پژوهشگاه
فضای مجازی

دفتر آبی ۷

مجموعه گزارش‌های پژوهشی
اسفند ماه ۱۴۰۳

کشورگشایی سایبری

مفهوم شناسی دیپلماسی سایبر و قابلیت‌های
دیپلماسی سایبری ایران، روسیه و رژیم صهیونیستی


بسم الله الرحمن

کشورگشایی سایبری

مفهوم شناسی دیپلماسی سایبر و قابلیت‌های دیپلماسی سایبری ایران، روسیه و رژیم صهیونیستی

دفترآبی (Research Paper) شمارهٔ هفتم (اسفند ۱۴۰۳)

مؤلف: فهیمه صابری
مدیر میزهای پژوهشی پژوهشگاه تهران فضای مجازی

نشانی: تهران، سعادت آباد، خیابان علامه شمالی، کوچه هجدهم غربی، پلاک ۱۷
تلفن: ۲۲۷۳۰۳۱-۰۲۱
کد پستی: ۱۹۹۷۹۸۷۶۲۹

مقالات پژوهشی (Research Paper) از مهم‌ترین ابزارهای توسعهٔ دانش هستند که با تکیه بر داده‌های تجربی به بررسی دقیق و جامع موضوعات تخصصی می‌پردازند. این مقالات معمولاً توسط پژوهشگران، استادان دانشگاه و محققان حرفه‌ای نوشته می‌شوند و به‌تفصیل از مشاهدات و داده‌های تحقیق بحث می‌کنند. مخاطب این مقالات نیز عمدتاً محققان و کارشناسان آن رشته است. امروزه در مسئلهٔ فضای مجازی و سایبری، به‌طور مرتب مقالات پرشماری توسط محققان و اندیشکده‌ها تولید می‌شود که به بررسی موشکافانهٔ مسائل جاری در این حوزه می‌پردازند. آگاهی از این مطالعات و رصد شرایط و ابعاد مختلف این حوزه از این رهگذر، برای کارشناسان و به‌خصوص قانون‌گذاران، حکمرانان و متولیان این عرصه ضروری است.

دفترهای آبی دسته‌ای از گزارش‌های تفصیلیِ تولیدشده در پژوهشگاه فضای مجازی، و محصول رصد مطالعات اندیشکده‌ها و نخبگان جهان و منطقه در این موضوع است.

پیشگفتار

دنیا با سرعت فزاینده‌ای به سمت اشاعهٔ فناوری‌های حاکمیت گریز می‌رود و این فناوری‌ها درحقیقت حاکمیت خود را خواهند داشت که توسط کمپانی‌های بزرگ راهبری می‌شود. در نتیجه دولت‌ها در خدمت این شرکت‌ها و سکوها در می‌آیند. این واقعیت دنیای امروز است و باید آن را به درستی درک کرد و دانست که دولت‌ها، قدرت سابق و سنتی را از دست خواهند داد.

در عین حال، مؤلفه‌ها و وظایف متفاوتی برای دولت‌ها تعریف می‌شود و دولتی دست بالاتر را خواهد داشت که بتواند برای توسعهٔ زیست بوم فناوری خود شرایط را مهیا کند تا زیست بوم تحت حمایت او هرچقدر که می‌تواند ، در داخل و خارج از کشور گسترش یابد. دیپلماسی سایبری نیز در همینجا تعریف می‌شود. به این صورت که دولت‌ها تلاش می‌کنند چهار مؤلفهٔ زیرساخت، خدمات پایه و کاربردی، و نیز محتوای خود را بدین طریق به خارج از مرزهای خود گسترش دهند. در این بستر، تنها برطرف‌کردن نیاز داخلی، قطع نظر از فراتر رفتن از مرزها ممکن نیست، زیرا در این صورت، به‌زودی سکوهایی با دسترسی جهانی و حجم محتوا و مخاطبِ بی‌شمار، سکوهای شما را خواهند بلعید.

درنتیجه، دیپلماسی سایبری باید در این چهار مسئله تسهیلگری کند. کشورهایی مانند آمریکا و چین یا حتی قطر، وزارت خارجهٔ خود را متناسب با این بستر، دگرگون کرده و فعال کرده‌اند. در حالی که برخی کشورها مانند کشور ما هنوز در مرحلهٔ تدوین آیین‌نامه‌ها و اساس‌نامه‌هاست و با ساختارهای سابق فعالیت می‌کند. لذا لازم است متناسب با این تغییرات، ساختار و وظایف دستگاه دیپلماسی نیز دگرگون شود و جایگاه‌ها و وظایف جدیدی تعریف کند.

ضرورت این تغییر نیز روشن است. امروز دیگر هیچ‌کس از فضای مجازی و سایبری به دور نیست و همهٔ مردم بخش قابل توجهی از شبانه‌روز خود را در بسترهای سایبری و مجازی، از

شبکه‌های اجتماعی گرفته تا بازی و گیم، می‌گذرانند. اگر دستگاهی به این باور برسد که در صورتی که تنها به مخاطبان بومی خود بسنده کند، توسط سکوهای جهانی و فراملی بلعیده می‌شود، حتماً آرایش متفاوتی در درون آن دستگاه برای حضور در این شرایط شکل خواهد گرفت و برای تسهیلگری جهت گسترش دادن بسترها به خارج از مرزهای خود اقدام خواهد کرد.

این تهدید و چنگ‌انداختنِ سکوها و شرکت‌ها به مخاطبانِ کشورهای مختلف تا حدی جدی است که امروز شرکت‌ها در راه ارائهٔ زیرساخت‌ها (مانند منظومه‌های ماهواره‌ای) برای ارائهٔ بی‌واسطه و بدون فیلترِ خدمات خود هستند. در صورتی که در این میدان رقابت جهانی منفعلانه عمل کنیم و با غفلت از دیپلماسی سایبری، تنها به ارائهٔ خدمات داخلی بسنده کنیم، درنهایت همان عرصهٔ داخلی را نیز از دست خواهیم داد و بهره‌های مختلفِ جامعهٔ مخاطب ما (داده، تراکنش‌های مالی و...) نیز نصیب دیگران خواهد شد.

میثم غلامی
سرپرست پژوهشگاه فضای مجازی
اسفندماه سال ۱۴۰۳

خلاصهٔ مدیریتی

این پژوهش به مفهوم‌شناسی دیپلماسی سایبری و قابلیت‌های دیپلماسی سایبری ایران، روسیه و رژیم اسرائیل می‌پردازد و به بررسی نقش این مفهوم در سیاست‌های داخلی و خارجی این سه کشور در عصر دیجیتال توجه دارد. دیپلماسی سایبری به‌عنوان ابزاری نوین در مدیریت روابط بین‌المللی و ایجاد قدرت نرم، در بستر فناوری‌های نوظهور مانند هوش مصنوعی، بلاکچین و اینترنت اشیا تحلیل شده است. ایران از دیپلماسی سایبری به‌عنوان ابزاری برای مقابله با فشارهای خارجی، گسترش نفوذ منطقه‌ای و مدیریت تهدیدات امنیتی استفاده می‌کند. روسیه، با تکیه بر فرهنگ استراتژیک و سیاست‌های سایبری چندلایه، فضای سایبری را به عرصه‌ای برای تقویت هژمونی ژئوپلیتیکی خود و تضعیف ساختارهای دموکراتیک غربی تبدیل کرده است. رژیم اسرائیل، با بهره‌گیری از فناوری‌های پیشرفته و نوآوری در دیپلماسی دیجیتال، در تقویت امنیت سایبری و گسترش همکاری‌های بین‌المللی پیشرو است. یافته‌ها نشان می‌دهد که هر سه کشور از دیپلماسی سایبری به‌عنوان ابزاری برای پیشبرد منافع ملی و تقویت حضور خود در نظام بین‌الملل استفاده می‌کنند. این پژوهش همچنین بر اهمیت توسعهٔ چارچوب‌های بین‌المللی و تقویت همکاری‌های چندجانبه در مدیریت فضای سایبری تأکید دارد.

واژه‌های کلیدی: دیپلماسی سایبری، قابلیت‌های سایبری، ایران، روسیه، رژیم اسرائیل، امنیت سایبری

مقدمه

در دنیای امروز، فضای سایبری به یکی از مهم‌ترین عرصه‌های روابط بین‌المللی و دیپلماسی تبدیل شده است. دیپلماسی سایبری، به‌عنوان ابزاری استراتژیک، نقش قابل‌توجهی در مدیریت منازعات، پیشبرد اهداف سیاسی و تعاملات بین‌المللی ایفا می‌کند. این نوع دیپلماسی شامل استفاده از ابزارهای دیجیتال و سایبری برای تأثیرگذاری بر افکار عمومی، برقراری ارتباطات سیاسی و کاهش تهدیدات امنیتی است. کشورهای ایران، روسیه و رژیم صهیونیستی به‌دلیل جایگاه جغرافیایی و ژئوپلیتیکی خود، نقش کلیدی در شکل‌دهی به رویکردهای دیپلماسی سایبری داشته‌اند. بررسی این سه کشور می‌تواند دیدگاه‌های منحصربه‌فردی دربارهٔ مفهوم دیپلماسی سایبری و قابلیت‌های عملیاتی آن ارائه دهد (Abbasi, 2024; Cohen, 2019; Frei, 2020).

اهمیت دیپلماسی سایبری در دنیای کنونی از این واقعیت ناشی می‌شود که تحولات فناوری و دیجیتالی‌شدن، مرزهای سنتی تعاملات بین‌المللی را از بین برده و فضای جدیدی را برای قدرت‌نمایی کشورها ایجاد کرده است. در حالی که روسیه از دیپلماسی سایبری به‌عنوان ابزاری برای تحکیم قدرت جهانی و تضعیف نظام‌های دموکراتیک غربی استفاده می‌کند، رژیم اسرائیل رویکردی فعال و پیشرفته را برای دفاع از زیرساخت‌های خود و پیشبرد سیاست‌های منطقه‌ای اتخاذ کرده است. ایران نیز با بهره‌گیری از استراتژی‌های نامتقارن، به‌دنبال تقویت موقعیت منطقه‌ای و مقابله با تهدیدات قدرت‌های غربی است (Chinn, 2015; Tsvetkova et al., 2022; Baram, 2017).

توسعهٔ فناوری‌های دیجیتال، نه تنها ساختارهای قدرت جهانی را تغییر داده، بلکه مدل‌های تعامل دیپلماتیک سنتی را نیز دگرگون کرده است. دیپلماسی سایبری، به‌عنوان بخشی از تحول در روابط بین‌المللی، به دولت‌ها اجازه می‌دهد تا با استفاده از ابزارهای جدید، رویکردهای خلاقانه‌ای برای اعمال نفوذ در صحنهٔ جهانی اتخاذ کنند. این تحول به‌طور ویژه در

کشورهایی مانند روسیه، رژیم اسرائیل و ایران مشهود است که از فضای سایبری برای پیشبرد منافع ملی و تأثیرگذاری بر سیاست‌های بین‌المللی استفاده می‌کنند. در همین راستا، استفاده از دیپلماسی سایبری به‌عنوان ابزاری برای ایجاد بازدارندگی، اعمال فشار و حتی کاهش تنش‌ها مورد توجه قرار گرفته است (Aquino, 2022; Kari, 2019; Baezner, 2019).

با وجود پژوهش‌های متعددی که دربارهٔ دیپلماسی سایبری این کشورها انجام شده است، شکاف‌هایی در بررسی جامع مفهومی و عملیاتی دیپلماسی سایبری میان این سه کشور وجود دارد. بسیاری از مطالعات تنها بر یک کشور یا جنبه‌ای خاص از این موضوع متمرکز بوده‌اند، در حالی که مقایسهٔ تطبیقی بین این کشورها می‌تواند بینش‌های جدیدی ارائه دهد. پژوهش‌هایی مانند تحلیل فرهنگ استراتژیک روسیه در سیاست‌های سایبری یا نقش دیپلماسی سایبری رژیم اسرائیل در تأثیرگذاری بر افکار عمومی ایرانیان، نمونه‌هایی از بررسی‌های موضوعی هستند که نیاز به نگاه گسترده‌تری دارند (Treggiari, 2016; Chinn, 2015; Kari, 2019).

از سوی دیگر، در حالی که روسیه با تمرکز بر ایجاد حاکمیت سایبری، تلاش می‌کند استقلال دیجیتالی خود را تقویت کند، رژیم اسرائیل در حال تقویت رهبری فناوری سایبری جهانی است. در این میان، ایران از استراتژی‌های نامتقارن برای کاهش شکاف فناوری و مقابله با تهدیدات خارجی استفاده می‌کند. چنین تفاوت‌هایی در رویکردها، باعث شده که دیپلماسی سایبری به یکی از حوزه‌های کلیدی مطالعه در روابط بین‌الملل تبدیل شود. شکاف‌های موجود در پژوهش‌ها نشان‌دهندهٔ نیاز به بررسی‌های جامع‌تر و مقایسه‌ای برای درک بهتر این تحولات است (Cohen, 2019; Frei, 2020; Tsvetkova et al., 2022).

این مقاله با هدف پر کردن این شکاف، به بررسی مفهوم دیپلماسی سایبری و قابلیت‌های عملیاتی ایران، روسیه و رژیم صهیونیستی می‌پردازد. با استفاده از تحلیل مقایسه‌ای و بررسی مطالعات پیشین، این مقاله تلاش دارد تا نقش این کشورها در شکل‌دهی به دیپلماسی سایبری بین‌المللی را روشن کند. همچنین، این پژوهش به شناسایی فرصت‌ها و چالش‌های موجود در این زمینه کمک کرده و پیشنهاداتی برای تحقیقات آینده ارائه می‌دهد (Baram, 2017; Aquino, 2022; Abbasi, 2024).

پیشینهٔ پژوهش

- Abbasi (۲۰۲۴) در پژوهش با عنوان «تهدیدات سایبری علیه ایران از سوی آمریکا و رژیم اسرائیل: راهبردهای مقابله ایران»، به بررسی روابط سایبری میان ایران، آمریکا و رژیم اسرائیل پرداخته است. این پژوهش به‌صورت کیفی و با استفاده از تحلیل منابع ثانویه انجام شده است. نتایج نشان می‌دهد که استراتژی‌های سایبری آمریکا و رژیم اسرائیل شامل حملات پیشگیرانه و نفوذ به زیرساخت‌های حیاتی ایران است، در حالی که ایران نیز با تقویت قابلیت‌های سایبری خود به مقابله پرداخته است. نتیجه‌گیری این پژوهش فضای سایبری را به‌عنوان عرصه‌ای برای تضادهای ژئوپلیتیکی معرفی کرده است و پیشنهاد شده است که چارچوب‌های بین‌المللی برای کاهش تنش‌ها و تقویت امنیت سایبری تدوین شود.
- Stachoń (۲۰۲۴) در مقاله‌ای با عنوان «قابلیت‌های سایبری ایران به‌عنوان ابزاری برای سیاست داخلی و خارجی»، نقش ظرفیت‌های سایبری ایران در امنیت منطقه‌ای و جهانی بررسی شده است. این مطالعه با تحلیل منابع ثانویه و داده‌های موردی نشان داده است که ایران از فضای سایبری برای مقاصد داخلی مانند نظارت و کنترل جریان اطلاعات و عملیات خارجی مانند جاسوسی و حملات سایبری استفاده می‌کند. نتیجه‌گیری پژوهش، ظرفیت‌های سایبری ایران را عاملی مهم در استراتژی امنیتی این کشور معرفی کرده است. پیشنهاد شده است که چارچوب‌های قانونی و همکاری‌های امنیتی برای مدیریت بهتر تهدیدات سایبری ایجاد شود.
- Amini Baghbaderani, E., & Nasrollahi, M. S (۲۰۲۴). در مقاله‌ای با عنوان «مفهوم‌شناسی و مطالعهٔ تطبیقی دیپلماسی سایبری، دیجیتال و همگرا (با تأکید بر بند هفتم سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای)»، به بررسی مفاهیم

دیپلماسی سایبری، دیجیتال و همگرا پرداخته شده است. این پژوهش با استفاده از روش تحلیل تطبیقی و توصیفی انجام شده است. نتایج نشان داده است که دیپلماسی سایبری و دیجیتال در چارچوب‌های حکمرانی متفاوت تعریف می‌شوند و پژوهش مفهوم جدیدی به نام «دیپلماسی همگرا» را پیشنهاد کرده است. نتیجه‌گیری این پژوهش بر اهمیت تدوین چارچوب‌های نظری و سیاستی برای حکمرانی در عصر فضای مجازی تأکید دارد. پیشنهاد شده است که مدل‌های سیاست‌گذاری برای تقویت دیپلماسی همگرا و همکاری‌های بین‌المللی در حکمرانی فضای مجازی طراحی شوند.

- Duguin & Pavlova (۲۰۲۳) در پژوهش با عنوان «نقش سایبر در جنگ روسیه علیه اوکراین: تأثیر و پیامدهای آن برای آیندهٔ جنگ‌های مسلحانه »، تأثیر فضای سایبری بر جنگ‌های مدرن را بررسی کرده‌اند. روش تحقیق این پژوهش تحلیل کیفی مبتنی بر مستندات تاریخی و تجربیات میدانی بوده است. نتایج نشان می‌دهد که حملات سایبری روسیه نقش مهمی در ایجاد بی‌ثباتی در زیرساخت‌های حیاتی اوکراین ایفا کرده و سایبر به‌عنوان یک مکمل در کنار جنگ نظامی شناخته شده است. نتیجه‌گیری بر اهمیت فضای سایبری به‌عنوان یکی از حوزه‌های کلیدی جنگ‌های آینده تأکید دارد. پیشنهاد پژوهش تقویت همکاری‌های بین‌المللی برای جلوگیری از سوءاستفاده از فناوری‌های سایبری است.
- Mohammad Yam Tasori, Bashir Hosseini, and Mahdi Sharifi (۲۰۲۲) در پایان‌نامه‌ای با عنوان «دیپلماسی سایبری رژیم صهیونیستی در قبال جمهوری اسلامی ایران؛ مطالعهٔ موردی صفحهٔ وزارت امور خارجهٔ رژیم اسرائیل به فارسی در اینستاگرام»، فعالیت‌های دیپلماسی سایبری رژیم اسرائیل علیه ایران بررسی شده است. روش تحقیق این مطالعه شامل استفاده از روش مطالعهٔ اسنادی و تحلیل محتوا برای بررسی تکنیک‌های روایت‌سازی در پلتفرم‌های رسانه‌ای بوده است. نتایج نشان داده است که رژیم اسرائیل از تکنیک‌های روایت‌سازی مانند تداعی

معانی و ارائهٔ شواهد برای ترویج تصاویر مثبت از خود و منفی از جمهوری اسلامی ایران استفاده کرده است. نتیجه‌گیری این پژوهش بر تأثیرگذاری دیپلماسی سایبری رژیم اسرائیل بر افکار عمومی ایرانیان تأکید دارد و پیشنهاد شده است که ایران استراتژی‌های مقابله‌ای را برای مدیریت افکار عمومی و تقویت حضور خود در فضای سایبری تدوین کند.

- Aquino, S. B. (۲۰۲۲) در پژوهش با عنوان «تغییر از عملیات نظامی به عملیات سایبری: مرور ادبیات دیپلماسی سایبری»، به تحلیل تغییرات دیپلماسی سایبری در روابط بین‌المللی پرداخته است. این پژوهش با استفاده از مرور سیستماتیک ادبیات و چارچوب نئورئالیسم، سیاست‌های سایبری دولت‌ها را بررسی کرده است. نتایج نشان داده که فضای سایبری به عرصه‌ای پیچیده برای روابط قدرت تبدیل شده و نیازمند بازنگری در نظریه‌های سنتی روابط بین‌الملل است. نتیجه‌گیری پژوهش بر اهمیت تفاوت سیاست‌ها و قابلیت‌های سایبری دولت‌ها تأکید دارد و پیشنهاد شده است که چارچوب‌های جدیدی برای مدیریت فضای سایبری تدوین گردد.
- Tsvetkova, Sytnik, and Grishanina (۲۰۲۲) در پژوهش با عنوان «دیپلماسی دیجیتال و روابط بین‌المللی دیجیتال: چالش‌ها و فرصت‌های جدید» به تحلیل نقش دیجیتال‌سازی در روابط بین‌المللی پرداخته‌اند. این پژوهش با تحلیل داده‌های شبکه‌های اجتماعی و کلان‌داده‌ها، به بررسی دیپلماسی دیجیتال در مناطق بحران‌زده مانند افغانستان، سوریه و ایران پرداخته است. نتایج نشان می‌دهد که سه چالش کلیدی شامل عدم اطمینان دیجیتال، تکه‌تکه شدن واقعیت دیجیتال، و استفاده از «فریمینگ» برای پیشبرد سیاست‌های خارجی وجود دارد. نتیجه‌گیری این پژوهش بر لزوم ایجاد توافق‌نامه‌های الزام‌آور بین‌المللی برای مدیریت فضای دیجیتال و تنظیم خطوط قرمز در این فضا تأکید می‌کند. پیشنهاد شده است که زیرساخت‌های داده تقویت و چارچوب‌های همکاری بین‌المللی تدوین شود.

- Ford (۲۰۲۲) در پژوهش با عنوان «مفهوم‌سازی دیپلماسی امنیت سایبری »، به بررسی چارچوب‌های نظری و ابعاد عملی دیپلماسی امنیت سایبری پرداخته است. روش تحقیق این مطالعه، تحلیل نظری و بررسی مستندات بین‌المللی مرتبط با دیپلماسی سایبری بوده است. نتایج نشان داده است که دیپلماسی سایبری می‌تواند ابزاری مؤثر برای کاهش تنش‌های سایبری و افزایش اعتماد بین دولت‌ها باشد. نتیجه‌گیری پژوهش بر ضرورت توسعهٔ مکانیسم‌های شفافیت و اعتمادسازی در فضای سایبری تأکید دارد. پیشنهاد شده است که کشورها چارچوب حقوقی جهانی برای مدیریت تهدیدات سایبری ایجاد کنند.
- Devanny et al. (۲۰۲۲) در پژوهش با عنوان «استراتژی در حوزه‌ای نامطمئن: تهدیدات و پاسخ‌ها در فضای سایبری» به تحلیل تهدیدات سایبری و استراتژی‌های پاسخ به آن‌ها پرداخته‌اند. این مطالعه با رویکرد توصیفی-تحلیلی، تهدیدات اصلی در فضای سایبری و استراتژی‌های مناسب برای مقابله با آن‌ها را شناسایی کرده است. نتایج پژوهش نشان می‌دهد که همکاری‌های بین‌المللی و ایجاد سیاست‌های امنیتی چندلایه برای مدیریت تهدیدات سایبری حیاتی است. نتیجه‌گیری این تحقیق بر ضرورت انعطاف‌پذیری و به‌روزرسانی مداوم استراتژی‌های امنیت سایبری تأکید دارد. پیشنهاد شده است که چارچوبی جهانی برای همکاری در شناسایی و پاسخ به تهدیدات سایبری ایجاد شود.
- Givens et al. (۲۰۲۲) در پژوهش با عنوان «پیش‌بینی واکنش‌های دولت ایران به حملات سایبری» به تحلیل رفتارهای احتمالی ایران در مواجهه با حملات سایبری پرداخته است. این پژوهش با استفاده از مدل‌سازی پیش‌بینی و تحلیل رفتارهای گذشتهٔ دولت ایران انجام شده است. یافته‌های این تحقیق نشان می‌دهد که واکنش ایران به عوامل مختلفی مانند شدت حمله و اهمیت زیرساخت‌های مورد هدف بستگی دارد. در نتیجه‌گیری این تحقیق، بر استفاده از ابزارهای دیپلماتیک و تقابلی توسط ایران

تأکید شده است. پیشنهاد پژوهش شامل تقویت رویکردهای دیپلماتیک و افزایش توان سایبری کشورها برای کاهش احتمال حملات سایبری است.

- Karim (۲۰۲۱) در پژوهش با عنوان «امنیت سایبری و دیپلماسی سایبری در نقطهٔ عطف: ارزیابی تحولات حقوقی بین‌المللی در بنگلادش»، به بررسی وضعیت دیپلماسی سایبری و امنیت سایبری در بنگلادش پرداخته است. روش تحقیق این مطالعه تحلیل حقوقی و مقایسه‌ای بوده است. نتایج پژوهش خلاءهای قانونی و ضعف در سیاست‌های سایبری بنگلادش را نشان داده است. نتیجه‌گیری بر لزوم تدوین سیاست‌های نوآورانه و چارچوب‌های قانونی برای بهبود امنیت سایبری تأکید دارد. پیشنهاد شده است که بنگلادش با تقویت توانایی‌های سایبری از طریق همکاری‌های بین‌المللی، چارچوب‌های قانونی قوی‌تری را ایجاد کند.
- Assoudeh (۲۰۲۰) در پایان‌نامه‌ای با عنوان «شکل‌دهی به استراتژی امنیت سایبری: چشم‌انداز مقایسه‌ای چین، ایران و روسیه»، استراتژی‌های امنیت سایبری این سه کشور را بررسی کرده است. این پژوهش با استفاده از مدل واقع‌گرایی نئوکلاسیک و تحلیل موردی انجام شده است. نتایج نشان می‌دهد که هر کشور بر اساس ویژگی‌های داخلی و سیاست خارجی خود، استراتژی‌های متفاوتی را اتخاذ کرده است؛ چین در پی تنظیم قوانین سایبری جدید، ایران برای ترویج ارزش‌های انقلاب اسلامی، و روسیه برای کنترل اوراسیا و تضعیف نظام‌های دموکراتیک غربی عمل می‌کند. نتیجه‌گیری بر تأثیر برداشت‌های متفاوت از فرصت‌ها و تهدیدات سایبری بر استراتژی‌های این کشورها تأکید دارد. پیشنهاد شده است که چارچوب‌های همکاری بین‌المللی برای مدیریت تهدیدات سایبری تدوین شود.
- Frei, J. (۲۰۲۰) در پژوهش با عنوان «نگرش‌های امنیت سایبری و دفاع سایبری ملی رژیم اسرائیل: سیاست‌ها و سازمان‌ها»، به تحلیل ساختارهای امنیت سایبری و دفاع سایبری رژیم اسرائیل پرداخته است. روش تحقیق این مطالعه، توصیفی و تحلیلی بوده و بر بررسی اسناد سیاستی و مشارکت‌های ملی و بین‌المللی رژیم

اسرائیل متمرکز بوده است. نتایج نشان می‌دهد که رژیم اسرائیل با تدوین راهبردهای جامع، همکاری‌های گستردهٔ بین‌المللی، و تأکید بر نوآوری، به یکی از پیشروترین کشورها در این حوزه تبدیل شده است. در نتیجه‌گیری پژوهش، بر نقش ادغام توانمندی‌های نظامی و غیرنظامی در تقویت دفاع سایبری و توسعهٔ روابط با شرکای بین‌المللی تأکید شده است. پیشنهاد شده است چارچوب‌های قانونی بین‌المللی برای مدیریت فضای سایبری تقویت شود و آموزش عمومی در این زمینه گسترش یابد.

- Martti J. Kari (۲۰۱۹) در پایان‌نامه‌ای با عنوان «فرهنگ استراتژیک روسیه در فضای سایبری: نظریهٔ فرهنگ استراتژیک به‌عنوان ابزاری برای توضیح درک تهدیدات سایبری روسیه و پاسخ به این تهدیدات»، به بررسی سیاست‌های سایبری روسیه در چارچوب فرهنگ استراتژیک پرداخته است. این پژوهش از تحلیل اسناد رسمی روسی و دکترین‌های امنیتی استفاده کرده است. نتایج نشان می‌دهد که نگاه روسیه به فضای سایبری به‌عنوان یک میدان جنگ استراتژیک با تکیه بر مفهوم «قلعهٔ محاصره‌شده» شکل گرفته است. نتیجه‌گیری پژوهش، بر لزوم مطالعهٔ تأثیر فرهنگ استراتژیک بر سیاست‌های سایبری دولت‌ها تأکید دارد و پیشنهاد شده است که چارچوب‌های همکاری بین‌المللی برای مدیریت تهدیدات سایبری تدوین گردد.
- Lubin (۲۰۱۹) در پژوهش با عنوان «بیمهٔ سایبری به‌عنوان ابزار دیپلماسی سایبری» به بررسی نقش بیمهٔ سایبری در کاهش اثرات حملات سایبری و تقویت دیپلماسی بین‌المللی پرداخته است. این مطالعه با استفاده از تحلیل کیفی و بررسی اسناد و قوانین مرتبط انجام شده است. نتایج نشان می‌دهد که بیمهٔ سایبری می‌تواند به‌عنوان ابزاری حمایتی، اثرات حملات سایبری را کاهش داده و اعتماد بین دولت‌ها را افزایش دهد. در نتیجه‌گیری این پژوهش آمده است که تقویت سیستم‌های بیمهٔ سایبری نقش مهمی در بهبود روابط دیپلماتیک ایفا می‌کند. پیشنهاد این تحقیق،

تدوین استانداردهای بین‌المللی برای بیمهٔ سایبری و ایجاد ساختارهای مشترک همکاری در این زمینه است.

- Baezner (۲۰۱۹) در پژوهش با عنوان «تحلیل نقاط حساس: فعالیت‌های سایبری ایران در زمینهٔ رقابت‌های منطقه‌ای و تنش‌های بین‌المللی»، فعالیت‌های سایبری ایران را در چارچوب رقابت‌های منطقه‌ای بررسی کرده است. این مطالعه با استفاده از روش مطالعهٔ موردی و تحلیل داده‌های سایبری از منابع باز انجام شده است. نتایج نشان داده است که ایران از فعالیت‌های سایبری به‌عنوان ابزاری برای پیشبرد منافع استراتژیک خود بهره می‌برد. نتیجه‌گیری پژوهش بر اهمیت تقویت دیپلماسی برای مدیریت فعالیت‌های سایبری و کاهش تنش‌ها تأکید دارد. پیشنهاد پژوهش، ایجاد پروتکل‌های همکاری بین‌المللی برای مدیریت فعالیت‌های سایبری است.
- Baezner (۲۰۱۹) در پژوهش با عنوان «تحلیل نقاط حساس: فعالیت‌های سایبری ایران در زمینهٔ رقابت‌های منطقه‌ای و تنش‌های بین‌المللی» به بررسی استفادهٔ ایران از حملات سایبری به‌عنوان ابزار جنگ نامتقارن پرداخته است. روش تحقیق این پژوهش تحلیل داده‌های کیفی و منابع ثانویهٔ مرتبط با امنیت سایبری بوده است. نتایج نشان می‌دهد که ایران با تمرکز بر جاسوسی سایبری و کنترل مخالفان داخلی و خارجی، فضای سایبری را به‌عنوان عرصه‌ای حیاتی برای اعمال نفوذ در سیاست‌های منطقه‌ای و بین‌المللی به کار گرفته است. نتیجه‌گیری این تحقیق، بر اهمیت مدیریت تهدیدات سایبری از طریق چارچوب‌های قانونی و همکاری‌های بین‌المللی تأکید دارد. پیشنهاد شده است که آگاهی عمومی دربارهٔ تهدیدات سایبری افزایش یابد و همکاری‌های بین‌المللی در زمینهٔ امنیت سایبری تقویت شود.
- Cohen (۲۰۱۹) در پژوهش با عنوان «قابلیت‌های سایبری ایران: ارزیابی تهدید برای منافع مالی و امنیتی رژیم اسرائیل»، حملات سایبری ایران به زیرساخت‌های حیاتی رژیم اسرائیل را تحلیل کرده است. این پژوهش با تحلیل تاریخی و توصیفی به بررسی گروه‌های تهدیدگر سایبری ایران مانند APT33 و Ashiyane پرداخته است.

نتایج نشان می‌دهد که این حملات شامل نفوذ به زیرساخت‌های بانکی، خطوط هوایی، و نیروهای دفاعی رژیم اسرائیل بوده است. نتیجه‌گیری پژوهش بر تأثیر بلندمدت استراتژی سایبری ایران بر امنیت اقتصادی و ملی رژیم اسرائیل تأکید دارد. پیشنهاد شده است که رژیم اسرائیل با تدوین سیاست‌های بازدارندگی و تقویت امنیت سایبری، هزینه‌های حملات ایران را افزایش دهد.

- Barrinha & Renard (۲۰۱۷) در پژوهش با عنوان «دیپلماسی سایبری: شکل‌گیری جامعهٔ بین‌المللی در عصر دیجیتال» مفهوم دیپلماسی سایبری و تأثیر آن بر تعاملات بین‌المللی را بررسی کرده‌اند. این تحقیق با مطالعهٔ تطبیقی و تحلیل کیفی تعاملات سایبری انجام شده است. نتایج نشان می‌دهد که دیپلماسی سایبری ابزاری مؤثر برای ایجاد اعتماد و تعاملات بین‌المللی است. نتیجه‌گیری پژوهش بر نقش دیپلماسی سایبری در کاهش تنش‌ها و افزایش همکاری‌ها بین دولت‌ها تأکید دارد. پیشنهاد شده است که چارچوب‌های جهانی برای تنظیم و مدیریت تعاملات سایبری ایجاد شود.
- Baram (۲۰۱۷) در پژوهش با عنوان «دفاع رژیم اسرائیل در عصر جنگ‌های سایبری» به بررسی تأثیر جنگ‌های سایبری بر امنیت ملی رژیم اسرائیل پرداخته است. این مطالعه با روش تحقیق توصیفی و تحلیل داده‌های تاریخی و معاصر انجام شده است. نتایج این پژوهش نشان می‌دهد که رژیم اسرائیل توانسته با توسعهٔ زیرساخت‌های پیشرفته و سرمایه‌گذاری در فناوری‌های نوین، تهدیدات سایبری را مدیریت و کاهش دهد. نتیجه‌گیری این تحقیق بر اهمیت همکاری‌های بین‌المللی در مقابله با تهدیدات سایبری تأکید می‌کند و پیشنهاد شده است که چارچوب‌های قانونی بین‌المللی برای مدیریت جنگ‌های سایبری توسعه یابد و شفافیت در سیاست‌های سایبری افزایش پیدا کند.
- Melysa et al. (۲۰۱۶) در پژوهش با عنوان «تحلیل استفاده از عملیات سایبری تهاجمی برای مقابله با تهدیدات هسته‌ای ایران» به بررسی نقش حملات سایبری در

مدیریت تهدیدات هسته‌ای پرداخته‌اند. این تحقیق با روش تحلیل موردی و بررسی عملیات سایبری گذشته انجام شده است. نتایج نشان می‌دهد که عملیات سایبری می‌تواند به کاهش تهدیدات هسته‌ای کمک کند، اما احتمال تشدید تنش‌ها نیز وجود دارد. نتیجه‌گیری این پژوهش بر اهمیت استفاده از عملیات سایبری به‌عنوان ابزار مکمل دیپلماسی تأکید دارد. پیشنهاد این تحقیق شامل تقویت سیاست‌های بازدارندگی سایبری و ایجاد استانداردهای بین‌المللی برای جلوگیری از سوءاستفاده از فضای سایبری است.

- Khalid & Safdar (۲۰۱۶) در پژوهش با عنوان «توافق هسته‌ای ایران: بازاندیشی سیاست خاورمیانه‌ای پاکستان» تأثیر توافق هسته‌ای ایران بر سیاست‌های منطقه‌ای پاکستان را تحلیل کرده‌اند. این تحقیق با استفاده از تحلیل سیاست‌های منطقه‌ای و اثرات توافق هسته‌ای بر آن‌ها انجام شده است. نتایج نشان می‌دهد که توافق هسته‌ای ایران فرصت‌های جدیدی برای همکاری بین پاکستان و کشورهای خاورمیانه فراهم کرده است. در نتیجه‌گیری این تحقیق بر ضرورت تقویت روابط اقتصادی و امنیتی میان پاکستان و ایران تأکید شده است. پیشنهاد شده است که همکاری‌های منطقه‌ای و تعاملات دیپلماتیک برای ثبات خاورمیانه تقویت شوند.
- Luigi Ferdinando Treggiari (۲۰۱۶) در پایان‌نامه‌ای با عنوان «مفاهیم روابط بین‌الملل در فضای سایبری: حاکمیت، جنگ و دیپلماسی در عصر دیجیتال»، به تحلیل مفاهیم کلیدی روابط بین‌الملل در زمینهٔ فضای سایبری پرداخته است. این پژوهش از تحلیل مفهومی و چارچوب‌های نظری روابط بین‌الملل استفاده کرده است. نتایج نشان داده است که فضای سایبری به‌عنوان ابزاری قدرتمند برای دولت‌ها و بازیگران غیردولتی، تعاریف سنتی از حاکمیت و قدرت را تغییر داده است. نتیجه‌گیری بر لزوم تدوین چارچوب‌های حقوقی بین‌المللی برای مدیریت فضای سایبری تأکید دارد و پیشنهاد شده است که همکاری‌های جهانی در زمینهٔ امنیت سایبری تقویت گردد.

- Chinn, J. N.(۲۰۱۵) در پایان‌نامه‌ای با عنوان «قدرت ارتباطی در دیپلماسی دیجیتال رژیم اسرائیل: به سوی نظریهٔ شبکه‌ای ژئوپلیتیک »، به بررسی استراتژی‌های دیپلماسی دیجیتال رژیم اسرائیل پرداخته است. روش تحقیق این پژوهش، تحلیل شبکه‌ای و استفاده از نظریهٔ قدرت ارتباطی کاستلز بوده است. نتایج نشان داده است که سفارت‌های رژیم اسرائیل در جوامع دیجیتال، استراتژی‌های موثری برای هدایت تعاملات و افزایش نفوذ خود داشته‌اند، اما کنسولگری‌ها در مقایسه با سفارت‌ها عملکرد محدودی در استفاده از این پلتفرم‌ها داشته‌اند. نتیجه‌گیری پژوهش به اهمیت تمرکز بر تعامل شبکه‌ای و استفادهٔ بهینه از ابزارهای دیجیتال برای افزایش تأثیرگذاری دیپلماسی رژیم اسرائیل اشاره دارد.
- Hussain & Abdullah(۲۰۱۵) در پژوهش با عنوان «توافق هسته‌ای ایران: پیامدها برای امنیت منطقه‌ای» تأثیر این توافق بر امنیت منطقه‌ای را مورد بررسی قرار داده‌اند. روش تحقیق این مطالعه تحلیل سیاسی و بررسی سیاست‌های امنیتی کشورهای منطقه بوده است. نتایج نشان داده است که توافق هسته‌ای باعث کاهش تنش‌های منطقه‌ای شده، اما نگرانی‌ها دربارهٔ فعالیت‌های غیرهسته‌ای ایران همچنان پابرجاست. در نتیجه‌گیری این تحقیق بر ضرورت همکاری‌های منطقه‌ای برای مدیریت پیامدهای این توافق تأکید شده است. پیشنهاد این پژوهش شامل تقویت دیپلماسی چندجانبه و ایجاد چارچوب‌های امنیتی جدید در منطقه است.
- Brower (۲۰۱۳) در پژوهش با عنوان «ارزیابی نظامی پیشگیرانه علیه ایران» به بررسی راهبردهای نظامی برای مقابله با ایران پرداخته است. روش تحقیق شامل تحلیل‌های نظامی و مطالعهٔ موردی بر روی سیاست‌های دفاعی بوده است. نتایج نشان داده است که هرگونه اقدام نظامی پیشگیرانه علیه ایران می‌تواند منجر به ایجاد خطرات بلندمدت برای امنیت منطقه شود. در نتیجه‌گیری آمده است که

دیپلماسی مؤثرترین ابزار برای کاهش تنش‌ها با ایران است. پیشنهاد پژوهش بر تقویت گفت‌وگوهای دیپلماتیک و کاهش تمرکز بر استراتژی‌های نظامی تأکید دارد.

- Farwell & Arakelian (۲۰۱۳) در پژوهش با عنوان «قابلیت‌های سایبری ایران و پیامدهای آن در جنگ‌های آینده»، توانایی‌های سایبری ایران را مورد بررسی قرار داده‌اند. این مطالعه با تحلیل توصیفی از توانایی‌های سایبری ایران و استراتژی‌های پیشگیرانهٔ دیگر کشورها انجام شده است. نتایج نشان داده است که قابلیت‌های سایبری ایران می‌توانند تهدیدی جدی برای دشمنان منطقه‌ای و بین‌المللی ایجاد کنند. نتیجه‌گیری این پژوهش بر تأثیرفزایندهٔ استراتژی‌های سایبری ایران بر امنیت منطقه‌ای تأکید دارد. پیشنهاد این تحقیق، توسعهٔ چارچوب‌های دفاع سایبری و تقویت هماهنگی‌های بین‌المللی برای مقابله با تهدیدات سایبری است.
- Tarock (۱۹۹۶) در پژوهش با عنوان «روابط ایران و آمریکا: به سوی رویارویی؟» به تحلیل تاریخی و سیاسی روابط ایران و آمریکا و احتمال بروز تنش‌های جدید پرداخته است. این مطالعه با روش تحلیل تاریخی و سیاسی انجام شده و نشان داده است که روابط دو کشور تحت تأثیر سوءتفاهم‌ها و تضادهای سیاسی قرار دارد. نتیجه‌گیری این پژوهش بر اهمیت گفت‌وگوی مستقیم و سازندهٔ بین دو کشور تأکید کرده است. پیشنهاد شده است که مکانیزم‌های میانجی‌گری و تقویت دیپلماسی برای حل مسائل و کاهش تنش‌ها ایجاد شوند.

روش‌شناسی

این پژوهش به روش مروری روایتی انجام شده است و با بهره‌گیری از منابع علمی منتشرشده، به بررسی مفهوم دیپلماسی سایبری و قابلیت‌های دیپلماسی سایبری در سه کشور ایران، روسیه و رژیم اسرائیل پرداخته است. فرآیند جمع‌آوری و تحلیل اطلاعات به شرح زیر صورت گرفته‌است:

- انتخاب منابع اطلاعاتی: مقالات و پایان‌نامه‌های علمی که از طریق پژوهش‌های پیشین و منابع ارسال‌شده توسط کاربر فراهم آمده‌اند، به‌عنوان پایهٔ این پژوهش انتخاب شدند. این منابع شامل ۲۹ مقاله و پایان‌نامهٔ معتبر بودند که به‌طور خاص بر دیپلماسی سایبری و جنبه‌های عملیاتی آن در کشورهای ایران، روسیه و رژیم اسرائیل تمرکز داشتند. معیار انتخاب منابع شامل ارتباط مستقیم با موضوع پژوهش، سطح علمی معتبر (مقالات داوری‌شده یا پایان‌نامه‌های دانشگاهی) و انتشار در حوزهٔ روابط بین‌الملل و امنیت سایبری بود.
- روش انتخاب و تحلیل مقالات: مقالات بر اساس عنوان، چکیده و کلمات کلیدی مرتبط انتخاب شدند. پس از انتخاب منابع، متن کامل هر مقاله بررسی شد تا داده‌ها و دیدگاه‌های مرتبط با مفهوم دیپلماسی سایبری و رویکردهای عملیاتی سه کشور استخراج شود. این تحلیل بر اساس شناسایی تم‌های اصلی مانند «مفهوم‌شناسی دیپلماسی سایبری»، «قابلیت‌های سایبری»، «چالش‌ها» و «فرصت‌ها» انجام شد.
- ترکیب داده‌ها: داده‌های استخراج‌شده از مقالات مختلف به شیوه‌ای ترکیب شدند که بتوانند دیدگاه‌های کلی و جامع دربارهٔ موضوع ارائه دهند. این ترکیب با استفاده از رویکردی توصیفی و تحلیلی انجام شد تا نقاط اشتراک و اختلاف بین سه کشور بررسی

شود. علاوه بر این، شکاف‌های پژوهشی در مطالعات قبلی شناسایی و در تحلیل یافته‌ها مورد تأکید قرار گرفت.

- ساختار تحلیل: پژوهش با دسته‌بندی اطلاعات به موضوعات اصلی مانند «مفهوم‌شناسی دیپلماسی سایبری»، «قابلیت‌ها و ابزارها»، «چالش‌ها» و «فرصت‌ها» ادامه یافت. این ساختار به محققان امکان می‌دهد تا تفاوت‌ها و شباهت‌های سه کشور را در زمینهٔ دیپلماسی سایبری به‌طور مستقیم مقایسه کنند.

یافته‌ها و تحلیل

مفهوم‌شناسی دیپلماسی سایبری

دیپلماسی سایبری علاوه بر ابزارهای فنی، به استراتژی‌هایی برای مدیریت فضاهای دیجیتال نیاز دارد. در این راستا، مفهوم «حاکمیت بر فضای سایبری» نقش محوری دارد. روسیه و چین نمونه‌هایی از کشورهایی هستند که حاکمیت سایبری را به‌عنوان بخشی از دیپلماسی سایبری خود مطرح کرده‌اند. در مقابل، کشورهایی مانند ایالات متحده و رژیم اسرائیل بر مفهوم «حاکمیت با فضای سایبری» تأکید دارند، که بر تقویت آزادی اینترنت و تنظیم مقررات سایبری جهانی تمرکز دارد (Treggiari, 2016; Kari, 2019).

این نوع دیپلماسی نه تنها توسط دولت‌ها، بلکه توسط بازیگران غیردولتی مانند شرکت‌های فناوری، سازمان‌های بین‌المللی، و گروه‌های جامعهٔ مدنی نیز به‌کار گرفته می‌شود. به‌عنوان مثال، شرکت‌های فناوری اطلاعات مانند مایکروسافت و گوگل نقش مهمی در شکل‌دهی به قواعد و چارچوب‌های بین‌المللی در فضای سایبری دارند. این رویکرد نشان‌دهندهٔ تحولی عمیق در مفهوم سنتی دیپلماسی است که در آن تنها دولت‌ها نقش اصلی را ایفا می‌کردند (Chinn, 2015; Aquino, 2022).

در سطح کاربردی، دیپلماسی سایبری شامل اقداماتی مانند مدیریت حملات سایبری، ایجاد تفاهم‌نامه‌های بین‌المللی در زمینهٔ امنیت سایبری، و استفاده از شبکه‌های اجتماعی برای دیپلماسی عمومی است. رژیم اسرائیل نمونهٔ بارزی از کشوری است که با بهره‌گیری از ابزارهای دیجیتال مانند هوش مصنوعی، توانسته است دیپلماسی سایبری خود را تقویت کرده و از آن برای مقابله با تهدیدات منطقه‌ای استفاده کند. این کشور از فناوری‌های پیشرفته برای دفاع از زیرساخت‌های خود و ترویج همکاری‌های بین‌المللی بهره‌برداری کرده است (Baram, 2017; Cohen, 2019).

دیپلماسی سایبری همچنین به‌عنوان یک ابزار تهاجمی مورد استفاده قرار می‌گیرد. روسیه، به‌ویژه از ابزارهایی مانند اطلاعات غلط و کارزارهای آنلاین برای تأثیرگذاری بر افکار عمومی و کاهش نفوذ غرب بهره می‌برد. این کشور از دیپلماسی سایبری برای مقابله با نفوذ فرهنگی غرب و تقویت سیاست‌های خود در اوراسیا استفاده کرده است. این رویکرد نشان‌دهندهٔ اهمیت استراتژیک دیپلماسی سایبری در رقابت‌های ژئوپلیتیک است (Kari, 2019; Tsvetkova et al., 2022).

در نهایت، مفهوم دیپلماسی سایبری به‌طور مداوم در حال تحول است و با تغییرات سریع فناوری و فضای دیجیتال تطبیق می‌یابد. این مفهوم اکنون به‌عنوان بخشی جدایی‌ناپذیر از سیاست خارجی کشورها محسوب می‌شود و نقش آن در شکل‌دهی به نظم جهانی آینده افزایش خواهد یافت. دیپلماسی سایبری نه تنها به‌عنوان ابزاری برای تعامل، بلکه به‌عنوان سلاحی در منازعات بین‌المللی ظاهر شده است، که اهمیت مطالعه و تحلیل عمیق آن را دوچندان می‌کند (Aquino, 2022; Frei, 2020).

۱. تحلیل نقش دیپلماسی سایبری در سیاست خارجی ایران، روسیه و رژیم اسرائیل

ایران: دیپلماسی سایبری به‌عنوان ابزار مقاومت

دیپلماسی سایبری ایران نقش کلیدی در سیاست خارجی این کشور ایفا می‌کند و به‌عنوان ابزاری برای مقابله با نفوذ قدرت‌های غربی و تقویت موقعیت ژئوپلیتیکی ایران مورد استفاده قرار می‌گیرد. ایران از فضای سایبری برای پیشبرد اهداف سیاسی و امنیتی خود بهره‌برداری کرده است. به‌عنوان مثال، حملات سایبری مانند ویروس «شمعون» که زیرساخت‌های حیاتی دشمنان منطقه‌ای را هدف قرار داده است، بخشی از راهبرد تهاجمی سایبری ایران بوده است. علاوه بر این، ایران با استفاده از ابزارهای سایبری مانند شبکه‌های اجتماعی، سعی در مقابله با جنگ نرم و تأثیرگذاری بر افکار عمومی داخلی و خارجی دارد (Abbasi, 2024; Kari, 2019).

روسیه: دیپلماسی سایبری به‌عنوان ابزار قدرت جهانی

روسیه دیپلماسی سایبری را به‌عنوان بخشی از استراتژی امنیت ملی و سیاست خارجی خود در نظر گرفته است. این کشور از ابزارهای سایبری برای نفوذ در فرآیندهای سیاسی و دموکراتیک کشورهای غربی و تقویت قدرت خود در عرصهٔ جهانی استفاده می‌کند. برای مثال، اتهامات مربوط به مداخلهٔ روسیه در انتخابات ریاست جمهوری ایالات متحده در سال ۲۰۱۶ و استفاده از کارزارهای اطلاعات غلط، نشان‌دهندهٔ نقش دیپلماسی سایبری در راهبرد ژئوپلیتیکی این کشور است. روسیه همچنین بر تقویت «حاکمیت سایبری» خود تأکید دارد و با ایجاد اینترنت مستقل، تلاش می‌کند کنترل کامل بر زیرساخت‌های سایبری داخلی خود داشته باشد (Tsvetkova et al., 2022; Kari, 2019).

رژیم صهیونیستی: دیپلماسی سایبری به‌عنوان ابزار دفاع و تعامل

رژیم اسرائیل با تمرکز بر امنیت سایبری و نوآوری، دیپلماسی سایبری را به یکی از ارکان سیاست خارجی خود تبدیل کرده است. این کشور از دیپلماسی سایبری برای تقویت روابط بین‌المللی و مقابله با تهدیدات سایبری منطقه‌ای استفاده می‌کند. به‌عنوان مثال، رژیم اسرائیل با ایجاد مراکز فناوری پیشرفته و همکاری با کشورهای دیگر در حوزهٔ امنیت سایبری، نقش مؤثری در شکل‌دهی به سیاست‌های جهانی در این زمینه ایفا کرده است. علاوه بر این، استفاده از هوش مصنوعی و ابزارهای تحلیل داده برای پیش‌بینی و مقابله با تهدیدات سایبری، بخشی از رویکرد دیپلماسی سایبری این کشور است (Baram, 2017; Cohen, 2019).

تأثیر بر نظام بین‌المللی

نقش دیپلماسی سایبری این سه کشور، فراتر از مرزهای ملی آن‌ها بوده و بر نظام بین‌المللی تأثیر گذاشته است. ایران از دیپلماسی سایبری برای ایجاد موازنه در برابر قدرت‌های بزرگ مانند ایالات متحده استفاده می‌کند، در حالی که روسیه با استفاده از ابزارهای سایبری، تلاش دارد نظم جهانی را به نفع خود تغییر دهد. رژیم اسرائیل نیز با ارائهٔ نوآوری‌های سایبری و همکاری بین‌المللی، به

شکل‌دهی استانداردهای امنیت سایبری جهانی کمک کرده است (Aquino, 2022; Frei, 2020).

نقش دیپلماسی سایبری در مقابله با تهدیدات

هر سه کشور از دیپلماسی سایبری برای مقابله با تهدیدات امنیتی و افزایش بازدارندگی استفاده می‌کنند. ایران از دیپلماسی سایبری برای مقابله با فشارهای غرب و تحریم‌ها بهره می‌برد، در حالی که روسیه با استفاده از ابزارهای سایبری، سیاست‌های بازدارندگی خود را تقویت کرده است. رژیم اسرائیل نیز با تمرکز بر دفاع سایبری، از این ابزار برای حفاظت از زیرساخت‌های حیاتی خود و جلوگیری از حملات سایبری استفاده می‌کند (Kari, 2019; Cohen, 2019).

تحلیل نهایی: تفاوت‌های استراتژیک

دیپلماسی سایبری این سه کشور بر اساس نیازها و شرایط ژئوپلیتیکی خاص آن‌ها تعریف شده است. در حالی که ایران بیشتر بر رویکردهای دفاعی و نامتقارن تمرکز دارد، روسیه از دیپلماسی سایبری برای تأثیرگذاری در سیاست‌های جهانی و مقابله با غرب بهره می‌برد. در مقابل، رژیم اسرائیل با تمرکز بر نوآوری و همکاری‌های بین‌المللی، دیپلماسی سایبری را به ابزاری مؤثر برای ارتقای موقعیت جهانی خود تبدیل کرده است (Chinn, 2015; Tsvetkova et al., 2022).

۲. مثال‌های واقعی از اقدامات دیپلماسی سایبری توسط ایران، روسیه و رژیم اسرائیل

اقدامات دیپلماسی سایبری ایران

حملات سایبری به زیرساخت‌های حیاتی دشمنان: ایران در سال‌های اخیر از توانایی‌های سایبری خود برای هدف قرار دادن زیرساخت‌های حیاتی دشمنان استفاده کرده است. یکی از مثال‌های برجسته، حملهٔ سایبری به شرکت نفتی آرامکو در عربستان سعودی بود که به انتشار ویروس «شمعون» منجر شد. این حمله به‌عنوان پاسخی به حملات سایبری علیه ایران تعبیر شد و تأثیرات جدی بر زیرساخت‌های نفتی این کشور داشت (Abbasi, 2024; Kari, 2019).

استفاده از شبکه‌های اجتماعی برای نفوذ در افکار عمومی: ایران با استفاده از شبکه‌های اجتماعی مانند توییتر و اینستاگرام، تلاش کرده است بر افکار عمومی جهانی و داخلی تأثیر بگذارد. به‌عنوان مثال، انتشار پیام‌های ضد رژیم اسرائیلی و ترویج دیدگاه‌های انقلاب اسلامی از طریق صفحات دولتی و غیررسمی، بخشی از استراتژی دیپلماسی سایبری ایران بوده است. این اقدامات با هدف مقابله با جنگ نرم دشمنان و تقویت پیام‌های ایدئولوژیک ایران انجام شده است (Baram, 2017).

مقابله با تحریم‌ها از طریق عملیات سایبری: ایران از توانایی‌های سایبری برای مقابله با تحریم‌های اقتصادی استفاده کرده است. یکی از نمونه‌های این اقدامات، تلاش برای نفوذ به سیستم‌های مالی و بانکی کشورهای غربی به‌منظور دور زدن تحریم‌ها بوده است. این تلاش‌ها نشان‌دهندهٔ نقش سایبری به‌عنوان ابزار مکمل دیپلماسی سنتی است (Chinn, 2015).

اقدامات دیپلماسی سایبری روسیه

مداخله در انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶: یکی از شناخته‌شده‌ترین اقدامات دیپلماسی سایبری روسیه، کارزارهای اطلاعاتی و سایبری برای تأثیرگذاری بر انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۱۶ بود. این کارزارها شامل انتشار اخبار جعلی، نفوذ به ایمیل‌های سیاسی، و استفاده از ربات‌های شبکه‌های اجتماعی برای ایجاد اختلافات داخلی در آمریکا بود (Tsvetkova et al., 2022).

حملات سایبری به زیرساخت‌های اوکراین: روسیه در سال‌های اخیر از حملات سایبری برای ایجاد بی‌ثباتی در اوکراین استفاده کرده است. یکی از نمونه‌های برجسته، حملهٔ سایبری به شبکهٔ برق اوکراین در سال ۲۰۱۵ بود که باعث قطعی برق گسترده در این کشور شد. این حمله بخشی از استراتژی کلی روسیه برای اعمال فشار بر دولت اوکراین و تضعیف زیرساخت‌های حیاتی آن بود (Baezner, 2019).

استفاده از دیپلماسی سایبری برای تضعیف اتحادیهٔ اروپا: روسیه با استفاده از اطلاعات غلط و کارزارهای سایبری، تلاش کرده است اتحاد و همبستگی اتحادیهٔ اروپا را تضعیف کند. این اقدامات

شامل حمایت از جنبش‌های افراطی، تشدید تنش‌های سیاسی داخلی در کشورهای اروپایی، و ایجاد شکاف در سیاست‌های مشترک امنیتی و اقتصادی اروپا بوده است (Kari, 2019).

اقدامات دیپلماسی سایبری رژیم اسرائیل

حملات سایبری به برنامهٔ هسته‌ای ایران: رژیم اسرائیل یکی از کشورهایی است که به‌طور گسترده از حملات سایبری برای پیشبرد اهداف استراتژیک خود استفاده کرده است. نمونهٔ بارز این حملات، ویروس استاکس‌نت است که با همکاری ایالات متحده طراحی شد و برنامهٔ هسته‌ای ایران را هدف قرار داد. این ویروس توانست به‌طور موقت فرآیند غنی‌سازی اورانیوم را مختل کند و برنامهٔ هسته‌ای ایران را به تأخیر بیندازد (Baram, 2017; Cohen, 2019).

همکاری‌های بین‌المللی در حوزهٔ امنیت سایبری: رژیم اسرائیل از دیپلماسی سایبری برای تقویت همکاری‌های بین‌المللی خود استفاده می‌کند. به‌عنوان مثال، این کشور با اتحادیهٔ اروپا و کشورهای دیگر در زمینهٔ مقابله با جرایم سایبری همکاری کرده و مراکز نوآوری سایبری مشترک ایجاد کرده است. این همکاری‌ها به تقویت جایگاه رژیم اسرائیل به‌عنوان رهبر جهانی در امنیت سایبری کمک کرده است (Frei, 2020).

پروژه‌های دیپلماسی عمومی در فضای سایبری: رژیم اسرائیل با استفاده از شبکه‌های اجتماعی، تلاش کرده است تصویر مثبتی از خود در میان افکار عمومی جهانی ایجاد کند. پروژه‌هایی مانند صفحهٔ رسمی وزارت امور خارجهٔ رژیم اسرائیل در اینستاگرام، که به زبان فارسی طراحی شده است، برای ارتباط با مردم ایران و تأثیرگذاری بر دیدگاه‌های آنان در مورد سیاست‌های رژیم اسرائیل به‌کار گرفته شده است (Tsvetkova et al., 2022).

۳. بررسی تأثیر فناوری‌های نوین بر تغییر مفهوم دیپلماسی سایبری

تحول در ابزارهای دیپلماسی سایبری

ظهور فناوری‌های نوین مانند هوش مصنوعی (AI)، کلان‌داده‌ها (Big Data)، و اینترنت اشیا (IoT) موجب تحول در مفهوم دیپلماسی سایبری شده است. این فناوری‌ها، دولت‌ها را قادر می‌سازند تا اطلاعات را به سرعت جمع‌آوری، تحلیل، و استفاده کنند و ابزارهایی کارآمدتر برای

مدیریت روابط بین‌المللی فراهم آورند. به‌عنوان مثال، رژیم اسرائیل از هوش مصنوعی برای پیش‌بینی تهدیدات سایبری و شناسایی الگوهای حمله استفاده می‌کند، که به آن‌ها اجازه می‌دهد سیاست‌های سایبری پیشگیرانه را به اجرا بگذارند(Baram, 2017; Cohen, 2019).

کلان‌داده‌ها و تصمیم‌گیری در دیپلماسی سایبری

کلان‌داده‌ها نقش کلیدی در تغییر مفهوم دیپلماسی سایبری ایفا می‌کنند. این فناوری، امکان تحلیل عمیق‌تر و سریع‌تر داده‌های مرتبط با سیاست خارجی و تهدیدات امنیتی را فراهم می‌کند. روسیه از تحلیل کلان‌داده‌ها برای شناسایی نقاط ضعف سیستم‌های سایبری دشمنان خود و طراحی حملات سایبری هدفمند بهره‌برداری کرده است. همچنین، این داده‌ها به بهبود استراتژی‌های نفوذ و ایجاد پیام‌های اطلاعاتی دقیق‌تر کمک می‌کنند(Tsvetkova et al., 2022).

نقش هوش مصنوعی در مدیریت بحران‌های سایبری

هوش مصنوعی به‌عنوان یکی از پیشرفته‌ترین ابزارهای فناوری نوین، در مدیریت بحران‌های سایبری نقشی اساسی دارد. به‌عنوان مثال، ایران از سیستم‌های هوش مصنوعی برای تشخیص و پاسخ سریع به حملات سایبری استفاده کرده و توانسته است در برخی موارد حملات دشمنان را خنثی کند. این فناوری همچنین به دولت‌ها امکان می‌دهد تا رفتارهای سایبری رقبا را مدل‌سازی و پیش‌بینی کنند و بر این اساس استراتژی‌های مؤثرتری را طراحی کنند(Aquino, 2022; Kari, 2019).

دیپلماسی سایبری و بلاکچین

بلاکچین، به‌عنوان فناوری ای امن و غیرمتمرکز، توانسته است مفهوم دیپلماسی سایبری را به شیوه‌ای اساسی تغییر دهد. این فناوری به کشورها امکان می‌دهد تا اطلاعات حساس را با امنیت بالا ذخیره و تبادل کنند و همچنین سیستم‌های رأی‌گیری الکترونیکی امن را توسعه دهند. به‌عنوان مثال، رژیم اسرائیل در پروژه‌های امنیت سایبری مرتبط با بلاکچین پیشرو بوده و این فناوری را برای ارتقای امنیت داده‌ها در تعاملات بین‌المللی به‌کار گرفته است(Frei, 2020; Cohen, 2019).

نقش فناوری‌های ارتباطی نوین

پلتفرم‌های جدید ارتباطی مانند شبکه‌های اجتماعی و ابزارهای واقعیت مجازی (VR) نیز تأثیر قابل‌توجهی بر دیپلماسی سایبری داشته‌اند. این فناوری‌ها به دولت‌ها امکان می‌دهند تا پیام‌های دیپلماتیک خود را به‌طور مستقیم به مخاطبان جهانی منتقل کنند. برای مثال، ایران از شبکه‌های اجتماعی به زبان‌های مختلف برای ترویج پیام‌های سیاسی خود و تأثیرگذاری بر افکار عمومی جهانی استفاده کرده است. در همین راستا، روسیه نیز با بهره‌گیری از شبکه‌های اجتماعی، تلاش کرده است تا تأثیرات سیاست‌های غرب را کاهش داده و روایت‌های جایگزین ارائه دهد (Chinn, 2015; Abbasi, 2024).

استفاده از فناوری اینترنت اشیا (IoT) در دیپلماسی سایبری

اینترنت اشیا (IoT) به‌طور فزاینده‌ای در دیپلماسی سایبری مورد توجه قرار گرفته است. دستگاه‌های متصل به اینترنت می‌توانند اطلاعات گسترده‌ای تولید کنند که برای نظارت و تحلیل در سطح بین‌المللی به‌کار می‌روند. روسیه و رژیم اسرائیل از IoT برای بهبود نظارت بر زیرساخت‌های حیاتی و مقابله با تهدیدات سایبری استفاده کرده‌اند. این فناوری به آن‌ها امکان می‌دهد تا نه‌تنها از حملات پیشگیری کنند، بلکه از فضای سایبری برای بهبود توان دیپلماتیک خود بهره ببرند (Tsvetkova et al., 2022; Baram, 2017).

قابلیت‌های دیپلماسی سایبری

۱. تحلیل مقایسه‌ای ابزارها و فناوری‌های استفاده‌شده در ایران، روسیه و رژیم اسرائیل

ایران: بهره‌برداری از ابزارهای نامتقارن

ایران به دلیل تحریم‌های اقتصادی و محدودیت‌های فناوری، استراتژی‌های سایبری خود را بر ابزارهای نامتقارن متمرکز کرده است. این کشور از حملات سایبری برای دستیابی به اهداف سیاسی و اقتصادی خود استفاده می‌کند. برای مثال:

- جاسوسی سایبری: ایران با استفاده از گروه‌های پیشرفتهٔ تهدید (APT) مانند APT33 و Ashiyane تلاش می‌کند اطلاعات حساس دشمنان منطقه‌ای و بین‌المللی را به‌دست آورد (Abbasi, 2024; Cohen, 2019).
- انتشار اطلاعات غلط: ایران از شبکه‌های اجتماعی برای تأثیرگذاری بر افکار عمومی و تضعیف دشمنان خود بهره می‌گیرد.
- حملات سایبری تهاجمی: نمونهٔ بارز این حملات، نفوذ به زیرساخت‌های انرژی عربستان سعودی و گسترش ویروس شمعون بوده است که خسارات قابل‌توجهی به دنبال داشت (Baram, 2017; Chinn, 2015).

روسیه: استفاده از ابزارهای اطلاعاتی پیشرفته

روسیه به‌عنوان یکی از پیشروترین کشورها در دیپلماسی سایبری، از طیف گسترده‌ای از ابزارهای سایبری برای اعمال نفوذ جهانی بهره می‌برد. این کشور از فناوری‌های پیشرفته اطلاعاتی برای پیشبرد اهداف استراتژیک خود استفاده می‌کند:

- کارزارهای اطلاعات غلط: روسیه از ابزارهای سایبری برای انتشار اخبار جعلی و تضعیف انسجام اجتماعی در کشورهای غربی استفاده می‌کند. به‌عنوان مثال، دخالت در انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶ نمونه‌ای از این کارزارهاست (Tsvetkova et al., 2022; Kari, 2019).
- حملات باج‌افزاری: روسیه با استفاده از حملات سایبری مانند WannaCry زیرساخت‌های حیاتی کشورهای غربی را هدف قرار داده است.
- حاکمیت سایبری: روسیه بر ایجاد اینترنت داخلی و مستقل تأکید دارد که به این کشور امکان کنترل کامل بر فضای سایبری داخلی را می‌دهد (Baezner, 2019).

رژیم اسرائیل: نوآوری و فناوری پیشرفته

رژیم اسرائیل از فناوری‌های پیشرفته و ابزارهای نوین سایبری برای تقویت دیپلماسی سایبری خود استفاده می‌کند. این کشور با تمرکز بر نوآوری و همکاری‌های بین‌المللی، قابلیت‌های خود را به سطح جهانی ارتقا داده است:

- هوش مصنوعی (AI): رژیم اسرائیل از AI برای تحلیل داده‌های سایبری و پیش‌بینی تهدیدات استفاده می‌کند. این فناوری به رژیم اسرائیل کمک کرده است تا واکنش‌های سریع و مؤثری به تهدیدات نشان دهد (Cohen, 2019; Frei, 2020).
- چارچوب‌های امنیتی: رژیم اسرائیل دارای یکی از پیشرفته‌ترین سیستم‌های دفاع سایبری است که از زیرساخت‌های حیاتی این کشور در برابر حملات سایبری محافظت می‌کند.
- همکاری‌های بین‌المللی: رژیم اسرائیل با ایجاد مراکز فناوری و نوآوری سایبری، همکاری‌های بین‌المللی در حوزهٔ امنیت سایبری را تقویت کرده است (Tsvetkova et al., 2022).

جدول(۱-۳): مقایسهٔ کلی ابزارها و فناوری‌ها بر اساس مقالات بررسی شده در این پژوهش

کشور	ابزارها و فناوری‌ها	ویژگی‌ها
ایران	جاسوسی سایبری، حملات تهاجمی، انتشار اطلاعات غلط	استراتژی‌های نامتقارن برای مقابله با محدودیت‌های فناوری و تحریم‌های اقتصادی.
روسیه	کارزارهای اطلاعات غلط، حملات باج‌افزاری، حاکمیت سایبری	استفادهٔ گسترده از ابزارهای اطلاعاتی برای نفوذ و ایجاد اختلال در سیستم‌های سیاسی و اقتصادی غرب.
رژیم اسرائیل	هوش مصنوعی، چارچوب‌های امنیتی پیشرفته، همکاری‌های بین‌المللی	نوآوری و رهبری جهانی در امنیت سایبری با تمرکز بر دفاع و توسعهٔ همکاری‌های بین‌المللی.

قوت‌ها و ضعف‌ها

- نقاط قوت:
  - ایران از استراتژی‌های نامتقارن برای بهره‌برداری از فضای سایبری در مقابله با قدرت‌های قوی‌تر استفاده می‌کند.
  - روسیه به‌طور موفقیت‌آمیزی از ابزارهای سایبری برای اعمال نفوذ در سیاست‌های جهانی بهره می‌برد.
  - رژیم اسرائیل با بهره‌گیری از فناوری‌های پیشرفته و همکاری‌های بین‌المللی، پیشرو در دفاع سایبری است.

- نقاط ضعف:
  - ایران با محدودیت دسترسی به فناوری‌های پیشرفته مواجه است.
  - روسیه به دلیل انزوای بین‌المللی و تحریم‌های غرب، با چالش‌هایی در توسعهٔ فناوری‌های جدید روبه‌رو است.
  - رژیم اسرائیل با تهدیدات مداوم از سوی دشمنان منطقه‌ای مانند ایران مواجه است.

۲. بررسی سیاست‌های دفاعی و تهاجمی در دیپلماسی سایبری ایران، روسیه و رژیم اسرائیل

ایران: تکیه بر سیاست‌های تهاجمی و مقاومت سایبری

سیاست‌های تهاجمی: ایران از سیاست‌های تهاجمی سایبری برای مقابله با دشمنان منطقه‌ای و بین‌المللی بهره می‌برد. این کشور از گروه‌های پیشرفتهٔ تهدید سایبری (APT) برای نفوذ به زیرساخت‌های حیاتی مانند سیستم‌های انرژی و مالی کشورهای منطقه‌ای استفاده کرده است. حملهٔ سایبری به شرکت نفتی آرامکو در سال ۲۰۱۲ و گسترش ویروس شمعون نمونه‌های بارز این سیاست‌ها هستند. همچنین، ایران از ابزارهای اطلاعاتی برای تضعیف دشمنان از طریق انتشار اطلاعات غلط و جنگ نرم بهره می‌برد (Abbasi, 2024; Baram, 2017).

سیاست‌های دفاعی: ایران با توجه به تهدیدات سایبری مداوم از سوی ایالات متحده و رژیم اسرائیل، سیاست‌های دفاعی خود را تقویت کرده است. استفاده از فایروال‌های ملی، تلاش برای استقلال سایبری و توسعهٔ زیرساخت‌های داخلی از جمله اقدامات ایران در این زمینه است. این سیاست‌ها با هدف کاهش آسیب‌پذیری در برابر حملات سایبری خارجی و افزایش توان بازدارندگی انجام می‌شود (Cohen, 2019; Aquino, 2022).

روسیه: تعادل میان تهاجم و دفاع

سیاست‌های تهاجمی: روسیه به‌طور گسترده از ابزارهای سایبری تهاجمی برای تأثیرگذاری بر سیاست‌های بین‌المللی استفاده می‌کند. کارزارهای اطلاعات غلط، نفوذ به سیستم‌های دموکراتیک و حملات باج‌افزاری نمونه‌هایی از سیاست‌های تهاجمی این کشور هستند. حملهٔ سایبری به شبکهٔ برق اوکراین در سال ۲۰۱۵ و دخالت در انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶ از اقدامات بارز روسیه در این زمینه است (Tsvetkova et al., 2022; Kari, 2019).

سیاست‌های دفاعی: روسیه با تأکید بر حاکمیت سایبری، تلاش می‌کند زیرساخت‌های دیجیتال خود را مستقل از اینترنت جهانی نگه دارد. پروژهٔ "RuNet" که شامل ایجاد یک اینترنت ملی و مستقل است، نمونه‌ای از این سیاست‌هاست. این رویکرد نه‌تنها برای دفاع در برابر حملات سایبری، بلکه برای کنترل بیشتر بر جریان اطلاعات داخلی و جلوگیری از نفوذ فرهنگی و سیاسی غرب طراحی شده است (Baezner, 2019).

رژیم اسرائیل: تمرکز بر دفاع فعال و تهاجم هدفمند

سیاست‌های تهاجمی: رژیم اسرائیل از سیاست‌های تهاجمی سایبری برای جلوگیری از تهدیدات منطقه‌ای و کاهش قدرت دشمنان خود استفاده می‌کند. برجسته‌ترین مثال، طراحی و گسترش ویروس استاکس‌نت برای هدف قرار دادن برنامهٔ هسته‌ای ایران است. این ویروس توانست به‌طور مؤثری فرآیند غنی‌سازی اورانیوم در ایران را مختل کند. علاوه بر این، رژیم اسرائیل از

ابزارهای جاسوسی پیشرفته برای نظارت بر فعالیت‌های دشمنان خود استفاده می‌کند (Frei, 2020; Baram, 2017).

سیاست‌های دفاعی: رژیم اسرائیل دارای یکی از پیشرفته‌ترین زیرساخت‌های امنیت سایبری در جهان است. این کشور از چارچوب‌های امنیتی پیشرفته و فناوری‌های هوش مصنوعی برای شناسایی و جلوگیری از تهدیدات استفاده می‌کند. همکاری‌های بین‌المللی رژیم اسرائیل در حوزهٔ امنیت سایبری نیز به تقویت دفاع سایبری این کشور کمک کرده است. برنامه‌هایی مانند همکاری با کشورهای اروپایی در زمینهٔ مقابله با جرایم سایبری از جملهٔ این اقدامات هستند (Chinn, 2015; Cohen, 2019).

جدول(۲-۳): مقایسهٔ سیاست‌های دفاعی و تهاجمی بر اساس مقالات بررسی شده در این پژوهش

کشور	سیاست‌های تهاجمی	سیاست‌های دفاعی
ایران	حملات به زیرساخت‌های حیاتی، انتشار اطلاعات غلط	فایروال ملی، توسعهٔ زیرساخت‌های داخلی
روسیه	حملات باج‌افزاری، نفوذ به انتخابات	ایجاد اینترنت ملی (RuNet)، کنترل بر جریان اطلاعات داخلی
رژیم اسرائیل	طراحی ویروس استاکس‌نت، جاسوسی سایبری	چارچوب‌های امنیتی پیشرفته، استفاده از هوش مصنوعی و همکاری‌های بین‌المللی

۳. شناسایی نقاط قوت و ضعف ایران، روسیه و رژیم اسرائیل در حوزهٔ قابلیت‌های سایبری

نقاط قوت ایران:

- استفاده از استراتژی‌های نامتقارن: ایران از ابزارهای نامتقارن برای مقابله با دشمنان قوی‌تر بهره می‌گیرد. این استراتژی‌ها شامل جاسوسی سایبری و نفوذ به زیرساخت‌های حیاتی مانند سیستم‌های انرژی و مالی کشورهای دشمن است. برای مثال، حمله به شرکت نفتی آرامکو نشان‌دهندهٔ توانایی ایران در اجرای حملات سایبری تأثیرگذار است (Abbasi, 2024; Baram, 2017).

• جاسوسی سایبری مؤثر: گروه‌های APT ایرانی مانند APT33 توانسته‌اند اطلاعات حساس دشمنان منطقه‌ای و بین‌المللی را به‌دست آورند. این اقدامات به ایران اجازه می‌دهد تهدیدات خارجی را پیش‌بینی و مدیریت کند(Cohen, 2019; Aquino, 2022).

• تأثیرگذاری بر افکار عمومی: ایران از شبکه‌های اجتماعی و اطلاعات سایبری برای تأثیرگذاری بر افکار عمومی جهانی و داخلی استفاده می‌کند. این استراتژی به ایران کمک کرده است تا تصویر خود را در برابر دشمنان بهبود بخشد و از جنگ نرم علیه دشمنان خود استفاده کند(Chinn, 2015).

نقاط ضعف ایران:

• محدودیت در فناوری‌های پیشرفته: تحریم‌های اقتصادی و محدودیت‌های بین‌المللی دسترسی ایران به فناوری‌های پیشرفتهٔ سایبری را محدود کرده و این کشور را مجبور به استفاده از راهکارهای کمتر پیشرفته کرده است(Kari, 2019).

• وابستگی به استراتژی‌های تهاجمی: نبود زیرساخت‌های قوی سایبری دفاعی باعث شده ایران به‌طور گسترده به حملات تهاجمی متکی باشد که ممکن است در بلندمدت پایدار نباشد(Tsvetkova et al., 2022).

نقاط قوت روسیه:

• ابزارهای تهاجمی پیشرفته: روسیه با استفاده از کارزارهای اطلاعات غلط و حملات باج‌افزاری، نقش برجسته‌ای در تهدید زیرساخت‌های حیاتی دشمنان جهانی خود ایفا کرده است. برای مثال، دخالت در انتخابات ایالات متحده و حمله به شبکهٔ برق اوکراین، نمونه‌های موفق از این اقدامات است(Baezner, 2019; Kari, 2019).

• ایجاد حاکمیت سایبری داخلی: روسیه با ایجاد پروژه‌هایی مانند "RuNet"، زیرساخت‌های داخلی خود را تقویت کرده و توانسته از نفوذ خارجی به سیستم‌های دیجیتال خود جلوگیری کند(Tsvetkova et al., 2022).

• توانایی‌های اطلاعاتی گسترده: روسیه با تحلیل کلان‌داده‌ها و استفاده از ابزارهای اطلاعاتی پیشرفته، توانسته است نقاط ضعف دشمنان خود را شناسایی و از آن‌ها بهره‌برداری کند (Frei, 2020).

نقاط ضعف روسیه:

• انزوای بین‌المللی: سیاست‌های تهاجمی روسیه منجر به تحریم‌ها و انزوای بین‌المللی شده است که توانایی این کشور در دسترسی به فناوری‌های جهانی را محدود می‌کند (Aquino, 2022).

• تهدیدات داخلی به دلیل محدودیت اینترنت: کنترل بیش‌ازحد بر اینترنت داخلی ممکن است موجب محدودیت در نوآوری و ایجاد نارضایتی داخلی شود (Kari, 2019).

نقاط قوت رژیم صهیونیستی:

• نوآوری و فناوری پیشرفته: رژیم اسرائیل با استفاده از هوش مصنوعی و فناوری‌های پیشرفتهٔ امنیت سایبری، توانسته است به یکی از رهبران جهانی در این حوزه تبدیل شود. این کشور از ابزارهای پیشرفته برای پیش‌بینی و جلوگیری از حملات سایبری استفاده می‌کند (Baram, 2017; Cohen, 2019).

• زیرساخت‌های قوی سایبری: چارچوب‌های امنیتی پیشرفتهٔ رژیم اسرائیل به این کشور اجازه داده است زیرساخت‌های حیاتی خود را در برابر حملات سایبری محافظت کند. مراکز نوآوری سایبری در رژیم اسرائیل نمونه‌ای از این زیرساخت‌ها هستند (Tsvetkova et al., 2022).

• همکاری‌های بین‌المللی: رژیم اسرائیل از طریق همکاری‌های گستردهٔ بین‌المللی، موقعیت خود را در امنیت سایبری جهانی تقویت کرده است. این کشور با اتحادیهٔ اروپا و دیگر کشورها در زمینهٔ مقابله با جرایم سایبری همکاری می‌کند (Frei, 2020).

نقاط ضعف رژیم صهیونیستی:

- تهدیدات مداوم منطقه‌ای: رژیم اسرائیل به‌طور مداوم با تهدیدات سایبری از سوی ایران و سایر دشمنان منطقه‌ای مواجه است که باعث افزایش هزینه‌ها و نیاز به بهبود مداوم در زیرساخت‌های سایبری می‌شود(Chinn, 2015).
- تعادل میان امنیت و آزادی: رژیم اسرائیل در تلاش است تا میان نیاز به امنیت سایبری و حفظ آزادی اینترنت تعادل برقرار کند، اما این تعادل در مواقعی به چالش کشیده می‌شود(Kari, 2019).

نقاط قوت و ضعف ایران، روسیه و رژیم اسرائیل در حوزهٔ سایبری نشان‌دهندهٔ تفاوت‌های ساختاری و استراتژیک آن‌ها است. ایران با تمرکز بر استراتژی‌های نامتقارن و روسیه با استفاده از ابزارهای تهاجمی پیشرفته، توانسته‌اند تهدیداتی جدی در سطح جهانی ایجاد کنند. در مقابل، رژیم اسرائیل با نوآوری و همکاری‌های بین‌المللی، نه تنها در دفاع، بلکه در پیشبرد دیپلماسی سایبری موفق بوده است. این تحلیل اهمیت تطبیق سیاست‌های سایبری با شرایط ژئوپلیتیکی هر کشور را برجسته می‌کند.

۴. ارائهٔ نمونه‌های عملی از حملات سایبری، دفاع سایبری و اقدامات بین‌المللی در حوزهٔ دیپلماسی سایبری

حملات سایبری

ایران: حملهٔ سایبری به شرکت نفتی آرامکو: در سال ۲۰۱۲، حملهٔ سایبری به شرکت نفتی آرامکو در عربستان سعودی که به انتشار ویروس «شمعون» منجر شد، به‌عنوان یکی از بزرگ‌ترین حملات سایبری در تاریخ شناخته شد. این حمله باعث تخریب داده‌های حدود ۳۰ هزار کامپیوتر در این شرکت شد و زیرساخت‌های انرژی عربستان را به‌شدت تحت تأثیر قرار داد. ایران به‌عنوان متهم اصلی این حمله شناخته شد و هدف آن کاهش توان عملیاتی دشمن و ارسال پیام قدرت سایبری بود(Abbasi, 2024; Baram, 2017).

روسیه: حملهٔ سایبری به شبکهٔ برق اوکراین: در سال ۲۰۱۵، روسیه با حمله‌ای سایبری به شبکهٔ برق اوکراین، توانست بخشی از سیستم توزیع برق این کشور را مختل کند. این حمله که با بدافزاری به نام "BlackEnergy" انجام شد، به‌عنوان یک نمونهٔ برجسته از استفاده از ابزارهای سایبری برای ایجاد بی‌ثباتی در کشورهای رقیب شناخته می‌شود. هدف این حمله، تضعیف زیرساخت‌های حیاتی اوکراین و اعمال فشار سیاسی بود (Tsvetkova et al., 2022; Kari, 2019).

رژیم اسرائیل: حملهٔ سایبری به برنامهٔ هسته‌ای ایران (استاکس‌نت): یکی از مشهورترین حملات سایبری، انتشار ویروس استاکس‌نت بود که با همکاری رژیم اسرائیل و ایالات متحده برای تخریب سانتریفیوژهای برنامهٔ هسته‌ای ایران طراحی شد. این ویروس توانست به‌طور مؤثر فرآیند غنی‌سازی اورانیوم را مختل کرده و برنامهٔ هسته‌ای ایران را به تأخیر بیندازد. این حمله نشان‌دهندهٔ توان بالای رژیم اسرائیل در استفاده از ابزارهای سایبری تهاجمی است (Cohen, 2019; Frei, 2020).

دفاع سایبری

ایران: توسعه فایروال ملی: ایران با توسعهٔ فایروال ملی و ایجاد شبکهٔ داخلی اینترنت، تلاش کردهٔ است از زیرساخت‌های حیاتی خود در برابر حملات خارجی محافظت کند. این رویکرد به ایران اجازه می‌دهد تا نفوذ خارجی به فضای دیجیتال خود را محدود کرده و کنترل بیشتری بر ارتباطات داخلی داشته باشد (Chinn, 2015; Aquino, 2022).

روسیه: پروژهٔ RuNet: روسیه با پروژه‌ای به نام "RuNet"، اینترنت داخلی و مستقل خود را توسعه داده است. این پروژه به این کشور اجازه می‌دهد که جریان اطلاعات داخلی را کاملاً تحت کنترل داشته باشد و در مواقع بحران، اینترنت جهانی را قطع کند. این اقدام بخشی از استراتژی روسیه برای کاهش وابستگی به زیرساخت‌های اینترنت بین‌المللی و افزایش توان دفاع سایبری است (Baezner, 2019; Tsvetkova et al., 2022).

رژیم اسرائیل: همکاری امنیت سایبری بین‌المللی: رژیم اسرائیل با ایجاد مراکز نوآوری سایبری و همکاری با کشورهای دیگر، توانسته است زیرساخت‌های سایبری خود را تقویت

کند. همکاری رژیم اسرائیل با کشورهای اروپایی و ایالات متحده در زمینهٔ مقابله با حملات سایبری، بخشی از استراتژی دفاعی این کشور برای حفاظت از زیرساخت‌های حیاتی و تبادل اطلاعات دربارهٔ تهدیدات سایبری است (Frei, 2020; Baram, 2017).

اقدامات بین‌المللی

ایران: مقاومت در برابر تحریم‌های سایبری: ایران از دیپلماسی سایبری برای مقابله با تحریم‌های اقتصادی و سایبری بهره می‌گیرد. تلاش‌های این کشور برای نفوذ به سیستم‌های بانکی و مالی کشورهای غربی، بخشی از این اقدامات است. همچنین، ایران در سازمان‌های بین‌المللی مانند اتحادیهٔ مخابرات بین‌المللی (ITU) به دنبال ترویج قوانین و سیاست‌هایی است که از حاکمیت دیجیتال کشورها حمایت کنند (Abbasi, 2024).

روسیه: نفوذ در سیاست‌های سایبری جهانی: روسیه از طریق حضور فعال در سازمان‌های بین‌المللی مانند سازمان ملل، تلاش می‌کند قوانین جهانی فضای سایبری را به نفع خود تغییر دهد. این کشور پیشنهادهایی مانند معاهدات عدم استفاده از سلاح‌های سایبری را مطرح کرده است، در حالی که در عمل به استفاده از ابزارهای سایبری برای تأثیرگذاری بر سیاست‌های جهانی ادامه می‌دهد (Kari, 2019; Tsvetkova et al., 2022).

رژیم اسرائیل: ایجاد استانداردهای امنیت سایبری: رژیم اسرائیل با رهبری در توسعهٔ استانداردهای امنیت سایبری، نقش مهمی در تنظیم قوانین بین‌المللی این حوزه ایفا کرده است. این کشور با مشارکت در کنفرانس‌های جهانی و ارائهٔ پیشنهادهای عملی برای مدیریت جرایم سایبری، به شکل‌دهی سیاست‌های سایبری جهانی کمک کرده است. علاوه بر این، رژیم اسرائیل از دیپلماسی سایبری برای گسترش روابط تجاری در حوزهٔ فناوری سایبری استفاده می‌کند (Cohen, 2019; Frei, 2020).

این نمونه‌ها نشان می‌دهند که حملات سایبری، دفاع سایبری، و اقدامات بین‌المللی در سه کشور ایران، روسیه و رژیم اسرائیل به‌شکل متفاوتی طراحی و اجرا شده‌اند. در حالی که ایران از ابزارهای نامتقارن برای مقابله با محدودیت‌ها استفاده می‌کند، روسیه با ابزارهای

پیشرفته به دنبال تغییر نظم جهانی است. از سوی دیگر، رژیم اسرائیل با تمرکز بر نوآوری و همکاری‌های بین‌المللی، نقش رهبری در امنیت سایبری ایفا می‌کند. این تفاوت‌ها نشان‌دهندهٔ تنوع در رویکردهای سایبری بر اساس شرایط ژئوپلیتیکی و اهداف ملی است.

بحث و بررسی

تحلیل مفهوم دیپلماسی سایبری در سه کشور

ایران: دیپلماسی سایبری به‌عنوان ابزاری برای مقاومت و نفوذ منطقه‌ای: ایران مفهوم دیپلماسی سایبری را به‌طور ویژه در چارچوب «مقاومت سایبری» و مقابله با نفوذ غرب تعریف کرده است. این مفهوم در سیاست‌های ایران به معنای ترکیبی از ابزارهای دفاعی و تهاجمی برای حفاظت از منافع ملی و گسترش نفوذ منطقه‌ای تعبیر می‌شود. ایران از دیپلماسی سایبری برای مقابله با تحریم‌های اقتصادی و پاسخ به حملات سایبری دشمنان استفاده کرده است. در این راستا، استفاده از حملات سایبری هدفمند علیه زیرساخت‌های دشمنان منطقه‌ای، مانند شرکت نفتی آرامکو، به‌عنوان بخشی از سیاست خارجی سایبری ایران شناخته می‌شود. دیپلماسی سایبری ایران همچنین شامل استفاده از شبکه‌های اجتماعی برای انتشار پیام‌های سیاسی و تقویت نفوذ ایدئولوژیک در میان مخاطبان منطقه‌ای و بین‌المللی است (Abbasi, 2024; Baram, 2017).

روسیه: دیپلماسی سایبری به‌عنوان ابزاری برای نفوذ ژئوپلیتیکی: روسیه دیپلماسی سایبری را به‌عنوان بخشی از استراتژی کلان خود برای گسترش نفوذ در نظام جهانی و مقابله با نفوذ غرب می‌بیند. درک روسیه از دیپلماسی سایبری بر اساس نظریه‌های قدرت سخت و نرم است که در آن ابزارهای سایبری برای اعمال فشار، ایجاد بی‌ثباتی در کشورهای رقیب، و تقویت موقعیت استراتژیک خود استفاده می‌شوند. نمونه‌ای از این سیاست، حملات سایبری گسترده به زیرساخت‌های کشورهای اروپایی و دخالت در انتخابات ریاست‌جمهوری ایالات متحده است که هدف آن تضعیف اعتماد عمومی به نهادهای دموکراتیک و برجسته‌سازی نقاط ضعف غرب بوده است. روسیه همچنین بر مفهوم «حاکمیت سایبری» تأکید دارد و تلاش می‌کند از طریق

ایجاد اینترنت داخلی، کنترل کامل بر فضای سایبری خود داشته باشد (Tsvetkova et al., 2022; Frei, 2020).

رژیم اسرائیل: دیپلماسی سایبری به‌عنوان ابزاری برای نوآوری و دفاع: در رژیم اسرائیل، دیپلماسی سایبری به‌عنوان یک ابزار نوآورانه برای دفاع از زیرساخت‌های حیاتی و تقویت روابط بین‌المللی تعریف شده است. این کشور مفهوم دیپلماسی سایبری را به گونه‌ای توسعه داده است که شامل ایجاد استانداردهای بین‌المللی امنیت سایبری و تقویت همکاری‌های چندجانبه باشد. رژیم اسرائیل به‌طور خاص از فناوری‌های پیشرفته‌ای مانند هوش مصنوعی و بلاکچین برای تحلیل داده‌های سایبری و پیش‌بینی تهدیدات استفاده می‌کند. علاوه بر این، پروژه‌هایی مانند همکاری با اتحادیهٔ اروپا و ایالات متحده در حوزهٔ امنیت سایبری نشان‌دهندهٔ تعریف گسترده‌تری از دیپلماسی سایبری است که به‌طور هم‌زمان شامل دفاع و تعامل بین‌المللی می‌شود (Cohen, 2019; Baram, 2017).

مقایسهٔ تطبیقی مفاهیم: مقایسهٔ سه کشور نشان می‌دهد که در حالی که ایران و روسیه بیشتر بر ابعاد تهاجمی دیپلماسی سایبری تمرکز دارند، رژیم اسرائیل دیپلماسی سایبری را به‌عنوان ابزاری برای دفاع پیشرفته و گسترش همکاری‌های بین‌المللی توسعه داده است. روسیه با تأکید بر جنگ اطلاعاتی و کنترل سایبری داخلی، دیپلماسی سایبری را به ابزار قدرت نرم خود تبدیل کرده است، در حالی که ایران مفهوم دیپلماسی سایبری را عمدتاً در چارچوب مقابله با فشارهای خارجی و حفظ هویت ملی گسترش داده است. رژیم اسرائیل، برخلاف دو کشور دیگر، بیشتر به دنبال استفاده از دیپلماسی سایبری برای تثبیت موقعیت جهانی خود در حوزهٔ فناوری است (Tsvetkova et al., 2022; Abbasi, 2024).

تحول در مفهوم دیپلماسی سایبری: تحول در مفهوم دیپلماسی سایبری در این سه کشور به‌وضوح نشان می‌دهد که هر کشور بر اساس نیازهای ژئوپلیتیکی و شرایط داخلی خود، تعریف خاصی از این مفهوم ارائه داده است. در حالی که ایران به‌دنبال ایجاد موازنه در برابر قدرت‌های جهانی است، روسیه از دیپلماسی سایبری برای اعمال فشار و تغییر نظم جهانی استفاده می‌کند. رژیم اسرائیل نیز با تکیه بر برتری فناوری و استفاده از ابزارهای دیجیتال،

نقش فعالی در شکل‌دهی به استانداردهای جهانی این حوزه ایفا می‌کند (Chinn, 2015; Frei, 2020).

تناقض در استفاده از ابزارهای سایبری: بررسی موضع‌گیری‌ها و اقدامات عملی

روسیه: حمایت از مقررات بین‌المللی در مقابل اقدامات تهاجمی

موضع‌گیری رسمی: روسیه به‌عنوان یکی از فعال‌ترین کشورها در عرصهٔ دیپلماسی سایبری، همواره از ایجاد قوانین بین‌المللی برای مدیریت فضای سایبری حمایت کرده است. این کشور در سازمان ملل پیشنهادهایی مانند معاهدهٔ عدم استفاده از سلاح‌های سایبری و ایجاد چارچوبی برای اعتمادسازی در فضای مجازی ارائه داده است. این موضع‌گیری‌ها نشان‌دهندهٔ تلاش روسیه برای معرفی خود به‌عنوان بازیگری مسئول در فضای بین‌المللی است (Tsvetkova et al., 2022).

اقدامات عملی: در مقابل، روسیه به‌طور گسترده از ابزارهای سایبری برای تضعیف نظام‌های دموکراتیک غربی و نفوذ در زیرساخت‌های حیاتی استفاده کرده است. یکی از برجسته‌ترین نمونه‌ها، دخالت سایبری در انتخابات ریاست‌جمهوری ایالات متحده در سال ۲۰۱۶ است. این اقدام با هدف ایجاد بی‌اعتمادی به نظام انتخاباتی آمریکا و تضعیف وحدت داخلی این کشور انجام شد، که کاملاً با موضع رسمی روسیه در سازمان‌های بین‌المللی تناقض دارد (Kari, 2019; Baezner, 2019).

ایران: تأکید بر حاکمیت سایبری در برابر حملات تهاجمی

موضع‌گیری رسمی: ایران در مجامع بین‌المللی مانند اتحادیهٔ مخابرات بین‌المللی (ITU)، از اصول حاکمیت سایبری و ضرورت حفاظت از حریم دیجیتال کشورها حمایت کرده است. این کشور بر لزوم تدوین قوانین بین‌المللی برای جلوگیری از استفادهٔ تهاجمی از فضای سایبری تأکید دارد و حملات سایبری را به‌عنوان تهدیدی برای امنیت بین‌المللی معرفی می‌کند (Abbasi, 2024).

اقدامات عملی: با این حال، اقدامات ایران در فضای سایبری تناقض آشکاری با این مواضع دارد. حمله به زیرساخت‌های نفتی آرامکو در عربستان سعودی و نفوذ به سیستم‌های انرژی و مالی کشورهای غربی نشان‌دهندهٔ استفادهٔ گستردهٔ ایران از ابزارهای تهاجمی سایبری برای پیشبرد اهداف منطقه‌ای و بین‌المللی است. این تناقض، موضع ایران را در زمینهٔ مسئولیت‌پذیری بین‌المللی در فضای سایبری تضعیف می‌کند (Chinn, 2015; Baram, 2017).

رژیم اسرائیل: تأکید بر همکاری‌های بین‌المللی در مقابل حملات سایبری تهاجمی

موضع‌گیری رسمی: رژیم اسرائیل در سطح بین‌المللی، به‌عنوان یکی از مدافعان اصلی همکاری‌های چندجانبه در زمینهٔ امنیت سایبری شناخته می‌شود. این کشور از پروژه‌هایی مانند استانداردسازی قوانین سایبری و ایجاد چارچوب‌های جهانی برای مقابله با جرایم سایبری حمایت کرده است. رژیم اسرائیل همچنین به‌طور فعال در کنفرانس‌های بین‌المللی سایبری شرکت می‌کند و خواستار همکاری جهانی برای مقابله با تهدیدات سایبری است (Frei, 2020; Cohen, 2019).

اقدامات عملی: در مقابل، اقدامات تهاجمی رژیم اسرائیل در فضای سایبری، به‌ویژه علیه برنامهٔ هسته‌ای ایران، به‌طور کامل با این مواضع همخوانی ندارد. طراحی و اجرای ویروس استاکس‌نت، که برنامهٔ غنی‌سازی اورانیوم ایران را مختل کرد، نمونه‌ای از استفادهٔ تهاجمی رژیم اسرائیل از فضای سایبری است. این اقدام اگرچه به‌عنوان دفاع پیشگیرانه توجیه می‌شود، اما با رویکرد رسمی رژیم اسرائیل در زمینهٔ تقویت همکاری‌های بین‌المللی و احترام به حاکمیت دیجیتال تناقض دارد (Baram, 2017).

رویکردهای چندگانه در تنظیم قوانین سایبری: یکی دیگر از تناقضات مهم، مواضع سه کشور در تنظیم قوانین سایبری است. در حالی که روسیه، ایران و رژیم اسرائیل به لزوم تدوین چارچوب‌های قانونی برای مدیریت فضای سایبری تأکید می‌کنند، هر یک به شیوه‌ای متفاوت از این فضا برای تضعیف دیگر کشورها استفاده کرده‌اند. این تناقض‌ها نشان‌دهندهٔ شکاف میان تعهدات رسمی و رفتار عملی در فضای بین‌المللی است. برای مثال، ایران و روسیه بر لزوم

احترام به حاکمیت دیجیتال تأکید دارند، اما در عمل از حملات سایبری برای نقض این حاکمیت در کشورهای دیگر استفاده می‌کنند (Aquino, 2022; Tsvetkova et al., 2022).

تأثیر تناقضات بر نظم بین‌المللی: این تناقضات نه‌تنها اعتبار کشورها در سازمان‌های بین‌المللی را تحت‌الشعاع قرار می‌دهد، بلکه به بی‌اعتمادی عمومی در تنظیم چارچوب‌های جهانی برای مدیریت فضای سایبری منجر می‌شود. کشورهای غربی، به‌ویژه ایالات متحده و اتحادیهٔ اروپا، بارها اقدامات روسیه و ایران را به‌عنوان تهدیدی برای نظم بین‌المللی معرفی کرده‌اند. در عین حال، رژیم اسرائیل با وجود نقش پیشرو در امنیت سایبری، به دلیل اقدامات تهاجمی خود با انتقادات مشابهی مواجه شده است (Frei, 2020; Cohen, 2019).

مقایسهٔ نقش فناوری‌های نوین در سیاست‌های سایبری ایران، روسیه و رژیم اسرائیل

هوش مصنوعی در سیاست‌های سایبری: هوش مصنوعی (AI) در دیپلماسی سایبری این سه کشور کاربردهای متنوعی دارد. رژیم اسرائیل از AI برای شناسایی تهدیدات سایبری و توسعهٔ سامانه‌های پیش‌بینی حملات استفاده می‌کند. این کشور توانسته است به یکی از پیشروترین کشورها در امنیت سایبری تبدیل شود (Cohen, 2019; Frei, 2020). روسیه از AI در تحلیل کلان‌داده‌ها بهره‌برداری کرده و حملات پیچیده‌ای مانند نفوذ به انتخابات ایالات متحده را طراحی کرده است (Tsvetkova et al., 2022). ایران نیز با وجود محدودیت‌های تکنولوژیکی، AI را برای مدیریت شبکه‌های اجتماعی و توسعهٔ ابزارهای دفاعی به‌کار گرفته است (Abbasi, 2024).

بلاکچین و تحولات سایبری: بلاکچین نقش مهمی در امنیت و سیاست‌های مالی سایبری ایفا می‌کند. رژیم اسرائیل از این فناوری برای تأمین امنیت داده‌ها، قراردادهای هوشمند، و سیستم‌های رأی‌گیری دیجیتال بهره می‌برد (Baram, 2017). روسیه با توسعهٔ روبل دیجیتال، از بلاکچین برای کاهش وابستگی به سیستم‌های مالی غرب استفاده می‌کند (Baezner, 2019). ایران نیز این فناوری را برای مقابله با تحریم‌های اقتصادی و تقویت

زیرساخت‌های مالی سایبری به‌کار گرفته است، اگرچه هنوز در توسعهٔ گستردهٔ آن با چالش‌های اساسی روبه‌رو است (Kari, 2019).

اینترنت اشیا و امنیت زیرساخت‌ها: اینترنت اشیا (IoT) در هر سه کشور برای مدیریت زیرساخت‌ها و تقویت امنیت سایبری کاربرد دارد. رژیم اسرائیل با توسعهٔ فناوری‌های IoT، توانسته است امنیت زیرساخت‌های انرژی، حمل‌ونقل، و بهداشت خود را افزایش دهد (Frei, 2020). روسیه IoT را برای کنترل زیرساخت‌های نظامی و صنعتی به‌کار گرفته و با ترکیب آن با کلان‌داده‌ها، توانایی‌های خود را در پیشگیری از تهدیدات ارتقا داده است (Tsvetkova et al., 2022). ایران نیز IoT را برای مدیریت زیرساخت‌های انرژی و شهری مورد استفاده قرار می‌دهد، اما دسترسی محدود به فناوری پیشرفته، استفاده از این ابزار را برای ایران دشوار کرده است (Chinn, 2015).

تحلیل داده‌های کلان: تحلیل کلان‌داده‌ها (Big Data) در شناسایی و مدیریت تهدیدات سایبری نقش کلیدی ایفا می‌کند. روسیه با تحلیل داده‌های کلان، نقاط ضعف دشمنان خود را شناسایی کرده و در جنگ اطلاعاتی موفقیت‌های قابل توجهی کسب کرده است (Tsvetkova et al., 2022). ایران از داده‌های کلان برای نظارت بر فعالیت‌های داخلی و انتشار پیام‌های هدفمند در شبکه‌های اجتماعی بهره می‌برد (Abbasi, 2024). رژیم اسرائیل نیز با ترکیب کلان‌داده‌ها و هوش مصنوعی، سامانه‌هایی پیشرفته برای مقابله با تهدیدات سایبری ایجاد کرده است (Cohen, 2019).

هوش مصنوعی و حملات سایبری: رویکرد روسیه به استفاده از AI در طراحی حملات سایبری مانند دخالت در انتخابات آمریکا و نفوذ به سیستم‌های مالی اروپا، نشان‌دهندهٔ قدرت این فناوری در جنگ سایبری است (Tsvetkova et al., 2022). رژیم اسرائیل AI را عمدتاً برای دفاع سایبری استفاده می‌کند، اما حملاتی مانند استاکس‌نت نیز نشان‌دهندهٔ توان تهاجمی این کشور است (Baram, 2017; Frei, 2020). ایران از AI برای حملات با مقیاس کوچک‌تر و نفوذ در شبکه‌های اطلاعاتی کشورهای منطقه‌ای استفاده کرده است (Abbasi, 2024).

تفاوت در تأثیر فناوری‌ها: فناوری‌های نوین بر اساس نیازها و اولویت‌های سه کشور به‌طور متفاوتی به کار گرفته می‌شوند. ایران از فناوری‌ها برای جبران محدودیت‌های تکنولوژیکی و مقابله با فشارهای اقتصادی استفاده می‌کند (Chinn, 2015). روسیه این ابزارها را برای گسترش نفوذ جهانی و تضعیف رقبا به کار می‌گیرد (Baezner, 2019). رژیم اسرائیل با استفاده از فناوری‌های پیشرفته و همکاری‌های بین‌المللی، به‌دنبال تثبیت موقعیت خود به‌عنوان رهبر جهانی امنیت سایبری است (Cohen, 2019).

نقش فضای سایبری در سیاست‌های آینده

تحول در روابط بین‌المللی: فضای سایبری در حال تبدیل‌شدن به یکی از ارکان اصلی روابط بین‌المللی است. کشورها از این فضا برای اعمال نفوذ در سیاست‌های جهانی و تغییر معادلات قدرت استفاده می‌کنند. برای مثال، روسیه با استفاده از ابزارهای سایبری توانسته است تأثیر قابل توجهی بر انتخابات و فرآیندهای دموکراتیک کشورهای غربی بگذارد. در آینده، پیش‌بینی می‌شود که جنگ اطلاعاتی و استفاده از کارزارهای اطلاعات غلط برای تضعیف اعتماد عمومی به نهادهای سیاسی در سطح بین‌المللی افزایش یابد (Tsvetkova et al., 2022; Frei, 2020).

دیپلماسی دیجیتال: ابزار مذاکره و همکاری: فضای سایبری به بستری برای گسترش دیپلماسی دیجیتال تبدیل شده است. در آینده، کشورها از این فضا برای تسهیل مذاکرات، حل منازعات، و ایجاد چارچوب‌های همکاری در حوزه‌های مختلف استفاده خواهند کرد. رژیم اسرائیل به‌عنوان یکی از پیشروان امنیت سایبری، توانسته است با ایجاد مراکز نوآوری و استانداردهای امنیتی، همکاری‌های بین‌المللی خود را تقویت کند. انتظار می‌رود که کشورهای بیشتری از این مدل برای تقویت روابط خود در سطح جهانی استفاده کنند (Cohen, 2019; Baram, 2017).

امنیت سایبری به‌عنوان اولویت استراتژیک: فضای سایبری به حوزه‌ای حیاتی برای امنیت ملی تبدیل شده است. در آینده، امنیت سایبری نه‌تنها برای دفاع از زیرساخت‌های حیاتی،

بلکه به‌عنوان یکی از ابزارهای اصلی بازدارندگی و تهاجم مورد استفاده قرار خواهد گرفت. روسیه با ایجاد اینترنت مستقل (RuNet) و توسعهٔ ابزارهای پیشرفتهٔ سایبری، در تلاش است تا کنترل کامل بر فضای سایبری خود داشته باشد. در مقابل، رژیم اسرائیل بر تقویت دفاع سایبری و استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی برای پیش‌بینی تهدیدات تمرکز دارد. ایران نیز به دنبال استقلال سایبری و کاهش وابستگی به فناوری‌های خارجی است (Tsvetkova et al., 2022; Kari, 2019).

رقابت در توسعهٔ فناوری‌های نوین: فناوری‌هایی مانند هوش مصنوعی، بلاکچین، و اینترنت اشیا (IoT) نقش فزاینده‌ای در سیاست‌های آیندهٔ کشورها ایفا خواهند کرد. رژیم اسرائیل در توسعهٔ فناوری‌های پیشرفته برای امنیت سایبری پیشتاز است و پیش‌بینی می‌شود که در آینده نیز نقش بیشتری در ایجاد استانداردهای جهانی ایفا کند. روسیه از این فناوری‌ها برای تقویت قدرت سایبری خود و گسترش نفوذ در کشورهای همسایه استفاده خواهد کرد. ایران نیز با تمرکز بر توسعهٔ فناوری‌های بومی، تلاش می‌کند تا توانایی خود در مدیریت فضای سایبری را ارتقا دهد (Baram, 2017; Aquino, 2022).

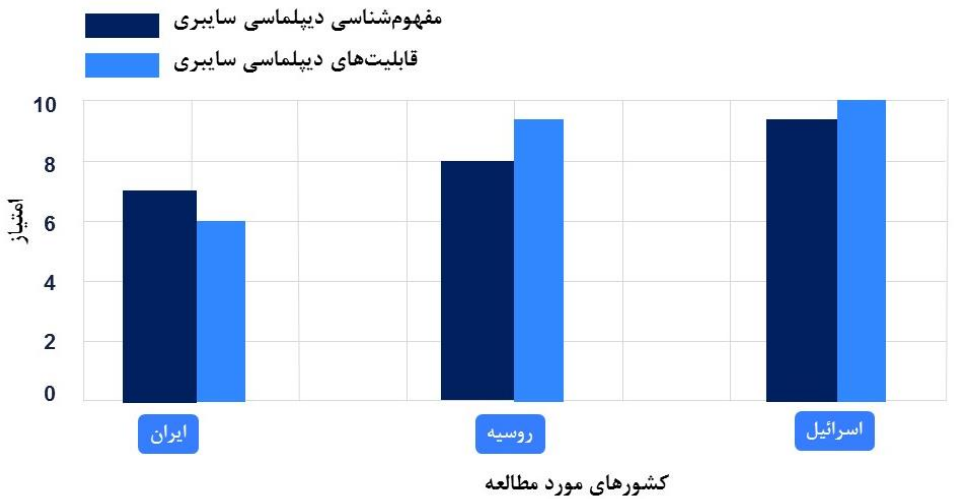
چالش‌های حاکمیت سایبری و تنظیم مقررات: یکی از چالش‌های بزرگ آینده، تنظیم قوانین بین‌المللی برای مدیریت فضای سایبری است. روسیه و ایران از مفهوم «حاکمیت سایبری» برای کنترل کامل بر فضای دیجیتال داخلی خود حمایت می‌کنند، در حالی که رژیم اسرائیل به دنبال تنظیم استانداردهای بین‌المللی برای ایجاد یک فضای باز و ایمن است. این تفاوت‌ها می‌تواند به تضادهای بیشتری در مذاکرات جهانی منجر شود. پیش‌بینی می‌شود که تلاش‌ها برای تدوین معاهدات جهانی در زمینهٔ استفادهٔ مسئولانه از فضای سایبری افزایش یابد (Tsvetkova et al., 2022; Frei, 2020).

افزایش اهمیت دیپلماسی سایبری در منازعات منطقه‌ای: فضای سایبری در آینده نه تنها به‌عنوان ابزاری برای رقابت بین قدرت‌های بزرگ، بلکه در منازعات منطقه‌ای نیز اهمیت بیشتری پیدا خواهد کرد. ایران از فضای سایبری برای تقویت نفوذ خود در خاورمیانه و مقابله با فشارهای غرب استفاده خواهد کرد. روسیه تلاش می‌کند تا از این فضا برای ایجاد بی‌ثباتی در مناطق

استراتژیک استفاده کند. رژیم اسرائیل نیز با استفاده از دیپلماسی سایبری، به‌دنبال کاهش تهدیدات منطقه‌ای و تقویت امنیت ملی خود خواهد بود (Baram, 2017; Kari, 2019).

جدول(۱-۴): مقایسهٔ دیپلماسی سایبر و قابلیت‌های سایبری ایران، روسیه و رژیم اسرائیل

جنبه	ایران	روسیه	رژیم اسرائیل
تمرکز استراتژیک	توانمندی‌های دفاعی و تهاجمی با تمرکز بر نفوذ منطقه‌ای و مقابله با قدرت‌های غربی	استفاده از توانمندی‌های سایبری به‌عنوان ابزاری برای نفوذ استراتژیک جهانی	استراتژی‌های پیشگیرانه و دفاعی برای حفظ برتری تکنولوژیکی و امنیت منطقه‌ای
اهداف اصلی	حفاظت از حاکمیت ملی، مبارزه با مخالفان داخلی و مقابله با تهدیدهای آمریکا و رژیم اسرائیل	حفظ تسلط اطلاعاتی، تضعیف دموکراسی‌های غربی و تضمین ثبات سیاسی داخلی	جلوگیری از حملات سایبری به زیرساخت‌های حیاتی و تضعیف دشمنان منطقه‌ای مانند ایران
ابزارهای سایبری	جاسوسی سایبری، خرابکاری (حملات به زیرساخت‌های حیاتی) و تبلیغات در شبکه‌های اجتماعی	کارزارهای اطلاعات غلط، حملات باج‌افزار و تهدیدهای پیشرفته علیه زیرساخت‌های غربی	ادغام هوش مصنوعی پیشرفته، چارچوب‌های امنیتی قوی و ابزارهای جاسوسی سایبری تهاجمی
چالش‌ها	تحریم‌های اقتصادی که دسترسی به فناوری را محدود می‌کند؛ اتکا به استراتژی‌های نامتقارن	انزوای تکنولوژیک از غرب و تحریم‌های بین‌المللی	تهدیدهای مداوم از سوی دشمنان منطقه‌ای مانند ایران و توازن میان نیازهای عملیاتی و هنجارهای جهانی
فرصت‌ها	گسترش نفوذ منطقه‌ای و بهره‌برداری از عدم تقارن برای مقابله با دشمنان قوی‌تر	تثبیت حاکمیت سایبری و استفاده از فضای سایبری برای مقابله با محدودیت‌های نظامی سنتی	پیشرو بودن در نوآوری امنیت سایبری و تقویت همکاری‌های بین‌المللی برای بهره‌برداری راهبردی



نمودار(۱-۴):مقایسه‌ای‌از‌مفهوم‌شناسی‌دیپلماسی‌سایبری‌و‌قابلیت‌های‌سایبری‌سه‌کشور‌ایران، روسیه‌و‌رژیم‌صهیونیستی

در نمودار بالا، عملکرد سه کشور ایران، روسیه و رژیم اسرائیل در دو جنبهٔ «مفهوم‌شناسی دیپلماسی‌سایبر» و «قابلیت‌های‌دیپلماسی‌سایبری» مقایسه شده‌است.

- رژیم اسرائیل: بالاترین امتیاز را در هر دو حوزهٔ دارد که نشان‌دهندهٔ درک بهتر و استفادهٔ بهینه‌تر از دیپلماسی‌سایبری‌است.
- روسیه: در مفهوم‌شناسی و قابلیت‌ها عملکرد خوبی داشته، اما نسبت به رژیم اسرائیل‌کمی‌پایین‌تر‌است.
- ایران:امتیاز‌پایین‌تری‌در‌هر‌دو‌بخش‌داردکه‌نشان‌می‌دهدهمچنان‌در‌حال‌توسعهٔ درک‌واستفاده‌از‌دیپلماسی‌سایبری‌است.

این‌داده‌ها‌بر‌اساس‌تحلیل‌مقالات‌ومنابع‌در‌این‌پژوهش‌ارائه‌شده‌اند.

نتیجه‌گیری

دیپلماسی سایبری به‌عنوان یکی از حوزه‌های کلیدی در روابط بین‌المللی قرن ۲۱، نقش برجسته‌ای در سیاست‌های خارجی کشورها ایفا می‌کند. تحلیل سیاست‌های سایبری ایران، روسیه و رژیم اسرائیل نشان داد که این سه کشور با توجه به شرایط ژئوپلیتیکی، اهداف ملی و سطح دسترسی به فناوری، از دیپلماسی سایبری به‌شیوه‌ای متمایز استفاده می‌کنند. ایران از فضای سایبری برای مقابله با فشارهای خارجی، تقویت نفوذ منطقه‌ای، و بهره‌برداری از ابزارهای نامتقارن استفاده می‌کند. روسیه، با تأکید بر جنگ اطلاعاتی و کنترل کامل بر فضای سایبری داخلی، به‌دنبال بازتعریف نظم جهانی و کاهش نفوذ غرب است. در مقابل، رژیم اسرائیل با رویکردی نوآورانه، از دیپلماسی سایبری برای تقویت همکاری‌های بین‌المللی، حفاظت از زیرساخت‌های حیاتی و ترویج امنیت جهانی بهره می‌گیرد.

فناوری‌های نوین مانند هوش مصنوعی، بلاکچین، و اینترنت اشیا، به‌طور چشم‌گیری مفهوم دیپلماسی سایبری را گسترش داده‌اند. این فناوری‌ها، کشورها را قادر ساخته‌اند تا از فضای سایبری به‌عنوان ابزاری برای دفاع، حمله، و تعاملات دیپلماتیک استفاده کنند. با این حال، تنش‌ها و تناقضات میان مواضع رسمی و اقدامات عملی، چالش‌هایی جدی برای ایجاد اعتماد و تنظیم قوانین بین‌المللی در این حوزه به همراه داشته است.

در نهایت، فضای سایبری به‌سرعت در حال تبدیل شدن به یکی از ارکان اصلی قدرت ملی و نظم جهانی است. در آینده، کشورها باید با تعادل میان اقدامات تهاجمی و دفاعی، از این فضا برای پیشبرد اهداف مشترک و مقابله با تهدیدات جهانی استفاده کنند. بهبود همکاری‌های بین‌المللی و تدوین چارچوب‌های حقوقی جامع، برای مدیریت بهتر فضای سایبری ضروری خواهد بود. این حوزه، به دلیل پیچیدگی و تأثیرگذاری بالای خود، نیازمند تحقیقات بیشتر و

سیاست‌گذاری‌های دقیق‌تری است تا به بستری برای همکاری جهانی و نه رقابت و منازعه تبدیل شود.

پیشنهادات

تدوین چارچوب‌های حقوقی بین‌المللی: کشورها باید با همکاری یکدیگر چارچوب‌های حقوقی جامع و الزام‌آوری را برای مدیریت فضای سایبری تدوین کنند. این چارچوب‌ها می‌توانند شامل قوانین منع حملات سایبری، استانداردهای امنیت سایبری، و معاهدات حفاظت از داده‌ها باشند. چنین اقداماتی می‌تواند به کاهش تناقضات میان گفتار و رفتار کشورهای مختلف کمک کرده و اعتماد جهانی را در این حوزه تقویت کند.

تقویت همکاری‌های بین‌المللی: ایجاد نهادهای بین‌المللی یا گسترش نقش سازمان‌هایی مانند سازمان ملل برای مدیریت بحران‌های سایبری و تقویت همکاری‌های چندجانبه ضروری است. رژیم اسرائیل با تجربهٔ موفق خود در ایجاد همکاری‌های سایبری می‌تواند الگویی برای سایر کشورها باشد. در این راستا، مشارکت ایران و روسیه در مذاکرات بین‌المللی نیز می‌تواند به کاهش تنش‌ها و افزایش شفافیت کمک کند.

- سرمایه‌گذاری در فناوری‌های نوین: کشورها باید سرمایه‌گذاری بیشتری در توسعه و بهره‌برداری از فناوری‌های نوین مانند هوش مصنوعی، بلاکچین، و اینترنت اشیا انجام دهند. این فناوری‌ها می‌توانند برای بهبود دفاع سایبری و ایجاد ابزارهای پیشرفته برای مدیریت تهدیدات استفاده شوند. در این زمینه، ایران می‌تواند با تقویت توانایی‌های بومی و کاهش وابستگی به فناوری خارجی، بهره‌وری بیشتری از فضای سایبری داشته باشد.
- آموزش و ظرفیت‌سازی در حوزهٔ سایبری: آموزش کارشناسان سایبری و ایجاد ظرفیت‌های انسانی در این حوزه باید در اولویت برنامه‌های ملی قرار گیرد. کشورها می‌توانند با ایجاد دانشگاه‌ها و مراکز تحقیقاتی پیشرفته، نسل جدیدی از

متخصصان سایبری را پرورش دهند. این اقدام نه‌تنها به تقویت دفاع سایبری کمک می‌کند، بلکه توان رقابتی کشورها در عرصهٔ بین‌المللی را افزایش می‌دهد.

- ایجاد سامانه‌های بازدارندگی سایبری: کشورها باید سامانه‌های بازدارندگی مؤثری طراحی کنند تا توان پاسخ‌گویی به حملات سایبری را داشته باشند. بازدارندگی سایبری می‌تواند شامل استراتژی‌هایی مانند شناسایی مهاجمان، حملات متقابل هدفمند، و اعمال تحریم‌های اقتصادی علیه عاملان حملات سایبری باشد. این اقدامات می‌توانند هزینهٔ حملات سایبری را برای مهاجمان افزایش داده و امنیت سایبری جهانی را بهبود بخشند.
- ارتقای شفافیت در فضای سایبری: برای کاهش تنش‌ها و ایجاد اعتماد، کشورها باید اطلاعات بیشتری دربارهٔ سیاست‌های سایبری خود ارائه دهند. شفافیت در زمینهٔ اهداف، قابلیت‌ها، و استراتژی‌های سایبری می‌تواند به کاهش سوءتفاهم‌ها و پیشگیری از منازعات کمک کند. این رویکرد به‌ویژه برای ایران و روسیه که اغلب در معرض اتهامات تهاجمی قرار دارند، از اهمیت بالایی برخوردار است.
- ایجاد چارچوب‌های همکاری منطقه‌ای: علاوه بر تعاملات بین‌المللی، کشورهای منطقه‌ای می‌توانند با ایجاد چارچوب‌های همکاری سایبری، از منافع مشترک خود در برابر تهدیدات سایبری محافظت کنند. برای مثال، ایران می‌تواند از طریق همکاری با کشورهای منطقه‌ای خاورمیانه در حوزهٔ امنیت سایبری، نفوذ خود را گسترش دهد و ظرفیت‌های دفاعی مشترکی ایجاد کند.
- پیشگیری از استفادهٔ سیاسی از فضای سایبری: کشورها باید از فضای سایبری به‌عنوان بستری برای همکاری و توسعه استفاده کنند، نه ابزاری برای تشدید رقابت‌ها و اختلافات سیاسی. استفادهٔ بیش از حد از کارزارهای اطلاعات غلط و حملات سایبری می‌تواند به بی‌اعتمادی جهانی منجر شود. توافقات بین‌المللی دربارهٔ منع استفاده از فضای سایبری برای اهداف سیاسی می‌تواند این روند را محدود کند.

- تمرکز بر تأثیرات اجتماعی و اقتصادی دیپلماسی سایبری: پژوهش‌ها و سیاست‌ها باید به جنبه‌های اجتماعی و اقتصادی دیپلماسی سایبری نیز توجه کنند. توسعهٔ اقتصاد دیجیتال و کاهش آسیب‌های اجتماعی ناشی از جنگ اطلاعاتی، از جمله اقداماتی است که باید در دستور کار کشورها قرار گیرد. رژیم اسرائیل در این زمینه می‌تواند الگویی برای سایر کشورها باشد.
- افزایش آگاهی عمومی دربارهٔ امنیت سایبری: افزایش آگاهی عمومی دربارهٔ تهدیدات و چالش‌های سایبری می‌تواند تأثیر قابل‌توجهی بر کاهش آسیب‌پذیری‌ها داشته باشد. این اقدامات می‌توانند شامل برنامه‌های آموزشی برای کاربران عادی و تقویت مهارت‌های سایبری در سطح جامعه باشد.

منابع

۱. امینی باغبادرانی، احسان، و نصراللهی، محمدصادق. (۱۴۰۳). شناسایی مفهوم و مطالعهٔ تطبیقی دیپلماسی سایبری و دیجیتال با تأکید بر بند هفتم سیاست‌های کلی شبکه‌های اطلاعاتی-رایانه‌ای. فصلنامهٔ راهبرد اجتماعی فرهنگی، ۱۳(۲)، ۵۱۱-۵۵۰. doi:10.22034/SCS.2023.411493.1479.

۲. تصوری، امیرمحمد، حسینی، سید بشیر و شریفی، سید مهدی (۲۰۲۴). دیپلماسی سایبری رژیم اسرائیل بر دیتای اینستاگرام جمهوری اسلامی ایران. هفتمین همایش بین المللی مطالعات دینی، علوم انسانی و اخلاق زیستی در جهان اسلام..

۳. تصوری، امیرمحمد (۱۴۰۱). دیپلماسی سایبری رژیم صهیونیستی در قبال جمهوری اسلامی ایران: مورد مطالعهٔ صفحهٔ وزارت امور خارجهٔ رژیم اسرائیل به فارسی در اینستاگرام. پایان‌نامهٔ کارشناسی ارشد، دانشگاه صداوسیمای جمهوری اسلامی ایران.

۴. تصوری، امیرمحمد و حسینی، سید بشیر و شریفی، سید مهدی (۱۴۰۲)، دیپلماسی سایبری رژیم اسرائیل در قبال جمهوری اسلامی ایران با تاکید بر اینستاگرام، هفتمین همایش بین المللی مطالعات دینی، علوم انسانی و اخلاق زیستی در جهان اسلام، تهران

۵. قنبری، سمیه. (۱۳۹۹). دیپلماسی سایبری روسیه برای تحول در رژیم حکمرانی فضای مجازی. فصلنامهٔ علمی مطالعات آسیای مرکزی و قفقاز، ۲۶(۱۰۹)، ۱۴۰-۱۷۴.

6. Abbasi, U. S. A. (2024). Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran. Global Strategic & Security Studies Review, IX(I), 44–56.
7. Aquino, S. B. (2022). Shifting from Kinetic to Cyber: A Cyber Diplomacy Literature Review. International Journal of Cyber Diplomacy, 3, 3–11.
8. Assoudeh, M. (2020). Shaping Cybersecurity Strategy: China, Iran, and Russia in a Comparative Perspective. Doctoral Dissertation, University of Nevada, Reno.
9. Baezner, M. (2019). Hotspot Analysis: Iranian cyber-activities in the context of regional rivalries and international tensions. Center for Security Studies, ETH Zürich.
10. Baram, G. (2017). Israeli defense in the age of cyber war. Middle East Quarterly, 24.
11. Brower, K. S. (2013). Pre-Empting Iran. The RUSI Journal, 158(5), 80–89.

12. Chinn, J. N. (2015). Communication Power in Israeli Digital Diplomacy: Towards a Networked Theory of Geopolitics. Doctoral Dissertation, Texas A&M University.
13. Cohen, S. (2019). Iranian Cyber Capabilities: Assessing the Threat to Israeli Financial and Security Interests. Cyber, Intelligence, and Security, 3(1), 71–89.
14. Devanny, J., Goldoni, L., & Medeiros, B. (2022). Strategy in an Uncertain Domain: Threat and Response in Cyberspace. Journal of Strategic Security, 15(2), 34–47.
15. Duguin, S., & Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Policy Department for External Relations, European Parliament.
16. Farwell, J. P., & Arakelian, D. (2013). What Does Iran's Cyber Capability Mean For Future Conflict? The Whitehead Journal of Diplomacy and International Relations.
17. Ford, C. A. (2022). Conceptualizing cyberspace security diplomacy. The Cyber Defense Review, 35–38.
18. Frei, J. (2020). Israel's National Cybersecurity and Cyberdefense Posture. Center for Security Studies (CSS), ETH Zürich.
19. Givens, A., Sanders, N., & Douglas, C. J. (2022). Forecasting Iranian Government Responses to Cyberattacks. Journal of Advanced Military Studies, 13(1), 219–237.
20. Kari, M. J. (2019). Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – A Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats. JYU Dissertations, 122.
21. Khalid, P., & Safdar, A. (2020). Iran's Nuclear Agreement: Rethinking Pakistan's Middle East Policy. International Affairs, 347–366.
22. Lancelot, J. (2020). Cyber-diplomacy: Cyberwarfare and the Rules of Engagement. Journal of Cyber Security Technology, 4, 1–15.
23. Martti, J. K. (2019). Russian Strategic Culture in Cyberspace: Theory of Strategic Culture. JYU Dissertations.
24. Stachoń, M. (2024). Iranian Cyber Capabilities as a Tool of Domestic and Foreign Policy. Scientific Reports of Fire University, 2(89), 267–290.
25. Tarock, A. (1996). US: Iran Relations: Heading for Confrontation? Third World Quarterly, 17(1), 149–167.
26. Treggiari, L. F. (2016). Concepts of International Relations applied to cyberspace: Sovereignty, war and diplomacy in the digitized age. Master's Thesis, University of Venice.

27. Tsvetkova, N. A., Sytnik, A. N., & Grishanina, T. A. (2022). Digital diplomacy and digital international relations: Challenges and new advantages. Vestnik of Saint Petersburg University International Relations, 15(2), 174–196

RESEARCH PAPERS

دفترهای آبی

مقالات پژوهشی (Research Papers) از مهم ترین ابزارهای توسعهٔ دانش هستند که با تکیه بر داده‌های تجربی به بررسی دقیق و جامع موضوعات تخصصی می‌پردازند.
دفترهای آبی دسته‌ای از گزارش‌های تفصیلی تولیدشده در پژوهشگاه فضای مجازی، و محصولِ رصد مطالعات تحقیقی اندیشکده‌ها و نخبگان جهان در موضوعات مرتبط با فَضای مجازی است.

پژوهشگاه
فضای مجازی