



## جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی‌سازی ایران

اسماعیل دهقان<sup>۱</sup>، افشین متقی دستنائی<sup>۲</sup>

### چکیده

تحولات فضای مجازی در سال‌های اخیر موجب شده است که جنگ روایت‌ها به یکی از مهم‌ترین مؤلفه‌های ژئوپلیتیک نوین و امنیت ملی ایران تبدیل گردد. مسئله اصلی این پژوهش تبیین چگونگی تأثیر کنش‌های بازیگران فراملی و رسانه‌های برون‌مرزی بر امنیتی‌سازی فضای مجازی ایران و آینده‌های محتمل آن است. هدف مقاله تحلیل ساختاری این میدان منازعه و ترسیم سناریوهای فراروی حکمرانی روایی با تأکید بر امنیت شناختی تعریف می‌شود. این پژوهش از نظر روش‌شناسی از رویکرد آینده‌پژوهی کیفی و روش سناریونویسی بهره می‌گیرد و با استفاده از تحلیل خبرگان، هشت متغیر کلیدی مؤثر بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی شناسایی می‌شود. در ادامه، برای این متغیرها حالات مطلوب، ایستا و بحرانی تعریف می‌گردد و با تدوین ماتریس‌های سازگاری متقابل، سناریوهای کلان استخراج و ارزیابی می‌شوند. یافته‌ها نشان می‌دهد که سناریوی ایستا با عنوان تعادل روایی شکننده با احتمال ۳۸/۸۸ درصد محتمل‌ترین وضعیت آینده است، در حالی که سناریوی بحرانی با احتمال ۳۳/۳۳ درصد و سناریوی مطلوب با احتمال ۲۷/۷۹ درصد در رتبه‌های بعدی قرار می‌گیرند. نتایج پژوهش نشان می‌دهد که آینده جنگ روایت‌ها در فضای مجازی ایران بیش از آنکه به شدت مداخله خارجی وابسته باشد، به کیفیت حکمرانی روایی و توان مدیریت سناریوهای آینده وابسته است. پژوهش نتیجه می‌گیرد که استمرار وضعیت ایستا می‌تواند به صورت تدریجی امنیت شناختی کشور را تضعیف کند و گذار آگاهانه به سمت بازدارندگی هوشمند و حکمرانی شناخت‌محور به‌عنوان راهبردی پیش‌دستانه برای کاهش آسیب‌پذیری ژئوپلیتیکی ایران در فضای مجازی ضرورت پیدا می‌کند.

**واژگان کلیدی:** ژئوپلیتیک فضای مجازی، جنگ روایت‌ها، امنیتی‌سازی، حکمرانی فضای مجازی، سناریوی آینده‌پژوهانه.

۱. دانشجوی دکتری جغرافیای سیاسی، گروه جغرافیای سیاسی، دانشکده جغرافیا، دانشگاه خوارزمی (نویسنده مسئول)

۲. استاد جغرافیای سیاسی، دانشکده جغرافیا، دانشگاه خوارزمی.

# The Battle of Narratives in the Geopolitics of Cyberspace and the Future Scenarios of Iran's Securitization

*Ismail Dehghan<sup>1</sup>, Afshin motaghi Dastenaie<sup>2</sup>*

## Abstract

The developments in cyberspace in recent years have made the battle of narratives one of the most important components of modern geopolitics and national security in Iran. The main issue of this research is to explain how the narrative action of transnational actors and cross-border media affects the securitization of Iran's cyberspace and its possible futures. The aim of the article is to analyze the structure of this conflict field and to draw scenarios for narrative governance with an emphasis on cognitive security. In terms of methodology, this research uses a qualitative futures research approach and scenario writing method, and using expert analysis, eight key variables affecting the battle of narratives in cyberspace and geopolitics are identified. Subsequently, desirable, static, and critical states are defined for these variables, and macro scenarios are extracted and evaluated by developing mutual compatibility matrices. The findings show that the static scenario, titled fragile narrative equilibrium, is the most likely future state with a probability of 38.88 percent, while the critical scenario with a probability of 33.33 percent and the favorable scenario with a probability of 27.79 percent are ranked next. The results of the study show that the future of the battle of narrative in Iran's cyberspace depends more on the quality of narrative governance and the ability to manage future scenarios than on the intensity of foreign intervention. The study concludes that the continuation of the static situation can gradually weaken the country's cognitive security, and a conscious transition towards smart deterrence and cognitive-based governance is necessary as a proactive strategy to reduce Iran's geopolitical vulnerability in cyberspace.

**Keywords:** Cyberspace Geopolitics; Narrative Warfare; Securitization; Cyberspace Governance; Futures Scenario Planning.

1. Ph.D candidate, Geopolitics, Department of Geopolitics, Faculty of Geography, Kharazmi University (Writer-in-charge)

2. Geopolitics, Lecturer, Faculty of Geography, Kharazmi University





## مقدمه و بیان مسئله

در هزاره سوم، فضای مجازی از یک بستر ارتباطی صرف عبور کرده و به میدان اصلی منازعات ژئوپلیتیکی و عرصه جنگ روایت‌ها بدل شده است. توسعه شتابان فناوری‌های دیجیتال سبب شده است که مرزهای جغرافیایی و حاکمیتی کمرنگ شوند و بازیگران رقیب برای تسخیر اذهان و مهندسی افکار عمومی تلاش کنند. این تحولات در جمهوری اسلامی ایران نیز به دلیل موقعیت خاص ژئوپلیتیکی و فشارهای بین‌المللی، ابعاد پیچیده‌تری یافته است. در این بستر، فضای سایبر تنها محل تبادل اطلاعات نیست، بلکه به کانونی برای تولید معنا، شکل‌دهی به ادراک جمعی و در نهایت امنیتی‌سازی فضای واقعی تبدیل شده است. مسئله بنیادین پژوهش حاضر این است که چگونه جنگ روایت‌ها در زیست‌بوم فضای مجازی، مولفه‌های امنیت ملی ایران را تحت تأثیر قرار می‌دهد و چه سناریوهایی برای آینده این رویارویی متصور است. در واقع، دشمنان با بهره‌گیری از جنگ شناختی و بازنمایی‌های رسانه‌ای، می‌کوشند تا مسائل اجتماعی و فرهنگی را به چالش‌های امنیتی مبدل سازند.

از منظر ژئوپلیتیک انتقادی، امنیت پدیده‌ای عینی و ثابت نیست، بلکه برساخته‌ای است که از طریق گفتمان‌ها و روایت‌های مسلط شکل می‌گیرد. در فضای مجازی، این سازوکار از طریق بمباران اطلاعاتی، شایعه‌پراکنی و برجسته‌سازی کاذب تهدیدات عمل می‌کند و جامعه را در وضعیت اضطراب دائم و واکنش‌پذیری نگه می‌دارد. بنابراین، شناخت دقیق مکانیسم‌های تبدیل «روایت مجازی» به «واقعیت امنیتی» ضرورتی اجتناب‌ناپذیر محسوب می‌شود. پژوهش حاضر با درک این ضرورت، تلاش دارد تا فراتر از توصیف وضعیت موجود، به واکاوی آینده‌های محتمل و سناریوهای پیش‌روی ایران در مواجهه با این پدیده بپردازد. عدم شناخت صحیح از این روندها، می‌تواند موجب غافل‌گیری راهبردی شود و هزینه‌های مدیریت بحران را برای نظام حکمرانی افزایش دهد.

این مطالعه برای دستیابی به دقت علمی و تحلیل نظام‌مند، رویکرد آینده‌پژوهی را اتخاذ کرده است و از روش‌های تحلیل ساختاری و سناریونویسی بهره می‌برد. بدین منظور، پس از شناسایی متغیرهای کلیدی مؤثر بر جنگ روایت‌ها، از نرم‌افزار MICMAC<sup>1</sup> برای سنجش میزان تأثیرگذاری و وابستگی متغیرها استفاده می‌شود. این تحلیل مشخص می‌کند که کدام پیشران‌ها نقشی کلیدی در جهت‌دهی به فضای امنیتی ایران ایفا می‌کنند. در ادامه، نرم‌افزار

1. Matrix of Cross-Impact Multiplication Applied to Classification



Scenario Wizard برای تدوین و پالایش سناریوهای سازگار به کار گرفته می‌شود تا تصاویر شفافی از آینده‌های ممکن، محتمل و مطلوب ارائه گردد. نتایج حاصل از این فرایند، نه تنها به غنای ادبیات نظری در حوزه ژئوپلیتیک سایبری کمک می‌کند، بلکه ابزاری کارآمد برای سیاست‌گذاران امنیتی و فرهنگی فراهم می‌آورد. در نهایت، هدف این پژوهش آن است که با ترسیم نقشه راه آینده، امکان گذار از انفعال در برابر جنگ روایت‌ها به کنشگری هوشمندانه و تأمین امنیت پایدار میسر شود.

### مبانی نظری و پیشینه شناسی تحقیق

تحولات شتابان در فناوری‌های ارتباطی و گسترش شبکه‌های اجتماعی در دهه اخیر، محیط امنیتی جمهوری اسلامی ایران را به صورت بنیادین دگرگون کرده‌اند شکل گرفته است. فضای مجازی دیگر صرفاً بستر تبادل اطلاعات یا سرگرمی محسوب نمی‌شود، بلکه به میدان رقابت ژئوپلیتیکی و نبرد ادراکی میان بازیگران دولتی و غیردولتی تبدیل شده است شکل گرفته است. در این میدان تازه، «ترس» نه فقط پیامد حاشیه‌ای رویدادها، بلکه خود به «بزار قدرت» و «سلاح راهبردی» بدل شده است شکل گرفته است. در چنین وضعیتی، بخشی از کنشگران خارجی و همسو با آنان در داخل، با اتکا بر تکنیک‌های عملیات روانی، هوش مصنوعی مولد، و شبکه‌های اجتماعی جهانی، می‌کوشند تصویر ایران را به عنوان کشوری ناکارآمد، ناامن، در آستانه فروپاشی و فاقد مشروعیت سیاسی بازنمایی کنند ساخته‌اند. این روند موجب شکل‌گیری آن چیزی می‌شود که در این پژوهش از آن با عنوان «ترس دروغین دیجیتال» یاد می‌شود تعریف می‌گردد. ترسی که نه بر تجربه زیسته اکثریت جامعه و نه بر داده‌های عینی مبتنی است، بلکه عمدتاً محصول برجسته‌سازی گزینشی اتفاقات، تحریف واقعیت‌ها، و تولید انبوه روایت‌های سیاه‌نما در پلتفرم‌های فراملی است تشکیل می‌شود.

این «ترس دیجیتال» اگر بدون مدیریت فعال رها شود، می‌تواند به کاهش سرمایه اجتماعی، فرسایش اعتماد به نهادهای قانونی، و در نهایت تبدیل نارضایتی‌های پراکنده به کنش‌های پرریسک خیابانی بینجامد و امنیت ملی را تضعیف کند منجر شود. از همین رو، سیاست‌های حاکمیت در تنظیم و حکمرانی بر فضای مجازی را نمی‌توان صرفاً از زاویه «محدودیت» یا «کنترل» فهم کرد، بلکه باید آن را در چارچوب «دفاع مشروع» یک دولت در برابر جنگ ترکیبی ادراکی، سایبری و رسانه‌ای تحلیل نمود تفسیر شود. تجربه حملات سایبری پیچیده مانند «استاکس‌نت»



علیه زیرساخت‌های هسته‌ای ایران در دهه گذشته، نشان داد که دشمنان ایران نه فقط در پی فشار اقتصادی و نظامی، بلکه در پی تضعیف مؤلفه‌های قدرت ملی در همه ابعاد - از جمله قدرت نرم، سرمایه اجتماعی، و انسجام روایتی - هستند آشکار شده است (Lindsay, 2013). در واکنش به این شرایط، ایجاد و تقویت نهادهایی مانند شورای عالی فضای مجازی و تدوین سیاست‌های کلان شبکه ملی اطلاعات، در واقع تلاشی برای بازبانی حاکمیت ملی در عرصه‌ای است که شرکت‌های فراملی، پلتفرم‌های غربی و دولت‌های رقیب می‌کوشند آن را به حیطه خلوت ژئوپلیتیکی خود بدل کنند صورت گرفته است (Deibert, 2019).

از این منظر، پرسش اصلی پژوهش حاضر آن است که در چارچوب جنگ روایت‌ها در ژئوپلیتیک فضای مجازی، سیاست‌های امنیتی‌سازی و دفاعی جمهوری اسلامی ایران چگونه شکل می‌گیرند و در صورت تداوم روندهای موجود، این آسیب‌ها و تهدیدهای ادراکی ایران را به کدام آینده ممکن خواهند کشاند؟ بر این اساس، اهداف اصلی فصل اول عبارت‌اند از: تبیین مفهومی جنگ روایت‌ها در ژئوپلیتیک فضای مجازی انجام می‌گیرد، توضیح نظریه امنیتی‌سازی و انطباق آن با شرایط ایران صورت می‌پذیرد؛ معرفی مفهوم «ترس دروغین دیجیتال» و پیوند آن با مشروعیت سیاسی و امنیت ملی صورت می‌گیرد؛ تبیین منطق دفاع مشروع حاکمیت و ضرورت حکمرانی هوشمند بر فضای مجازی ارائه می‌شود.

### پیشینه شناسی تحقیق

در سطح بین‌المللی، ادبیات قابل توجهی درباره تأثیر فضای مجازی بر امنیت ملی و جنگ روایت‌ها شکل گرفته است شکل گرفته است. مطالعاتی مانند (Riordan, 2023) مفهوم «ژئوپلیتیک روایت‌ها» را طرح کرده و نشان می‌دهند که چگونه دولت‌ها و بازیگران غیردولتی با استفاده از روایت‌های تجزیه‌طلبانه، قومیتی و هویتی، انسجام کشورهای هدف را تضعیف می‌کنند نشان داده‌اند. در حوزه امنیت سایبری، آثار متعددی از اندیشکده RAND به تأثیر عملیات اطلاعاتی و نفوذ دیجیتال بر ثبات سیاسی کشورها اشاره کرده‌اند و نشان داده‌اند که چگونه حملات شناختی می‌توانند به اندازه حملات نظامی، نظم سیاسی را متزلزل کنند پرداخته‌اند (RAND, 2020). مطالعاتی مانند (Deibert, 2019) نیز مفهوم «کنترل دیجیتال حاکمیتی» را به عنوان واکنش دولت‌ها به سلطه پلتفرم‌های فراملی و تهدیدات سایبری مطرح کرده‌اند بر جسته کرده‌اند. با وجود



این، بسیاری از این پژوهش‌ها ایران را از زاویه نگاه بیرونی و اغلب با پیش فرض‌های انتقادی نسبت به سیاست‌های حاکمیتی تحلیل کرده و کمتر به منطق دفاعی و شرایط ویژه فشارهای خارجی علیه ایران توجه کرده‌اند نادیده گرفته‌اند.

در داخل ایران، حوزه‌های مختلفی به بررسی ابعاد اجتماعی و امنیتی فضای مجازی پرداخته‌اند شکل گرفته است. بخشی از ادبیات به تأثیر شبکه‌های اجتماعی بر سرمایه اجتماعی، اعتماد عمومی و مشارکت سیاسی اختصاص دارد (فاضلی، ۱۳۹۸؛ حسینی و همکاران، ۱۴۰۰) انجام شده است. مطالعات دیگری نقش فضای مجازی در بروز ناآرامی‌های مقطعی و بسیج‌های سریع اجتماعی را بررسی کرده و بر ضرورت حکمرانی هوشمند تأکید کرده‌اند پرداخته‌اند (افراسیابی و زارع، ۱۳۹۹). در حوزه امنیت سایبری، پژوهش‌هایی به بررسی تهدیدهای زیرساختی، حملات سایبری و ضرورت توسعه شبکه ملی اطلاعات پرداخته‌اند و تلاش کرده‌اند مدل‌های بومی امنیت دیجیتال ارائه دهند صورت پذیرفته است (موسوی، ۱۴۰۱). با این حال، کمتر پژوهشی به طور همزمان سه سطح «ژئوپلیتیک»، «جنگ روایت‌ها» و «آینده پژوهی امنیتی‌سازی<sup>۱</sup>» را در یک چارچوب نظری واحد تلفیق کرده است انجام داده است.

وجه تمایز اصلی این پژوهش در چند نکته کلیدی نهفته است قرار می‌گیرد: نخست آن که، رویکرد این پژوهش اساساً «درون‌زا و دفاعی» است؛ یعنی به جای بازتولید روایت‌های انتقادی غربی، تلاش می‌کند منطق امنیتی‌سازی ایران را در برابر جنگ روایت‌ها، از زاویه حفاظت از حاکمیت ملی و امنیت جمعی تحلیل کند صورت می‌دهد. دوم آن که، این پژوهش جنگ روایت‌ها را نه صرفاً موضوعی رسانه‌ای، بلکه پدیده‌ای ژئوپلیتیکی می‌بیند که در آن فضای مجازی به میدان جدید رقابت قدرت‌های منطقه‌ای و فرمانطقه‌ای بدل شده است تلقی می‌کند. سوم آن که، پژوهش حاضر از ابزارهای آینده پژوهی و تحلیل ساختاری به‌ویژه MICMAC و Scenario Wizard برای ترسیم سناریوهای محتمل فراروی امنیتی‌سازی ایران بهره می‌گیرد و به پرسش «این آسیب‌ها ایران را به کجا خواهد کشاند» به صورت نظام‌مند پاسخ می‌دهد استفاده می‌کند. بدین ترتیب، پژوهش حاضر می‌کوشد پلی میان ادبیات نظری ژئوپلیتیک، مطالعات امنیتی و روش‌های آینده پژوهی ایجاد کند و تصویری واقع‌گرایانه از گزینه‌های پیش‌روی حاکمیت ایران در مدیریت جنگ روایت‌ها ارائه نماید ترسیم کند.



## مبانی نظری

### ژئوپلیتیک و ژئوپلیتیک فضای مجازی

ژئوپلیتیک در تعریف کلاسیک خود، به مطالعه تأثیر عوامل جغرافیایی - شامل موقعیت، منابع و فضا - بر رفتار سیاسی دولت‌ها و توزیع قدرت در نظام بین‌الملل می‌پردازد اطلاق می‌شود (Flint, 2017). با این حال، در دهه‌های اخیر با ظهور فضای سایبری و شبکه‌های مجازی، مفهوم «فضا» دیگر صرفاً به قلمرو فیزیکی محدود نمی‌ماند و حوزه‌ای نو با عنوان «ژئوپلیتیک فضای مجازی» مطرح می‌شود شکل می‌گیرد (Riordan, 2023). در این رویکرد، پلتفرم‌های دیجیتال، زیرساخت‌های ارتباطی، داده‌ها و الگوریتم‌ها به عنوان «قلمروهای جدید قدرت» تلقی می‌شوند و رقابت دولت‌ها برای نفوذ بر افکار عمومی جهانی، کنترل داده‌های راهبردی و شکل‌دهی به روایت‌ها، جلوه‌ای تازه از کشمکش ژئوپلیتیکی را بازنمایی می‌کند آشکار می‌گردد (Demchak & Dombrowski, 2011). ایران به دلیل موقعیت ژئوپلیتیکی خاص خود در آسیای جنوب غربی، منابع انرژی، عمق راهبردی منطقه‌ای و ظرفیت‌های جمعیتی، از دیرباز در کانون رقابت قدرت‌های بزرگ قرار داشته است قرار گرفته است. با دیجیتالی شدن ارتباطات و سیاست، این رقابت از سطح مرزهای فیزیکی به درون گوشی‌های تلفن همراه شهروندان ایرانی منتقل می‌شود و به شکل «نبرد بر سر ادراک ایرانیان نسبت به خود، حاکمیت و آینده کشور» باز تعریف می‌گردد تبدیل می‌شود.

### جنگ روایت‌ها<sup>۱</sup>

«جنگ روایت‌ها» به رقابت سازمان‌یافته بازیگران مختلف برای تحمیل، تثبیت یا بی‌اعتبارسازی داستان‌ها و روایت‌هایی درباره واقعیت سیاسی و اجتماعی اشاره دارد دلالت می‌کند (Riordan, 2023). در این جنگ، هدف صرفاً انتقال اطلاعات نیست، بلکه ساختن «معنا» و «چارچوب تفسیر» برای رویدادهاست، به گونه‌ای که مخاطب جهان را از زاویه‌ای خاص ببیند و بر اساس آن، احساس، قضاوت و کنش کند هدف‌گذاری می‌شود. در جنگ روایت‌ها علیه ایران، چند محور ثابت قابل تشخیص است شکل می‌گیرد: القای تصویر ایران به عنوان کشوری دائماً بحرانی، ناامن و فاقد آینده برای جوانان انجام می‌شود؛ بر جسته‌سازی گزینشی ناکامی‌ها و نادیده گرفتن دستاوردها صورت می‌گیرد؛ شخصی‌سازی و احساساتی کردن روایت‌ها برای دور زدن تفکر نقاد و تحلیل عقلانی به

1. Narrative Warfare



کار گرفته می‌شود؛ پیوند زدن هر مسئله جزئی داخلی با پروژه‌های کلان تغییر نظام سیاسی دنبال می‌شود. این فرایند، بخشی از آن چیزی است که در ادبیات جدید امنیتی و اطلاعاتی از آن با عنوان «جنگ شناختی»<sup>۱</sup> یاد می‌شود؛ جنگی که در آن هدف نه تخریب زیرساخت فیزیکی، بلکه هدف گیری ذهن و اراده جامعه است هدف قرار می‌گیرد (Luna-Reyes & Gil-Garcia, 2021).

## فضای مجازی<sup>۲</sup>

«فضای مجازی» در معنای محدود، به زیرساخت‌های دیجیتال و شبکه‌های ارتباطی اطلاق می‌شود، اما در معنای گسترده‌تر، به تعبیر کاستلز، شبکه‌ای از فضاهای جریان اطلاعات، ارتباطات و معناست که ساختارهای قدرت را دگرگون می‌کند تعبیر می‌شود (Castells, 2012). در ایران نیز فضای مجازی از سطح ابزار ارتباطی فراتر رفته و به «عرصه‌ای برای شکل‌گیری افکار عمومی، بسیج اجتماعی و رقابت گفتمانی» تبدیل شده است تبدیل می‌شود. این فضا، از دو جهت برای امنیت ملی ایران اهمیت می‌یابد بر جسته می‌شود: از یک سو فرصتی برای تقویت ارتباط حاکمیت با مردم، افزایش شفافیت، ارتقای سواد رسانه‌ای و بیان دیدگاه‌ها به‌شمار می‌آید فراهم می‌کند؛ از سوی دیگر، به دلیل حضور پلتفرم‌های خارجی، الگوریتم‌های ناشناخته و امکان مداخله سازمان‌یافته خارجی، بستر آسیب‌پذیری ادراکی و امنیتی نیز محسوب می‌شود شکل می‌گیرد (Deibert, 2019). در چنین شرایطی، حکمرانی بر فضای مجازی - شامل تنظیم مقررات، توسعه زیرساخت بومی، ارتقای سواد رسانه‌ای و مقابله با عملیات روانی - نه به معنای «امنیتی کردن جامعه» بلکه به معنای «حفاظت از حاکمیت ملی در قلمرو دیجیتال» تفسیر می‌شود.

## امنیتی‌سازی ایران<sup>۳</sup>

نظریه «امنیتی‌سازی» که توسط مکتب کینهاگ توسعه یافته، توضیح می‌دهد چگونه یک موضوع از سطح «بحث عادی سیاسی» به سطح «تهدید وجودی» ارتقا می‌یابد و در نتیجه، توجیه‌گر اتخاذ اقدامات فوق‌العاده توسط دولت‌ها می‌شود مطرح می‌کند (Buzan, Wæver, & de Wilde, 1998). در این چارچوب، وقتی بازیگر سیاسی با خطاب قرار دادن مخاطب، موضوعی

1. Cognitive Warfare
2. virtual space
3. Securitization



را به‌عنوان تهدیدی برای «بقای دولت، جامعه یا هویت» معرفی می‌کند و مخاطب نیز این ادعا را می‌پذیرد، فرایند امنیتی‌سازی رخ می‌دهد شکل می‌گیرد. در مورد ایران، بخشی از ادبیات انتقادی غربی، هرگونه اقدام دولت در تنظیم فضای مجازی - از فیلترینگ برخی پلتفرم‌ها تا ایجاد شبکه ملی اطلاعات - را «امنیتی‌سازی فضای عمومی» تفسیر می‌کند و آن را مغایر آزادی بیان معرفی می‌کند بازنمایی می‌کند (RAND, 2020). این در حالی است که از منظر درون‌زا و بومی، این اقدامات بیشتر در چارچوب «پاسخ دفاعی» به تهدیدات ترکیبی و عملیات روانی خارجی قابل فهم است قرار می‌گیرد؛ تهدیداتی که به دنبال تبدیل نارضایتی‌های طبیعی و اصلاح‌طلبانه به بحران مشروعیت و حتی بی‌ثبات‌سازی ساخت سیاسی هستند عمل می‌کنند. بنابراین، این پژوهش میان دو سطح تمایز قائل می‌شود انجام می‌دهد: سطح «امنیتی‌سازی سرکوبگرانه»، که در آن هر نقدی به مثابه تهدید تلقی و منابع قدرت برای خفه کردن صداها بسیج می‌شود تعریف می‌گردد؛ سطح «امنیتی‌سازی دفاعی و بازدارنده»، که در آن دولت در برابر تهدیدات سازمان‌یافته و جنگ روایت‌های دشمن، اقدامات حفاظتی و تنظیمی انجام می‌دهد تا از فروپاشی نظم سیاسی و اجتماعی جلوگیری کند صورت می‌پذیرد. در این چارچوب، سیاست‌های جمهوری اسلامی ایران در حوزه فضای مجازی با همه کاستی‌ها و نیاز به اصلاح بیشتر ذیل منطق دوم یعنی «امنیتی‌سازی دفاعی» قابل تحلیل است، زیرا در یک محیط ژئوپلیتیکی خصمانه و تحت فشار حداکثری، نادیده گرفتن تهدیدات دیجیتال می‌تواند هزینه‌های جبران‌ناپذیری برای امنیت و توسعه کشور به همراه داشته باشد منجر شود.

## روش‌شناسی پژوهش

این پژوهش با هدف تبیین مسیرهای محتمل آینده امنیتی‌سازی جمهوری اسلامی ایران در بستر جنگ روایت‌ها در فضای مجازی انجام می‌شود. با توجه به ماهیت پیچیده و چندبعدی مسئله درهم‌تنیدگی متغیرهای ژئوپلیتیک، فناورانه، اجتماعی و روایتی و سطح بالای عدم قطعیت، روش‌های خطی و پیش‌بینی‌محور کلاسیک کفایت نمی‌کنند و تصویر دقیق و معتبری از آینده ارائه نمی‌دهند. بر همین اساس، چارچوب این پژوهش بر مبنای رویکرد آینده‌پژوهی راهبردی<sup>۱</sup> و به‌طور مشخص بر دو ابزار تحلیل ساختاری MICMAC و سناریوسازی با Scenario Wizard استوار می‌شود. در این رویکرد، ابتدا متغیرهای مؤثر بر آینده جنگ روایت‌ها بر اساس محیط‌شناسی



ژئوپلیتیک فصل دوم استخراج و عملیاتی می‌شوند، سپس روابط متقاطع آن‌ها با MICMAC تحلیل می‌گردند و در نهایت ترکیب‌های سازگار آینده با استفاده از Scenario Wizard به صورت سناریوهای بدیل ترسیم می‌شوند. این زنجیره روش شناختی امکان می‌دهد که روندهای مؤثر بر امنیت ملی ایران در حوزه فضای مجازی نه صرفاً به صورت توصیفی، بلکه به صورت ساختاری، آینده‌نگر و راهبردی تحلیل شوند.

### استخراج و عملیاتی‌سازی متغیرها

گام نخست در روش‌شناسی این پژوهش، استخراج متغیرهای کلیدی مؤثر بر آینده جنگ روایت‌ها و فرآیند امنیتی‌سازی فضای مجازی ایران است. این متغیرها بر پایه چهار محیط تحلیل شده در فصل دوم، یعنی «محیط خارجی»، «محیط داخلی»، «محیط فناورانه» و «محیط اجتماعی-روایتی» شناسایی می‌شوند و سپس به گونه‌ای عملیاتی تعریف می‌گردند که قابلیت استفاده در تحلیل ساختاری MICMAC و سناریوسازی را داشته باشند.

### مراحل استخراج متغیرها

در این مرحله، تمام عوامل، روندها و محرک‌هایی که در متن فصل دوم به‌عنوان پیشران یا مانع در محیط ژئوپلیتیک جنگ روایت‌ها معرفی شده‌اند، به صورت فهرست اولیه متغیرها استخراج می‌شوند. اسنادی مانند مصوبات شورای عالی فضای مجازی، سند سیاست‌های کلی شبکه ملی اطلاعات و گزارش‌های حکمرانی سایبری بررسی می‌شوند تا متغیرهایی که در سیاست‌گذاری رسمی جمهوری اسلامی ایران به‌عنوان عناصر مهم امنیت و حکمرانی فضای مجازی شناخته شده‌اند، شناسایی گردند. مقالات علمی و گزارش‌های اندیشکده‌های داخلی و بین‌المللی درباره جنگ روایت‌ها، عملیات نفوذ شناختی و ژئوپلیتیک سایبری ایران بررسی می‌شوند تا متغیرهای تکرار شونده و مهم در این حوزه استخراج شوند. فهرست اولیه متغیرها در یک فرایند چندمرحله‌ای پالایش می‌شود، متغیرهای هم‌معنا ادغام می‌شوند و متغیرهای بسیار جزئی و غیرراهبردی حذف می‌گردند تا در نهایت مجموعه‌ای قابل مدیریت از متغیرهای کلیدی به دست آید. پنل نخبگانی با توجه به تخصص‌های مرتبط متغیرها را استخراج می‌کنند، تا به عنوان خبرگان بی‌طرف با توجه تخصص به غنای علمی مقاله بیفزایند.



### جدول پنل نخبگانی

ردیف	تخصص	مدرک
۱	ژئوپلیتیک و مطالعات استراتژیک	دکتری روابط بین‌الملل
۲	ژئوپلیتیک و امنیت ملی	کارشناس ارشد علوم سیاسی
۳	ارتباطات و رسانه	دکتری علوم ارتباطات
۴	جامعه‌شناسی افکار عمومی	دکتری جامعه‌شناسی
۵	حکمرانی و سیاست‌گذاری فضای مجازی	دکتری فناوری اطلاعات
۶	مقررات‌گذاری سایبری و شبکه ملی اطلاعات	کارشناس ارشد فناوری اطلاعات
۷	امنیت سایبری و جنگ نرم	دکتری مدیریت راهبردی
۸	امنیت اطلاعات و عملیات سایبری	کارشناس ارشد فناوری اطلاعات
۹	آینده‌پژوهی و تحلیل ساختاری	دکتری جغرافیای سیاسی
۱۰	سناریونویسی راهبردی	دکتری مدیریت استراتژیک
۱۱	ارتباطات و رسانه	دکتری مدیریت فرهنگی

جدول ۱- منبع: نگارندگان

### عملیاتی‌سازی متغیرها برای تحلیل MICMAC

برای آن که متغیرهای استخراج‌شده در چارچوب MICMAC قابل استفاده شوند، هر متغیر به صورت دقیق تعریف مفهومی و سپس به صورت شاخص پذیر تعریف عملیاتی می‌شود. در تعریف عملیاتی، برای هر متغیر، ابعاد قابل اندازه‌گیری (مانند شدت، فراوانی، جهت و سرعت تغییر) مشخص می‌شوند تا خبرگان بتوانند میزان تأثیر هر متغیر بر سایر متغیرها را به صورت عددی در ماتریس اثر متقاطع (۰ تا ۳ یا ۰ تا ۴) برآورد کنند. به این ترتیب، میان تحلیل کیفی فصل دوم و تحلیل کمی - ساختاری فصل سوم پیوند برقرار می‌شود و از گسست روش شناختی جلوگیری می‌شود.

### تحلیل ساختاری متغیرها با استفاده از MICMAC

پس از تعیین مجموعه نهایی متغیرها، برای کشف ساختار درونی سیستم و شناسایی متغیرهای



راهبردی و حساس، از روش تحلیل ساختاری MICMAC استفاده می‌شود. MICMAC ابزاری برای شناسایی متغیرهایی است که بیشترین قدرت تأثیرگذاری و بیشترین سطح وابستگی را در سیستم دارند و به این ترتیب متغیرهای کلیدی، راهبردی، وابسته و محیطی را آشکار می‌کند.

### تشکیل ماتریس اثر متقاطع

در این گام، یک ماتریس مربعی با ابعاد  $n \times n$  تشکیل می‌شود که در آن  $n$  تعداد متغیرهای استخراج‌شده از فصل دوم است. برای هر زوج متغیر  $(I, J)$ ، میزان تأثیر مستقیم متغیر  $I$  بر متغیر  $J$  توسط خبرگان ارزیابی می‌شود. این ارزیابی معمولاً بر اساس یک مقیاس ترتیبی انجام می‌شود که به صورت نمونه شامل مقادیر زیر می‌شود:

۰: عدم تأثیر تعیین می‌شود.

۱: تأثیر ضعیف تعیین می‌شود.

۲: تأثیر متوسط تعیین می‌شود.

۳: تأثیر قوی تعیین می‌شود.

برای کاهش سوگیری، جمع‌آوری قضاوت‌ها از یک پانل چند تخصصی متشکل از خبرگان حوزه‌های ژئوپلیتیک، امنیت سایبری، ارتباطات و جامعه‌شناسی انجام می‌شود و میانگین یا مد نظرات به‌عنوان مقدار نهایی در ماتریس ثبت می‌شود.

### محاسبه تأثیرات مستقیم و غیرمستقیم

پس از تکمیل ماتریس، نرم‌افزار MICMAC ابتدا جمع سطری و ستونی ماتریس را محاسبه می‌کند. جمع سطری، «قدرت تأثیرگذاری مستقیم» هر متغیر را نشان می‌دهد و جمع ستونی، «سطح وابستگی مستقیم» آن متغیر به سایر متغیرها را نشان می‌دهد. در مرحله بعد، MIC-  
MAC با تکرار ضرب ماتریس در خودش، تأثیرات غیرمستقیم (زنجیره‌ای) را محاسبه می‌کند و به این ترتیب متغیرهایی را که در ظاهر کم‌اهمیت‌اند ولی از طریق زنجیره‌ها اثر ساختاری قوی دارند، آشکار می‌کند. در پایان این مرحله، برای هر متغیر دو شاخص کلیدی «قدرت تأثیر» و «سطح وابستگی» به صورت مستقیم و غیرمستقیم محاسبه می‌شود.



## ترسیم نقشه قدرت - وابستگی و طبقه‌بندی متغیرها

خروجی محاسبات MICMAC در یک نمودار دو بعدی (قدرت تأثیر در محور افقی و وابستگی در محور عمودی) نمایش داده می‌شود. بر اساس موقعیت هر متغیر در این صفحه، متغیرها در چهار دسته اصلی طبقه‌بندی می‌شوند.

### متغیرهای راهبردی<sup>۱</sup>

این متغیرها قدرت تأثیر بالا و وابستگی نسبتاً پایینی دارند. تغییر در این متغیرها موجب تغییرات گسترده در کل سیستم می‌شود و به همین دلیل کانون اصلی سیاست‌گذاری و مداخله راهبردی محسوب می‌شوند.

### متغیرهای کلیدی - بحرانی<sup>۲</sup>

این متغیرها هم‌زمان دارای قدرت تأثیر بالا و وابستگی بالا هستند. این متغیرها نقش حلقه‌های میانی زنجیره‌های تأثیر را دارند و هر گونه بی‌ثباتی یا سوءمدیریت در آن‌ها می‌تواند کل سیستم امنیتی‌سازی را شکننده کند.

### متغیرهای وابسته<sup>۳</sup>

این متغیرها قدرت تأثیر پایین و وابستگی بالا دارند و بیش از آن که محرک تغییر باشند، نتیجه و برون‌داد تغییرات در سایر متغیرها محسوب می‌شوند.

### متغیرهای خودمختار یا محیطی<sup>۴</sup>

این متغیرها هم قدرت تأثیر و هم وابستگی پایینی دارند و عمدتاً عناصر محیط عمومی یا زمینه‌ای سیستم به شمار می‌آیند و در کوتاه‌مدت کمتر در حوزه کنترل سیاست‌گذار قرار می‌گیرند. در این پژوهش، توجه ویژه به آن دسته از متغیرهای راهبردی و کلیدی می‌شود که مستقیماً بر دو متغیر «شدت امنیتی‌سازی فضای مجازی» و «سطح اعتماد عمومی به روایت‌های

1. Driver / Key Variables
2. Stake / Relay Variables
3. Dependent Variables
4. Autonomous / Environmental Variables



رسمی» اثر می‌گذارند، زیرا این دو متغیر در سنجش موفقیت یا ناکامی حاکمیت در مدیریت جنگ روایت‌ها نقش تعیین‌کننده‌ای دارند.

### پیوند نتایج MICMAC با مسئله امنیتی‌سازی ایران

نتایج تحلیل MICMAC نه‌تنها ساختار درونی متغیرهای مؤثر بر جنگ روایت‌ها را نمایش می‌دهد، بلکه نشان می‌دهد کدام مسیرهای مداخله، از نگاه راهبردی برای جمهوری اسلامی ایران اولویت دارند. به عنوان نمونه، اگر «سواد رسانه‌ای کاربران» و «ظرفیت شبکه ملی اطلاعات» در زمره متغیرهای راهبردی با تأثیر بالا قرار گیرند، این نتیجه تأیید می‌کند که تمرکز بر تقویت زیرساخت بومی و ارتقای توان تشخیص و مقاوم‌سازی ذهنی جامعه، نسبت به رویکردهای صرفاً محدودساز و انتظامی، کارآمدتر و پایدارتر خواهد بود. بدین ترتیب، MICMAC پایه تحلیلی لازم را برای ورود به مرحله سناریوسازی فراهم می‌کند.

### طراحی سناریوهای آینده با استفاده از Scenario Wizard

پس از شناسایی متغیرهای راهبردی و کلیدی در MICMAC، گام بعدی، بازنمایی ترکیب‌های مختلف آینده از طریق سناریوسازی است که با نرم‌افزار Scenario Wizard انجام می‌شود. این نرم‌افزار با تکیه بر تحلیل سازگاری متقاطع بین حالت‌های مختلف متغیرهای کلیدی، سناریوهای منسجم، محتمل و از نظر منطقی سازگار را تولید می‌کند.

### انتخاب متغیرهای محوری سناریو

نخست، از بین متغیرهای راهبردی و کلیدی شناسایی شده در MICMAC، آن دسته از متغیرهایی که دو ویژگی اهمیت بالا و عدم قطعیت زیاد را هم‌زمان دارند، به عنوان متغیرهای محوری سناریو انتخاب می‌شوند. به طور معمول ۲ تا ۴ متغیر محوری برگزیده می‌شوند تا هم پوشش کافی از فضای مسئله حاصل شود و هم تعداد سناریوها در سطحی قابل تحلیل باقی بماند. در زمینه این پژوهش، متغیرهایی مانند سطح اعتماد عمومی به روایت‌های رسمی، شدت مداخله روایت‌های خارجی و مدل حکمرانی و تنظیم‌گری فضای مجازی در ایران نامزد اصلی متغیرهای محوری محسوب می‌شوند.

## تعریف حالت‌های ممکن برای متغیرهای محوری

برای هر متغیر محوری، چند حالت متمایز و در عین حال واقع‌بینانه تعریف می‌شود. به عنوان مثال: برای «مدل حکمرانی فضای مجازی»، حالت‌هایی مانند «حکمرانی مشارکتی و اقناعی»، «حکمرانی ترکیبی تنظیمی - مشارکتی» و «حکمرانی عمدتاً محدودساز و امنیتی» تعریف می‌شوند، برای «سطح اعتماد عمومی»، حالت‌هایی مانند «اعتماد بالا»، «اعتماد متوسط» و «اعتماد پایین و شکننده» تعریف می‌شوند، برای «شدت مداخله روایت‌های خارجی»، حالت‌هایی مانند «مداخله محدود»، «مداخله هدفمند» و «تهاجم روایتی گسترده» تعریف می‌شوند.

## تشکیل ماتریس سازگاری و محاسبه سناریوها

پس از تعریف حالت‌های ممکن، تمامی ترکیب‌های ممکن از این حالت‌ها تولید می‌شوند. در Scenario Wizard برای هر جفت حالت، میزان سازگاری یا ناسازگاری را بر اساس قواعد و قضاوت‌های خبرگان و با تکیه بر روابط ساختاری کشف‌شده در MICMAC ارزیابی می‌کند. در ادامه، نرم‌افزار ترکیب‌هایی را که بالاترین مجموع سازگاری داخلی را دارند، به عنوان سناریوهای محتمل و قابل دفاع معرفی می‌کند. خروجی نرم‌افزار معمولاً شامل مجموعه‌ای محدود از سناریوهای سازگار است که هر کدام تصویری متفاوت از آینده جنگ روایت‌ها و وضعیت امنیتی‌سازی در ایران ارائه می‌دهند.

## تحلیل کیفی و تأویل راهبردی سناریوها

پس از تولید سناریوها، هر سناریو به صورت کیفی تفسیر می‌شود. در این تفسیر، پرسش اصلی پژوهش یعنی «این آسیب‌ها و چالش‌ها ایران را به کجا خواهد کشاند» از منظر هر سناریو پاسخ داده می‌شود. بر این اساس، به صورت نمونه می‌توان سناریوهای زیر را تبیین کرد:

- سناریوی «بازدارندگی فعال و حکمرانی مشارکتی روایت‌ها» که در آن، با تقویت زیرساخت بومی، افزایش سواد رسانه‌ای و ارتقای اعتماد عمومی، توان حاکمیت برای مدیریت جنگ روایت‌ها بالا می‌رود و فضای مجازی به فرصت تقویت اقتدار ملی تبدیل می‌شود.
- سناریوی «تعادل شکننده و فرسایش اعتماد» که در آن، بخشی از اقدامات ساختاری انجام می‌شود، اما پراکندگی در سیاست‌گذاری و فشارهای خارجی موجب باقی ماندن آسیب‌پذیری‌های جدی در سطح امنیتی‌سازی فضای مجازی می‌شود.





- سناریوی «انزوای سایبری امنیتی و شکنندگی روایتی» که در آن، بدون تقویت زیرساخت و سرمایه اجتماعی، رویکرد یک‌سویه محدودساز اتخاذ می‌شود و در نتیجه، بخش‌هایی از جامعه به سمت پلتفرم‌ها و روایت‌های رقیب رانده می‌شوند و شکاف روایتی تعمیق می‌یابد. روش‌شناسی این پژوهش یک رویکرد ترکیبی و مرحله‌به‌مرحله را دنبال می‌کند. در گام نخست، با اتکا به محیط‌شناسی جنگ روایت‌ها در ژئوپلیتیک‌فصل دوم، متغیرهای مؤثر بر آینده امنیتی‌سازی فضای مجازی ایران استخراج و عملیاتی می‌شوند. در گام دوم، با استفاده از تحلیل ساختاری MICMAC، روابط متقاطع این متغیرها تحلیل می‌شوند، متغیرهای راهبردی و کلیدی شناسایی می‌شوند و نقشه قدرت وابستگی سیستم ترسیم می‌شود. در گام سوم، با بهره‌گیری از Scenario Wizard، ترکیب‌های مختلف از حالت‌های متغیرهای کلیدی بررسی می‌شوند، سناریوهای سازگار آینده تولید می‌شوند و هر سناریو از منظر تأثیر بر آینده امنیتی‌سازی و وضعیت جمهوری اسلامی ایران در جنگ روایت‌ها تحلیل می‌شود. این رویکرد، ضمن پایبندی به دفاع عقلانی و مستند از عملکرد حاکمیت و ظرفیت‌های ساختاری جمهوری اسلامی ایران، امکان می‌دهد تصویر آینده نه بر اساس گمانه‌زنی‌های خطی، بلکه بر اساس تحلیل ساختاری، سناریویی و راهبردی ترسیم شود و مسیرهای بهینه سیاست‌گذاری برای تقویت امنیت روایتی و تاب‌آوری ملی پیشنهاد شوند.

برای تحلیل جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی‌سازی ایران، این پژوهش چارچوب مفهومی خاصی را پیشنهاد می‌کند طراحی می‌کند که بر سه محور اصلی «ترس»، «ادراک» و «کنش امنیتی» استوار است بنا می‌شود.

### مثلث مفهومی ترس - ادراک - کنش امنیتی

در این مدل، «ترس دیجیتال»<sup>۱</sup> نقطه آغاز فرایند تلقی می‌شود تعریف می‌گردد. ترس به وسیله روایت‌ها و تصاویر خاص در فضای مجازی تولید، تقویت یا مهندسی می‌شود و مستقیماً بر ادراک شهروندان نسبت به وضعیت کشور، کارآمدی حاکمیت و آینده خود اثر می‌گذارد تأثیر می‌گذارد. ادراک‌های شکل گرفته، به نوبه خود، الگوی کنش را در دو سطح تعیین می‌کنند، سطح

1. Digital fear



کنش شهروندان (از انفعال و مهاجرت ذهنی تا اعتراض و کنش خیابانی)، سطح کنش حاکمیت (از اصلاحات تدریجی و گفت‌وگوی فعال تا اقدامات بازدارنده و امنیتی‌سازی)، شکل می‌دهد. به بیان دیگر، اگر ترس دیجیتال به صورت کنترل نشده و بدون پاسخ روایتی مناسب رها شود، می‌تواند ادراک منفی و اغراق‌شده‌ای از بحران در جامعه ایجاد کند و حاکمیت را ناگزیر به اتخاذ سیاست‌های سخت‌گیرانه‌تر نماید تبدیل کند. این چرخه می‌تواند به شکل‌گیری «مارپیچ تشدید امنیتی‌سازی»<sup>۱</sup> منجر شود؛ یعنی هر چه ترس دیجیتال بیشتر شود، حاکمیت ناامن‌تر احساس کند و اقدامات امنیتی بیشتری اتخاذ کند و این اقدامات نیز دوباره دستاویز جنگ روایت‌ها برای القای تصویر «حکومت سرکوبگر» گردد و ادراک منفی را تقویت کند باز تولید شود. در مقابل، اگر حاکمیت بتواند با حکمرانی هوشمند بر فضای مجازی - شامل توسعه پلتفرم‌های بومی پر کیفیت، افزایش شفافیت، حضور فعال در عرصه روایت‌سازی، و ارتقای سواد رسانه‌ای جامعه سطح «ترس دروغین دیجیتال»<sup>۲</sup> را کاهش دهد و روایت‌های بدیل معتبر ارائه کند، ادراک عمومی می‌تواند واقع‌بینانه‌تر و متوازن‌تر شود و نیاز به امنیتی‌سازی سخت‌گامش یابد شکل بگیرد.

### جایگاه کاربر ایرانی به عنوان بازیگر میانجی

در این مدل، کاربر ایرانی نه یک قربانی منفعل و نه عامل کاملاً خودمختار بلکه بازیگر میانجی بین پیام دیجیتال و کنش واقعی تلقی می‌شود محسوب می‌گردد. رفتار کاربران از لایک، بازنشر و تولید محتوا گرفته تا مشارکت در هشتگ‌ها و کمپین‌ها نقش تعیین‌کننده‌ای در موفقیت یا شکست جنگ روایت‌ها دارد ایفا می‌کند. سطح سواد رسانه‌ای، اعتماد به رسانه‌های داخلی، تجربه زیسته، تعلق ملی و سرمایه فرهنگی کاربران، متغیرهایی هستند که میزان تأثیرپذیری آنان از ترس دیجیتال را تعیین می‌کنند مشخص می‌سازند (Hosseini et al., 2021). بر این اساس، سیاست‌گذاری حاکمیت اگر صرفاً بر کنترل فنی متمرکز شود و به توانمندسازی شناختی کاربران توجه نکند، در بلندمدت ناپایدار و کم‌اثر خواهد بود باقی می‌ماند.

در دهه‌ی اخیر، به‌ویژه در بازه‌ی زمانی ۲۰۱۹ تا ۲۰۲۵، فضای مجازی از یک ابزار ارتباطی صرف فراتر رفته و به میدان درگیری قدرت‌های سیاسی، اقتصادی و امنیتی در سطح ملی و بین‌المللی تبدیل شده است (Castells, 2024). در این میان، ایران به‌عنوان بازیگری مهم در

1. The spiral of escalating securitization
2. False digital fear



ژئوپلیتیک خاورمیانه، به یکی از کانون‌های اصلی جنگ روایت‌ها بدل شده است؛ جنگی که در آن روایت‌های رقیب درباره‌ی مشروعیت حاکمیت، کارآمدی نظام سیاسی، وضعیت حقوق بشر، نقش منطقه‌ای ایران و حتی سبک زندگی جامعه‌ی ایرانی در حال رقابت و تقابل دائمی هستند (Riordan, 2023). ویژگی متمایز این دوره، تلاقی سه روند است؛ نخست، تشدید فشارهای ژئوپلیتیک و تحریم‌ها علیه ایران؛ دوم، گسترش نفوذ پلتفرم‌های فراملی مانند اینستاگرام، تلگرام و توئیتر در میان کاربران ایرانی؛ و سوم، افزایش وابستگی بخشی از جامعه به روایت‌های تولیدشده خارج از مرزهای حاکمیت ملی (Klein, 2022). بنابراین، فهم جنگ روایت‌ها در ایران بدون درک ساختار محیطی آن، یعنی ترکیب محیط خارجی، داخلی، فناورانه و اجتماعی-روایتی، ممکن نیست. این بخش با اتخاذ رویکردی محیط‌شناختی، تلاش می‌کند شبکه‌ای از فرصت‌ها و تهدیدها را که از تعامل این چهار محیط بر امنیت ملی و انسجام روایی ایران اثر می‌گذارد، تبیین کند. چارچوب کلی این بخش، با نگاه دفاعی نسبت به منطق کنش حاکمیت در برابر فشارهای بیرونی و آسیب‌های درونی تنظیم شده است تا روشن شود چرا حاکمیت در بسیاری از موارد ناگزیر به امنیتی‌سازی فضای مجازی و مدیریت سختگیرانه‌ی روایت‌ها می‌شود.

## محیط خارجی

### الف) بازیگران بین‌المللی

در سطح خارجی، سه گروه از بازیگران بیشترین نقش را در شکل‌دهی به جنگ روایت‌ها علیه ایران در فضای مجازی ایفا می‌کنند؛ قدرت‌های فرامنطقه‌ای به‌ویژه ایالات متحده، بازیگران منطقه‌ای رقیب مانند اسرائیل و عربستان سعودی و شبکه‌ای از سازمان‌ها و رسانه‌های غیردولتی که عمدتاً در غرب مستقر هستند. ایالات متحده با بهره‌گیری از سازوکار «دیپلماسی دیجیتال<sup>۱</sup>» و «قدرت نرم<sup>۲</sup>»، طی سال‌های اخیر تلاش کرده است تصویر ایران را در افکار عمومی جهانی و در میان ایرانیان، در قالب تهدید امنیت بین‌الملل و نظامی غیرقابل اصلاح بازنمایی کند (Riordan, 2023). این سیاست به‌ویژه پس از خروج آمریکا از برجام و تشدید تحریم‌ها، در قالب کمپین‌های رسانه‌ای هماهنگ در توئیتر، یوتیوب و رسانه‌های فارسی‌زبان مستقر در خارج، صورت‌بندی شده است (Klein, 2022). اسرائیل نیز به‌عنوان رقیب منطقه‌ای ایران، راهبرد پیچیده‌تری در حوزه روایت‌ها دنبال کرده است.

1. Digital diplomacy
2. soft power



این بازیگر علاوه بر عملیات سایبری و افشای گزینشی اسناد، از شبکه‌ای از کارشناسان، اندیشکده‌ها و رسانه‌ها برای تثبیت روایت «تهدید هسته‌ای ایران» و «رفتار بی‌ثبات‌کننده‌ی منطقه‌ای تهران» استفاده کرده است (Cohen & Avivi, 2021). در جنگ‌های روایت، هر افشاگری یا عملیات اطلاعاتی، نه فقط یک اقدام امنیتی، بلکه مواد خام تولید روایت ضدایرانی در شبکه‌های اجتماعی محسوب می‌شود. در سطح منطقه، عربستان سعودی و برخی هم‌پیمانان آن، با تکیه بر رسانه‌های برون‌مرزی و کمپین‌های سازمان‌یافته در شبکه‌های اجتماعی، تلاش کرده‌اند ایران را در نقش مداخله‌گر در کشورهای عربی و عامل بی‌ثباتی در خلیج فارس بازنمایی کنند (Al-Dosari, 2023). در این چارچوب، هر رویداد منطقه‌ای مانند بحران یمن، تحولات سوریه یا مناقشه‌ی لبنان، بهانه‌ای برای راه‌اندازی موج‌های رسانه‌ای و حمله‌روایی به ایران در فضای مجازی می‌شود.

### ب) پلتفرم‌های فراملی

پلتفرم‌های فراملی مانند اینستاگرام، تلگرام، ایکس (توییتر سابق) و یوتیوب، در ظاهر شرکت‌های تجاری خصوصی هستند اما در عمل در متن ژئوپلیتیک قدرت و امنیت قرار دارند (Castells, 2024). معماری این پلتفرم‌ها، قوانین استفاده، الگوریتم‌های انتشار محتوا و شیوه‌ی همکاری آن‌ها با دولت‌های غربی، همگی به گونه‌ای است که قدرت بیشتری برای اثرگذاری به بازیگران مستقر در غرب و متحدان آن‌ها می‌دهد. در مورد ایران، پلتفرم‌های دیجیتال فراملی به دلیل استقرار حقوقی و نهادی در خارج از قلمرو حاکمیت دولت ایران و تبعیت از رژیم‌های مقرراتی غربی، عملاً نوعی «حاکمیت دیجیتال موازی»<sup>۱</sup> ایجاد کرده‌اند؛ وضعیتی که در آن تصمیم‌گیری درباره دیده‌شدن یا حذف محتوا، برجسته‌سازی روایت‌ها و جهت‌دهی به افکار عمومی، نه توسط نهادهای قانونی داخلی بلکه توسط شرکت‌های پلتفرمی و اکوسیستم سیاست‌گذاری فناوری در غرب اعمال می‌شود و این فرایند، توان حاکمیت دولت‌ها برای اعمال اراده قانونی و حفاظت از امنیت ملی در قلمرو دیجیتال را به چالش می‌کشد شکل می‌دهد (Deibert, 2021).

### محیط داخلی

#### الف) ساختار قدرت

در داخل کشور، ساختار قدرت در حوزه‌ی فضای مجازی حول چند نهاد کلیدی سامان یافته

1. Parallel digital governance



است؛ شورای عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات، نهادهای امنیتی و فرهنگی، قوه قضاییه، شورای عالی فضای مجازی به‌عنوان نهاد بالادستی، مسئول تعیین سیاست‌های کلان، تدوین راهبردهای دفاعی و امنیتی و هماهنگی میان دستگاه‌های مختلف است. این شورا، به ویژه پس از ۲۰۱۹، بیش از گذشته بر ضرورت حفظ حاکمیت ملی در فضای مجازی و مدیریت جنگ روایت‌ها تأکید کرده است. در این چارچوب، اقداماتی مانند تقویت شبکه ملی اطلاعات، حمایت از پلتفرم‌های داخلی، تدوین مقررات برای مدیریت محتوای مخرب، و ایجاد سازوکارهای رصد و پایش روایت‌های ضدایرانی، بخشی از تلاش ساختار قدرت برای دفاع از امنیت ملی در برابر تهدیدات نرم محسوب می‌شود (Jalili & Riazi, 2022).

### ب) افکار عمومی

افکار عمومی ایران در این دوره تحت تأثیر دو منبع اصلی روایت قرار گرفته است؛ از یک‌سو رسانه‌های رسمی و نهادهای قانونی، و از سوی دیگر، شبکه‌ی گسترده‌ای از رسانه‌های غیردولتی، کانال‌های تلگرامی، صفحات اینستاگرامی، اینفلوئنسرها و رسانه‌های برون مرزی (Ahmadi, 2023). رخدادهای سیاسی و اجتماعی مهم مانند اغتشاشات آبان ۱۳۹۸، شیوع کرونا و فتنه‌ی ۱۴۰۱، به‌ویژه پرونده‌ی مهسا امینی، نشان دادند بخش قابل توجهی از مردم در لحظات بحران به روایت‌های غیررسمی اعتماد بیشتری می‌کنند و این مسئله شکاف روایی میان دولت و جامعه را برجسته کرده است (Rahimi, 2023). این شکاف زمانی خطرناک‌تر می‌شود که روایت‌های غیررسمی از سوی بازیگران خارجی هدایت یا تقویت شوند و به سمت برساختن تصویر دروغ حاکمیت ناکارآمد و سرکوبگر حرکت کنند، زیرا در این حالت، نارضایتی‌های واقعی اجتماعی با روایت‌های طراحی شده‌ی خارجی پیوند می‌خورند و ظرفیت بی‌ثباتی را افزایش می‌دهند (Klein, 2022).

### پ) سیاست‌های نظارتی و تنظیم‌گری

در واکنش به این شرایط، سیاست‌های نظارتی ایران در فضای مجازی، به‌ویژه از سال ۲۰۱۹ به بعد، به سمت سخت‌گیرانه‌تر و در عین حال هدفمندتر شدن حرکت کرده است؛ به‌گونه‌ای که افزایش فیلترینگ پلتفرم‌های خارجی، محدودسازی دسترسی در شرایط بحران‌های امنیتی و اجتماعی، و تلاش برای تدوین و تصویب قوانین جامع‌تر در حوزه حکمرانی داده و کنترل محتوای آنلاین، به‌عنوان بخشی از راهبرد دولت برای مدیریت تهدیدات ادراکی و جنگ روایت‌ها دنبال



می‌شود اتخاذ شده است. از منظر حکمران، این سیاست‌ها قرار است هزینه‌ی عملیات روانی و جنگ روایت‌ها علیه ایران را افزایش دهند و از تبدیل اعتراضات مجازی به نا اغتشاشات میدانی جلوگیری کنند. با این حال، این سیاست‌ها پیامدهای دوگانه‌ای دارند؛ از یک سو قدرت کنترلی دولت را افزایش می‌دهند و از سوی دیگر، در صورت افراط یا سوءاجرا، می‌توانند به گسترش بی‌اعتمادی عمومی و تقویت روایت «انسداد اطلاعاتی» منجر شوند (Castells, 2024). بنابراین، محیط داخلی جنگ روایت‌ها، ترکیبی پیچیده از تلاش برای دفاع و خطر تشدید شکاف دولت جامعه را نشان می‌دهد.

## محیط فناوریانه

### الف) زیرساخت‌های ارتباطی و شبکه ملی اطلاعات

محیط فناوریانه، بستر مادی و فنی جنگ روایت‌ها را تعریف می‌کند. ایران طی سال‌های اخیر سرمایه‌گذاری قابل توجهی در توسعه‌ی شبکه ملی اطلاعات، مراکز داده‌ی داخلی، تقویت پهنای باند داخلی و سامانه‌های بومی DNS<sup>1</sup> و مدیریت ترافیک انجام داده است (Jalili & Riazi, 2022). هدف اصلی این اقدامات، کاهش وابستگی به زیرساخت‌های جهانی و امکان پذیر کردن تاب‌آوری ارتباطی در برابر تحریم‌ها و حملات سایبری است. شبکه ملی اطلاعات برای ایران علاوه بر کارکرد اقتصادی و فنی، کارکرد امنیتی روایتی هم دارد؛ زیرا با تقویت مسیرهای داخلی و ایجاد امکان مدیریت ترافیک، ظرفیت دولت برای کنترل جریان اطلاعات، مقابله با حملات سایبری و کاهش نفوذ پلتفرم‌های خارجی افزایش می‌یابد. حاکمیت این اقدام را بخشی از حق طبیعی خود برای «حفظ حاکمیت دیجیتال» تلقی می‌کند.

### ب) وابستگی به فناوری خارجی و تحریم‌ها

با وجود این تلاش‌ها، ایران همچنان در حوزه‌ی برخی فناوری‌های کلیدی مانند زیرساخت‌های ابری پیشرفته، تجهیزات شبکه‌ی نسل جدید، نرم‌افزارهای راهبردی و خدمات به‌روزرسانی امنیتی، وابستگی نسبی به خارج دارد. تحریم‌های آمریکا و اروپا، دسترسی ایران به بسیاری از سرویس‌ها و تجهیزات را محدود کرده‌اند و این مسئله هم هزینه‌ی توسعه‌ی زیرساخت را افزایش داده و هم باعث عقب‌ماندگی نسبی در برخی حوزه‌ها شده است..



## محیط اجتماعی-روایتی

### الف) سواد رسانه‌ای و ظرفیت تحلیل

محیط اجتماعی-روایتی تعیین می‌کند پیام‌ها چگونه دریافت، تفسیر و باز تولید می‌شوند. پژوهش‌های داخلی نشان می‌دهند سطح سواد رسانه‌ای در میان گروه‌های مختلف جامعه‌ی ایران به شدت نابرابر است؛ در مناطق شهری بزرگ و میان نسل جوان تحصیل کرده، توانایی تشخیص خبر جعلی، تحلیل منبع و فهم عملیات روانی بالاتر است، اما در مناطق محروم، روستاها و میان گروه‌هایی با دسترسی محدود به آموزش، این توانایی ضعیف‌تر است (Rahimi, 2023). این نابرابری باعث می‌شود برخی گروه‌ها بیشتر در معرض تأثیر روایت‌های تحریک‌آمیز، اخبار جعلی و پروپاگاندای خارجی قرار گیرند. در شرایط بحران، این گروه‌ها ممکن است ناخواسته به باز تولیدکنندگان روایت‌های طراحی شده‌ی دشمنان تبدیل شوند، در حالی که خود تصور می‌کنند تنها خبر را منتقل می‌کنند (Ahmadi, 2023).

### ب) تنوع هویتی، قومیت‌ها و شکاف‌های اجتماعی

ایران جامعه‌ای چندقومیتی و چندفرهنگی است. قومیت‌ها، زبان‌ها، خرده‌فرهنگ‌ها و گرایش‌های مذهبی متنوعی در کشور حضور دارند که هر یک روایت‌های تاریخی و هویتی خاص خود را دارند (Kamangir, 2021). در شرایط عادی، این تنوع می‌تواند به غنای فرهنگی منجر شود، اما در دوران بحران، اگر مدیریت نشود، ممکن است به واگرایی و شکل‌گیری روایت‌های رقیب نسبت به روایت ملی بیانجامد (Rahimi, 2023). در سال‌های اخیر، برخی رسانه‌های خارجی و شبکه‌های اجتماعی بر برجسته‌سازی شکاف‌های قومی، مذهبی و جنسیتی در ایران تمرکز کرده‌اند تا انسجام ملی را هدف بگیرند (Klein, 2022). در مقابل، تلاش شده است با تأکید بر روایت ملت واحد با تنوع فرهنگی و ارائه‌ی تصویر مثبتی از همزیستی اقوام در رسانه‌های رسمی، این شکاف‌ها را مدیریت کند. می‌توان گفت محیط‌شناسی جنگ روایت‌ها در ژئوپلیتیک‌فضای مجازی ایران نشان می‌دهد که ایران در قلب یک میدان چندلایه قرار دارد. از بیرون، قدرت‌های جهانی و منطقه‌ای تلاش می‌کنند با استفاده از پلتفرم‌های فراملی و فناوری‌های دیجیتال، روایت‌های خود را بر افکار عمومی ایرانیان تحمیل کنند (Cohen & Avivi, 2021). از درون، حاکمیت در پی دفاع از امنیت ملی و انسجام اجتماعی است، اما با چالش‌های جدی ناشی از شکاف اعتماد، ضعف سواد رسانه‌ای در برخی سطوح و محدودیت‌های فناوری‌های فناورانه روبه‌رو است (Rahimi, 2023). چنانچه این



محیط‌ها به صورت راهبردی و آینده‌پژوهانه تحلیل و مدیریت نشوند، تداوم وضعیت کنونی می‌تواند ایران را به سمت امنیتی‌سازی شدیدتر فضای مجازی، کاهش ظرفیت‌های توسعه‌ی ارتباطی و فرسایش تدریجی سرمایه‌ی اجتماعی حاکمیت سوق دهد (Castells, 2024). در عین حال، اگر سیاست‌گذار ایرانی بتواند با بهره‌گیری از ابزارهای تحلیلی مانند MICMAC و سناریونویسی، روابط میان این محیط‌ها را بهتر بشناسد و سیاست‌های روایی هوشمندانه‌تری طراحی کند، می‌تواند تهدیدهای موجود را به فرصت‌هایی برای تقویت اقتدار ملی و روایت‌های درونی تبدیل کند (Jalili & Riazi, 2022).

## یافته‌ها و تجزیه و تحلیل داده‌ها

### الف: یافته‌های تحقیق

#### متغیرهای تأثیرگذار بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی ایران

برای انجام این پژوهش نخست از طریق مطالعات کتابخانه‌ای و تحلیل محتوای مصاحبه با خبرگان حوزه رسانه و امنیت، ۳۴ متغیر تأثیرگذار بر ژئوپلیتیک روایت‌ها در فضای مجازی ایران مطابق جدول ۲ شناسایی شد.



جدول ۲. متغیرهای تأثیرگذار بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی ایران

ردیف	مؤلفه اصلی	متغیر	کد
۱	ژئوپلیتیک خارجی	میزان مداخله بازیگران فراملی در فضای مجازی ایران	X۱
۲		شدت رقابت روایتی منطقه‌ای علیه ایران	X۲
۳		نقش رسانه‌های فارسی‌زبان برون‌مرزی در شکل‌دهی افکار عمومی	X۳
۴		استفاده سیاسی از شبکه‌های اجتماعی جهانی علیه ایران	X۴
۵		پیوند جنگ روایت‌ها با فشارهای سیاسی و تحریمی	X۵
۶		هم‌افزایی روایت‌های امنیتی دشمنان منطقه‌ای ایران	X۶
۷		نقش دیاسپورای ایرانی در بازتولید روایت‌های معارض	X۷
۸		تأثیر بحران‌های ژئوپلیتیکی منطقه‌ای بر فضای روایتی ایران	X۸
۹	حکمرانی فضای مجازی	میزان انسجام نهادی در سیاست‌گذاری فضای مجازی	X۹
۱۰		میزان کارآمدی شورای عالی فضای مجازی در مدیریت جنگ روایت‌ها	X۱۰
۱۱		سطح اجرای شبکه ملی اطلاعات	X۱۱
۱۲		کیفیت قوانین و مقررات ناظر بر فضای مجازی	X۱۲
۱۳		ظرفیت حکمرانی داده در کشور	X۱۳
۱۴		میزان هماهنگی میان نهادهای فرهنگی، امنیتی و رسانه‌ای	X۱۴
۱۵		سرعت واکنش حکمرانی به بحران‌های روایتی	X۱۵
۱۶		رویکرد سیاستی حاکم در مواجهه با شبکه‌های اجتماعی	X۱۶



X17	شدت عملیات روانی و اطلاعاتی علیه ایران	امنیت سایبری و جنگ نرم	۱۷
X18	میزان نفوذپذیری فضای مجازی کشور		۱۸
X19	توان دفاع سایبری کشور در برابر حملات اطلاعاتی		۱۹
X20	نقش بات‌ها و شبکه‌های سازمان‌یافته در جنگ روایت‌ها		۲۰
X21	سطح امنیت پلتفرم‌های بومی		۲۱
X22	پیوند تهدیدات سایبری با ناآرامی‌های اجتماعی		۲۲
X23	توانایی شناسایی و خنثی‌سازی روایت‌های مخرب		۲۳
X24	میزان آمادگی امنیتی نهادها در جنگ شناختی		۲۴
X25	سطح اعتماد عمومی به روایت‌های رسمی		۲۵
X26	نابرابری سواد رسانه‌ای در جامعه		۲۶
X27	تنوع هویتی و قومی و تأثیر آن بر پذیرش روایت‌ها	اجتماعی، رسانه‌ای و آینده‌پژوهی	۲۷
X28	نقش اینفلوئنسرها در جهت‌دهی روایت‌ها		۲۸
X29	شدت شکاف نسلی در مصرف رسانه‌ای		۲۹
X30	میزان اثرگذاری رسانه‌های داخلی		۳۰
X31	آمادگی جامعه برای مواجهه با جنگ شناختی		۳۱
X32	ظرفیت یادگیری نهادی از بحران‌های روایتی گذشته		۳۲
X33	میزان آینده‌نگری راهبردی در سیاست‌گذاری فضای مجازی		۳۳
X34	توان مدیریت سناریوهای آینده جنگ روایت‌ها		۳۴

### شناسایی متغیرهای کلیدی تأثیرگذار بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی سازی ایران

برای انتخاب ارزش هر یک از متغیرها بر پایه پنل خبرگی، پرسشنامه ماتریس تحلیل اثرات تنظیم و در اختیار خبرگان قرار گرفت. خبرگان به تأثیر عوامل بر یکدیگر بین ۰ تا ۳ نمره‌گذاری



کردند. نتایج پرسشنامه به نرم افزار MicMac فراخوانده شد. خروجی این نرم افزار متغیرهای کلیدی را مشخص کرد که ورودی نرم افزار Scenario wizard خواهند بود.

## وضعیت ماتریس اثرات متقابل (MD۱)

جدول ۳. تحلیل اولیه داده‌های ماتریس اثرات متقابل

شاخص	ابعاد ماتریس	تعداد تکرار	صفر	یک	دو	سه	P	جمع	درصد پرشدگی
مقدار	۳۴×۳۴	۲	۳۴۰	۴۰۱	۲۳۸	۱۶۸	۹	۸۱۶	۷۰,۵۵۸

منبع: پژوهش محققان

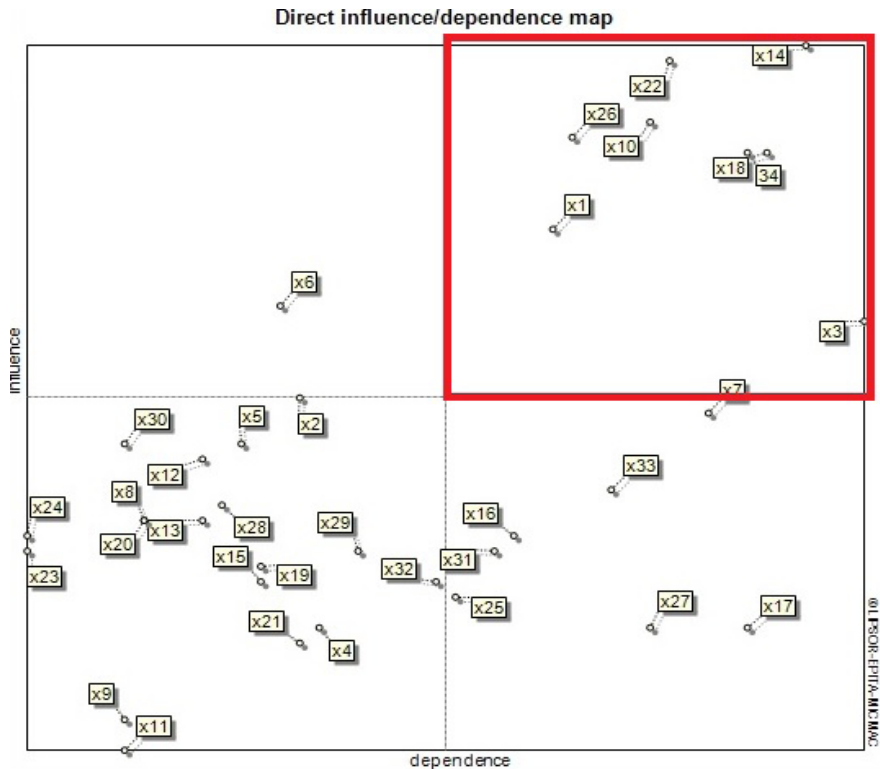
بر پایه جدول شماره ۳، ابعاد ماتریس ۳۴×۳۴ و درجه پرشدگی ماتریس ۷۰,۵۵۸ درصد است که نشان می‌دهد عوامل انتخاب شده تأثیر نسبتاً زیاد و پراکنده‌ای بر همدیگر داشته و در واقع سیستم از وضعیت ناپایداری برخوردار است. از مجموع ۸۱۶ رابطه قابل ارزیابی در این ماتریس، ۳۴۰ رابطه با ارزش عددی صفر است که بیان می‌کند متغیرها بر همدیگر تأثیر نداشته یا از همدیگر تأثیر نپذیرفته‌اند. ۴۰۱ رابطه تأثیر کم متغیرها بر همدیگر را نشان می‌دهد. ۲۳۸ رابطه نمایانگر تأثیرگذاری نسبتاً قوی متغیرها بر یکدیگر است. ۱۶۸ رابطه عددشان سه است؛ بدین معنی که روابط متغیرهای کلیدی، بسیار زیاد و از تأثیرگذاری و تأثیرپذیری بالایی برخوردار است. در نهایت نیز ۹ رابطه نشان‌دهنده رابطه پتانسیلی و غیرمستقیم متغیرها بر یکدیگرند.

### تحلیل سیستم و تعیین تأثیرگذاری تأثیرپذیری متقابل متغیرها بر یکدیگر

متغیرهای کلیدی، متغیرهایی به‌شمار می‌روند که قابل دست‌کاری و کنترل هستند و به‌طور قابل توجهی بر پویایی سیستم تأثیر می‌گذارند. متغیرهای ناحیه شمال غرب تأثیرگذار هستند اما به‌ندرت کنترل‌پذیر به‌شمار می‌روند، در حالی که متغیرهای ناحیه جنوب غربی کمترین تأثیر را دارند و کلیدی نیستند. متغیرهای ناحیه جنوب شرقی به دیگر متغیرها وابسته هستند و تحت تأثیر قرار می‌گیرند. در برابر، متغیرهای ناحیه شمال شرقی راهبردی و کلیدی هستند و



قابلیت مدیریت و تأثیرگذاری دارند و قابلیت بیشتری برای تبدیل شدن به کلیدی بودن دارند که به در کادر قرمز فرار گرفته اند.



شکل ۱. نمودار پراکنده‌گی متغیرهای مستقیم و جایگاه آن در محور تأثیرگذاری - تأثیرپذیری

بر پایه مطالب پیش گفته و شکل ۱، هشت متغیر میزان مداخله بازیگران فراملی در فضای مجازی ایران (X۱)، نقش رسانه‌های فارسی‌زبان برون مرزی در شکل‌دهی افکار عمومی (X۳)، میزان کارآمدی شورای عالی فضای مجازی در مدیریت جنگ روایت‌ها (X۱۰)، میزان هماهنگی میان نهادهای فرهنگی، امنیتی و رسانه‌ای (X۱۴)، میزان نفوذپذیری فضای مجازی کشور (X۱۸)، پیوند تهدیدات سایبری با ناآرامی‌های اجتماعی (X۲۲)، نابرابری سواد رسانه‌ای در جامعه (X۲۶) و توان مدیریت سناریوهای آینده جنگ روایت‌ها (X۳۴) به عنوان متغیرهای کلیدی بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی سازی ایران شناسایی شدند.



## تبیین محتمل‌ترین سناریوی فراروی جنگ روایت‌ها در ژئوپلیتیک‌فضای مجازی و امنیتی‌سازی ایران

### حالت‌های احتمالی متغیرهای کلیدی

حالت‌های مختلفی پیشروی هشت متغیر کلیدی قابل تصور است که در شناخت جنگ روایت‌ها در ژئوپلیتیک‌فضای مجازی و سناریوهای فراروی امنیتی‌سازی ایران اهمیت به سزایی دارد. مطابق وضعیت‌های احتمالی جنگ روایت‌ها در ژئوپلیتیک‌فضای مجازی و سناریوهای فراروی امنیتی‌سازی ایران در مجموع ۲۹ حالت برای هشت متغیر کلیدی طراحی شده که در جدول ۴ آمده است.

جدول ۴. شرح حالت‌های احتمالی ممکن برای متغیرهای کلیدی تأثیرگذار بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی‌سازی ایران

کد	متغیر کلیدی	حالت	شرح حالت‌های احتمالی	وضعیت
A	میزان مداخله بازیگران فراملی در فضای مجازی ایران	A۱	مداخله خارجی به دلیل بازدارندگی داخلی کاهش می‌یابد	مطلوب
		A۲	مداخله خارجی کنترل شده باقی می‌ماند	ایستا
		A۳	مداخله خارجی به شدت افزایش یافته است	بحرانی
B	نقش رسانه‌های فارسی‌زبان برون مرزی در شکل‌دهی افکار عمومی	B۱	نقش رسانه‌های خارجی تضعیف شده است	مطلوب
		B۲	رسانه‌های برون مرزی نقش محدود ایفا می‌کنند	ایستا
		B۳	رسانه‌های برون مرزی روایت‌های بحران‌زا تولید می‌کنند	بحرانی
C	میزان کارآمدی شورای عالی فضای مجازی در مدیریت جنگ روایت‌ها	C۱	شورا سیاست‌های آینده‌نگر و هوشمند تدوین می‌کند	مطلوب
		C۲	شورا سیاست‌های ثابت و تکراری اجرا می‌کند	ایستا
		C۳	شورا دچار ناکارآمدی و افت عملکرد شده است	بحرانی



مطلوب	نهادهای هماهنگی حداکثری و هم‌افزایی رسیده‌اند	D <sub>1</sub>	میزان هماهنگی میان نهادهای فرهنگی، امنیتی و رسانه‌ای	D
ایستا	نهادهای همکاری معمول اما بدون ابتکار دارند	D <sub>2</sub>		
بحرانی	نهادهای دچار اختلاف و ناهماهنگی عمیق شده‌اند	D <sub>3</sub>		
مطلوب	نفوذپذیری با پدافند غیرعامل روایی مهار می‌شود	E <sub>1</sub>	میزان نفوذپذیری فضای مجازی کشور	E
ایستا	نفوذ فضای مجازی در سطح ثابت حفظ می‌شود	E <sub>2</sub>		
بحرانی	نفوذ فضای مجازی بی‌رویه و کنترل‌ناپذیر شده است	E <sub>3</sub>		
مطلوب	پیوند میان تهدید سایبری و ناآرامی‌ها به‌طور کامل گسسته شده است	F <sub>1</sub>	پیوند تهدیدات سایبری با ناآرامی‌های اجتماعی	F
ایستا	تهدیدات سایبری ارتباط منظم اما کم‌رنگ با ناآرامی‌ها دارند	F <sub>2</sub>		
بحرانی	تهدیدات سایبری بحران‌های اجتماعی را تحریک می‌کنند	F <sub>3</sub>		
ایستا	شکاف سواد رسانه‌ای تغییری نمی‌کند	G <sub>1</sub>	نابرابری سواد رسانه‌ای در جامعه	
مطلوب	نابرابری سواد رسانه‌ای بسیار شدید شده است	G <sub>2</sub>		
ایستا	مدیریت آینده بدون نوآوری و صرفاً حفظ وضع موجود انجام می‌شود	Y <sub>1</sub>	توان مدیریت سناریوهای آینده جنگ روایت‌ها	Y
		Y <sub>2</sub>		
بحرانی	مدیریت آینده به‌شدت ضعیف و منفعل می‌شود			

منبع: پژوهش محققان

## شناسایی الگوهای پیش روی بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و

### سناریوهای فراروی امنیتی‌سازی ایران

این مرحله از پژوهش شامل تهیه فهرستی از حالت‌های ممکن برای هفت متغیر کلیدی و طراحی پرسشنامه در قالب ماتریس متقاطع برای تهیه داده‌های مورد نیاز است. با استفاده از نرم‌افزار Scenario Wizard، بیش از سه‌هزار مدل یکپارچه از ۲۲ موقعیت بالقوه مرتبط با بر جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی‌سازی ایران پیش‌بینی شد. تجزیه و تحلیل نتایج؛ شش الگو با سازگاری قوی، ۲۵۱ الگو با سازگاری ضعیف و ۵۱ الگوی ناسازگار را نشان داد. شکل ۳ تابلوی سناریوهای قوی را نشان می‌دهد. در این تابلو رنگ سبز برای وضعیت مطلوب، رنگ زرد برای وضعیت ایستا و رنگ قرمز برای شرایط بحرانی است که ۱۳ موقعیت را با شش الگو سناریوی قوی نشان می‌دهد.

Scenario No. 1	Scenario No. 2	Scenario No. 3	Scenario No. 4	Scenario No. 5	Scenario No. 6
مطلوب پیوند میان تهدید سایبری و ناآرامی‌ها به‌طور کامل گسسته شده است		ایستا مدیریت آینده بدون نوآوری و صرفاً حفظ وضع موجود انجام می‌شود		مطلوب شورا سیاست‌های آینده‌نگر و هوشمند تدوین می‌کنند	مطلوب توان مدیریت سناریوها با دقت بالا پیش‌بینی می‌شود
	ایستا تهدیدات سایبری ارتباط منظم اما کج‌رنگ با ناآرامی‌ها دارند	ایستا نهادهای همکاری معمول اما بدون ابتکار دارند	بحرانی رسانه‌های بیرون‌مرزی روایت‌های بحرانی‌زا تولید می‌کنند	ایستا شورا سیاست‌های ثابت و تکراری اجرا می‌کنند	ایستا مدیریت آینده بدون نوآوری و صرفاً حفظ وضع موجود انجام می‌شود
مطلوب توان مدیریت سناریوها با دقت بالا پیش‌بینی می‌شود	بحرانی رسانه‌های بیرون‌مرزی روایت‌های بحرانی‌زا تولید می‌کنند		بحرانی شورا دچار ناکارآمدی و افست عملکرد شده است		بحرانی نهادهای دچار اختلاف و ناهماهنگی عمیق شده‌اند

شکل ۲. تابلوی سناریوهای با سازگاری قوی و محتمل



همان گونه که در شکل ۲ (سناریوی قوی و محتمل) مشاهده می‌شود تعداد وضعیت‌های ایستا بر دیگر وضعیت‌های ممکن برتری دارد. از این وضعیت‌های احتمالی ۳۸,۸۸ درصد ایستا، ۳۳,۳۳ درصد بحرانی، ۲۷,۷۹ درصد مطلوب قرار داشته‌اند. بنابراین سناریوی وضعیت ایستا محتمل‌ترین سناریوی جنگ روایت‌ها در ژئوپلیتیک فضای مجازی ایران می‌باشد.

### ب: تجزیه و تحلیل یافته‌ها

#### الگو جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی سازی ایران سناریوی اول و محتمل تعادل روایی شکننده در فضای مجازی<sup>۱</sup>

سناریوی قوی در تابلو سناریونویس با احتمال وقوع ۳۸/۸۸ درصد به عنوان محتمل‌ترین مسیر آینده ترسیم می‌شود. در این وضعیت، مداخله بازیگران فراملی در سطحی میانی و کنترل شده باقی می‌ماند و رسانه‌های برون مرزی نیز به طور مستمر اما غیر غالب در فرآیند شکل دهی به افکار عمومی نقش ایفا می‌کنند. این فشار خارجی پایدار اما محدود، کارآمدی شورای عالی فضای مجازی را به سطحی واکنشی تقلیل می‌دهد و سیاست‌گذاری‌ها بیشتر معطوف به مهار پیامدها می‌شود تا خلق ابتکارهای پیش‌دستانه دنبال گردد. هم‌زمان، هماهنگی نهادی میان نهادهای فرهنگی، امنیتی و رسانه‌ای در حد حداقلی حفظ می‌شود و امکان هم‌افزایی ساختاری شکل نمی‌گیرد. در نتیجه این وضعیت نهادی، نفوذپذیری فضای مجازی در سطحی حساس اما تثبیت شده باقی می‌ماند و امکان بهره‌برداری مستمر کنشگران رقیب فراهم می‌شود. پیوند تهدیدات سایبری با ناآرامی‌های اجتماعی به شکل مقطعی و موجی فعال می‌ماند و هر مسئله اجتماعی بالقوه قابلیت تبدیل شدن به بحران روایی کوتاه مدت را پیدا می‌کند. هم‌زمان، نابرابری سواد رسانه‌ای در جامعه بدون مداخله مؤثر سیاستی باز تولید می‌شود و بخش‌هایی از افکار عمومی در معرض روایت‌های تحریف شده قرار می‌گیرند. برآیند این زنجیره علی موجب می‌شود توان مدیریت سناریوهای آینده در سطح حفظ وضع موجود متوقف بماند و نظام حکمرانی روایی قادر به فاصله گرفتن از منطق واکنش نباشد. در نتیجه، تعادل موجود شکننده باقی می‌ماند و هر گونه تغییر در شدت مداخله خارجی یا بروز بحران داخلی می‌تواند سیستم را به سمت سناریوی بحرانی سوق دهد.



### سناریوی دوم فرسایش حکمرانی و انحراف روایی<sup>۱</sup>

احتمال وقوع این سناریو ۳۳/۳۳ درصد آینده‌ای پرریسک را ترسیم می‌کند. در این مسیر، شدت مداخله بازیگران فراملی افزایش می‌یابد و رسانه‌های برون‌مرزی به کنشگران اصلی در تعیین دستور کار ذهنی جامعه تبدیل می‌شوند. این غلبه روایی خارجی، کارآمدی شورای عالی فضای مجازی را به شدت تضعیف می‌کند و سیاست‌گذاری‌های آن با ناتوانی اجرایی و کاهش مشروعیت مواجه می‌شود. در ادامه، هماهنگی نهادی میان دستگاه‌های مسئول دچار اختلال می‌شود و شکاف‌های تصمیم‌گیری و اجرایی تشدید می‌گردد. ناهماهنگی نهادی شرایطی ایجاد می‌کند که نفوذپذیری فضای مجازی به سطح بحرانی برسد و حملات سایبری و عملیات روایت‌محور با هزینه کم و اثرگذاری بالا انجام شوند. در چنین بستری، پیوند تهدیدات سایبری با ناآرامی‌های اجتماعی به صورت فعال برقرار می‌شود و کنش‌های اطلاعاتی مستقیماً در خدمت تحریک و هدایت بی‌ثباتی قرار می‌گیرند. هم‌زمان، نابرابری سواد رسانه‌ای در جامعه تعمیق پیدا می‌کند و شکاف شناختی میان گروه‌های اجتماعی افزایش می‌یابد و ظرفیت تشخیص روایت‌های مخرب تضعیف می‌شود. مجموع این متغیرها موجب می‌شود توان مدیریت سناریوهای آینده به سطحی انفعالی و کوتاه‌مدت تنزل پیدا کند و تصمیم‌گیری‌ها عمدتاً با منطق امنیتی و هزینه‌زا انجام شوند. در نهایت، جنگ روایت‌ها به ابزار مؤثر فشار ژئوپلیتیکی علیه ثبات داخلی تبدیل می‌شود و مسیر انحراف استراتژیک در حکمرانی فضای مجازی تقویت می‌گردد.

### سناریوی سوم، سناریوی بازدارندگی هوشمند و ثبات شناختی<sup>۲</sup>

با احتمال وقوع سناریو ۲۷/۷۹ درصد مسیر مطلوب اما کم‌احتمال آینده محسوب می‌شود. در این سناریو، ارتقای توان مدیریت سناریوها نقطه آغاز تحول قرار می‌گیرد و این ارتقا به افزایش معنادار کارآمدی شورای عالی فضای مجازی در سیاست‌گذاری آینده‌نگر و داده‌محور منجر می‌شود. کارآمدی نهادی تقویت‌شده، هماهنگی نهادی پایدار میان نهادهای مسئول ایجاد می‌کند و کنش‌ها در چارچوب راهبردی منسجم و مشترک سامان می‌یابند. در نتیجه این انسجام داخلی، هزینه و اثربخشی مداخله بازیگران فراملی کاهش پیدا می‌کند و نقش رسانه‌های برون‌مرزی تضعیف می‌شود. کاهش فشار خارجی و انسجام نهادی باعث می‌شود نفوذپذیری فضای

1. Governance Erosion and Narrative Deviation
2. Smart Deterrence and Cognitive Stability



مجازی به صورت نظام‌مند کنترل شود و ظرفیت پدافند شناختی تقویت گردد. در این شرایط، پیوند تهدیدات سایبری با ناآرامی‌های اجتماعی به تدریج گسسته می‌شود و امکان بهره‌برداری از شکاف‌های اجتماعی کاهش می‌یابد. این وضعیت با ثبات فرصت می‌دهد تا سیاست‌های آموزشی و فرهنگی به کاهش تدریجی نابرابری سواد رسانه‌ای منجر شوند و سطح تاب‌آوری شناختی جامعه افزایش یابد. برآیند نهایی این فرآیندها موجب می‌شود توان مدیریت سناریوهای آینده به سطحی فعال و پیش‌دستانه برسد و نظام ژئوپلیتیک جنگ روایت‌ها وارد وضعیت ثبات و بازدارندگی نرم شود. در نتیجه، امنیت شناختی تقویت می‌شود و اثرگذاری فشارهای روایی خارجی به حداقل ممکن تقلیل پیدا می‌کند.

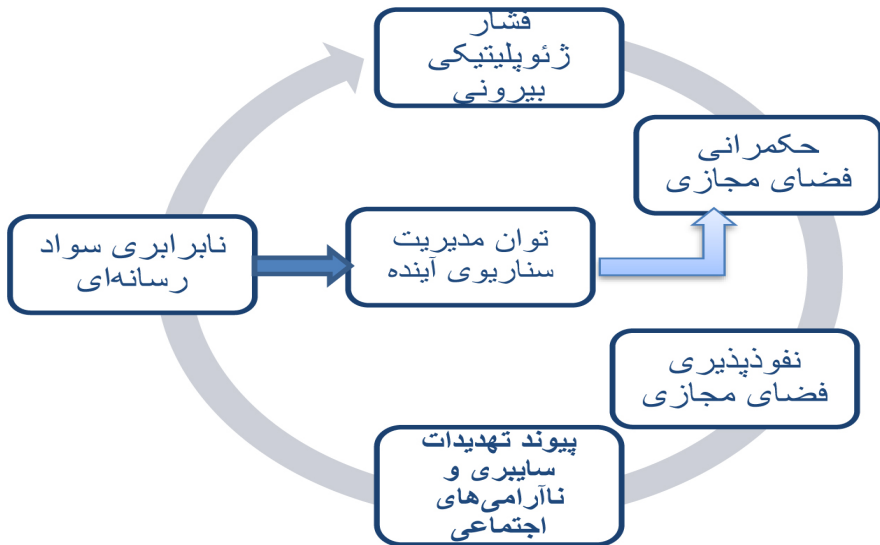
### نتیجه‌گیری و پیشنهاد

یافته‌های این مقاله نشان می‌دهد که جنگ روایت‌ها در فضای مجازی ایران نه یک پدیده مقطعی یا صرفاً رسانه‌ای، بلکه یک عرصه ژئوپلیتیکی چندلایه است که در آن قدرت، امنیت و معنا به صورت هم‌زمان تولید و بازتوزیع می‌شوند. تحلیل متغیرها و سناریوها آشکار می‌سازد که کنش بازیگران فراملی، عملکرد رسانه‌های برون‌مرزی و ساختار حکمرانی فضای مجازی در داخل کشور در یک رابطه علی-تعاملی دائمی قرار دارند و هیچ‌یک به تنهایی قادر به تبیین وضعیت امنیت شناختی کشور نیستند. از این منظر، امنیتی‌سازی فضای مجازی نه یک انتخاب اختیاری، بلکه پیامد ساختاری شرایط ژئوپلیتیکی جدید تلقی می‌شود که در آن روایت به ابزار اصلی اعمال قدرت تبدیل شده است. نتایج سناریونویسی نشان می‌دهد که سناریوی ایستا با عنوان تعادل روایی شکننده، محتمل‌ترین وضعیت آینده جنگ روایت‌ها در فضای مجازی ایران است و این امر بیانگر نوعی قفل‌شدگی ساختاری در نظام حکمرانی روایی است. در این وضعیت، اگرچه سیستم از فروپاشی کامل مصون می‌ماند، اما ناتوانی در گذار به وضعیت مطلوب، زمینه را برای لغزش تدریجی به سمت بحران فراهم می‌سازد. تثبیت نفوذپذیری فضای مجازی، تداوم نابرابری سواد رسانه‌ای و واکنشی ماندن نهادهای سیاست‌گذار از جمله نشانه‌هایی است که نشان می‌دهد حفظ وضع موجود خود به یک ریسک راهبردی تبدیل می‌شود و امنیت شناختی را در بلندمدت تضعیف می‌کند. سناریوی بحرانی که با فرسایش حکمرانی و انحراف روایی مشخص می‌شود، به‌مثابه هشدار تحلیلی مقاله قابل تفسیر است و نشان می‌دهد که تشدید مداخله بازیگران فراملی در غیاب هماهنگی نهادی می‌تواند جنگ روایت‌ها را به محرک مستقیم ناآرامی‌های اجتماعی تبدیل کند.



در این وضعیت، امنیتی‌سازی سخت و واکنشی نه‌تنها قادر به مهار بحران نخواهد بود، بلکه خود به بازتولید بی‌اعتمادی و شکاف شناختی منجر می‌شود.

مقاله نشان می‌دهد که پیوند خوردن تهدیدات سایبری با شکاف‌های اجتماعی در چنین شرایطی، نشانه عبور مسئله از سطح رسانه‌ای به سطح امنیت ملی است که هزینه‌های آن به‌صورت تصاعدی افزایش پیدا می‌کند. در مقابل، سناریوی مطلوب با عنوان بازدارندگی هوشمند و ثبات شناختی نشان می‌دهد که امکان مدیریت فعال جنگ روایت‌ها وجود دارد، اما تحقق آن مستلزم تغییر رویکرد در سطح حکمرانی است. تقویت توان مدیریت سناریوها، ارتقای کارآمدی شورای عالی فضای مجازی و نهادینه‌سازی هماهنگی نهادی از جمله پیش‌شرط‌هایی هستند که می‌توانند مداخله خارجی را پرهزینه و کم‌اثر کنند. این سناریو به‌روشنی نشان می‌دهد که امنیت پایدار در فضای مجازی نه از مسیر انسداد صرف، بلکه از مسیر افزایش تاب‌آوری شناختی و کاهش نابرابری سواد رسانه‌ای حاصل می‌شود. در جمع‌بندی نهایی، مقاله استدلال می‌کند که آینده جنگ روایت‌ها در ژئوپلیتیک فضای مجازی ایران بیش از آنکه به ابزارهای فنی وابسته باشد، به کیفیت حکمرانی و توان سیاست‌گذاری شناخت‌محور وابسته است. سناریوی ایستا اگرچه محتمل‌ترین مسیر است، اما مطلوب‌ترین مسیر نیست و تداوم آن می‌تواند کشور را به‌صورت تدریجی به سناریوی بحرانی سوق دهد. از این رو، گذار آگاهانه و مرحله‌ای به سمت سناریوی بازدارندگی هوشمند به‌عنوان راهبردی پیش‌دستانه، عقلانی‌ترین گزینه برای تأمین امنیت شناختی و کاهش آسیب‌پذیری ژئوپلیتیکی ایران در فضای مجازی تلقی می‌شود.



شکل ۳. مدل مفهومی جنگ روایت‌ها در ژئوپلیتیک فضای مجازی و سناریوهای فراروی امنیتی سازی ایران

مدل مفهومی این پژوهش بر این فرض بنیادین استوار می‌شود که فضای مجازی در ایران صرفاً یک بستر فنی یا ارتباطی تلقی نمی‌شود، بلکه به‌عنوان میدانی ژئوپلیتیکی و روایت‌محور عمل می‌کند که در آن، قدرت‌ها از طریق تولید، توزیع و تثبیت معنا به رقابت می‌پردازند. در این چارچوب، جنگ روایت‌ها به‌مثابه شکل متأخر جنگ ترکیبی فهم می‌شود که هدف اصلی آن نه تصرف سرزمین، بلکه تأثیرگذاری بر ادراک، اعتماد و مشروعیت در سطح جامعه است تعریف می‌شود. در سطح نخست مدل، محیط ژئوپلیتیکی بیرونی شامل بازیگران فراملی، رسانه‌های برون مرزی و پلتفرم‌های دیجیتال جهانی قرار می‌گیرد که با بهره‌گیری از ظرفیت‌های نرم‌افزاری، الگوریتمی و رسانه‌ای، روایت‌هایی خاص درباره ایران تولید و باز تولید می‌کنند. این روایت‌ها، به‌ویژه در شرایط تشدید فشارهای سیاسی، تحریمی و منطقه‌ای، به‌صورت هدفمند بر شکاف‌های اجتماعی، هویتی و حکمرانی تمرکز می‌کنند تا از طریق عملیات شناختی، زمینه بی‌ثبات‌سازی ادراکی را فراهم کنند دنبال می‌شود. در سطح دوم، حکمرانی فضای مجازی ایران به‌عنوان متغیر میانجی و تعیین‌کننده وارد مدل می‌شود که کیفیت آن می‌تواند شدت و جهت اثرگذاری



فشارهای بیرونی را تعدیل یا تشدید کند. انسجام نهادی، کارآمدی سیاست‌گذاری، شفافیت ارتباطی و توان اقناع افکار عمومی در این سطح، نقشی کلیدی در تبدیل تهدیدات روایی به بحران امنیتی یا مهار آن‌ها ایفا می‌کند انجام می‌دهد. در این چارچوب، امنیتی‌سازی فضای مجازی نه به‌عنوان کنشی صرفاً سرکوبگرانه، بلکه به‌عنوان پاسخی دفاعی در برابر تهدیدات سازمان‌یافته و ترکیبی معنا می‌یابد تبیین می‌شود. در سطح سوم مدل مفهومی، جامعه و افکار عمومی به‌عنوان میدان اثرپذیری اصلی جنگ روایت‌ها قرار می‌گیرد. سطح اعتماد عمومی، میزان سواد رسانه‌ای، و شدت نابرابری شناختی میان گروه‌های اجتماعی، تعیین می‌کند که روایت‌های رقیب تا چه اندازه قابلیت نفوذ، بازنشر و تبدیل شدن به کنش اجتماعی را دارند مشخص می‌سازد. هر چه این مؤلفه‌ها تضعیف شوند، پیوند میان عملیات سایبری، روایت‌سازی خارجی و ناآرامی‌های اجتماعی تقویت می‌شود تقویت می‌گردد. در مرکز این مدل، توان مدیریت سناریوهای آینده به‌عنوان متغیر کلیدی تنظیم‌گر قرار می‌گیرد که امکان گذار میان وضعیت‌های ایستا، بحرانی و مطلوب را فراهم می‌کند. این متغیر نشان می‌دهد که آینده امنیتی‌سازی فضای مجازی ایران نه به‌صورت خطی و جبری، بلکه به‌صورت سناریومحور و وابسته به کیفیت تصمیم‌گیری راهبردی شکل می‌گیرد رقم می‌خورد. بر این اساس، مدل مفهومی پژوهش پیوندی منسجم میان ژئوپلیتیک جنگ روایت‌ها، حکمرانی فضای مجازی و امنیت شناختی برقرار می‌کند و چارچوب تحلیلی لازم برای استخراج سناریوهای آینده‌پژوهانه را فراهم می‌سازد ارائه می‌دهد.

## فهرست منابع

۱. افراسیابی، ح.، و زارع، م (۱۳۹۹). شبکه‌های اجتماعی و امنیت ملی: مطالعه‌ای بر ناآرامی‌های شهری در ایران. فصلنامه مطالعات امنیت ملی، ۱۶(۳)، ۷۵-۱۰۹.
۲. حسینی، م.، و همکاران (۱۴۰۰). شبکه‌های اجتماعی، سرمایه اجتماعی و اعتماد سیاسی در ایران. فصلنامه مطالعات اجتماعی ایران، ۱۵(۲)، ۱۱۵-۱۴۶.
۳. فاضلی، ن. (۱۳۹۸). جامعه شبکه‌ای و تحولات فرهنگ سیاسی در ایران. نشر نی.
۴. موسوی، ع. (۱۴۰۱). امنیت سایبری و شبکه ملی اطلاعات در ایران: چالش‌ها و فرصت‌ها. فصلنامه سیاست‌گذاری فضای مجازی، ۳(۱)، ۹-۳۸.
5. Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner.
6. Castells, M. (2012). Networks of outrage and hope: Social movements in the Internet age. Polity Press.
7. Deibert, R. (2019). Reset: Reclaiming the Internet for civil society. House of Anansi.
8. Demchak, C. C., & Dombrowski, P. (2011). Cyber Westphalia: Asserting state sovereignty in cyberspace. *Georgetown Journal of International Affairs*, 12(2), 29-38.
9. Flint, C. (2017). Introduction to geopolitics (3rd ed.). Routledge.
10. Godet, M., & Durance, P. (2011). Strategic foresight: For corporate and regional development. UNESCO.
11. Hosseini, S., Ahmadi, M., & Rezaei, A. (2021). Media literacy and political trust in the age of social networks: Evidence from Iran. *Journal of Information Society Studies*, 7(2), 45-68.
12. Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365-404.
13. Luna-Reyes, L. F., & Gil-Garcia, J. R. (2021). Cognitive warfare and digital democracy. *Government Information Quarterly*, 38(4), 101-118.
14. RAND Corporation. (2020). Information operations and regime stability in the digital age. RAND.
15. Riordan, J. (2023). The geopolitics of narratives in the digital age. *International Affairs*, 99(4), 1053-1075.
16. Ahmadi, S. (2023). Social media and protest narratives in Iran. Tehran



- Social Research Center.
17. Al-Dosari, M. (2023). Digital geopolitics of Iran-Saudi information rivalry. Riyadh Policy Review.
  18. Castells, M. (2024). Power and communication networks in the digital age. Oxford University Press.
  19. Cohen, I., & Avivi, D. (2021). Cyber narratives and Middle East conflicts. Tel Aviv Security Institute.
  20. Center for Human Rights in Iran. (2025, July 29). *Iran: Proposed cyber bill gives authorities sweeping new powers to block and punish online content*. <https://iranhumanrights.org/2025/07/iran-proposed-cyber-bill-gives-authorities-sweeping-new-powers-to-block-and-punish-online-content/>
  21. Jalili, A., & Riazi, M. (2022). National Information Network: A path to cyber sovereignty. Iran ICT Journal.
  22. Kamangir, R. (2021). Ethnic identity and online narratives in Iran. Persian Media Studies.
  23. Klein, N. (2022). Disinformation wars and geopolitical influence. Harvard Digital Review.
  24. Rahimi, N. (2023). Media literacy and social cohesion in Iran. University of Isfahan Press.
  25. Riordan, S. (2023). Digital diplomacy and national security. Cambridge Political Studies.
  26. Deibert, R. J. (2021). Reset: Reclaiming the internet for civil society. House of Anansi Press.
  27. Ahmadi, S., Vahidi, F., & Rezaei, N. (2024). Operationalizing variables for strategic foresight in cyber conflicts. Journal of Futures Studies, 15(3), 112–135.
  28. Doen, T., & Durance, P. (2015). MICMAC methodology: A practical guide. Foresight Laboratory Publications.
  29. Godet, M., & Durance, P. (2011). Strategic foresight: For corporate and regional development. UNESCO.
  30. Von Reibnitz, H. (2019). Scenario Wizard software user manual and methodological guidelines. Institute for Futures Research.

