Strategic Studies of International Politics
https://jpir.journals.umz.ac.ir/ E-ISSN: 2717-0551
Vol. 9, No. 2, Issue. 18, Summer 2026 *** Received: 2026/04/01 Accepted: 2026/06/06
Research paper

National Security Developments in Iran with an Emphasis on International Relations and the Expansion of Cyberspace*

Mahdi Haji Ahmadi
Ph.D. Student in Communication Sciences, Islamic Azad University, Central Tehran Branch, Tehran, Iran.
Email: Mahdi.Hajiahmadi1282@iau.ac.ir 0000-0003-3418-0540
Nazanin Malekian
Associate Professor of Communication Sciences, Islamic Azad University, Central Tehran Branch, Tehran, Iran. (Corresponding Author)
Email: N.Malekiyan@iauctb.ac.ir 0000-0001-7957-2674

Abstract

The development of cyberspace and international relations has become pivotal in transforming national security dynamics, particularly in developing countries such as Iran. Cyberspace creates opportunities for cyber diplomacy and strengthening national identity while simultaneously generating challenges, including cyberattacks and misinformation. This study employs an exploratory mixed-methods approach to examine their impacts on Iran's national security and propose strategies for leveraging opportunities and mitigating threats. In the qualitative phase, data were collected through semi-structured interviews and focus group discussions and analyzed using thematic analysis. In the quantitative phase, strategies were prioritized using the Quantitative Strategic Planning Matrix (QSPM). Findings identified three primary themes: (1) cyber diplomacy and international relations, offering opportunities to promote the national narrative but constrained by coordination deficiencies; (2) cybersecurity and emerging threats, emphasizing indigenous technologies to counter attacks on critical infrastructure; and (3) social and identity-related impacts, highlighting cyberspace's dual role in fostering national cohesion. The QSPM identified developing cyber diplomacy, strengthening infrastructure, and formulating comprehensive regulations as top priorities. Recommendations include establishing a digital diplomacy unit, investing in indigenous technologies, and promoting media literacy education to enhance Iran's national security in the digital era, and strengthening institutional coordination and resilience against evolving digital security challenges.

Keywords: National Security, Cyber Security, Sustainibility, International Relations, Cyberspace.

* This article is derived from a doctoral Thesis focused on the " The Strategic Pattern of Cyberspace Management in Iran with an Emphasis on Sustaining National Security and International Relations" The research is being conducted under the supervision of Dr. Nazanin Malakian by Mahdi Haj Ahmad at the Communications Sciences Department of the Central Tehran Branch of Azad University.

Extended Abstract

Introduction: The rapid expansion of cyberspace has transformed the nature of national security and international relations, particularly in developing countries such as Iran. Cyberspace creates opportunities for cyber diplomacy, international communication, promoting national narratives, and strengthening national identity, while also generating challenges such as cyberattacks, misinformation, threats to critical infrastructure, and technological dependency. These developments demonstrate that national security can no longer be understood solely through traditional military and territorial threats. In Iran, the growing interaction between cyberspace and international relations therefore requires strategic approaches that can capitalize on digital opportunities while reducing emerging vulnerabilities. Accordingly, this study examines the interconnected relationship between cyberspace, international relations, and national security in Iran and identifies strategies for managing the opportunities and threats associated with the digital environment.

Research Question: The study asks: How can cyberspace be effectively employed to strengthen Iran's international relations and national security, and how can cyber, social, and political threats arising from cyberspace be managed within Iran's national security framework? More specifically, it examines how digital diplomacy can strengthen Iran's international position, how cyberattacks and technological dependency affect national security and critical infrastructure, and how cyberspace influences national identity and social cohesion.

Research Hypothesis: The study proceeds from the proposition, implicit in its research objectives, that the expansion of cyberspace has a dual and interconnected effect on Iran's national security: it can strengthen international relations, cyber diplomacy, and national identity when strategically managed, but it can simultaneously increase vulnerability through cyberattacks, misinformation, technological dependency, and social polarization. Accordingly, an integrated and coordinated policy framework is expected to improve the balance between these opportunities and threats.

Methodology and Theoretical Framework: An exploratory mixed-methods design was employed, consisting of a qualitative phase followed by a quantitative phase. In the qualitative stage, data were collected through semi-structured interviews with 30 senior managers, policymakers, academics, and cybersecurity and digital-diplomacy experts, together with four focus group discussions involving 6–8 participants per session. Participants were selected through purposive snowball sampling until theoretical saturation was achieved. The data were analyzed in MAXQDA through open, axial, and selective coding. Triangulation, member checking, and three Delphi rounds were used to validate and refine the themes. A seven-point Likert scale was employed in the Delphi process, and high expert agreement was confirmed by Kendall's $W = 0.85$ ($p < 0.01$); intercoder reliability exceeded 0.80. In the quantitative phase, qualitative findings were organized through SWOT analysis and translated into IFE and EFE matrices. The Quantitative Strategic Planning Matrix (QSPM) was then used to prioritize strategic alternatives according to weighted attractiveness scores (STAS). The theoretical framework integrates the concept of national security with cyberspace studies and three major international-relations perspectives: realism, liberalism, and constructivism. It is further informed by Castells's network society, Harvey's space-time compression, and media diplomacy. Realism explains cyber competition and deterrence; liberalism highlights technological cooperation and multilateral governance; constructivism addresses

identity, norms, and social meanings; while network society and space-time compression explain the structural and operational effects of digital connectivity.
Research Findings: Qualitative analysis produced more than 150 initial codes, 25 axial codes, and three principal themes. The first theme, cyber diplomacy and international relations, shows that platforms such as Twitter, Instagram, and Telegram can facilitate direct communication with global audiences, promote Iran's national narrative, support public diplomacy, reduce the costs of traditional diplomacy, and enable rapid responses to international crises. However, weak institutional coordination and restrictions on access to global platforms limit these benefits. The second theme, cybersecurity and emerging threats, identifies cyberattacks against critical infrastructure, technological dependency, shortages of specialized personnel, digital espionage, and phishing as major vulnerabilities. At the same time, artificial intelligence, big data, indigenous cybersecurity technologies, and security operations centers offer important defensive opportunities. The third theme, social and identity-related impacts, demonstrates cyberspace's dual influence on national cohesion. Digital campaigns can strengthen national and cultural identity and civic participation, whereas misinformation, anti-cultural content, weak media literacy, and social polarization can undermine trust and unity. Delphi validation confirmed strong agreement among experts regarding these themes. QSPM results ranked cyber diplomacy development first (STAS = 6.8), strengthening cybersecurity infrastructure and indigenous technologies second (STAS = 6.5), and comprehensive digital-content regulation and media literacy third (STAS = 6.2). International cooperation on cyber norms ranked fourth (5.9), while artificial intelligence for cyber-threat detection ranked fifth (5.7). Sensitivity analysis indicated that moderate changes in cyber-threat attractiveness scores did not alter the ranking.
Conclusion: The study concludes that cyberspace is neither inherently a security opportunity nor an exclusive source of threat; rather, its effects depend on governance, institutional coordination, technological capacity, and strategic integration with foreign policy. The findings demonstrate that cyber diplomacy can enhance Iran's international communication and narrative capacity, while indigenous cybersecurity capabilities can reduce vulnerabilities associated with attacks and technological dependence. Comprehensive regulation and media literacy are also necessary to address misinformation and social fragmentation. The study therefore recommends establishing a specialized digital-diplomacy unit within the Ministry of Foreign Affairs, strengthening cooperation with non-state actors, investing in indigenous cyber technologies and specialized training, establishing security operations centers for critical infrastructure, developing comprehensive digital-content regulations, expanding media-literacy programs, and participating in international cyber coalitions. Overall, the research argues for coherent, integrated cyberspace governance capable of converting digital opportunities into sustainable national-security capabilities while reducing cyber, social, and political vulnerabilities.
Keywords: National Security, Cyber Security, Sustainibility, International Relations, Cyberspace.

E-ISSN: 2717-0551 / University of Mazandaran / Quarterly of Strategic Studies of International Politics

10.22080/jpir.2026.30615.1505

فصلنامه علمی مطالعات راهبردی سیاست بین الملل
سال نهم، شماره دوم (پیاپی ۱۸)، تابستان ۱۴۰۵، صص. ۳۵-۶۰
تاریخ دریافت: ۱۴۰۵/۰۱/۱۲ ـ تاریخ پذیرش: ۱۴۰۵/۰۳/۱۶

مقاله پژوهشی

تحولات امنیت ملی در ایران با تأکید بر روابط بین‌الملل و توسعهٔ فضای مجازی*

مهدی حاجی‌احمدی
دانشجوی دکتری رشتهٔ علوم ارتباطات دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران.
Email: Mahdi.Hajiahmadi1282@iau.ac.ir 0000-0003-3418-0540
نازنین ملکیان
دانشیار علوم ارتباطات دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران. (نویسنده مسئول)
Email: N.Malekiyan@iauctb.ac.ir 0000-0001-7957-2674

چکیده

توسعهٔ فضای مجازی و روابط بین‌المللی به‌عنوان عوامل کلیدی در تحولات امنیت ملی، به‌ویژه در کشورهای درحال‌توسعه مانند ایران، اهمیتی روزافزون یافته‌اند. فضای مجازی ضمن ایجاد فرصت‌هایی برای دیپلماسی سایبری و تقویت هویت ملی، چالش‌هایی نظیر حملات سایبری و انتشار اطلاعات نادرست را به همراه دارد. این پژوهش با رویکرد آمیختهٔ اکتشافی به بررسی تأثیر این عوامل بر امنیت ملی ایران پرداخته و راهبردهایی برای بهره‌برداری از فرصت‌ها و مدیریت تهدیدات ارائه می‌دهد. در فاز کیفی، داده‌ها از طریق مصاحبه‌های نیمه ساختاریافته و بحث‌های گروهی متمرکز گردآوری و با روش تحلیل مضمون بررسی شدند. در فاز کمی، راهبردها با مدل QSPM اولویت‌بندی گردیدند. یافته‌ها سه مضمون اصلی را استخراج کرد: ۱) دیپلماسی سایبری و روابط بین‌المللی (با فرصت ترویج روایت ملی، اما محدودشده توسط ناهماهنگی‌ها)؛ ۲) امنیت سایبری و تهدیدات نوظهور (تأکید بر فناوری‌های بومی در برابر حملات به زیرساخت‌ها)؛ ۳) تأثیرات اجتماعی و هویتی (نقش دوگانه در انسجام ملی). مدل QSPM توسعهٔ دیپلماسی سایبری، تقویت زیرساخت‌ها و تدوین قوانین جامع را به‌عنوان اولویت‌ها شناسایی کرد. پیشنهادها شامل تأسیس واحد دیپلماسی دیجیتال، سرمایه‌گذاری در فناوری بومی و آموزش سواد رسانه‌ای است تا امنیت ملی ایران در عصر دیجیتال تقویت شود.

کلیدواژه‌ها: امنیت ملی، امنیت سایبری، پایداری، روابط بین‌الملل، فضای مجازی.

شاپای الکترونیک: ۰۵۵۱-۲۷۱۷/ دانشگاه مازندران/ فصلنامه علمی مطالعات راهبردی سیاست بین الملل

doi 10.22080/jpir.2026.30615.1505

* این مقاله مستخرج از رسالهٔ دکتری با عنوان؛ «الگوی راهبردی مدیریت فضای مجازی در ایران با تأکید بر پایداری امنیت ملی و روابط بین‌المللی» است که در گروه علوم ارتباطات دانشگاه آزاد واحد تهران مرکز به راهنمایی دکتر نازنین ملکیان و توسط مهدی حاجی‌احمدی در حال انجام است.

۱. مقدمه

فضای مجازی به‌عنوان محرکی نوظهور، با بازتعریف تعاملات جهانی و ایجاد فرصت‌های بی‌نظیر برای دیپلماسی، اقتصاد و ارتباطات بین‌المللی، به یکی از عوامل تعیین‌کننده در امنیت ملی ایران تبدیل شده است. این فضا، ضمن تأمین بستری برای تقویت جایگاه کشور در مناسبات بین‌المللی، با چالش‌هایی چون تهدیدات سایبری و پیچیدگی‌های ناشی از وابستگی فناوری مواجه است.

ظهور فناوری اطلاعات و ارتباطات و گسترش فضای مجازی، تحولی عمیق در ابعاد مختلف زندگی بشری ایجاد کرده و تأثیرات قابل‌توجهی بر حوزه‌های اقتصادی، سیاسی، اجتماعی و نظامی داشته است (تومی، ۱۳۸۴). فضای مجازی، به‌عنوان بستری بدون مرز، فرصت‌ها و چالش‌هایی بی‌سابقه برای امنیت ملی کشورها به وجود آورده است (Nye, 2023: 67). این فضا، شامل شبکه‌های اجتماعی، پلتفرم‌های دیجیتال، هوش مصنوعی و زیرساخت‌های سایبری، نقش محوری در بازتعریف روابط بین‌المللی ایفا می‌کند و ابزار قدرتمندی برای دیپلماسی سایبری، مدیریت بحران‌های بین‌المللی و تجارت الکترونیک فراهم کرده است (UNODC, 2020). بااین‌حال، تهدیداتی نظیر حملات سایبری و انتشار اطلاعات نادرست، چالش‌هایی جدی برای امنیت ملی ایجاد کرده‌اند (Kello & Arquilla, 2023: 45). در ایران، فضای مجازی به‌عنوان یکی از عوامل کلیدی در تحولات امنیت ملی شناخته شده و نقش برجسته‌ای در فرآیندهای تصمیم‌گیری دولتی ایفا می‌کند، اما هم‌زمان تهدیدات جدیدی مانند حملات سایبری و تشدید تنش‌های اجتماعی را به همراه داشته است (حاجی‌احمدی و همکاران، ۱۴۰۳: ۹۱). امنیت ملی که در گذشته عمدتاً بر حفاظت از تمامیت ارضی و دفاع نظامی متمرکز بود، در عصر دیجیتال مفهومی پیچیده‌تر یافته و شامل ابعاد غیرنظامی مانند امنیت سایبری و تأثیرات رسانه‌های اجتماعی شده است (قنبرلو، ۱۳۹۷: ۴۳).

روابط بین‌المللی ایران، تحت تأثیر تحریم‌ها، تنش‌های ژئوپلیتیکی و دیپلماسی منطقه‌ای، با چالش‌های ناشی از فضای مجازی گره خورده است (Chen et al., 2021: 68). همچنین، تحولات روابط بین‌المللی، به‌ویژه تحریم‌های یک‌جانبهٔ فناوری و تنش‌های ژئوپلیتیکی، فضای مجازی را به عرصه‌ای کلیدی برای جنگ ترکیبی تبدیل کرده است. این تحریم‌ها نه‌تنها دسترسی به فناوری‌های پیشرفتهٔ دفاعی و امنیتی را محدود کرده‌اند، بلکه با ایجاد بستری برای عملیات سایبری کم‌هزینه و هدفمند، انگیزهٔ بازیگران متخاصم را برای بهره‌برداری از آسیب‌پذیری‌های زیرساختی افزایش داده و به تشدید تهدیدات سایبری علیه امنیت ملی ایران منجر شده‌اند. این پیچیدگی،

پرسش‌هایی اساسی را مطرح می‌کند: چگونه فضای مجازی می‌تواند به‌طور مؤثر در تقویت روابط بین‌المللی و امنیت ملی ایران به کار گرفته شود؟ و چگونه می‌توان تهدیدات سایبری و چالش‌های اجتماعی - سیاسی ناشی از این فضا را مدیریت کرد؟

با وجود پیشرفت‌هایی مانند ابلاغ سند راهبردی جمهوری اسلامی ایران در فضای مجازی و تأکید بر توسعهٔ شبکهٔ ملی اطلاعات به‌عنوان بستری بومی و امن، همچنان شکاف‌هایی در هماهنگی سیاست‌های سایبری داخلی با دیپلماسی بین‌المللی وجود دارد. این تناقض، امنیت ملی را در برابر جنگ ترکیبی آسیب‌پذیر کرده و مسألهٔ اصلی پژوهش حاضر را برجسته می‌کند.

این پژوهش به دنبال بررسی تعامل بین توسعهٔ فضای مجازی و روابط بین‌المللی در شکل‌دهی به سیاست‌های امنیت ملی ایران و تحلیل چگونگی استفاده از فرصت‌های فضای مجازی برای تقویت دیپلماسی و همکاری‌های بین‌المللی و هم‌زمان شناسایی و مدیریت تهدیدات سایبری و اجتماعی آن بر امنیت ملی ایران است.

۲. پیشینهٔ پژوهش

مطالعات داخلی در حوزهٔ تعامل فضای مجازی و امنیت ملی عمدتاً بر نقش چندبعدی این فضا در حکمرانی و تهدیدات آن تمرکز کرده‌اند. حاجی‌احمدی و ملکیان (۱۴۰۳) و روحانی و همکاران (۱۴۰۲) بر هماهنگی رسانه‌ای با سیاست خارجی و تأثیرات سیاسی، اقتصادی، فرهنگی و امنیتی فضای مجازی بر حکمرانی ملی تأکید دارند و آن را عامل کلیدی در نظم اجتماعی می‌دانند. آقایی و همکاران (۱۴۰۲)، پاسبان (۱۴۰۲) و ندری و همکاران (۱۴۰۲) نیز نقش فضای مجازی در انقلاب‌های مدنی، ایجاد کنش‌های مثبت/منفی سیاسی - امنیتی و اثرات مخرب ناشی از فقدان قوانین بازدارنده را برجسته کرده‌اند. بااین‌حال، این مطالعات اغلب توصیفی بوده و کمتر به تعامل پویای فضای مجازی با روابط بین‌المللی در زمینهٔ امنیت ملی ایران پرداخته‌اند؛ همچنین، سیاست‌گذاری جزیره‌ای و رهاشدگی فضای مجازی را به‌عنوان آسیب اصلی شناسایی کرده‌اند، اما راهبردهای عملی جامعی ارائه نداده‌اند.

پژوهش‌های قدیمی‌تر داخلی مانند پالیزبان (۱۳۹۴) و قدسی (۱۳۹۲) نیز دوگانهٔ فرصت - تهدید فضای مجازی را مطرح کرده و بر الزامات امنیتی و فرصت‌های معرفی قابلیت‌های ملی تأکید دارند، اما به دلیل قدمت، تحولات اخیر سایبری و ژئوپلیتیکی (مانند تحریم‌های فناوری) را پوشش نداده‌اند.

در ادبیات خارجی، تمرکز بیشتر بر جنبه‌های جهانی تهدیدات و دیپلماسی سایبری است. جانسون و وایت[1] (۲۰۲۴)، نس و خینواسارا[2] (۲۰۲۴) و موانگی[3] (۲۰۲۴) نقش شبکه‌های اجتماعی در انتشار اطلاعات نادرست، چالش حفاظت از داده‌ها و کاهش اعتماد عمومی ناشی از حملات سایبری را بررسی کرده‌اند. فیشرکلر[4] و همکاران (۲۰۲۲)، دوباک[5] (۲۰۲۱) و پاتل و چاداساما[6] (۲۰۲۱) نیز بر تفاوت عملیات سایبری با درگیری‌های سنتی، لزوم تفکر استراتژیک بلندمدت و تهدیدات ساختاری فضای مجازی برای امنیت ملی تأکید دارند. بیولا و مانور[7] (۲۰۲۲) و مایورر[8] (۲۰۲۰) دیپلماسی دیجیتال را ابزاری برای مدیریت بحران و شکل‌دهی افکار عمومی می‌دانند؛ درحالی‌که فارل و نیومن[9] (۲۰۱۹) با نظریهٔ «وابستگی متقابل سلاح‌شده[10]» نشان می‌دهند چگونه شبکه‌های سایبری به ابزار اعمال قدرت در روابط بین‌الملل تبدیل شده‌اند. مطالعات اولیه‌تر مانند همپتون[11] و همکاران (۲۰۱۱) و کاپلان و هینلین[12] (۲۰۱۰) نیز بر پتانسیل شبکه‌های اجتماعی در تعاملات میان‌فرهنگی و پیشگیری از سوءاستفاده تأکید کرده‌اند.

با وجود غنای این مطالعات، انتقاد اصلی بر تمرکز یک‌جانبهٔ آن‌هاست: پژوهش‌های خارجی اغلب زمینه‌های بومی کشورهای درحال‌توسعه مانند ایران (تحریم‌ها، جنگ ترکیبی و دیپلماسی سایبری منطقه‌ای) را نادیده گرفته و بیشتر جنبه‌های فنی یا جهانی را بررسی کرده‌اند؛ همچنین، کمتر به تعامل هم‌زمان فضای مجازی، روابط بین‌المللی و امنیت ملی پرداخته‌اند و رویکردهای روش‌شناختی آن‌ها عمدتاً تک‌بعدی (توصیفی یا نظری) بوده است. نقطهٔ افتراق و نوآوری پژوهش حاضر در سه جنبهٔ کلیدی است:

1. Johnson & White
2. Ness & Khinvasara
3. Mwangi
4. Fischerkeller
5. Dobák
6. Patel & Chudasama
7. Bjola, C., & Manor, I.
8. Maurer, T.
9. Farrell, H., & Newman, A. L.
10. Weaponized Interdependence
11. Hampton
12. Kaplan & Haenlein

الف) تحلیل متعامل و هم‌زمان کارکردهای فضای مجازی، روابط بین‌المللی و امنیت ملی در زمینهٔ خاص ایران با تأکید بر تحولات اخیر (مانند سند راهبردی ۱۴۰۱ و تهدیدات جنگ ترکیبی)؛

ب) استفاده از رویکرد آمیختهٔ اکتشافی (کیفی - کمی) برای دستیابی به نتایجی جامع‌تر و عملی‌تر؛

ج) ارائهٔ اولویت‌بندی راهبردها با مدل QSPM که شکاف عدم ارائهٔ راهکارهای سیاستی عملی در مطالعات پیشین را پر می‌کند.

۳. مبانی نظری پژوهش

این پژوهش به بررسی تحولات امنیت ملی در ایران، با تمرکز بر نقش فضای مجازی و روابط بین‌الملل می‌پردازد. به همین منظور، یک چارچوب نظری یکپارچه بر اساس مفاهیم کلیدی امنیت ملی، فضای مجازی و سه مکتب اصلی روابط بین‌الملل (رئالیسم، لیبرالیسم، سازه‌انگاری)، به همراه نظریه‌های مرتبط ارائه می‌شود. این رویکرد چندبعدی به ما امکان می‌دهد تا فرصت‌ها و چالش‌های ناشی از فضای مجازی برای امنیت ملی ایران را در بستر روابط بین‌الملل تحلیل کنیم.

۳-۱. تعاریف و مفاهیم اساسی

امنیت ملی: در گذشته، امنیت ملی عمدتاً به حفظ سرزمین، استقلال سیاسی، اقتصادی و فرهنگی و حفاظت از منافع ملی محدود می‌شد (Buzan et al., 1998: 76). بوزان (۱۹۹۱) آن را "حالتی از آرامش و اطمینان" در برابر تهدیدات داخلی و خارجی تعریف می‌کند (Buzan, 1991: 23). با ظهور فضای مجازی، این مفهوم گسترش یافته و ابعاد جدیدی نظیر امنیت سایبری، امنیت اطلاعاتی و امنیت فرهنگی را در بر می‌گیرد که فراتر از مرزهای فیزیکی عمل می‌کند.

فضای مجازی: فضای مجازی، محیطی تعاملی و غیرفیزیکی است که شامل شبکه‌های اجتماعی، وب‌سایت‌ها، ایمیل‌ها و سایر ابزارهای دیجیتالی می‌شود که افراد و سازمان‌ها در آن به‌صورت الکترونیکی با یکدیگر ارتباط برقرار می‌کنند (Denning, 2018: 52). کشتری (۲۰۱۷)، اشاره می‌کند که این فضا هم می‌تواند به تقویت امنیت ملی کمک و هم به‌عنوان منبع تهدید عمل کند (Kshetri, 2017: 225).

فضای مجازی فرصت‌های فراوانی برای امنیت ملی ایجاد کرده است. ازجملهٔ این فرصت‌ها می‌توان به ارتقا و تسهیل ارتباطات، انتقال سریع اطلاعات و مدیریت بهتر منابع اشاره کرد (Gady, 2017: 12). فضای مجازی همچنین چالش‌های متعددی را

برای امنیت ملی ایجاد کرده است که اهم آن‌ها عبارت‌اند از: حملات سایبری، انتشار اطلاعات نادرست و اختلال در سیستم‌های حیاتی (Kaspersky Lab, 2014: 8).

۲-۳. پیوند نظریات روابط بین‌الملل با تحولات امنیت ملی و فضای مجازی

فلسفهٔ اثرگذاری فضای مجازی بر امنیت ملی را می‌توان از منظر سه مکتب اصلی روابط بین‌الملل تبیین کرد:

۱-۲-۳. رئالیسم

رئالیسم بر منازعه و رقابت میان دولت‌ها به‌عنوان کنشگران اصلی نظام بین‌الملل تأکید دارد و امنیت را دغدغهٔ نخست کشورها می‌داند (Korab-Karpowicz, 2018: 1). دولت‌ها برای دست‌یابی به امنیت، به دنبال کسب قدرت هستند و این امر منجر به رقابت دائمی می‌شود (Snyder, 2002: 155). امنیت در این دیدگاه شامل سه مؤلفهٔ تهدید نظامی، حفظ وضع موجود و حفظ محوریت دولت است (سازمند، ۱۳۹۵). از منظر رئالیستی، فضای مجازی یک عرصهٔ جدید برای رقابت قدرت‌ها و تهدیدات سایبری است. حملات سایبری دولتی نمونه‌ای از این رقابت در فضای دیجیتال است (Hala et al., 2025) که به افزایش تلاش‌ها برای بازدارندگی سایبری منجر می‌شود.

۲-۲-۳. لیبرالیسم

لیبرالیست‌ها علاوه بر قدرت نظامی، به ابعاد دیگر امنیت ملی نظیر امنیت اقتصادی نیز توجه دارند و نقش بازیگران غیردولتی مانند سازمان‌های بین‌المللی را مهم می‌دانند (Collins, 2010: 45). آن‌ها به همکاری، نهادهای بین‌المللی و راه‌حل‌های چندجانبه برای کاهش تهدیدات امنیتی معتقدند. فضای مجازی فرصت‌هایی برای همکاری فناورانه و توسعهٔ قوانین سایبری فراهم می‌کند. کاربرد هوش مصنوعی در شناسایی بلادرنگ تهدیدات (Yudhistira & Andrew, 2022) نمونه‌ای از این همکاری فناورانه است که می‌تواند دفاع سایبری را تقویت کند.

۳-۲-۳. سازه‌انگاری

سازه‌انگاری بر ساخت اجتماعی واقعیت، نقش هویت‌ها، هنجارها و فرهنگ در سیاست جهانی تأکید دارد (حاجی‌احمدی و ملکیان، ۱۴۰۳: ۱۳۸). هویت‌ها و منافع دولت‌ها توسط هنجارها و تعاملات اجتماعی شکل می‌گیرد (کلومبیس و ولف، ۱۳۷۵: ۵۱). تغییر در ادراکات و انتظارات می‌تواند به تغییر در روابط بین‌الملل و دست‌یابی به صلح منجر شود (Mearsheimer, 1994: 11). سازه‌انگاری به تأثیر فضای مجازی بر شکل‌گیری هویت ملی و ناسیونالیسم سایبری می‌پردازد. تلاش‌های ایران برای حفظ

گفتمان فرهنگی در فضای دیجیتال و مبارزه با اطلاعات نادرست، از این منظر قابل تحلیل است. فضای مجازی ابزاری برای بازتعریف هویت‌ها و هنجارها در سطح ملی و بین‌المللی است.

۳-۳. نظریه‌های تکمیلی فضای مجازی و تحولات روابط بین‌الملل

این بخش به نظریاتی می‌پردازد که مستقیماً به تأثیر فضای مجازی بر روابط بین‌الملل و به تبع آن امنیت ملی می‌پردازند:

۳-۳-۱. جامعهٔ اطلاعاتی و جامعهٔ شبکه‌ای

جامعهٔ اطلاعاتی بر محور توسعهٔ تکنولوژی‌های نوین اطلاعاتی و جریان اطلاعات سازمان‌دهی شده است (محسنی، ۱۳۸۰: ۹). کاستلز (۱۹۹۷) معتقد است که توسعهٔ شبکه‌های تکنولوژی اطلاعاتی، جامعهٔ شبکه‌ای را شکل داده که در آن تعاملات دیجیتال و فراتر از مرزهای جغرافیایی صورت می‌گیرد و اهمیت جریان‌های اطلاعاتی بر نقاط جغرافیایی غلبه می‌کند. این نظریه ساختار کلان و زیربنایی تحولات را تبیین می‌کند که چرا فضای مجازی قادر به ایفای نقش در روابط بین‌الملل و امنیت ملی است. این ساختار قدرت و تعاملات را از حالت سلسله‌مراتبی و جغرافیامحور به حالتی شبکه‌ای و مبتنی بر «جریان‌ها» تغییر داده است.

۳-۳-۲. فشرده‌سازی فضا و زمان

این تئوری را دیوید هاروی (۱۹۸۹) مطرح کرد و معتقد بود که توسعهٔ فناوری دیجیتال و حمل‌ونقل سریع، ساختار جدیدی از تعاملات اجتماعی و اقتصادی را شکل داده است. او تأکید کرد که فضای مجازی جهان را به یک «دهکدهٔ جهانی» تبدیل کرده و مرزهای جغرافیایی را کاهش داده است (Harvey, 1989). این فرآیند منجر به کاهش زمان و کوچک شدن فضا می‌شود (گل‌محمدی، ۱۳۸۶: ۴۶). این نظریه چگونگی بی‌اثر شدن مرزهای جغرافیایی و تسریع تعاملات اقتصادی، اجتماعی و سیاسی را توضیح می‌دهد. در بُعد امنیت ملی، این فشرده‌سازی، هم فرصت‌های جدیدی برای واکنش سریع به تهدیدات ایجاد می‌کند و هم چالش‌هایی را در نظارت و کنترل مرزهای سایبری به وجود می‌آورد.

۳-۳-۳. دیپلماسی رسانه‌ای

بر اساس گفتمان دیپلماسی رسانه‌ای، فضای مجازی و رسانه‌های نوین ابزاری برای دیپلماسی و حل تنش‌های بین‌المللی هستند و امکان ارتباط مستقیم دولت‌ها و مردم را فراهم می‌کنند. ابو (۱۹۹۶)، دیپلماسی رسانه‌ای را هرگونه استفاده از رسانه‌ها برای

ترویج سیاست خارجی توصیف می‌کند (Ebo, 1996: 44). به عبارتی، این دیپلماسی مجموعهٔ سازوکارهایی است که از طریق آن می‌توان سیاست‌ها را بر مردم، احزاب، سازمان‌های بین‌المللی و دیگر دولت‌ها اعمال نمود و به معنای به‌کارگیری رسانه‌ها برای تکمیل و ارتقاء سیاست خارجی است (Gilboa, 2002). پراساد (۲۰۰۲)، آن را نقشی می‌داند که رسانه‌ها در فعالیت‌های دیپلماتیک بازی می‌کنند (Prasad, 2002: 122) و تیلور (۱۹۹۷) آن را هنر ایجاد ارتباط، حل مناقشات و اقناع جوامع دیگر از طریق رسانه‌های جهانی می‌داند (Taylor, 1997: 83). فضای مجازی با فراهم‌کردن امکان تعامل بدون نیاز به حضور فیزیکی، نقشی مهم در این عرصه دارد. خود مفهوم دیپلماسی نیز از «علم مطالعهٔ اسناد» به «علم ادارهٔ روابط بین‌المللی» برای مدیریت اختلافات تکامل یافته است. رسانه‌ها به دلیل سرعت و پوشش گسترده، گزارش‌های مربوط به رویدادهای مهم را شکل می‌دهند (Zhang, 2010: 236) که این موضوع به چالشی برای نهادهای دیپلماسی تبدیل شده است.

۳-۴. جمع‌بندی مبانی نظری و پیوند نظریات

نظریه‌های ارائه‌شده در این پژوهش به‌صورت یکپارچه و مکمل عمل می‌کنند تا چارچوبی تحلیلی جامع برای بررسی تحولات امنیت ملی ایران با تأکید بر روابط بین‌المللی و توسعهٔ فضای مجازی فراهم کنند. نظریهٔ جامعهٔ شبکه‌ای کاستلز (۱۹۹۷) بستر زیربنایی را تبیین می‌کند و توضیح می‌دهد که چرا ساختار شبکه‌ای فضای مجازی، تعاملات فراتر از مرزها را ممکن ساخته و آن را به عاملی کلیدی در امنیت ملی و روابط بین‌الملل تبدیل کرده است. نظریهٔ فشرده‌سازی فضا - زمان هاروی (۱۹۸۹) مکانیسم عملیاتی این تحولات را روشن می‌سازد؛ به‌گونه‌ای که بی‌اثر شدن مرزهای جغرافیایی، تسریع تهدیدات سایبری (مانند جنگ ترکیبی) و فرصت‌های واکنش سریع را در ابعاد امنیتی توضیح می‌دهد.

مکاتب اصلی روابط بین‌الملل نیز ابعاد مختلف این تعاملات را پوشش می‌دهند: رئالیسم رقابت قدرت‌ها و تهدیدات سایبری خارجی را در فضای مجازی برجسته و ضرورت بازدارندگی بومی را توجیه می‌کند؛ لیبرالیسم فرصت‌های همکاری فناورانه و چندجانبه (مانند حکمرانی مشترک سایبری) را تأکید دارد؛ و سازه‌انگاری نقش فضای مجازی در ساخت هویت ملی، ناسیونالیسم سایبری و مبارزه با اطلاعات نادرست را تحلیل می‌کند. گفتمان دیپلماسی رسانه‌ای (Gilboa, 2002; Zhang, 2010) نیز کاربرد عملی این تحولات را در سیاست خارجی نشان می‌دهد و بر استفاده استراتژیک از رسانه‌های دیجیتال برای ترویج روایت ملی و مدیریت بحران‌ها تمرکز دارد.

این چارچوب یکپارچه نه‌تنها پژوهش را از تحلیل توصیفی فراتر می‌برد، بلکه امکان تفسیر یافته‌های تجربی را نیز فراهم می‌کند: مضمون دیپلماسی سایبری عمدتاً با لیبرالیسم و دیپلماسی رسانه‌ای همخوانی دارد؛ مضمون امنیت سایبری و تهدیدات نوظهور از منظر رئالیسم و جامعهٔ شبکه‌ای قابل تبیین است و مضمون تأثیرات اجتماعی - هویتی ریشه در سازه‌انگاری و فشرده‌سازی فضا - زمان دارد.

۴. روش‌شناسی پژوهش

پژوهش حاضر از رویکرد آمیخته اکتشافی (کیفی سپس کمی) بهره گرفته است تا ابتدا ابعاد پدیده را شناسایی و سپس راهبردها را اولویت‌بندی کند. این رویکرد امکان ترکیب عمق داده‌های کیفی با دقت کمی را فراهم می‌کند و اعتبار یافته‌ها را افزایش می‌دهد.

در مرحلهٔ کیفی، هدف شناسایی کارکردها، چالش‌ها و راهبردهای اولیه مدیریت فضای مجازی در چارچوب امنیت ملی و روابط بین‌المللی بود. جامعهٔ آماری شامل مدیران ارشد، سیاست‌گذاران، صاحب‌نظران دانشگاهی و کارشناسان حوزهٔ امنیت سایبری و دیپلماسی دیجیتال (از نهادهایی مانند مرکز ملی فضای مجازی، وزارت امور خارجه و دانشگاه‌ها) بود. نمونه‌گیری به روش هدفمند گلوله‌برفی انجام شد و تا رسیدن به اشباع نظری ادامه یافت که درنهایت به حجم نمونهٔ ۳۰ نفر برای مصاحبه‌های نیمه ساختاریافته و ۴ جلسه بحث گروهی متمرکز (هر جلسه ۶-۸ نفر)، منجر شد.

داده‌ها با استفاده از نرم‌افزار MAXQDA تحلیل مضمون[1] شدند. فرآیند کدگذاری شامل سه مرحلهٔ کدگذاری باز، محوری و انتخابی بود و برای افزایش اعتبار، از روش مثلث‌سازی (ترکیب مصاحبه و FGD) و بررسی توسط اعضا[2] استفاده و سپس برای تأیید و پالایش مضامین، از تکنیک دلفی در سه راند بهره گرفته شد. پرسش‌نامه لیکرت ۷ درجه‌ای (۱=کاملاً بی‌اهمیت تا ۷=کاملاً مهم) برای کارشناسان توزیع گردید. در راند سوم، اجماع نهایی حاصل شد و ضریب هماهنگی کندال ($p < ۰.۸۵$, ۰/۰۱=) توافق بالای کارشناسان را تأیید کرد. پایایی کدگذاری نیز با توافق بین‌کدگذارها[3] بیش از ۰/۸ محاسبه شد.

در مرحلهٔ کمی، راهبردهای استخراج‌شده از فاز کیفی با مدل ماتریس برنامه‌ریزی استراتژیک کمی (QSPM) اولویت‌بندی شدند. ابتدا عوامل کلیدی داخلی و خارجی از

1. Thematic Analysis
2. Member Checking
3. Inter-Coder Reliability

ماتریس SWOT (تدوین‌شده بر پایهٔ یافته‌های کیفی) به ماتریس‌های IFE و EFE تبدیل گردیدند. وزن عوامل توسط کارشناسان تعیین و امتیاز جذابیت (AS) راهبردها نسبت به هر عامل تخصیص یافت. امتیاز کل جذابیت (STAS) محاسبه و اولویت‌ها استخراج شدند.

جدول ۱. اطلاعات مصاحبه‌شوندگان

ردیف	کدمصاحبه شونده	تحصیلات	سن	جنسیت	حوزه فعالیت
۱	P1	دکتری	۶۷	مرد	استاد دانشگاه
۲	P2	دکتری	۴۴	زن	استاد دانشگاه
۳	P3	کارشناسی ارشد	۳۴	زن	معاون مدیر کل - امور خارجه
۴	P4	کارشناسی ارشد	۵۶	مرد	کارشناس - شورای عالی فضای مجازی
۵	P5	دکتری	۳۴	مرد	استاد دانشگاه
۶	P6	دکتری	۵۶	مرد	استاد دانشگاه
۷	P7	دکتری	۳۵	مرد	استاد دانشگاه
۸	P8	دکتری	۵۰	زن	استاد دانشگاه
۹	P9	دکتری	۶۲	مرد	استاد دانشگاه
۱۰	P10	کارشناسی ارشد	۴۰	زن	معاون - سازمان فاوا
۱۱	P11	دکتری	۶۷	مرد	مدیر - مرکز ملی فضای مجازی
۱۲	P12	دکتری	۴۴	مرد	کارشناس - وزارت اطلاعات
۱۳	P13	کارشناسی ارشد	۳۴	مرد	مدیرکل - وزارت فرهنگ
۱۴	P14	کارشناسی ارشد	۵۶	مرد	مشاور - وزارت فرهنگ
۱۵	P15	کارشناسی ارشد	۳۴	زن	کارشناس - - وزارت کشور
۱۶	P16	دکتری	۵۶	زن	مدیر مرکز پژوهشی - نیروی انتظامی
۱۷	P17	کارشناسی ارشد	۳۵	زن	کارشناس امنیتی - وزارت دفاع
۱۸	P18	دکتری	۵۰	مرد	کارشناس - وزارت اطلاعات
۱۹	P19	دکتری	۶۲	مرد	مدیرکل - وزارت کشور
۲۰	P20	کارشناسی ارشد	۴۰	مرد	کارشناس - وزارت دفاع
۲۱	P21	کارشناسی ارشد	۳۹	مرد	مدیرکل - وزارت ارتباطات
۲۲	P22	کارشناسی ارشد	۳۳	زن	معاون مدیرکل - وزارت ارتباطات
۲۳	P23	دکتری	۶۷	مرد	کارشناس اجتماعی - وزارت کشور
۲۴	P24	دکتری	۳۹	مرد	معاون مدیر - وزارت کشور

۲۵	P25	دکتری	۴۷	زن	کارشناس - وزارت کشور
۲۶	P26	کارشناسی ارشد	۵۱	مرد	مشاور - وزارت کشور
۲۷	P27	دکتری	۴۵	مرد	کارشناس - صداوسیما
۲۸	P28	کارشناسی ارشد	۳۹	زن	مدیر - صداوسیما
۲۹	P29	کارشناسی ارشد	۵۶	مرد	مدیر - صداوسیما
۳۰	P30	کارشناسی ارشد	۵۵	مرد	مشاور - وزارت ارتباطات

مأخذ: یافته‌های پژوهش، ۱۴۰۳

پژوهش حاضر، همچون بسیاری از مطالعات کیفی - کمی در حوزه‌های حساس امنیتی، با محدودیت‌هایی مواجه بوده است. نمونه‌گیری در مرحلهٔ کیفی عمدتاً هدفمند و مبتنی بر دسترسی به کارشناسان بود که ممکن است تعمیم‌پذیری یافته‌ها را محدود کند. حساسیت موضوع امنیت ملی و فضای مجازی نیز موجب شد برخی مشارکت‌کنندگان از ارائهٔ دیدگاه‌های صریح یا جزئی اجتناب ورزند که می‌تواند بر عمق داده‌ها تأثیر گذاشته باشد. در مرحلهٔ کمی، وابستگی مدل QSPM به قضاوت کارشناسان، نتایج را تا حدی ذهنی می‌نماید و با تغییر ترکیب کارشناسان ممکن است متفاوت شود. همچنین، عدم دسترسی به داده‌های رسمی طبقه‌بندی‌شده در حوزهٔ تهدیدات سایبری، تحلیل را به منابع غیرمحرمانه محدود کرد.

۵. تجزیه‌وتحلیل و یافته‌های پژوهش

یافته‌های این پژوهش از طریق رویکرد آمیخته اکتشافی (کیفی - کمی) به دست آمده و در دو فاز کیفی و کمی ارائه می‌شوند. این یافته‌ها بر اساس تحلیل داده‌های مصاحبه‌های نیمه‌ساختاریافته با ۳۰ نفر از مدیران، سیاست‌گذاران، صاحب‌نظران و کنشگران مدنی (جدول ۱)، جلسات بحث گروهی متمرکز (FGD) و تحلیل کمی با استفاده از مدل QSPM استخراج شده‌اند. هدف این بخش، ارائهٔ نتایج حاصل از بررسی تأثیر توسعهٔ فضای مجازی و روابط بین‌المللی بر تحولات امنیت ملی ایران است. در فاز کیفی، تمرکز بر شناسایی الگوها و مضامین اصلی بود؛ درحالی‌که فاز کمی بر اولویت‌بندی راهبردها تأکید داشت. نتایج نشان‌دهندهٔ نقش دوگانهٔ فضای مجازی به‌عنوان فرصت و تهدید در امنیت ملی ایران هستند.

۵-۱. فاز کیفی: شناسایی مضامین کلیدی

در فاز کیفی، داده‌های خام از مصاحبه‌های نیمه ساختاریافته و چهار جلسه بحث گروهی متمرکز (هر جلسه با ۸-۶ شرکت‌کننده) جمع‌آوری شدند. این داده‌ها با

استفاده از نرم‌افزار MAXQDA تحلیل شدند و از روش کدگذاری برای استخراج مضامین استفاده شد.

در کدگذاری اولیه، بیش از ۱۵۰ کد اولیه شناسایی شد و سپس به ۲۵ کد محوری و درنهایت به سه مضمون اصلی تقلیل یافتند. این مضامین بر اساس اهمیت و ارتباط با اهداف پژوهش انتخاب شدند. برای افزایش اعتبار، از روش مثلث‌سازی (ترکیب داده‌های مصاحبه، بحث گروهی و بازخورد شرکت‌کنندگان) استفاده شد.

جدول ۲. مضامین و کدهای محوری به‌دست‌آمده

مضمون اصلی	کدهای محوری
دیپلماسی سایبری و روابط بین‌المللی	۱- استفاده از شبکه‌های اجتماعی برای دیپلماسی عمومی ۲- ترویج روایت ملی در فضای مجازی ۳- مقابله با تبلیغات منفی بین‌المللی ۴- مدیریت بحران‌های جهانی از طریق فضای مجازی ۵- همکاری با بازیگران غیردولتی در دیپلماسی سایبری ۶- هماهنگی ضعیف نهادهای داخلی در دیپلماسی سایبری ۷- تأثیر فیلترینگ بر دیپلماسی سایبری ۸- کاهش هزینه‌های دیپلماسی سنتی با فضای مجازی ۹- استفاده از توییتر برای اطلاع‌رسانی بحران ۱۰- نقش اینستاگرام در دیپلماسی عمومی ۱۱- تأثیر کمپین‌های دیجیتال بر روابط منطقه‌ای
امنیت سایبری و تهدیدات نوظهور	۱- حملات سایبری به زیرساخت‌های حیاتی ۲- استفاده از هوش مصنوعی در دفاع سایبری ۳-وابستگی به فناوری‌های خارجی ۴- کمبود نیروی متخصص سایبری ۵- توسعهٔ فناوری‌های بومی سایبری ۶- تأثیر حملات سایبری بر اعتماد عمومی ۷- نقش داده‌های بزرگ در امنیت سایبری ۸- جاسوسی دیجیتال و تهدیدات امنیتی ۹- توسعهٔ مراکز عملیات امنیت ۱۰-ضرورت آموزش متخصصان سایبری ۱۱- آسیب‌پذیری زیرساخت‌های حیاتی در برابر حملات سایبری
تأثیرات اجتماعی و هویتی	۱- انتشار اطلاعات نادرست در شبکه‌های اجتماعی ۲- تقویت هویت ملی از طریق فضای مجازی ۳- تأثیر شبکه‌های اجتماعی بر انسجام اجتماعی ۴- نقش فضای مجازی در اعتراضات اجتماعی ۵- ضعف در سواد رسانه‌ای عمومی ۶- تأثیر محتوای ضدفرهنگی بر امنیت اجتماعی ۷- نقش کمپین‌های فرهنگی در فضای مجازی ۸- تأثیر شبکه‌های اجتماعی بر مشارکت مدنی ۹- ضرورت تنظیم قوانین محتوای دیجیتال ۱۰- تأثیر فضای مجازی بر وحدت ملی

مأخذ: یافته‌های پژوهش، ۱۴۰۳

در ادامه، هر مضمون با جزئیات بیشتر، همراه با نقل‌قول‌های نمونه از مصاحبه‌شوندگان، توصیف و تحلیل می‌شود:

۱-۱-۵. مضمون اول: دیپلماسی سایبری و روابط بین‌المللی

این مضمون بر نقش فضای مجازی به‌عنوان ابزاری برای تقویت دیپلماسی عمومی، رسانه‌ای و بین‌المللی تمرکز دارد. مصاحبه‌شوندگان تأکید کردند که پلتفرم‌های

دیجیتال مانند توییتر، اینستاگرام و تلگرام، امکان ارتباط مستقیم با افکار عمومی جهانی را فراهم کرده‌اند و به ایران کمک می‌کنند تا روایت‌های رسمی خود را در برابر تبلیغات منفی رسانه‌های غربی ترویج دهد.

فرصت‌های شناسایی‌شده: افزایش تعاملات دیپلماتیک از طریق کمپین‌های رسانه‌ای آنلاین، مانند اطلاع‌رسانی دربارهٔ دستاوردهای علمی ایران در مجامع بین‌المللی. شرکت‌کنندگان اشاره کردند که این ابزارها هزینهٔ دیپلماسی سنتی را کاهش می‌دهند و امکان واکنش سریع به بحران‌های جهانی را فراهم می‌کنند.

چالش‌ها: نبود استراتژی یکپارچه و هماهنگی ضعیف بین وزارتخانه‌ها و نهادها منجر به ناهماهنگی در پیام‌رسانی شده است. همچنین، محدودیت‌های دسترسی به پلتفرم‌های جهانی (مانند فیلترینگ) به‌عنوان مانع اصلی ذکر شد.

زیرمضامین: شامل "ترویج روایت ملی" (با ۱۵ کد مرتبط)، "مدیریت بحران‌های بین‌المللی" (۱۰ کد) و "همکاری با بازیگران غیردولتی" (۷ کد) بود.

۲-۱-۵. مضمون دوم: امنیت سایبری و تهدیدات نوظهور

این مضمون به تهدیدات فنی و سایبری فضای مجازی می‌پردازد و نشان‌دهندهٔ افزایش وابستگی زیرساخت‌های ملی به فناوری دیجیتال است. مصاحبه‌شوندگان بر حملات سایبری به‌عنوان تهدید اصلی تأکید کردند که می‌تواند سیستم‌های حیاتی مانند شبکه‌های برق، نفت و ارتباطات را مختل کند.

فرصت‌های شناسایی‌شده: استفاده از هوش مصنوعی و داده‌های بزرگ برای پیش‌بینی و مقابله با تهدیدات.

چالش‌ها: کمبود نیروی متخصص و وابستگی به فناوری‌های خارجی به‌عنوان نقاط ضعف اصلی شناسایی شدند. علاوه بر این، افزایش حملات فیشینگ و جاسوسی دیجیتال از طریق اپلیکیشن‌های محبوب، به‌عنوان تهدید روزمره ذکر شد.

زیرمضامین: شامل "حملات دولتی و غیردولتی" (۱۷ کد)، "تقویت دفاع سایبری" (۱۲ کد) و "مدیریت ریسک فناوری" (۹ کد) بود.

۳-۱-۵. مضمون سوم: تأثیرات اجتماعی و هویتی

این مضمون بر جنبه‌های فرهنگی، اجتماعی و هویتی فضای مجازی تمرکز دارد و نشان‌دهندهٔ تأثیر دوگانهٔ آن بر انسجام ملی است. مصاحبه‌شوندگان اشاره کردند که شبکه‌های اجتماعی می‌توانند به تقویت هویت فرهنگی کمک کنند، اما اغلب به انتشار محتوای مخرب و کاهش اعتماد اجتماعی منجر می‌شوند.

فرصت‌های شناسایی‌شده: تقویت گفتمان ملی از طریق کمپین‌های فرهنگی آنلاین و افزایش مشارکت مدنی در مسائل ملی

چالش‌ها: انتشار اطلاعات نادرست، محتوای ضدفرهنگی و تشدید قطبی‌سازی اجتماعی. همچنین، ضعف در سواد رسانه‌ای عمومی (به‌ویژه در نسل جوان) به‌عنوان عامل تشدیدکننده ذکر شد.

زیرمضامین: شامل "شکل‌گیری هویت ملی" (۱۳ کد)، "انتشار اطلاعات نادرست" (۱۱ کد) و "انسجام اجتماعی" (۸ کد) بود.

درنهایت، مضامین استخراج‌شده از طریق روش دلفی در سه راند اعتبارسنجی شدند. در راند اول، پرسش‌نامهٔ لیکرت ۷ درجه‌ای (۱=کاملاً بی‌اهمیت تا ۷=کاملاً مهم) به کارشناسان ارسال و میانگین امتیازات اولیه محاسبه شد. در راند دوم، نظرات متفاوت جمع‌آوری و پالایش شدند و در راند سوم، اجماع نهایی با ضریب کندال (Kendall's $W = 0.85, p < 0.01$) به دست آمد. این فرآیند نشان‌دهندهٔ توافق ۸۵ درصدی کارشناسان بر اهمیت و اعتبار مضامین بود که از طریق کاهش واریانس امتیازات (از ۱.۲ در راند اول به ۰.۴ در راند سوم) تأیید شد.

۲-۵. فاز کمی: اولویت‌بندی راهبردها

در فاز کمی پژوهش، راهبردهای استخراج‌شده از فاز کیفی ابتدا در ماتریس SWOT (نقاط قوت، ضعف، فرصت‌ها و تهدیدات) جایابی شدند.

جدول ۳. ماتریس SWOT تحولات امنیت ملی ایران با تأکید بر روابط بین‌المللی و توسعهٔ فضای مجازی

نقاط ضعف(Weaknesses)	نقاط قوت(Strengths)
ناهماهنگی نهادی و سیاست‌گذاری جزیره‌ای در فضای مجازی	ظرفیت رسانه‌ای و دیپلماتیک داخلی بالا (مانند رسانهٔ ملی و دیپلماسی فعال)
کمبود نیروی متخصص پیشرفته و مهاجرت مغزها	تخصص فنی و نیروی انسانی متخصص در حوزه سایبری
اجرای ضعیف قوانین و محدودیت‌های فیلترینگ داخلی	چارچوب‌های قانونی و اسنادی موجود (سند راهبردی ۱۴۰۱، شبکهٔ ملی اطلاعات)
وابستگی به فناوری خارجی و تأثیر تحریم‌ها	سرمایه‌گذاری دولتی در فناوری بومی
کمبود داده و زیرساخت‌های هوش مصنوعی پیشرفته	دیپلماسی منطقه‌ای قوی (ائتلاف با روسیه، چین و سازمان شانگهای)
تهدیدها(Threats)	فرصت‌ها(Opportunities)
حملات سایبری گسترده با منشأ خارجی (جنگ ترکیبی)	دسترسی جهانی به افکار عمومی از طریق پلتفرم‌های دیجیتال

تبلیغات منفی و انتشار اطلاعات نادرست توسط دشمنان	پیشرفت جهانی هوش مصنوعی و فناوری‌های نوین
تحریم‌های فناوری و محدودیت دسترسی به ابزارهای دفاعی	ائتلاف‌های بین‌المللی و منطقه‌ای برای حکمرانی سایبری (شانگهای، بریکس)
وابستگی خارجی و عملیات نفوذ سایبری (مانند استاکس‌نت و حملات اخیر)	رشد آموزش عمومی و سواد رسانه‌ای
تشدید تنش‌های ژئوپلیتیکی و تأثیر بر امنیت زیرساخت‌های حیاتی	فرصت‌های همکاری فناورانه با کشورهای هم‌سو

مأخذ: یافته‌های پژوهش، ۱۴۰۳

عوامل کلیدی داخلی و خارجی از تحلیل مضمون کیفی شناسایی و در ماتریس‌های ارزیابی عوامل داخلی (IFE) و خارجی (EFE) وارد شدند. وزن هر عامل (از ۰ تا ۱، مجموع ۱.۰۰ در هر ماتریس) بر اساس اجماع نظر همان گروه کارشناسان (از طریق پرسش‌نامه و روش دلفی محدود) تعیین شد؛ وزن بالاتر به عوامل مهم‌تر تخصیص یافت. امتیاز جذابیت (AS) هر راهبرد نسبت به هر عامل از ۱ تا ۴ (۱=جذابیت پایین، ۴=جذابیت بالا) توسط کارشناسان داده شد و میانگین امتیازها محاسبه گردید (با انحراف معیار پایین برای اطمینان از اجماع). امتیاز جذابیت وزنی (TAS) از ضرب وزن عامل در میانگین AS به دست آمد و امتیاز کل جذابیت راهبرد (STAS) از مجموع امتیاز جذابیت وزنی محاسبه شد. این فرآیند کاملاً مبتنی بر قضاوت کارشناسی بود و از روش آماری تکمیلی دیگری استفاده نشد.

جدول ۴. اولویت‌بندی راهبردهای مدیریت فضای مجازی با مدل QSPM

راهبرد	عوامل خارجی (فرصت/تهدید)	عوامل داخلی (قوت/ضعف)	امتیاز جذابیت	اولویت
توسعهٔ دیپلماسی سایبری و تقویت حضور بین‌المللی در پلتفرم‌های دیجیتال	فرصت: دسترسی جهانی به افکار عمومی (۳.۵)؛ تهدید: تبلیغات منفی (۳.۲)	قوت: ظرفیت رسانه‌ای داخلی (۳.۴)؛ ضعف: ناهماهنگی نهادها (۲.۹)	6.8	1
تقویت زیرساخت‌های امنیت سایبری و سرمایه‌گذاری در	فرصت: پیشرفت هوش مصنوعی (۳.۳)؛	قوت: تخصص فنی موجود (۳.۱)؛ ضعف: کمبود نیروی متخصص (۲.۸)	6.5	2

فناوری‌های بومی	تهدید: حملات سایبری (۳.۶)			
تدوین قوانین جامع برای تنظیم محتوای دیجیتال و افزایش سواد رسانه‌ای	فرصت: آموزش عمومی (۳.۰)؛ تهدید: اطلاعات نادرست (۳.۴)	قوت: چارچوب‌های قانونی موجود (۲.۹)؛ ضعف: اجرای ضعیف (۲.۹)	6.2	3
همکاری بین‌المللی برای تدوین هنجارهای سایبری	فرصت: ائتلاف‌های جهانی (۳.۱)؛ تهدید: تحریم‌ها (۳.۰)	قوت: دیپلماسی فعال (۳.۰)؛ ضعف: محدودیت‌های بین‌المللی (۲.۸)	5.9	4
استفاده از هوش مصنوعی برای شناسایی و مقابله با تهدیدات سایبری	فرصت: فناوری‌های نوین (۳.۲)؛ تهدید: وابستگی خارجی (۲.۹)	قوت: سرمایه‌گذاری دولتی (۲.۹)؛ ضعف: کمبود داده (۲.۷)	5.7	5

مأخذ: یافته‌های پژوهش، ۱۴۰۳

نتایج نشان می‌دهد توسعهٔ دیپلماسی سایبری بالاترین اولویت را دارد (STAS=۶.۸)؛ زیرا جذابیت بالایی در عوامل خارجی و داخلی نشان می‌دهد. تقویت زیرساخت‌های سایبری (STAS=۶.۵) در رتبهٔ دوم و تدوین قوانین جامع (STAS=۶.۲) در رتبهٔ سوم قرار گرفتند. تحلیل حساسیت (تغییر ±۰.۵ در AS تهدیدات سایبری) ترتیب اولویت‌ها را تغییر نداد.

همان‌گونه که ملاحظه شد، توسعهٔ دیپلماسی سایبری بالاترین امتیاز را کسب کرد؛ زیرا به‌طور مستقیم بر بهبود تصویر بین‌المللی ایران تأثیر می‌گذارد و می‌تواند تحریم‌های رسانه‌ای را خنثی کند. این راهبرد با امتیاز بالا در عوامل خارجی (مانند دسترسی جهانی) و داخلی (ظرفیت رسانه‌ای) توجیه می‌شود.

تقویت زیرساخت‌های امنیت سایبری در رتبهٔ دوم قرار گرفت؛ زیرا حملات سایبری به‌عنوان تهدید فوری شناسایی شدند و سرمایه‌گذاری بومی می‌تواند وابستگی را کاهش دهد. امتیاز بالا در تهدیدات خارجی نشان‌دهندهٔ اولویت آن است. تدوین قوانین جامع

در اولویت سوم است؛ زیرا به کاهش آسیب‌پذیری‌های اجتماعی کمک می‌کند، اما اجرای آن نیاز به هماهنگی بیشتری دارد. همکاری بین‌المللی و استفاده از هوش مصنوعی در اولویت‌های پایین‌تر قرار گرفتند، اما به‌عنوان راهبردهای مکمل ضروری هستند؛ زیرا می‌توانند فرصت‌های جهانی را بهره‌برداری و ریسک‌های فنی را مدیریت کنند. تحلیل حساسیت نشان داد که تغییر در امتیاز تهدیدات سایبری (افزایش به ۴.۰) اولویت این راهبردها را تغییر نمی‌دهد.

۳-۵. بحث و بررسی

تلفیق یافته‌های کیفی و کمی نشان‌دهندهٔ تعامل پیچیده بین فضای مجازی، روابط بین‌المللی و امنیت ملی ایران هستند. ابعاد مهم این تعاملات عبارت‌اند از:

الف) پیوند با روابط بین‌المللی: فضای مجازی به ایران امکان داده تا از طریق دیپلماسی سایبری، روایت‌های خود را در سطح جهانی ترویج دهد و با تبلیغات منفی مقابله کند. برای مثال، استفاده از پلتفرم‌های دیجیتال در مذاکرات بین‌المللی (مانند توافقات منطقه‌ای) می‌تواند تنش‌ها را کاهش دهد، اما ناهماهنگی داخلی این فرصت را محدود می‌کند. اولویت اول QSPM (توسعهٔ دیپلماسی سایبری) این پیوند را تأیید می‌کند.

ب) امنیت سایبری و پایداری ملی: تهدیدات سایبری، به‌ویژه حملات هدفمند به زیرساخت‌ها، پایداری امنیت ملی را تهدید می‌کنند. یافته‌های کیفی نشان‌دهندهٔ نیاز به فناوری‌های بومی است که با اولویت دوم QSPM همخوانی دارد. این تهدیدات نه‌تنها فنی، بلکه می‌توانند به بی‌ثباتی اجتماعی منجر شوند.

ج) تأثیرات اجتماعی و هویتی: فضای مجازی به‌عنوان شمشیری دو لبه عمل می‌کند؛ هم ابزاری برای تقویت هویت ملی (مانند کمپین‌های فرهنگی) و هم بستری برای انتشار اطلاعات نادرست که انسجام اجتماعی را تضعیف می‌کند. اولویت سوم QSPM (تدوین قوانین) بر نیاز به مدیریت این تأثیرات تأکید دارد. یافته‌ها نشان می‌دهند که بدون افزایش سواد رسانه‌ای، این چالش‌ها می‌توانند به بحران‌های داخلی تبدیل شوند.

به‌طورکلی، تحلیل یکپارچه حاکی از آن است که فرصت‌های فضای مجازی (مانند دیپلماسی سریع) بیشتر از تهدیدات هستند، اما مدیریت ضعیف می‌تواند تعادل را برهم بزند. مدل مفهومی استخراج‌شده نشان‌دهندهٔ چرخه‌ای است که در آن دیپلماسی سایبری به امنیت سایبری کمک می‌کند و هر دو بر هویت اجتماعی تأثیر می‌گذارند.

یافته‌های پژوهش نشان می‌دهند که فضای مجازی نقشی دوگانه در امنیت ملی ایران ایفا می‌کند. از یک سو، ابزاری برای تقویت دیپلماسی و جایگاه بین‌المللی ایران است (با اولویت توسعهٔ دیپلماسی سایبری)، و از سوی دیگر، چالش‌هایی نظیر حملات سایبری و انتشار اطلاعات نادرست را به همراه دارد (با تمرکز بر تقویت زیرساخت‌ها و قوانین). این یافته‌ها ضرورت سیاست‌گذاری منسجم را برجسته می‌کنند که می‌تواند مرزهای جغرافیایی را بی‌اثر کرده و تعاملات جهانی و داخلی را تسریع کند. پیشنهاد می‌شود نهادهای دولتی بر اساس اولویت‌های QSPM، برنامه‌های عملیاتی تدوین کنند تا از فرصت‌ها بهره‌برداری و تهدیدات را مدیریت کنند.

۶. نتیجه‌گیری

این پژوهش با بهره‌گیری از رویکرد آمیخته اکتشافی (کیفی - کمی) به بررسی تأثیر توسعهٔ فضای مجازی و روابط بین‌المللی بر تحولات امنیت ملی ایران پرداخته و نتایج آن نقش دوگانهٔ فضای مجازی را به‌عنوان فرصتی برای تقویت دیپلماسی و تهدیدی برای پایداری ملی برجسته کرده است. در فاز کیفی، سه مضمون اصلی از طریق تحلیل ۱۵۰ کد اولیه و ۳۲ کد محوری استخراج شدند که نشان‌دهندهٔ تأثیر عمیق فضای مجازی بر ابعاد سیاسی، فنی و فرهنگی امنیت ملی است. در فاز کمی، با استفاده از مدل QSPM، راهبردهای پیشنهادی اولویت‌بندی شدند و توسعهٔ دیپلماسی سایبری، تقویت زیرساخت‌های امنیت سایبری و تدوین قوانین جامع برای تنظیم محتوای دیجیتال به ترتیب بالاترین اولویت‌ها را کسب کردند.

یافته‌های پژوهش نشان می‌دهد که فضای مجازی به کشور امکان می‌دهد تا از طریق دیپلماسی سایبری، جایگاه بین‌المللی خود را ارتقا دهد و با تبلیغات منفی مقابله کند. بااین‌حال، تهدیدات سایبری مانند حملات هدفمند به زیرساخت‌ها و چالش‌های اجتماعی نظیر انتشار اطلاعات نادرست، انسجام ملی را به خطر می‌اندازد. این نتایج در بخش‌هایی با پیشینهٔ پژوهش همخوانی و تفاوت‌هایی نیز نشان می‌دهد. برای مثال، یافته‌های کیفی مبنی بر نقش دوگانهٔ فضای مجازی در تقویت هویت ملی و هم‌زمان تشدید قطبی‌سازی اجتماعی، با مطالعات حاجی‌احمدی و ملکیان (۱۴۰۳) و روحانی و همکاران (۱۴۰۲) هم‌سو است، اما پژوهش حاضر با تمرکز بر روابط بین‌المللی، این تأثیر را گسترده‌تر از جنبه‌های داخلی بررسی کرده و نشان می‌دهد که دیپلماسی سایبری می‌تواند به‌عنوان ابزاری برای مقابله با تحریم‌ها عمل کند. همچنین اولویت‌بندی راهبردهای سایبری در فاز کمی با پژوهش‌های بین‌المللی مانند جانسون و وایت (۲۰۲۴) و نس و خینواسارا (۲۰۲۴) همخوانی دارد که بر مدیریت تهدیدات

سایبری در بخش‌های حساس تأکید می‌کنند، اما تفاوت کلیدی در تأکید این پژوهش بر فناوری‌های بومی است که با توجه به تحریم‌های ایران، کاربردی‌تر نشان می‌دهد. در مقابل، یافته‌های مربوط به ضعف در سواد رسانه‌ای با پژوهش پالیزبان (۱۳۹۴) و قدسی (۱۳۹۲) سازگار است. درنهایت، این پژوهش بر ضرورت سیاست‌گذاری منسجم تأکید دارد تا هم از فرصت‌های فضای مجازی بهره‌برداری شود و هم تهدیدات آن به حداقل برسد.

بر اساس یافته‌های پژوهش که نقش دوگانهٔ فضای مجازی را در امنیت ملی ایران برجسته کرد و با توجه به اولویت‌بندی راهبردها در مدل QSPM، پیشنهادها زیر برای بهره‌برداری از فرصت‌ها و مدیریت تهدیدات فضای مجازی ارائه می‌شود:

الف) توسعهٔ دیپلماسی سایبری و تقویت حضور بین‌المللی

- ایجاد واحد تخصصی دیپلماسی دیجیتال در وزارت امور خارجه
- تقویت همکاری با بازیگران غیردولتی
- سیاست‌گذاری مبنی بر کاهش فیلترینگ

ب) تقویت زیرساخت‌های امنیت سایبری و فناوری‌های بومی

- سرمایه‌گذاری در فناوری‌های بومی سایبری
- آموزش نیروی متخصص سایبری
- تأسیس مراکز عملیات امنیت در زیرساخت‌های حیاتی (مانند شبکه‌های برق و آب)

ج) تدوین قوانین جامع و افزایش سواد رسانه‌ای

- تدوین چارچوب‌های قانونی برای تنظیم محتوای دیجیتال
- اجرای برنامه‌های آموزشی سواد رسانه‌ای
- کمپین‌های فرهنگی آنلاین

د) همکاری بین‌المللی و بهره‌گیری از فناوری‌های نوین

- مشارکت در ائتلاف‌های سایبری جهانی
- استفاده از هوش مصنوعی در امنیت سایبری

برای اجرای مؤثر این پیشنهادها، تشکیل کارگروهی متشکل از نمایندگان وزارتخانه‌های امور خارجه، ارتباطات، دفاع و فرهنگ و ارشاد اسلامی ضروری است تا هماهنگی بین‌بخشی را تضمین کنند. همچنین تخصیص بودجهٔ مشخص و زمان‌بندی برای اجرای این برنامه‌ها، همراه با نظارت مستمر بر نتایج، می‌تواند موفقیت سیاست‌گذاری‌ها را افزایش دهد. این پیشنهادها نه‌تنها به تقویت جایگاه ایران در فضای

مجازی کمک می‌کنند، بلکه با مدیریت تهدیدات، پایداری امنیت ملی در برابر چالش‌های نوظهور و بهبود روابط بین‌المللی کشور را تقویت خواهند کرد.

فهرست منابع

الف- فارسی

- آقایی، سیدداوود، صادقی، سیدسعید، و هادی، داریوش. (۱۳۹۱). «واکاوی نقش اینترنت و رسانه‌های اجتماعی جدید در تحولات منطقهٔ خاورمیانه و شمال افریقا (اطلاع‌رسانی، سازمان‌دهی و گسترش سریع تحولات)»، فصل‌نامهٔ روابط خارجی. ۴(۲)، ۳۳-۷.
- پاسبان، ابوالفضل. (۱۴۰۲). «حاکمیت حقوقی دولت‌ها بر فضای مجازی و تأثیر آن بر امنیت ملی»، فصل‌نامهٔ سیاست دفاعی. ۳۲(۱۲۵)، ۴۸-۱۱.
- پالیزبان، محسن. (۱۳۹۴). «بررسی رابطهٔ اینترنت و امنیت ملی جمهوری اسلامی ایران»، فصل‌نامهٔ سیاست. ۴۵(۳)، ۶۵۴-۶۳۵.
- تومی، ایلکا. (۱۳۸۴). جامعه دانایی و پرسش‌های پژوهشی آینده. ترجمهٔ اسماعیل یزدان‌پور. تهران: نشر مرکز پژوهش‌های ارتباطات کشور.
- حاجی‌احمدی، مهدی و ملکیان، نازنین. (۱۴۰۳). «واکاوی نقش دیپلماسی رسانه‌ای در قدرت داخلی و روابط بین‌المللی کشورهای درحال‌توسعه»، فصل‌نامهٔ سیاست خارجی. ۳۸(۳)، ۱۶۶-۱۲۷.
- روحانی، ابوالفضل و روحانی، مهدی. (۱۴۰۲). «نقش فضای مجازی در حکمرانی ملی ج.ا.ایران»، مطالعات بین رشته‌ای دانش راهبردی. ۱۳(۵۳)، ۸۴-۶۱.
- قدسی، امیر. (۱۳۹۲). «تأثیر فضای مجازی بر امنیت ملی ج. ا. ایران و ارائه راهبرد با تأکید بر ایفای نقش سرمایهٔ اجتماعی»، فصل‌نامهٔ راهبرد دفاعی. ۱۱(۴۴)، ۱۸۶-۱۴۹.
- قنبرلو، عبداله. (۱۳۹۷). امنیت ملی: مفهوم، تئوری، و عمل، فصل‌نامهٔ سیاست کاربردی. ۱(۱)، ۶۷-۴۱.
- کاستلز، مانوئل. (۱۳۸۵). عصر اطلاعات: اقتصاد، جامعه و فرهنگ جلد ۱، ظهور جامعهٔ شبکه‌ای. ترجمهٔ احد علیقلیان، افشین خاکباز، حسن چاوشیان. تهران: نشر طرح نو.
- کلومبیس، تئودور، ولف، جیمز. (۱۳۷۵). رویکردهای مختلف در مطالعهٔ سیاست. (وحید بزرگی، مترجم). تهران: انتشارات جهاد دانشگاهی.
- گل‌محمدی، احمد. (۱۳۸۶). جهانی‌شدن، فرهنگ، هویت. تهران: نشر نی.
- محسنی، منوچهر. (۱۳۸۰). جامعه‌شناسی جامعهٔ اطلاعاتی. تهران: نشر دیدار.

- ندری، غلامرضا، بخشایشی، احمد، دارابی، علی، مقصودی، مجتبی. (۱۳۹۸). «بررسی نقش سیاسی - امنیتی شبکه‌های اجتماعی مجازی بر امنیت ملی ج. ا. ا.»، فصل‌نامهٔ پژوهش‌های حفاظتی امنیتی. ۸(۲۹)، ۸۸-۶۳.

ب- انگلیسی

- Bell, D. (1980). The social framework of the information society. In The microelectronics revolution (pp. 211-230). Basil Blackwell.
- Bjola, C., & Manor, I. (2022). The Oxford Handbook of Modern Diplomacy. Oxford University Press, pp. 451-468.
- Castells, M. (1997). The informational city: Information technology, economic restructuring, and the urban-regional process. Blackwell.
- Castells, M. (2010). The rise of the network society: The information age: Economy, society, and culture. Wiley-Blackwell.
- Chen, H., Chau, M., & Xu, H. (2021). Cybersecurity and national security in the digital age. Springer.
- Chudasama, D & Patel, K. (2021). National security threats in cyberspace. National Journal of Cyber Security Law, 4(1), p12-20.
- Dobák, I. (2021). Thoughts on the evolution of national security in cyberspace. Security and Defence Quarterly, 33(1), 75–85.
- Ebo, E. (1996). Media diplomacy and foreign policy: Toward a theoretical framework. In A. Malek (Ed.) , News media and foreign relations, pp. 44-56. Routledge.
- Farrell, H., & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, 44(1), 42–79.
- Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). Cyber Persistence Theory: Redefining National Security in Cyberspace. Oxford University Press.
- Hampton, K. N., Goulet, L. S., Rainie, L., & Purcell, K. (2011). Social networking sites and our lives. Pew Research Center.
- Harvey, D. (1989). The condition of postmodernity: An enquiry into the origins of cultural change. Blackwell Publishers.
- Johnson, R., & White, M. (2024). The Impact of Social Media on Global Security: A New Perspective. International Security Review, 28(1), 89-112.
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59–68.
- Kaspersky Lab. (2014). Stuxnet worm analysis.
- Kello, L., & Arquilla, J. (2023). Cyber threats and strategic challenges in global politics. Political Science Quarterly, 138(1), 42–60.
- Maurer, T. (2020). Cyberspace and International Relations: Rising Powers, Proxies, and Norms, Doctoral dissertation, university of Berlin.
- Mearsheimer, J. J. (1994). The false promise of international institutions. International Security, 19(3), 5–49.
- Mwangi, P. (2024). Cybersecurity Threats and National Ssmecurity in the Digital Age. American Journal of International Relations, 9(1), 26–35.

- Ness, S., & Khinvasara, T. (2024). Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector. Journal of Engineering Research and Reports, 26(2), 107-117.
- Nye, J. (2023). Digital power and diplomacy in the 21st century. Journal of International Affairs, 76(2), 65–82.
- Prasad, R. (2002). Communication and foreign policy. Journal of Communication, 52(4), 122-135.
- Sheafer, T., & Gabay, I. (2009). The media and public diplomacy: A strategic contest over international agenda building and frame building. Political Communication, 26(4), 445-467.
- Taylor, M. (1997). Global communications, international affairs and the media since 1945. Routledge.
- UNODC. (2020). Global report on cybercrime and digital cooperation. United Nations Office on Drugs and Crime.