A Strategic Model for Cyberspace Governance in Iran: Emphasizing the Sustainability of National Security and International Relations

Mehdi Haji Ahmadi[۱]

Nazanin Malekian[*۲]

Extended Abstract

۱. Introduction

In the twenty-first century, cyberspace has emerged as one of the most critical arenas of national and international power. This domain simultaneously offers vast opportunities for economic, cultural, scientific, and diplomatic development while posing serious threats to national security, social cohesion, cultural identity, and political independence of nations. For the Islamic Republic of Iran, which operates in a complex geopolitical environment, faces extensive international sanctions, and is continually targeted by hybrid operations, cognitive warfare, organized cyberattacks, and foreign media-informational campaigns, strategic management of cyberspace is no longer merely a technical or cultural issue; rather, it constitutes a dual strategic imperative. First, ensuring the sustainability of national security against cyber threats, informational infiltration, and soft warfare; second, intelligently harnessing the potential of this space to enhance soft power, improve the country's global image, and advance diplomatic objectives through digital diplomacy. Despite numerous policy-making efforts in recent years, a persistent gap remains: the absence of an integrated strategic model capable of pursuing these two overarching goals in a synergistic manner. Many prior approaches have been either excessively security-oriented and restrictive or entirely open and inattentive to hybrid threats. The present study aims to address this theoretical and practical lacuna by developing an indigenous, multidimensional model for cyberspace governance in Iran that establishes a dynamic balance between security imperatives and opportunity creation.

۲. Theoretical Framework

The theoretical framework of this study conceptualizes cyberspace as a multidimensional arena for redefining power, identity, security, and international interactions. Accordingly, an integrated framework is developed based on three complementary theoretical pillars: Cyber Governance Theory, Securitization Theory, and Soft Power and Digital Diplomacy Theory. Cyber Governance Theory provides the structural and institutional perspective, emphasizing the need to strengthen domestic infrastructures, establish integrated governance structures, enhance media literacy and cognitive resilience, and participate strategically in global cyber governance (Alkan, 2012; Fischerkeller et al., 2022). Securitization Theory explains how cyberspace is constructed as a security issue through threat-oriented discourse and how excessive securitization may lead to restrictive policies, international isolation, and weakened soft power (Buzan, Wæver & de Wilde, 1998; Betz, 201۷; Lehto, 2022). Finally, Soft Power and Digital Diplomacy Theory highlights cyberspace as an arena for attraction, cultural influence, international image-building, diplomatic interaction, and trust-building (Nye, 2004; Bjola & Holmes, 2015; Maurer, 2020). Together, these dimensions provide the theoretical basis for simultaneously strengthening national security and sustainable international relations.

۳. Methodology

This applied research employed a mixed-methods sequential exploratory design (qualitative followed by quantitative). In the qualitative phase, data were collected through semi-structured interviews with 15 senior managers and policymakers from the fields of national security, information technology, media, and international relations. Additionally, Delphi sessions and focused group discussions (FGD) were conducted with 15 other experts and specialists. Qualitative data were analyzed using thematic content analysis and systematic coding (open, axial, and selective). In the quantitative phase, the classic SWOT framework was utilized to identify and categorize internal factors (strengths and weaknesses) and external factors (opportunities and threats). Subsequently, the strategies derived from the qualitative phase were prioritized using the

---

This article is derived from a doctoral dissertation entitled “A Strategic Model for Cyberspace Governance in Iran with Emphasis on the Sustainability of National Security and International Relations,” being conducted by Mehdi Haji Ahmadi under the supervision of Dr. Nazanin Malekian in the Department of Communication Sciences, Islamic Azad University, Central Tehran Branch

۱ Ph.D. Candidate in Communication Sciences, Department of Communication Sciences, Faculty of Communication and Media, Islamic Azad University, Central Tehran Branch, Tehran, Iran.
Email: mahdi.hajiahmadi1282@iau.ir

۲ Associate Professor of Communication Sciences, Department of Communication Sciences, Faculty of Communication and Media, Islamic Azad University, Central Tehran Branch, Tehran, Iran. (Corresponding Author)
Email: n.malekiyan@iauctb.ac.ir

Quantitative Strategic Planning Matrix (QSPM) based on attractiveness scores. Instrument validity was confirmed through expert content evaluation, and reliability was established via Cronbach's alpha (≥ 0.7).

٤. Results & Discussion

Internal environmental analysis revealed that Iran's cyberspace governance possesses notable strengths: highly skilled and experienced human resources in cybersecurity, relatively resilient security infrastructure, active monitoring systems, secure data centers, and proven success in managing and containing domestic cyber crises. Nevertheless, deep structural weaknesses limit the full exploitation of these strengths: a historically negative and predominantly threat-centric perception of cyberspace, the absence of a unified management structure and weak inter-institutional coordination, legal gaps and fragmented policymaking, heavy dependence on foreign technology and software, and—most critically—significant deficiencies in public digital and media literacy as well as a shortage of attractive, competitive, nationally identity-based content.

Externally, substantial opportunities were identified: prospects for expanding international and regional cooperation in cybersecurity, rapid growth of the digital economy and online services, advancement of e-government, high domestic innovation capacity and knowledge-based enterprises, and the potential to leverage emerging technologies (particularly artificial intelligence) in cybersecurity. In contrast, external threats were assessed as highly serious: organized cyberattacks by state and non-state actors, digital espionage and sabotage operations, extensive information warfare, infiltration and incitement via social networks, and the spillover of geopolitical and political tensions into the cyber domain. The results of the Internal Factors Evaluation (IFE = 3.91) and External Factors Evaluation (EFE = 3.55) matrices indicate that the overall factor scores exceed the average (2.5), signifying that strengths and opportunities collectively outweigh weaknesses and threats, thereby creating favorable conditions for adopting development-oriented and offensive strategies rather than purely defensive ones.

٥. Conclusions & Suggestions

Based on the prioritization conducted via the QSPM matrix, the strategies with the highest attractiveness scores were determined as follows:

١. Maximizing the utilization of existing specialized human capital for dual purposes: widespread education in digital literacy and cybersecurity across societal levels and managerial cadres, and fostering educational, research, and experiential exchange collaborations with aligned countries and international organizations.

٢. Transforming successful experiences in managing domestic cyber crises into a driving force for indigenous technology development and gradual reduction of dependence on foreign suppliers.

٣. Systematically enhancing awareness, security skills, and digital literacy among users, organizations, and policymakers.

٤. Strengthening predictive, preventive, and rapid-response capabilities against external cyberattacks by leveraging existing specialized expertise.

٥. Improving macro-level crisis management to mitigate the adverse impacts of political and geopolitical tensions on cybersecurity and national social stability.

The proposed model rests on three synergistic pillars:

١. Technical pillar: secure infrastructure, indigenous technology, advanced warning and monitoring systems;

٢. Cognitive pillar: high media and digital literacy, societal cognitive resilience against soft warfare and misinformation;

٣. Cultural-diplomatic pillar: production of attractive and credible content rooted in national-Islamic identity, proactive digital diplomacy, and intelligent participation in global internet governance discourses.

Keywords: national security, cyberspace, international relations, strategic planning, cyberspace governance.

الگوی راهبردی مدیریت فضای مجازی با تأکید بر پایداری امنیت ملی و روابط بین‌المللی

مهدی حاجی احمدی[۱]

نازنین ملکیان*[۲]

تاریخ دریافت: ۱۴۰۴/۱۱/۲۱

تاریخ پذیرش: ۱۴۰۵/۰۵/۲۱

چکیده

پژوهش حاضر با هدف تدوین الگوی راهبردی مدیریت فضای مجازی در ایران با تأکید بر پایداری امنیت ملی و روابط بین‌الملل انجام شد. با وجود پژوهش‌های پراکنده، تاکنون الگویی یکپارچه که تعامل هم‌افزای این دو حوزه را تبیین کند، ارائه نشده است. این پژوهش با روش ترکیبی (اکتشافی متوالی) انجام شد. در بخش کیفی، داده‌ها از طریق مصاحبه با ۲۳ مدیر و سیاست‌گذار و جلسات FGD با ۱۵ خبره جمع‌آوری و با تحلیل محتوای موضوعی پردازش شد و ٦٠ کد کلیدی در قالب نقاط قوت (٦)، ضعف (۱۱)، فرصت (۷) و تهدید (۹) دسته‌بندی گردید. در بخش کمی، از ماتریس‌های IFE، EFE و QSPM برای اولویت‌بندی راهبردها استفاده شد. یافته‌ها نشان داد که نمره عوامل داخلی (۱/۹٦) و خارجی (۱/۷۲) پایین‌تر از میانگین است و موقعیت ایران را در منطقه تدافعی (WT) نشان می‌دهد که بیانگر چربش ضعف‌های ساختاری (نبود رگولاتور مستقل، فقدان قانون جامع، رویکرد واکنشی و بی‌اعتمادی) بر پتانسیل‌های فنی است. بر اساس اولویت‌بندی QSPM، راهبردهای تدافعی WT2 با نمره ٤/۲۵ و WT1 با نمره ٤/۱۷ در صدر قرار دارند که نشان‌دهنده ضرورت تمرکز بر اصلاحات درون‌سیستمی (جرم‌زدایی، بازسازی سرمایه اجتماعی، تدوین قانون جامع و شفاف‌سازی رگولاتوری) پیش از هرگونه اقدام توسعه‌ای است. الگوی نهایی، مبتنی بر پنج بُعد کلیدی (امنیتی- پدافندی، نهادی- حقوقی، اجتماعی- فرهنگی، بین‌المللی- دیپلماتیک و فنی- زیرساختی) طراحی شده و نوآوری آن در ارائه الگویی بومی با قابلیت پیاده‌سازی در شرایط خاص ایران، اولویت‌بندی کمی راهبردها و شناسایی سه الگوی روابط متقابل (تقابلی، هم‌افزا و شرطی) میان امنیت ملی و روابط بین‌الملل است. مدیریت راهبردی فضای مجازی در ایران در گرو عبور از پارادایم صرفاً امنیتی- محدودکننده به‌سوی حکمرانی هوشمند، مشارکتی و مبتنی بر اعتماد است که با اصلاحات ساختاری، بازسازی سرمایه اجتماعی و دیپلماسی فعال، به پایداری امنیت ملی، بهبود تصویر بین‌المللی و ارتقای جایگاه ایران در نظام حکمرانی جهانی اینترنت می‌انجامد.

واژگان کلیدی: امنیت ملی، فضای مجازی، روابط بین‌الملل، مدیریت فضای مجازی، الگوی راهبردی.

این مقاله مستخرج از رساله دکتری با موضوع الگوی راهبردی مدیریت فضای مجازی در ایران با تأکید بر پایداری امنیت ملی و روابط بین‌المللی می‌باشد، که در گروه علوم ارتباطات دانشگاه آزاد واحد تهران مرکز به راهنمایی دکتر نازنین ملکیان و توسط مهدی حاجی احمدی در حال انجام است.

۱. دانشجوی دکتری، گروه علوم ارتباطات، دانشکده ارتباطات و رسانه، دانشگاه آزاد، واحد تهران مرکزی، تهران، ایران.

Email: mahdi.hajiahmadi1282@iau.ir

۲. دانشیار، گروه علوم ارتباطات، دانشکده ارتباطات و رسانه، دانشگاه آزاد، واحد تهران مرکزی، تهران، ایران. (نویسنده مسئول)

Email: n.malekiyan@iauctb.ac.ir

مقدمه

فضای مجازی در عصر حاضر، دیگر یک «ابزار» ارتباطی یا بستری برای سرگرمی نیست؛ بلکه به عرصه‌ای برای تعریف مجدد قدرت، هویت و حاکمیت در سطح ملی و بین‌المللی تبدیل شده است. این فضا با ویژگی‌های ذاتی خود یعنی فرامرزی بودن، غیرمتمرکز بودن، سرعت انتشار و هزینه پایین ورود، معادلات سنتی قدرت را برهم زده و هم‌زمان فرصت‌های بی‌سابقه‌ای برای دیپلماسی عمومی، اقتصاد دیجیتال و بازنمایی ملی و نیز تهدیدات نوظهوری برای امنیت شناختی، فرهنگی و زیرساختی کشورها پدید آورده است؛ به‌گونه‌ای که امنیت ملی در عصر دیجیتال فراتر از مرزهای فیزیکی رفته و به‌شدت تحت تأثیر پویایی‌ها، بازیگران و ساختارهای فضای مجازی قرار دارد (Kello & Arquilla, 2023). با این حال، چالش‌هایی نظیر حملات سایبری، انتشار اطلاعات نادرست، تأثیرگذاری سیاسی- فرهنگی، اختلال در زیرساخت‌های حیاتی و عملیات ضداستراتژیک، تهدیدی جدی برای امنیت ملی به‌شمار می‌روند (Alguliyev et al., 2021; Dobrovolska & Rozhkova, 2024). در چنین شرایطی، کشوری مانند ایران که در تقاطع تنش‌های ژئوپلیتیکی، تحریم‌های چندلایه، جنبش‌های اجتماعی پویا و هویتی چندلایه (اسلامی- ایرانی) قرار دارد، با پرسش راهبردی مواجه است که پاسخ به آن، کیفیت آینده ملی و جایگاه بین‌المللی آن را رقم خواهد زد: چگونه می‌توان مدیریت فضای مجازی را چنان سامان داد که هم‌زمان از کیان امنیت ملی در برابر تهدیدات سایبری و شناختی صیانت کند و از ظرفیت‌های آن برای تقویت اعتبار بین‌المللی و تعاملات دیپلماتیک بهره گیرد؟

این پرسش از آن‌رو اهمیت راهبردی می‌یابد که پاسخ‌های موجود در ایران، یا یک‌سویه و مبتنی بر نگاه «امنیتی- محدودکننده» هستند که ضمن ایجاد هزینه‌های سنگین برای قدرت نرم و تعاملات بین‌المللی، نتوانسته‌اند تهدیدهای شناختی و ترکیبی را مهار کنند، یا در سوی دیگر، رویکردهای «آزادمنش» بدون توجه به بافت خاص سیاسی، فرهنگی و تحریمی کشور، به آسیب‌پذیری‌های جدی در حوزه‌های اطلاعاتی و اعتماد عمومی دامن زده‌اند. تجربه تاریخی مدیریت فضای مجازی در ایران، به‌ویژه پس از رویدادهای سیاسی- اجتماعی دهه اخیر، نشان داده است که سیاست‌های صرفاً واکنشی و بخشی، نه تنها پاسخگوی چالش‌های پیچیده و چندلایه نیستند، بلکه خود به عاملی برای تشدید بحران‌های هویتی، شکاف نسلی و بی‌اعتمادی نهادی بدل شده‌اند (پاسبان، ۱۴۰۲؛ ندری و همکاران، ۱۳۹۷). تجربه کشورهای توسعه‌یافته نیز نشان می‌دهد که راهبردهای مؤثر امنیت سایبری بر سه پایه اصلی استوار است: ادغام فناوری‌های پیشرفته، بهبود مستمر چارچوب‌های قانونی و توسعه توانمندی‌های انسانی (Abrahams et al., 2024; Safitra et al., 2023). از این‌رو، ضرورت گذار از رویکردهای جزیره‌ای و مقطعی به سمت یک الگوی راهبردی یکپارچه، پویا و بومی که بتواند تعامل میان امنیت ملی و روابط بین‌الملل را در بستر فضای مجازی تبیین و هدایت کند، به یک نیاز اساسی و فوری تبدیل شده است. این ضرورت زمانی برجسته‌تر می‌شود که بدانیم خسارات جهانی ناشی از تهدیدات سایبری در سال ۲۰۲۳ از تولید ناخالص داخلی بسیاری از اقتصادهای بزرگ فراتر رفت و پیش‌بینی می‌شود تا چند سال آینده حدود ۲۰۰ زتابایت داده دیجیتال ذخیره شود که خود انگیزه‌ای قوی برای تهاجمات سایبری خواهد بود (Morgan, 2024). همچنین ناامنی سایبری می‌تواند منجر به افشای اطلاعات محرمانه، اختلال در زیرساخت‌های حیاتی، بی‌ثباتی اجتماعی، تروریسم سایبری، جاسوسی و جرایم سازمان‌یافته شود (Betz, 2017; Lehto, 2022). بنابراین، تأمین فضای سایبری پایدار، اولویت راهبردی دولت‌ها و نیازمند همکاری مستمر بین‌المللی، بهبود نظارت و تحلیل تهدیدها و افزایش آگاهی عمومی است (Dobrovolska & Rozhkova, 2024).

با وجود این ضرورت آشکار، مرور انتقادی ادبیات پژوهش نشان می‌دهد که تحقیقات موجود در ایران، با وجود کمیت قابل‌توجه، دچار سه نقص اساسی هستند که مانع از تدوین چنین الگویی شده است: نخست، بخش عمده پژوهش‌های داخلی (مانند پالیزداران، ۱۳۹۴؛ قدسی، ۱۳۹۲؛ رستگارخالد و محمدیان، ۱۳۹۲) عمدتاً به شناسایی تهدیدات و آسیب‌شناسی فضای مجازی پرداخته‌اند، اما این تحلیل‌ها غالباً تک‌بُعدی و فاقد نگاه سیستمی به تعامل امنیت و دیپلماسی هستند. به‌عبارت دیگر،

فضای مجازی در این پژوهش‌ها صرفاً به‌عنوان «تهدید» یا «فرصت» تلقی شده، نه به‌عنوان عرصه‌ای برای مدیریت راهبردی توأمان این دو حوزه. دوم، پژوهش‌هایی که به‌طور مشخص به مدیریت فضای مجازی پرداخته‌اند (مانند روحانی و همکاران، ۱٤۰۲؛ مهربانی‌فر، ۱٤۰۳) اغلب در سطح کلیات سیاستی باقی مانده و از ارائه الگویی عملیاتی، با شاخص‌های مشخص و قابلیت اجرایی، ناتوان بوده‌اند. این مطالعات، هرچند بر ضرورت مدیریت منسجم تأکید دارند، اما نه ساختار آن را ترسیم کرده‌اند و نه مسیر پیاده‌سازی آن را در شرایط خاص ایران نشان داده‌اند. سوم، پژوهش‌های محدودی که به رابطه فضای مجازی و روابط بین‌الملل پرداخته‌اند (حاجی‌احمدی و ملکیان، ۱٤۰۳)، عمدتاً بر نقش رسانه‌های جمعی در دیپلماسی متمرکز شده‌اند و از ابعاد فنی، امنیتی و شناختی مدیریت فضای مجازی غافل مانده‌اند. در سطح بین‌المللی نیز، با وجود غنای نسبی نظریه‌ها (مانند نظریه ثبات سایبری فیشرکلر و همکاران، ۲۰۲۲؛ نظریه جنگ اطلاعاتی بیل و همکاران، ۲۰۲٤؛ نظریه دیپلماسی دیجیتال بیولا و هولمز، ۲۰۱۵)، این پژوهش‌ها عمدتاً در بستر جوامع باز، با دسترسی آزاد به فناوری و بدون محدودیت‌های تحریمی شکل گرفته‌اند و لذا امکان کاربست مستقیم آن‌ها در فضای خاص ایران، با چالش‌های جدی روبه‌روست. بررسی‌ها حاکی از آن است که کمتر از ۳۰ درصد کشورها در حال حاضر از استراتژی‌های کارآمد مدیریت فضای مجازی در روابط بین‌المللی برخوردارند (UNODC, 2023) که این خود نشان‌دهنده خلاء جهانی در این حوزه است. این شکاف، یعنی نبود الگویی که همزمان بر چهار محور «فنی»، «امنیتی»، «فرهنگی- شناختی» و «دیپلماتیک» استوار باشد و در بستر تحریمی و خاص ایران قابل پیاده‌سازی گردد، به‌عنوان خلاء نظری و عملی اصلی این پژوهش شناسایی می‌شود.

بنابراین، هدف اصلی این پژوهش، پر کردن این خلاء از طریق ارائه الگویی راهبردی است که مبتنی بر واقعیت‌های داخلی و با بهره‌گیری هوشمندانه از تجارب موفق بین‌المللی طراحی شده است. این الگو در پی آن است که نشان دهد «پایداری امنیت ملی» و «پایداری روابط بین‌الملل» در فضای مجازی نه تنها اهداف متضادی نیستند، بلکه با مدیریت صحیح می‌توانند به‌عنوان دو نیروی هم‌افزا، یکدیگر را تقویت کنند. به‌عبارت دقیق‌تر، امنیت ملی در عصر دیجیتال بدون «قدرت جذب» و «اعتبار بین‌المللی» ناپایدار است و روابط بین‌الملل نیز بدون «پشتیبانی امنیتی» و «تاب‌آوری شناختی» در برابر تهدیدات، به انفعال و وابستگی خواهد انجامید. این نگاه دوگانه- هم‌افزا، هسته مفهومی الگوی مورد نظر این پژوهش را تشکیل می‌دهد.

۱- پیشینه پژوهش

مرور نظام‌مند پژوهش‌های پیشین، هسته اصلی شناسایی خلاء نظری و عملی هر مطالعه است. با این هدف، در این بخش پژوهش‌های داخلی و خارجی مرتبط با مدیریت فضای مجازی، امنیت ملی و روابط بین‌الملل به‌صورت تطبیقی بررسی می‌شوند تا ضمن شناسایی دستاوردها و کاستی‌های هر یک، جایگاه و نوآوری پژوهش حاضر مشخص گردد.

۱-۱- پژوهش‌های داخلی

پژوهش‌های داخلی در حوزه فضای مجازی و امنیت ملی را می‌توان در سه دسته کلی جای داد. دسته نخست، پژوهش‌هایی هستند که عمدتاً به شناسایی تهدیدات و آسیب‌پذیری‌های فضای مجازی برای امنیت ملی پرداخته‌اند. پالیزداران (۱۳۹٤) نشان داد که اینترنت در کنار فرصت‌های گسترده، می‌تواند تهدیداتی جدی برای امنیت ملی ایجاد کند و این امر مستلزم سیاست‌گذاری دقیق و هوشمندانه است. قدسی (۱۳۹۲) نیز نتیجه گرفت که فضای مجازی از یک‌سو ساختارهای امنیتی و فرهنگی را در معرض خطر قرار می‌دهد و از سوی دیگر ابزار مؤثری برای معرفی ظرفیت‌های ملی محسوب می‌شود. رستگارخالد و محمدیان (۱۳۹۲) دریافتند که استفاده زیاد از فضای مجازی با کاهش احساس امنیت اجتماعی رابطه دارد. ندری و همکاران (۱۳۹۷) نیز بیان کردند که شبکه‌های اجتماعی همانند شمشیری دولبه می‌توانند هم فرصت‌ساز و هم تهدیدزا باشند و ضعف در سیاست‌گذاری و رهاشدگی فضای مجازی، زمینه‌ساز تخریب انسجام ملی و مشروعیت‌زدایی از نظام سیاسی می‌شود.

دسته دوم، پژوهش‌هایی هستند که بر ابعاد نهادی، قانونی و حکمرانی فضای مجازی متمرکز بوده‌اند. پاسبان (۱۴۰۲) نشان داد که نبود قوانین بازدارنده و سیاست‌گذاری جزیره‌ای می‌تواند تهدیدی جدی برای امنیت ملی باشد و موجب آسیب‌پذیری در حوزه‌های اطلاعاتی و سیاسی گردد. روحانی و همکاران (۱۴۰۲) فضای مجازی را عاملی تأثیرگذار بر ابعاد مختلف حکمرانی ملی شامل سیاست، اقتصاد، فرهنگ و امنیت دانسته و بر ضرورت مدیریت منسجم آن برای تقویت حکمرانی ملی تأکید کرده‌اند. مهربانی‌فر (۱۴۰۳) نتیجه گرفت که در سیاست‌گذاری‌های رسانه‌ای کشور، جایگاه رسانه‌های محلی و نحوه ارتقای مشارکت مردمی در فضای مجازی به‌درستی تعریف نشده است.

دسته سوم، پژوهش‌هایی هستند که به نقش فضای مجازی در دیپلماسی و روابط بین‌الملل پرداخته‌اند. حاجی‌احمدی و ملکیان (۱۴۰۳) در دو پژوهش جداگانه نشان دادند که هماهنگی رسانه ملی با سیاست خارجی می‌تواند نقش مؤثری در تقویت حکمرانی و نظم اجتماعی داشته باشد و همچنین استفاده از شبکه‌های اجتماعی تأثیر معناداری بر احساس امنیت اجتماعی دارد.

با وجود تنوع موضوعی، پژوهش‌های داخلی عمدتاً دچار سه خلاء اساسی هستند: (۱) رویکرد تک‌بعدی و تهدیدمحور که فضای مجازی را صرفاً به‌عنوان منشأ تهدید تلقی می‌کند و از ظرفیت‌های دیپلماتیک و قدرت نرم آن غافل است؛ (۲) فقدان الگوی عملیاتی و یکپارچه که بتواند هم‌زمان امنیت ملی و روابط بین‌الملل را پوشش دهد؛ (۳) غفلت از بافت خاص ایران (تحریم‌ها، ساختار نهادی و الزامات فرهنگی) در ارائه راهکارها.

۱-۲- پژوهش‌های خارجی

پژوهش‌های خارجی در حوزه فضای مجازی و امنیت بین‌الملل از غنای نظری بیشتری برخوردارند، اما اغلب در بستر جوامع باز و بدون محدودیت‌های تحریمی شکل گرفته‌اند. فیشرکلر و همکاران (Fischerkeller et al., 2022) با ارائه نظریه «ثبات سایبری»، تأکید کردند که کشورها باید از رویکردهای سنتی امنیتی فاصله گرفته و با همکاری بین‌المللی، چارچوبی برای پایداری امنیت در فضای سایبری ایجاد کنند. جانسون و وایت (Johnson & White, 2024) نشان دادند که شبکه‌های اجتماعی می‌توانند با انتشار اطلاعات نادرست و تحریک تنش‌های سیاسی، امنیت جهانی را تهدید کنند؛ و از این‌رو، تنظیم‌گری و نظارت دقیق بر فعالیت این شبکه‌ها ضروری است. نس و خینواسارا (Ness & Khinvasara, 2024) در پژوهشی درباره تهدیدهای نوظهور سایبری اعلام کردند که وابستگی جوامع مدرن به فناوری اطلاعات، آسیب‌پذیری امنیتی و اقتصادی را افزایش داده و لزوم توسعه راهبردهای دفاع سایبری را برجسته ساخته است. مایورر (Maurer, 2020) با بررسی رابطه فضای مجازی و روابط بین‌الملل نشان داد که نوع نگرش دولت‌ها به فضای سایبری بر رفتار و سیاست خارجی آن‌ها در عرصه جهانی تأثیر مستقیم دارد. بیولا و هولمز (Bjola & Holmes, 2015) نیز دیپلماسی دیجیتال را به‌عنوان ابزاری مکمل برای تقویت قدرت نرم و پاسخ فعال به تهدیدات فضای مجازی معرفی کرده‌اند.

مهم‌ترین کاستی پژوهش‌های خارجی، (۱) نادیده گرفتن موانع ساختاری و تحریمی کشورهایی مانند ایران، (۲) غلبه رویکردهای غرب‌محور و بی‌توجهی به بافت‌های فرهنگی- سیاسی خاص، و (۳) فقدان الگویی که بتواند هم‌زمان به الزامات امنیتی و دیپلماتیک کشورهای غیرغربی پاسخ دهد، است.

۱-۳- جمع‌بندی تطبیقی و تبیین نوآوری پژوهش

با مقایسه تطبیقی پژوهش‌های داخلی و خارجی، شکاف اساسی در ادبیات پژوهش به‌وضوح قابل شناسایی است: از یک‌سو، پژوهش‌های داخلی عمدتاً سلبی، تهدیدمحور و فاقد نگاه سیستمی به تعامل امنیت و روابط بین‌الملل هستند و الگویی عملیاتی و بومی برای مدیریت هم‌افزای این دو حوزه ارائه نداده‌اند. از سوی دیگر، پژوهش‌های خارجی با وجود غنای نظری، در فضایی کاملاً متفاوت (بدون تحریم، با دسترسی آزاد به فناوری) شکل گرفته و برای کاربست در شرایط خاص ایران (با محدودیت‌های فناورانه، تحریم‌های بین‌المللی، ساختار نهادی خاص و الزامات فرهنگی- مذهبی) نیازمند

بومی‌سازی اساسی هستند. همچنین، هیچ یک از پژوهش‌های مرور شده، الگویی سه‌بُعدی (شامل ابعاد فنی، شناختی و فرهنگی) ارائه نداده‌اند که بتواند به‌طور هم‌زمان به پایداری امنیت ملی و تقویت روابط بین‌الملل بینجامد.

نوآوری پژوهش حاضر در این است که با تلفیق رویکردهای نظری (حکمرانی سایبری، امنیتی‌سازی و قدرت نرم) و بهره‌گیری از روش ترکیبی (SWOT و QSPM)، الگویی راهبردی و بومی برای مدیریت فضای مجازی ایران ارائه می‌دهد که ضمن توجه به محدودیت‌های تحریمی و ساختاری، بر هم‌افزایی امنیت ملی و روابط بین‌الملل تأکید دارد و شاخص‌های عملیاتی برای پیاده‌سازی آن در شرایط خاص کشور فراهم می‌آورد.

۲- مروری بر مبانی نظری

۲-۱- پیشینه نظری

چارچوب نظری این پژوهش بر این پیش‌فرض بنیادین استوار است که فضای مجازی را نه یک پدیده صرفاً فنی، بلکه باید به‌مثابه عرصه‌ای چندبُعدی برای بازتعریف قدرت، هویت، امنیت و تعاملات بین‌المللی در نظر گرفت. از این‌رو، برای دستیابی به الگویی راهبردی که بتواند هم‌زمان به پایداری امنیت ملی و روابط بین‌الملل بینجامد، چارچوبی ترکیبی از سه رکن نظری اصلی طراحی شده است که هر یک، بخشی از مسئله پژوهش را تبیین می‌کنند و در نهایت، در قالب مدل عملیاتی پژوهش، همگرا می‌شوند. این سه رکن عبارتند از: (۱) نظریه حکمرانی سایبری، (۲) نظریه امنیتی‌سازی (با تأکید بر رویکرد کپنهاگ)، و (۳) نظریه قدرت نرم و دیپلماسی دیجیتال.

۲-۱-۱- نظریه حکمرانی سایبری؛ چارچوبی برای تحلیل ساختار حاکمیت در فضای مجازی

حکمرانی سایبری به مجموعه‌ای از مکانیسم‌ها، نهادها، قوانین و رویه‌هایی اشاره دارد که از طریق آن‌ها، بازیگران مختلف (دولت‌ها، بخش خصوصی، جامعه مدنی و نهادهای بین‌المللی) مدیریت امور مربوط به فضای مجازی را سامان می‌دهند (Alkan, 2012). این نظریه به‌ویژه برای تبیین چالش‌های حاکمیت ملی در فضای مجازی کارآمد است، زیرا فضای مجازی به‌دلیل ویژگی‌های ذاتی خود (غیرمکانی، فرامرزی، غیرمتمرکز و پویا) مفهوم سنتی حاکمیت ملی را به چالش کشیده و مفهوم «حاکمیت سایبری» را مطرح کرده است. این حاکمیت دیگر صرفاً کنترل فنی زیرساخت‌ها نیست، بلکه شامل توانایی دولت در تعیین قواعد داخلی، حفاظت از امنیت شهروندان، مدیریت جریان اطلاعات و حفظ هویت فرهنگی در برابر نفوذ خارجی است. با این حال، در محیطی فرامرزی که هیچ دولتی به‌تنهایی آن را کنترل نمی‌کند، این توانایی با موانع جدی روبه‌روست که از سه منبع اصلی نشأت می‌گیرند: (۱) تسلط شرکت‌های چندملیتی خصوصی بر زیرساخت‌ها و ایجاد شکاف حاکمیتی (صلاحیت حقوقی بدون قدرت اجرایی)، (۲) نقش تعیین‌کننده بازیگران غیردولتی در تولید محتوا و شکل‌دهی هنجارهای جهانی، و (۳) فقدان چارچوب حقوقی بین‌المللی الزام‌آور و اختلاف عمیق میان رویکرد چندذینفعی غربی و تأکید بر حاکمیت ملی کشورهای غیرغربی (Fischerkeller et al., 2022).

نظریه حکمرانی سایبری در این پژوهش به‌عنوان چارچوبی برای تحلیل نقاط ضعف ساختاری مدیریت فضای مجازی ایران به‌کار گرفته شده است. به‌عبارت دیگر، این نظریه نشان می‌دهد که موفقیت مدیریت فضای مجازی در ایران، منوط به گذار از «حاکمیت مطلق بر قلمرو» به «حاکمیت توانمند بر تأثیرگذاری» است؛ یعنی تقویت زیرساخت‌های داخلی، ارتقای سواد رسانه‌ای و تاب‌آوری شناختی جامعه، و مشارکت هوشمند در گفتمان‌های جهانی برای شکل‌دهی هنجارها بر اساس ارزش‌های اسلامی- ایرانی.

۲-۱-۲- نظریه امنیتی‌سازی (مکتب کپنهاگ)؛ تبیین چگونگی تبدیل فضای مجازی به مسئله امنیتی

نظریه امنیتی‌سازی که توسط مکتب کپنهاگ (به‌ویژه باری بوزان و اولی ویور) صورت‌بندی شده است، بر این ایده استوار است که «امنیت» یک مفهوم عینی و از پیش تعیین‌شده نیست، بلکه برساختی گفتمانی است که در آن، یک کنشگر (معمولاً

دولت) با ارائه یک «گفتمان تهدید» (securitizing move)، مسئله‌ای را از حوزه سیاست‌های عادی به حوزه اضطراری و فراتر از رویه‌های معمول منتقل می‌کند و بدین ترتیب، برای مقابله با آن، اختیارات فراخوانی می‌کند (Buzan, Wæver & de Wilde, 1998). در مورد فضای مجازی، این نظریه به‌خوبی تبیین می‌کند که چگونه تهدیدات سایبری (همانند حملات سایبری خارجی، نفوذ بازیگران خارجی، خرابکاری و جاسوسی دیجیتال) به‌عنوان تهدیدات هستی‌بخش برای امنیت ملی برساخته می‌شوند و دولت‌ها را به اتخاذ سیاست‌های اضطراری و بعضاً محدودکننده سوق می‌دهند (Betz, 2017; Lehto, ۲۰۲۲). با این حال، امنیتی‌سازی بیش‌ازحد فضای مجازی نیز می‌تواند پیامدهای معکوس داشته باشد و به محدودیت‌های غیرضروری، انزوای بین‌المللی و تضعیف قدرت نرم بینجامد (Dobrovolska & Rozhkova, 2024).

در این پژوهش، نظریه امنیتی‌سازی برای تحلیل ریشه‌های نگاه منفی اولیه به فضای مجازی و سیاست‌های محدودکننده (همانند فیلترینگ و برخوردهای صرفاً امنیتی) به‌کار گرفته شده است. از سوی دیگر، این نظریه به پژوهش کمک می‌کند تا راهبردهای متوازنی پیشنهاد دهد که از امنیتی‌سازی افراطی پرهیز کرده و در عین حال، تهدیدات واقعی را جدی بگیرد. برای نمونه، راهبردهایی مانند «ارتقای آموزش و آگاهی امنیتی کاربران» و «استفاده از تجربه مدیریت بحران برای توسعه فناوری بومی» در چارچوب این نظریه، به‌عنوان راهکارهایی برای کاهش اضطراری‌سازی و جایگزینی آن با مدیریت راهبردی تلقی می‌شوند.

۲-۱-۳- نظریه قدرت نرم و دیپلماسی دیجیتال؛ چارچوبی برای تحلیل روابط بین‌الملل در فضای مجازی

نظریه قدرت نرم که توسط جوزف نای (Nye, 2004) صورت‌بندی شده است، بر توانایی یک بازیگر برای شکل‌دهی به ترجیحات دیگران از طریق جذابیت و اقناع، نه اجبار و زور، تأکید دارد. نای معتقد است که در عصر اطلاعات، افکار عمومی (چه در سطح ملی و چه بین‌المللی) به منبعی کلیدی برای قدرت تبدیل شده و دولت‌ها دیگر نمی‌توانند آن را نادیده بگیرند (Huntington, 1993). در این میان، دیپلماسی دیجیتال (Bjola & Holmes, 2015) به‌عنوان بسط عملیاتی قدرت نرم در فضای مجازی، به کارگیری فناوری‌های نوین و شبکه‌های اجتماعی برای پیشبرد اهداف سیاست خارجی، ارتباط با مخاطبان جهانی، مدیریت تصویر بین‌المللی و پاسخ به تهدیدات سایبری از طریق ابزارهای دیپلماتیک تعریف می‌شود (Maurer, 2020). این نظریه نشان می‌دهد که فضای مجازی نه تنها عرصه‌ای برای تهدید، بلکه بستری بی‌نظیر برای بازسازی روایت ملی، گسترش نفوذ فرهنگی و ساخت اعتماد بین‌المللی است. از این منظر، مدیریت موفق فضای مجازی می‌تواند به تقویت قدرت نرم، بهبود تصویر بین‌المللی و کاهش تنش‌های دیپلماتیک کمک کند (Johnson & White, 2024; Ness & Khinvasara, 2024).

نظریه قدرت نرم و دیپلماسی دیجیتال در این پژوهش، چارچوبی برای تحلیل فرصت‌های بین‌المللی (همکاری‌های بین‌المللی، مشارکت در پروژه‌های مشترک، بهره‌گیری از تجربیات موفق کشورها) و طراحی راهبردهای مرتبط با ارتقای تصویر بین‌المللی و تعاملات دیپلماتیک فراهم می‌کند. این نظریه به پژوهش کمک می‌کند تا از نگاه صرفاً دفاعی و محدودکننده به فضای مجازی فاصله گرفته و بر ظرفیت‌های آن برای دیپلماسی فرهنگی، قدرت نرم و تعاملات سازنده بین‌المللی تأکید کند، به‌گونه‌ای که فضای مجازی نه تنها به ابزاری برای دفاع فرهنگی، بلکه به کانالی مؤثر برای تقویت روابط بین‌المللی پایدار و مبتنی بر احترام متقابل تبدیل شود.

۲-۱-٤- جمع‌بندی نظری و کاربست عملیاتی

تلفیق سه نظریه مذکور، هسته نظری الگوی راهبردی این پژوهش را شکل می‌دهد. این تلفیق بر این پیش‌فرض استوار است که پایداری امنیت ملی و پایداری روابط بین‌الملل در فضای مجازی نه دو هدف متضاد، بلکه دو روی یک سکه هستند و مدیریت راهبردی فضای مجازی باید هم‌زمان هر دو را محقق کند. نظریه حکمرانی سایبری، چارچوب ساختاری و نهادی را فراهم می‌کند و نشان می‌دهد که چگونه ضعف‌های ساختاری (مانند نبود رگولاتور یکپارچه، تصمیم‌گیری پراکنده و خلاءهای قانونی) مانع از مدیریت کارآمد می‌شوند. نظریه امنیتی‌سازی، فرآیند تبدیل فضای مجازی به مسئله امنیتی و

پیامدهای آن (نگاه منفی، سیاست‌های محدودکننده و واکنش‌های اضطراری) را تبیین می‌کند و هشدار می‌دهد که امنیتی‌سازی افراطی می‌تواند به انزوای بین‌المللی و تضعیف قدرت نرم بینجامد. نظریه قدرت نرم و دیپلماسی دیجیتال نیز نشان می‌دهد که چگونه فضای مجازی می‌تواند به عرصه‌ای برای جذابیت، تعاملات دیپلماتیک و ساخت اعتماد بین‌المللی تبدیل شود و از این طریق، به پایداری روابط بین‌الملل کمک کند.

از منظر عملیاتی، این سه نظریه در قالب یک الگوی سه‌بُعدی در این پژوهش عملیاتی می‌شوند: بعد فنی- ساختاری (برگرفته از نظریه حکمرانی سایبری) که بر تقویت زیرساخت‌های امن، توسعه فناوری بومی و ایجاد ساختار یکپارچه حاکمیتی تأکید دارد؛ بُعد شناختی- امنیتی (برگرفته از نظریه امنیتی‌سازی) که بر ارتقای سواد رسانه‌ای، مدیریت بحران، تاب‌آوری شناختی و کاهش نگاه تهدیدمحور متمرکز است؛ و بُعد فرهنگی- دیپلماتیک (برگرفته از نظریه قدرت نرم و دیپلماسی دیجیتال) که بر تولید محتوای بومی جذاب، دیپلماسی دیجیتال، بهبود تصویر بین‌المللی و تعاملات سازنده با جامعه جهانی تأکید دارد. این سه بُعد در تعامل با یکدیگر، الگویی را شکل می‌دهند که در آن، امنیت ملی و روابط بین‌الملل نه تنها در تعارض نیستند، بلکه به‌عنوان دو نیروی هم‌افزا، یکدیگر را تقویت می‌کنند. به‌عبارت دیگر، امنیت ملی بدون قدرت جذب و اعتبار بین‌المللی ناپایدار است و روابط بین‌الملل نیز بدون پشتیبانی امنیتی و تاب‌آوری شناختی در برابر تهدیدات، به انفعال و وابستگی خواهد انجامید. این نگاه دوگانه- هم‌افزا، هسته مفهومی الگوی مورد نظر این پژوهش را تشکیل می‌دهد و در بخش یافته‌ها و مدل نهایی، به‌صورت شماتیک ترسیم خواهد شد.

۳- روش پژوهش

پژوهش حاضر از نظر هدف، کاربردی و از نظر روش، ترکیبی (کیفی- کمی) با رویکرد متوالی اکتشافی (ابتدا کیفی، سپس کمی) است. این انتخاب روش‌شناختی به‌دلیل ماهیت مسئله پژوهش است که هم نیازمند کشف عمیق ابعاد پنهان مدیریت فضای مجازی از دیدگاه خبرگان (بخش کیفی) و هم نیازمند اولویت‌بندی و کمّی‌سازی راهبردها (بخش کمی) است.

در بخش کیفی، از دو روش موازی برای جمع‌آوری داده‌ها استفاده شده است: (۱) مصاحبه‌های نیمه‌ساختاریافته عمیق با ۱۵ مدیر و سیاست‌گذار، و (۲) جلسات بحث گروهی متمرکز (FGD) با ۱۵ خبره و صاحب‌نظر. جامعه پژوهش در بخش کیفی شامل کلیه مدیران، سیاست‌گذاران و خبرگان فعال در حوزه‌های فناوری اطلاعات، رسانه، امنیت ملی و روابط بین‌الملل بود. نمونه‌گیری به‌صورت هدفمند (قضاوتی) و با استفاده از روش گلوله‌برفی انجام شد. حجم نمونه (۱۵) نفر برای مصاحبه و ۱۵ نفر برای (FGD) بر اساس اصل اشباع نظری تعیین گردید؛ به‌گونه‌ای که پس از انجام مصاحبه‌های چهاردهم و پانزدهم، داده‌های جدیدی به کدهای استخراجی اضافه نشد و اشباع نظری حاصل گردید. ملاک‌های ورود به پژوهش عبارت بودند از: (۱) داشتن حداقل ۵ سال سابقه کار مرتبط در یکی از حوزه‌های چهارگانه (فناوری اطلاعات، رسانه، امنیت ملی، روابط بین‌الملل)؛ (۲) داشتن سابقه تصدی پست‌های مدیریتی یا سیاست‌گذاری در سطح ملی؛ (۳) انتشار حداقل ۵ مقاله یا تألیف کتاب در حوزه مرتبط با فضای مجازی؛ و (٤) عضویت در هیئت علمی دانشگاه‌های معتبر کشور و ملاک خروج نیز، انصراف از مشارکت در هر مرحله از پژوهش بود. از ۱۵ مصاحبه‌شونده، ٤ نفر متخصص فناوری اطلاعات و امنیت سایبری، ۳ نفر متخصص رسانه و ارتباطات، ٤ نفر متخصص امنیت ملی و ٤ نفر متخصص روابط بین‌الملل بودند. همچنین در جلسات FGD، ۱۵ خبره با ترکیبی مشابه طی دو جلسه مشارکت داشتند. در بخش مصاحبه‌ها، از راهنمای مصاحبه نیمه‌ساختاریافته با سؤالات باز استفاده شد. در جلسات FGD نیز از پروتکل بحث گروهی با محورهای از پیش تعیین‌شده مبتنی بر یافته‌های اولیه مصاحبه‌ها بهره گرفته شد. مدت زمان هر مصاحبه بین ٤۵ تا ۹۰ دقیقه و هر جلسه FGD حدود ۱۲۰ دقیقه بود. برای تأمین روایی، از روش‌های بررسی روایی محتوایی توسط متخصصین و بررسی همکاران (ارزیابی کدها توسط دو پژوهشگر مستقل) استفاده شد. برای تأمین پایایی، از روش توافق بین کدگذاران (هولستی) استفاده گردید که ضریب توافق ۰/۸۲

به‌دست آمد که نشان‌دهنده پایایی مطلوب است. همچنین پایایی پرسشنامه به‌وسیله محاسبه ضریب آلفای کرونباخ در سطح ۰/۷۱ تأیید شد. داده‌های حاصل از مصاحبه‌ها و جلسات FGD با استفاده از روش تحلیل محتوای موضوعی و کدگذاری سه‌مرحله‌ای (باز، محوری و انتخابی) پردازش شدند. فرآیند کدگذاری با نرم‌افزار MAXQDA انجام گرفت. در نهایت، ٦٠ کد استخراج گردید که در قالب نقاط قوت (٦ کد)، نقاط ضعف (۱۱ کد)، فرصت‌ها (۷ کد) و تهدیدها (۹ کد) طبقه‌بندی شدند و مبنای طراحی ماتریس SWOT قرار گرفتند. برای اطمینان از اجماع خبرگان، یافته‌های کدگذاری در جلسات FGD مورد بحث و تأیید نهایی قرار گرفت.

در بخش کمی، پس از تأیید کدهای استخراجی توسط خبرگان، از دو مدل تحلیلی استفاده شد:

۱. ماتریس ارزیابی عوامل داخلی (IFE) و خارجی (EFE): این ماتریس‌ها برای تعیین وزن نسبی و امتیاز نهایی هر یک از عوامل داخلی و خارجی طراحی شدند. ضرایب اهمیت و امتیازات هر عامل بر اساس نظر خبرگان و با استفاده از مقیاس لیکرت ۵ درجه‌ای تعیین گردید.

۲. ماتریس برنامه‌ریزی استراتژیک کمی (QSPM): برای اولویت‌بندی راهبردهای استخراجی، از ماتریس QSPM استفاده شد. در این ماتریس، راهبردهای پیشنهادی بر اساس امتیاز جذابیت (AS) و مجموع نمره وزنی (TAS) اولویت‌بندی شدند و راهبردهای نهایی با بالاترین اولویت انتخاب گردیدند.

٤- یافته‌های پژوهش

همان‌طوری که اشاره شد در این پژوهش، داده‌های کیفی با استفاده از مصاحبه با ۱۵ نفر از مدیران و سیاست‌گذاران مرتبط با حوزه‌های فناوری اطلاعات، رسانه، امنیت ملی و روابط بین‌الملل و ۱۵ نفر از متخصصین موضوع در قالب بحث گروهی متمرکز جمع‌آوری شد. این مصاحبه‌ها به‌صورت نیمه‌ساختاریافته انجام شد تا دیدگاه‌ها، تجربیات عملی و نگرش‌های فردی شرکت‌کنندگان در زمینه مدیریت فضای مجازی شناسایی شود. داده‌های جمع‌آوری شده با استفاده از تحلیل محتوای موضوعی و کدگذاری سیستماتیک پردازش شدند. این فرایند شامل شناسایی مضامین اصلی، زیرمضامین و شاخص‌های مرتبط با مدیریت فضای مجازی بود. نمونه‌ای از کدگذاری یک مصاحبه ارائه شده است.

جدول ۱. نمونه‌ای از کدگذاری اولیه

کد	متن پاسخ مصاحبه‌شونده	نکات کلیدی/ کد
V1	نگاه اولیه به فضای مجازی در کشور منفی بود. بسیاری معتقد بودند اینترنت و شبکه‌های اجتماعی تهدیدی جدی برای امنیت ملی هستند و به جای بهره‌برداری، بیشتر به محدود کردن آن فکر می‌شد.	نگاه منفی اولیه به فضای مجازی
V2	هیچ ساختار و سازوکار مشخصی برای مدیریت فضای مجازی وجود نداشت. سیستم‌ها و سیاست‌ها دیر شکل گرفتند و فضای مجازی خود را به کشور تحمیل کرد.	نبود ساختار و سازوکار مشخص
V3	توسعه سریع اینترنت و شبکه‌های اجتماعی باعث شد سیاست‌گذاران نتوانند مدیریت مناسبی ارائه دهند و فضای مجازی بدون کنترل رشد کند.	عدم مدیریت صحیح بر فضای مجازی
V4	کاربران با سرعت بالایی به استفاده از شبکه‌های اجتماعی و خدمات آنلاین روی آوردند، بدون این‌که زیرساخت‌های امنیتی و قانونی آماده باشند.	رشد سریع فضای مجازی و نیاز به زیرساخت
V5	پس از چند سال غفلت، شورای عالی فضای مجازی و کمیسیون تنظیم مقررات ایجاد شد، اما این اقدامات دیرهنگام بودند.	مدیریت و تنظیم مقررات دیرهنگام
V6	تصمیم‌گیری در این حوزه پراکنده بود و نهادهای مختلف بدون هماهنگی روی محتوا و امنیت فضای مجازی کار می‌کردند.	تصمیم‌گیری پراکنده و چندنهادی
V7	تا زمانی که مدیریت یکپارچه ایجاد نشود، نمی‌توان فضای مجازی را سامان داد. نیاز به مشخص شدن نقش رگولاتور داریم.	نیاز به مدیریت یکپارچه و تعیین رگولاتور

V8	همکاری بین‌المللی و تبادل تجربه با دیگر کشورها هنوز محدود است؛ این فرصت می‌تواند تهدیدات سایبری خارجی را کاهش دهد.	کمبود همکاری بین‌المللی و فرصت بالقوه
V9	نبود قوانین جامع درباره حفاظت داده‌ها و امنیت سایبری باعث ایجاد خلاء قانونی و آسیب‌پذیری در مقابل حملات شده است.	ضعف در چارچوب قانونی و سیاست‌گذاری
V10	توسعه فناوری داخلی و سرمایه‌گذاری در نوآوری می‌تواند استقلال سایبری کشور را افزایش دهد و وابستگی به فناوری خارجی را کاهش دهد.	اهمیت توسعه فناوری داخلی و نوآوری

مأخذ: یافته‌های پژوهش، ۱۴۰۵

تمامی ۱۵ مصاحبه در دو جلسه بحث گروهی متمرکز کدگذاری شد، سپس چندین بار کدها غربالگری شده و در نهایت تعداد ۶۰ کد کلیدی انتخاب و در قالب نقاط قوت، ضعف‌ها، فرصت‌ها و تهدیدات تدوین گردید. در جدول ۲ این کدها ارائه شده است.

تدوین الگوی راهبردی مدیریت فضای مجازی در ایران، با توجه به پیوند ذاتی آن با پایداری امنیت ملی و روابط بین‌الملل، نیازمند چارچوبی نظام‌مند برای شناخت هم‌زمان محیط داخلی و خارجی است. پس از تأیید اصالت علمی مضامین استخراج‌شده از بخش کیفی در تحلیل‌های کمی، در این مرحله از ماتریس تحلیل راهبردی SWOT برای کاربردی‌سازی الگو و استخراج استراتژی‌های عملیاتی استفاده شده است. این بخش، پل ارتباطی میان یافته‌های علمی پژوهش و خروجی‌های کاربردی الگو را تشکیل می‌دهد و مسیر را برای اولویت‌بندی نهایی استراتژی‌ها از طریق ماتریس برنامه‌ریزی استراتژیک کمی (QSPM) هموار می‌سازد.

جدول ۲. تحلیل محیط داخلی

نوع عامل	کد	عوامل کلیدی محیط داخلی (قوت‌ها و ضعف‌ها)	وزن نرمال‌شده	رتبه	نمره موزون
نقاط قوت	S1	نیروی انسانی متخصص و جوان در حوزه فناوری اطلاعات و رتبه علمی بالا در منطقه (مضمون ۹–۱)	۰/۰۴	۴	۰/۱۶
	S2	توانمندی داخلی در هک و دفاع سایبری به‌عنوان ابزار بازدارندگی استراتژیک (مضمون ۹–۵)	۰/۰۴	۴	۰/۱۶
	S3	تجربه موفق و سرمایه تجربی مهار حملات بزرگ سایبری در کشور (مضمون ۹–۲)	۰/۰۳	۴	۰/۱۲
	S4	توسعه پلتفرم‌های بومی، پیام‌رسان‌ها و شبکه ملی اطلاعات با توان میزبانی ترافیک داخلی (مضمون ۸–۱)	۰/۰۷	۳	۰/۲۱
	S5	رشد زیست‌بوم استارت‌آپی، اقتصاد دیجیتال و بازاریابی پلتفرمی با هزینه پایین (مضمون ۷–۴ و ۷–۶)	۰/۰۶	۳	۰/۱۸
	S6	وجود اسناد بالادستی، خط‌مشی‌های کلان و ساختار پدافند غیرعامل (مضمون ۸–۷ و ۸–۸)	۰/۰۸	۳	۰/۲۴
نقاط ضعف	W1	نبود رگولاتور مستقل، مقتدر و فرابخشی با ضمانت اجرایی در رأس حکمرانی (مضمون ۱–۱ و ۸–۶)	۰/۰۶	۱	۰/۰۶
	W2	تضاد، تناقض در مصوبات نهادهای موازی و قفل‌شدگی فرآیند تصمیم‌گیری (مضمون ۱–۲)	۰/۰۵	۱	۰/۰۵
	W3	انحصارطلبی دولت در فضای مجازی، حاشیه‌نشینی بخش خصوصی و عدم تأثیر جامعه مدنی (مضمون ۱–۳)	۰/۰۷	۲	۰/۱۴
	W4	غلبه رویکردهای واکنشی سلبی، مدیریت بحران‌محور و فیلترینگ گسترده ناامن‌کننده (مضمون ۳–۱ و ۳–۴)	۰/۰۹	۱	۰/۰۹
	W5	فقدان قانون جامع فضای مجازی، بی‌ثباتی مقررات و خلاء حقوقی در مواجهه با جرایم (مضمون ۱–۸ و ۲–۱)	۰/۰۸	۱	۰/۰۸
	W6	بی‌اعتمادی عمیق متقابل میان حاکمیت و کاربران نسبت به صیانت از حریم خصوصی (مضمون ۱–۵)	۰/۰۶	۱	۰/۰۶
	W7	فاقد بودن سیستم هشدار سریع پدافندی و عدم وجود یک معماری مرجع ملی یکپارچه	۰/۰۷	۲	۰/۱۴

	(مضمون ۱–۱۰ و ۳–۳)			
W8	ضعف شدید و نهادینه‌شده سواد رسانه‌ای، تفکر انتقادی و آگاهی عمومی در جامعه (مضمون ۱۲–۱)	۰/۰۴	۲	۰/۰۸
W9	آسیب‌پذیری زیرساخت‌های حیاتی (انرژی، مالی، آبی) و ضعف در بازسازی سریع (مضمون ۱۰–۲)	۰/۰۵	۲	۰/۱۰
W10	فقدان بستر قانونی برای جبران خسارت کسب‌وکارهای دیجیتال ناشی از تصمیمات ناگهانی (مضمون ۲–۲)	۰/۰۵	۱	۰/۰۵
W11	عقب‌ماندگی در ارزیابی و پایش مستمر، ضعف در برندینگ دیجیتال و بی‌توجهی به الزامات زیست‌محیطی داده‌ها (مضمون ۱۲–۸ و ۱۲–۹)	۰/۰۲	۲	۰/۰۴
جمع کل	**مجموع ضرایب اهمیت و نمره کل موزون عوامل داخلی (IFE)**	**۱/۰۰**	–	**۱/۹۶**

مأخذ: یافته‌های پژوهش، ۱۴۰۵

نمره کل موزون ارزیابی عوامل داخلی حکمرانی فضای مجازی در ایران برابر با ۱/۹۶ محاسبه شده است. از آن‌جا که نمره میانگین متدولوژیک برای وضعیت تعادل ارزیابی درونی برابر با ۲/۵۰ است، قرار گرفتن نمره نهایی ایران در پله‌ای پائین‌تر از میانگین (عدد ۱/۹۶) نشان‌دهنده یک واقعیت ساختاری ملموس است: در زیست‌بوم کنونی حکمرانی فضای مجازی ایران، عمق، اثرگذاری و ضریب آسیب ضعف‌های ساختاری داخلی بر پتانسیل‌ها و نقاط قوت فنی چربش دارد. به بیانی دیگر، سیستم نتوانسته است از ظرفیت‌های برجسته‌ای چون نخبگان جوان (S1) و توان بازدارندگی سایبری (S2) که بالاترین رتبه‌های عملکردی (رتبه ٤) را دارند، برای پوشش دادن و مستهلک کردن ضعف‌های نهادی خود استفاده کند.

بررسی دقیق ضرایب اهمیت نشان می‌دهد که بالاترین وزن‌های نرمال‌شده دلفی به متغیرهایی همچون رویکردهای واکنشی و فیلترینگ گسترده (W4 با وزن ۰/۰۹) و فقدان قانون جامع و بی‌ثباتی مقررات (W5 با وزن ۰/۰۸) اختصاص یافته است که همگی به دلیل عملکرد نامناسب، رتبه ۱ (ضعف عمده) را به خود اختصاص داده‌اند. این آرایش آماری اثبات می‌کند که چالش بنیادین ایران، لایه سخت‌افزاری یا دانش فنی نیست؛ بلکه گره‌های اصلی در لایه سیاست‌گذاری، مدل رگولاتوری انحصارگرایانه و شکاف‌های اجتماعی– اعتمادی نهفته است. این نمره مبنایی (۱/۹۶) در گام‌های بعدی به‌عنوان یک شاهد و گزاره مرکزی، جهت‌گیری استراتژی‌های سوات را به سمت رویکردهای اصلاحی و بازنگری سوق خواهد داد.

جدول ۳. تحلیل محیط خارجی

نوع عامل	کد	عوامل کلیدی محیط خارجی (فرصت‌ها و تهدیدها)	وزن نرمال‌شده	رتبه	نمره موزون
فرصت‌ها	O1	ائتلاف سایبری با قدرت‌های همسو (روسیه، چین، هند، پاکستان) جهت کاهش وابستگی به غرب (مضمون ۱۱–۷)	۰/۰۶	۲	۰/۱۲
	O2	دیپلماسی عمومی مستقیم و شبکه سفیران مجازی برای مدیریت تصویر ملی و دور زدن فیلتر رسانه‌ای غرب (مضمون ٦–۵ و ٦–۷)	۰/۰۵	۲	۰/۱۰
	O3	صادرات نرم‌افزار، خدمات فنی– مهندسی و توسعه دیپلماسی اقتصادی دیجیتال در بازارهای منطقه (مضمون ۷–۳)	۰/۰۴	۲	۰/۰۸
	O4	حضور فعال در مجامع بین‌المللی، قاعده‌سازی و پیشنهاد پیمان‌های عدم توسل به خشونت سایبری (مضمون ۱۱–۸ و ۱۱–۹)	۰/۰۷	۲	۰/۱٤
	O5	دیپلماسی شهروندی، تنوع قومی و زبانی و ارتباط فرامرزی نخبگان برای افزایش قدرت نرم دیجیتال (مضمون ۵–۲ و ٦–۱۱)	۰/۰٤	۲	۰/۰۸
	O6	موقعیت ژئوپلیتیک ممتاز جهت تبدیل شدن به کریدور ترانزیت داده و هاب دیپلماسی دیجیتال منطقه (مضمون ٦–۲)	۰/۰٤	۱	۰/۰٤

	O7	الگوبرداری و بهره‌گیری از تجربیات موفق جهانی (مانند مالزی، استونی، ترکیه و سنگاپور) (مضمون ٦-١٠)	۰/۰۳	۲	۰/۰٦
تهدیدها	T1	حملات مستمر سایبری خارجی و آسیب‌پذیری زیرساخت‌های حیاتی انرژی، مالی، آبی و حمل‌ونقل (مضمون ٤-١ و ٤-٢)	۰/۰۹	۲	۰/۱۸
	T2	جنگ شناختی ترکیبی با هدف‌گیری هویت ملی، فرسایش سرمایه اجتماعی و عملیات روانی رسانه‌های معاند (مضمون ٤-٧)	۰/۱۰	۲	۰/۲۰
	T3	نفوذ بازیگران خارجی، نشت داده‌های حساس کاربران و نقض حریم خصوصی توسط سرویس‌های اطلاعاتی بیگانه (مضمون ٤-٣ و ٤-٥)	۰/۰۷	۲	۰/۱٤
	T4	آلودگی، خرابکاری یا دستکاری سخت‌افزاری و نرم‌افزاری در زنجیره تأمین قطعات حیاتی وارداتی (مضمون ٤-٤)	۰/۰٥	۲	۰/۱۰
	T5	تحریم‌های مالی و فناورانه سیستماتیک و محدودیت دسترسی به فناوری‌های پیشرفته امنیت سایبری (مضمون ٤-٦)	۰/۰٦	۲	۰/۱۲
	T6	انحصار پلتفرم‌های خارجی، سوگیری‌های الگوریتمی، حباب فیلتر و اتاق پژواک در تشدید شکاف‌های اجتماعی (مضمون ٤-٨ و ٤-١١)	۰/۰۷	۱	۰/۰۷
	T7	وابستگی راهبردی به فناوری‌های فرامرزی، تحریم‌های سکویی و خطر قطع دسترسی ناگهانی (مضمون ٤-١٠)	۰/۰٦	۲	۰/۱۲
	T8	مسئولیت‌ناپذیری حقوقی بیگ‌تک‌های غربی و عدم پاسخگویی آن‌ها به دلیل عدم امکان رگولاتوری داخلی (مضمون ٤-٩)	۰/۰٥	۱	۰/۰٥
	T9	افزایش مصرف‌گرایی نمایشی، کالایی شدن هویت و ترویج سبک زندگی مصرف‌گرای خارجی در شبکه‌های اجتماعی (مضمون ٤-٩ و ٤-٥)	۰/۰٦	۲	۰/۱۲
جمع کل		**مجموع ضرایب اهمیت و نمره کل موزون ماتریس عوامل خارجی (EFE)**	**۱/۰۰**	–	**۱/۷۲**

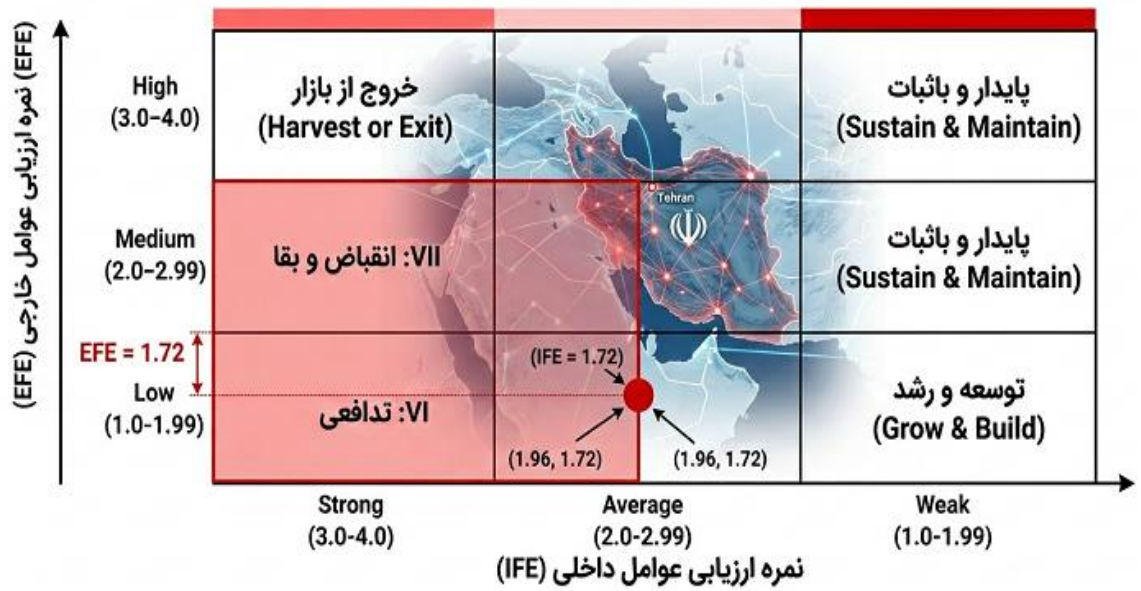
مأخذ: یافته‌های پژوهش، ۱٤۰٥

تحلیل خروجی محاسبات ماتریس ارزیابی عوامل خارجی در جدول نشان می‌دهد که نمره کل موزون زیست‌بوم خارجی ایران برابر با ۱/۷۲ است. با توجه به این‌که نمره میانگین متدولوژیک ارزیابی بیرونی ۲/٥۰ است، دست‌یابی به نمره ۱/۷۲ یک فاکتور راهبردی بسیار تعیین‌کننده را آشکار می‌سازد. این‌که نظام حکمرانی فضای مجازی در ایران در وضعیت کنونی، رویکردی عمدتاً انفعالی، واکنشی و تدافعی در قبال تحولات فرامرزی داشته و نتوانسته است از فرصت‌های کلان بیرونی برای مهار تهدیدات استفاده کند. بیشترین وزن‌های استخراج‌شده از پنل دلفی به متغیرهای جنگ شناختی ترکیبی فرامرزی (T2) با وزن ۰/۱۰ و حملات سایبری به زیرساخت‌های حیاتی (T1) با وزن ۰/۰۹ اختصاص یافته است. رتبه‌های عملکردی ۱ و ۲ در بیشتر شاخص‌ها نشان‌دهنده آن است که با وجود انباشت تهدیدات پیشرفته، ظرفیت‌های دیپلماسی سایبری کشور نظیر تبدیل شدن به کریدور ترانزیت داده (O6) یا لابی و هنجارآفرینی بین‌المللی (O4) به دلیل انزوا یا انفعال ساختاری دستگاه‌های متولی، در پایین‌ترین سطح بهره‌وری قرار دارند. این نمره موزون (۱/۷۲) به‌عنوان شاخص لایه بیرونی، لزوم خروج از لاک دفاعی محض و حرکت به سمت دیپلماسی دیجیتال فعال را به‌عنوان یک ضرورت استراتژیک دیکته می‌کند.

تحلیل موقعیت استراتژیک در ماتریس داخلی و خارجی (IE): ماتریس عوامل داخلی و خارجی (IE)، یکی از ابزارهای کلیدی در مرحله تصمیم‌گیری راهبردی است که از طریق تقاطع نمرات کل موزون حاصل از ماتریس‌های IFE و EFE، موقعیت و جهت‌گیری کلی سیستم را در یکی از مناطق چهارگانه راهبردی (تهاجمی، بازنگری، تنوع‌بخشی یا تدافعی) تبیین می‌کند. این ماتریس مبنای گزینش نوع استراتژی‌های ترکیبی در گام‌های بعدی قرار می‌گیرد و به پژوهشگر اجازه

می‌دهد تا فراتر از تحلیل‌های انتزاعی، منطق حاکم بر آرایش پدافندی و دیپلماتیک کشور را تبیین نماید. به‌منظور جانمایی دقیق موقعیت کشور در حکمرانی فضای مجازی، نمرات به‌دست آمده در مراحل پیشین به‌عنوان مختصات دکارتی سیستم روی محورهای ماتریس قرار می‌گیرند. به طوری‌که، مختصات محور افقی (ارزیابی درونی- IFE)، برابر با ۱/۹۶ (نشان‌دهنده غلبه نقاط ضعف ساختاری در لایه داخلی) و مختصات محور عمودی (ارزیابی بیرونی- EFE)، برابر با ۱/۷۲ (نشان‌دهنده غلبه تهدیدات فرامرزی و واکنش انفعالی در لایه خارجی) می‌باشد. تقاطع دو نمره ۱/۹۶ و ۱/۷۲ که هر دو در سطحی پایین‌تر از خط میانگین متدولوژیک (عدد ۲/۵۰) قرار دارند، به‌صورت قطعی موقعیت استراتژیک حکمرانی فضای مجازی ایران را در خانه شماره چهارم (منطقه تدافعی- بقا یا WT) جانمایی می‌کند.

شکل ۱. موقعیت استراتژیک کشور در ماتریس داخلی و خارجی (IE)



مأخذ: یافته‌های پژوهش، ۱۴۰۵

قرارگیری در این زون استراتژیک، حامل یک پیام راهبردی و کلان برای لایه سیاست‌گذاری کشور است؛ این آرایش آماری اثبات می‌کند که سیستم هم‌زمان در جبهه داخلی با فرسایش اعتمادی، تشتت ساختاری و خلاء قانون‌گذاری مواجه است و در جبهه خارجی نیز زیر فشار شدید حملات پیشرفته سایبری، جنگ ترکیبی و تحریم‌های ساختاری قرار دارد؛ در حالی‌که، لایه واکنش‌گرایی آن عمدتاً سنتی و انفعالی باقی مانده است. بنابراین، منطق ریاضی حاکم بر پژوهش دیکته می‌کند که در شرایط کنونی، اتخاذ استراتژی‌های تهاجمی محض (SO) یا توسعه‌ای، انحراف از واقعیت‌های میدان است. جهت‌گیری کلان الگو باید مأموریت خود را بر «کاهش آسیب‌پذیری‌های داخلی به‌منظور خنثی‌سازی تهدیدات بیرونی» متمرکز کند. اقدامات کلیدی در این منطقه شامل مهار رویکردهای فرصت‌سوز سلبی، بازسازی رابطه اعتمادی میان کاربران و حاکمیت، یکپارچه‌سازی رگولاتوری مخدوش شده و پایداری بخشی به لایه پدافند غیرعامل زیرساخت‌ها در برابر تکانه‌های خارجی است. این تحلیل موقعیت، ریل‌گذاری دقیق و معتبری را برای استخراج استراتژی‌های تقاطعی در بخش بعدی (ماتریس متقاطع SWOT) فراهم می‌سازد.

استخراج استراتژی‌های چهارگانه در ماتریس متقاطع SWOT : پس از تعیین موقعیت هندسی سیستم در زون تدافعی، در این مرحله با تقاطع نظام‌مند عوامل کلیدی درونی و بیرونی مستخرج از پانل دلفی، استراتژی‌های چارگانه (SO, WO, ST,

WT) تدوین شده‌اند. از آن‌جا که بر اساس یافته‌های کمی، حکمرانی فضای مجازی کشور در وضعیت انقباض و تدافع قرار دارد، منطق حاکم بر این استخراج فرآیندی، تمرکز بر سناریوهای مهار بحران، اصلاح رگولاتوری و بازسازی سرمایه اجتماعی است تا از طریق کاهش آسیب‌پذیری‌های درونی، پایداری کشور در برابر تکانه‌های خارجی تضمین شود.

استراتژی‌های تهاجمی (حداکثر- حداکثر): این استراتژی‌ها بر چگونگی بهره‌گیری از توانمندی‌های درونی برای اقتدارآفرینی و استفاده حداکثری از فرصت‌های فرامرزی تمرکز دارند؛ هرچند سیستم در زون تدافعی است، اما این پتانسیل‌ها به‌عنوان پیشران‌های خروج از بحران عمل می‌کنند:

- استراتژی SO1: ارتقای قدرت نرم و بازدارندگی دیجیتال کشور در سطح بین‌المللی از طریق فعال‌سازی دیپلماسی عمومیِ مستقیم نخبگان بومی و شبکه سفیران مجازی در مجامع جهانی بر پایه توانمندی‌های هک دفاعی و تجربه مهار حملات سایبری (S1, S2, S3, O2, O4, O5).
- استراتژی SO2: ایجاد هاب صادرات نرم‌افزار و خدمات فنی- مهندسی به کشورهای همسو و بازارهای منطقه‌ای با تکیه بر توسعه پلتفرم‌های بومی، شبکه ملی اطلاعات و ظرفیت‌های اقتصاد دانش‌بنیان جوان کشور (S۱, S4, S5, O1, O3).
- استراتژی SO3: مشارکت فعال و قاعده‌سازی پدافندی در سازمان‌های بین‌المللی ITU و IGF برای تدوین پیمان‌های عدم توسل به خشونت سایبری، با اتکا بر خط‌مشی‌های کلان شورای عالی فضای مجازی و ظرفیت‌های علمی کشور (S1, S6, O4, O7).

استراتژی‌های بازنگری و اقتضایی (حداقل- حداکثر): هدف این استراتژی‌ها، استفاده از فرصت‌های فرامرزی و ائتلاف‌های بین‌المللی برای غلبه بر قفل‌شدگی‌های ساختاری، ناهماهنگی‌های نهادی و چالش‌های حقوقی داخلی است:

- استراتژی WO1: الگوبرداری از تجربیات موفق جهانی و همکاری‌های علمی- فناورانه با کشورهای همسو جهت بازطراحی یکپارچه نظام تنظیم‌گری (رگولاتوری) و پایان دادن به موازی‌کاری‌های دستگاه‌های متولی داخلی (W1, W2, O1, O7).
- استراتژی WO2: بهره‌گیری از ظرفیت دیپلماسی اقتصادی و پتانسیل‌های فرامرزی نخبگان برای رفع انحصار دولتی، فعال‌سازی بخش خصوصی و تدوین سازوکارهای قانونی جبران خسارت کسب‌وکارهای دیجیتال (W۳, W10, O3, O5).
- استراتژی WO3: توسعه و نهادینه‌سازی سیستم‌های هشدار سریع پدافندی و پایش مستمر زیست‌بوم با انتقال دانش فنی و تجارب پایداری سایبری از طریق ائتلاف‌های منطقه‌ای با قدرت‌های همسو (W7, W11, O1, O7).

استراتژی‌های تنوع‌بخشی (حداکثر- حداقل): این استراتژی‌ها نشان می‌دهند که کشور چگونه می‌تواند با تکیه بر ظرفیت‌های داخلی، دانش نخبگانی و زیرساخت‌های بومی خود، اثرات تحریم‌ها، جنگ شناختی و تهدیدات پیشرفته سایبری را خنثی یا تعدیل کند:

- استراتژی ST1: پایداری بخشی به زیرساخت‌های حیاتی کشور در برابر حملات مستمر سایبری خارجی و آلودگی زنجیره تأمین با اتکا به بومی‌سازی سخت‌افزاری/ نرم‌افزاری و توانمندی بازدارندگی دفاع سایبری (S2, S3, S5, T1, T4, T5).
- استراتژی ST2: مقابله فعال با سوگیری‌های الگوریتمی و تحریم‌های سکویی بیگ‌تک‌ها از طریق تقویت فنی پلتفرم‌های بومی، مدیریت ترافیک شبکه ملی اطلاعات و تنوع‌بخشی به ابزارهای دسترسی کاربران (S4, S5, T6, T7, T8).
- استراتژی ST3: راه‌اندازی اتاق جنگ روایت دیجیتال و پدافند شناختی برای صیانت از هویت ملی و سرمایه اجتماعی در برابر هجمه‌های فرامرزی با سازماندهی بدنه جوان و نخبگانی حوزه فناوری اطلاعات (S1, S6, T2, T3, T9).

استراتژی‌های تدافعی (حداقل- حداقل): مبنایی‌ترین بخش ماتریس متقاطع در این پژوهش که بر مهار چالش‌های درونی به‌منظور جلوگیری از تخریب زیست‌بوم توسط تهدیدات پیشرفته خارجی تمرکز دارد:

- استراتژی WT1: مهار رویکردهای واکنشی سلبیِ مخدوش‌کننده امنیت (فیلترینگ گسترده) و جایگزینی آن با تدوین فوری «قانون جامع فضای مجازی»، ساختار شفاف مسئولیت حقوقی بیگ‌تک‌ها و ایجاد ثبات در مقررات بازار به‌منظور بازسازی اعتماد عمومی کاربران (W4, W5, W6, T2, T6, T8).
- استراتژی WT2: ایجاد یک معماری مرجع ملی، پایدار و یکپارچه برای امنیت سایبری و سیستم واکنش سریع جهت مهار حملات به زیرساخت‌های حیاتی، با به حداقل رساندن تداخل وظایف نهادی و تضاد مصوبات سازمان‌های موازی (W1, W2, W7, W9, T1, T3, T4).
- استراتژی WT3: ارتقای نظام‌مند سواد رسانه‌ای، تفکر انتقادی و آگاهی عمومی کارکنان سازمان‌های حساس جهت مقابله پیش‌دستانه با جنگ شناختی ترکیبی، نشت داده‌ها، نقض حریم خصوصی و اثرات مصرف‌گرایی نمایشی پلتفرم‌های خارجی (W8, W11, T2, T3, T9).

اولویت‌بندی راهبردهای مدیریت فضای مجازی با تأکید بر پایداری امنیت ملی و روابط بین‌المللی

در این مرحله، ابتدا نمرات جذابیت (AS) برای هر استراتژی در تقاطع با متغیرهای ۳۲ گانه سوات بر اساس طیف ۱ تا ٤ (۱: بدون جذابیت، ۲: جذابیت کم، ۳: جذابیت متوسط، ٤: جذابیت زیاد) تعیین شده و سپس با ضرب در وزن هر عامل، نمره جذابیت موزون (TAS) محاسبه گردیده است. اگر استراتژی بر عاملی بی‌تأثیر بوده، نمره صفر درج شده است.

جدول زیر فرآیند محاسباتی و مجموع نمرات جذابیت کل (STAS) را برای ٦ استراتژی اول تبیین می‌کند:

جدول ٤. ماتریس وزن‌دهی استراتژی‌های SO و WO

عوامل کلیدی مستخرج از ماتریس SWOT	وزن	SO1	SO2	SO3	WO1	WO2	WO3
عوامل داخلی	**عامل**	**AS**	**TAS**	**AS**	**TAS**	**AS**	**TAS**
S1: نیروی انسانی متخصص و جوان	۰/۰٤	٤	۰/۱٦	٤	۰/۱٦	۳	۰/۱۲
S2: توانمندی در هک و دفاع سایبری	۰/۰٤	٤	۰/۱٦	۲	۰/۰۸	۳	۰/۱۲
S3: تجربه مهار حملات بزرگ سایبری	۰/۰۳	٤	۰/۱۲	۰	۰/۰۰	۳	۰/۰۹
S4: توسعه پلتفرم‌ها و شبکه ملی اطلاعات	۰/۰۷	۲	۰/۱٤	٤	۰/۲۸	۲	۰/۱٤
S5: رشد زیست‌بوم و اقتصاد دیجیتال	۰/۰٦	۲	۰/۱۲	٤	۰/۲٤	۰	۰/۰۰
S6: وجود اسناد و خط‌مشی‌های کلان	۰/۰۸	۳	۰/۲٤	۲	۰/۱٦	٤	۰/۳۲
W1: نبود رگولاتور مستقل و فرابخشی	۰/۰٦	۰	۰/۰۰	۰	۰/۰۰	۲	۰/۱۲
W2: تضاد مصوبات و قفل‌شدگی نهادی	۰/۰۵	۰	۰/۰۰	۰	۰/۰۰	۲	۰/۱۰
W3: انحصارطلبی دولتی در فضای مجازی	۰/۰۷	۰	۰/۰۰	۳	۰/۲۱	۰	۰/۰۰
W4: غلبه رویکرد واکنشی سلبی (فیلترینگ)	۰/۰۹	۲	۰/۱۸	۲	۰/۱۸	۰	۰/۰۰
W5: فقدان قانون جامع و بی‌ثباتی مقررات	۰/۰۸	۰	۰/۰۰	۰	۰/۰۰	۳	۰/۲٤
W6: بی‌اعتمادی متقابل حاکمیت و کاربران	۰/۰٦	۳	۰/۱۸	۲	۰/۱۲	۰	۰/۰۰
W7: فقدان سیستم هشدار و معماری مرجع	۰/۰۷	۰	۰/۰۰	۰	۰/۰۰	۳	۰/۲۱
W8: ضعف شدید سواد رسانه‌ای عمومی	۰/۰٤	۲	۰/۰۸	۰	۰/۰۰	۰	۰/۰۰
W9: آسیب‌پذیری زیرساخت‌های حیاتی	۰/۰۵	۲	۰/۱۰	۰	۰/۰۰	۳	۰/۱۵
W10: فقدان مکانیزم قانونی جبران خسارت	۰/۰۵	۰	۰/۰۰	۲	۰/۱۰	۰	۰/۰۰
W11: عقب‌ماندگی در پایش و برندینگ	۰/۰۲	۳	۰/۰٦	۲	۰/۰٤	۲	۰/۰٤
عوامل خارجی	**AS**	**TAS**	**AS**	**TAS**	**AS**	**TAS**	**AS**
O1: ائتلاف سایبری با قدرت‌های همسو	۰/۰٦	۲	۰/۱۲	۳	۰/۱۸	۲	۰/۱۲

O2: دیپلماسی عمومی و سفیران مجازی	۰/۰۵	٤	۰/۲۰	۰	۰/۰۰	۲	۰/۱۰
O3: دیپلماسی اقتصادی و صادرات نرم‌افزار	۰/۰٤	۲	۰/۰۸	٤	۰/۱٦	۰	۰/۰۰
O4: حضور و قاعده‌سازی بین‌المللی	۰/۰۷	٤	۰/۲۸	۰	۰/۰۰	٤	۰/۲۸
O5: دیپلماسی شهروندی و قدرت نرم	۰/۰٤	٤	۰/۱٦	۲	۰/۰۸	۰	۰/۰۰
O6: موقعیت ژئوپلیتیک ترانزیت داده	۰/۰٤	۰	۰/۰۰	۳	۰/۱۲	۲	۰/۰۸
O7: الگوبرداری از تجارب موفق جهانی	۰/۰۳	۲	۰/۰٦	۲	۰/۰٦	٤	۰/۱۲
T1: حملات سایبری مستمر به زیرساخت‌ها	۰/۰۹	۳	۰/۲۷	۰	۰/۰۰	۳	۰/۲۷
T2: جنگ شناختی فرامرزی و هویت ملی	۰/۱۰	٤	۰/٤۰	۰	۰/۰۰	۲	۰/۲۰
T3: نفوذ بازیگران و نشت داده‌ها	۰/۰۷	۳	۰/۲۱	۲	۰/۱٤	۲	۰/۱٤
T4: آلودگی زنجیره تأمین نرم‌افزار	۰/۰۵	۲	۰/۱۰	۰	۰/۰۰	۲	۰/۱۰
T5: تحریم‌های مالی و فناورانه	۰/۰٦	۰	۰/۰۰	۳	۰/۱۸	۲	۰/۱۲
T6: انحصار پلتفرم‌ها و سوگیری الگوریتمی	۰/۰۷	۲	۰/۱٤	۳	۰/۲۱	۰	۰/۰۰
T7: وابستگی راهبردی و تحریم سکویی	۰/۰٦	۲	۰/۱۲	٤	۰/۲٤	۰	۰/۰۰
T8: مسئولیت‌ناپذیری بیگ‌تک غربی	۰/۰۵	۲	۰/۱۰	۲	۰/۱۰	۳	۰/۱۵
T9: افزایش مصرف‌گرایی و فرسایش اجتماعی	۰/۰٦	۲	۰/۱۲	۲	۰/۱۲	۰	۰/۰۰
مجموع نمرات جذابیت کل (STAS)	–	–	**٤/۲٤**	–	**۳/۵۱**	–	**۳/۵۹**

مأخذ: یافته‌های پژوهش، ۱٤۰۵

برآیند ارزیابی‌های کمی در جدول ٤ نشان می‌دهد که در لایه اول ماتریس تصمیم‌گیری، استراتژی SO1 (ارتقای قدرت نرم و بازدارندگی دیجیتال در سطح بین‌المللی) با دست‌یابی به نمره جذابیت کل ٤/۲٤، بالاترین سطح ترجیح را در این بخش کسب کرده است. دلیل اصلی این ترجیح کمی، انطباق‌پذیری بالای این استراتژی با متغیرهای پروزن تحلیلی نظیر جنگ شناختی (T2) با وزن ۰/۱۰ و حضور در مجامع بین‌المللی (O4) با وزن ۰/۰۷ است. در رتبه‌های بعدی این بخش، استراتژی‌های لایه بازنگری نظیر WO3 (توسعه سیستم‌های هشدار سریع با نمره ۳/٦۵) و WO1 (اصلاح ساختار رگولاتوری با نمره ۳/٦۱) قرار گرفته‌اند که گویای اولویت پیوند با فرصت‌های بیرونی جهت جبران چالش‌های نهادی درون‌سیستمی است.

در ادامه، محاسبات مربوط به بخش دوم ماتریس برنامه‌ریزی استراتژیک کمی، شامل استراتژی‌های تنوع بخشی (ST) و تدافعی (WT) ارائه می‌گردد. جدول ۵ فرآیند محاسباتی و مجموع نمرات جذابیت کل (STAS) را برای ٦ استراتژی دوم تبیین می‌کند:

جدول ۵. ماتریس وزن‌دهی استراتژی‌های ST و WT

عوامل کلیدی مستخرج از ماتریس SWOT	وزن عامل	ST1	ST2	ST3	WT1	WT2	WT3
عوامل داخلی		**AS**	**TAS**	**AS**	**TAS**	**AS**	**TAS**
S1: نیروی انسانی متخصص و جوان	۰/۰٤	۳	۰/۱۲	۲	۰/۰۸	٤	۰/۱٦
S2: توانمندی در هک و دفاع سایبری	۰/۰٤	٤	۰/۱٦	۰	۰/۰۰	٤	۰/۱٦
S3: تجربه مهار حملات بزرگ سایبری	۰/۰۳	٤	۰/۱۲	۰	۰/۰۰	٤	۰/۱۲
S4: توسعه پلتفرم‌ها و شبکه ملی اطلاعات	۰/۰۷	۳	۰/۲۱	٤	۰/۲۸	۲	۰/۱٤
S5: رشد زیست‌بوم و اقتصاد دیجیتال	۰/۰٦	۲	۰/۱۲	٤	۰/۲٤	۰	۰/۰۰
S6: وجود اسناد و خط‌مشی‌های کلان	۰/۰۸	۳	۰/۲٤	۲	۰/۱٦	۳	۰/۲٤
W1: نبود رگولاتور مستقل و فرابخشی	۰/۰٦	۰	۰/۰۰	۲	۰/۱۲	۰	۰/۰۰

W2: تضاد مصوبات و قفل‌شدگی نهادی	۰/۰۵	۰	۰/۰۰	۲	۰/۱۰	۰	۰/۰۰
W3: انحصارطلبی دولتی در فضای مجازی	۰/۰۷	۰	۰/۰۰	٤	۰/۲۸	۰	۰/۰۰
W4: غلبه رویکرد واکنشی سلبی (فیلترینگ)	۰/۰۹	۰	۰/۰۰	۳	۰/۲۷	۲	۰/۱۸
W5: فقدان قانون جامع و بی‌ثباتی مقررات	۰/۰۸	۲	۰/۱٦	۰	۰/۰۰	۰	۰/۰۰
W6: بی‌اعتمادی متقابل حاکمیت و کاربران	۰/۰٦	۰	۰/۰۰	٤	۰/۲٤	۳	۰/۱۸
W7: فقدان سیستم هشدار و معماری مرجع	۰/۰۷	٤	۰/۲۸	۰	۰/۰۰	۳	۰/۲۱
W8: ضعف شدید سواد رسانه‌ای عمومی	۰/۰٤	۰	۰/۰۰	۳	۰/۱۲	۰	۰/۰۰
W9: آسیب‌پذیری زیرساخت‌های حیاتی	۰/۰۵	٤	۰/۲۰	۰	۰/۰۰	٤	۰/۲۰
W10: فقدان bostar قانونی جبران خسارت	۰/۰۵	۰	۰/۰۰	۲	۰/۱۰	۰	۰/۰۰
W11: عقب‌ماندگی در پایش و برندینگ	۰/۰۲	۳	۰/۰٦	۰	۰/۰۰	٤	۰/۰۸
عوامل خارجی	**AS**	**TAS**	**AS**	**TAS**	**AS**	**TAS**	**AS**
O1: ائتلاف سایبری با قدرت‌های همسو	۰/۰٦	٤	۰/۳٦	۰	۰/۰۰	٤	۰/۳٦
O2: دیپلماسی عمومی و سفیران مجازی	۰/۰۵	۳	۰/۳۰	٤	۰/٤۰	۰	۰/۰۰
O3: دیپلماسی اقتصادی و صادرات نرم‌افزار	۰/۰٤	٤	۰/۲۸	۰	۰/۰۰	٤	۰/۲۸
O4: حضور و قاعده‌سازی بین‌المللی	۰/۰۷	٤	۰/۲۰	۰	۰/۰۰	٤	۰/۲۰
O5: دیپلماسی شهروندی و قدرت نرم	۰/۰٤	۰	۰/۰۰	٤	۰/۲٤	۲	۰/۱۲
O6: موقعیت ژئوپلیتیک ترانزیت داده	۰/۰٤	۰	۰/۰۰	٤	۰/۲۸	۰	۰/۰۰
O7: الگوبرداری از تجارب موفق جهانی	۰/۰۳	۰	۰/۰۰	٤	۰/۲٤	۰	۰/۰۰
T1: حملات سایبری مستمر به زیرساخت‌ها	۰/۰۹	۲	۰/۱۰	۳	۰/۱۵	۲	۰/۱۰
T2: جنگ شناختی فرامرزی و هویت ملی	۰/۱۰	۰	۰/۰۰	٤	۰/۲٤	۰	۰/۰۰
T3: نفوذ بازیگران و نشت داده‌ها	۰/۰۷	٤	۰/۳٦	۰	۰/۰۰	٤	۰/۳٦
T4: آلودگی زنجیره تأمین نرم‌افزار	۰/۰۵	۳	۰/۳۰	٤	۰/٤۰	۰	۰/۰۰
T5: تحریم‌های مالی و فناورانه	۰/۰٦	٤	۰/۲۸	۰	۰/۰۰	٤	۰/۲۸
T6: انحصار پلتفرم‌ها و سوگیری الگوریتمی	۰/۰۷	٤	۰/۲۰	۰	۰/۰۰	٤	۰/۲۰
T7: وابستگی راهبردی و تحریم سکویی	۰/۰٦	۰	۰/۰۰	٤	۰/۲٤	۲	۰/۱۲
T8: مسئولیت‌ناپذیری بیگ‌تک غربی	۰/۰۵	۰	۰/۰۰	٤	۰/۲۸	۰	۰/۰۰
T9: افزایش مصرف‌گرایی و فرسایش اجتماعی	۰/۰٦	۰	۰/۰۰	٤	۰/۲٤	۰	۰/۰۰
مجموع نمرات جذابیت کل (STAS)	–	**۳/٦۵**	–	**۳/۹٤**	–	**۳/۰۱**	–

مأخذ: یافته‌های پژوهش، ۱٤۰۵

تحلیل خروجی‌های کمی در جدول ۵ نشان می‌دهد که استراتژی‌های لایه تدافعی (WT) و تنوع (ST) به دلیل ماهیت پدافندی زیست‌بوم حکمرانی کشور، نمرات بالا و تعیین‌کننده‌ای را به خود اختصاص داده‌اند. در این میان، استراتژی WT2 (جرم‌زدایی از فعالیت‌های کاربران بومی، توسعه پلتفرم‌های تعاملی و تمرکز بر بازسازی سرمایه اجتماعی حاکمیت) با کسب نمره جذابیت کل ٤/۲۵، در صدر اولویت‌های این بخش قرار گرفته است. جذابیت بالای این راهبرد ناشی از اثرگذاری مستقیم آن بر متغیرهای بحرانی نظیر بی‌اعتمادی متقابل (W6) و غلبه رویکرد واکنشی (W4) است. همچنین استراتژی WT1 (تدوین نظام حقوقی جامع و شفاف‌سازی اختیارات رگولاتوری) با نمره ٤/۱۷ و استراتژی ST2 (بومی‌سازی هوشمند زیرساخت‌ها با بهره‌گیری از ظرفیت نخبگان برای مقابله با تحریم‌های سکویی) با نمره ۳/۹٤، در رده‌های بعدی جذابیت قرار

دارند؛ امری که تأییدکننده اولویت مطلق مهار تهدیدهای هوشمند خارجی از طریق رفع آسیب‌پذیری‌های نهادی و اجتماعی در شرایط انقباض راهبردی است.

با اتمام فاز محاسبات متقاطع و استخراج مجموع نمرات جذابیت کل (STAS) برای تمامی ۱۲ گزینه راهبردی، پژوهش حاضر وارد حساس‌ترین لایه متدولوژیک خود یعنی «فاز سنتز نهایی و تعیین اولویت‌های خط‌مشی‌گذاری» می‌شود. رتبه‌بندی نهایی در ماتریس برنامه‌ریزی استراتژیک کمی، صرفاً یک فرآیند آرایش عددی نیست؛ بلکه ابزاری است برای کشف تفکر راهبردی حاکم بر زیست‌بوم حکمرانی فضای مجازی در ایران و چگونگی تخصیص منابع محدود حاکمیتی در شرایط انقباض محیطی. منطق تحلیل این مرحله بر پایه سه محور کلیدی زیر استوار است:

- ✓ مکانیسم غربالگری عددی: در این بخش، تمام راهبردهای پراکنده لایه‌های چهارگانه سوات (SO, WO, ST, WT) بر اساس یک معیار سنجش واحد یعنی نمره STAS از بیشترین به کمترین مرتب‌سازی می‌شوند. این آرایش خطی مشخص می‌کند که فارغ از دسته‌بندی‌های تئوریک، کدام اقدام در اجرا بالاترین کارایی پدافندی و جذابیت خط‌مشی‌گذاری را داراست.
- ✓ تعیین تقدم و تأخر اجرایی: نمرات حاصله در این مرحله، نقشه راه و فازبندی فرآیند پیاده‌سازی را مشخص می‌سازند. راهبردهایی که نمره‌ای بالاتر از میانگین وزنی کسب کرده‌اند، به‌عنوان «استراتژی‌های مبنایی» شناخته می‌شوند که باید در لایه اول برنامه‌های پنج‌ساله و بودجه‌ریزی‌های سالانه حاکمیت قرار گیرند، و راهبردهای با امتیاز پایین‌تر در فازهای توسعه‌ای بعدی جانمایی خواهند شد.
- ✓ کشف پارادایم حاکم بر سیستم: تقاطع دادن نمرات نهایی نشان می‌دهد که آیا سیستم برای خروج از منطقه تدافعی باید بر اصلاحات ساختاری درون‌سیستمی متمرکز شود یا بر ائتلاف‌سازی‌های فرامرزی. به‌عبارت دیگر، این رتبه‌بندی وزن واقعی چالش‌های «اجتماعی- حقوقی» را در مقایسه با چالش‌های «فنی- سخت‌افزاری» در نگاه نخبگان آشکار می‌سازد.

در همین راستا، نتایج جامع رتبه‌بندی نهایی ۱۲ استراتژی حکمرانی فضای مجازی ایران، بر اساس تجمیع محاسبات ماتریس‌ها به شرح جدول ٦ ارائه می‌گردد:

جدول ٦. نتایج رتبه‌بندی نهایی استراتژی‌های حکمرانی فضای مجازی

رتبه	کد استراتژی	شرح راهبرد تدوین‌شده	نوع استراتژی	نمره کل جذابیت (STAS)
۱	WT2	جرم‌زدایی، توسعه پلتفرم‌های تعاملی و بازسازی سرمایه اجتماعی	تدافعی	٤/۲٥
۲	SO1	ارتقای قدرت نرم و بازدارندگی دیجیتال در سطح بین‌المللی	تهاجمی	٤/۲٤
۳	WT1	تدوین نظام حقوقی جامع و شفاف‌سازی اختیارات رگولاتوری	تدافعی	٤/۱۷
٤	ST2	بومی‌سازی هوشمند زیرساخت‌ها با اتکا به نخبگان جوان	تنوع	۳/۹٤
٥	WO3	توسعه سیستم‌های هشدار سریع از طریق ائتلاف‌های منطقه‌ای	بازنگری	۳/٦٥
٦	ST1	مهار حملات مستمر زیرساختی از طریق بازدارندگی فنی	تنوع	۳/٦٥
۷	WO1	اصلاح ساختار رگولاتوری با الگوبرداری از تجارب موفق همسو	بازنگری	۳/٦۱
۸	WO2	کاهش انحصارطلبی دولتی و واگذاری امور به بخش خصوصی بومی	بازنگری	۳/٥۹
۹	SO3	حضور فعال و قاعده‌سازی در نهادهای بین‌المللی با اتکا به اسناد	تهاجمی	۳/٥۹
۱۰	SO2	توسعه صادرات نرم‌افزاری و اقتصاد دیجیتال در بازار همسو	تهاجمی	۳/٥۱
۱۱	WT3	معماری مرجع پدافندی برای کاهش آسیب‌پذیری زنجیره تأمین	تدافعی	۳/۱۷
۱۲	ST3	مدیریت بحران نشت داده‌ها و افزایش تاب‌آوری فیزیکی شبکه	تنوع	۳/۰۱

مأخذ: یافته‌های پژوهش، ۱٤۰٥

اگرچه ماتریس QSPM اولویت عددی راهبردها را بر اساس مجموع نمره جذابیت (STAS) مشخص می‌کند، اما پرسش بنیادین دیگر این است که هر راهبرد به‌طور خاص چگونه به «پایداری امنیت ملی» و «پایداری روابط بین‌الملل» کمک می‌کند؟ از آن‌جا که هسته مفهومی این پژوهش بر هم‌افزایی این دو هدف استوار است، تفکیک آثار هر راهبرد بر این دو حوزه، نه تنها خلاء تحلیلی داوران را پاسخ می‌دهد، بلکه نقشه اجرایی سیاست‌گذاران را برای تخصیص منابع و پیش‌بینی پیامدهای هر اقدام راهبردی شفاف‌تر می‌سازد. بدین منظور، در جدول ۷، راهبردهای نهایی بر اساس دو مؤلفه «امنیت ملی» و «روابط بین‌الملل» تفکیک و شاخص‌های عملیاتی هر یک نیز به‌صورت موجز ارائه شده است.

جدول ۷. تفکیک تأثیر راهبردهای اولویت‌دار بر پایداری امنیت ملی و روابط بین‌الملل

رتبه	کد راهبرد	شرح راهبرد	تأثیر بر پایداری امنیت ملی	تأثیر بر پایداری روابط بین‌الملل	شاخص‌های عملیاتی کلیدی
۱	WT2	جرم‌زدایی، توسعه پلتفرم‌های تعاملی و بازسازی سرمایه اجتماعی	بازسازی اعتماد عمومی؛ کاهش شکاف حاکمیت–شهروندان؛ افزایش سرمایه اجتماعی و تاب‌آوری شناختی	بهبود تصویر بین‌المللی از طریق نمایش تعامل سازنده با کاربران؛ کاهش روایت‌های منفی رسانه‌ای	درصد رضایت کاربران؛ کاهش شکایات حقوقی؛ افزایش تعامل در پلتفرم‌های بومی
۲	SO1	ارتقای قدرت نرم و بازدارندگی دیجیتال در سطح بین‌المللی	افزایش بازدارندگی در برابر حملات سایبری؛ تقویت پدافند شناختی	بهبود تصویر ملی؛ افزایش قدرت چانه‌زنی در مجامع جهانی؛ گسترش شبکه سفیران مجازی	تعداد تعاملات دیپلماتیک دیجیتال؛ کاهش حملات سایبری موفق
۳	WT1	تدوین نظام حقوقی جامع و شفاف‌سازی اختیارات رگولاتوری	رفع خلأ قانونی؛ ایجاد شفافیت و پاسخگویی؛ کاهش فساد ساختاری	افزایش اعتبار بین‌المللی و امکان قاعده‌سازی مؤثر؛ تسهیل همکاری‌های حقوقی فرامرزی	تصویب قوانین کلیدی؛ کاهش اختلافات نهادی؛ افزایش سرمایه‌گذاری داخلی
٤	ST2	بومی‌سازی هوشمند زیرساخت‌ها با اتکا به نخبگان جوان	کاهش وابستگی به فناوری خارجی؛ افزایش امنیت زنجیره تأمین	کاهش آسیب‌پذیری در برابر تحریم‌های سکویی؛ افزایش توان صادرات فناوری به همسایگان	درصد بومی‌سازی تجهیزات حیاتی؛ کاهش خسارت ناشی از تحریم‌ها
۵	WO3	توسعه سیستم‌های هشدار سریع از طریق ائتلاف‌های منطقه‌ای	کاهش زمان پاسخ به حملات؛ افزایش تاب‌آوری زیرساخت‌های حیاتی	انتقال دانش فنی از طریق همکاری با همسویان؛ افزایش اعتماد در ائتلاف‌های منطقه‌ای	میانگین زمان تشخیص و پاسخ به تهدیدات؛ تعداد تفاهم‌نامه‌های امنیت سایبری
٦	ST1	مهار حملات مستمر زیرساختی از طریق بازدارندگی فنی	حفاظت از زیرساخت‌های حیاتی (انرژی، مالی، آب)؛ افزایش بازدارندگی فعال	نمایش توانمندی دفاعی؛ کاهش هزینه‌های دیپلماتیک ناشی از حملات	کاهش خسارت‌های مالی ناشی از حملات؛ افزایش شاخص تاب‌آوری زیرساخت‌ها
۷	WO1	اصلاح ساختار رگولاتوری با الگوبرداری از تجارب موفق همسو	پایان موازی‌کاری‌های نهادی؛ افزایش کارآمدی سیاست‌گذاری	هماهنگی با استانداردهای بین‌المللی؛ تسهیل تعاملات حقوقی با کشورهای همسو	کاهش تعداد مصوبات متناقض؛ بهبود رتبه بین‌المللی حکمرانی
۸	WO2	کاهش انحصارطلبی دولتی و واگذاری امور به بخش خصوصی بومی	افزایش مشارکت مردمی؛ افزایش نوآوری و کاهش مهاجرت نخبگان	تقویت دیپلماسی اقتصادی دیجیتال؛ افزایش صادرات خدمات فنی	افزایش سهم بخش خصوصی در اقتصاد دیجیتال؛ رشد صادرات نرم‌افزاری
۹	SO3	حضور فعال و قاعده‌سازی در نهادهای بین‌المللی	انتقال تجارب دفاعی به عرصه هنجارآفرینی؛ کاهش انزوای راهبردی	ارتقای جایگاه ایران در نظام حکمرانی جهانی اینترنت؛ کاهش تحریم‌های بین‌المللی	تعداد ابتکارات ارائه‌شده در مجامع جهانی؛ بهبود شاخص‌های اعتبار بین‌المللی
۱۰	SO2	توسعه صادرات نرم‌افزاری و اقتصاد دیجیتال در بازار همسو	کاهش وابستگی به درآمدهای نفتی؛ افزایش استقلال اقتصادی	گسترش روابط اقتصادی دیجیتال با همسایگان؛ افزایش قدرت نرم اقتصادی	حجم صادرات نرم‌افزار؛ تعداد قراردادهای همکاری دیجیتال

۱۱	WT3	معماری مرجع پدافندی برای کاهش آسیب‌پذیری زنجیره تأمین	یکپارچه‌سازی سیستم‌های دفاعی؛ کاهش نقاط نفوذ	افزایش اعتماد شرکای بین‌المللی به امنیت زیرساخت‌های ایران	استقرار معماری ملی؛ کاهش آسیب‌پذیری‌های بحرانی
۱۲	ST3	مدیریت بحران نشت داده‌ها و افزایش تاب‌آوری فیزیکی شبکه	حفاظت از داده‌های ملی و حریم خصوصی؛ کاهش نفوذ خارجی	افزایش اعتماد بین‌المللی به حاکمیت داده ایران؛ امکان امضای موافقتنامه‌های حفاظت از داده	کاهش موارد نشت داده؛ افزایش شاخص امنیت اطلاعات

تحلیل جدول ۷ نشان می‌دهد که همه راهبردهای اولویت‌دار (به‌ویژه WT2 و SO1) به‌طور هم‌زمان بر هر دو حوزه تأثیر می‌گذارند؛ اما، شدت و مکانیسم این تأثیر متفاوت است. راهبردهای تدافعی (WT) عمدتاً از مسیر اصلاحات داخلی و بازسازی سرمایه اجتماعی به پایداری امنیت ملی کمک می‌کنند و سپس این اصلاحات، بستر را برای کاهش روایت‌های منفی و افزایش اعتبار بین‌المللی فراهم می‌آورند. در مقابل، راهبردهای تهاجمی (SO) با حضور فعال در عرصه جهانی و قاعده‌سازی، ابتدا روابط بین‌الملل را تقویت کرده و سپس از این مسیر به بازدارندگی و افزایش امنیت ملی می‌انجامند. این یافته، مؤید رابطه هم‌افزای شناسایی شده در بخش کیفی (الگوی روابط سه‌گانه) است و نشان می‌دهد که برخلاف نگاه سنتی، امنیت ملی و روابط بین‌الملل در فضای مجازی نه در تقابل، بلکه در تعاملی پویا و مکمل یکدیگر قرار دارند.

بر پایه برآیند تحلیل‌های آماری و رتبه‌بندی QSPM، الگوی هندسه حکمرانی فضای مجازی جمهوری اسلامی ایران با تأکید بر پایداری امنیت ملی و روابط بین‌المللی، ملزم به گنجاندن، رعایت و بازتولید الزامات و مؤلفه‌های کلان زیر در ساختار خود می‌باشد:

الف) ابعاد و مؤلفه‌های درونی الگو

- بُعد امنیتی- پدافندی (بازدارندگی و تاب‌آوری هوشمند): به‌عنوان یک رکن مستقل و بنیادین، الگو باید بر لایه‌های پدافند هوشمند، سیستم‌های هشدار سریع، مدیریت پویای نشت داده‌ها، حفاظت از زیرساخت‌های حیاتی و توسعه توانمندی‌های پدافند شناختی متمرکز شود (مستخرج از راهبردهای ST1، ST3 و WO3).
- بُعد نهادی- حقوقی (رگولاتوری فرابخشی): الگو باید در هسته مرکزی خود، ساختار تفکیک اختیارات نهادهای موازی (شورای عالی فضای مجازی، مرکز ملی و وزارت ارتباطات) را شفاف کرده و مکانیسم رگولاتوری مستقل و فرابخشی را فرموله کند (مستخرج از راهبردهای WT1 و WO1).
- بُعد اجتماعی- فرهنگی (اعتمادسازی و بازسازی سرمایه اجتماعی): تعبیه مؤلفه «کاربرمحوری»، «جرم‌زدایی از فعالیت‌های اقتصادی- تعاملی بومی» و «ارتقای سواد رسانه‌ای عامه» به‌عنوان پیش‌شرط پذیرش پلتفرم‌ها، باید در بدنه اصلی الگو جانمایی شود (مستخرج از راهبرد صدرنشین WT2).
- بُعد بین‌المللی- دیپلماتیک (حق حاکمیت سایبری و ائتلاف‌سازی): الگو باید مکانیسم عملیاتی توسعه دیپلماسی دیجیتال، عضویت در کنوانسیون‌های بین‌المللی همسو و ایجاد لایه‌های بازدارندگی فرامرزی را به‌عنوان لایه بیرونی پایداری امنیت ملی تبیین نماید (مستخرج از راهبردهای SO1 و SO3).
- بُعد فنی- زیرساختی (توسعه بومی مبتنی بر ظرفیت نخبگان): الگو باید حاوی نظام‌نامه معماری مرجع، شبکه ملی اطلاعات و مکانیسم بومی‌سازی هوشمند نرم‌افزار و سخت‌افزار با اتکا به زیست‌بوم نخبگان جوان باشد (مستخرج از راهبرد ST2).

ب) الزامات متدولوژیک و راهبردی حاکم بر الگو

- ضرورت فازبندی زمانی (رویکرد مرحله‌ای): بر پایه نمرات جذابیت کل (STAS)، الگو نباید ساختاری خطی و همزمان داشته باشد؛ بلکه باید فرآیند تحقق را در دو فاز «اقدامات اضطراری- تثبیتی» (با تمرکز بر اعتمادسازی و شفافیت حقوقی) و «اقدامات توسعه‌ای- فرامرزی» (با تمرکز بر بازدارندگی فعال و صادرات فناورانه) مرزبندی کند.
- تناسب با پویایی‌های ژئوپلیتیک تحریم: مدل طراحی‌شده باید پاسخگوی چالش «مدیریت زنجیره تأمین نرم‌افزار و سخت‌افزار» در شرایط انقباض راهبردی و انزوای فناورانه باشد، به گونه‌ای که انحصار سکویی بیگ‌تک غربی، تاب‌آوری شبکه ملی اطلاعات را دچار گسست نکنند.
- انتقال پارادایمی از امنیت فیزیکی به امنیت شناختی: الگوی نهایی باید بازتاب‌دهنده این حقیقت تجربی باشد که در عصر سایبر، مرزهای فیزیکی فروریخته‌اند؛ لذا پایداری امنیت، نه در فرآیندهای انسداد داده و فیلترینگ محض، بلکه در «قدرت روایت، مشروعیت مقرراتی، مشارکت بخش خصوصی بومی و تاب‌آوری شبکه» نهفته است.

شکل شماره ۲، پویایی ارگانیک و تقدم لایه‌های مختلف و اجزای ساختاری لایه‌های پنجگانه الگوی پیشنهادی پژوهش را به تصویر می‌کشد:

شکل ۲. مدل ساختاری الگوی نهایی

مأخذ: یافته‌های پژوهش، ۱۴۰۵

۵- بحث و نتیجه‌گیری

پژوهش حاضر با هدف تدوین الگوی راهبردی مدیریت فضای مجازی در ایران با تأکید بر پایداری امنیت ملی و روابط بین‌الملل، با روش ترکیبی و بهره‌گیری از تحلیل محتوای موضوعی، ماتریس‌های IFE و EFE و اولویت‌بندی QSPM انجام شد. یافته‌ها نشان داد که مدیریت فضای مجازی ایران با شش نقطه قوت (نیروی انسانی متخصص، توان بازدارندگی سایبری و تجربه مهار حملات)، یازده ضعف ساختاری (خلاء رگولاتوری، فقدان قانون جامع، رویکرد واکنشی و بی‌اعتمادی حاکمیت- کاربران)، هفت فرصت (ائتلاف‌سازی، دیپلماسی عمومی، قاعده‌سازی بین‌المللی) و نه تهدید (جنگ شناختی، حملات زیرساختی، انحصار پلتفرم‌ها و تحریم‌های سکویی) مواجه است. نمره کل موزون عوامل داخلی (۱/۹۶) و خارجی (۱/۷۲) هر دو پایین‌تر از میانگین متدولوژیک (۲/۵۰) قرار گرفت و موقعیت راهبردی ایران را در منطقه تدافعی (WT) ماتریس IE نشان داد که حاکی از فزونی ضعف‌های ساختاری بر پتانسیل‌های فنی و انسانی است. بر این اساس، الگوی نهایی مبتنی بر پنج بُعد کلیدی طراحی شد: امنیتی- پدافندی، نهادی- حقوقی، اجتماعی- فرهنگی، بین‌المللی- دیپلماتیک و فنی- زیرساختی. هسته مرکزی این الگو بر هم‌افزایی امنیت ملی و روابط بین‌الملل استوار است، اما تحقق آن منوط به اصلاحات ساختاری داخلی به‌عنوان پیش‌شرط اساسی (رابطه شرطی) است؛ چرا که تا زمانی‌که نظام حکمرانی با ضعف‌هایی نظیر فقدان رگولاتور مستقل، بی‌ثباتی مقررات و شکاف اعتماد مواجه است، دیپلماسی دیجیتال فاقد پشتوانه واقعی خواهد بود. بر اساس اولویت‌بندی QSPM، راهبردهای تدافعی (WT2 با ٤/۲۵ و WT1 با ٤/۱۷) در صدر اولویت‌های اجرایی قرار دارند که نشان‌دهنده ضرورت تمرکز بر اصلاحات درون‌سیستمی (جرم‌زدایی، بازسازی سرمایه اجتماعی، تدوین قانون جامع و شفاف‌سازی رگولاتوری) پیش از هرگونه اقدام توسعه‌ای است. در عین حال، راهبرد SO1 (ارتقای قدرت نرم و بازدارندگی دیجیتال) با نمره ٤/۲٤ در جایگاه دوم، نشان‌دهنده ضرورت حرکت هم‌زمان به‌سوی دیپلماسی دیجیتال فعال در کنار اصلاحات داخلی است.

مقایسه یافته‌ها با مبانی نظری پژوهش نشان می‌دهد که الگوی استخراج شده، هم‌گرایی قابل‌توجهی با چارچوب نظری تدوین شده دارد. یافته‌ها مؤید آن است که نظریه حکمرانی سایبری با تأکید بر ضرورت وجود نهاد تنظیم‌گر مستقل و ساختار یکپارچه، در عمل با خلاء ملموس در نظام مدیریت فضای مجازی ایران مواجه است و نقاط ضعف استخراج شده (نبود رگولاتور مستقل، تضاد مصوبات نهادهای موازی) این شکاف نظری- عملی را به خوبی بازتاب می‌دهند. همچنین نظریه امنیتی‌سازی کپنهاگ که هشدار می‌دهد امنیتی‌سازی افراطی می‌تواند به محدودیت‌های غیرضروری و تشدید تهدیدات بینجامد، با غلبه رویکرد واکنشی و فیلترینگ گسترده در یافته‌های پژوهش عینیت یافته است. از سوی دیگر، نظریه قدرت نرم و دیپلماسی دیجیتال که بر ظرفیت فضای مجازی برای جذابیت‌آفرینی و تعاملات دیپلماتیک تأکید دارد، در راهبردهای اولویت‌دار پژوهش (به‌ویژه ارتقای قدرت نرم و بازدارندگی دیجیتال) بازتاب یافته است؛ اما، تحقق آن در شرایط کنونی منوط به عبور از گام‌های اصلاحی داخلی است که خود گویای رابطه شرطی شناسایی شده در الگوی پژوهش می‌باشد. به‌عبارت دیگر، چارچوب نظری ترکیبی این پژوهش، نه تنها با یافته‌ها همخوانی دارد، بلکه توانسته است تعامل پیچیده میان ابعاد فنی، نهادی، اجتماعی و دیپلماتیک را به‌خوبی تبیین کند.

مقایسه با پیشینه پژوهش نشان می‌دهد که یافته‌های این پژوهش با جهت‌گیری کلی پژوهش‌های پیشین که عمدتاً بر ضرورت مدیریت منسجم و تقویت همکاری‌های بین‌المللی تأکید داشته‌اند، همسو است؛ اما، در عین حال تمایز آشکاری با آن‌ها دارد. پژوهش‌های داخلی پیشین (همچون پاسبان، ۱٤۰۲؛ ندری و همکاران، ۱۳۹۷؛ پالیزداران، ۱۳۹٤؛ قدسی، ۱۳۹۲) عمدتاً به شناسایی تهدیدات و آسیب‌شناسی فضای مجازی پرداخته و رویکردی غالباً سلبی و انفعالی داشته‌اند، در حالی‌که یافته‌های این پژوهش نشان می‌دهد که راهبردهای تدافعیِ مبتنی بر اصلاحات داخلی، پیش‌نیاز هرگونه اقدام تهاجمی یا

توسعه‌ای در عرصه بین‌المللی هستند. همچنین در مقایسه با پژوهش‌های خارجی (همچون فیشرکلر و همکاران، ۲۰۲۲؛ جانسون و وایت، ۲۰۲٤؛ نس و خینواسارا، ۲۰۲٤؛ مایورر، ۲۰۲۰؛ بیولا و هولمز، ۲۰۱۵) که اغلب در بستر جوامع آزاد و بدون تحریم شکل گرفته‌اند، این پژوهش با تأکید بر واقعیت‌های خاص ایران (تحریم، ساختار قدرت متمرکز و الزامات فرهنگی- مذهبی)، الگویی بومی ارائه می‌دهد که ضمن بهره‌گیری از تجارب جهانی، برای شرایط خاص کشور قابلیت پیاده‌سازی دارد. همچنین در حالی‌که بیشتر پژوهش‌های پیشین به‌طور مجزا به ابعاد امنیتی یا دیپلماتیک فضای مجازی پرداخته‌اند؛ این پژوهش با شناسایی سه الگوی روابط متقابل (تقابلی، هم‌افزا و شرطی)، برای نخستین بار تعامل پویا میان این دو حوزه را به‌صورت نظام‌مند تبیین کرده است.

تمایز اصلی این پژوهش نسبت به مطالعات پیشین در سه محور است: ارائه الگویی یکپارچه و بومی با قابلیت پیاده‌سازی در شرایط خاص ایران؛ اولویت‌بندی کمی راهبردها بر اساس نظر خبرگان و کاربران که از برخورد سلیقه‌ای با سیاست‌گذاری جلوگیری می‌کند؛ و شناسایی سه الگوی روابط متقابل (تقابلی، هم‌افزا و شرطی) میان امنیت ملی و روابط بین‌الملل که نشان می‌دهد برخلاف نگاه رایج، این دو حوزه نه‌تنها در تعارض نیستند، بلکه با اصلاحات هوشمندانه می‌توانند به‌عنوان نیروهای هم‌افزا عمل کنند. در مجموع، مدیریت راهبردی فضای مجازی در ایران در گرو عبور از پارادایم صرفاً امنیتی- محدودکننده به‌سوی حکمرانی هوشمند، مشارکتی و مبتنی بر اعتماد است؛ گذاری که با اصلاحات ساختاری، بازسازی سرمایه اجتماعی و دیپلماسی فعال، به پایداری امنیت ملی، کاهش آسیب‌پذیری، بهبود تصویر بین‌المللی و ارتقای جایگاه ایران در نظام حکمرانی جهانی اینترنت می‌انجامد.

پیشنهادهای کاربردی

- ✓ تدوین و تصویب قانون جامع فضای مجازی با مشارکت همه ذی‌نفعان و ایجاد نهاد رگولاتور مستقل، مقتدر و فرابخشی،
- ✓ بازنگری اساسی در رویکرد فیلترینگ و جایگزینی با برچسب‌گذاری هوشمند محتوا و ایجاد سازوکار جبران خسارت کسب‌وکارهای دیجیتال،
- ✓ راه‌اندازی سامانه ملی هشدار سریع و سیستم دفاع هوشمند مبتنی بر هوش مصنوعی،
- ✓ ایجاد شبکه سفیران مجازی و اتاق جنگ روایت دیجیتال در وزارت امور خارجه،
- ✓ تشکیل ائتلاف سایبری با کشورهای همسو (روسیه، چین، هند، پاکستان)،
- ✓ سرمایه‌گذاری راهبردی روی مدل‌های زبانی فارسی و توسعه پلتفرم‌های بومی رقابتی،
- ✓ ارتقای نظام‌مند سواد رسانه‌ای و تفکر انتقادی از مقطع مدرسه و ایجاد سامانه راستی‌آزمایی سریع.

پیشنهادهای پژوهشی

- ✓ بررسی تأثیر محاسبات کوانتومی بر امنیت سایبری و توسعه الگوریتم‌های مقاوم کوانتومی،
- ✓ مطالعه نقش اینترنت اشیاء و متاورس در بازتعریف امنیت ملی و حریم خصوصی،
- ✓ طراحی الگوی حکمرانی هوش مصنوعی مولد با رویکرد بومی و مبتنی بر ارزش‌های اسلامی- ایرانی،
- ✓ بررسی پیامدهای زیست‌محیطی حکمرانی فضای مجازی و ارائه چارچوب حکمرانی پایدار و سبز.

منابع

- پاسبان، ابوالفضل. (۱٤۰۲). حاکمیت حقوقی دولت‌ها بر فضای مجازی و تأثیرآن بر امنیت ملی. سیاست دفاعی، ۳۲(۱۲۵)، ۱۱-٤۸.
- پالیزبان، محسن. (۱۳۹٤). بررسی رابطه اینترنت و امنیت ملی جمهوری اسلامی ایران. سیاست- مجله دانشکده حقوق و علوم سیاسی، ٤۵(۳)، ٦۳۵-٦۵٤.
- حاجی احمدی، مهدی و ملکیان، نازنین. (۱٤۰۳). واکاوی نقش دیپلماسی رسانه‌ای در قدرت داخلی و روابط بین‌المللی کشورهای درحال‌توسعه. فصلنامه سیاست خارجی، ۳۸(۳)، ۱٦٦-۱۲۷.
- حاجی احمدی، مهدی و ملکیان، نازنین (۱٤۰۳). مطالعه پدیدارشناسانه تأثیر شبکه‌های اجتماعی بر احساس امنیت اجتماعی (مطالعه موردی: متولدین دهه ۷۰). فصلنامه مطالعات فرهنگ- ارتباطات، مهر ۱٤۰۳.
- روحانی، ابوالفضل و روحانی، مهدی. (۱٤۰۲). نقش فضای مجازی در حکمرانی ملی جمهوری اسلامی ایران. مطالعات بین رشته‌ای دانش راهبردی، ۱۳(۵۳)، ۸٤-٦۱.
- رستگارخالد، امیر و محمدیان، فاطمه. (۱۳۹۲). استفاده از اینترنت و احساس امنیت اجتماعی. مطالعات فرهنگ- ارتباطات، ۱٤ (۲۲)، ۸۹-۵۳.
- قدسی، امیر. (۱۳۹۲). تأثیر فضای مجازی بر امنیت ملی جمهوری اسلامی ایران و ارائه راهبرد (با تأکید بر ایفای نقش سرمایه اجتماعی). راهبرد دفاعی، ۱۱(٤٤)، ۱٤۹-۱۸٦.
- مهربانی‌فر، حسین. (۱٤۰۳). واکاوی نسبت رسانه‌های محلی و حکمرانی مردمی در سیاست‌های رسانه‌ای فرادستی نظام جمهوری اسلامی ایران. مطالعات میان‌رشته‌ای تمدنی انقلاب اسلامی، ۲(۷)، ۱۳۵-۱٦۱.
- ندری، غلامرضا؛ بخشایشی، احمد؛ دارابی، علی و مقصودی، مجتبی. (۱۳۹۸). بررسی نقش سیاسی- امنیتی شبکه‌های اجتماعی مجازی بر امنیت ملی جمهوری اسلامی ایران. فصلنامه پژوهش‌های حفاظتی امنیتی، ۸(۲۹)، ٦۳-۸۸

- Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1-25.
- Alexander, C. A., & Wang, L. (2025). Cyber risk management: Theories, frameworks, models, and practices. Computer and Telecommunication Engineering.
- Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2021). Information security as a national security component. Information Security Journal: A Global Perspective, 30(1), 1-18.
- Alkan, M. (2012). Siber Güvenlik ve Siber Savaşlar: Bilgi Güvenliği Derneği TBMM İnternet Komisyonu Sunumu.
- Baele, S. J., Bukhari, I., Whyte, C., Cuomo, S., Jensen, B., Payne, K., & Garcia, E. V. (2024). AI IR: Charting International Relations in the Age of Artificial Intelligence. International Studies Review, 26(2), Viae ۰۱۳.
- Betz, D. J. (2017). Cyberspace and the State: Towards a Strategy for Cyber-power. Routledge.
- Bjola, C., & Holmes, M. (2015). Digital diplomacy. New York: Taylor & Francis.
- Dobák, I. (۲۰۲۱). Thoughts on the evolution of national security in cyberspace. Security and Defence Quarterly, ۳۳(۱), ۸۵-۷۵.

- Dobrovolska, O., & Rozhkova, M. (2024). Development of the Country's Sustainable Cyberspace Strategy to Ensure the Country's National Security. SocioEconomic Challenges, ۸(۲), ۱۹۷-۲۱٤.
- Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). Cyber persistence theory: Redefining national security in cyberspace. Oxford University Press.
- Gerbner, G., & Gross, L. (1972). Living with television: The violence profile. Journal of Communication, 26(2), 173-199.
- Horkheimer, M., & Adorno, T. W. (1947). Dialectic of enlightenment (J. Cumming, Trans.). New York: Herder and Herder. (Original work published 1947).
- Huntington, S. P. (1993). The third wave: Democratization in the late twentieth century. University of Oklahoma Press.
- Johnson, R., & White, M. (2024). The Impact of Social Media on Global Security: A New Perspective. International Security Review, 28(1), -۸۹-۱۱۲.
- Kello, L., & Arquilla, J. (2023). Cyber threats and nuclear weapons: New dynamics in international security. Survival, 65(3), 45–68.
- Lehto, M. (2022). Cyber-attacks against critical infrastructure. In M. Lehto & P. Neittaanmäki (Eds.), Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.
- Maurer, T. (2020). Cyberspace and International Relations: Rising Powers, Proxies, and Norms (Doctoral dissertation).
- McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. Public Opinion Quarterly, 36(2), 176-187.
- Morgan S. (2024). Cybersecurity Facts, Figures, Predictions and Statistics Sponsored by eSentire.
- Nabi, R. L., & Riddle, K. (2008). The cultivation of social perceptions: A meta-analysis of long-term exposure to television. Human Communication Research, 34(3), 411-437.
- Ness, S., & Khinvasara, T. (۲۰۲٤). Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector. Journal of Engineering Research and Reports, 26(2), 107-۱۱۷.
- Noelle-Neumann, E. (1974). The spiral of silence: A theory of public opinion. Journal of Communication, 24(2), 43-51.
- Patel, K., & Chudasama, D. (2021). National security threats in cyberspace. National Journal of Cyber Security Law, 4(1), 12-۲۰.
- Ruël, H., & Bondarouk, T. (2014). E-HRM usage: A multi-level model of the influence of technology and organizational factors. In F. J. Martínez-López (Ed.), Handbook of strategic e-business management (pp. 621–643). Berlin, Heidelberg: Springer.
- Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.
- United Nations Office on Drugs and Crime (UNODC). (2023). World drug report 2023: Cybercrime and cryptocurrency. Vienna: United Nations.
- Wendt, A. (1999). Social theory of international politics. Cambridge: Cambridge University Press.