Political and International Approaches
Vol 18, No 2, 2026, PP 162-186
Journal Homepage: piaj.sbu.ac.ir
P-ISSN: 1735-739X
E-ISSN: 2645-4386

The Role of Technological Deterrence in the Efficacy of Russia's Networked Weapons Architecture: A Case Study of the Ukraine War

Fatemeh Mahrough[1] & Mohammad Amir Rezai[2]

DOI: 10.48308/piaj.2026.244357.1889 Received: 2026/1/27 Accepted: 2026/6/21

Original Article

Extended Abstract

Introduction: Since the end of the Cold War, the convergence of technological innovation and geopolitical transformation has fundamentally altered the foundations of classical deterrence theory. The transition from a deterrence logic based on arms accumulation and material hard power toward network-centric architectures and algorithmic governance signals a new era of military strategy. In this regard, the Ukraine war transcended its regional boundaries to become a critical laboratory for assessing the efficacy of integrating non-human technologies and artificial intelligence on the battlefield. The central research question asks: How has the integration of AI into Russia's networked weaponry architecture upgraded its technological deterrence capability during the Ukraine war? This study aims to explain Russia's transition from traditional, mass-based deterrence to data-driven deterrence, while identifying both the strategic strengths and systemic vulnerabilities of this emerging architecture.

Methods: This research employs a qualitative approach grounded in the Layered Analysis of Technological Deterrence framework. Data were collected through library and documentary methods at two operational levels: first, by coding official defense doctrines, think-tank reports, and field evidence from the Ukraine conflict; second, through comparative analysis of Russia's network-centric configurations, including missile defense architecture and sensor-to-shooter networks. John Boyd's (OODA) loop model was applied to assess operational processes. Thematic analysis, combined with data-command relationship mapping, enabled evaluation of causal links and the sustaina-

1. Assistant Professor of International Relations, Department of political science, Faculty of Law and Political science, Ferdowsi University of Mashhad, Mashhad, Iran (Corresponding Author). fmahroogh@um.ac.ir
2. MA student in International Relations, Department of political science, Faculty of Law and Political science, Ferdowsi University of Mashhad, Mashhad, Iran. Rezai.mohammaamir@mail.um.ac.ir

Political and International Approaches
Vol 18, No 2, 2026, PP 162-186
Journal Homepage: piaj.sbu.ac.ir
P-ISSN: 1735-739X
E-ISSN: 2645-4386

bility of technological advantages in high-intensity combat environments.
Results and discussions: By intertwining weapons systems engineering with AI, Russia has operationalized a new paradigm of military intelligence that, rather than mimicking human cognition, leverages raw computational power for predictive modeling and preemptive action. Technical examinations reveal that this networked architecture integrates smart defensive and offensive systems—such as the S-500 air defense system, 9M729 cruise missiles, and the Avangard hypersonic glide vehicle—with advanced surveillance and processing networks, including Orlan UAVs and the SORM data collection infrastructure. Within this matrix, multi-source sensor data (from satellites to land-based radars) is aggregated and piped directly into the fire chain via real-time processing loops within C4ISR systems. This integrated ecosystem transfers tactical initiative to the network, compressing the classical decision-to-action cycle from hours to minutes. The study reveals a direct correlation between the capacity to indigenize AI in military infrastructure and enhanced multi-domain reaction capabilities, effectively allowing defensive systems to optimize offensive operations. this extreme complexity and network dependency introduce significant systemic vulnerabilities, particularly regarding data corruption, cyber leaks, and electronic warfare countermeasures.
Conclusion: Russia has shifted the tactical and operational balance of power in its favor by transitioning from purely nuclear deterrence toward algorithmic battlefield superiority. The Active Multi-Domain Deterrence model shows that 21st-century security depends far more on proficiency in integrated network design and hostile-environment data management than on hardware accumulation. Nevertheless, the Ukraine war demonstrates that over-reliance on technology without rigorous information hardening and realistic assessment of supply chain limitations can induce strategic vulnerability. The theoretical implication for International Relations literature is the urgent necessity of revising classical deterrence theories to accommodate human–machine–data hybrid models, while offering defense policymakers a template for asymmetric deterrence through the cognitive upgrading of conventional weapons.
Keywords: Technological Deterrence, Russia-Ukraine War, Artificial Intelligence, Network-Centric Architecture, Multi-Domain Warfare.

Citation: Mahrough, Fatemeh & Rezai, Mohammad Amir. 2026. The Role of Technological Deterrence in the Efficacy of Russia's Networked Weapons Architecture: A Case Study of the Ukraine War, Political and International Approaches, Summer, Vol 18, No 2, PP 162-186.

دانشگاه شهید بهشتی ۱۳۳۸

رهیافت‌های سیاسی و بین‌المللی

دورهٔ هجدهم، شمارهٔ دوم، تابستان ۱۴۰۵، ۱۸۶-۱۶۲

سایت مجله: piaj.sbu.ac.ir

P-ISSN: 1735-739X

E-ISSN: 2645-4386

نقش بازدارندگی فناورانه در کارآمدی معماری شبکه‌ای تسلیحات روسیه: مطالعه موردی جنگ اوکراین

فاطمه محروق[۱] و محمد امیر رضائی[۲]

تاریخ دریافت: ۱۴۰۴/۱۱/۷ تاریخ پذیرش: ۱۴۰۵/۳/۳۱ DOI: 10.48308/piaj.2026.244357.1889

مقالهٔ پژوهشی

چکیده مبسوط

مقدمه و اهداف: از پایان جنگ سرد تاکنون، هم‌پوشانی میان نوآوری‌های فناورانه و تحولات ژئوپولیتیکی، بنیان‌های فهم کلاسیک «بازدارندگی» را دستخوش دگرگونی کرده است. گذار از منطق بازدارندگی مبتنی بر انباشت تسلیحاتی و قدرت سخت به‌سوی معماری‌های شبکه‌محور و حکمرانی الگوریتمی، نشانگر ورود به عصر نوینی از راهبرد نظامی است. در این راستا، جنگ روسیه و اوکراین فراتر از یک منازعه منطقه‌ای، به آزمونی واقعی برای سنجش کارآمدی ترکیب «فناوری‌های غیرانسانی» و هوش مصنوعی در میدان نبرد تبدیل شده است. مسئله اصلی پژوهش حاضر آن است که یکپارچه‌سازی هوش مصنوعی در معماری شبکه‌ای جنگ‌افزارهای روسیه چگونه موجب ارتقای توان بازدارندگی فناورانه این کشور در جنگ اوکراین شده است؟ هدف این مطالعه، تبیین گذار روسیه از بازدارندگی سنتی به بازدارندگی داده‌محور و شناسایی نقاط قوت و آسیب‌پذیری‌های این معماری نوین است.

روش: این پژوهش با رویکرد «کیفی» و بر اساس مدل مفهومی «تحلیل لایه‌ای بازدارندگی فناورانه» انجام شده است. گردآوری داده‌ها به روش کتابخانه‌ای و اسنادی در دو سطح صورت پذیرفت: نخست، استخراج و کدگذاری داده‌ها از متون رسمی دفاعی، گزارش‌های مراکز مطالعات راهبردی و شواهد میدانی جنگ اوکراین؛ و دوم، تحلیل تطبیقی پیکربندی سامانه‌های شبکه‌محور روسیه با تمرکز بر معماری پدافند موشکی و شبکه‌های سنجش و آتش. به‌منظور تجزیه‌وتحلیل داده‌ها، از مدل چرخه «مشاهده، سمت‌یابی، تصمیم و اقدام» برای بازنمایی فرآیندهای عملیاتی استفاده شد و یافته‌ها با روش تحلیل مضمون و نگاشت روابط داده-فرمان، به الگوی مفهومی بازدارندگی تفسیر گردیدند. این روش امکان ارزیابی پیوندهای علی و سنجش پایداری مزیت فناورانه در محیط‌های جنگی پرشدت را فراهم آورده است.

۱. استادیار روابط بین الملل، گروه علوم سیاسی، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران (نویسنده مسئول). fmahroogh@um.ac.ir

۲. محمدامیر رضایی، کارشناسی ارشد روابط بین الملل، گروه علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران. Rezai.mohammaamir@mail.um.ac.ir

دورهٔ هجدهم، شمارهٔ دوم، تابستان ۱۴۰۵، ۱۸۶-۱۶۲
سایت مجله: piaj.sbu.ac.ir
P-ISSN: 1735-739X
E-ISSN: 2645-4386

یافته ها: روسیه با در هم آمیختن مهندسی شبکه‌های تسلیحاتی و هوش مصنوعی، پارادایم نوینی از هوش نظامی را عملیاتی ساخته که به‌جای تقلید از شناخت انسانی، بر توان محاسباتی جهت «پیش‌بینی و اقدام پیش‌دستانه» استوار است. بررسی‌های نشان می‌دهد که این معماری شبکه‌ای از طریق یکپارچه‌سازی سامانه‌های پدافندی و تهاجمی هوشمند نظیر سامانه «اس-۵۰۰»، موشک‌های «۹ام۷۲۹» و گلایدر فراصوت «آوانگارد» با شبکه‌های نظارت و پردازش شامل پهپادهای «اورلان» و شبکه «سورم» شکل گرفته است؛ ساختاری پیچیده که در آن داده‌های حسگرهای چندمنبعی (از ماهواره تا رادار) پس از تجمیع، از طریق حلقه‌های پردازش بلادرنگ در بستر سامانه‌های فرماندهی و کنترل مستقیماً به زنجیره آتش متصل می‌شوند. استقرار این اکوسیستم یکپارچه، ضمن انتقال ابتکار عمل به شبکه، چرخه کلاسیک تصمیم تا اقدام را از مقیاس زمانی ساعت به دقیقه کاهش داده است. همبستگی مستقیم میان ظرفیت جذب و بومی‌سازی هوش مصنوعی در زیرساخت‌های نظامی با ارتقای توان واکنش چندساحتی روسیه است، به‌گونه‌ای که دفاع عملاً در خدمت تهاجم قرار گرفته است؛ هرچند یافته‌ها نشان می‌دهد که همین پیچیدگی و وابستگی شبکه‌ای، سطحی از آسیب‌پذیری سیستم در برابر نشت داده و تهدیدات جنگ الکترونیک را نیز به همراه داشته است.

نتیجه‌گیری: روسیه توانسته با گذار از بازدارندگی صرفاً هسته‌ای به سوی «برتری میدانی الگوریتمی»، موازنه قوا را در سطوح تاکتیکی و عملیاتی به نفع خود تغییر دهد. مدل «بازدارندگی چنددامنه‌ای فعال» که در این پژوهش تبیین شد، نشان می‌دهد که امنیت و بازدارندگی در قرن بیست‌ویکم بیش از انباشت جنگ‌افزار، به مهارت در طراحی شبکه‌های یکپارچه و مدیریت داده در محیط‌های متخاصم وابسته است. با این وجود، تجربه جنگ اوکراین ثابت کرد که اتکای بیش‌ازحد به فناوری بدون مقاوم‌سازی اطلاعاتی و در نظر گرفتن محدودیت‌های زنجیره تأمین (ناشی از تحریم‌ها)، می‌تواند به «آسیب‌پذیری راهبردی» منجر شود. پیامد نظری این پژوهش برای ادبیات روابط بین‌الملل، ضرورت بازنگری در نظریه‌های بازدارندگی و حرکت به سمت مدل‌های ترکیبی «انسان-ماشین-داده» است. برای سیاست‌گذاران دفاعی، تجربه روسیه الگویی از نحوه دستیابی به بازدارندگی نامتقارن از طریق هوشمندسازی تسلیحات متعارف را ارائه می‌دهد که البته نیازمند حفاظت سایبری مستمر است.

واژگان کلیدی: بازدارندگی فناورانه، جنگ روسیه و اوکراین، هوش مصنوعی، معماری شبکه‌محور، جنگ‌های چنددامنه‌ای.

استناددهی: محروق، فاطمه و رضایی، محمد امیر. ۱۴۰۵. نقش بازدارندگی فناورانه در کارآمدی معماری شبکه‌ای تسلیحات روسیه: مطالعه موردی جنگ اوکراین، رهیافت‌های سیاسی و بین المللی، تابستان، سال ۱۸، شمارهٔ ۲، ۱۸۶-۱۶۲.

مقدمه

در دوران پساجنگ سرد، تقاطع نوآوری‌های فناورانه و تحولات ژئوپلیتیک، معماری امنیت بین‌الملل و مفاهیم بنیادین «ثبات راهبردی» را دستخوش دگرگونی کرده است. گذار از منطق «بازدارندگی کلاسیک» که عمدتاً بر توازن قوای مادی و انباشت تسلیحات سخت استوار بود در یک حوزه مشخص تعریف می‌شد؛ به این معنا که سلاح هسته‌ای با سلاح هسته‌ای، و نیروی نظامی متعارف با نیروی نظامی متعارف بازدارندگی ایجاد می‌کرد. اما با پیچیده‌تر شدن نظام بین‌الملل و ظهور عرصه‌های جدید به‌سوی معماری بازدارندگی شبکه‌محور و شناختی، نشان‌دهنده تغییر بنیادین در ماهیت قدرت و الگوهای منازعه‌در نظام بین‌الملل است. در این چارچوب، بحران اوکراین را نباید صرفاً یک منازعه محدود منطقه‌ای تقلیل داد، بلکه این بحران نقطه عطفی در سنجش کارآمدی فناوری‌های نوپدید در محیط‌های عملیاتی پیچیده است. در این پارادایم جدید، موازنه تهدید و برتری راهبردی دیگر صرفاً با متغیرهای کمی مانند حجم آتش یا نیروی انسانی سنجیده نمی‌شود، بلکه قابلیت همگرایی میان زیرساخت‌های اطلاعاتی، سایبری و تصمیم‌سازی شبکه‌ای است که مزیت استراتژیک را تعیین می‌کند.

روسیه در راستای دکترین امنیت ملی و فرهنگ راهبردی خود تلاش کرده با تلفیق قدرت هوشمند و ابزارهای‌نوپدید سایبری-الگوریتمیک، الگویی نامتقارن برای موازنه در برابر غرب ایجاد کند. این الگو که می‌توان آن را در قالب بازدارندگی فناورانه چندلایه و بازدارندگی تقاطعی صورت‌بندی کرد، بر پایه تجمیع داده‌های اطلاعاتی و تسریع پردازش آن‌ها در سامانه‌های یکپارچه فرماندهی و کنترل بنا شده است. از منظر مطالعات راهبردی، پیامد اصلی چنین زیرساختی، فشرده‌سازی زمان و مکان در بحران‌هاست؛ به گونه‌ای که با کاهش چرخه تصمیم‌گیری استراتژیک از سطح کلان به واکنش‌های لحظه‌ای، معماری «مدیریت تشدید بحران» دگرگون شده و ابتکار عمل راهبردی از طریق برتری اطلاعاتی و سرعت در تصمیم‌سازی به بازیگر مهاجم یا بازدارنده منتقل می‌شود.

با وجود این، تجربه جنگ اوکراین نشان داده که چنین معماری پیشرفته‌ای خالی از ضعف نیست. آسیب‌پذیری در برابر نشت داده‌های حساس، محدودیت‌های زنجیره تأمین تحت رژیم تحریم، فرسایش تجهیزات و تهدیدات نوظهور در جنگ الکترونیک، همگی تأکید می‌کنند که بازدارندگی فناورانه نیز نیازمند نوآوری مستمر و پالایش دائمی سازوکارهای فرماندهی است. اهمیت تحلیل این ساختار نه تنها در شناخت توانمندی‌های یک قدرت نظامی بزرگ، بلکه در فهم مکانیسم‌های تحول بازدارندگی در عصر داده‌محور نهفته است. ادغام هوش مصنوعی در سامانه‌های جنگی شبکه‌ای، فصل تازه‌ای در منازعه‌نگاری گشوده که مرزهای میان حوزه‌های سنتی نبرد را کم‌رنگ ساخته و منطق چنددامنه‌ای را به هسته رقابت‌های راهبردی آینده بدل کرده است.

در بستر تحول راهبردهای نظامی معاصر، پرسش اصلی این پژوهش آن است که ادغام هوش مصنوعی در معماری شبکه‌ای جنگ‌افزارهای روسیه چگونه موجب ارتقای توان بازدارندگی فناورانه این کشور در جنگ اوکراین شده است؟ فرضیه مقاله آن است که یکپارچه‌سازی هوش مصنوعی در سامانه‌های فرماندهی و کنترل روسیه، با ایجاد چرخه‌های تصمیم‌سازی سریع‌تر، کاهش تأخیر اطلاعاتی و شکل‌دهی سازوکارهای

واکنش چندساحتی، توان بازدارندگی فناورانه را به‌طور معناداری افزایش داده و شکاف عملیاتی میان روسیه و نظام‌های دفاعی غرب را کاهش داده است.

بر همین اساس، ساختار این پژوهش با تمرکز بر مدل مفهومی هوش مصنوعی و جنگ شبکه‌محور، تحولات بازدارندگی فناورانه را در نظم جدید قدرت جهانی بررسی می‌کند و ضمن تحلیل ویژگی‌های فنی و عملیاتی معماری شبکه‌ای روسیه در جنگ اوکراین، در پایان با ارزیابی تطبیقیِ داده‌ها، به تبیین تأثیر این الگو بر تحول نظریه‌های بازدارندگی در قرن بیست‌ویکم می‌پردازد.

۱. روش پژوهش

این پژوهش بر مبنای رویکردی کیفی با بهره‌گیری از چارچوب «تحلیل لایه‌ای بازدارندگی فناورانه» طراحی گردیده است. گردآوری داده‌ها به‌صورت ترکیبی و در دو سطح انجام شد. نخست، استخراج و کدگذاری اطلاعات از متون رسمی، گزارش‌های مراکز مطالعات راهبردی و شواهد میدانی مستند مرتبط با جنگ اوکراین. دوم، تحلیل تطبیقی پیکربندی سامانه‌های شبکه‌محور روسیه با تمرکز بر سامانه پدافند موشکی دوربرد و شبکه سنجش، فرماندهی و آتش « سی-فور-آی-اِس-آر»، داده‌های خام در قالب مدل چرخه «مشاهده، سمت‌یابی، تصمیم و اقدام» بازنمایی و سپس از رهگذر تحلیل مضمون و نگاشت روابط داده وفرمان، به الگوی مفهومی بازدارندگی چندحوزه‌ای ترجمه گردید. این رویکرد ضمن اتکا بر اسناد و داده‌های عینی، با بهره‌گیری از استنتاج قیاسی، امکان ارزیابی پیوندهای علی و سنجش پایداری مزیت فناورانه روسیه در میدان نبرد را فراهم ساخته است.

۲. مدل مفهومی هوش مصنوعی و جنگ شبکه محور

۲-۱. هوش مصنوعی

هوش مصنوعی به‌عنوان یک پدیده علمی نوظهور، در دهه‌های اخیر پیشرفت‌های چشمگیری داشته و به بخش جدایی‌ناپذیری از فناوری‌های مدرن، از جمله در حوزه نظامی تبدیل شده است. با این حال، پیچیدگی مفهوم «هوش» و نبود اجماع بر تعریف آن، تدوین تعریف جامعی از هوش مصنوعی را به چالشی اساسی بدل کرده است. بازتعریف مفهوم هوش مصنوعی و بررسی دیدگاه‌های مختلف، زمینه‌ساز تحلیل اهمیت آن در جنگ‌های مدرن از منظر روابط بین‌الملل است.جان مک‌کارتی، از نخستین کسانی است که در سال ۱۹۵۶ اصطلاح «هوش مصنوعی» را ابداع کرد، آن راعلم و مهندسی ساخت ماشین‌های هوشمند، به‌ویژه برنامه‌های کامپیوتری هوشمند» تعریف می‌کند (McCarthy, 2007: 2). این تعریف بر توانایی محاسباتی سیستم‌ها برای انجام وظایف هوشمند تأکید دارد و هوش مصنوعی را از روش‌های بیولوژیکی متمایز می‌سازد. مک‌کارتی، هوش را«بخش محاسباتی توانایی دستیابی به اهداف در جهان» می‌داند. پئی وانگ (۲۰۱۹) هوش مصنوعی را از پنج منظر طبقه‌بندی می‌کند.

جدول۱، طبقه بندی هوش مصنوعی از نظر وانگ (Source: wang, ۲۰۱۹: ۱۷)

ساختارمحور	شبیه‌سازی ساختار مغز انسان، مانند شبکه‌های عصبی
رفتارمحور	سیستم‌هایی که رفتار انسانی را تقلید می‌کنند، مانند آزمون تورینگ
قابلیت‌محور	توانایی حل مسائل پیچیده، مانند سیستم «دیپ بلو» در شطرنج
عملکردمحور	تمرکز بر عملکردهای شناختی مانند جستجو، استدلال و یادگیری
اصل‌محور	بررسی رفتار کلی سیستم در موقعیت‌های مختلف در طول زمان

راسل و نورویگ در رویکردی نوین، هوش مصنوعی را حوزه‌ای می‌دانند که به طراحی و ساخت سامانه‌هایی می‌پردازد که قادرند درک کنند، استدلال کنند و با محیط خود **به‌صورت** هوشمندانه تعامل داشته باشند. آن‌ها تأکید می‌کنند که هدف نهایی، ایجاد ماشین‌هایی است که بتوانند در موقعیت‌های گوناگون، با استفاده از داده‌ها و دانش موجود، بهترین تصمیم یا اقدام ممکن را انتخاب نمایند. این رویکرد نه تنها به جنبه‌های فنی مانند الگوریتم‌ها و ساختارهای داده می‌پردازد، بلکه ابعاد شناختی، فلسفی و روان‌شناختی هوش را نیز در نظر می‌گیرد. از دیدگاه آنان، آزمودن توانایی هوش مصنوعی تنها به شبیه‌سازی انسان محدود نمی‌شود، بلکه شامل معیارهای عقلانیت و کارآمدی نیز هست (Russell & Norvig, 2021: 5).

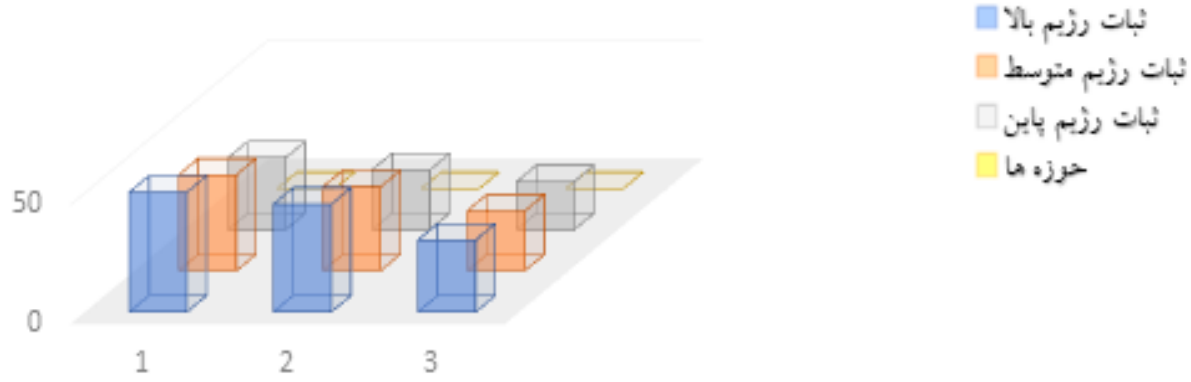
پرسش کلاسیک آلن تورینگ درباره اینکه آیا ماشین می‌تواند همچون انسان بیندیشد؟ همچنان یکی از مباحث محوری در حوزه هوش مصنوعی است. «تست تورینگ» این مسئله را به‌صورت ارزیابی توان ماشین در بازتولید رفتاری مشابه انسان مطرح می‌کند. در زمان طرح این ایده، باور رایج آن بود که اگرچه ماشین‌ها در انجام محاسبات پیچیده بر انسان برتری دارند، اما فاقد خلاقیت و شهود انسانی‌اند. باقری (۲۰۲۵) بر این باور است که با شتاب‌گیری پیشرفت پردازنده‌ها، الگوریتم‌های یادگیری و انباشت داده‌های عظیم، جهان در آستانه عبور از این تلقی تاریخی قرار گرفته است؛ تا جایی که به گفته او «ما احتمالاً آخرین نسلی هستیم که از هوش مصنوعی باهوش‌تر هستیم». تکامل الگوریتم‌های یادگیری، فاصله میان ذهن انسان و توان پردازشی ماشین را با سرعت بی‌سابقه کاهش داده است.

در این خصوص ساتن همچنان عنوان میکند که مهم‌ترین درس تاریخ هوش مصنوعی آن است که پیشرفت واقعی نه از تقلید ذهن انسان، بلکه از بهره‌گیری از توان محاسباتی و داده‌های وسیع حاصل می‌شود (Sutton & Barto, 2015: 17). از دیدگاه راهبردی، نقطه اتصال بحث این است که فناوری، به‌ویژه هوش مصنوعی، نه‌تنها ابزاری تاکتیکی، بلکه بنیان‌گذار مدل‌های جدید بازدارندگی و برتری اطلاعاتی است. همان‌طور که افزایش سرعت واکنش در جنگ شبکه‌محور مزیت راهبردی ایجاد می‌کند، توان هوش مصنوعی برای شناسایی، پیش‌بینی و اقدام پیش‌دستانه می‌تواند محاسبات دشمن را به‌طور کلی تغییر دهد (Gray, 2022: 130& Baylis, Wirtz).

به منظور سنجش نقش هوش مصنوعی در ارتقای امنیت و بازدارندگی، بهره‌گیری از نمایش بصری داده‌ها در قالب (نمودار ۱) میتوان سه سطح «ثبات رژیم بالا، متوسط و پایین» را در ارتباط با حوزه‌های

کلیدی امنیتی مقایسه کرد. بررسی‌ها نشان می‌دهد هرچه ظرفیت جذب و بومی‌سازی هوش مصنوعی بیشتر باشد، توان پیش‌بینی، واکنش سریع و بازدارندگی ارتقاء یافته و به حفظ یا افزایش امنیت ملی کمک می‌کند؛ این رابطه اما به زیرساخت فناورانه، اراده سیاسی و چارچوب‌های قانونی هر کشور وابسته است. گزارش‌ها درباره نوسازی نیروهای مسلح روسیه پس از ۲۰۰۸ نیز تأیید می‌کند که گذار به ساختار کوچک‌تر، پرتحرک‌تر و مجهز به فناوری پیشرفته، مبنای ارتقای بازدارندگی این کشور بوده است(Giles, 2017: 3).

نمودار۱. تاثیر هوش مصنوعی بر امنیت



منبع، ترسیم نویسنده‌گان بر گرفته از (Giles, ۲۰۱۷)

۲- ۲. جنگ شبکه‌محور

جنگ شبکه محور بر مبنای این فرض شکل گرفته که هم‌افزایی میان فناوری‌های ارتباطی پیشرفته، سامانه‌های شناسایی و هدف‌گیری و فرآیندهای فرماندهی و کنترل می‌تواند به افزایش برتری اطلاعاتی و نهایتاً برتری عملیاتی منجر شود. این رویکرد که نخستین‌بار در دهه ۱۹۹۰ توسط دفتر «انتقال نیروهای مشترک» وزارت دفاع ایالات متحده نظام‌مند گردید، بیان می‌کند که اتصال همه اجزای میدان نبرد اعم از نیروهای زمینی، دریایی، هوایی، فضایی و سایبری در یک شبکه امن و پرسرعت، ساختار و کارکرد سیستم‌های رزمی را دگرگون می‌سازد. بنیان‌های نظری آن هم‌راستا با مدل چرخه تصمیم‌گیری «مشاهده، سنجش، تصمیم، اقدام» جان بوید بوده و بر کاهش زمان این چرخه از طریق تبادل بلادرنگ داده و شکل‌گیری «آگاهی وضعیت مشترک» میان تمامی سطوح فرماندهی و نیروهای عملیاتی تأکید دارد(Boyd, 1976: 4).

جنگ شبکه‌محور، ایجاد یک بستر ارتباطی منعطف و مقاوم است که از طریق آن، تمامی عناصر میدان نبرد از حسگرها و سامانه‌های شناسایی تا واحدهای رزمی و مراکز فرماندهی در یک شبکه یکپارچه داده‌ای ادغام می‌شوند. چنین ساختاری موجب کاهش «مه جنگ»، افزایش آگاهی مشترک

از موقعیت و تسریع چرخه تصمیم‌گیری می‌شود (Sloan, 2016: 125). مدل پیشنهادی، ورودی‌های خود را از سه حوزه اصلی دریافت می‌کند نخست، سامانه‌های «حسگرشلیک» یکپارچه که گردش سریع اطلاعات از نقطه شناسایی تا نقطه آتش را تضمین می‌کنند. دوم، شبکه‌های ارتباطی امن و تاب‌آور در برابر تهدیدات جنگ الکترونیک و سوم، داده‌های چندمنبعی شامل سیگنالی، تصویری، حرارتی و راداری. این داده‌ها در فرایند میانی مدل، ابتدا از طریق شبکه‌سازی نیروها به هم پیوند می‌خورند، سپس در مراکز «سی-فور-آی-اِس-آر» پردازش و به آگاهی مشترک بدل می‌شوند، و در نهایت توسط الگوریتم‌های یادگیری ماشین تحلیل و اولویت‌بندی می‌شوند (Luddy, 2005: 6). روابط علّی در این مدل نشان می‌دهد که هم‌افزایی میان شبکه‌سازی و پردازش هوشمند داده‌ها، چرخه «اودا» را از مقیاس زمانی ساعت به دقیقه کاهش می‌دهد و ابتکار عمل را در میدان نبرد به‌دست فرمانده می‌سپارد. بدون این آگاهی مشترک، حتی پیشرفته‌ترین تحلیل‌های هوش مصنوعی نیز ارزش عملیاتی محدودی خواهند داشت (Alberts et al, 2000, p. 72).

نتایج مورد انتظار از پیاده‌سازی این مدل را می‌توان در سه محور خلاصه کرد نخست، تسریع نفوذ عملیاتی از طریق اجرای هم‌زمان عملیات‌های زمینی، هوایی، دریایی و سایبری در چارچوبی هماهنگ؛ دوم، کاهش تلفات انسانی و هزینه‌های مادی با جایگزینی مأموریت‌های پرخطر به‌وسیله سامانه‌های خودکار و پهپادی؛ و سوم، انعطاف کمتردیده‌شده در انتخاب زمان و مکان مداخله به‌منظور ضربه‌زدن در نقاط حساس نبرد. مطالعه موردی جنگ روسیه و اوکراین شواهد عینی این کارآمدی را نشان می‌دهد؛ جایی که اوکراین با ادغام پهپادهای شناسایی و رزمی نظیر« گلوبال هاوک» و « پردیتور» با سامانه‌های تحلیلی مبتنی بر هوش مصنوعی، توانسته دقت، سرعت و هماهنگی عملیات خود را به‌طور محسوسی ارتقا دهد (Alberts et al., 2000: 55).

۳. ریشه‌های تاریخی منازعه

تحلیل بحران اوکراین مستلزم بازکاوی مسیر تاریخی شکل‌گیری هویت ملی روسیه و پیوند آن با ایده امپراتوری است. تجربه روسیه با الگوهای شکل‌گیری دولت ملی در غرب اروپا تفاوت جدی دارد؛ انگلیس و فرانسه در قرون شانزدهم و هفدهم نخست دولت‌های ملی خود را تثبیت کردند و سپس به ایجاد امپراتوری‌های فرامرزی پرداختند که پس از جنگ جهانی دوم، به مرزهای ملی بازگشتند. روسیه، برعکس، بدون تجربه یک دولت ملی، مستقیماً به ساخت بزرگ‌ترین امپراتوری خشکی جهان روی آورد. این خاستگاه، عقب‌نشینی از چشم‌انداز امپراتوری را دشوار ساخت و تداوم نگاه امپراتوری‌محور را در هویت ملی نهادینه کرد (Kuzio, 2022). اگر پیمان ۱۷۰۷ میان انگلیس و اسکاتلند اتحاد نسبتاً برابری ایجاد کرد که با حفظ نظام‌های حقوقی و آموزشی محلی همراه بود، «معاهده پریاسلاو» ۱۶۵۴ بر اساس روایت روسیه نماد تسلیم اوکراین و آغاز سلطه این کشور تلقی می‌شود.

دوران شوروی این مشکل را تشدید کرد، برخلاف جمهوری‌های شوروی از جمله اوکراین که از هویت سیاسی-اداری مشخص برخوردار بودند، «جمهوری فدراتیو روسیه» فاقد چنین تمایزی بود و این موجب

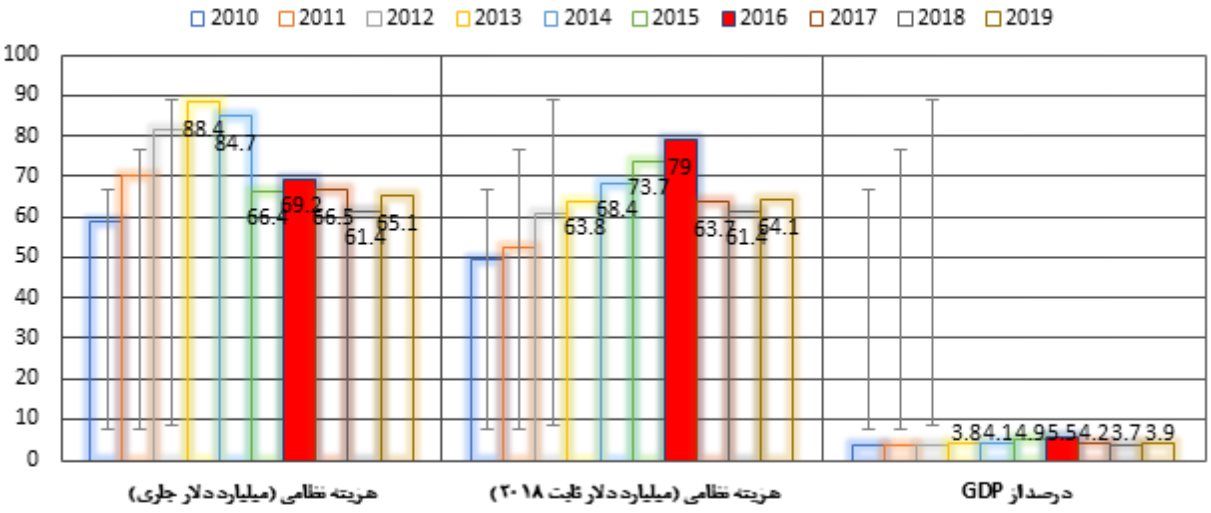
شـد مرزهـای هویتـی روس بـودن و شـوروی بـودن مخـدوش بمانـد. پـس از فروپاشـی، رهبـران روس همچنـان اوکرایـن را بخشـی از «فضـای نفـوذ طبیعـی» خـود دانسـتند و در نهایـت الگـوی مداخلـه روسـیه در جنـگ ۲۰۱۴ نشـان‌دهنده «اسـتراتژی تشـدید تدریجـی» سـه‌مرحله‌ای اسـت؛ نفـوذ اولیـه تیم‌هـای تخصصـی، حـملات فرامـرزی محـدود و ورود مسـتقیم یگان‌هـای زمینـی در اوت همـان سـال. ایـن رونـد، هم‌راسـتا بـا دکتریـن گراسـیموف، تلفیقـی از ابـزار نظامـی و غیرنظامـی بـرای پیشـبرد اهـداف و بـا محدودیت‌هـای سـاختاری روسـیه در اسـتفاده مسـتقیم و گسـترده از نیـروی نظامـی منطبـق بـود (Sutyagin, 2015: 2).

از دهـه ۱۹۹۰، بحـث هویـت ملـی روسـیه در پنـج رویکـرد اصلـی شـکل گرفتـه اسـت. سـه رویکـرد نخسـت مسـتقیماً بـا مسـئله اوکرایـن مرتبـط هسـتند و مبنـای ایدئولوژیـک بسـیاری از سیاسـت‌های خارجـی روسـیه را تشـکیل می‌دهنـد. نخسـت، هویـت اتحـادی و اوراسـیاگرایی کـه روسـیه را به‌عنـوان رهبـر طبیعـی حـوزه اوراسـیا تعریـف می‌کنـد؛ دوم، ملـت روس کـه سـه قـوم اسلاو شـرقی (روس‌هـا، اوکراینی‌هـا و بلاروسـی‌ها) را یـک ملـت واحـد می‌شـمارد و مشـروعیت اسـتقلال اوکرایـن را انـکار می‌کنـد؛ و سـوم، ملـت روس‌زبـان کـه زبـان روسـی را پایـه اصلـی هویـت دانسـته و حضـور روس‌زبانـان در اوکرایـن را مبنایـی بـرای مداخلـه معرفـی می‌کنـد. اوراسـیاگرایی کـه در دهـه ۱۹۳۰ میـان مهاجـران روس سـفید شـکل گرفـت، امـروز ایدئولـوژی غالـب کرملیـن اسـت و غـرب را تهدیـدی علیـه «جهـان روسـی» می‌بینـد.

ایـن دیـدگاه، اوکرایـن را «موجودیـت مصنوعـی» و «دولـت شکسـت‌خورده» معرفـی کـرده کـه بخش‌هـای روس‌زبانـش نیازمنـد «حمایـت» در برابـر ناسیونالیسـت‌های برآمـده از رویـداد یوروميـدان هسـتند. اختلافـات تاریخـی اوکرایـن تقسـیم سـرزمین میـان امپراتوری‌هـای روسـیه و اتریـش مجارسـتان در قـرون ۱۹ و ۲۰ باعـث شـکل‌گیری فرهنـگ و سیاسـت منطقـه‌ای متنـوع شـد. مقامـات روس، ملی‌گرایـی اوکراینـی را سـاخته و پرداختـه اتریـش می‌دانسـتند و حتـی آمـوزش و نشـر زبـان اوکراینـی را بـرای سـال‌ها ممنـوع کـرده بودنـد (Mankoff, 2022: 393). تجربـه کوتـاه اسـتقلال پـس از انـقلاب ۱۹۱۷؛ در چارچـوب رهیافت‌هـای «سـازه‌انگاری» و «امنیـت هستی‌شـناختی»، رهبـران روسـیه در دوران پسـاجنگ سـرد همـواره حاکمیـت ملـی اوکرایـن را از دریچـه‌ای تقلیل‌گرایانـه و مبتنـی بـر پیوندهـای درهم‌تنیـده هویتـی ارزیابـی کرده‌انـد.

در ایـن رویکـرد، انگاره‌هـای تاریخـی و هویتـی به‌عنـوان متغیرهـای مسـتقل و پیشـران در سیاسـت خارجـی مسـکو عمـل می‌کننـد؛ به‌گونـه‌ای کـه سیاسـت حمایـت از دیاسـپورای روس‌تبـار در قالـب یـک هـدف «ژئوکالچـرال»، بـا الزامـات بقـا و منافـع ژئوپلیتیـک و ژئواکونومیـک روسـیه در منطقـه «خـارجِ نزدیـک» پیونـد خـورده اسـت. در ایـن چارچـوب تحلیلـی، مداخلـه و الحـاق شـبه‌جزیره کریمـه در سـال ۲۰۱۴ را می‌تـوان تلاشـی بـرای احیـای مرزهـای هویتـی و پاسـخ بـه ادراک تهدیـد ناشـی از نفـوذ غـرب تفسـیر کـرد؛ منطقـه‌ای کـه تـا پیـش از واگـذاری آن در سـال ۱۹۵۴، دارای اهمیـت اسـتراتژیک و پیوسـتگی جمعیتـی بـا قلـب سـرزمین روسـیه بـود (Koolaee & Zangeneh, 2024, p. 40). همگرایـی ایـن متغیرهـای ژئوپلیتیـک و ژئوکالچـرال، اوکرایـن را در دکتریـن امنیتـی کرملیـن بـه یـک منطقـه حائـل و رکنـی حیاتـی بـرای حفـظ پرسـتیژ بین‌المللـی بـدل سـاخته اسـت. در نهایـت، ایـن سـاختارهای هویتـی بـا شـکل‌دهی عمیـق بـه «ادراک تهدیـد» رهبـران روسـیه، پیونـدی ارگانیـک بـا ابزارهـای سـخت و مـدرن جهـت حفـظ «موازنـه قـوا» برقـرار می‌کننـد.

نمودار ۲. هزینه های نظامی روسیه (۲۰۱۰-۲۰۱۹)



منبع: ترسیم نویسندگان، برگرفته ازداده های (SPIRI).

بررسی روند هزینه‌های نظامی روسیه در دهه‌های اخیر نشان می‌دهد که این کشور، پس از تجربه بحران‌های دهه ۱۹۹۰ و شوک‌های امنیتی اوایل قرن بیست‌ویکم، وارد یک چرخه مداوم افزایش و بازتخصیص منابع دفاعی شده است. بازتولید گفتمان «قدرت بزرگ» و ضرورت بازسازی توان نظامی به‌عنوان ابزار حفظ موقعیت ژئوپلیتیکی، باعث شد سرمایه دفاعی از اوایل دهه ۲۰۱۰ با شیبی محسوس رو به رشد گذارد. در چارچوب بازتولید بازدارندگی استراتژیک، بخش عمده‌ای از بودجه صرف ارتقای سه‌گانه هسته‌ای، سامانه‌های دفاع ضدبالستیک و زیرساخت‌های فرماندهی شده که باعث کنترل مقاوم در برابر جنگال شده است.

۴. الگوی جنگ شبکه‌محور روسیه در حوزه هوایی

ظرفیت بالای شبکه فرماندهی و کنترل روسیه برای اجرای موج‌های متراکم حملات هوایی، امکان هماهنگی همزمان میان سلاح‌های هدایت‌شونده، پهپادها و جنگنده‌ها را فراهم آورده است. این توانمندی، روسیه را قادر ساخته تا هم در نقش ضربه‌زننده نخست و هم به‌عنوان بازیگر بازدارنده فعال عمل کند. در بخش هوایی، روسیه از گونه‌های متنوع سلاح‌ها و حامل‌ها بهره برده است که طیف کامل عملیات هجومی، پدافندی را پوشش می‌دهد از جمله موشک‌های کروز «کالیبر» موشک‌های بالستیک کوتاه‌برد «اسکندر-ام». پهپادهای انتحاری «شاهد-۱۳۶» پهپادهای شناسایی «اورلان-۱۰» مهمات سرگردان «لنست». جنگنده‌های چندمنظوره «سوخو-۳۵اس»، بمب‌افکن‌های «سوخو-۳۴» بهره برداری از فناوری نوین اطلاعاتی شامل به‌کارگیری حسگرها، رایانه‌ها و سایر فنون اطلاعاتی در سامانه فرماندهی و کنترل نیروهای مسلح توأم با استفاده از سلاح‌های هوشمند هدایت‌شونده، تغییرات اساسی در مفاهیم عملیاتی و شیوه‌های فرماندهی و کنترل پدید آورده است (Tavakkol, 2006: 2)

مفاهیمی چون مهار و بازدارندگی در خلأ شکل نمی‌گیرند، بلکه ماهیتی پویا داشته و عمیقاً تحت تأثیر متغیرهایی نظیر موازنه قوا، رقابت قدرت و دگرگونی‌های ژئوپلیتیک قرار دارند. بر پایه همین بن‌مایه‌های رئالیستی و فرهنگ راهبردی، گستره کاربرد فناوری‌های تسلیحاتی روسیه علیه طیف وسیعی از زیرساخت‌های حیاتی اوکراین از شبکه‌های انرژی تا گره‌های فرماندهی نظامی و سامانه‌های پدافند هوایی را می‌توان بروز نوینی از استراتژی «فلج استراتژیک» و اعمال «بازدارندگی از طریق مجازات» ارزیابی کرد. در سطح عملیاتی، این رویکردِ پویا در قالب «حملات اشباع‌کننده و از طریق ترکیب امواج پی‌درپی تسلیحات نامتقارن نظیر پهپادهای انتحاری با موشک‌های کروز و بالستیک اجرا می‌شود. این تنوع در حامل‌ها، زمان واکنش سامانه‌های پدافندی را به حداقل رسانده و شانس رهگیری را مختل می‌سازد. در نتیجه، هم‌زمانی تخریب فیزیکی با ایجاد فشارهای روانی، نه‌تنها ظرفیت تاب‌آوری ملی دشمن را تضعیف می‌کند، بلکه با فروپاشی انسجام در معماری دفاع هوایی، توان واکنش سیستماتیک اوکراین را سلب کرده و مسیر را برای تحمیل اراده سیاسی و تثبیت موازنه قوا به نفع مسکو هموار می‌سازد (Nouri, 2019, p. 248).

با این حال در اوایل تصاویر ماهواره‌ای از حمله به پایگاه هوایی اُزرنه در مارس ۲۰۲۲ نشان‌دهنده عدم اصابت دقیق بسیاری از موشک‌ها به ساختارهای کلیدی بود، در حالی که حملات بعدی به شبکه برق اوکراین (مانند هدف‌گیری پست‌های برق در نوامبر ۲۰۲۲) دقت بالاتری را با تمرکز بر نقاط حساس زیرساختی نشان داد و این امر برتری روسیه در جنگ شبکه‌محور را برجسته می‌سازد (Williams, 2023: 39). هماهنگی دقیق در اجرای این حملات، که به‌ویژه در ماه‌های اوج عملیات مشهود بوده است، نشان می‌دهد روسیه از یک چرخه تصمیم‌گیری سریع و یکپارچه در حوزه هوایی بهره‌مند است. جنگ‌های هوایی مدرن با این سطح از هماهنگی و یکپارچگی، تنها به عرصه ملی محدود نمی‌شوند؛ پیامدهای چنین عملیات‌هایی به‌طور مستقیم بر امنیت بین‌المللی نیز اثرگذار است، زیرا شبکه‌های فرماندهی-کنترل پیشرفته قابلیت تطبیق و توسعه به سایر حوزه‌های نظامی مانند عملیات دریایی، زمینی و اطلاعاتی را دارند. با این حال ساختار مورد نظر نشان می‌دهد که قدرت هوایی، فراتر از یک ابزار حمله فیزیکی، به‌عنوان محور اتصال سایر ابزارهای جنگی در راهبرد شبکه‌محور عمل می‌کند (Gunneriusson &Bachmann 4 :2015 ,).

۴- ۱. کاربست پهپادی روسیه

عرصه پهپادهای رزمی روسیه نشان‌دهنده آن است که از سال ۲۰۱۴ به این سو، سرمایه‌گذاری فزاینده‌ای بر روی توسعه، بهینه‌سازی و بومی‌سازی سامانه‌های هوایی بدون سرنشین انجام داده و این حوزه را به یکی از محوری‌ترین مؤلفه‌های بازآرایی ساختار نبرد خود بدل ساخته است. این فرایند، به‌ویژه در پی ترکیب کارکردی این سامانه‌ها با الگوریتم‌های هوش مصنوعی و در چارچوب چرخه‌های پیچیده‌ی «ایستار» (اطلاعات، نظارت، هدف‌یابی و شناسایی) و پیوند مستقیم آن‌ها با آتش دقیق دورایستا، ستون فقرات راهبرد جنگ شبکه‌محور روسیه را شکل داده است (Cranny, 2025). در این الگو، پهپاد به‌عنوان «گره سنسور» بر علاوه جمع‌آوری داده، هم یک مولد داده زنده و قابل پردازش بلادرنگ برای بقیه عناصر شبکه عمل می‌کند.

پهپاد «اورلان-۱۰» در هر سه فاز اصلی جنگ اوکراین شامل آغاز تهاجم در فوریه ۲۰۲۲، تثبیت خطوط مقدم در تابستان ۲۰۲۲ و ضدحملات متقابل طی سال‌های ۲۰۲۳ و ۲۰۲۴ حضوری مداوم داشته است. در مرحله نخست، اورلان-۱۰ نقش «چشم» توپخانه دوربرد را ایفا کرد؛ پروازهای پیوسته این پهپاد بر فراز خارکیف و ایزیوم (BBC News, 2023) داده‌های دقیق مختصات واحدهای توپخانه اوکراین را به سامانه‌های «مالکا-ام» و «اسمرچ» منتقل می‌کرد. تاکتیک پرواز در ارتفاع متوسط همراه با مسیر سینوسی، احتمال رهگیری را کاهش داده و در مجموع اثر تاکتیکی آن به افزایش دقت آتش روسیه تا حد انهدام زره‌پوش‌ها در نخستین موج شلیک انجامید. در سپتامبر ۲۰۲۲ گروهی سه‌تایی از اورلان-۱۰ مجهز به ماژول جنگ الکترونیک «لیر-۳» موفق شدند ارتباط پهپادهای «بایرکدار» اوکراینی را قطع کرده و مسیر کنترل آن‌ها را منحرف سازند.

این اقدام موجب اختلال در فرآیند شناسایی دریایی اوکراین گردید و عملاً فرصت هدف‌گیری دقیق ناوگان دریای سیاه، از جمله ناو «آدمیرال ماکاروف»، را از بین برد. در محور دونتسک، اورلان–۱۰ پس از شناسایی و تعیین موقعیت یک سامانه پدافند هوایی «ناسامز» اوکراینی، مختصات هدف را به واحد حمله لنست منتقل کرد و تنها دوازده دقیقه بعد سامانه مزبور منهدم شد. تاکتیک به‌کاررفته شامل پرواز کم‌ارتفاع، بهره‌گیری از پوشش طبیعی زمین و ارسال مختصات رمزگذاری‌شده به یگان مهاجم بود. اثر راهبردی این عملیات در کاهش امنیت هوایی اوکراین در شعاع سی کیلومتری و گشودن مسیر برای حملات هوایی موجی بروز یافت.

پهپاد «فورپست–آر» نسخه بومی‌شده سامانه اسرائیلی «سرچر»، از سال ۲۰۱۹ با استفاده کامل از فناوری و قطعات داخلی روسیه تولید می‌شود و در جنگ اوکراین (Army Recognition, 2022). با برد عملیاتی حدود ۴۵۰ کیلومتر و مداومت پروازی نزدیک به ۱۸ ساعت، در مأموریت‌های ترکیبی شناسایی و رزمی در محورهای جنوبی و شرقی اوکراین (به‌ویژه خرسون و ماریوپل) به‌کار گرفته شده است. در تابستان ۲۰۲۲، برای نخستین‌بار با موشک‌های هدایت‌شونده دقیق سبک و ماژول‌های جنگ الکترونیک مجهز شد و در مأموریت‌های ضدپدافندی به کار رفت. گزارش‌ها نشان می‌دهد که در حمله به مواضع پدافند اوکراینی در شمال ماریوپل، دو فروند«فورپست–آر» با شلیک موشک‌های کوچک هدایت‌شونده موفق به انهدام رادار ضدهوایی «ام-۸۰۶» شدند. از پاییز ۲۰۲۳، این سامانه در قالب مأموریت‌های حلقه بسته حسگر-شلیک‌گر عمل کرده است. این پهپاد با ترکیب رادار جست‌وجوی هدف و سامانه اپتیکی پانورامیک، اهداف ثابت یا نیمه‌متحرک را شناسایی و مختصات را فوراً به واحدهای توپخانه و پهپادهای تهاجمی منتقل می‌کرد.

مهمات سرگردان «کوب–بِ‌اِل‌آ» زیرمجموعه گروه کلاشنیکف، نخستین بار در نبرد سوریه (۲۰۱۸–۲۰۱۹) آزمایش شد و از مارس ۲۰۲۲ به‌طور گسترده در محورهای شرقی و جنوبی اوکراین مورد استفاده قرار گرفت. این پهپاد کوچک مقیاس با برد عملیاتی حدود ۴۰ کیلومتر و توان حمل سرجنگی ۳ کیلوگرمی، توانایی انجام مأموریت مستقل دارد. در حمله ثبت‌شده در ژوئن ۲۰۲۲ به موضع توپخانه اوکراین در منطقه پوپاسنا، چند فروند «کوب–بِ‌اِل‌آ» پس از دریافت مختصات هدف از پهپاد اورلان ۱۰، به‌صورت نیمه‌خودکار و بدون

هدایت لحظه‌ای اپراتور عمل کرده، داده‌های تصویری اولیه را تطبیق داده، مواضع زرهی را طبقه‌بندی کرده و عملیات تهاجمی را در کمتر از ۱۲ دقیقه از زمان تشخیص تا برخورد اجرا کردند (Kallenborn, 2022: 7).

نسخه‌های جدید «کوب–بی‌اِل‌آ» از پاییز ۲۰۲۳ به قابلیت اجرای عملیات «گله‌ای» و پرتاب از روی بسترهای متحرک دریایی مجهز شده‌اند. در عملیات آزمایشی ناوگان دریای سیاه در سواستوپل (اکتبر ۲۰۲۳) نمونه‌های دریایی این پهپاد در قالب خوشه‌های سه‌تایی از رزم‌ناو کوچکی پرتاب شدند و با استفاده از الگوریتم‌های هدایت جمعی توانستند پنج موضع ضدهوایی اوکراینی را به‌صورت اشباع‌کننده و همزمان مورد حمله قرار دهند. این نوع عملکرد نه‌تنها موجب غافلگیری دفاع هوایی دشمن شد بلکه هزینه مقابله را به‌دلیل نیاز به شلیک چندباره موشک‌های پدافندی افزایش داد و به‌طور مستقیم در منطق بازدارندگی فناورانه روسیه منعکس گردید.

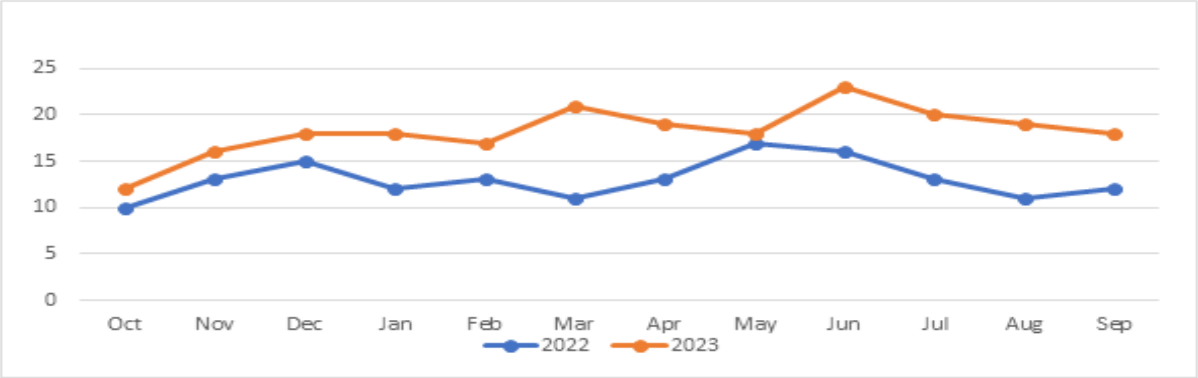
مهمات سرگردان «لنسِت» نیز به‌عنوان سلاح رزمی جدید گروه کلاشنیکف، از اواخر ۲۰۲۲ به‌طور سازمانی در واحدهای نیروی زمین روسیه ادغام شد. این سامانه با برد عملیاتی ۴۰ کیلومتر قادر به حمله دقیق نقطه‌ای علیه اهداف متحرک است. در عملیات دفاعی باخموت (مارس ۲۰۲۳)، لنسِت‌ها با استفاده از حسگر «لیدار» و فیوزهای هوشمند، زاویه برخورد را طوری تنظیم کردند که ضربه در نقاط آسیب‌پذیر زرهی مستقر در حومه شهر وارد شود؛ یکی از نمونه‌های ثبت‌شده، انهدام سامانه پدافند « ناسامس» در کمتر از ۹ دقیقه پس از شناسایی اولیه بود.

بر اساس داده‌های گردآوری‌شده تا ژانویه ۲۰۲۵، بیش از ۳۰۰۰ مأموریت عملیاتی لنسِت در اوکراین ثبت شده است، که بیش‌ترشان در قالب حملات «زنجیره‌دیزی» صورت گرفته‌اند؛ در این الگو، چند پرنده به‌طور متوالی یا هم‌زمان به یک سامانه دفاعی، سکوی توپخانه یا مرکز فرماندهی حمله می‌کنند تا احتمال نجات هدف تقریباً به صفر برسد. عملکرد عملیاتی روسیه از ابتدا با چالش‌های ملموسی مواجه بوده است چنانچه داده‌های منتقل‌شده از پهپاد اورلان–۱۰ به سامانه توپخانه «مالکا–ام» به‌دلیل اختلال رمزگذاری در شبکه فرماندهی زمینی اشتباه تفسیر شد و منجر به اصابت گلوله‌ها به موضع خودی روسیه در حاشیه بولدارا شد. خطا از عدم هم‌زمانی «جی-پی-اس» میان لینک «سی–فور–آی–اس–آر» زمینی و حسگر هوایی ناشی شد، مشکلی که بعدها با افزودن ماژول هم‌زمان‌سازی «گلوناس–فاز۲» و جایگزینی تراشه‌های غربی با محصولات صنایع «می‌کرا» رفع شد.

۴- ۲. سامانه‌های موشکی

در چارچوب دفاع هوایی و موشکی، روسیه با توسعه «اس-۴۰۰» و «اس-۵۰۰» توانسته لایه‌ای از پدافند پیشرفته را مستقر کند که به‌طور گسترده متکی بر سامانه‌های تشخیص خودکار تهدید، رادارهای آرایه‌فازی کاملاً دیجیتال، پردازش داده چندسکویی و شبکه‌های ارتباطی همزمان و مقاوم در برابر جنگال است. ارتقای مداوم الگوریتم‌های شناسایی سریع هدف، مسیریابی بهینه و تصمیم‌گیری بلادرنگ، به‌ویژه در مواجهه با تهدیدات بالستیک و هوایی پیچیده عنوان میشود، روندی که از اوایل دهه ۲۰۱۰ با نوسازی تدریجی «اس-۳۰۰»، تکامل کامل «اس-۴۰۰» و نهایتاً معرفی «اس-۵۰۰» به اوج خود رسید (Carlin, 2024).

نمودار ۳. تنوع استفاده موشک های روسیه (۲۰۲۲-۲۰۲۳)



منبع: گردآوری نویسندگان بر اساس داده‌های (CSIS,۲۰۲۳)

در پایان سال ۲۰۲۴، میانگین تعداد حملات پهپادی روسیه حدود دو هزار مورد در ماه برآورد می‌شد، اما این رقم در نیمه‌ی نخست سال ۲۰۲۵ به بیش از چهار هزار واحد افزایش یافت. تنها در حمله‌ی ۲۹ ژوئن ۲۰۲۵، در مجموع ۵۳۷ سلاح هوایی شامل ۴۷۷ پهپاد و ۶۰ موشک به سمت اهداف اوکراین شلیک شد، که رکورد بیشینه‌ی سه‌سالِ جنگ را شکست و نشان‌دهنده‌ی ورود تدریجی روسیه به مرحله‌ی «بازدارندگی فرسایشی» است (Bielieskov, 2025). سامانه دفاع هوایی «اس۴۰۰» روسیه، به عنوان یکی از پیشرفته‌ترین سیستم‌های پدافندی جهان، در محیط‌های عملیاتی مانند جنگ سوریه و مراحل اولیه درگیری اوکراین، موفقیت‌های قابل توجهی را به ثبت رسانده است (Deb, 2021). در مراحل اولیه جنگ اوکراین (۲۰۲۲) «اس۴۰۰» با رهگیری بیش از ۱۰۰۰ هدف، از جمله پهپادهای «بایرکدار تی‌بی۲» و موشک‌های اوکراینی، به بازدارندگی مؤثر کمک کرد (Gwadera & Wright, 2023).

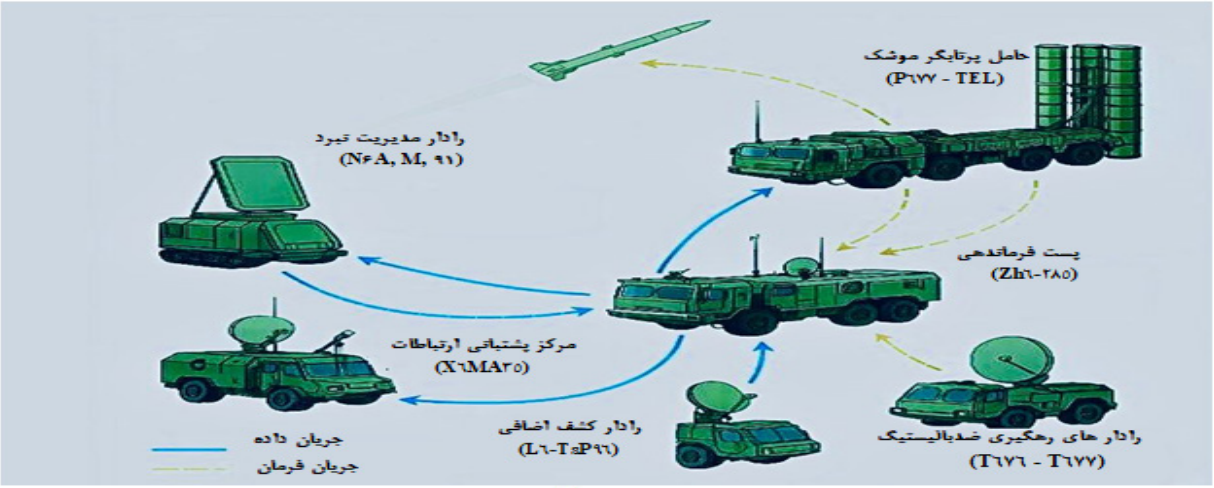
این موفقیت‌ها عمدتاً به دلیل قابلیت رهگیری همزمان تا ۸۰ هدف در بردهای بلند (تا ۴۰۰ کیلومتر) و ادغام با لایه‌دفاعی دیگر بوده است. پس از انفجار در پل کریمه در اکتبر ۲۰۲۲ که به گفته روسیه ناشی از انفجار یک کامیون حامل مواد منفجره بود، این سازه به یکی از اهداف اصلی حملات پهپادی و موشکی اوکراین تبدیل شد. بر اساس گزارش رسمی وزارت دفاع روسیه که در ۲ سپتامبر ۲۰۲۳ توسط الجزیره منتشر شد، سه پهپاد نیروی دریایی اوکراینی پیش از رسیدن به سازه اصلی در سواحل دریای سیاه منهدم شدند. مطابق تحلیل گزارش‌های نظامی موجود سامانه «اس-۴۰۰» مستقر در منطقه کرچ–تمریوک و سامانه‌های نزدیک برد «پانصیراس۱» انجام شده است که مأموریت حفاظتی از پل را بر عهده دارند (Al Jazeera, 2023).

در اقدامات بعدی، اوکراین کوشید با بهره‌گیری ترکیبی از موشک‌های بالستیک کوتاه‌برد «توچکا–یو»، راکت‌اندازهای دوربرد «هیمارس» و پهپادهای انتحاری بومی موسوم به «بیورِ»، موجی از حملات اشباع‌شده را علیه مراکز لجستیکی روسیه در منطقه لوهانسک سازماندهی کند. آتشبارهای سامانه اس–۴۰۰ توانستند بخش عمده‌ای از موشک‌ها را رهگیری کنند، اما هم‌زمانی و تنوع برد حملات موجب شد که

نرخ رهگیری پهپادهای انتحاری به‌طور محسوسی کاهش یابد. پیامد این وضعیت، کاهش نسبی خسارت کلی بود؛ با این وجود، شماری از پهپادها موفق به نفوذ به انبارهای سوخت و مهمات روسیه شدند. با آغاز ضدحمله اوکراین در محور خارکف، سامانه‌های اس–۴۰۰ مستقر در منطقه بریانسک مأموریت جنگنده‌های سوخو–۳۵ و بمب‌افکن‌های سوخو–۳۴ را با پوشش هوایی پیوسته پشتیبانی کردند. این دفاع در عمق مانع از نفوذ هواپیماها و موشک‌های میان‌برد اوکراینی گردید و در نتیجه، برتری نسبی هوایی روسیه در جبهه شمالی حفظ شد.

با توجه به موفقیت‌های نسبی یاد شده در مقابل از سپتامبر ۲۰۲۲ تا مه ۲۰۲۴ منابع غربی و گزارش‌های اوکراینی نابودی یا آسیب جدی حداقل ۱۲ سامانه «اس-۴۰۰» از جمله شش مورد در آوریل ۲۰۲۴ را ثبت کرده‌اند. عمده‌ی این حملات با استفاده از موشک‌های « ای-تَکمز »، نسخه‌های ارتقاءیافته نپتون و پهپادهای تهاجمی مدرن، عمدتاً در جغرافیای کریمه و لوهانسک انجام گرفته است. که نشان‌دهنده تغییر موازنه تاکتیکی و فشار بر آرایش نیروهای روسیه است. این تلفات شکاف‌هایی در سپر دفاعی روسیه به‌وجود آورد و مسکو را ناگزیر از جابجایی آتش‌بارها، از جمله انتقال و استقرار «اس-۵۰۰»، ساخت. با این حال، این عملکرد نسبی نشان‌دهنده اهمیت سامانه در راهبردهای بازدارندگی مدرن است.

شکل۱. مشخصات فنی سامانه اس ۵۰۰



منبع: ترسیم نویسندگان

سامانه اس-۵۰۰ که ساختار آن در شکل (۱) نمایش داده شده و تحت عنوان « اس-۵۰۰، پرومتئوس» شناخته می‌شود، پیشرفته‌ترین سطح فناوری دفاع هوایی و موشکی روسیه تاکنون به شمار می‌آید. این سامانه، با برد عملیاتی تا ۶۰۰ کیلومتر برای اهداف بالستیک و حدود ۵۰۰ کیلومتر برای اهداف آیرودینامیکی، قابلیت رهگیری و مقابله با موشک‌های قاره‌پیما، موشک‌های کروز، جنگنده‌های رادارگریز و پهپادهای رزمی را داراست. موشک‌های این سامانه، از جمله (۷۷ – اِن ۶ – اِن) و (۷۷ – اِن ۶ – اِن ۱)، با سرعت‌هایی برابر با ۲۰ ماخ قادر به مقابله با اهداف پرسرعت هایپرسونیک هستند (Anderson, 2025).

تصویر۱، موشک های مافوق صوت (۷۷ –اِن ۶ –اِن) و (۷۷ –اِن ۶ –اِن ۱)، برای استفاده توسط اس-۵۰۰

منبع: وزارت دفاع روسیه

افرادی از جمله توماس ویتینگتون (متخصص علوم نظامی)، تأکید کرده که روسیه احتمالاً در حال حاضر تنها باتری عملیاتی محدود از سامانه «اس-۵۰۰» را در اختیار دارد. این محدودیت کمی، سامانه را به طور قابل توجهی در برابر حملات اشباع موشکی و پهپادی اوکراین آسیب‌پذیر می‌سازد (Withington, 2024). با این حال آن چه که بسیاری از سایت‌های نظامی معتبر همچون «پایگاه اطلاعات نظامی جهانی»، «نشریه امنیت ملی» به صورت مشخص و با جزئیات به توانایی‌های این سامانه پرداخته‌است مشخص میکند که «اس-۵۰۰» علی رغم گزارش‌های موجود مبنی بر این که موشک‌های بالستیک پرسرعت مانند «آیتکمیز» آمریکایی می‌توانند از پوشش رهگیری سامانه «اس-۵۰۰» عبور کند، به عنوان یک سامانه قابل توجه در سیستم دفاعی روسیه عمل میکند (Korshak, 2024).

سرویس‌های اطلاعاتی روسیه در سال ۲۰۲۵ اعلام کردند که این سامانه در مناطق کلیدی همچون مسکو و کریمه مستقر شده و در آزمایش‌های میدانی موفق به رهگیری دقیق و مؤثر موشک‌ها شده است. برتری «اس-۵۰۰» در نسبت به سامانه‌های قدیمی‌تر همچون اس-۴۰۰ علاوه بر برد بیشتر، سرعت و دقت بالاتر، به دلیل قابلیت مقابله با سلاح‌های هایپرسونیک و ماهواره‌های پایین‌مدار است که در سامانه‌های پیشین امکان‌پذیر نبود. همچنین استفاده از فناوری هوش مصنوعی و مقاومت بالا در برابر جنگ‌های الکترونیک از دیگر نقاط قوت آن محسوب می‌شود(Sputnik, 2016). در نهایت این سامانه را می‌توان تجسم گذار روسیه از بازدارندگی سخت‌افزاری کلاسیک به بازدارندگی فناورانه چندلایه دانست. از مباحث مهم دیگر در جنگ اوکراین قدرت تهاجمی روسیه در استفاده از موشک است. توسعه موشک«۹-ام-۷۲۹، اس-اس-سی-۸» منجر به فروپاشی پیمان «آی-اِن-اِف» شد.

این موشک با برد ۵۰۰ تا ۲۵۰۰ کیلومتر، که از ۲۰۱۰ تا ۲۰۱۵ در قالب آزمایش‌های متعارف پیگیری شد، ظرفیت پرتاب زمینی میان‌برد را بازسازی کرد و پایه‌ای برای نسل جدید سامانه‌های روسی فراهم آورد (Ashley, 2019). این پیمان، موشک‌های زمین‌پایه با برد ۵۰۰ تا ۵۵۰۰ کیلومتر را ممنوع کرده بود؛ حذف آن، میدان مانور تاکتیکی روسیه را گسترش داد و بازدارندگی تهاجمی را در اروپا و حوضه دریای سیاه

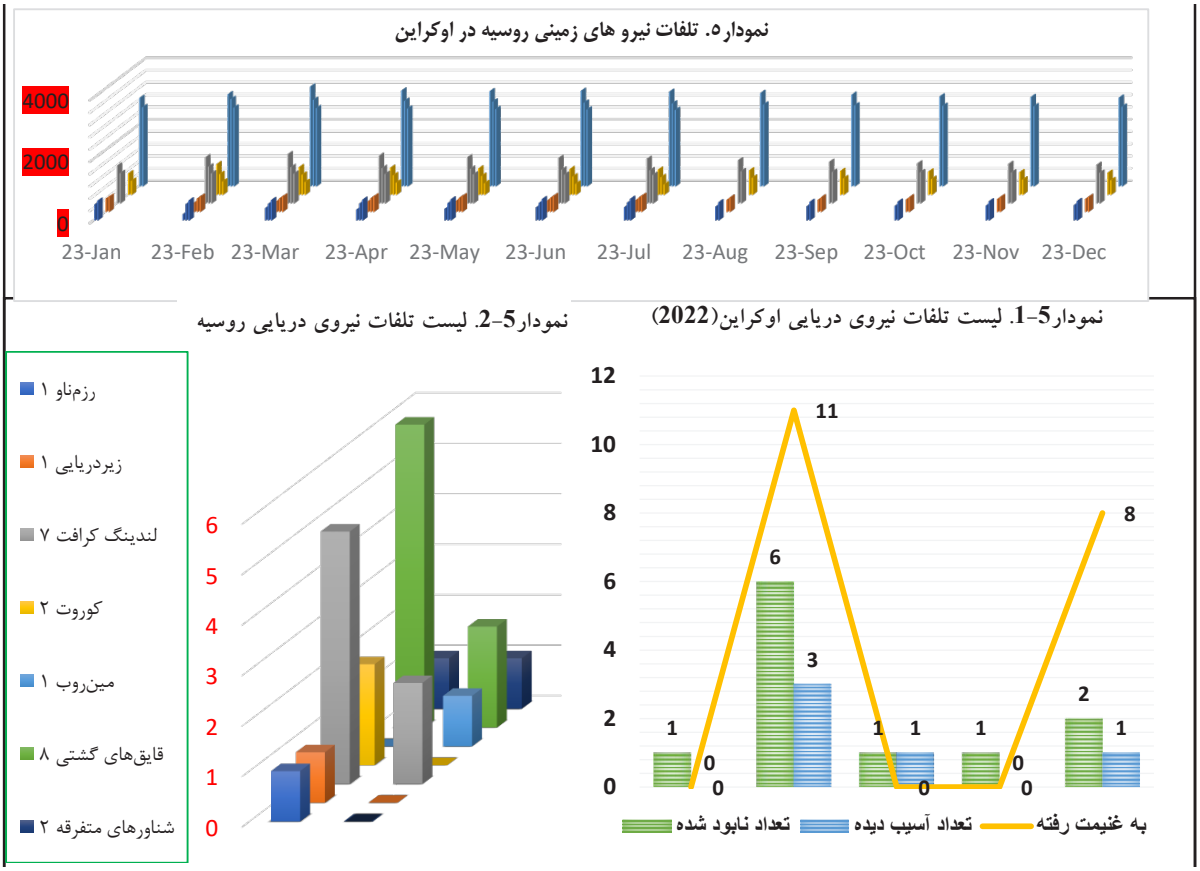
تثبیت کرد. در کاربرد عملی، عملیات روسیه در اوکراین از سال ۲۰۲۲ الگوی «نفوذ عمقی» را نشان داد. در مرحله آغازین، سامانه‌های «ایسکَندر-ام/کا، برد ۵۰۰ کیلومتر، دقت ۵ متر»، «کالیبر، برد ۲۵۰۰ کیلومتر، سرعت ۸ ماخ» و «خا-۱۰۱، برد ۲۵۰۰ کیلومتر، دقت ۳ متر) مراکز فرماندهی و شبکه‌های پدافند هوایی را هدف قرار دادند، که منجر به انهدام قابل توجه در زیرساخت‌های کلیدی در کی‌یف و خارکف شد. این فرایند، بخشی از ادغام آتش و اطلاعات است؛ جایی که شلیک دقیق با نرخ موفقیت را به طور بی سابقه ای افزایش داد (Arbatov & Oznobishchev, 2022: 33).

۵. الگوی جنگ دریایی و زمینی روسیه در پرتو شواهد تجربی از جنگ اوکراین

روسیه در جریان جنگ اوکراین، به‌طور همزمان درگیر دو بُعد مکمل و درعین‌حال متمایز از منازعه بوده است. جنگ دریایی و جنگ زمینی در مقیاس راهبردی. بررسی هم‌زمان این دو بُعد آشکار می‌سازد که الگوی عملیاتی روسیه را می‌توان ذیل مفهوم «جنگ چنددامنه‌ای» تحلیل کرد، جایی که فشار عملیاتی بر چند جبهه مختلف، هم ظرفیت‌های مادی و هم شبکه فرماندهی و پشتیبانی را به چالش می‌کشد. تا تاریخ ۱۳ اکتبر ۲۰۲۵، مجموع خسارات ثبت‌شده تجهیزات روسی در جنگ اوکراین به ۲۲۹۰۹ واحد رسیده است؛ از این میان، ۱۷۶۷۴ واحد نابود شده، ۹۲۳ واحد آسیب‌دیده، ۱۱۷۰ واحد رهاشده و ۳۱۴۲ واحد نیز توسط نیروهای اوکراینی به غنیمت گرفته شده‌اند. در این میان، تلفات در رده خودروهای زرهی رزمی شامل حدود ۱۳۲۹۳ واحد بوده که بخش اعظم آن، یعنی حدود ۱۰۳۵۴ واحد، به طور کامل منهدم شده است (Janovsky, 2025). علاوه برتعداد تلفات غیرانسانی ناشی از این ناکارآمدی‌ها،تا تاریخ ۱۰ اکتبر ۲۰۲۵، شمار کشته‌شدگان نظامی روسیه که اسامی‌شان ثبت شده، به ۱۳۵۱۰۰ نفر رسیده و تنها در بازه زمانی ۲۶ سپتامبر تا ۱۰ اکتبر ۲۰۲۵، ۲۴۸۵ مورد جدید به این فهرست اضافه شده است.

در نیمه اول سال ۲۰۲۵، روش‌های آماری حداقل ۵۲ هزار مرگ را تخمین زده‌اند، در حالی که سند منسوب به پروژه اوکراینی «می‌خواهم زندگی کنم» رقم بسیار بالاتری (۸۶۷۴۴ کشته) را گزارش می‌دهد که در سقف بالای دامنه پذیرفتنی قرار دارد. بخش ترکیب نیروها نشان می‌دهد که داوطلبان از سپتامبر ۲۰۲۴ تاکنون بزرگ‌ترین دسته کشته‌شدگان را تشکیل می‌دهند و تا ۱۰ اکتبر ۲۰۲۵، مرگ ۵٬۸۱۴ افسر تأیید شده است (Mediazona, 2025). بررسی تطبیقی این دو جبهه نشان می‌دهد که روسیه درگیر عملیات زمینی کلاسیک همراه با جنگ سایبری و اطلاعاتی است که همزمان باید با تهدیدهای مستمر در حوزه دریایی و زمینی روبه‌رو شود. از دست رفتن شناورهای پشتیبانی در دریای سیاه، کارایی زنجیره تأمین به جبهه‌های جنوبی، به‌ویژه در مناطق زاپروژیا و خرسون، را مستقیماً کاهش داده است. متقابلاً، ضعف نیروی زمینی در تثبیت سریع سرپل‌ها یا حفاظت از مناطق ساحلی، شانس بازیابی ابتکارعمل دریایی را حداقل در کوتاه‌مدت محدود کرده است. این وضعیت، جنگ اوکراین را به مصداق روشن نبرد چنددامنه‌ای تبدیل کرده است که در آن شکست یا نقصان در یک بُعد، به‌طور زنجیره‌ای بر ابعاد دیگر اثر می‌گذارد.

از دید نظریه جنگ شبکه‌محور، ناکارآمدی در لایه‌های لجستیک و پدافند ترکیبی چه در دریا و چه در خشکی باعث کاهش قابلیت هم‌زمان‌سازی نیروها و افزایش آسیب‌پذیری در برابر حملات فرصت‌طلبانه دشمن می‌شود که برای دقت بیشتر به بررسی نمودار۵. تلفات نیروهای زمینی روسیه در اوکراین، نمودار۵-۱. لیست تلفات نیروهای دریایی اوکراین و نمودار۵-۲. لیست تلفات نیروی‌های دریایی روسیه میپردازیم.



منبع: ترسیم نویسنده گان، برگرفته از داده‌های (Oryx, 2025)

در جریان درگیری‌های دریایی، نیروی دریایی روسیه متحمل خسارات قابل توجهی شد که بر قابلیت‌های عملیاتی آن تأثیر عمیقی گذاشت. به طور خاص، زیردریایی بی-۲۳۷ با نام «روستوف-نا-دونو» در یک حمله موشکی آسیب شدیدی دید که تعمیر آن از منظر اقتصادی توجیه‌پذیر نیست و عملاً این شناور را از رده خارج کرده است. علاوه بر این، ناوهای دوزیست از کلاس‌های روپوچا و تاپیر در بندر بردیانسک به طور کامل نابود شدند، که نشان‌دهنده آسیب‌پذیری پایگاه‌های ساحلی روسیه در برابر حملات دقیق است. این تلفات نه تنها بر ظرفیت حمل و نقل و پشتیبانی لجستیکی روسیه تأثیر گذاشته، بلکه بر استراتژی کلی دریایی آن در دریای سیاه سایه افکنده است.

در مقابل، نیروی دریایی اوکراین نیز با چالش‌های سنگینی روبرو شد و در مجموع ۳۵ شناور را از دست داد، که این رقم شامل تلفات قابل توجهی در ساختار دفاع ساحلی آن می‌شود. از جمله موارد برجسته، ناوچه «هتمن ساهایداچنی» بود که به منظور جلوگیری از تصرف توسط نیروهای روسی، به صورت خودغرق منهدم گردید - اقدامی استراتژیک که هرچند از دسترسی دشمن جلوگیری کرد، اما به قیمت از دست رفتن یک دارایی کلیدی تمام شد.

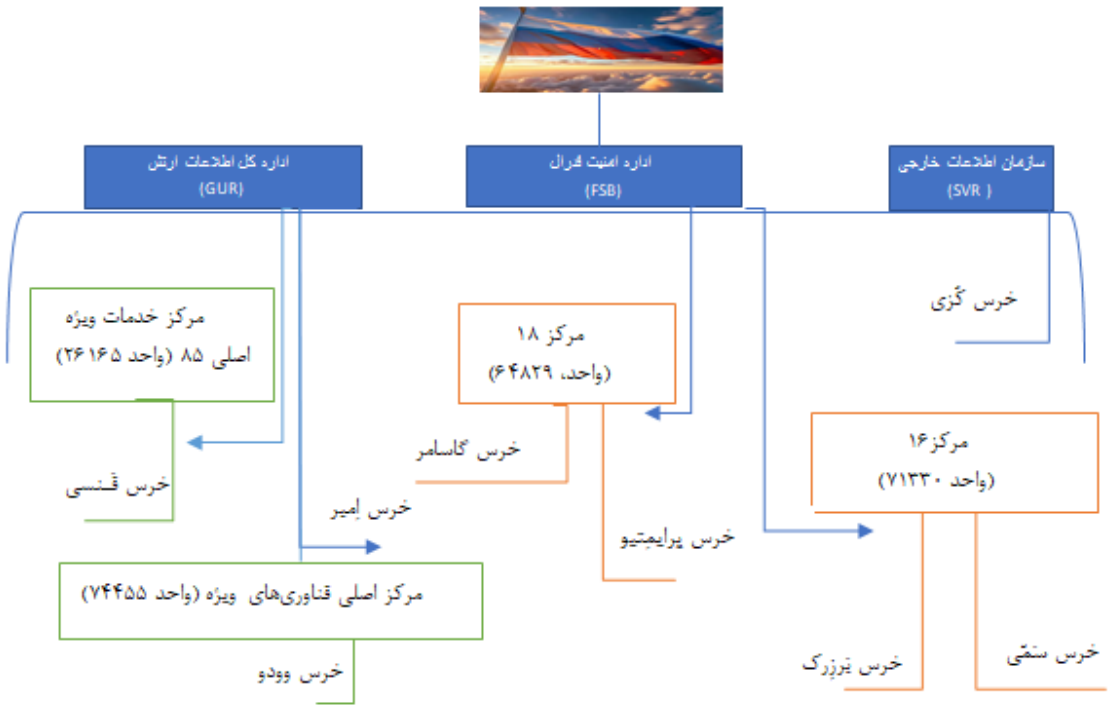
این الگوی تلفات دوجانبه، بر طبیعت نامتقارن جنگ دریایی در منطقه تأکید می‌ورزد و نشان می‌دهد که چگونه تاکتیک‌های دفاعی و پیشگیرانه می‌توانند بر توازن قدرت تأثیرگذار باشند. با وجود آنکه

روسیه در جریان نبرد با سامانه‌های نوین غربی در هر دو عرصه‌ی زمینی و دریایی متحمل خسارات قابل ملاحظه‌ای گردیده است، این امر لزوماً دلالت بر کارآمدی نازل یا ناتوانی عملیاتی آن ندارد. تاریخ حاکی است که حتی قدرت‌های بزرگ نیز در مواجهه با فناوری‌های جدید، دوره‌ای از سازگاری و بازتنظیم دکترین را تجربه می‌کنند؛ چنان‌که ارتش سرخ در ابتدای عملیات باباروسا، با وجود عقب‌نشینی‌های سنگین، نهایتاً ورق نبرد را بازگرداند. در مقیاس معاصر، استمرار توان روسیه در اجرای عملیات ترکیبی، حفظ برتری موشکی، و تطبیق ساختار نیروهایش نشان از ظرفیت انعطاف‌پذیر این کشور دارد. می توان گفت همانطور که در بخش مربوط به قدرت هوایی روسیه همچنان در استفاده از فناوری‌های نوین که «اس-۵۰۰» بارز ترین آن است؛ نسبت به اوکراین برتری دارد این امر توانسته بازدارندگی فناورانه‌ای را که پیش‌تر به آن اشاره شد، به خوبی حفظ کند.

۶. جنگ اطلاعاتی و سایبری

محتوای تصویری تولیدشده توسط دولت روسیه که هدف آن شکل‌دهی به ادراک عمومی و تثبیت مشروعیت سیاسی است، بخشی از جنگ شناختی و عملیات اطلاعاتی محسوب می‌شود که در چارچوب جنگ ترکیبی اهمیت دارد (Fedor & Fredheim, 2018: 161). بررسی ساختار اطلاعاتی این کشور نشان می‌دهد سه نهاد اصلی، ارکان محوری در اجرای عملیات سایبری و اطلاعاتی روسیه هستند. هر یک از این ارکان مأموریت‌ها و روش‌های تخصصی ویژه‌ای دارد که با هماهنگی یکدیگر، فشار مضاعفی بر سامانه‌های دفاع سایبری اوکراین وارد می‌کنند. در ادامه، به توصیف گروه‌های وابسته به این ارکان مطابق به شکل (۲) می‌پردازد.

شکل ۲: بازیگران سایبری روس



منبع: ترسیم نویسنده گان، برگرفته از داده های(CSIS)

همـان طـور کـه در شـکل آورده شـده اداره امنیـت فـدرال، سـرویس اطلاعـات خارجـی و اداره اصلـی اطلاعـات ستاد کل نیروهـای مسلح روسـیه، عملیـات سـایبری علیـه اوکرایـن و متحدانـش را از طریـق گروه‌هـای تخصصـی اجـرا می‌کننـد. گـروه خـرس گاسـامر وابسـته بـه مرکـز ۱۸(واحـد ۶۴۸۲۹) و فعـال از سـال ۲۰۱۷ اسـت کـه عملیـات فیشـینگ علیـه مقامـات بریتانیـا (فوریـه ۲۰۲۳) و زیرسـاخت‌های ارتباطـی اوکرایـن را انجـام می‌دهـد و روش‌هـای آن شـامل سـرورهای فرماندهـی و کنتـرل و حسـاب‌های جعلـی در شـبکه‌های اجتماعـی بـرای پنهان‌سـازی کدهـای مخـرب در محتـوای پربازدیـد می‌شـود. گـروه خـرس پرایمیتیـو وابسـته بـه مرکـز ۱۸ و فعـال از سـال ۲۰۱۳ اسـت کـه بیـش از ۵۰۰۰ حملـه بـه بیـش از ۱۰۰۰ سـامانه دولتـی اوکرایـن بـا تمرکـز بـر وزارتخانه‌هـای دفـاع و امنیـت اجـرا کـرده و روش‌هـای آن شـامل ضمیمه‌هـای آلـوده مایکروسـافت آفیـس، ایمیل‌هـای جعلـی از نهادهـای بین‌المللـی و بهره‌بـرداری از آسـیب‌پذیری‌های روز صفـر اسـت.

گـروه سـندورم وابسـته بـه (واحـد ۷۴۴۵۵) و شناخته‌شـده بـرای حـملات ویرانگـر ماننـد بدافـزار نوتپتیـا (شـبکه بـرق اوکرایـن، ۲۰۱۵-۲۰۱۶) و خسـارات میلیـارد دلاری، ۲۰۱۷) اسـت کـه تمرکـز فعلـی آن تخریـب سـامانه‌های انـرژی و ارتباطـی اوکرایـن و اخـتلال در لجسـتیک نظامـی می‌باشـد. در محیـط امنیتـی نویـن بین‌المللـی، مفهـوم کلاسـیک بازدارندگـی کـه ریشـه در پارادایـم جنـگ سـرد دارد، بـرای کاربسـت در فضـای سـایبر بـا چالش‌هـای سـاختاری مواجـه اسـت یکـی از موانـع بنیادیـن در ایـن عرصـه، مشـکل انتسـاب اسـت کـه بـه دلیـل ماهیـت ناشـناسِ حـملات، امـکان اقـدام تلافی‌جویانـه و در نتیجـه منطـق «بازدارندگـی از طریـق مجـازات» را تضعیـف می‌کنـد بـا ایـن وجـود، از آنجـا کـه دولت‌هـا بـه عنـوان بازیگـران اصلـی نظـام بین‌الملـل در شـبکه‌ای از وابسـتگی متقابـل قـرار دارنـد و خـود را ملـزم بـه حفـظ نظـم بین‌المللـی می‌داننـد، همچنـان در برابـر سـازوکارهای بازدارنـده تأثیرپذیرنـد. از منظـر اسـتراتژیک، فرمول‌بنـدی یـک بازدارندگـی مؤثـر (بـه ویـژه در برابـر تهدیـدات سـایبری قدرت‌هـای رقیـب ماننـد روسـیه و چیـن علیـه زیرسـاخت‌های حیاتـی، نیازمنـد اتخـاذ رویکـرد بازدارندگـی متقاطـع اسـت؛ بـه ایـن معنـا کـه پاسـخ دولـت هـدف نبایـد لزومـاً بـه فضـای سـایبر محـدود شـود، بلکـه می‌توانـد شـامل بهره‌گیـری از تمامـی ابزارهـای دیپلماتیـک، اطلاعاتـی و نظامـی در سـایر عرصه‌هـا باشـد (Dehghani, 2018:132).

نتیجه‌گیری

پژوهـش حاضـر بـا تمرکـز بـر همگرایـی هـوش مصنوعـی، شبکه‌سـازی تسـلیحات و معمـاری پیشـرفته سـامانه‌های پدافنـد راهبـردی روسـیه در بسـتر جنـگ اوکرایـن، کوشـید چارچوبـی تحلیلـی بـرای تبییـن بازدارندگـی فناورانـه ارائه کنـد. یافته‌هـا آشـکار سـاخت کـه روسـیه توانسـته اسـت بـا تلفیـق سـه مؤلفـه کلیـدی، یعنـی کنتـرل دیجیتـال در زمـان واقعـی، تـوان پهپـادی و قابلیت‌هـای موشـکی پیشـرفته، شـکاف فنـاوری خـود بـا غـرب را در سـطوح عملیاتـی و تاکتیکـی کاهـش دهـد. ایـن گـذار، بیانگـر تغییـر جهـت از بازدارندگـی سـنتی مبتنـی بـر نیـروی هسـته‌ای بـه سـوی برتـری میدانـی الگوریتمـی و داده‌محـور اسـت؛ سـاختاری کـه ریشـه در معمـاری ترکیبـی فرماندهـی، کنتـرل، ارتبـاط، رایانـه، اطلاعـات، شناسـایی و نظـارت هوشـمند دارد. مطالعـه سـامانه‌های روسـی در جنـگ اوکرایـن نشـان داد مزیـت روسـیه بیـش از آنکـه در برتـری سـخت‌افزاری باشـد، در نحـوه یکپارچه‌سـازی جریان‌هـای داده چندمنبعـی، هوشمندسـازی حلقـه فرمـان تـا آتـش و هم‌افزایـی میـان سـامانه‌های تهاجمـی و دفاعـی نهفتـه

است؛ به این معنا که دفاع در خدمت تهاجم عمل می‌کند. با این حال، نتایج نشان می‌دهد که اتکای بیش‌ازحد به زیرساخت‌های فناورانه بدون مقاوم‌سازی اطلاعاتی و سایبری می‌تواند به آسیب‌پذیری راهبردی منجر شود.

در سطح کلان، پیامدهای این پژوهش هم برای سیاست‌گذاری دفاعی و هم برای نظریه‌پردازی در حوزه بازدارندگی قابل توجه است. از دیدگاه عملی، تجربه روسیه در طراحی و بهره‌گیری از معماری تسلیحاتی ترکیبی می‌تواند الگوی مؤثری برای کشورهایی با محدودیت بودجه یا زیر فشار تحریم‌های نظامی باشد. از منظر نظری نیز، مدل پیشنهادی «بازدارندگی چنددامنه‌ای فعال» افقی تازه برای تحلیل رفتار نظامی قدرت‌های میان‌رده و بزرگ در منازعات فرسایشی بلندمدت ترسیم می‌کند. در نهایت، مرور داده‌های میدانی از منابع تصویری و آماری و گزارش‌های مشترک نشان داد که پیوند میان سامانه‌های داده‌محور و تصمیم‌گیری الگوریتمی به‌طور مستقیم با کاهش تلفات انسانی و تجهیزاتی و افزایش دقت عملیاتی ارتباط دارد. استمرار این روند و شتاب در ادغام هوش مصنوعی با زیرساخت‌های تسلیحاتی گواه آن است که آینده بازدارندگی بیش از هر زمان به مهارت در طراحی شبکه‌های یکپارچه، مدیریت داده در محیط‌های متخاصم و انطباق سازمانی با تهدیدات نوظهور وابسته است. بدین ترتیب، بازدارندگی آینده بیش از اینکه بر پایه انباشت جنگ‌افزار استوار باشد، بر اساس تلفیق انسان، ماشین و داده شکل خواهد گرفت؛ بازدارندگی‌ای پویا، هوشمند و خودیادگیرنده.

منابع

- دهقانی، ع. ا. (۱۳۹۷)، بازدارندگی سایبری در امنیت جهانی: تهدیدات سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا. فصلنامه رهیافت‌های سیاسی و بین‌المللی. قابل دسترس در: https:// piaj.sbu.ac.ir/article_99570.html (تاریخ دسترسی: ۶ اردیبهشت ۱۴۰۵).
- کولایی، ا. و زنگنه، س. (۱۴۰۳)، تأثیر جنگ اوکراین بر روابط ایران و روسیه. فصلنامه رهیافت‌های سیاسی و بین‌المللی. قابل دسترس در: https://doi.org/10.48308/piaj.2024.233313.1442 (تاریخ دسترسی: ۶ اردیبهشت ۱۴۰۵).
- نوری، ع. (۱۳۹۸)، بررسی ابعاد سیاست‌های مهار و بازدارندگی در روابط روسیه و آمریکا و تحلیل پیامدهای آن بر منافع و امنیت ایران. فصلنامه سیاست جهانی، دوره ۸، شماره ۲، صص. ۲۴۷-۲۹۰. قابل دسترس در: https://doi.org/10.22124/wp.2019.3702 (تاریخ دسترسی: ۶ اردیبهشت ۱۴۰۵).
- توکل، ا. (۱۳۸۵)، جنگ شبکه‌محور. فصلنامه علوم و فناوری نظامی، شماره ۶، صص. ۵۹-۷۶. (تاریخ دسترسی: ۱۸ آبان ۱۴۰۳).
- باقری، ر. (۱۴۰۴)، کاربردها و فرصت‌های هوش مصنوعی در عصر اطلاعات و تحلیل داده‌ها. ارائه در کنفرانس، دانشکده علوم اداری و اقتصادی، دانشگاه فردوسی مشهد، مشهد، ایران.

Refrences

- Allen, G. and Chan, T. (2017), Artificial Intelligence and National Security, Belfer Center

for Science and International Affairs, Harvard Kennedy School. Available at: https://www.belfercenter.org/publication/artificial-intelligence-and-national-security (Accessed on: 20/12/2024).
- Al Jazeera (2023), "Russia says Ukraine sea drones destroyed in failed attack on Crimea bridge" Available at: https://www.aljazeera.com/news/2023/9/2/russia-says-ukraine-sea-drones-destroyed-in-failed-attack-on-crimea-bridge, (Accessed on: 2/9/2023).
- Anderson, C. (2025), "S-500 Missile System: Russia's Next-Gen Air and Missile Shield", DefenseFeeds, Available at: https://defensefeeds.com/military-tech/army/air-defense-systems/s-500-missile-system, (Accessed on: 20/11/2025).
- Arbatov, A. and Oznobishchev, S. (Eds.) (2022), Russia: Arms Control, Disarmament and International Security, Moscow: IMEMO RAS & SIPRI.
- Army Recognition (2022), "Russia uses Forpost R armed drone with guided missile to destroy rocket launcher of Ukrainian army", Army Recognition, Available at: https://www.armyrecognition.com/russia_ukraine_war_2022/russia_uses_forpost-r_armed_drone_with_guided_missile_to_destroy_rocket_launcher_of_ukrainian_army.html, (Accessed on: 29/12/2024).
- Ashley, R. P., Jr. (2019), "Russian and Chinese nuclear modernization trends: Remarks at the Hudson Institute", Defense Intelligence Agency, Available at: https://www.dia.mil/Articles/Speeches-and-Testimonies/Article/1859890, (Accessed on: 8/12/2024).
- Alberts, D. S., Garstka, J. J. and Stein, F. P. (1999), Network centric warfare: Developing and leveraging information superiority (2nd ed., revised), Washington, D.C.: U.S. Department of Defense C4ISR Cooperative Research Program, Available at: https://apps.dtic.mil/sti/tr/pdf/ADA406255.pdf, (Accessed on: 20/8/2025).
- Bachmann, S.-D. and Gunneriusson, H. (2015), "Hybrid wars: The 21st-century's new threats to global peace and security", Scientia Militaria, South African Journal of Military Studies, Vol. 43, No. 1, pp. 77-98. (doi:10.5787/43-1-1110).
- Baqeri, R. (2025), "Applications and opportunities of artificial intelligence in the age of information and data analytics", Conference presentation, Faculty of Administrative and Economic Sciences, Ferdowsi University of Mashhad, Mashhad, Iran [in Persian].
- Baylis, J., Wirtz, J. J. and Gray, C. S. (Eds.) (2022), Strategy in the contemporary world (6th ed.), Oxford: Oxford University Press.
- BBC News (2023), "Ukraine war: Map of Russian control and claimed advances", BBC, Available at: https://www.bbc.com/news/world-europe-60506682, (Accessed on: 20/11/2024).
- Bendett, S. (2024), "The role of AI in Russia's confrontation with the West", Center for a New American Security, Available at: https://ai4gs.org/wp-content/uploads/2024/05/Russia-AI_2024-final.pdf, (Accessed on: 20/12/2025).
- Bielieskov, M. (2025), "Putin's escalating air offensive is overwhelming Ukraine's defenses", Atlantic Council, Available at: https://www.atlanticcouncil.org/blogs/ukrainealert/putins-escalating-air-offensive-is-overwhelming-ukraines-defenses/, (Accessed on: 20/12/2025).
- Boyd, J. R. (1976), "Destruction and creation", Self-published manuscript, Available at: https://www.coljohnboyd.com/static/documents/1976-09-03__Boyd_John_R__Destruction_and_Creation.pdf, (Accessed on: 8/11/2024).
- Carlin, M. (2024), "S-500: Russia's new air defense that could win a war against NATO?",

The National Interest, Available at: https://nationalinterest.org/blog/buzz/s-500-russias-new-air-defense-could-win-war-against-nato-211109, (Accessed on: 10/12/2025).
- Cranny-Evans, S. (2025), "Unmanned advantage: Russia's drones and the fight for ISTAR in Ukraine", European Security & Defence, Available at: https://euro-sd.com/2025/04/articles/43651/unmanned-advantage-russias-drones-and-the-fight-for-istar-in-ukraine/, (Accessed on: 20/12/2025).
- Deb, S. (2021), "Explained: How S400 air defence system works?", DefenceXP Premium, Available at: https://defencexp.com/indian-air-force/explained-how-s400-air-defence-system-works/, (Accessed on: 11/8/2024).
- Dehghani, A. A. (2018). Cyber deterrence in global security: Russian and Chinese cyber threats against U.S. critical infrastructure. Political and International Approaches, Available at: https://piaj.sbu.ac.ir/article_99570.html (Accessed on: 26 /4/ 2026).
- Fedor, J. and Fredheim, R. (2018), ""We need more clips about Putin, and lots of them:" Russia's state commissioned online visual culture", Nationalities Papers, Vol. 45, No. 2, pp. 161–181. (doi:10.1080/00905992.2016.1266608).
- Giles, K. (2017), "Assessing Russia's reorganized and rearmed military", Carnegie Endowment for International Peace, Available at: https://carnegieendowment.org/2017/05/04/assessing-russia-s-reorganized-and-rearmed-military-pub-69853, (Accessed on: 20/10/2024).
- Janovsky, J. and Mitzer, S. (2025), "Attack On Europe: Documenting Equipment Losses In The Russian Ukrainian War", Oryx Blog, Available at: https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html, (Accessed on: 10/12/2025).
- Kallenborn, Z. (2022), "Russia may have used a killer robot in Ukraine. Now what?", Bulletin of the Atomic Scientists, Available at: https://thebulletin.org/2022/03/russia-may-have-used-a-killer-robot-in-ukraine-now-what/, (Accessed on: 20/11/2024).
- Korshak, S. (2024), "ATACMS comes out on top versus Russia's S-500 anti-missile system", Kyiv Post, Available at: https://www.kyivpost.com/post/34782, (Accessed on: 20/11/2025).
- Kuzio, T. (2022), "Why Russia invaded Ukraine", Horizons: Journal of International Relations and Sustainable Development, No. 21, pp. 40–47, Available at: https://www.cirsd.org/sr-latn/horizons/horizons-summer-2022-issue-no.21/why-russia-invaded-ukraine, (Accessed on: 10/12/2024).
- Koolaee, E. and Zangeneh, S. (2024), "The impact of the Ukraine war on Iran and Russia's relations", Political and International Approaches, Available at: https://piaj.sbu.ac.ir/article_104385.html (Accessed on: 26 /4/ 2026).
- Luddy, J. (2005), "The challenge and promise of network-centric warfare", Lexington Institute, Available at: https://www.lexingtoninstitute.org/wp-content/uploads/challenge-promise-network-centric-warfare.pdf, (Accessed on: 8/11/2024).
- Mankoff, J. (2022), "Russia's war in Ukraine. Identity, history and conflict", SIRIUS – Zeitschrift für Strategische Analysen, Vol. 6, No. 4, pp. 392–395. (doi:10.1515/sirius-2022-4008).
- McCarthy, J. (2007), "What is artificial intelligence?", Stanford University, Available at: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf, (Accessed on: 4/11/2024).
- Mediazona, and BBC Russian Service (2025), "Casualties of the Russian military in the war with Ukraine", Meduza (statistical estimate), Available at: https://en.zona.media/article/2025/10/10/casualties_eng-trl, (Accessed on: 20/12/2025).
- Nouri, A. (2019), "Investigating the Dimensions of Containment and Deterrence Policies in

Russia-US Relations and Analyzing their Impacts on Iran's Interests and Security", World Politics, 8(2), pp. 247-290, Available at: https://doi.org/10.22124/wp.2019.3702(Accessed on: 26 /4/ 2026).
- Russell, S. and Norvig, P. (2021), Artificial intelligence: A modern approach (4th ed.), Hoboken, NJ: Pearson.
- Sloan, E. C. (2016), Modern military strategy: An introduction (2nd ed.), London: Routledge. (doi:10.4324/9781315740034).
- Sputnik (2016), "Russia's S 500 missile system to begin tests this year", Defaiya, Available at: https://www.defaiya.com/news/Products/Products/2016/02/04/russia-s-s-500-missile-system-to-begin-tests-this-year, (Accessed on: 12/11/2024).
- Sutton, R. S. and Barto, A. G. (2015), Reinforcement Learning: An Introduction (2nd ed., in progress), Cambridge, MA: MIT Press, Available at: https://web.stanford.edu/class/psych209/Readings/SuttonBartoIPRLBook2ndEd.pdf, (Accessed on: 11/9/2024).
- Sutyagin, I. (2015), "Russian forces in Ukraine", Royal United Services Institute, Available at: https://rusi.org/explore-our-research/publications/briefing-papers/russian-forces-ukraine, (Accessed on: 11/12/2024).
- Tavakkol, A. (2006), "Network Centric Warfare", Quarterly Journal of Military Science and Technology, No. 6, pp. 59–76, Available at: https://www.magiran.com/paper/10240, (Accessed on: 8/11/2024) [in Persian].
- Wang, P. (2019), "On defining artificial intelligence", Journal of Artificial General Intelligence, Vol. 10, No. 2, pp. 1–37. (doi:10.2478/jagi-2019-0002).
- Williams, I. (2023), "Putin's missile war: Russia's strike campaign in Ukraine", Center for Strategic and International Studies (CSIS) Missile Defense Project, Available at: https://www.csis.org/analysis/putins-missile-war, (Accessed on: 8/11/2024).
- Withington, T. (2024), "Russia has just one S 500 air-defense system: It arrived in Crimea amid a storm of Ukrainian rockets", Royal United Services Institute (RUSI), Available at: https://www.rusi.org/news-and-comment/in-the-news/russia-has-just-one-s-500-air-defense-system-it-arrived-crimea-amid-storm-ukrainian-rockets, (Accessed on: 20/12/2025).