International journal of Central Eurasia Studies
Scopus
Homepage: jcep.ut.ac.ir
Online ISSN: 2345-3117

Russian Information Warfare: Explaining Defense Logic, Roots, and Strategies

Meisam Belbasi [1] and Ahmad Ghojavand [2]

1. Assistant Professor, Department of Islamic Studies, Faculty of Theology, University of Mazandaran, Babolsar, Iran.
Email: M.Belbasi@umz.ac.ir (Corresponding Author)
2. M.A. in Media Management, Islamic Republic of Iran Broadcaster University, Tehran, Iran.

Article Info.

Article Type:
Research Paper

Article History:
Received:
17 August 2025
Revised:
23 November 2025
Approved:
22 January 2026
Published Online:
18 February 2026

Keywords:
InformationWarfare,
Narrative Analysis,
Strategic Culture,
Reflexive Control,
Cognitive Warfare,
NATO,
Russia.

ABSTRACT

This study challenges the dominant narrative of Russia's unilateral aggression by examining the strategic, historical, and doctrinal logic that underlies its information warfare. The central question is to what extent these activities can be interpreted as a "defensive counter-narrative" in response to Western policies and discourses. The main premise is that Russia's intelligence strategy is not an act of unprovoked aggression but rather an asymmetric, defensive response to perceived geopolitical and intelligence threats from the West. The research was conducted using qualitative narrative analysis and drawing on a wide range of sources, including official and declassified documents from the US and Russian governments, military doctrines, reports from Western think tanks, and academic studies on media bias. The findings show that Russia's strategy is rooted in a "strategic culture of encirclement" inherited from the Cold War and evolved through the integration of concepts such as "cognitive warfare" and "reflexive control". From Moscow's perspective, tools such as the use of "frozen conflicts" and information tactics within the framework of "active defense" are employed to counter Western efforts to undermine Russian sovereignty through soft power tools. The study concludes that the Russian-Western intelligence confrontation constitutes a self-reinforcing cycle of strategic misunderstandings, in which each side interprets its actions as defensive while viewing the actions of the other as offensive. This "war of narratives" is less a competition over objective truth and more a clash of opposing strategic cultures, where narratives themselves become the primary weapons of conflict.

Cite this article: Belbasi. M. and A. Ghojavand (2026), "Russian Information Warfare: Explaining Defense Logic, Roots and Strategies", **Central Eurasia Studies**, Vol. 18, No. 2, pp. 1-33.

http//doi.org/10.22059/JCEP.2026.400885.450349

 Publisher: University of Tehran

Introduction: In the twenty-first century, information has emerged as an autonomous domain of conflict, functioning as a strategic battlefield rather than merely a supplementary instrument for political or military action. Russia's confrontation with the West, particularly the United States and NATO, illustrates this transformation clearly. The dominant Western narrative depicts Russia as an aggressive actor employing propaganda, cyberattacks, troll networks, and disinformation to undermine democratic institutions, exploit social divisions, and expand geopolitical influence. From this standpoint, Moscow's actions appear as coordinated assaults on the liberal international order. Yet such interpretations often overlook the strategic logic shaping Russian behavior. From the Kremlin's perspective, many asymmetric intelligence and information activities constitute defensive responses to perceived existential threats. NATO enlargement, "color revolutions" and the securitization of the Euro-Atlantic environment reinforce a deeply embedded sense of encirclement within Russian strategic culture. Cold War legacies-particularly Soviet "active measures" and the concept of "reflexive control"-continue to frame information operations as tools for protecting sovereignty and identity rather than instruments of pure aggression. This study challenges prevailing Western assumptions by tracing the historical, doctrinal, and strategic foundations of Russian information warfare and arguing that these campaigns often operate as defensive counter-narratives.

Research question: The main question asks to what extent Russia's information warfare can be interpreted as a defensive counter-narrative responding to Western policies and discourses, rather than as unprovoked aggression. Existing literature focuses predominantly on how Russia conducts cyber operations, disinformation campaigns, and media manipulation, while paying limited attention to the underlying motivations. This study shifts the focus toward the doctrinal foundations, security perceptions, and cultural-historical roots that shape Moscow's information strategy.

Research hypothesis: Russian information warfare reflects a defensive, asymmetric strategy rooted in a siege mentality and post–Cold War insecurity, employing defensive, reflexive control, cyber,

and narrative tools to deter threats and offset weaknesses.

Methodology and theoretical framework: This research employs qualitative narrative analysis to examine how Russian intelligence and information activities are interpreted, justified, and normalized. Unlike quantitative approaches that emphasize frequency, scale, or network metrics, narrative analysis reveals meaning, structure, and function in texts produced by state and non-state actors. The corpus includes doctrines, official statements, analytical reports, and policy documents on Russian information operations from 2014 to 2025, alongside Western responses. Data collection relies on documentary and library-based sources. The theoretical framework integrates strategic culture theory, particularly Snyder's emphasis on historical vulnerability, distrust of the West, and the "besieged fortress" mindset, with Jervis's security dilemma, explaining how defensive actions may be misinterpreted as offensive, thereby generating escalation.

Results and discussion: The findings indicate that Russian information warfare constitutes a coherent and historically embedded strategy rather than opportunistic aggression. It operates across three interrelated dimensions: historical continuity, doctrinal evolution, and operational practice. Historically, Russia has long regarded information as central to statecraft; Soviet-era institutions normalized manipulation as a permanent feature of conflict. Experiences such as the Chechen wars reinforced the importance of narrative dominance, demonstrating how military success could be undermined by hostile framing. Doctrinal evolution after Georgia (2008) and Ukraine (2014) formalized information as a critical battlefield, emphasizing reflexive control and cognitive targeting. The doctrine of "active defense" legitimizes preventive measures abroad as homeland protection, explaining why actions perceived as aggressive in the West are understood in Moscow as deterrence. Operationally, Russia employs a dense ecosystem of state agencies, intelligence services, media outlets, online platforms, and cyber units, using techniques such as information preemption, narrative flooding, hacking, and exploitation of frozen conflicts. These practices are anchored in a strategic narrative portraying Russia as a victim of Western encirclement. The analysis reveals a self-reinforcing dynamic: each side views its own

behavior as defensive while interpreting the other as hostile, deepening mistrust and sustaining escalation.

Conclusion: Russia's information warfare is best understood as a defensive counter-narrative rooted in historical vulnerability, siege culture, and asymmetric adaptation. Although tactics such as cyber operations and disinformation often appear offensive, they are framed as mechanisms to preserve sovereignty and deter perceived threats. Paradoxically, this defensive logic reproduces the security dilemma it seeks to escape, as mutual suspicion entrenches escalation. By integrating strategic culture and narrative analysis, this study moves beyond simplistic offensive–defensive binaries and underscores the importance of addressing narrative dynamics in efforts toward de-escalation.

Keywords: Information Warfare, Narrative Analysis, Strategic Culture, Reflexive Control, Cognitive Warfare, NATO, Russia.

مجله بین‌المللی مطالعات اوراسیای مرکزی
Scopus
Homepage: jcep.ut.ac.ir
شاپا الکترونیکی: ۲۳۴۵-۳۱۱۷

جنگ اطلاعاتی روسیه؛ تبیین منطق دفاعی، ریشه‌ها و راهبردها

میثم بلباسی[۱] و احمد قُجاوند[۲]

۱. استادیار، گروه معارف اسلامی، دانشکدهٔ الهیات، دانشگاه مازندران، بابلسر، ایران

نویسندهٔ مسئول: M.Belbasi@umz.ac.ir

۲. کارشناسی ارشد مدیریت رسانه، دانشگاه صداوسیما، تهران، ایران

اطلاعات مقاله

نوع مقاله: علمی‌پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۵/۲۶

تاریخ بازنگری: ۱۴۰۴/۰۹/۰۲

تاریخ پذیرش: ۱۴۰۴/۱۱/۰۲

تاریخ انتشار برخط: ۱۴۰۴/۱۱/۲۹

واژگان اصلی:
جنگ اطلاعاتی،
تحلیل روایی،
فرهنگ راهبردی،
کنترل انعکاسی،
جنگ شناختی،
ناتو،
روسیه.

چکیده

در این نوشتار با بازاندیشی در روایت رایج در مورد سرشت کنش‌های روسیه در برابر کشورهای غربی و منافع آن‌ها، منطق راهبردی، تاریخی و مبنای نظری حاکم بر اقدام‌های این کشور در عرصهٔ جنگ اطلاعاتی را بررسی می‌کنیم. پرسش اصلی این است که این اقدام‌های روسیه در جنگ اطلاعاتی، چقدر می‌تواند به‌عنوان «ضدروایت دفاعی» در برابر سیاست‌ها و روایت‌های غربی تفسیر شود. فرضیهٔ اصلی این است که راهبرد اطلاعاتی روسیه نه تهاجمی بی‌دلیل، بلکه پاسخی نامتقارن و دفاعی به تهدیدهای ژئوپلیتیکی و اطلاعاتی ادراک‌شده از سوی غرب است. این نوشتار با روش تحلیل روایی کیفی و بهره‌گیری از منابع گسترده شامل اسناد رسمی و از طبقه‌بندی خارج‌شده دولت‌های آمریکا و روسیه، آیین‌های نظامی، گزارش‌های اندیشکده‌های غربی و مطالعات دانشگاهی در مورد سوگیری رسانه‌ای انجام شده است. یافته‌ها نشان می‌دهد راهبرد روسیه در جنگ اطلاعاتی ریشه در «فرهنگ راهبردی محاصره» دارد که از دوران جنگ سرد باقی مانده و با مفاهیم نوینی مانند «جنگ شناختی» و «کنترل بازتابی» تکامل یافته است. ابزارهایی مانند بهره‌گیری از «درگیری‌های منجمد» و تاکتیک‌های اطلاعاتی در چارچوب «دفاع فعال» به کار گرفته می‌شوند تا از دیدگاه مسکو، مانع تلاش سازمان‌یافتهٔ غرب برای تضعیف حاکمیت روسیه به‌وسیلهٔ ابزارهای نرم شوند. نتیجهٔ نوشتار این است که رویارویی اطلاعاتی روسیه و غرب چرخهٔ خودتقویت‌شونده از سوءبرداشت‌های راهبردی را شکل می‌دهد. چرخه‌ای که در آن، هر طرف اقدام‌های خود را دفاعی و اقدام‌های طرف مقابل را تهاجمی می‌داند. این «جنگ روایت‌ها» بیش از اینکه نبرد بر سر حقیقت باشد، بازتاب رویارویی دو فرهنگ راهبردی متضاد است که در آن، روایت‌ها خود به سلاح اصلی درگیری تبدیل شده‌اند.

استناد: بلباسی، میثم و احمد قُجاوند (۱۴۰۴)، «جنگ اطلاعاتی روسیه؛ تبیین منطق دفاعی، ریشه‌ها و راهبردها»، **مطالعات اوراسیای مرکزی**، دوره ۱۸، شماره ۲، صص. ۳۳-۱

http//doi.org/ 10.22059/JCEP.2026.400885.450349

ناشر: دانشگاه تهران

مقدمه

در دهه‌های اخیر، فضای اطلاعاتی به عرصه‌ای تعیین‌کننده در رقابت‌های ژئوپلیتیک تبدیل شده که رویارویی روسیه و غرب نمونهٔ شاخص آن است. گفتمان رایج غربی، روسیه را بازیگری تهاجمی تصویر می‌کند که با ابزارهایی مانند مهندسی ادراک و حمله‌های سایبری، درپی بی‌ثبات‌کردن نظام‌های دموکراتیک است (Treyger, Cheravitch, & Cohen, 2022). در این رویکرد، اقدام‌های مسکو بیشتر تهدیدی مستقیم شناخته شده و انگیزه‌های احتمالی دفاعی آن نادیده گرفته می‌شود. در برابر، کرملین این اقدام‌ها را نه تهاجم، بلکه پاسخی دفاعی به تهدیدهایی مانند گسترش ناتو و در بستر «فرهنگ راهبردی محاصره» می‌داند. در این زمینه، مفاهیمی مانند «کنترل بازتابی» ابزاری برای موازنهٔ نامتقارن با غرب هستند. پژوهش‌های پیشین بیشتر بر «چگونگی» تاکتیکی متمرکز بوده و کمتر به «چرایی» راهبردی پرداخته‌اند (Zori, 2025)؛ بنابراین جای خالی مدلی که ریشه‌های تاریخی و آیین روسیه را یک «ضدروایت دفاعی» تبیین کند، احساس می‌شود.

در این نوشتار با روش تحلیل روایی کیفی، منطق راهبردی اقدام‌های روسیه را به‌عنوان یک «ضدروایت دفاعی» واکاوی می‌کنیم. نوآوری این نوشتار در سه محور است: نخست، تغییر زاویهٔ دید رایج و تفسیر کنش‌های روسیه به‌عنوان پاسخی عقلانی به محیط خصمانه. دوم، تبیین آیین روسیه بر پایهٔ مفاهیم «کنترل بازتابی» و «فرهنگ راهبردی محاصره». سوم، تحلیل این رویارویی نه به‌عنوان نبردی یک‌طرفه، بلکه چرخه‌ای از سوءبرداشت‌های متقابل میان دو فرهنگ راهبردی.

پیشینهٔ پژوهش

در محور نخست، شمار قابل توجهی از پژوهش‌ها بر نقش روایت‌ها و ابزارهای رسانه‌ای در درگیری میان روسیه و غرب تمرکز کرده‌اند. قربانی شیخ‌نشین و احمدی‌نژاد (۱۴۰۲) در «تحلیل روایی بحران اوکراین؛ تقابل روایت‌ها و پادروایت‌ها» با اتکا به تحلیل گفتار رهبران دو طرف نشان داده‌اند که تقابل روایت و پادروایت در تثبیت قطب‌بندی و تداوم بحران نقش محوری داشته و هر طرف از روایت‌سازی برای مشروعیت‌بخشی به مواضع خود بهره برده است. سیمبر و رضاپور (۱۳۹۷) در «قدرت نرم روسیه در خارج نزدیک؛ ابزارها و چالش‌ها» منابع قدرت نرم روسیه مانند زبان، رسانه و کلیسا را شناسایی کرده‌اند. آنان استدلال می‌کنند که اقدام‌های تهاجمی مسکو سبب تضعیف جذابیت این منابع در کشورهای همسایه شده است. لطفیان (۱۴۰۴) در «تهدیدهای هسته‌ای در جنگ اوکراین و تأثیر افکار عمومی روسیه بر سیاست بازدارندگی هسته‌ای کرملین»، بازخوانی تهدیدهای هسته‌ای در جنگ اوکراین و تأثیر

افکار عمومی، تضعیف تابوی هسته‌ای و تأثیر دیدگاه‌های شهروندان و نخبگان روسیه بر سیاست بازدارندگی و علامت‌دهی هسته‌ای کرملین در جریان جنگ اوکراین را بررسی می‌کند. دهقانی‌فیروزآبادی و امیری (۱۳۹۷) در «زمینه‌یابی سه‌وجهی جایگاه قدرت نرم در سیاست خارجی روسیه (۲۰۱۹-۲۰۰۰)»، با واکاوی ابعاد تاریخی، روایی و اسنادی، روند جدی‌ترشدن کاربست قدرت نرم در سیاست خارجی روسیه در سال‌های ۲۰۰۰ تا ۲۰۱۹ را تحلیل می‌کنند. خان‌محمدی (۱۴۰۱) در «جنگ اطلاعاتی و شناختی روسیه و تأثیرگذاری اجتماعی و افکار عمومی؛ مطالعهٔ موردی اوکراین»، نشان داده است که ریشه‌های جنگ اطلاعاتی روسیه به آیین امنیتی اطلاعاتی دههٔ ۱۹۹۰ بازمی‌گردد و استفاده از رسانه‌های اجتماعی، هویت‌های جعلی و هدف‌گیری خرد بخش‌های عملیاتی، اساسی این راهبرد را تشکیل می‌دهند.

در عرصهٔ بین‌المللی، جونز[1] (۲۰۲۵) در «جنگ سایه‌ای روسیه علیه غرب» تصویری تهاجمی از عملیات اطلاعاتی روسیه ارائه می‌دهد و بر شبکه‌ای و سایه‌واربودن آن تأکید می‌کند؛ این روایت نمونه‌ای از برداشت غربی است که این مقاله آن را نقد می‌کند. زولمن[2] (۲۰۲۴) نیز در «جنگ پیش‌بینی‌شده: چگونه رسانه‌های جریان اصلی غرب، گسترش ناتو به‌سوی شرق را به‌عنوان یکی از عوامل مؤثر در تهاجم ۲۰۲۲ روسیه به اوکراین نادیده گرفتند» نشان می‌دهد رسانه‌های جریان اصلی غربی نقش گسترش ناتو در تشدید بحران اوکراین را حذف کرده و بدین‌سان روایتی یک‌سویه علیه روسیه تولید کرده‌اند. فیشر[3] (۲۰۲۳) در «عینیت و سوگیری رسانه‌ای در پوشش غربیِ مناقشه روسیه-اوکراین» با تحلیل محتوای رسانه‌های غربی شواهدی از سوگیری ساختاری در بازنمایی بحران ارائه می‌دهد. مجموعهٔ این مطالعات نشان می‌دهد روایت دفاعی روسیه در فضای رسانه‌ای غربی بیشتر به حاشیه رانده می‌شود.

در محور دوم، پژوهش‌ها به ریشه‌ها و منطق دفاعی رفتار اطلاعاتی روسیه توجه کرده‌اند. باقری و کاظمی (۱۴۰۲) در «امنیتی‌سازی مجدد روسیه توسط ناتو و کشورهای غربی بر اساس نظریهٔ امنیت جمعی»، با بهره‌گیری از نظریهٔ امنیت جمعی نشان می‌دهند فرآیند امنیتی‌سازیِ دوبارهٔ روسیه به‌وسیلهٔ ناتو و کشورهای غربی پس از بحران اوکراین موجب تشدید نگرانی‌های دفاعی مسکو شده و این فرایند زمینه‌ساز شکل‌گیری چارچوب دفاعی در سیاست اطلاعاتی روسیه است. وثوقی و موسائی (۱۴۰۳) در «نقش غرب در بحران‌های ۲۰۱۴ و ۲۰۲۲

1. Jones
2. Zollmann
3. Fisher

اوکراین و طولانی‌شدن آن‌ها» نشان می‌دهند راهبردهایی مانند طعمه‌گذاری، موازنه‌سازی و مداخله‌جویی هدفمند در تشدید و تداوم بحران‌های اوکراین نقش داشته‌اند. از این دیدگاه اقدام‌های روسیه بیشتر به‌عنوان واکنشی به تهدیدانگاری و مهار فعال غرب تفسیر می‌شود. مصلی‌نژاد (۱۳۹۲) در «موازنهٔ راهبردی و سیاست‌گذاری امنیتی روسیه در نظام بین‌الملل»، تغییرهای سیاست امنیتی روسیه از دورهٔ یلتسین تا پوتین را بررسی و الگوهای موازنهٔ نرم و سخت روسیه در برابر یک‌جانبه‌گرایی آمریکا را تبیین می‌کند. دهقانی فیروزآبادی و مرادی (۱۳۹۵) در «تهدید غرب، برداشت روسیه و بحران اوکراین» با بازخوانی برداشت روسیه از تهدید غرب و بحران اوکراین، رفتار روسیه در اوکراین را واکنشی به تهدیدهای امنیتی ناشی از گسترش ناتو و نفوذ آمریکا در محیط امنیتی روسیه می‌دانند. حاجی یوسفی و ذوالفقاری (۱۳۹۶) در «فرهنگ راهبردی و سیاست خارجی خاورمیانه‌ای روسیه»، سیاست خارجی روسیه را متأثر از فرهنگ راهبردی این کشور دانسته و نقش روسیه به‌عنوان یک قدرت بزرگ را در مقابله با نظم جهانی زیر سلطهٔ غرب تحلیل می‌کنند. کرمی (۱۴۰۳) در «مکتب ژئوپلیتیک روسی؛ معمای پایداری آسیب‌پذیری و گسترش‌گرایی»، مکتب ژئوپلیتیک روسیه را تبیین و مفاهیمی مانند عمق راهبردی، منطقهٔ حائل و گسترش‌گرایی را به‌عنوان راهکارهای روسیه برای جبران آسیب‌پذیری‌های جغرافیایی‌اش معرفی می‌کند.

در سطح بین‌المللی، سابانادزه و دالای[1] (۲۰۲۵) در «درک راهبرد روسیه در دریای سیاه: چگونه می‌توان رویکرد اروپا و ناتو نسبت به این منطقه را تقویت کرد»، نشان می‌دهند که فرهنگ راهبردی روسیه بر ادراک تهدید وجودی از سوی غرب مبتنی است و رفتار روسیه در حوزه‌هایی مانند دریای سیاه، بیشتر واکنش به احساس محاصرهٔ ژئوپلیتیکی است؛ ورشینین و کریپوپالوف[2] (۲۰۲۴) نیز در «فرهنگ راهبردی روسیه در بازنگری تاریخی» بر تداوم مؤلفه‌های ضدغربی از دورهٔ شوروی تا امروز تأکید دارند و این تداوم را زمینه‌ساز نگرش دفاعی معاصر روسیه می‌دانند. وو و سینگ (۲۰۲۵) در «آیین تقابل اطلاعاتی روسیه در عمل (۲۰۱۴ تا امروز): نیت، تحول و پیامدها»، آیین مقابلهٔ اطلاعاتی روسیه را چارچوبی چندلایه متشکل از ابعاد سایبری، تبلیغاتی و روانی می‌دانند که در زمان صلح و جنگ فعال است. برژینسکی و آریک (۲۰۲۵) در «راهبرد ناتو برای مقابله با روسیه» نیز از دیدگاه ناتو اقدام‌های اطلاعاتی روسیه را تهدیدی فعال می‌دانند و لزوم پاسخ فشاری متقابل را مطرح می‌کنند.

1. Sabanadze & Dalay
2. Vershinin & Krivopalov

محور سوم به آیین رویارویی اطلاعاتی و تحول فناوری اختصاص دارد. نورمحمدی (۱۴۰۰) در «فضای مجازی و تحول مفهوم و اشکال جنگ در روابط بین‌الملل»، تحول ساختاری فضای مجازی را تشریح و افزایش دامنه، سرعت و دقت عملیات اطلاعاتی را برجسته می‌کند؛ این دگرگونی محیط عمل را برای راهبردهای اطلاعاتی روسیه تغییر داده است. آقایی و عبداللهی (۱۴۰۴) در «امنیت انرژی اتحادیهٔ اروپا زیر تأثیر تهدیدهای سایبری روسیه» با بازخوانی امنیت انرژی اتحادیهٔ اروپا زیر تأثیر تهدیدهای سایبری روسیه و با کاربست رویکرد نوواقع‌گرایی تدافعی، حمله‌های سایبری روسیه به زیرساخت‌های انرژی اروپا را بخشی از جنگ ترکیبی برای بی‌ثبات‌کردن این اتحادیه تحلیل می‌کنند. خان‌محمدی (۱۴۰۱) در «راهبرد بازدارندگی چندوجهی روسیه (متعارف، هسته‌ای، سایبری، تروریسم)» در راهبرد بازدارندگی چندوجهی روسیه، راهبرد جامع روسیه را در ترکیب ابزارهای هسته‌ای، متعارف، سایبری و ضدتروریسم برای مقابله با تهدیدها و تأثیرگذاری بر دشمنان بالقوه تحلیل می‌کند.

چارچوب مفهومی و نظری پژوهش

برای افزایش دقت علمی، مفاهیم تخصصی به‌کار استفاده‌شده در این نوشتار این‌گونه تعریف می‌شوند:

جنگ شناختی: نبردی برای تسلط بر ذهن انسان؛ حوزه‌ای از جنگ که هدف آن نه تخریب زیرساخت‌های فیزیکی، بلکه «دستکاری روانشناختی تصمیم‌گیرندگان دولتی» و تضعیف ارادهٔ جامعه برای مقاومت است (Information Warfare…, 2024).

کنترل بازتابی: آیین راهبردی روسی که هدف آن «وادارکردن حریف به گرفتن تصمیم‌های داوطلبانه‌ای است که به‌سود شماست». این کار با دستکاری اطلاعات و تضعیف سیستم تصمیم‌گیری او انجام می‌شود، به‌گونه‌ای که حریف تصور کند درحال گرفتن تصمیمی منطقی و مستقل است (Mullaney, 2022: 195).

عملیات هک و نشت: «عملیات هک و نشت»[1] به‌عنوان مرزی جدید در شکل‌های دیجیتال دخالت خارجی شناخته می‌شود. این نوع عملیات شامل دو مرحلهٔ اصلی است: ۱. هک: دسترسی به اطلاعات محرمانه به‌وسیلهٔ ابزارهای هک. ۲. نشت: انتشار و پخش این اطلاعات

1. Hack and Leak Operation (HLO)

به‌صورت گسترده. این عملیات به‌عنوان «شبیه‌سازی رسوایی» توصیف شده‌اند. به این معنی که تلاش‌های عمدی برای جهت‌دادن به قضاوت‌های اخلاقی علیه هدفی مشخص هستند (Shires, 2020: 11).

بهانه‌های اطلاعاتی[1]: نوعی خاص از عملیات اطلاعاتی است که در آن روایتی دروغین و مهندسی‌شده به‌طور پیش‌دستانه منتشر می‌شود تا مسئولیت ارتکاب جنایت بین‌المللی یا اقدام غیرقانونی از عامل اصلی گرفته شود و به طرف مقابل یا یک عامل ساختگی نسبت داده شود (Jordash et al., 2025: 3, 22–23).

درگیری منجمد[2]: وضعیتی که در آن دشمن‌های نظامی فعال متوقف شده‌اند، اما هیچ توافق صلحی برای حل‌وفصل سیاسی درگیری امضا نشده است. این وضعیت که بیشتر با حضور نیروهای پاسدار صلح (به‌طور معمول روسی) همراه است، به روسیه اهرم فشار دائمی بر سیاست داخلی و خارجی کشورهای میزبان می‌دهد و درعمل حق حاکمیت آن‌ها را محدود می‌کند. رویکردی که یادآور «آیین برژنف» در دوران اتحاد شوروی است (Sprague, 2016: 8).

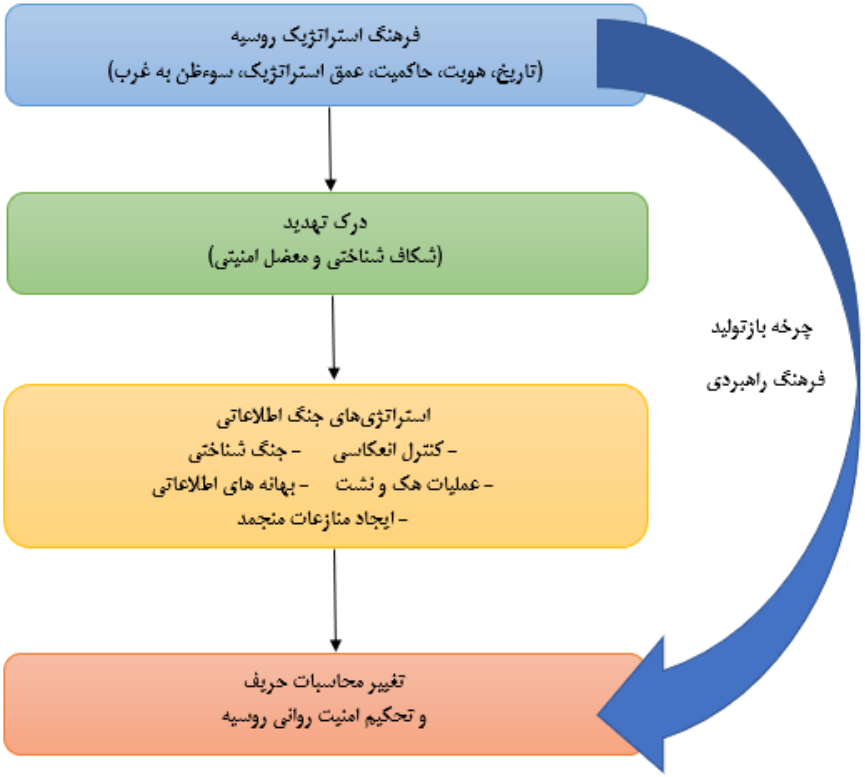
در این نوشتار برای پرهیز از مقایسهٔ سطحی، از چارچوب نظری «فرهنگ راهبردی» بهره می‌بریم؛ مفهومی که اسنایدر آن را مجموعه‌ای از باورها و الگوهای رفتاری مشترک نخبگان امنیتی برای درک جهان و پاسخ به تهدیدهای تعریف می‌کند (Snyder, 1977). در مورد روسیه، پژوهش زهرانی و شیراوند این فرهنگ را دارای «منطقی تدافعی» و متشکل از مؤلفه‌هایی مانند تصور تهدید، ویژگی‌های ژئوپلیتیک، اندیشهٔ قدرت بزرگ، اقتدارگرایی و هویت اسلاو–ارتدوکس می‌دانند (زهرانی و شیراوند، ۱۳۹۶: ۱۰۵).

«فرهنگ راهبردی» روسیه که ریشه در تاریخ و جغرافیا دارد، به‌دلیل آسیب‌پذیری مرزهای باز، بر اولویت «عمق راهبردی» و بدبینی به غرب استوار است. این فرهنگ با تلاش برای احیای جایگاه «قدرت بزرگ»، تفاوت بنیادین خود با غرب را نمایان می‌کند (Puustinen, 2023: 1-3). همچنین تحلیل این تقابل نیازمند درک «ادراک تهدید» و نظریهٔ «معمای امنیتی[3]» است که نشان می‌دهد چگونه اقدام‌های دفاعی یک طرف ممکن است تهاجمی تفسیر شود (Jervis, 1976). این شکاف ادراکی هستهٔ اصلی تقابل روسیه و ناتو است. در حالی‌که ناتو گسترش خود را سیاست «درهای باز» می‌داند، سند نظامی روسیه به‌روشنی «گسترش ناتو» را

1. Information Alibis
2. Frozen Conflict
3. Security Dilemma

تهدیدی علیه امنیت ملی معرفی می‌کند (The Military Doctrine…, 2014: 3).

شکل ۱. مدل مفهومی‌نظری نوشتار



منبع: نویسندگان

همان‌طور که پوچک و دین[1] تشریح می‌کنند، این «درک ناقص» از منطق یکدیگر، که ریشه در تفاوت ادراک تهدید و چارچوب‌های فرهنگی و شناختی امنیتی دارد، سبب شده است که هر اقدام دفاعی از سوی ناتو، در مدل شناختی مسکو به‌عنوان یک حرکت تهاجمی برای محاصره و تضعیف روسیه تفسیر شود (Pucek & Deen, 2024). برای درک عمق نگرانی مسکو، باید به اسناد بالادستی این کشور هم مراجعه کرد. در «راهبرد امنیت ملی فدراسیون روسیه» (نسخهٔ به‌روزرسانی شده در سال ۲۰۲۱)، این سند تأکید می‌کند که غرب از راه «نفوذ اطلاعاتی و فرهنگی» به‌دنبال تضعیف حاکمیت و یکپارچگی سرزمینی روسیه است. این ادراک

1. Pucek & Deen

تهدید، زیربنای مشروعیت‌بخشی به اقدام‌های سایبری و رسانه‌ای روسیه به‌عنوان «اقدام‌های متقابل مشروع» است (کولایی و عرفانی، ۱۴۰۳: ۴۱). این چارچوب تلفیقی، متشکل از نظریهٔ فرهنگ راهبردی و مفهوم ادراک تهدید، امکان می‌دهد درک کنیم که چرا روسیه و غرب، با وجود رویارویی با داده‌های یکسان، به تفسیرها و راهبردهای به‌طور کامل متفاوت می‌رسند.

روش‌شناسی پژوهش

این نوشتار با رویکرد کیفی و بر پایهٔ «تحلیل روایی»[1] انجام شده است. انتخاب این رویکرد ناشی از سرشت پرسش نوشتار و ضرورت تمرکز بر «چرایی» و «چگونگی تفسیر» اقدام‌های روسیه در جنگ اطلاعاتی است. تحلیل روایی امکان بررسی ساختار، محتوای معنایی و کارکرد روایت‌هایی را فراهم می‌کند که بازیگران اصلی برای مشروعیت‌بخشی به اقدام‌های خود تولید و بازنمایی می‌کنند. جامعهٔ پژوهش شامل متن‌ها، اسناد، گزارش‌ها و داده‌های مربوط با جنگ اطلاعاتی روسیه در سال‌های ۲۰۱۴ تا ۲۰۲۵ است که به‌صورت مستقیم یا غیرمستقیم به راهبردها، آیین‌ها، یا عملیات اطلاعاتی روسیه و واکنش‌های غرب به آن پرداخته‌اند. داده‌ها به‌صورت کتابخانه‌ای و اسنادی گردآوری شده‌اند.

ریشه‌های تاریخی جنگ اطلاعاتی روسیه

از دوران تزارها در روسیه، اطلاعات همواره عنصری حیاتی بوده است، اما اهمیت آن پس از دههٔ ۱۹۹۰ و در رهبری پوتین با انتصاب افسران اطلاعاتی پیشین در مناصب مهم افزایش یافته است (Østbø, 2024: 963). جنگ دوم چچن (۱۹۹۹) نقطهٔ عطفی بود که موجب شد سیاست رسانه‌ای کرملین از رویکردی به‌نسبت آزاد به کنترلی سخت‌گیرانه و سازمان‌یافته برای مدیریت افکار عمومی تغییر یابد (Belin, 2002: 1-3). ریشهٔ اصلی جنگ اطلاعاتی نوین روسیه در جنگ سرد و راهبرد «اقدام‌های فعال» شوروی نهفته است. چارچوبی که فراتر از تبلیغات، شامل عملیات پنهان برای تضعیف دشمن از درون و ایجاد شکاف در غرب بود (Jones, 2025: 1). در برابر، اسناد تاریخی مانند «طرح راهبرد روانی ایالات متحد» در سال ۱۹۵۴ که بر بهره‌برداری از نارضایتی‌های داخلی شوروی تمرکز داشت (United States Psychological…, 1954) نشان می‌دهد که نگرانی‌های امروز روسیه از دخالت‌های خارجی در واقعیت‌های

1. Narrative Analysis

تاریخی ریشه دارد. نخبگان روسیهٔ پساشوروی این دیدگاه امنیتی سنتی را به ارث برده‌اند. بنابراین اقدام‌های کنونی روسیه نه یک انحراف، بلکه تکامل فرهنگ دوران جنگ سرد است که بر مبنای باور روسیه به تلاش دائمی غرب برای تضعیف آن استوار است (Vershinin & Krivopalov, 2024: 43).

مبانی آیین‌محور روسیه

برای درک عمیق‌تر فرهنگ راهبردی روسیه، باید با مفهوم بنیادین «ذهنیت قلعهٔ محاصره‌شده» آشنا شد. ریشهٔ این ذهنیت را می‌توان در گسترش ناتو و حرکت غرب به‌سمت «حیاط خلوت روسیه» جست‌وجو کرد (Mearsheimer, 2014: 1). در این زمینه، در اسناد راهبردی روسیه آمده است: «چشم‌انداز گسترش ناتو به شرق برای روسیه پذیرفتنی نیست، زیرا تهدیدی برای امنیت ملی این کشور به شمار می‌آید (کولایی و دیگران، ۱۴۰۱: ۱۳۰). این الگو به وضعیت شناختی اشاره دارد که در آن، نخبگان حاکم، کشور را در محاصرهٔ دائمی دشمنان خارجی می‌بینند. این ذهنیت نتیجهٔ مستقیم سیاست‌های غرب است. ایالات متحد با «وسواس برای واردکردن اوکراین به ناتو و تبدیل آن به سنگر غرب در مرز روسیه»، این کشور را به واکنش نظامی وادار کرد، زیرا نخبگان روس این سیاست را «تهدید وجودی» می‌دیدند (Mearsheimer, 2022: 13).

این مفهوم با ریشه در تاریخ انزوا، الگویی شناختی ایجاد کرده است که در آن نخبگان، کشور را در محاصرهٔ دشمنان و انتقادهای داخلی را «ستون پنجم» می‌پندارند؛ ذهنیتی که توجیه‌گر کنترل شدید داخلی است. در دوران پس از جنگ سرد، این نگرش به آیین نظامی «ضدانقلابی» در واکنش به انقلاب‌های رنگی تکامل یافت (Meister, 2016: 7). از دید مسکو این تحولات، عملیات براندازی غرب با ابزارهایی مانند «بنیاد ملی برای دموکراسی»[1] است که وابستگی مالی آن‌ها به کنگره، این ادعا را تأیید می‌کند (Investing in Freedom…, 2025). همچنین باید گفت این ذهنیت فقط واکنشی سیاسی نیست، بلکه در عناصر پایدار فرهنگ راهبردی روسیه ریشه دارد. برخی از مؤلفه‌های این فرهنگ عبارت‌اند از: «چشم‌انداز قدرت بزرگ و بازگشت به شکوه امپراتوری روسیه، ترس از تهدیدهای خارجی، رویکرد ژئوپلیتیک‌محور، حفظ یکپارچگی سرزمینی و داشتن یک مأموریت تمدنی خاص». این عناصر

1. National Endowment for Democracy

در کنار هم، چارچوب ذهنی می‌سازند که اقدام‌های خارجی را به‌عنوان بخشی از یک تقابل دائمی برای بقا توجیه می‌کند (رحیمی چسلی و همکاران، ۱۴۰۲: ۹).

راهبرد روسیه به‌تازگی به مفهوم «جنگ شناختی» تکامل یافته است که در آن هدف دشمن نه تسخیر سرزمین، بلکه «تخریب ذهنی» و فرسایش هویت جامعه براورد می‌شود. از این‌رو فضای اطلاعاتی، سنگری حیاتی است و هرگونه نفوذ خارجی، حمله به امنیت ملی به شمار می‌آید (Bryc & Domańska, 2024). روسیه با آگاهی از ضعف‌های اقتصادی و نظامی خود، به جنگ نامتقارن روی آورده و بر سرمایه‌گذاری در حوزهٔ اطلاعات متمرکز شده است (Rodari, 2021: 103). مسکو اقدام‌های خود را با این استدلال توجیه می‌کند که «فقط در حال کپی‌کردن ابزارها و فن‌هایی است که خود غرب» برای ترویج دموکراسی به کار می‌گیرد (Meister, 2016: 5). این رویکرد، که در آن مرز میان دفاع و تهاجم کم‌رنگ است، بستر اصلی همهٔ اقدام‌های اطلاعاتی روسیه را تشکیل می‌دهد.

جنگ اطلاعاتی به‌عنوان ابزار سیاست خارجی

در اسناد راهبردی روسیه آمده است که «پشتیبانی اطلاعاتی از فعالیت‌های سیاست خارجی، یکی از حوزه‌های مهم در سیاست خارجی فدراسیون روسیه به‌شمار می‌رود. این حوزه شامل برقراری ارتباط با بخش‌های گسترده‌ای از افکار عمومی جهان و اطلاع‌رسانی دقیق در مورد مواضع روسیه در برابر مسائل اصلی بین‌المللی، ابتکارها و اقدام‌های سیاست خارجی و دستاوردهای فرهنگی، علمی و فکری این کشور است. هدف اصلی، شکل‌دادن به درکی مثبت از روسیه در خارج از کشور و ایجاد نگرشی دوستانه نسبت به آن است» (کولایی ودیگران، ۱۴۰۱: ۲۸۳). راهبرد روسیه در برابر همسایگان، بهره‌گیری از «درگیری‌های منجمد» به‌عنوان ابزار نفوذ ژئوپلیتیک است. هدف کرملین با تکیه بر «سندروم امپراتوری»، تثبیت فضای پساشوروی به‌عنوان «حوزهٔ مسئولیت ویژه» خود است. سیاستی که در عمل حاکمیت این کشورها را تضعیف و مانع همگرایی آن‌ها با اروپا می‌شود (Alieksiejchenko, 2024: 41).

اندرو اسپراگ[1] در تحلیل خود از الگوهای مداخلهٔ روسیه نشان می‌دهد که اقدام‌های مسکو تصادفی نیست، بلکه از منطق ژئوپلیتیک مشخص پیروی می‌کند. بر اساس این تحلیل، مداخلهٔ روسیه و حمایت از جنبش‌های جدایی‌طلبانه زمانی رخ می‌دهد که سه شرط به‌طور هم‌زمان

1. Andrew Sprague

وجود داشته باشد:

ـ حضور اقلیت قومی ناآرام که به‌عنوان نقطهٔ ورود و اهرم فشار داخلی عمل می‌کند؛

ـ تلاش دولت میزبان برای غربی‌سازی: گرایش به‌سمت ناتو یا اتحادیهٔ اروپا به‌عنوان «خط قرمز» برای مسکو براورد می‌شود؛

ـ نبود گزینه‌های ژئوپلیتیکی جایگزین، یعنی حضورنداشتن قدرت رقیبی که مایل به مقابله با نفوذ روسیه باشد (Sprague, 2016: 23).

این الگو در مواردی مانند ورانیستریا (مولداوی)، اوستیای جنوبی و آبخازیا (گرجستان) و دونباس (اوکراین) مشهود است؛ که روسیه با حمایت از جدایی‌طلبان، مانع همگرایی این کشورها با ناتو شد. در همهٔ این موارد، جنگ اطلاعاتی ابزار اصلی برای بسیج اقلیت‌ها، تضعیف دولت مرکزی و توجیه مداخلهٔ مسکو بوده است (Pucek & Deen, 2024).

راهبرد کلان روسیه: بازنگری در نظم جهانی به‌وسیلهٔ دفاع فعال

الگوی کنش راهبردی روسیه در دورهٔ پساشوروی بیانگر تداوم تلاش این کشور برای حفظ و بازتعریف ژئوپلیتیک به‌جامانده از نظم شوروی است. در این چارچوب، مهار گسترش ناتو به قلمروهای پیشین شوروی به یکی از محورهای پایدار سیاست خارجی و امنیتی روسیه تبدیل شده است (بلنک، ۱۴۰۴). بنابراین اقدام‌های اطلاعاتی روسیه ابزاری برای راهبرد کلان «بازنگری‌خواهی»[1] در نظم پس از جنگ سرد است که نقطهٔ عطف آن در سخنرانی سال ۲۰۰۷ پوتین در مونیخ و چالش با هژمونی آمریکا نمایان شد. این رویکرد در فرهنگ راهبردی ریشه دارد که روابط بین‌الملل را بازی مجموع صفر می‌بیند. جایی که هر پیشروی غرب، تهدیدی برای امنیت روسیه است (Sabanadze & Dalay, 2025: 19-21). از دیدگاه مسکو، ناتو ابزاری تهاجمی برای مهار روسیه است و گرایش همسایگان به غرب «طرحی ضدروسی»[2] شناخته می‌شود. بر این اساس، اقدام‌های روسیه نوعی «دفاع فعال» در حوزهٔ نفوذ تاریخی‌اش تعریف می‌شود؛ آیینی که با کم‌رنگ‌کردن مرز دفاع و تهاجم، اقدام‌های پیشگیرانه در برابر تهدیدهای را توجیه می‌کند (Sabanadze & Dalay, 2025: 11-12). جنگ اطلاعاتی روسیه رویکردی «برآمده از ضعف» است که انعطاف‌پذیری بیشتری را در برابر رقیبی با منابع اقتصادی و فناورانه بسیار بزرگ‌تر فراهم می‌کند (Meister, 2016: ii, 1, 7, 8):

1. Revisionism
2. Anti-Russia

ـ تضعیف انسجام غرب: روسیه تلاش می‌کند «تردید درونی را در جوامع غربی که به‌طور فزاینده‌ای شکننده و از هم گسسته شده‌اند، تقویت کند». هدف مسکو «فلج‌کردن و خرابکاری در فرآیندهای تصمیم‌گیری اتحادیهٔ اروپا و ناتو است».

ـ جلوگیری از گسترش نفوذ غرب: اقدام‌های غیرنظامی روسیه واکنشی به «فشار غرب بر روسیه و جایگاه این کشور در حوزهٔ پساشوروی» است. مسکو «بی‌ثباتی، فساد و دولت‌های ضعیف را تشویق می‌کند تا روابط مبتنی بر وابستگی را حفظ کند».

ـ ارائهٔ روایت جایگزین: هدف اصلی رسانه‌های خارجی روسیه «ارائهٔ جهان‌بینی روسی به‌عنوان جایگزینی برای دیدگاه غربی» است. این رسانه‌ها اکنون بر «ترویج نظریه‌های توطئه و بدنام کردن غرب» تمرکز دارند.

این راهبرد کلان که هدف نهایی آن نه پیروزی در جنگ نظامی، بلکه تغییر توازن قدرت در تقابلی دائمی است، بستر اصلی همهٔ اقدام‌های اطلاعاتی روسیه را تشکیل می‌دهد.

کالبدشناسی عملیات اطلاعاتی روسیه: بازیگران و روش‌ها

برای درک کامل راهبرد اطلاعاتی روسیه، باید بازیگران و روش‌های مشخصی را تحلیل کنیم که این راهبرد را پیاده می‌کنند. هر یک از این بازیگران و گروه‌ها در تولید، پردازش و توزیع محتوای هم‌سو با راهبرد کلان روسیه نقشی ویژه دارند. فعالیت آن‌ها به‌گونه‌ای هماهنگ است که محتوای تولیدشده را سطح‌های بالای حاکمیتی، به‌سرعت به‌وسیلهٔ رسانه‌ها و سکوهای وابسته منتشر و بازیگران غیررسمی و شبکه‌های سایبری تقویت می‌کنند. نتیجهٔ این فرایند، ایجاد فضای اطلاعاتی سرشار از روایت‌های متناقض و جهت‌داری است که با تاکتیک موسوم به «شلنگ آتشین دروغ[1]» هم‌خوانی دارد. چنین سازوکاری نه‌تنها به آماده‌کردن افکار عمومی پیش از اقدام‌های نظامی کمک می‌کند، بلکه پس از شکل‌گیری رویداد نیز به تحریف واقعیت و پوشاندن مسئولیت واقعی منجر می‌شود (Jordash et al., 2025). جدول ۱، ساختار و نقش بازیگران اصلی در عملیات اطلاعاتی روسیه و تاکتیک‌های اصلی آن‌ها را به‌صورت نظام‌مند نشان می‌دهد.

---

۱. Firehose of Falsehood: مدلی از عملیات نفوذ اطلاعاتی که بر حجم، سرعت و تکرار پیام‌های نادرست برای تضعیف توان تمایز مخاطب میان حقیقت و ساختگی تکیه دارد (Paul & Matthews, 2016).

جدول ۱. کالبدشناسی عملیات اطلاعاتی روسیه: بازیگران و تاکتیک‌ها

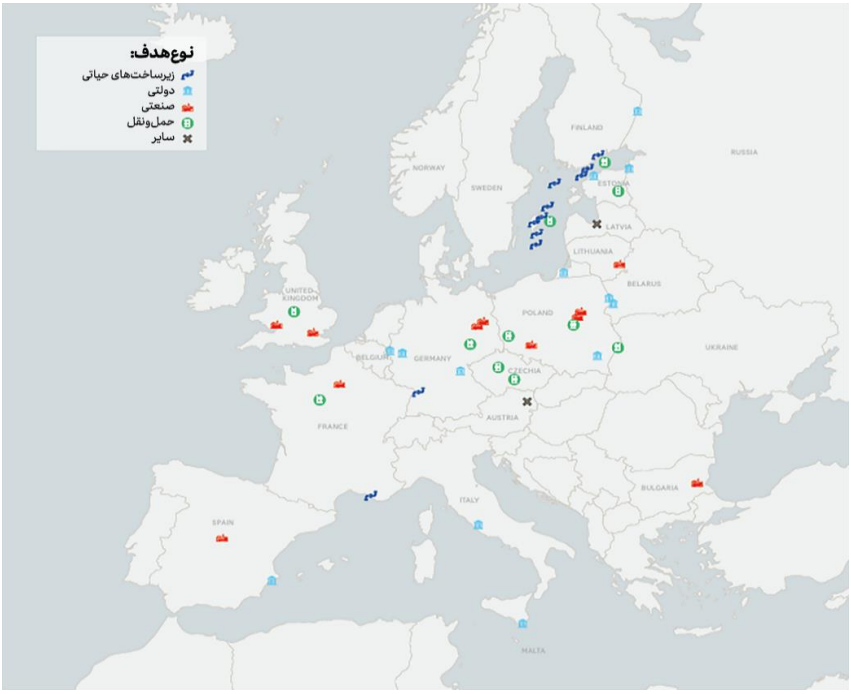
گروه بازیگر	نقش و وظایف	تاکتیک‌های مهم	نمونه‌های بیان‌شده در گزارش‌های متعدد
نهادهای دولتی روسیه (کرملین، وزارت دفاع، وزارت خارجه)	طراحی راهبرد کلان، هماهنگی عملیات میدانی و اطلاعاتی، صدور دستور عمل	انتشار «بهانه‌های اطلاعاتی» پیش‌دستانه، مقصر جلوه‌دادن طرف مقابل، روایت‌سازی سیاسی و حقوقی	ادعای استفادهٔ اوکراین از زایشگاه ماریوپول به‌عنوان پایگاه نظامی
رسانه‌های دولتی و وابسته (آرتی، اسپوتنیک، کانال‌های تلویزیونی ملی)	پخش و تقویت پیام‌های رسمی، تولید مستندهای ساختگی یا تحریف‌شده	گزارش‌های میدانی ساختگی، مصاحبه‌های هدایت‌شده، استفاده از زبان احساسی و القاب منفی	پوشش هم‌سو با مواضع رسمی در مورد حمله به تئاتر ماریوپول
سکوهای آنلاین کنترل‌شده (کانال‌های تلگرام وابسته، وب‌سایت‌های تولیدکنندهٔ محتواهای جهت‌دار)	توزیع سریع و هدفمند محتوا در محیط‌های بسته و نیمه‌بسته	انتشار محتوای چندرسانه‌ای (ویدئو، عکس) با برچسب‌گذاری گمراه‌کننده، استفاده از میم‌ها و شوخی‌های سیاسی برای جلب توجه	روایت متناقض و فوری در مورد حمله به سد کاخوفکا
چهره‌های پرنفوذ و مبلغان پشتیبان دولت	انتقال پیام به مخاطب محلی و بین‌المللی با ظاهری غیررسمی	بازنشر پیام‌های رسمی با لحن شخصی، ایجاد حس «شاهد عینی»	ویدئوهای کاربران به‌ظاهر مستقل در حمله به ایستگاه قطار کراماتورسک
شبکه‌های هماهنگ سایبری	گسترش دامنهٔ پیام، حمله به روایت‌های مخالف	تاکتیک «شلنگ آتشین دروغ[1]» (حجم عظیم اطلاعات متناقض)، حمله سایبری به منابع خبری مستقل	بمباران خبری و ادعاهای هم‌زمان متناقض در مورد اردوگاه اسرا در اولنیفکا

منبع: نویسندگان

1. Firehose of Falsehood

همچنین گزارش گوگل، یوتیوب را میدان نبرد اساسی میان کانال‌های دولتی روسیه و منابع خبری مستقل معرفی می‌کند. این سکو عرصهٔ جنگی دوطرفه است که در آن روسیه هم‌زمان با ترویج روایت‌های خود، درپی سرکوب روایت‌های رقیب است (Huntley, 2023). جنگ اطلاعاتی روسیه فراتر از روایت‌سازی، بخشی از راهبرد یکپارچه «جنگ ترکیبی» است که تهاجم نظامی، حمله‌های سایبری و عملیات نفوذ را هماهنگ می‌کند (Ukraine: An Overview…, 2022). داده‌ها نشان می‌دهد گروه‌های هکری وابسته به روسیه با استفاده از «بدافزارهای پاک‌کننده[1]»، ده‌ها حملهٔ مخرب را علیه نهادهای دولتی و زیرساخت‌های حیاتی اوکراین اجرا کرده‌اند (Burt, 2022). این حمله‌ها به کشورهای اروپاییِ پشتیبان اوکراین، به‌ویژه در جناح شرقی ناتو نیز گسترش یافته است، اما کشورهای دارای روابط نزدیک با مسکو (مانند مجارستان و صربستان) از آن در امان مانده‌اند (Jones, 2025: 12).

شکل ۲. منطقهٔ جغرافیایی حمله‌های روسی در سال‌های ۲۰۲۲ تا ۲۰۲۵



Source: Jones, 2025

1. Wiper Malware

راهبردهای مقابله‌ای دوگانه: حمله به خارج، کنترل در داخل

نخستین لایهٔ حیاتی راهبرد اطلاعاتی مسکو، ایمن‌سازی فضای داخلی با هدف حفظ حاکمیت اطلاعاتی است (Doctrine of Information Security…, 2016). این رویکرد فراتر از سانسور، به‌دنبال ایجاد «مصونیت اطلاعاتی»[1] است تا شهروندان با پذیرش فعالانهٔ روایت‌های رسمی، در برابر نفوذ اطلاعاتی غرب «واکسینه» شوند و جبههٔ داخلی پیش از هر اقدام خارجی مستحکم شود. درواقع پس از سال ۲۰۱۲، در پاسخ به تظاهرات گسترده[2]، دولت روسیه برای مدیریت افکار عمومی کنترل بر اینترنت را با ابزارهای قانونی و فنی تشدید کرد. بر اساس قانون سال ۲۰۱۲، دادستان کل اختیار یافت وب‌سایت‌های با محتوای افراطی، اطلاعات نادرست یا دعوت به تظاهرات را بدون نیاز به حکم دادگاه مسدود کند (Litvinova, 2025). این راهبرد با مجموعه‌ای از ابزارهای قانونی و فنی که به‌ویژه پس از سال ۲۰۱۲ تشدید شدند، جنبهٔ عملی به خود گرفته است و برخی از آن‌ها این‌گونه است:

ـ **قوانین محدودکننده:** در مارس ۲۰۱۹ قانونی امضا شد که انتشار آن‌لاین «اطلاعات مشکوک» را که زندگی، سلامت، اموال یا نظم عمومی را تهدید کند یا سبب اختلال در زیرساخت‌های حیاتی (مانند حمل‌ونقل، انرژی یا خدمات اجتماعی) شود، غیرقانونی اعلام کرد. این قانون که جرائم سنگینی تا سقف یک میلیون روبل برای اشخاص حقوقی در نظر گرفته است، به مقام‌ها اجازه می‌دهد وب‌سایت‌های متخلف را فوری مسدود کنند (Robinson et al., 2019: 9). پس از تهاجم سال ۲۰۲۲ به اوکراین، قوانین سخت‌گیرانه‌تری اجرا شد که انتشار اطلاعات «نادرست» (غیررسمی) در مورد ارتش را با مجازات‌هایی تا ۱۵ سال زندان جرم‌انگاری می‌کند (Lim and Bradshaw, 2023: 10).

ـ **کنترل زیرساخت:** قانون «اینترنت مستقل» (۲۰۱۹): به دولت روسیه اختیار می‌دهد که در شرایط اضطراری، اینترنت کشور را از شبکهٔ جهانی جدا کند. این تلاشی آشکار برای ساختن «اینترنت ملی» شبیه به «دیوار آتش بزرگ چین» است.

ـ **افزایش نظارت:** دولت روسیه زیرساخت‌های نظارتی خود را تقویت کرده است. این اقدام‌ها، به سازمان فدرال نظارت بر ارتباطات اجازه می‌دهد ترافیک اینترنت را به‌صورت زنده کنترل کند و محتوایی را که با سیاست‌های دولت در تضاد است، فیلتر یا مسدود کند.

---

1. Information Immunity

۲. اعتراض‌هایی که در سال‌های ۲۰۱۱ تا ۲۰۱۳ در واکنش به نتایج انتخابات پارلمانی و ریاست جمهوری در روسیه شکل گرفت.

ـ فیلترینگ و مسدودکردن: مسدودکردن وب‌سایت‌های مخالف و سکوهای خارجی مانند فیس‌بوک و توییتر به تاکتیک رایج تبدیل شده است. این اقدام‌ها همچنین شامل کندکردن عمدی سرعت ترافیک و استفاده از «فایروال‌ها»[1] برای محدودکردن دسترسی به اطلاعات است (Litvinova, 2025).

ـ فشار بر سکوهای فناوری: غول‌های فناوری مانند گوگل و متا[2]، پیوسته برای حذف محتوایی که از نظر دولت روسیه «افراطی» یا «غیرقانونی» است، زیر فشار قرار می‌گیرند. آنها در صورت تمکین‌نکردن، با جریمه‌های سنگین روبه‌رو می‌شوند (Huntley, 2023).

هم‌زمان با کنترل فضا، دولت برای «تحکیم افکار عمومی» به تولید روایت‌های ایجابی در اکوسیستمی کنترل‌شده می‌پردازد (Information warfare by…, 2024). هدف از پرکردن فضا با «تبلیغات و نظریه‌های توطئه»، منفعل نگه‌داشتن مخاطب داخلی است (Rodari, 2021: 104). راهبردی که هر صدای مخالفی را به‌عنوان کارزار خارجی، بی‌اعتبار می‌کند. با این‌حال، راهبرد «قلعهٔ اطلاعاتی» با تبدیل سیاست حاکمیت دیجیتال به ابزاری سیاسی برای کنترل داخلی، پیامدهای منفی داشته است. این رویکرد به حاشیه‌راندن بازیگران مستقل و تقویت شرکت‌های وابسته و همچنین امنیتی‌سازی فضا در تقابل با غرب، نظارت داخلی را توجیه کرده است. سرانجام، این سیاست به‌جای نوآوری به ایجاد فضایی متمرکز و راکد با اولویت جایگزینی واردات منجر شده است (Ustyuzhantseva & Popova, 2024: 11-12). این ایمن‌سازی داخلی روسیه، همراه با ایجاد بستری برای راهبردهای خارجی، آسیب‌پذیری کشور در برابر شوک‌های اطلاعاتی را افزایش داده است. روسیه از روش‌های پیچیده و متنوعی برای اجرای جنگ اطلاعاتی در عرصهٔ بین‌الملل استفاده می‌کند که در ادامه به تفصیل می‌آید:

ـ تغییر از قدرت سخت به قدرت هوشمند: روسیه در قرن بیست‌ویکم از قدرت هوشمند و جنگ اطلاعاتی برای دستیابی به هدف‌های راهبردی خود بهره می‌برد. این رویکرد، تکاملی از «اقدام‌های فعال» دوران شوروی است که فن‌های آشکار و پنهان برای تأثیرگذاری بر رویدادها و رفتارهای کشورهای خارجی را شامل می‌شد.

ـ استفاده از اکوسیستم پیچیده: براساس گزارش مرکز روابط جهانی آمریکا، روسیه «اکوسیستمی» پیچیده شامل کانال‌های رسمی، غیررسمی و ابزارهای سایبری را برای انتشار

---

۱. در فضای مجازی، فایروال (Firewall) به سیستم امنیتی گفته می‌شود که با نظارت و فیلترکردن ترافیک شبکه، از دسترسی غیرمجاز به یک شبکهٔ خصوصی جلوگیری می‌کند.

2. Meta

روایت‌های جهت‌دار ایجاد کرده است. این سیستم که نسخهٔ به‌روز شدهٔ کارزارهای اطلاعات نادرست شوروی است، با هدف ایجاد درگیری، دشمنی و بی‌ثباتی در کشورهای هدف فعالیت می‌کند.

ـ پراکندگی اطلاعات نادرست و گمراه‌کننده: روسیه بارها از اطلاعات نادرست و گمراه‌کننده استفاده می‌کند، به‌ویژه با گسترش اینترنت و رسانه‌های اجتماعی. این تاکتیک‌ها با هدف تضعیف، دستکاری و گمراه‌کردن اطلاعاتی که مردم مصرف می‌کنند، به کار می‌روند تا هدف‌های سیاسی و نظامی روسیه پیش برده شود (Topor & Tabachnik, 2021: 115).

این رویکرد واکنشی به سوءگیری نظام‌مند رسانه‌های غربی است. تحلیل‌ها نشان می‌دهد ۸۳ درصد پوشش خبری بنگاه‌هایی مانند بی‌بی‌سی و سی‌ان‌ان مبتنی بر «روزنامه‌نگاری جنگ» و انسانیت‌زدایی از دشمن بوده است (Fisher, 2023: 80) و نقش تحریک‌آمیز «گسترش ناتو» نیز به‌طور کلی نادیده گرفته شده است (Zollmann, 2024: 373). از دید مسکو، این چارچوب‌بندی یک‌جانبه، اقدامی تهاجمی براورد می‌شود که نیازمند پاسخی متقابل است. روسیه برای اجرای راهبرد بازدارندگی روایی خود، از ابزارهای مختلفی استفاده می‌کند:

ـ بازیگران غیردولتی: در لایهٔ بازیگران غیردولتی، راهبرد روسیه بهره‌گیری از شبکه‌ای پیچیده از هکرها برای پیشبرد جنگ اطلاعاتی با قابلیت انکار بالا است. در این مدل، نهادهایی مانند «سرویس امنیت فدرال»[1]، در برابرِ دادن مصونیت قضایی به هکرها، از مهارت آن‌ها برای حمله‌های سایبری (مانند هک کمیتهٔ ملی حزب دموکرات[2] در سال ۲۰۱۶) علیه هدف‌های خارجی بهره می‌برند، تا ضمن تضعیف نهادهای غربی، مسئولیت مستقیم دولت را انکار کنند (Mullins, 2024: 14).

ـ ترویج روایت: به‌جای انتشار صرف اطلاعات نادرست، روسیه بر ترکیب «حقایق مناسب» با «آرمان‌های ملی» برای ساخت روایتی جایگزین استوار است که راستی‌آزمایی آن دشوار باشد. هدف، ایجاد «مه اطلاعاتی» است که مخاطب را به این نتیجه برساند که هیچ حقیقتی مطلق نیست (Information Warfare by…, 2024).

ـ رسانه‌های بین‌المللی: رسانه‌هایی مانند آر تی و اسپوتنیک با ارائهٔ «روایت حذف‌شده»، نقش غرب در بحران‌ها را به چالش کشیده و هم‌زمان با افشای عملیات تبلیغاتی مخفی ناتو، استدلال «قربانی بودن» مسکو را تقویت می‌کنند (GT Investigates..., 2022).

1. Federal Security Service
2. Democratic National Committee

چارچوب‌بندی غربی از آیین روسیه به‌عنوان افسانه

راهبرد اطلاعاتی روسیه با ضدروایتی نظام‌مند از سوی غرب روبه‌رو است که با فن‌های چارچوب‌بندی، نگرانی‌های امنیتی مسکو را با عنوان «افسانهٔ سیاسی» بی‌اعتبار می‌کند. در این رویکرد، مفهوم افسانه ابزاری قدرتمند برای مشروعیت‌زدایی از رقیب و بسیج افکار عمومی است. یک نمونهٔ بارز از این چارچوب‌بندی، تحلیل‌های مداوم «مؤسسهٔ مطالعات جنگ»[1] است. این اندیشکده، که یکی از تأثیرگذارترین منابع تحلیلی غرب است، روسیه را «افسانه‌ای ساختگی» برای بسیج داخلی و توجیه جنگ اوکراین می‌داند (Zori, 2025). در این دیدگاه، آیین دفاعی مسکو نه واقعیتی راهبردی، بلکه ابزاری برای آماده‌کردن افکار عمومی برای درگیری طولانی‌مدت و توجیه هزینه‌های آن برآورد می‌شود (Stoanova, 2025)؛ رویکردی که به‌جای درک فرهنگ راهبردی، انگیزه‌های دفاعی روسیه را فقط تبلیغاتی دانسته و رد می‌کند. چارچوب‌بندی یک‌جانبهٔ غرب با نادیده‌گرفتن ریشه‌های تاریخی و راهبردی نگرانی‌های روسیه، امکان گفت‌وگو را بسته و چرخهٔ درگیری را تشدید کرده است (Zollmann, 2024: 377). این رویکرد از دید مسکو، انکار دغدغه‌های امنیتی‌اش شناخته شده و با وادارکردن آن به تشدید ضدروایت‌ها، به امنیتی‌سازی متقابل می‌انجامد که در آن هر طرف، دیگری را تهدیدی وجودی می‌پندارد. سرانجام مرشایمر[2] به روشنی بیان می‌کند، یک روایت متعارف بدون سند و مدرک است. او می‌نویسد: «درحالی‌که این روایت [تهاجم امپریالیستی پوتین] بارها و بارها در رسانه‌های جریان اصلی و تقریباً همهٔ رهبران غربی تکرار شده است، هیچ مدرکی برای حمایت از آن وجود ندارد.» (Mearsheimer, 2022: 14).

کنترل بازتابی

چارچوب راهبردی روسیه در جنگ اطلاعاتی، به‌وسیلهٔ مفهوم بنیادین «کنترل بازتابی»[3] ترجمه می‌شود. این نظریه، که استراتژیست‌های شوروی مانند «ولادیمیر لفور»[4] توسعه داده‌اند، به معنای «انتقال اطلاعاتی به حریف است که او را وادار می‌کند داوطلبانه تصمیمی بگیرد که از پیش تعیین کرده‌اید» (Thomas, 2004). هدف اصلی، نه پیروزی در نبرد مستقیم، بلکه فلج‌کردن فرآیند تصمیم‌گیری دشمن و وادارکردن او به انجام اشتباه‌های راهبردی است.

1. Institute for the Study of War
2. Mearsheimer
3. Reflexive Control
4. Vladimir Lefebvre

این چارچوب، همان‌طور که سامانتا مولانی[1] در تحلیل خود از کارزارهای روسیه نشان می‌دهد، در دو مطالعهٔ موردی اوکراین و ایالات متحد به روشنی قابل ردیابی است. در اوکراین، استفاده از عنصر «فریب» از ۲۵ درصد (پیش از پیوسته‌سازی کریمه) به ۶۱ درصد (پس از تهاجم به شرق) افزایش یافت که بیانگر حرکت به‌سمت دستکاری پیچیدهٔ ادراک است (Mullaney, 2022: 197). در برابر، در ایالات متحد که امکان درگیری نظامی وجود نداشت، کنترل بازتابی بر ضعف‌های اجتماعی و سیاسی متمرکز شد و تمرکز بر تشدید قطبی‌شدگی بود. پس از سال ۲۰۱۶ تاکتیک «نشت اطلاعات» ۸ درصد کاهش، اما «جدل» و «تقویت پیام» به ترتیب ۴ درصد و ۷ درصد رشد داشت که نشان‌دهندهٔ گذار به راهبرد بلندمدت تخریبی است (Mullaney, 2022: 200).

راهبرد متقابل غرب: از بازدارندگی تا چالش تهاجمی

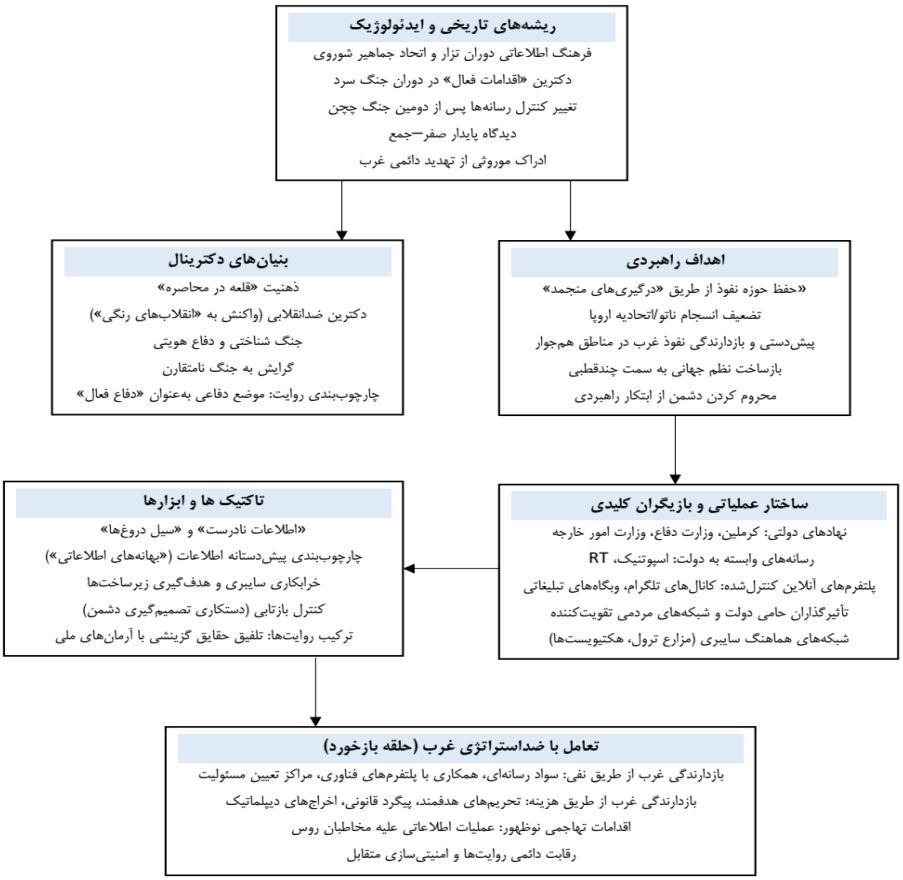
با تشدید موجی از حمله‌های خرابکارانه و جنگ ترکیبی شامل آتش‌افروزی، بمب‌گذاری و عملیات سایبری که به‌طور گسترده به روسیه نسبت داده می‌شود، دولت‌های غربی می‌کوشند پاسخ‌های مؤثر، هماهنگ و بازدارنده‌ای شکل دهند. آن‌ها در کنار تقویت تدابیر امنیت سایبری و زیرساختی، از واکنش‌های اطلاعاتی و دیپلماتیک نیز سود برده‌اند، اما هنوز در ارائهٔ واکنش‌های بازدارنده‌ای که فشار واقعی بر عاملان ایجاد کند، با چالش روبه‌رو هستند (Rathbone et al., 2024). پاسخ غرب به اقدام‌های روسیه، به‌جای تقابل روایی صرف، به‌طور فزاینده‌ای در چارچوب راهبرد بازدارندگی تعریف می‌شود:

ـ بازدارندگی از راه انکار: این رویکرد دفاعی، با هدف کاهش شانس موفقیت عملیات روسیه طراحی شده است. ابزارهای آن شامل تقویت تاب‌آوری اجتماعی با آموزش سواد رسانه‌ای، همکاری با شرکت‌های فناوری برای حذف حساب‌های ساختگی و ایجاد نهادهای تخصصی مانند «مرکز ارتباطات راهبردی ناتو» برای شناسایی و افشای کارزارهای اطلاعات نادرست است.

ـ بازدارندگی از راه هزینه: این رویکرد تهاجمی‌تر، به‌دنبال تنبیه روسیه برای اقدام‌هایش است. ابزارهایش شامل تحریم‌های اقتصادی هدفمند علیه افراد و نهادهای دخیل در جنگ اطلاعاتی، پیگرد قانونی عوامل اطلاعاتی و اقدام‌های دیپلماتیک مانند اخراج دیپلمات‌ها می‌شود (Jones, 2025: 15).

1. Samantha Mullaney

شکل۳. مدل تحلیلی کلان «جنگ اطلاعاتی روسیه: معماری راهبردی و پویایی‌ها»



منبع: نویسندگان

مهم‌ترین بعد این رویارویی، پذیرش «چالش عملیات تهاجمی سایبری» از سوی نهادهای غربی است. تحلیل‌های اندیشکده‌هایی مانند «سی‌اس‌آی‌اس»[1] به روشنی خواستار کارزار تهاجمی حساب‌شده علیه روسیه می‌شوند که شامل «عملیات اطلاعاتی و نفوذی است که جمعیت روسیه را هدف قرار می‌دهد» (Jones, 2025: 15).

۱. مرکز مطالعات راهبردی و بین‌المللی (Center for Strategic and International Studies)

نتیجه

این نوشتار در پاسخ به این پرسش که «چه منطق راهبردی، تاریخی و آیین‌محوری، اقدام‌های روسیه در جنگ اطلاعاتی را هدایت می‌کند؟»، نشان می‌دهد که راهبرد اطلاعاتی روسیه پدیده‌ای فقط تهاجمی نیست، بلکه سرشتی واکنشی و دفاعی دارد که در فرهنگ راهبردی «ذهنیت محاصره» و تاریخ جنگ سرد ریشه دارد. این آیین با بهره‌گیری از مفاهیمی مانند «کنترل بازتابی»، ابزاری نامتقارن برای بقا است. رویارویی کنونی، «چرخهٔ خودتقویت‌شونده»[1] ناشی از امنیتی‌سازی متقابل است. غرب اقدام‌های مسکو را تهدید وجودی می‌خواند و روسیه نیز با استناد به تحرک‌های غرب (مانند گسترش ناتو)، آن را تهدیدی علیه حاکمیت خود می‌داند. در این چرخه، هر دو طرف با تفسیر اقدام‌های یکدیگر به‌عنوان تأیید نیت‌های خصمانه، خود را مدافع و طرف مقابل را متجاوز می‌پندارند.

این پویایی، همان چیزی است که مرشایمر (۲۰۲۲) آن را «حقیقت تراژیک» می‌نامد: «حقیقت تراژیک این است که اگر غرب توسعهٔ ناتو در اوکراین را دنبال نمی‌کرد، بعید بود که امروز جنگی در اوکراین رخ دهد و کریمه همچنان بخشی از اوکراین باقی می‌ماند». در واقع، این جنگ روایت‌ها بازتابی از همین رویارویی راهبردی است که در آن، هر دو طرف خود را مدافع و دیگری را متجاوز می‌بینند. این دو جهان‌بینی ناسازگار، یعنی رویکرد غربی در برابر رویکرد روسی، هرگونه اجماع بر سر قوانین بازی را غیرممکن می‌کند. در نتیجه، اگرچه هر دو طرف درگیر جنگ اطلاعاتی هستند، فلسفه‌ها، تاکتیک‌ها و هدف‌های بنیادین آن‌ها به‌طور قابل توجهی متفاوت است. این تفاوت‌ها برآمده از نظام‌های سیاسی و الزام‌های راهبردی هریک از آن‌ها است. در این نوشتار با تمرکز بر جایگاه «فرستنده» آیین روسیه را بررسی کردیم. پیشنهاد می‌شود پژوهش‌های آینده با رویکرد «گیرنده»، به سنجش میزان پذیرش روایت‌ها توسط مخاطبان، اثربخشی واقعی «کنترل انعکاسی» بر تصمیم‌گیری‌های غرب و طراحی مدل‌های ارزیابی تأثیرهای روانی جنگ شناختی بپردازند تا درک عمیق‌تری از این رویارویی به دست آید.

1. Feedback Loop

جدول ۲. دو فلسفهٔ متضاد برای نظم اطلاعاتی جهانی

ویژگی	رویکرد روسیه	رویکرد غرب
چارچوب	جامع و یکپارچه با دیگر شکل‌های جنگ، فعالیتی دائمی	به‌طور سنتی بیشتر بر عملیات اطلاعاتی تاکتیکی هنگام درگیری‌ها متمرکز بوده است، اما اکنون درحال تحول به‌سوی درک گسترده‌تری از محیط اطلاعاتی است.
هدف‌ها	بی‌ثبات‌کردن دشمنان، کاشتن بذر بی‌اعتمادی، تقسیم جوامع، تحمیل تصمیم‌ها و بازپس‌گیری حوزهٔ نفوذ خود	مقابله با روایت‌های ساختگی، ترویج ارزش‌های دموکراتیک و اطلاعات دقیق، پاسداری از زیرساخت‌های حیاتی و ایجاد تاب‌آوری در برابر اطلاعات نادرست
تاکتیک‌ها	اطلاعات نادرست، روایت‌های جهت‌دار، هک، حمله‌های سایبری، استفاده از نیروهای نیابتی، مزارع ترول و دیپ‌فیک	راستی‌آزمایی، برنامه‌های سواد رسانه‌ای، ارتباطات راهبردی، اشتراک‌گذاری اطلاعات و پیش‌خنثی‌سازی[1]
کنترل داخلی	کنترل شدید رسانه‌های داخلی و جریان اطلاعات، سانسور و نظارت	تأکید بر رسانه‌های آزاد و مستقل، شفافیت و بیشینه‌کردن دسترسی به اطلاعات

منبع: نویسندگان

منابع

فارسی

آقایی، سیدداود و رضا عبداللهی (۱۴۰۴)، «امنیت انرژی اتحادیهٔ اروپا زیر تأثیر تهدیدهای سایبری روسیه»، **مطالعات اوراسیای مرکزی**، دورهٔ ۱۸، شمارهٔ ۱، صص. ۲۸-۱، (doi:

1. Pre-Bunking

.10.22059/jcep.2025.394596.450321

باقری، رضا و علیرضا کاظمی (۱۴۰۲)، «امنیتی‌سازی مجدد روسیه توسط ناتو و کشورهای غربی بر اساس نظریهٔ امنیت جمعی»، **مطالعات کشورها**، دورهٔ ۱، شمارهٔ ۴، صص.۶۰۷-۶۳۰، (doi: 10.22059/jcountst.2023.363511.1051).

بلنک، استفن جی (۱۴۰۴)، **چشم‌انداز امروزین ارتش روسیه**، برگردان: الهه کولایی و سیده مطهره حسینی، تهران: دانشگاه تهران.

حاجی یوسفی، امیرمحمد و عباس ذوالفقاری (۱۳۹۶)، «فرهنگ راهبردی و سیاست خارجی خاورمیانه‌ای روسیه»، **روابط خارجی**، دورهٔ ۹، شمارهٔ ۲، صص. ۱۶۵-۱۹۲، قابل دسترسی در: (https://dor.isc.ac/dor/20.1001.1.20085419.1396.9.2.6.9)، (تاریخ دسترسی: ۱۴۰۴/۰۷/۰۳).

خان‌محمدی، زهره (۱۴۰۱)، «جنگ اطلاعاتی و شناختی روسیه و تأثیرگذاری اجتماعی و افکار عمومی؛ مطالعهٔ موردی اوکراین»، **امنیت بین‌الملل**، دورهٔ ۵، شمارهٔ ۴۲، صص.۱۴۳-۱۶۰، قابل دسترسی در: https://isdsac.ir/monthly-magazines/# (تاریخ دسترسی: ۱۴۰۴/۰۷/۰۳).

خان‌محمدی، زهره (۱۴۰۱)، «راهبرد بازدارندگی چندوجهی روسیه (متعارف، هسته‌ای، سایبری، تروریسم)»، **امنیت بین‌الملل**، دورهٔ ۵، شمارهٔ ۴۱، صص. ۱۵۵-۱۷۳، قابل دسترسی در: https://isdsac.ir/monthly-magazines/# (تاریخ دسترسی: ۱۴۰۴/۰۷/۰۳).

دهقانی‌فیروزآبادی، سیدجلال و منوچهر مرادی (۱۳۹۵)، «تهدید غرب، برداشت روسیه و بحران اوکراین»، **روابط خارجی**، دورهٔ ۸، شمارهٔ ۲، صص. ۲۵-۵۵، قابل دسترسی در: (https://dor.isc.ac/dor/20.1001.1.20085419.1395.8.2.2.8)، (تاریخ دسترسی: ۱۴۰۴/۰۷/۰۳).

دهقانی فیروزآبادی، سیدجلال و مهدی امیری (۱۳۹۷)، «زمینه‌یابی سه‌وجهی جایگاه قدرت نرم در سیاست خارجی روسیه (۲۰۱۹-۲۰۰۰)»، **سیاست جهانی**، دورهٔ ۷، شمارهٔ ۴، صص. ۹۹-۱۳۲، (doi: 10.22124/wp.1970.3472).

رحیمی‌چسلی، قاسم، مجید روحی‌دهبنه و مهناز گودرزی (۱۴۰۲)، «بررسی تقابل ایالات متحده و فدراسیون روسیه در بحران اوکراین از دریچهٔ فرهنگ راهبردی»، **سیاست جهانی**، دورهٔ ۱۲، شمارهٔ ۳، صص.۲۹-۵۲،
(doi: 10.22124/wp.2024.25438.3247).

زهرانی، مصطفی و صارم شیراوند (۱۳۹۶)، «بررسی تأثیر فرهنگ راهبردی بر سیاست خارجی

فدراسیون‌روسیه»، **مطالعات آسیای مرکزی و قفقاز**، دورهٔ ۲۳، شمارهٔ ۹۷، صص.۱۰۳-۱۳۷. قابل دسترسی در:
https://ca.ipisjournals.ir/article_24967_b05f1c54b7595590394fdef928ede449.pdf (تاریخ دسترسی: ۱۴۰۴/۰۷/۰۹).

سیمبر، رضا و دانیال رضاپور (۱۳۹۷)، «قدرت نرم روسیه در خارج نزدیک؛ ابزارها و چالش‌ها»، مطالعات **آسیای مرکزی و قفقاز**، دورهٔ ۲۴، شمارهٔ ۱۰۴، صص. ۶۲-۹۱، قابل دسترسی در: https://ca.ipisjournals.ir/article_35025.html (تاریخ دسترسی: ۱۴۰۴/۰۷/۰۳).

قربانی شیخ‌نشین، ارسلان و حمید احمدی‌نژاد (۱۴۰۲)، «تحلیل روایی بحران اوکراین؛ تقابل روایت‌ها و پادروایت‌ها»، **مطالعات اوراسیای مرکزی**، دورهٔ ۱۶، شمارهٔ ۲، صص.۲۴۷-۲۷۲، (doi: 10.22059/jcep.2023.361309.450152).

کرمی، جهانگیر (۱۴۰۳)، «مکتب ژئوپلیتیک روسی؛ معمای پایداری آسیب‌پذیری و گسترش گرایی»، **مطالعات اوراسیای مرکزی**، دورهٔ ۱۷، شمارهٔ ۱، صص. ۳۳۳-۳۰۹، (doi: 10.22059/jcep.2024.374703.450211).

کولایی، الهه، سیکا سعدالدین و زهره خان‌محمدی (۱۴۰۱)، **مجموعه سندهای راهبردی فدراسیون روسیه (۲۰۲۱-۱۹۹۳)**، گردآوری و ترجمه، تهران: پژوهشکده مطالعات راهبردی.

کولایی، الهه و فاطمه عرفانی (۱۴۰۳)، «بهره‌برداری آمریکا از انقلاب‌های رنگی در روابط با روسیه»، **انقلاب‌پژوهی**، دورهٔ ۲، شمارهٔ ۳، صص.۲۷-۵۰، (doi:10.22034/fademo.2024.478718.1055).

لطفیان، سعیده (۱۴۰۴)، «تهدیدهای هسته‌ای در جنگ اوکراین و تأثیر افکار عمومی روسیه بر سیاست بازدارندگی هسته‌ای کرملین»، **مطالعات اوراسیای مرکزی**، دورهٔ ۱۸، شمارهٔ ۱، صص. ۳۰۳-۳۳۴ ، (doi: 10.22059/jcep.2025.390640.450305).

مصلی‌نژاد، عباس (۱۳۹۲)، «موازنهٔ راهبردی و سیاست‌گذاری امنیتی روسیه در نظام بین‌الملل»، **مطالعات اوراسیای مرکزی**، دورهٔ ۶، شمارهٔ ۲، صص. ۱۲۱-۱۴۰، (doi: 10.22059/jcep.2014.36774).

نورمحمدی، مرتضی (۱۴۰۰)، «فضای مجازی و تحول مفهوم و اشکال جنگ در روابط بین‌الملل»، **امنیت بین‌الملل**، دورهٔ ۴، شمارهٔ ۲۷، صص. ۳۸-۴۹. قابل دسترسی در: https://isdsac.ir/monthly-magazines/# (تاریخ دسترسی: ۱۴۰۴/۰۷/۱۲).

وثوقی، سعید و علی موسائی (۱۴۰۳)، «نقش غرب در بحران‌های ۲۰۱۴ و ۲۰۲۲ اوکراین و طولانی‌شدن آن‌ها»، **مطالعات اوراسیای مرکزی**، دورهٔ ۱۷، شمارهٔ ۲، صص. ۴۶۳-۴۹۰، (doi: 10.22059/jcep.2024.377585.450230).

English

Alieksiejchenko, Oleksander (2024), "Frozen Conflicts in the Post-Soviet Area as a Tool of Russian Influence in the Region", **International Relations**, Vol. 58, No. 1, pp. 41–45, (doi: 10.17721/1728-2292.2024/1-58/41-45).

Belin, Laura (2002), "Russian Media Policy in the First and Second Chechen Campaigns", 52nd Conference of the Political Studies Association, Aberdeen, Scotland, Available at: https://bleedingheartland.com/static/media/2018/12/Belin2002conferencepaper.pdf (Accessed on: 10/08/2025).

Bryc, Agnieszka, and Maria Domańska (2024), "Russia in the Trenches of Cognitive Warfare", **New Eastern Europe**, Available at: https://neweasterneurope.eu/2024/09/09/russia-in-the-trenches-of-cognitive-warfare/ (Accessed on: 09/08/2025).

Brzezinski, Ian and Ryan Arick (2025), "A NATO Strategy for Countering Russia", **Atlantic Council, Scowcroft Center for Strategy and Security**, Available at: https://www.atlanticcouncil.org/wp-content/uploads/2025/02/A-NATO-strategy-for-countering-Russia.pdf (Accessed on: 15/09/2025).

Burt, Tom (2022), "The Hybrid War in Ukraine", **Microsoft on the Issues**, Available at: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/ (Accessed on: 03/08/2025).

Doctrine of Information Security of the Russian Federation (2016), **Russian Federation** (Security Council of the Russian Federation, December 2016, No. 646), Available at: http://www.scrf.gov.ru/security/information/DIB_engl/ (Accessed on: 18/09/2025).

Fisher, Henry O (2023), **Media Objectivity and Bias in Western Coverage of the Russian-Ukrainian Conflict**, Master's Dissertation, Södertörn University, Available at: https://www.divaportal.org/smash/get/diva2:1766691/FULLTEXT01.pdf (Accessed on: 11/08/2025).

GT Investigates: Western Freelance Journalists Expose NATO Propaganda Fomenting Ukraine Crisis, Suffer Merciless Attacks by 'Civilized' West (2022), **Global Times Reporters**, Available at: https://www.globaltimes.cn/page/202206/1268125.shtml (Accessed on: 17/08/2025).

Huntley, Shane (2023), "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape", **Google Threat Analysis Group**, Available at: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/(Accessed on: 05/08/2025).

Information Warfare by Russia: Focus on Its Strategies, Objectives, and Case Studies (2024), **Nakasone Peace Institute**, Available at: https://www.npi.or.jp/en/research/data/dfc9df0a88f4dd46e0a67a19dac82fa168ee9870.pdf (Accessed on: 22/09/2025).

Investing in Freedom: An Introduction to the National Endowment for Democracy (2025), **National Endowment for Democracy**, Available at: https://www.ned.org/investing-in-freedom-an-introduction-to-the-national-endowment-for-democracy/ (Accessed on: 25/08/2025).

Jervis, Robert (1976), **Perception and Misperception in International Politics**, Princeton: Princeton University Press.

Jones, Seth G (2025), "Russia's Shadow War Against the West (CSIS Briefs)", **Center for Strategic and International Studies**, Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250318_Jones_Russia_Shadow.pdf (Accessed on: 14/09/2025).

Jordash, Wayne, Scott Martin, Anastasiia Vorobiova, Nadiia Vaskivska, Vitalii Zhuhai, and Peter Pomerantsev (2025), "Manufacturing Impunity: Russian Information Operations in Ukraine", **Global Rights Compliance**, Available at: https://globalrightscompliance.org/wp-content/uploads/2025/05/Manufacturing-Impunity.pdf (Accessed on: 26/09/2025).

Lim, Gabrielle and Samantha Bradshaw (2023), "Chilling Legislation: Tracking the Impact of 'Fake News' Laws on Press Freedom Internationally", **Center for International Media Assistance (CIMA)**, Available at: https://cima.ned.org/publication/chilling-legislation/ (Accessed on: 29/08/2025).

Litvinova, Dasha (2025), "Going Online in Russia Can Be Frustrating, Complicated and Even Dangerous", **The Associated Press**, Available at: https://apnews.com/article/russia-internet-censorship-social-media-youtube-web-2b3c7ca90f83573be7af7f3fc20f9ecd (Accessed on: 13/10/2025).

Mearsheimer, John J. (2014), "Why the Ukraine Crisis is the West's Fault: The Liberal Delusions that Provoked Putin", **Foreign Affairs**, Vol. 93, No. 5, pp. 77–89, Available at: https://www.mearsheimer.com/wp-content/uploads/2019/06/Why-the-Ukraine-Crisis-Is.pdf (Accessed on: 24/10/2025).

Mearsheimer, John J. (2022), "The Causes and Consequences of the Ukraine War", **Horizons**, Summer, No. 21, pp. 12–27, Available at: https://www.cirsd.org/files/000/000/009/75/401141581c665840ebdf7c1304da4a9486211f99.pdf (Accessed on: 17/09/2025).

Meister, Stefan (2016), "Isolation and Propaganda: the Roots and Instruments of Russia's Disinformation Campaign", **Transatlantic Academy Paper Series**, April, No. 6, pp. 1-14, Available at: https://dgap.org/system/files/article_pdfs/meister_isolationpropoganda_apr16_web_1.pdf (Accessed on: 11/08/2025).

Mullaney, Samantha (2022), "Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020", **The Cyber Defense Review**, Vol. 7, No. 4, pp. 193–211, Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/12_Mullaney.pdf (Accessed on: 19/08/2025).

Mullins, Sam (2024), "The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence", **Irregular Warfare Center**, Available at: https://irregularwarfarecenter.org/wp-content/uploads/The-Role-of-Non-State-Actors-as-Proxies-in-Irregular-Warfare-and-Malign-State-Influence.pdf (Accessed on: 11/09/2025).

Østbø, Jardar (2024), "The Russian Hybrid Intelligence State: Reconceptualizing the Politicization of Intelligence and the 'Intelligencization' of Politics", **Intelligence and National Security**, Vol. 39, No. 6, pp. 963–985, (doi:org/10.1080/02684527.2024.2370134).

Pucek, Kaspar, and Bob Deen (2024), "NATO's New Russia Strategy Requires a Better Understanding of the Threat from Moscow (and How to Counter It)", **Clingendael Institute**, Available at: https://www.clingendael.org/publication/natos-new-russia-strategy-requires-better-understanding-threat-moscow-and-how-counter (Accessed on: 14/07/2025).

Puustinen, Jussi (2023), "A Look into the Origins of Russian Strategic Culture", **Combined Strategic Analysis Group**, Available at: https://nesa-center.org/dev/wp-content/uploads/2023/07/2023-0711_A-Look-into-the-Origins-of-Russian-Strategic-Culture.pdf (Accessed on: 19/07/2025).

Rathbone, John P., Henry Foy, and Raphael Minder (2024), "West Grapples with Response to Russian Sabotage Attempts", **Financial Times**, Available at: https://www.ft.com/content/bf128ebf-2e3f-40a3-b7ec-bcd1b477ab9a (Accessed on: 13/08/2025).

Robinson, Olga, Alistair Coleman, and Shayan Sardarizadeh (2019), "A Report of Anti-Disinformation Initiatives", **Oxford Technology & Elections Commission, Oxford Internet Institute**, Available at: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/08/A-Report-of-Anti-Disinformation-Initiatives.pdf (Accessed on: 13/08/2025).

Rodari, Adriano (2021), "Russia's (Un) Controlled Disinformation", **Duodecim Astra**, No. 1, pp. 98–120, Available at: https://www.coleurope.eu/sites/default/files/uploads/page/11%20Adriano%20Rodari%20%20Russia%E2%80%99s%20%28un%29Controlled%20Disinformation%20%28Duodecim%20Astra%29_0.pdf (Accessed on: 07/10/2025).

Sabanadze, Natalie and Galip Dalay (2025), Understanding Russia's Black Sea Strategy: How to Strengthen Europe and NATO's Approach to the Region, **Chatham House**, Available at: https://www.chathamhouse.org/sites/default/files/2025-07/2025-07-28-russias-black-sea-strategy-sabanadze-dalay.pdf (Accessed on: 26/08/2025).

Shires, James (2020), "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics", **Texas National Security Review**, Vol. 3, No. 4, pp. 11-28, Available at: https://tnsr.org/wp-content/uploads/2020/08/TNSR-Vol3-Iss4-Shires.pdf (Accessed on: 24/09/2025).

Snyder, Jack L. (1977), "The Soviet Strategic Culture: Implications for Limited Nuclear Operations", **RAND Corporation**, Available at: https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf (Accessed on: 05/10/2025).

Sprague, Andrew (2016), Russian Meddling in Its Near Abroad: The Use of Frozen Conflicts as a Foreign Policy Tool, No. 28, pp. 1-28, Institut Barcelona d'Estudis Internacionals, Available at: https://www.ibei.org/ibei_studentpaper28_71440.pdf (Accessed on: 01/10/2025).

Stoanova, Eli (2025), "Kremlin Is Preparing Russians for Long-Term Conflict with the West, Says ISW Analysis", **Fakti.bg**, Available at: https://fakti.bg/en/world/989451-kremlin-is-preparing-russians-for-long-term-conflict-with-the-west-says-isw-analysis (Accessed on: 15/09/2025).

The Military Doctrine of the Russian Federation (2014), **Russian Federation** (Approved by the President of the Russian Federation on December 25, 2014, No. Pr.-2976) [English Translation], Available at: https://rusmilsec.blog/wp-content/uploads/2021/08/mildoc_rf_2014_eng.pdf (Accessed on: 22/09/2025).

Thomas, Timothy (2004), "Russia's Reflexive Control Theory and the Military", **Journal of Slavic Military Studies**, Vol. 17, No. 2, pp. 237–256, (doi: 10.1080/13518040490450529).

Topor, Lev, and Alexander Tabachnik (2021), "Russian Cyber Information Warfare: International Distribution and Domestic Control", J**ournal of Advanced Military Studies**, Vol. 12, No. 1, pp. 112–127, (doi: 10.21140/mcuj.20211201005).

Treyger, Elina, Joe Cheravitch, and Raphael S. Cohen (2022), "Russian Disinformation Efforts on Social Media", **RAND Corporation**, Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z2/RAND_RR4373z2.pdf (Accessed on: 29/09/2025).

Ukraine: An Overview of Russia's Cyberattack Activity in Ukraine (2022), **Microsoft Digital Security Unit**, Available at: https://www.iisf.ie/files/UserFiles/Documents/2022/MS_UkraineSpecialReport.pdf (Accessed on: 17/09/2025).

United States Psychological Strategy Plan for General War (NSC 5500–A) (1954), In Foreign Relations of the United States, 1950–1955; The Intelligence Community 1950–1955, **Office of the Historian**, Available at: https://history.state.gov/historicaldocuments/frus1950-55Intel/d127, (Accessed on: 03/08/2025).

Ustyuzhantseva, Olga and Evgeniya Popova (2024), "Shaping Digital Sovereignty in Russia: Actors and Debates", **Problems of Post-Communism**, Vol. 72, No. 1, pp. 76–87, (doi: 10.1080/10758216.2024.2346202).

Vershinin, Aleksandr A. and Alexei A. Krivopalov (2024), "Russian Strategic Culture in Retrospect", **Russia in Global Affairs**, Vol. 22, No. 2, pp. 28–49, (doi: 10.31278/1810-6374-2024-22-2-28-49).

Voo, Julia and Virpratap V. Singh (2025), "Russia's Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications", **The International Institute for Strategic Studies**, Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/06/russias-information--confrontation-doctrine--in-practice-/09-pub25-077-russia-information-confrontation-v5.pdf (Accessed on: 03/10/2025).

Zollmann, Florian (2024), "A War Foretold: How Western Mainstream News Media Omitted NATO Eastward Expansion as a Contributing Factor to Russia's 2022 Invasion of Ukraine", **Media, War & Conflict**, Vol. 17, No. 3, pp. 373–392, (doi: 10.1177/17506352231216908).

Zori, Yuri (2025), "ISW: Kremlin Pushes 'Alone against the West' Myth to Rally Russians against Ukraine and NATO", **Euromaidan Press**, Available at: https://euromaidanpress.com/2025/07/29/isw-kremlin-pushes-alone-against-the-west-myth-to-rally-russians-against-ukraine-and-nato/, (Accessed on: 29/08/2025).