزمی را افزایش داد (Slusher et al., 2025: 27). اما وابستگی گسترده به شبکه‌های داده‌ای و ارتباطات ماهواره‌ای از جمله استفاده نظامی - غیردولتی از استارلینک، هزینه‌هایی هم به همراه داشت: حملات متمرکز جنگ الکترونیک و تلاش‌های روسیه برای اختلال یا اختلال در سرویس‌های ماهواره‌ای در برخی

1. Automatic Target Recognition

2. Orientation

3. EW

4. SIGINT

5. UAV/ Sensor Nodes

مقاطع کارایی این شبکه‌ها را تضعیف کرد (Wang et al., 2024: 12). گزارش‌های میدانی همچنین نشان می‌دهد که در زمستان‌های ۲۰۲۳-۲۰۲۴، حملات هدفمند به زیرساخت‌های انرژی و شبکه‌های ارتباطی، فشار عملیاتی و سیاسی قابل توجهی بر ظرفیت‌های دفاعی اوکراین وارد ساخت (United Nations Human Rights Monitoring Mission in Ukraine, 2024).

مدل غیرمتمرکز اوکراینی مبتنی بر بسیج داوطلبان سایبری و تعامل با بخش خصوصی، نقطه قوت بزرگی در سال‌های اولیه جنگ بود؛ اما پژوهش‌ها نشان داده‌اند که استمرار این الگو در دوره‌های طولانی‌مدت به مشکلاتی منجر شده است: فرسایش نیروی انسانی داوطلب، نوسان کیفیت تخصص‌ها و نیاز مداوم به مدیریت هماهنگ و استانداردسازی فرایندها (Kaushik, 2023: 1). نبود چارچوب‌های رسمی مناسب برای یکپارچه‌سازی داده‌ها و رویه‌ها و نیز مشکلات قانونی/پرداختی مرتبط با داوطلبان، از جمله محدودیت‌هایی است که کارایی بلندمدت مدل غیرمتمرکز را به چالش می‌کشد.

نتیجه این که اوکراین نمونه‌ای از گذار مؤثر به جنگ شبکه‌ای است؛ اما این گذار همراه با یک معادله «هزینه-فایده» است: افزایش سرعت و دقت تصمیم‌گیری هم‌زمان با افزایش آسیب‌پذیری در برابر اختلالات ارتباطی، جنگ الکترونیک و فشار طولانی‌مدت بر سرمایه انسانی. بنابراین برای بهره‌برداری از مزایای «انقلاب در امور نظامی» مبتنی بر هوش مصنوعی، کشورها باید علاوه بر سرمایه‌گذاری در فناوری، بر توسعه سازوکارهای استانداردسازی، تبادل بین‌سازمانی، تاب‌آوری زیرساختی و سیاست‌های حمایت از نیروی انسانی تمرکز کنند. این یافته‌ها با استدلال ما درباره اهمیت ترکیب متغیرهای «سخت» (فناوری) و «نرم» (سازمانی-گفتمانی) در تحلیل «انقلاب در امور نظامی» نوین همخوانی دارد.

یکی از ابعاد تعیین‌کننده جنگ اوکراین، انتقال میدان نبرد به حوزه سایبری و اطلاعاتی است؛ جایی که هوش مصنوعی به‌عنوان یک «تسریع‌کننده راهبردی» توانسته هم در سطح عملیات‌های تهاجمی-دفاعی و هم در سطح جنگ روایت‌ها اثرگذار باشد. این بخش بر

مبنای دو سطح مادی و معنایی جنگ‌های ترکیبی، به تحلیل نقش یگان‌های سایبری مجهز به هوش مصنوعی در این جنگ می‌پردازد.

استراتژی متمرکز روسیه در برابر الگوی غیرمتمرکز اوکراین

روسیه از سال ۲۰۱۴ یک دکترین سایبری متمرکز را دنبال کرده که در آن نهادهای امنیتی همچون جی.آر.یو و اف.اس.بی نقش اصلی را ایفا می‌کنند. در جریان تهاجم ۲۰۲۲، حملات سایبری گسترده‌ای علیه زیرساخت‌های حیاتی اوکراین از جمله شبکه برق، بانک‌ها و سامانه‌های فرماندهی-کنترل اجرا شد. این حملات عمدتاً شامل حملات ممانعت از سرویس‌دهی^۱، بدافزارهای پاک‌کننده اطلاعات و عملیات‌های ترکیبی هم‌زمان با حملات موشکی بود (Pinko, 2023: 62-64). با این حال، کارایی این عملیات‌ها محدود بود و نتوانست به فلج شدن کامل زیرساخت‌ها بینجامد.

در مقابل، اوکراین با تکیه بر مدل غیرمتمرکز شامل «ارتش فناوری اطلاعات» متشکل از متخصصان، داوطلبان سایبری و همکاری با بخش خصوصی غربی، توانست بخش بزرگی از این حملات را خنثی کند. نقش هوش مصنوعی در اینجا حیاتی بود؛ سامانه‌های هوش مصنوعی با تحلیل بلادرنگ ترافیک شبکه، حملات را شناسایی و دفاع خودکار را امکان‌پذیر کردند (Slusher et al., 2025: 27). این انعطاف‌پذیری سازمانی، نشان‌دهنده اهمیت متغیرهای واحد-سطحی در چارچوب واقع‌گرایی نئوکلاسیک است.

کاربرد هوش مصنوعی در جنگ روایت‌ها و عملیات‌های روانی

از منظر سازه‌نگاری، جنگ اوکراین بیش از هر چیز یک جنگ روایت‌ها بود. روسیه با بهره‌گیری از تاریخ‌نگاری ایدئولوژیک و روایت «نازی‌زدایی» کوشید مشروعیت تهاجم خود را تثبیت کند (Aleksjeva, 2023: 6). این روایت‌ها با کمپین‌های اطلاعات غلط، دیپ‌فیک‌ها و عملیات رسانه‌ای در فضای مجازی همراه شد (Thornton & Miron, 2022: 118-120). در مقابل، اوکراین توانست با هوشمندسازی پیام‌رسانی دیجیتال و استفاده از الگوریتم‌های هوش مصنوعی برای تحلیل افکار عمومی جهانی، روایت «مدافع

1. DOS

دموکراسی» را غالب کند. ابزارهایی مانند اپلیکیشن دییا^۱ که یک پلتفرم حکمرانی الکترونیکی دولت اوکراین است و کمپین‌های شبکه‌های اجتماعی که به صورت هدفمند پیام‌ها را به مخاطبان مختلف ارسال می‌کردند، نقش کلیدی در بسیج حمایت بین‌المللی ایفا کردند (Slusher et al., 2025: 26–27).

عملیات‌های نفوذ سایبری و تشدید معمای امنیت

عملیات‌های نفوذ سایبری بخشی جدایی‌ناپذیر از استراتژی روسیه است. حملات مکرر علیه زیرساخت انرژی، نیروگاه‌های هسته‌ای و سامانه‌های فرماندهی نظامی اجرا شد، هرچند نتایج عملیاتی محدود بود (Pinko, 2023: 64). روسیه همچنین از حملات «سایبر-روانی» برای تأثیرگذاری بر روحیه شهروندان و تصمیم‌گیران اوکراینی استفاده کرد (Thornton & Miron, 2022: 119). در همین چارچوب برخی گزارش‌ها حاکی از آن است که روسیه از الگوریتم‌های هوش مصنوعی برای بهینه‌سازی حملات فیشینگ هدفمند و توسعه بدافزارهای تطبیق‌پذیر استفاده کرده است؛ روندی که بیانگر ظهور یک رقابت تسلیحاتی سایبری مبتنی بر هوش مصنوعی است، حتی اگر نتایج عملیاتی فوری محدود باقی مانده باشد. در سوی مقابل، اوکراین با بسیج یک «ارتش داوطلبان سایبری» و استفاده از سامانه‌های تشخیص نفوذ مبتنی بر هوش مصنوعی توانست بخش زیادی از این حملات را مهار کند (Slusher et al., 2025: 27). اما همان‌طور که واقع‌گرایی نئوکلاسیک پیش‌بینی می‌کند، هر نوآوری دفاعی اوکراین به‌عنوان تهدیدی برای روسیه تلقی شد و چرخه‌ای از «تشدید معمای امنیت سایبری» شکل گرفت.

جبهه سایبری و اطلاعاتی جنگ اوکراین نشان داد که هوش مصنوعی به طور هم‌زمان دو سطح مادی و معنایی جنگ‌های ترکیبی را دگرگون کرده است. در سطح مادی، هوش مصنوعی چرخه دفاع و حمله سایبری را تسریع و پیچیده‌تر کرد. در سطح معنایی، الگوریتم‌ها توانستند روایت‌ها را شکل داده و افکار عمومی را دست‌کاری کنند. ترکیب این دو بعد همان چیزی است که در چارچوب «انقلاب در امور نظامی» می‌توان آن را یک

1. Diia

تحول پارادایمی در جنگ‌های معاصر دانست. افزون بر این، موفقیت نسبی اوکراین در دفاع سایبری غیرمتمرکز - به‌ویژه با تکیه بر سامانه‌های هوش مصنوعی - توانست شبکه‌سازی لازم برای حفظ تسریع چرخه تصمیم‌گیری و کارایی عملیات پهبادی را تضمین کند؛ به این ترتیب، جبهه‌های سایبری و فیزیکی در یک رابط عملیاتی هم‌افزا به هم گره خوردند.

جمع‌بندی درس‌های کلیدی از جنگ اوکراین

تحلیل میدانی جنگ اوکراین چندین درس اساسی برای فهم آینده جنگ‌های ترکیبی در عصر هوش مصنوعی به همراه دارد:

الف- تشدید معمای امنیت سایبری

هوش مصنوعی با فشرده‌سازی چرخه تصمیم‌گیری و افزایش سرعت و پیچیدگی حملات، فرصت پاسخ‌دهی دولت‌ها را کاهش داد و وسوسه اقدامات پیش‌دستانه را تقویت کرد. این امر موجب تشدید «معمای امنیت» در فضای سایبری شد؛ وضعیتی که در آن هر نوآوری دفاعی یک طرف، به‌عنوان تهدیدی برای طرف مقابل تلقی می‌شود و چرخه‌ای از رقابت تسلیحاتی سایبری شکل می‌گیرد (Devanny, 2024: 16).

ب- اهمیت سازگاری سازمانی

تجربه اوکراین نشان داد که صرفاً برخورداری از فناوری‌های پیشرفته کافی نیست. انعطاف‌پذیری سازمانی و توانایی ادغام داوطلبان و بخش خصوصی در مدل دفاع غیرمتمرکز، مزیتی کلیدی در برابر دکتترین متمرکز روسیه بود (Pinko, 2023: 63). این یافته تأییدی بر دیدگاه نئوکلاسیک رئالیستی است که بر اهمیت ظرفیت‌های واحد-سطحی در تبدیل فشارهای ساختاری به سیاست‌های عملیاتی تأکید دارد.

پ- هم‌افزایی مادی- معنایی در جنگ‌های ترکیبی

حملات سایبری علیه زیرساخت‌های حیاتی، وقتی با عملیات روانی، اطلاعات غلط و روایت‌های ایدئولوژیک همراه شدند، قدرت تخریبی دوچندانی یافتند. روسیه کوشید از روایت «نازی‌زدایی» برای مشروعیت‌بخشی به تهاجم خود بهره گیرد (Aleksejeva, 2023: 5-6). در حالی که اوکراین با کمک الگوریتم‌های هوش مصنوعی در مدیریت افکار عمومی جهانی، توانست روایت «مدافع دموکراسی» را تثبیت کند (Slusher, 2025: 27). این هم‌افزایی مادی- معنایی نشان می‌دهد که جنگ‌های ترکیبی در عصر هوش مصنوعی نه تنها بر زیرساخت‌ها، بلکه بر ذهن و هویت جوامع نیز متمرکز هستند (Thornton & Miron, 2022: 118-120).

ت- بازتعریف بازدارندگی و مشروعیت بین‌المللی

جنگ اوکراین ثابت کرد که بازدارندگی صرفاً متکی بر قدرت نظامی متعارف نیست، بلکه به ظرفیت دفاع سایبری، روایت‌سازی دیجیتال و بسیج حمایت بین‌المللی وابسته است. در این میان استفاده گسترده از نیروهای سایبری غیردولتی و داوطلب توسط اوکراین (و هم‌پیمانانش)، هرچند کارایی عملیاتی داشت، اما مرز میان جنگ و صلح و همچنین مسئولیت‌پذیری دولت‌ها در قبال اقدامات پروکسی‌ها را مخدوش کرد. این وضعیت نه تنها به تشدید معمای امنیت انجامید (در چارچوب واقع‌گرایی نئوکلاسیک)، بلکه هنجارهای حاکم بر مشروعیت در فضای سایبری را نیز به چالش کشید (Foca, 2024: 261-262). جنگ اوکراین به‌عنوان نخستین آزمایش میدانی گسترده از تلفیق هوش مصنوعی با جنگ‌های ترکیبی، تصویری روشن از آینده امنیت بین‌المللی ترسیم کرد. درس‌های این جنگ، هم در سطح نظری- با تشدید معمای امنیت و بازتعریف هنجارها- و هم در سطح عملی- با برجسته ساختن اهمیت انعطاف‌پذیری سازمانی و هم‌افزایی مادی-معنایی- پیامدهای عمیقی دارد. خاورمیانه با توجه به ماهیت نظام‌های متخاصم، حضور پررنگ بازیگران غیردولتی، و سابقه تاریخی رقابت‌های تسلیحاتی به‌ویژه مستعد بازتولید و حتی

تشدید این الگوهاست. از این منظر، تجربه اوکراین نه صرفاً یک مطالعه موردی، بلکه هشدار راهبردی برای امنیت آینده خاورمیانه محسوب می‌شود.

تطبیق با خاورمیانه: تهدیدها و فرصت‌ها

تحلیل مقایسه‌ای پنج بازیگر اصلی خاورمیانه نشان می‌دهد که منطقه وارد مرحله‌ای از رقابت فناورانه چندلایه شده است که در آن هوش مصنوعی نه تنها ابزار نظامی، بلکه عامل بازتعریف بازدارندگی، مشروعیت و هویت امنیتی دولت‌ها به شمار می‌آید. تجربه جنگ اوکراین به‌ویژه در زمینه تسریع چرخه تصمیم‌گیری-اقدام و نقش هوش مصنوعی در تشدید معمای امنیت سایبری، الگویی ارزشمند برای تحلیل تحولات منطقه‌ای فراهم کرده است (Omer, 2025: 3).

الف- ایران: تمرکز بر بومی‌سازی و بازدارندگی نامتقارن

از منظر واقع‌گرایی نئوکلاسیک، تمرکز بالای تصمیم‌گیری و ساختارهای امنیتی متمرکز، ضمن افزایش کنترل، انعطاف‌پذیری عملیاتی را کاهش می‌دهد (Hogeveen, 2024: 15). الگوی تصمیم‌گیری متمرکز بر پایه توانمندی‌های بومی ایران مشابه الگوی روسیه در جنگ اوکراین، می‌تواند موجب کندی در واکنش به تهدیدات پویا شود و در نهایت، معمای امنیت سایبری را از طریق افزایش سوءظن تشدید کند. لذا جایگزینی راهبرد بازدارندگی نامتقارن مورد توجه و تأکید ایران بوده است (Hogeveen, 2024: 16).

ب- اسرائیل: برتری فناورانه و تشدید معمای امنیت منطقه‌ای

تسریع چرخه تصمیم‌گیری-اقدام توسط اسرائیل (Cohen, 2024: 120)، ضمن افزایش کارایی رزمی، وسوسه اقدام پیش‌دستانه را تقویت کرده و باعث می‌شود بازیگران رقیب برای جبران نابرابری، به تاکتیک‌های نامتقارن روی آورند (Hitman, 2024: 36). این فرایند، مصداق روشن تشدید معمای امنیت در فضای سایبری خاورمیانه است. در سطح سازه‌نگارانه نیز اسرائیل با برجسته‌سازی روایت «برتری فناورانه»، از هوش مصنوعی به‌عنوان ابزاری برای تثبیت هویت خود به‌عنوان «قدرت هوشمند منطقه‌ای» بهره می‌گیرد.

پ- عربستان سعودی: نوسازی با اتکای مالی و وابستگی فناورانه

دولت ریاض در راستای سند چشم‌انداز ۲۰۳۰، هوش مصنوعی را محور بازسازی ساختار دفاعی خود قرار داده و در این زمینه ۱۰۰ میلیارد دلار سرمایه‌گذاری کرده و همچنین برنامه‌ریزی برای اختصاص ۴۰ میلیارد دلار اضافی برای سرمایه‌گذاری در شرکت‌های هوش مصنوعی را اعلام نموده است (Omer, 2025: 6). با این حال از دیدگاه واقع‌گرایی نئوکلاسیک، عربستان هنوز به شدت به فناوری خارجی وابسته است و این وابستگی می‌تواند به آسیب‌پذیری ساختاری تبدیل شود. این کشور در تلاش است تا مدل دفاع غیرمتمرکز با مشارکت بخش خصوصی و دانشگاهی ایجاد کند.

ت- ترکیه: بازیگر میانی با چرخه تصمیم‌گیری سریع و تاثیرگذار

توسعه پهپادهای بیرق‌دار تی‌بی-۲ و کارگو-۲ باعث فشرده‌سازی قابل توجه تسريع چرخه تصمیم‌گیری یا اقدام در نیروهای مسلح ترکیه شده است (Omer, 2025: 8). این برتری فناورانه می‌تواند از دید رقبا تهدیدزا تعبیر شده و به شکل‌گیری پویایی‌های جدید معمای امنیتی در شرق مدیترانه بینجامد. ترکیه الگوی نیمه‌متمرکز نوآوری دفاعی را دنبال می‌کند که تلفیقی از خودکفایی فناورانه و کنترل سیاسی است (Kurç, 2025: 392).

ث- امارات متحده عربی: از واردکننده فناوری تا قدرت داده‌محور

امارات متحده عربی با دریافت سرمایه‌گذاری ۱.۵ میلیارد دلاری مایکروسافت در حوزه هوش مصنوعی، خود را به عنوان قطب پذیرش فناوری‌های دفاعی مبتنی بر هوش مصنوعی معرفی کرده است. امارات با پروژه‌های بزرگی چون «استارگیت» به یکی از پیشروترین مراکز فناوری هوش مصنوعی در منطقه تبدیل شده است (Omer, 2025: 7). در سطح معنایی (سازه‌نگاری)، امارات از فناوری هوش مصنوعی برای تقویت روایت «نوآوری صلح‌محور» در سیاست خارجی خود بهره می‌گیرد و آن را ابزاری برای قدرت نرم و مشروعیت بین‌المللی می‌داند (Arafeh, 2025). این رویکرد در تقابل با اسرائیل است که

1. Bayraktar TB2

2. Kargu-2

هوش مصنوعی را در خدمت دکترین بازدارندگی سخت خود و افزایش کارایی عملیاتی نظامی تعریف کرده است.

در یک جمع‌بندی تطبیقی الگوی رقابت فناورانه در خاورمیانه در سه سطح قابل تحلیل است: مدل متمرکز اقتدارگرایانه (ایران و عربستان)، مدل فناورانه غیرمتمرکز و شبکه‌ای (اسرائیل و امارات) و مدل میانه تطبیقی (ترکیه). موفق‌ترین بازیگران آینده، آن‌هایی خواهند بود که بتوانند نوآوری فناورانه را با سازگاری سازمانی و روایت‌سازی هوشمند پیوند دهند. این پویایی‌ها، زمینه‌ساز ورود به مرحله بعدی تحلیل یعنی تحلیل تهدیدها در پرتو درس‌های اوکراین است.

تحلیل تهدیدها در پرتو درس‌های اوکراین

تجربه جنگ اوکراین نشان داد که هوش مصنوعی، تهدیدهایی بنیادین را در ابعاد امنیت سایبری، بازدارندگی منطقه‌ای و ثبات راهبردی ایجاد می‌کند.

* تشدید معمای امنیت سایبری در سطح منطقه‌ای

هوش مصنوعی در محیط راهبردی خاورمیانه همانند اوکراین، به‌عنوان تسریع‌کننده معمای امنیت عمل می‌کند. کوتاه‌سازی و چرخه تصمیم‌گیری سریع و تأثیرگذار، از دید رقابتی منطقه‌ای تهدیدی بالقوه تلقی می‌شود و آنان را به اتخاذ راهبردهای نامتقارن سوق می‌دهد. در چارچوب واقع‌گرایی نئوکلاسیک، چنین پویایی‌هایی منجر به افزایش احتمال سوءبرداشت و اقدام پیش‌دستانه متقابل می‌شود؛ زیرا بازیگران منطقه‌ای در شرایط فشار ادراکی، تهدیدها را بیش از واقع برآورد می‌کنند (Hogeveen, 2024: 16).

* آسیب‌پذیری زیرساخت‌های حیاتی و بازتعریف مفهوم جبهه

حملات سایبری روسیه علیه شبکه‌های انرژی و ارتباطات اوکراین، بازتعریف مفهوم جبهه را به دنبال داشت (Thornton & Miron, 2022: 119). کشورهای منطقه به‌ویژه در حوزه امنیت انرژی و زیرساخت‌های دیجیتال، با خطر بالای حملات مبتنی بر هوش مصنوعی روبه‌رو هستند. وابستگی روزافزون به شبکه‌های داده‌ای بین‌المللی، خود نوعی

آسیب‌پذیری ساختاری ایجاد کرده است (Omer, 2025: 6). الگوی حملات روسیه به سامانه استارلینک در اوکراین نمونه‌ای هشداردهنده برای کشورهایی است که زیرساخت‌های فرماندهی و کنترل خود را به پلتفرم‌های ابری واگذار کرده‌اند (Slusher et al., 2025: 27).

* رقابت تسلیحاتی سایبری و مبهم شدن مرز جنگ و صلح

افزایش نقش «فضای خاکستری» میان جنگ و صلح در اوکراین در خاورمیانه نیز احتمال تشدید رقابت‌ها را افزایش داده است. ترکیب هوش مصنوعی با سامانه‌های تسلیحاتی خودمختار، می‌تواند منجر به بروز «رقابت تسلیحاتی بدون ترمز» شود (Foca, 2024: 262). از منظر سازه‌انگاری، رقابت بر سر روایت «برتری فناورانه» با عملیات اطلاعاتی و دیپ‌فیک‌های مبتنی بر هوش مصنوعی، می‌تواند منجر به بحران اعتماد عمومی و تضعیف مشروعیت سیاسی دولت‌ها شود (Cohen, 2024: 120).

در یک جمع‌بندی می‌توان گفت که تهدیدات نوین خاورمیانه در عصر هوش مصنوعی، سه ویژگی اصلی دارند: اول، تسریع تصمیم‌گیری و تشدید واکنش پیش‌دستانه؛ دوم، گسترش دامنه جبهه‌ها به زیرساخت‌های غیرنظامی و سوم، افزایش ابهام در تمایز میان جنگ و صلح. این سه روند، تصویر روشنی از «خاورمیانه پسا هوش مصنوعی» ارائه می‌دهند.

سناریوهای آینده

طبق سناریوی اول، اوکراینی‌سازی شدید و معمای امنیت فناورانه خاورمیانه وارد مرحله‌ای از رقابت تسلیحاتی فناورانه می‌شود که مشابه الگوی جنگ اوکراین است (Sarkin & Sotoudehfar, 2024: 8). این تحول منجر به چرخه تصمیم‌گیری سریع و تأثیرگذار و تشدید «معمای امنیت فناورانه» می‌شود. شتاب فناورانه بدون وجود سازوکارهای اعتماد متقابل، احتمال اشتباه محاسباتی در رقابت میان بازیگران اصلی را چندبرابر می‌کند. بر اساس سناریوی دوم، بی‌ثباتی از درون و جنگ روایت‌ها فضای رقابت از میدان نظامی به عرصه روانی و روایتی منتقل می‌شود. بازیگران منطقه‌ای از هوش مصنوعی برای

تولید محتوای جعلی و عملیات روانی علیه گروه‌های اجتماعی هدف استفاده می‌کنند (UNIDIR, 2024: 12). به تعبیر سازه‌انگاران، این پدیده نوعی «جنگ بر سر معنا» است (Wendt, 1999: 254). در چنین محیطی، اعتماد اجتماعی و انسجام داخلی کشورها به هدف اصلی حملات سایبری تبدیل می‌شود.

مطابق سناریوی سوم، بازدارندگی شکننده و مهارشده رقابت فناورانه وجود دارد اما توسط ترس از هزینه‌های تصاعدی و سازوکارهای غیررسمی مهار می‌شود (Sarkin & Sotoudehfar, 2024: 13). دولت‌های منطقه‌ای به درک این نکته می‌رسند که حمله به زیرساخت‌های حیاتی سایبری می‌تواند واکنش زنجیره‌ای غیرقابل کنترل را به همراه داشته باشد. مکانیسم‌های اعتمادسازی و تبادل اطلاعات تهدید میان قدرت‌های منطقه‌ای، عامل کلیدی در جلوگیری از تشدید درگیری است.

نتیجه‌گیری

این پژوهش با هدف تحلیل نقش راهبردی یگان‌های سایبری مجهز به هوش مصنوعی در دگرگونی معادلات نظامی و استخراج درس‌های استراتژیک از تجربه جنگ اوکراین برای امنیت خاورمیانه انجام شد. این پژوهش با پر کردن خلأ موجود در ادبیات که عمدتاً بر ابعاد صرفاً تکنیکی هوش مصنوعی متمرکز بود، نشان داد که برتری راهبردی نوآورانه در گرو تلفیق نوآوری فناورانه با انعطاف‌پذیری نهادی و مدیریت هوشمندانه روایت‌ها است. تحلیل‌ها نشان داد که ظهور هوش مصنوعی در فضای سایبری صرفاً یک تحول تکنولوژیک نیست، بلکه یک «انقلاب در امور نظامی» است که به طور هم‌زمان ابعاد مادی (رقابت سخت‌افزاری) و معنایی (جنگ روایت‌ها) در جنگ‌های ترکیبی را دگرگون ساخته است. چارچوب نظری تلفیقی مقاله - ترکیب واقع‌گرایی نئوکلاسیک و سازه‌انگاری - توانست این دگرگونی چندبعدی را به طور منسجم تبیین کند.

یافته‌های این پژوهش بر پایه مطالعه موردی جنگ اوکراین، سه نتیجه اساسی را برجسته می‌سازد: اول، تشدید معمای امنیت فناورانه؛ هوش مصنوعی به عنوان یک «تسریع‌کننده راهبردی» با فشردن چرخه شناسایی-تصمیم‌گیری-عمل، فرصت پاسخ‌دهی دولت‌ها را کاهش داده و معمای امنیت را در فضای سایبری تشدید کرده است. این پدیده

اعتبار واقع‌گرایی نئوکلاسیک در تبیین رقابت‌های فناورانه در سطح واحد - سطحی را تأیید می‌کند.

دوم، اهمیت سازگاری سازمانی بر انباشت سخت‌افزار: موفقیت نسبی اوکراین در دفاع سایبری ناشی از انعطاف‌پذیری سازمانی، مدل غیرمتمرکز فرماندهی و ادغام سریع ظرفیت‌های بخش خصوصی و داوطلبان بود. در مقابل، همین مدل غیرمتمرکز در مراحل بعدی جنگ با چالش‌هایی چون فرسایش نیروهای داوطلب، دشواری هماهنگی میان واحدهای مستقل و آسیب‌پذیری در برابر حملات هدفمند روسیه به زیرساخت‌های ارتباطی روبه‌رو شد؛ واقعیتهایی که نشان می‌دهد انعطاف‌پذیری سازمانی نیازمند توازن میان تمرکز و چابکی است.

سوم، هم‌افزایی مادی-معنایی و فرسایش بازدارندگی کلاسیک: جبهه سایبری جنگ اوکراین ترکیبی از حملات زیرساختی و عملیات‌های شناختی مبتنی بر هوش مصنوعی است (مانند تولید انبوه دیپ‌فیک‌ها). این پدیده نشان داد که نبرد برای تسلط بر «روایت‌ها» و «ادراکات جمعی» به اندازه نبرد بر سر زیرساخت‌ها اهمیت دارد؛ پدیده‌ای که سازه‌نگاری به‌خوبی آن را توضیح می‌دهد و زمینه‌ساز شکل‌گیری نوعی بازدارندگی شناختی^۱ است؛ یعنی توانایی مهار تهاجمات سایبری-روانی که هدف آن تضعیف اراده عمومی و مشروعیت سیاسی است.

تطبیق درس‌های اوکراین با محیط امنیتی خاورمیانه نشان می‌دهد که منطقه وارد فاز جدیدی از رقابت فناورانه شده است که می‌تواند به «اوکراینی‌سازی امنیتی» یا فرسایش درونی دولت‌ها منجر شود: رقابت میان بازیگران کلیدی مانند ایران، اسرائیل و ترکیه در توسعه سامانه‌های تصمیم‌یار مبتنی بر هوش مصنوعی، چرخه تصمیم‌گیری را کوتاه‌تر کرده و احتمال اقدام پیش‌دستانه و سوءمحاسبه را افزایش می‌دهد. اتکای فزاینده کشورها به زیرساخت‌های دیجیتال، آن‌ها را به اهدافی جذاب برای حملات سایبری هوش مصنوعی‌محور تبدیل کرده و در عین حال جنگ‌های شناختی، تهدیدی مستقیم برای انسجام اجتماعی و مشروعیت دولت‌ها پدید آورده است.

1. Cognitive Deterrence

در مجموع، این پژوهش نشان می‌دهد که آینده امنیت خاورمیانه نه در قدرت مطلق نظامی، بلکه در توانایی دولت‌ها برای مدیریت هوشمندانه تعامل میان فناوری، سازمان و روایت‌های هویتی در عصر الگوریتم‌ها نهفته است. توصیه‌های سیاستی بر اساس سطوح مختلف تحلیل به این شرح پیشنهاد می‌گردد: در سطح ملی، اولویت‌بندی تاب‌آوری سازمانی و دفاع شبکه‌ای از طریق اصلاح ساختارهای متمرکز، ارتقای همکاری میان بخش خصوصی - دانشگاهی و تشکیل واحدهای ترکیبی انسانی - هوش مصنوعی در نیروهای مسلح توصیه می‌شود. در سطح تعاملی / منطقه‌ای، ایجاد سازوکارهای اعتماد سایبری منطقه‌ای برای تبادل اطلاعات تهدیدات، هماهنگی واکنش‌های اضطراری و تنظیم محدودیت‌های استفاده از سامانه‌های هوش مصنوعی تهاجمی مورد تاکید قرار می‌گیرد و در سطح هنجاری / ساختاری، تدوین هنجارهای منطقه‌ای در فضای خاکستری و ایجاد رژیم‌های بازدارندگی شناختی برای جلوگیری از گسترش عملیات روانی مبتنی بر الگوریتم‌ها و دیپ‌فیک‌ها پیشنهاد می‌شود.

تعارض منافع

تعارض منافع ندارم.

ORCID

Mehdi Abbaszadeh



<https://orcid.org/0000-0003-1893-2132>

Fathabadi

Mosayyeb Rostami



<https://orcid.org/0009-0009-8184-8014>

Khanmakani

منابع

- پیرمحمدی، سعید، هدایتی شهیدانی، مهدی، نیاکویی، سیدامیر، (۱۴۰۴)، «رقابت آمریکا و چین در حوزه هوش مصنوعی؛ از ملی‌گرایی فنی تا جغرافیای سیاسی فنی»، *نشریه مطالعات کشورها*، دوره ۳، شماره ۱، ۳۸۱۳۹۲.۱۱۵۴، <https://doi.org/10.22059/jcountst.2024.381392.1154>.

- ترکی، هادی، (۱۴۰۳)، «رهیافت جدید قدرت مبتنی بر هوش مصنوعی؛ مطالعه موردی رقابت آمریکا و چین از ۲۰۱۰ تا ۲۰۲۳»، *مطالعات راهبردی آمریکا*، دوره ۴، شماره ۲، <https://doi.org/10.47176/asr.2024.1206>.
- شکوهی، سعید و کریمی پرشه، سجاده، (۱۴۰۲)، «جنگ هیبریدی روسیه در منازعه ۲۰۲۲ اوکراین»، *پژوهش‌های روابط بین‌الملل*، دوره ۱۳، شماره ۲، <http://doi.org/10.22034/irr.2023.400126.2390>.
- دهقانی فیروزآبادی، سیدجلال، چهرآزاد، سعید، (۱۴۰۲)، «هوش مصنوعی و مسئله‌دار کردن درون مایه‌های امنیت ملی»، *پژوهش‌های راهبردی سیاست*، دوره ۱۲، شماره ۴۶، <doi:10.22054/QPSS.2022.70690.3130>.
- عباس‌زاده فتح‌آبادی، مهدی، رستمی خانمکانی، مصیب، (۱۴۰۴)، «ابعاد مادی و غیرمادی ژئوپلیتیک نوین هوش مصنوعی: پویایی‌های رقابت آمریکا و چین»، *رهیافت‌های سیاسی و بین‌المللی*، دوره ۱۷، شماره ۳، <https://doi.org/10.48308/piaj.2025.240434.1712>.
- محمدی منفرد، حسن، تقی‌پور جاوی، تیرداد، (۱۴۰۳)، «نقش فناوری هوش مصنوعی در دگرگونی ماهیت جنگ: براساس مطالعه اسناد راهبردی رژیم صهیونیستی»، *فصلنامه مطالعات بنیادین و کاربردی جهان اسلام*، دوره ۶، شماره ۴، <https://doi.org/10.22034/fasiw.2025.483659.1394>.
- میراحمدی، سعید، امیدی، علی، (۱۴۰۳)، «کاربرد هوش مصنوعی در تصمیم‌گیری سیاست خارجی؛ ظرفیت‌ها و چالش‌ها»، *پژوهش‌های راهبردی سیاست*، دوره ۱۳، شماره ۵۰، [doi: 10.22054/qps.2024.75471.3301](doi:10.22054/qps.2024.75471.3301).
- نوروزی، پژمان؛ هلال‌ات، عماد و مقومی، امیررضا، (۱۴۰۱)، «واکاوی جنگ روسیه و اوکراین از منظر امنیت هستی‌شناختی»، *مطالعات آسیای مرکزی و قفقاز*، دوره ۲۸، شماره ۱۲۰، <https://doi.org/703164>.

References

- Aleksejeva, Liva, (2023), "Russian Disinformation Narratives on Ukraine", *NATO StratCom Centre of Excellence*, [https:// www.stratcomcoe.org](https://www.stratcomcoe.org).
- Arafah, Nur, (2025), "The Promise and Risks of Artificial Intelligence: Uneven Investment in the Technology Will Widen Regional Inequalities in the Middle East and North Africa", *Carnegie Endowment for*

International Peace, <https://carnegieendowment.org/middle-east/diwan/2025/09/the-promise-and-risks-of-artificial-intelligence?lang=en>.

- Cohen, David, (2024), *Israel and the Algorithmic Battlefield*, Tel Aviv University Press.
- Devanny, Joe, (2024), “Artificial Intelligence and Cyber Power (Research Publications No. 63)”, Jack D. Gordon Institute for Public Policy, Florida International University, available at: https://digitalcommons.fiu.edu/jgi_research/63.
- Foca, Andreea Cosmina, (2024), “The Impact of the Ukrainian-Russian War on European Cyber Security”, *EURINT*, Vol. 11, No. 2 259–270, <https://doi.org/10.47743/eurint-2024-FOC>.
- Grzegorzewski, Mark; Smith, Margaret & Koven, Barnett, (2022), “Civil Cyber Defense: A New Model for Cyber Civic Engagement”, *The Cyber Defense Review*, Vol. 7, No. 3, <http://www.jstor.org/stable/48755361>.
- Hitman, Gadi, (2024), “What Went Wrong: Israeli Misconceptions and the October 2023 Surprise”, *Middle East Policy*, Vol. 31, No. 2. <https://doi.org/10.1111/mepo.12762>.
- Hogeveen, Bart, (2024), “The Silent Siege: Cyber-enabled IP Theft in the Foreign Interference Landscape”, In N. Kovalčíková (Ed.), *Hacking Minds and Machines: Foreign Interference in the Digital Era* (pp. 13–26), European Union Institute for Security Studies (EUISS).
- Kaushik, Akanksha, (2023), “Ukraine's Cyber Defence: Insights on Private Sector Contributions Since the Russian Invasion (Policy Brief)”, *GLOBSEC*, available at: <https://www.globsec.org/sites/default/files/2023>.
- Kozub-Karkut, Magdalena, (2019), “Neoclassical Realism and Foreign Policy Analysis – A Possible Way of Integration”, *Teoria Polityki*, Vol. 3, No. 1, 201–227, <https://doi.org/10.4467/25440845TP.19.011.10294>.
- Kurç, Caglar, (2025), “Balancing Aspiration and Reality: Autarky in Turkish Defence Industrialisation”, *Journal of Defence Studies*, Vol. 12, No. 2, 134–145, <https://doi.org/10.1080/14702436.2025.2472705>.

- Lobell, Steven; Ripsman, Norrin M & Taliaferro, Jeffery, (2009), *Neoclassical Realism, the State, and Foreign Policy*, Cambridge University Press.
- Meibauer, Gostav et al., (2021), “Rethinking Neoclassical Realism at Theory’s End”, *International Studies Review*, Vol. 23, No. 1, 268–295. <https://doi.org/10.1093/isr/viaa018>.
- Nye, Joseph. , (2014), *The Regime Complex for Managing Global Cyber Activities*, Centre for International Governance Innovation and Chatham House, [https:// www. cigionline. org/ publications/regime-complex-managing-global-cyber-activities](https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities).
- Nye, Joseph, (2010), *Cyber Power*, *Belfer Center for Science and International Affairs*, Harvard Kennedy School.
- Omer, Nur, (2025), “AI as a Force Multiplier in the Middle East Defense Systems”, *INNOV8 Research Center*, available at: <https://innov8.krd/wp-content/uploads/2025/05/AI-AS-A-FORCE-MULTIPLIER-IN-THE-MIDDLE-EAST-DEFENSE-SYSTEMS.pdf>.
- Pinko, Eyal, (2023), “The Cyber Domain in the Russo-Ukrainian War”, *BESA Center Perspectives Paper*, Vol. 1, No. 2, 203. [https:// www.researchgate. net/ publication/372344739](https://www.researchgate.net/publication/372344739).
- Ripsman, Norrin; Taliaferro, Jeffrey & Lobell, Steven, (2016), *Neoclassical Realist Theory of International Politics*, Oxford University Press.
- Sarkin, Jeremy. Julian & Sotoudehfar, S, (2024), “Artificial Intelligence and Arms Races in the Middle East”, *Defense & Security Analysis*, Vol. 40, No. 2, 1–17, <https://doi.org/10.1080/14751798.2024.2302699>.
- Slusher, Matt et al., (2025), *Space and Data Domain Lessons from Russia-Ukraine, In Conflict in Focus: Lessons from Russia-Ukraine*, (Episode Summaries, pp. 26–27), Center for Strategic and International Studies (CSIS). <https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience>.
- Thornton, Rod & Miron, Marina, (2022), “Winning Future Wars: Russian Offensive Cyber and its Vital Importance in Moscow’s Strategic

Thinking”, *The Cyber Defense Review*, Vol. 7, No. 3, [https:// doi. org/ 10.2307/48687352](https://doi.org/10.2307/48687352).

- United Nations Human Rights Monitoring Mission in Ukraine, (2024), “Attacks On Ukraine's Electricity Infrastructure Threaten Key Aspects of Life as Winter Approaches – UN Human Rights Monitors Say United Nations in Ukraine”, available at: <https://ukraine.un.org/en/278995-attacks-ukraine%E2%80%99s-electricity-infrastructure-threaten-key-aspects-life-winter-approaches-%E2%80%93>.
- United Nations Institute for Disarmament Research (UNIDIR), (2024), “The Impact of Artificial Intelligence on Regional Security Threat Perceptions and the Middle East WMD-free Zone”, available at: <https://unidir.org/publication/the-impact-of-artificial-intelligence-on-regional-security-threat-perceptions-and-the-middle-east-wmd-free-zone>.
- Valeriano, Brandon & Maness, Ryan, (2015), *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*, Oxford University Press.
- Wang, Peng; Zhang, Hu & Zhang, Ke, (2024), “Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security”, *CSIS Interpret: China*, available at: <https://interpret.csis.org/translations/starlink-militarization-challenges-and-responses-to-space-intelligence-and-information-security>.
- Wendt, Alexander, (1999), *Social Theory of International Politics*, Cambridge University Press.

In Persian

- Pirmohammadi, Saeed; Hedayati Shahidani, Mehdi & Niakoui, Seydamir, (2025), "US-China Competition in the Field of Artificial Intelligence; From Technical Nationalism to Technical Geopolitics", *Journal of Country Studies*, Vol. 3, No. 1, [https:// doi.org/ 10.22059/ jcountst.2024.381392.1154](https://doi.org/10.22059/jcountst.2024.381392.1154). [In Persian]
- Turki, Hadi, (1403), "A New Power Approach Based on Artificial Intelligence; A Case Study of US-China Competition from 2010 to 2023", *American Strategic Studies*, Vol. 4, No. 2. [https:// doi.org/ 10.47176/asr.2024.1206](https://doi.org/10.47176/asr.2024.1206). [In Persian]

- Shokoohi, Saeed & Karimi Parsheh, Sajjad, (1402), "Russia's Hybrid War in the 2022 Ukraine Conflict", *International Relations Research*, Vol. 13, No. 2, <http://doi.org/10.22034/irr.2023.400126.2390>. [In Persian]
- Dehghani Firouzabadi, Seyed Jalal & Chehrazad, Saeed, (1402), "Artificial Intelligence and Problematizing National Security Themes", *Quarterly of Political Strategic Studies*, Vol. 12, No. 46. doi:10.22054/ QPSS.2022. 70690.3130. [In Persian]
- Abbaszadeh Fathabadi, Mehdi & Rostami Khanmakani, Mosayeb, (1404), "Material and Non-Material Dimensions of the New Geopolitics of Artificial Intelligence: Dynamics of US-China Competition", *Political and International Approaches*, Vol. 17, No. 3, <https://doi.org/10.48308/piaj.2025.240434>. 1712. [In Persian]
- Mohammadi Monfared, Hassan & Taghipour Javi, Tirdad, (1403), "The Role of Artificial Intelligence Technology in Changing the Nature of War: Based on a Study of the Strategic Documents of the Zionist Regime", *Quarterly Journal of Fundamental and Applied Studies of the Islamic World*, Vol. 4, No. 22. <https://doi.org/10.22034/fasiw.2025.483659.1394>. [In Persian]
- Mirahmadi, Saeed & Omid, Ali, (1403), "The Application of Artificial Intelligence in Foreign Policy Decision-Making; Capacities and Challenges", *Quarterly of Political Strategic Studies*, Vol. 13, No. 50. doi: 10.22054/qps.2024.75471.3301. [In Persian]
- Norouzi, Pejman; Hilalat, Emad & Moghumi, Amirreza, (1401), "Analysis of the Russia-Ukraine War from the Perspective of Ontological Security", *Central Asian and Caucasus Studies*, Vol. 28, No. 120. [In Persian]

استناد به این مقاله: عباس‌زاده فتح‌آبادی، مهدی و رستمی خانمکانی، مصیب، (۱۴۰۵)، «تحلیل نقش یگان‌های سایبری مجهز به هوش مصنوعی در تغییر معادلات نظامی: مطالعه موردی جنگ اوکراین و درس‌های آن برای امنیت خاورمیانه»، *پژوهش‌های راهبردی سیاست*، دوره ۱۵، شماره ۵۸، ۲۱۳-۲۴۶.

Doi: 10.22054/qps.2026.89724.3713



Quarterly of Political Strategic Studies is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License