فصلنامه علمی شناخت پژوهی مطالعات سیاسی
سال ۲، شماره ۴(۷)،۷۵-۵۵
تاریخ دریافت: ۱۴۰۴/۰۶/۰۴
تاریخ پذیرش: ۱۴۰۴/۰۷/۱۳

Journal of cognitive research in political studies
Vol.2, No4 (7), 55-75
Reseived Date: 1404/08/26
Accept Date: 2025/10/05

DOI: 10.20241403/CRPS.2508.1057.4.7.3

ژئوپلیتیک جنگ سایبری و راهبردهای امنیتی رژیم صهیونیستی و جمهوری اسلامی ایران: تحلیل تقابل و بازدارندگی سایبری (۲۰۲۵-۲۰۱۰)

دانیال رضاپور[۱]

شماره ٤(٧)
سال ۲
فصل زمستان ١٤٠٤

مقاله پژوهشی

تاریخ دریافت:
١٤٠٤/٠٦/٠٤
تاریخ پذیرش:
١٤٠٤/٠٧/١٣
صص: ٧٥-٥٥

چکیده

فضای سایبر به‌عنوان بستر اصلی تبادل و گردش اطلاعات به‌عنوان «پنجمین میدان جنگ» پس از دریا، زمین، هوا و فضا نامیده‌اند. برخی کارشناسان بر این باورند که جنگ در فضای سایبر می‌تواند به سمتی پیش برود که در کوتاه‌ترین زمان ممکن، سامانه‌های کنترلی یک کشور یا حتی چند کشور به‌طور کامل از دست دولت‌های آن خارج شود. در چنین شرایطی، جهان مدرن ظرف چند ثانیه از حرکت و پویایی بازمی‌ایستد و فاجعه‌ای به‌مراتب مصیبت‌بارتر از یک جنگ هسته‌ای رقم خواهد خورد. این مقاله با مطالعه تحولات دکترین امنیتی- دفاعی رژیم صهیونیستی و ج.ا.ایران به‌دنبال فهم چارچوب‌مند ظرفیت‌های سایبری در شکل‌دهی به راهبرد بازدارندگی نوین آن در مقابله با تهدیدات داخلی و خارجی است. از این‌رو سؤال پژوهش این‌گونه مطرح می‌شود که ژئوپلیتیک جنگ سایبری در غرب آسیا چگونه بر راهبردهای امنیتی رژیم صهیونیستی در قبال جمهوری اسلامی ایران اثر گذاشته و متقابلاً چه نقشی برای ایران در تقابل و بازدارندگی سایبری علیه این رژیم قابل شناسایی است؟ بر این اساس فرضیه پژوهش چنین مطرح می‌شود که رژیم صهیونیستی با توجه به محدودیت‌های ژئوپلیتیکی و تهدیدات امنیتی ناشی از قدرت‌یابی ایران، جنگ سایبری را به‌عنوان یکی از ابزارهای اصلی مهار امنیتی ایران به‌کار گرفته است؛ اما در مقابل، جمهوری اسلامی ایران با توسعه ظرفیت‌های بومی و بهره‌گیری از توان بازدارندگی سایبری، توانسته بخشی از این فشارها را خنثی کرده و به بازیگری فعال در بازتعریف موازنه قدرت سایبری و امنیتی غرب آسیا تبدیل شود. پژوهش پیش‌رو مبتنی بر روش کیفی با رویکرد توصیفی- تحلیلی است که از طریق گردآوری داده‌ها به صورت اسنادی، کتابخانه‌ای به اجرا درمی‌آید.

کلمات کلیدی: ج.ا.ایران، رژیم صهیونیستی، غرب آسیا، جنگ سایبری، بازدارندگی سایبری

[۱] استادیار روابط بین الملل گروه علوم سیاسی، دانشگاه گیلان، رشت، ایران. danyalrezapoor@gmail.com

استناد: رضاپور، دانیال. (۱۴۰۴). ژئوپلیتیک جنگ سایبری و راهبردهای امنیتی رژیم صهیونیستی و جمهوری اسلامی ایران: تحلیل تقابل و بازدارندگی سایبری (۲۰۲۵-۲۰۱۰). شناخت پژوهی مطالعات سیاسی، ۲(۴)، ۷۵-۵۵. doi: 10.20241403/CRPS.2508.1057.4.7.3

Rezapoor, D. (2025). The Geopolitics of Cyber War and the Security Strategies of the Zionist Regime and the Islamic Republic of Iran: Analysis of Cyber Confrontation and Deterrence (2010-2025). Cognitive Research in Political Studies, 2(4), 55-75. doi: 10.20241403/CRPS.2508.1057.4.7.3

مقدمه

در دوران پهلوی، ایران پس از ترکیه، رژیم صهیونیستی را به رسمیت شناخت و در دهه ۱۹۷۰، روابط دیپلماتیک، نظامی و تجاری میان دو طرف گسترش یافت. ایران به تأمین‌کننده اصلی نفت این رژیم تبدیل شد. با پیروزی انقلاب اسلامی در ۱۹۷۹، سیاست خارجی ایران دگرگون شد؛ شناسایی رژیم صهیونیستی لغو گردید، روابط قطع شد و نمایندگی آن به فلسطینیان واگذار شد. رژیم صهیونیستی، که ابتدا امیدوار به احیای روابط بود، با تداوم سیاست‌های ضدصهیونیستی ایران، این امید را از دست داد و رویکرد امنیتی خود را از تمرکز بر اعراب به مقابله با ایران تغییر داد. در دهه‌های بعد، با محدودیت عمق استراتژیک و تهدیدات ژئوپلیتیکی، رژیم صهیونیستی فاقد ظرفیت برای جنگ مستقیم با ایران بود. بنابراین، با برجسته شدن پرونده هسته‌ای ایران، راهبرد مهار غیرمستقیم را برگزید و از ۲۰۱۰، سیاست «منطقه خاکستری» را اتخاذ کرد. هدف این سیاست، وارد آوردن فشار به ایران بدون ورود به جنگ مستقیم بود، با ابزارهایی مانند عملیات سایبری، ترور و جاسوسی (Qeitasi & Mousavi-Tabar, 2024: 260). در این میان، عملیات سایبری به‌عنوان شکلی نوین از «جنگ قدرت سیاسی» در غرب آسیا برجسته شد. رژیم صهیونیستی با بهره‌گیری از فناوری‌های غربی، فضای سایبری را به عرصه‌ای حیاتی برای اهداف نظامی، دفاعی و اطلاعاتی تبدیل کرد. محیط سایبری، با گستردگی و سرعت بالا، به این رژیم امکان داد توان نظامی خود را ارتقا دهد و موازنه قدرت را تغییر دهد. رژیم صهیونیستی سرمایه‌گذاری گسترده‌ای در امنیت سایبری انجام داد و امروزه با ۱۲ درصد از ۵۰۰ شرکت بزرگ امنیت سایبری و بیش از ۴۷۰ استارتاپ، دومین مرکز بزرگ جهان است. در ۲۰۲۱، صادرات محصولات سایبری آن سه برابر بریتانیا بود (Habibi & Karafashani, 2024: 140). در سال‌های اخیر، حملات سایبری علیه ایران شدت یافته است. جنگ سایبری، هرچند نوظهور به نظر می‌رسد، در سه دهه گذشته بخشی از مناقشات دو طرف بوده. تبادل حملات سایبری، به‌ویژه علیه اهداف غیرنظامی، دامنه منازعه را گسترش داده است. ویژگی اصلی آن محرمانه بودن است؛ حملات بدون پذیرش مسئولیت و با دشواری شناسایی منبع انجام می‌شوند. از منظر راهبردی، این حملات در چارچوب «جنگ بین دو جنگ» قرار می‌گیرند، که مهاجم را قادر می‌سازد از راه دور و پنهانی اهداف خود را دنبال کند. این کنش، علاوه بر اجتناب از تلفات، امکان جمع‌آوری اطلاعات، ارسال پیام بازدارنده و فشار بر زیرساخت‌ها را فراهم می‌آورد (Amaliya, 2025: 2). هم‌زمانی عملیات سایبری با اقدامات نظامی در «جنگ ۱۲ روزه»، نشان داد که جنگ سایبری دیگر تاکتیک خاکستری نیست، بلکه بخشی جدایی‌ناپذیر از درگیری‌های

مسلحانه شده است. بنابراین، جنگ سایبری یکی از ابعاد اصلی ژئوپلیتیک و امنیت منطقه‌ای در غرب آسیا، به‌ویژه در روابط ایران و رژیم صهیونیستی، محسوب می‌شود. در پرتو این تحولات، سؤال پژوهش چنین است: ژئوپلیتیک جنگ سایبری در غرب آسیا چگونه بر راهبردهای امنیتی رژیم صهیونیستی در قبال جمهوری اسلامی ایران اثر گذاشته و متقابلاً چه نقشی برای ایران در بازدارندگی سایبری قابل شناسایی است؟ فرضیه پژوهش بیان می‌دارد که رژیم صهیونیستی با محدودیت‌های ژئوپلیتیکی و تهدیدات ناشی از قدرت‌یابی ایران، جنگ سایبری را به‌عنوان ابزار اصلی مهار ایران به‌کار گرفته؛ اما ایران با توسعه ظرفیت‌های بومی و بهره‌گیری از بازدارندگی سایبری، بخشی از فشارها را خنثی کرده و به بازیگری فعال در بازتعریف موازنه قدرت سایبری و امنیتی غرب آسیا تبدیل شده است.

۱ـ پیشینه تحقیق

عمر (۲۰۲۵) در مقاله «جنگ سایبری ایران و رژیم صهیونیستی و دخالت آمریکا» بیان می‌کند که منازعه میان ایران و رژیم صهیونیستی وارد عرصه جنگ سایبری شده است؛ عرصه‌ای که بازتابی از رقابت جهانی قدرت برای دستیابی به اهداف استراتژیک با حداقل ریسک فیزیکی است. به باور او، این جنگ ریشه در رقابت ژئوپلیتیک، ایدئولوژیک و الزامات امنیت ملی دارد و شامل حملات و ضدحملات متقابل به زیرساخت‌ها و نهادهای دولتی است. نمونه شاخص آن، حمله استاکس‌نت در ۲۰۱۰ است که با همکاری آمریکا و رژیم صهیونیستی علیه تأسیسات هسته‌ای ایران انجام شد. پس از آن، ایران ظرفیت‌های سایبری خود را توسعه داد و رژیم صهیونیستی نیز با اقدامات متقابل واکنش نشان داد. در نتیجه، رقابتی پایدار و پرچالش در فضای دیجیتال غرب آسیا شکل گرفت. آمریکا نیز نقشی دوگانه دارد؛ از یک‌سو پشتیبانی فنی و عملیاتی به رژیم صهیونیستی ارائه می‌دهد و از سوی دیگر، خود هدف حملات ایران قرار می‌گیرد.

آملیا (۲۰۲۵) در مقاله «جنگ سایبری ایران و رژیم صهیونیستی: یک رقابت ژئوپلیتیکی» بر گسترش مناقشه دو طرف از دهه ۱۹۹۰ تاکنون تأکید می‌کند و معتقد است این روند، به‌ویژه پس از جنگ رژیم صهیونیستی و حماس، به سطحی تازه رسیده است. او نتیجه می‌گیرد که جنگ سایبری ابزاری کلیدی برای تضعیف امنیت طرف مقابل و کاهش هژمونی اوست و هر دو بازیگر در پی تثبیت موقعیت خود به‌عنوان قدرت مسلط در غرب آسیا هستند.

DOR: 20.1001.1.30926459.1404.2.4.3.1

هارون (۲۰۲۴) در مقاله «هوش مصنوعی و جنگ سایبری در مناقشه ایران و رژیم صهیونیستی و تأثیر آن بر امنیت کشورهای خلیج‌فارس» به پیامدهای این تقابل بر کشورهای عربی خلیج‌فارس می‌پردازد. از منظر رئالیسم تدافعی، این کشورها به دلیل موقعیت ژئوپلیتیکی آسیب‌پذیرند و ناگزیر باید بر تقویت تاب‌آوری سایبری، بهره‌گیری از ابزارهای امنیتی مبتنی بر هوش مصنوعی و همکاری منطقه‌ای تمرکز کنند. او نتیجه می‌گیرد که چنین رویکردی می‌تواند امنیت و ثبات آن‌ها را در برابر تهدیدات فناورانه ارتقاء دهد. عباسی (۲۰۲۴) در مقاله «تهدیدات سایبری علیه ایران از سوی آمریکا و رژیم صهیونیستی: راهبردهای مقابله‌ای ایران» بر اهمیت فزاینده جنگ سایبری در روابط پرتنش سه‌جانبه تأکید دارد. وی جنگ سایبری را پدیده‌ای اجتناب‌ناپذیر با پیامدهای بالقوه فاجعه‌بار می‌داند و با رویکرد کیفی به تحلیل راهبردهای سایبری ایران، آمریکا و رژیم صهیونیستی می‌پردازد. قیطاسی و همکاران (۱۴۰۳) در مقاله «منطقه خاکستری؛ راهبرد رژیم صهیونیستی علیه ایران از ۲۰۱۰ تا ۲۰۲۳» نشان می‌دهند که رژیم صهیونیستی برای مهار ایران، به‌جای تقابل مستقیم، از ترور، جاسوسی، تبلیغات، جنگ نیابتی، فشار اقتصادی و حملات سایبری در قالب راهبرد «منطقه خاکستری» بهره گرفته است.

نوآوری پژوهش حاضر در پیوند تحلیلی این منابع است. در کنار بررسی تاریخی منازعه سایبری ایران و رژیم صهیونیستی، نقش قدرت‌های فرامنطقه‌ای، فناوری‌های نوین و هوش مصنوعی نیز در چارچوب ژئوپلیتیک و امنیت منطقه‌ای مورد توجه قرار گرفته است. همچنین با رویکرد تطبیقی، هم‌زمان کنش‌های رژیم صهیونیستی و بازدارندگی ایران تحلیل و چارچوب «منطقه خاکستری» در متن رقابت سایبری بازتبیین شده است. این تلفیق، دیدگاهی جامع از تعامل میان فناوری، امنیت و سیاست منطقه‌ای ارائه می‌دهد و ظرفیت تحلیل نوین در زمینه بازدارندگی سایبری و راهبردهای امنیتی را فراهم می‌سازد.

۲ـ چارچوب نظری

سنت واقع‌گرایی یا «واقع‌گرایی سیاسی» از مهم‌ترین نظریه‌های سیاست بین‌الملل در قرن بیستم است که به دیدگاه غالب در روابط بین‌الملل بدل شد. این رویکرد بر سیاست قدرت و پیگیری منافع ملی تأکید دارد و دولت را بازیگر اصلی نظام بین‌الملل می‌داند. واقع‌گرایان، قدرت را اساس سیاست جهانی قلمداد کرده و آن را غالباً بر حسب ظرفیت نظامی تعریف می‌کنند. واقع‌گرایی با تفکیک سیاست از اخلاق، مشروعیت لازم برای افزایش توان نظامی و برتری‌جویی قدرت‌های بزرگ را

فراهم می‌کند و تصویری بدبینانه از سیاست جهانی ارائه می‌دهد؛ جهانی که در آن دولت‌ها در محیطی آکنده از تهدید دائمی جنگ، همواره در پی کسب قدرت هستند. بنابراین، همکاری میان دولت‌ها محدود و صلح پایدار غیرممکن ارزیابی می‌شود. هانس مورگنتا، یکی از برجسته‌ترین نظریه‌پردازان این مکتب، بر این باور است که ماهیت انسان ثابت و گرایش به قدرت در ذات او نهفته است و همین امر اغلب به مناقشه و جنگ می‌انجامد؛ رخدادی که باید همواره برای آن آماده بود. در این چارچوب، امنیت ملی و بقای دولت، ارزش‌های محوری واقع‌گرایی محسوب می‌شوند و سیاست خارجی بر اساس منافع ملی شکل می‌گیرد. به‌علاوه، در این نگاه، اخلاق و جامعه انسانی محدود به مرزهای دولت‌اند و وارد عرصه روابط بین‌الملل نمی‌شوند، زیرا نظام جهانی در فضایی بی‌نظم، پر از اختلاف و تهدید دائمی تعریف می‌شود. بر این اساس، کشورها نمی‌توانند به یک‌دیگر اعتماد کامل داشته باشند و مهم‌ترین وظیفه رهبران، حفاظت از بقای دولت‌ها در محیطی تهدیدآمیز است. واقع‌گرایان رهبران را بازیگرانی عقلانی می‌دانند که پیش از هر اقدام، هزینه‌ها و منافع تصمیمات خود را می‌سنجند. در چنین شرایطی، اتکا به دیگر کشورها یا نهادهای بین‌المللی امری غیرعقلانی و حتی خطرناک تلقی می‌شود؛ بنابراین دولت‌ها برای بقا ناگزیر به خوداتکایی و ایجاد موازنه قدرت روی می‌آورند (Ebrahimi et al., 2017: 125-126). در پیوند با این رویکرد، مفاهیم «هژمونی» و «هژمون» پیشینه‌ای طولانی در روابط بین‌الملل دارند. یکی از مهم‌ترین متون در این زمینه کتاب جنگ پلوپونزی توسیدید (۴۳۱ ق.م.) است که به هژمونی آتن و پیامدهای آن در نظام دولت‌شهرهای یونانی می‌پردازد. در نگاه سنتی، هژمونی به شرایط عدم توازن قدرت در نظام بین‌الملل اشاره دارد که طی آن یک دولت با قدرت مادی، اقتصادی یا نظامی چشمگیر قادر به اعمال سلطه بر دیگر بازیگران می‌شود. چنین دولتی «هژمون» نامیده می‌شود و توانایی کنترل ساختارها و جهت‌دهی به رفتار دیگر واحدها را دارد. برتری هژمون می‌تواند از عوامل متعددی چون موقعیت جغرافیایی، منابع طبیعی، ظرفیت اقتصادی، توان نظامی، جمعیت، انسجام اجتماعی، کیفیت حکومت، دیپلماسی و نوآوری فناورانه ناشی شود. در این چارچوب، هژمونی فرآیندی از بالا به پایین است که استمرار آن عمدتاً بر اتکای هژمون به قابلیت‌های مادی و قدرت اجبار یا نفوذ استوار است. از منظر واقع‌گرایی، نظام تک‌قطبی جهانی مصداق بارز نظام هژمونی است (Ameliya, 2025: 4). در مناقشه ایران و رژیم صهیونیستی، رویکرد واقع‌گرایی می‌تواند تبیین‌گر رقابت برای بقا و امنیت در محیط آنارشیک غرب آسیا باشد؛ محیطی که در آن هر دو بازیگر از ابزارهای نظامی و سایبری برای تضعیف یک‌دیگر و افزایش قدرت نسبی خود بهره می‌گیرند. در این رقابت، دستیابی به

DOR: 20.1001.1.30926459.1404.2.4.3.1

هژمونی منطقه‌ای و سایبری هدف راهبردی محسوب می‌شود، زیرا هر یک از طرفین در تلاش است با کاهش نفوذ رقیب و اعمال سلطه بر فضای امنیتی و فناورانه منطقه، منافع ملی خود را تضمین کند. از این منظر، جنگ سایبری ابزاری رئالیستی برای تحقق هژمونی و بازتعریف موازنه قدرت در غرب آسیا است.

۳ـ راهبردهای ژئوپلیتیکی- امنیتی رژیم صهیونیستی و ج.ا.ایران در غرب آسیا

الف: رژیم صهیونیستی: در استراتژی نظامی رژیم صهیونیستی، سه لایه امنیتی تعریف شده است: نخست، همسایگان متصل به مرزهای فلسطین؛ دوم، لایه پیرامونی؛ و سوم، ایران. در راهبرد ۲۰۱۹ تأکید شده است که در لایه دوم و سوم نباید هیچ ارتش قدرتمندی شکل گیرد و در صورت ظهور چنین ارتشی، رژیم باید با حملات پیش‌دستانه آن را نابود کند (Elhami et al., 2024: 96). در محیط پیچیده غرب آسیا، این استراتژی صرفاً نظامی نیست، بلکه اهداف سیاسی، روانی و ژئوپلیتیکی را نیز دنبال می‌کند. عملیات‌های هوایی کوتاه‌مدت ابزار اصلی تل‌آویو برای ارسال پیام بازدارنده، مدیریت تهدیدات و تحکیم انسجام داخلی بوده‌اند. از ۱۹۷۳ به بعد، نیروی هوایی مأموریت نابودی راکتور عراق (۱۹۸۱) و برنامه تسلیحاتی سوریه (۲۰۰۷) را بر عهده داشت و مواضع گروه‌هایی چون سازمان آزادی‌بخش فلسطین، حماس، حزب‌الله و جهاد اسلامی را هدف قرار داد. از اوایل ۲۰۰۰ نیز آماده اجرای گزینه حمله به تأسیسات کلیدی ایران شد (Rodman, 2022: 4). با افزایش نگرانی نسبت به انتقال تسلیحات ایرانی، رژیم دکترین «کارزار بین جنگ‌ها» (مَبام) را برای جلوگیری از توان‌افزایی دشمنان در زمان صلح اتخاذ کرد. نخستین اقدام آن حمله ژانویه ۲۰۱۳ به کاروان موشکی SA-17 در دمشق بود که آغازگر سلسله حملات علیه حزب‌الله و بعدها اهداف ایرانی در سوریه شد. مَبام همچون جنگ فرسایشی دهه ۱۹۶۰ علیه مصر، بر حملات هوایی محدود با اهداف مشخص استوار است. تا اوایل ۲۰۲۴، صدها حمله و بیش از ۵۵۰۰ مهمات به کار رفت (Joshua, 2022: 13). با وجود پیشرفت در پهپادها و پدافند، تمرکز بر تهاجم باقی مانده است. هرچند پدافند داخلی رژیم در برابر اشباع آسیب‌پذیر است، رهبران همچنان به اثربخشی این دکترین در مهار ایران باور دارند. در ادامه، دکترین «بگین» مبنای اقداماتی چون عملیات اپرا علیه رآکتور اوسیراک عراق (۱۹۸۱) و حمله ۲۰۰۷ به رآکتور سوریه بود. این دکترین تضمین می‌کند رژیم تنها دارنده سلاح هسته‌ای در غرب آسیا باقی بماند و هرگونه توانمندی هسته‌ای رقیب با حمله پیش‌دستانه

نابود شود. در مورد ایران، پیچیدگی ژئوپلیتیکی و فشارهای بین‌المللی رژیم را از اوایل دهه ۲۰۰۰ به اتخاذ طیف گسترده‌ای از اقدامات آشکار و پنهان سوق داد (Gaietta, 2025: 10). توان اطلاعاتی- عملیاتی رژیم علیه ایران قابل توجه است. موساد بین سال‌های ۱۳۸۸ تا ۱۳۹۰ پنج دانشمند هسته‌ای ایران را هدف قرار داد و در سال ۱۳۹۹ محسن فخری‌زاده ترور شد. علاوه بر آن، حملات خرابکارانه به تأسیسات هسته‌ای، از جمله ویروس استاکس‌نت در نطنز، خسارت‌های سنگینی وارد کرد (Farhadian et al, 2024: 200). در عرصه بین‌المللی، تل‌آویو جنگ‌های محدود را ابزار نمایش اراده و بازدارندگی معرفی می‌کند. این عملیات‌ها با استناد به «دفاع مشروع» یا «واکنش به تهدید قریب‌الوقوع» توجیه می‌شوند تا مشروعیت حقوقی و دیپلماتیک حفظ گردد (Slater, 2021). در واقع، سیاست جنگ محدود پاسخی صرف به تهدیدات نظامی نیست بلکه بخشی از راهبردی وسیع‌تر برای مهار محور مقاومت، ترمیم مشروعیت داخلی و تثبیت بازدارندگی است. هرچند نتایج آن همیشه با اهداف رسمی همخوانی ندارد، استمرار این الگو نشان می‌دهد که نخبگان سیاسی و نظامی رژیم همچنان به کارآمدی نسبی آن باور دارند. این امر بازتابی از چالش‌های داخلی رژیم، از بحران مشروعیت تا شکاف اجتماعی، است. در نتیجه، جنگ محدود نه‌تنها ابزار نظامی بلکه راهبردی برای مدیریت بحران‌های چندلایه سیاسی و امنیتی محسوب می‌شود.

ب: ج.ا. ایران: ایرانیان به صبر استراتژیک و یادگیری از بحران‌ها شهرت دارند. سپهبد شهید قاسم سلیمانی، معمار استراتژی بازدارندگی ایران، سپاه پاسداران را «یک نظام فکری» معرفی کرد که هدفش «ایجاد فرصت از دل بحران» است. این رویکرد به کل جمهوری اسلامی تعمیم یافته و محور مقاومت نیز با حمایت ایران، انعطاف‌پذیری و تاب‌آوری بالایی نشان داده است. ادغام این گروه‌ها در جوامع خود و روابط فراملی آن‌ها، شبکه‌ای سیاسی، اقتصادی، نظامی و ایدئولوژیک شکل داده که در دوره‌های بحران به‌منزله بیمه‌ای حیاتی عمل می‌کند (Cano, 2025: 16). راهبرد بازدارندگی فعال ایران در برابر رژیم صهیونیستی بر محاسبات امنیتی، الزامات ژئوپلیتیکی و پاسخ به تهدیدات منطقه‌ای استوار است. برخلاف بازدارندگی سنتی که به تهدید و توازن قوا متکی است، بازدارندگی فعال ترکیبی از پیش‌دستی، جنگ شناختی و پیام‌های راهبردی است. پس از حمله آمریکا به عراق در ۲۰۰۳ و نگرانی از تهاجم، ایران تمرکز بیشتری بر حوزه هوایی گذاشت. این روند در دوره احمدی‌نژاد شتاب گرفت و با تهدید حمله احتمالی به برنامه هسته‌ای ایران تقویت شد. در ۲۰۰۸ ایران نیروی مستقل پدافند هوایی تشکیل داد و سرمایه‌گذاری در حوزه دفاع هوایی را با

DOR: 20.1001.1.30926459.1404.2.4.3.1

الهام از منطق نامتقارن توسعه داد. این رویکرد مشابه نظریه جولیان کوربت[1] است که معتقد بود به چالش کشیدن یک حوزه کافی است تا آزادی عمل دشمن محدود شود (Bahgat & Ehteshami, 2021: 12-15). ایران نیز بدون نیاز به تسلط کامل، صرفاً با تحمیل هزینه و بهره‌برداری محدود توانسته در جنگ‌های اخیر، به‌ویژه جنگ ۱۲ روزه، این رویکرد را عملی کند. تلاش‌های ایران در این حوزه بر سه مؤلفه متمرکز بوده است: نخست، پدافند هوایی زمینی شامل رادارها، موشک‌های زمین‌به‌هوا و جنگ الکترونیک که با تحرک بالا و تنوع فرکانسی توسعه یافته‌اند. دوم، موشک‌های زمین‌به‌زمین که به دلیل نبود جنگنده‌های مدرن، به مرکز ثقل توان تهاجمی ایران بدل شده‌اند و بازدارندگی منطقه‌ای را تقویت می‌کنند. سوم، پهپادها به‌عنوان ابزار ارزان و مؤثر برای شناسایی، جمع‌آوری اطلاعات و انجام حملات. این سه مؤلفه با هم امکان به چالش کشیدن برتری هوایی دشمن را فراهم کرده‌اند و در جنگ‌های اخیر به‌صورت عملیاتی فراتر از مرزهای ایران به‌کار گرفته شده‌اند (Ostovar, 2019: 21). به‌طور کلی، راهبرد بازدارندگی فعال ایران بر ایجاد ساختاری چندلایه از پاسخ و دفاع در برابر رژیم صهیونیستی تأکید دارد. این ساختار بر هم‌افزایی ارکان نظامی و دیپلماتیک استوار است و علاوه بر قدرت سخت‌افزاری، از مدیریت روایت، موازنه تهدیدات و تحمیل هزینه‌های بلندمدت بهره می‌گیرد. برخلاف تصور مبتنی بر پاسخ صرفاً نظامی، ایران از بازدارندگی هوشمند و فعال استفاده می‌کند تا جبهه‌های متنوعی برای دفاع از منافع خود ایجاد کند. این راهبرد ضمن اتکا بر قابلیت‌های نظامی، بر روایت‌سازی و جنگ شناختی متمرکز است و تلاش دارد با هزینه‌سازی مداوم، آزادی عمل دشمن را محدود و امنیت راهبردی ایران را در محیط پرتهدید منطقه تضمین کند.

۴ـ رقابت ژئوپلیتیکی و عملیات سایبری: تحلیل استراتژیک مناقشه ایران و رژیم صهیونیستی

موانع همکاری در آسیای غربی که ریشه در درگیری‌های قومی، قبیله‌ای و ایدئولوژیک دارند، همراه با ضعف عمق استراتژیک و آسیب‌پذیری‌های ناشی از عدم تقارن قدرت ملی رژیم صهیونیستی، موجب شده است دکترین دفاعی این رژیم از الگوی جنگ‌های کلاسیک فاصله گرفته و به‌سوی بهره‌گیری از ابزارهای نامتعارف بازدارندگی حرکت کند. طی دهه اخیر، رژیم صهیونیستی با بازتعریف ابزارهای امنیتی، سرمایه‌گذاری در توانمندی‌های سایبری و اتخاذ رویکرد دفاعی با

[1] ulian Corbett

قابلیت‌های تهاجمی پنهان، راهبرد جدیدی را دنبال کرده است. در اسناد راهبردی آن، ایران، لبنان، سوریه و گروه‌های غیردولتی چون حزب‌الله، حماس و جهاد اسلامی به‌عنوان تهدیدات اصلی معرفی شده‌اند و احتمال درگیری در حوزه‌هایی همچون تسلیحات کشتارجمعی، موشک‌های بالستیک و تهدیدات سایبری رو به افزایش است (Mirzaei & Ghorashi, 2024: 310). در این چارچوب، ارتقای توان سایبری جایگاه ویژه‌ای یافته و رژیم در پی تبدیل‌شدن به قدرت برتر سایبری در منطقه است. نیروهای دفاعی این رژیم با اتکا به فناوری‌های پیشرفته و هوش مصنوعی، ابزارهایی همچون «گنبد آهنین» را برای رهگیری موشک‌های حماس و حزب‌الله به کار می‌گیرند. کاربردهای هوش مصنوعی عمدتاً شامل پیش‌بینی تهدیدات و تحلیل اطلاعات است. همچنین، رژیم صهیونیستی عملیات‌های سایبری متعددی علیه ایران انجام داده که نمونه بارز آن استاکس‌نت بود و تأسیسات هسته‌ای ایران را هدف قرار داد (Haroon, 2024: 13). از منظر واقع‌گرایی، ایران برای رژیم صهیونیستی تهدیدی وجودی محسوب می‌شود، زیرا می‌تواند ثبات منطقه‌ای و ژئوپلیتیک غرب آسیا را بر هم زند. نگرانی اصلی رژیم، برنامه تسلیحاتی هسته‌ای ایران است که باعث شده اقداماتی چون تلاش‌های دیپلماتیک بین‌المللی، تهدیدات نظامی و حملات سایبری به‌منظور جلوگیری از دستیابی ایران به سلاح هسته‌ای صورت گیرد. رژیم صهیونیستی بر این باور است که تقویت قدرت ایران مانع تحقق اهداف آن، از جمله گسترش نفوذ در غزه و لبنان و تحقق آرمان «رژیم صهیونیستی بزرگ» خواهد شد. بنابراین با اتخاذ راهبردهای سایبری و اطلاعاتی فعال، در پی بازدارندگی و تضمین امنیت خود بدون ورود به جنگ مستقیم است. در مقابل، جمهوری اسلامی ایران طی یک دهه گذشته سرمایه‌گذاری گسترده‌ای در توسعه توان سایبری داشته و از این ظرفیت به‌عنوان ابزاری نامتقارن علیه رژیم صهیونیستی بهره گرفته است. ایران از فناوری سایبری برای حمله به زیرساخت‌های غیرنظامی، شبکه‌های مالی و سامانه‌های امنیتی استفاده کرده و حتی توانایی نفوذ در سامانه‌های پهپادی رژیم را پیگیری کرده است. این کشور در سال ۲۰۱۱ بودجه‌ای معادل یک میلیارد دلار برای ارتقای توان سایبری اختصاص داد و تجهیزات پیشرفته‌ای مانند ابزارهای نظارتی، اطلاعاتی و جاسوسی سایبری توسعه داد. به‌کارگیری فناوری‌های بین‌المللی نیز توان ایران را در این حوزه افزایش داده است. توان سایبری ایران به بخشی کلیدی از راهبرد دفاع نامتقارن این کشور بدل شده است. حملات به سامانه‌های راداری و امنیتی رژیم صهیونیستی، علاوه بر تضعیف امنیت ملی این رژیم، امکان بهره‌برداری ایران از فرصت‌های نظامی مستقیم را فراهم می‌کند. ایران توسعه توانمندی‌های سایبری را به‌عنوان بخشی از راهبرد هژمونیک خود برای چالش با جایگاه رژیم

DOR: 20.1001.1.30926459.1404.2.4.3.1

صهیونیستی در غرب آسیا می‌داند. در نتیجه، پیشرفت امنیت سایبری ایران موقعیت آن را در منطقه تقویت کرده و آن را به بازیگری توانمند در برابر رژیم صهیونیستی و کشورهای غربی بدل ساخته است (Amaliya, 2025: 8). با توجه به تلاقی مطالب فوق یکی از دلایل اصلی افزایش فعالیت‌های سایبری رژیم صهیونیستی و ج.ا.ایران درک این بازیگران از کارکرد چندوجهی فضای سایبری به‌عنوان ابزاری برای جنگ، دفاع و همچنین جمع آوری اطلاعات است. این روند از اوایل دهه ۲۰۰۰ آغاز شد؛ دوره‌ای که ایران تمرکز خود را صرفاً بر بهره‌گیری از ظرفیت‌های سایبری برای اهداف اطلاعاتی قرار داده بود. این وضعیت تا وقوع حمله معروف استاکس‌نت ادامه داشت؛ حمله‌ای که به باور بسیاری حاصل همکاری مشترک ایالات‌متحده و رژیم صهیونیستی با هدف فلج کردن یا مختل‌سازی برنامه هسته‌ای ایران بود و نقطه عطفی در آغاز تقابل آشکار سایبری میان دو طرف محسوب می‌شود. از آن پس، مناسبات سایبری ایران و رژیم صهیونیستی وارد مرحله‌ای از تقابل مستمر و چندلایه شد که ابعاد آن نه‌تنها در حوزه نظامی، بلکه در زمینه‌های اقتصادی، اطلاعاتی و زیرساختی نیز گسترش یافت. در ادامه، این پژوهش به بررسی چند رویداد شاخص در قالب مصادیق عینی تقابل ژئوپلیتیکی سایبری ایران و رژیم صهیونیستی می‌پردازد:

۴ـ۱ـ حمله به تأسیسات هسته‌ای ایران

حمله سایبری به رآکتور هسته‌ای ایران در سال ۲۰۰۹ نخستین نمونه جدی از جنگ سایبری محسوب می‌شود و آغازگر دوره‌ای تازه در بهره‌گیری از فضای مجازی در جنگ بود. کیم ستر به نقل از دویچه‌وله فارسی می‌نویسد که ویروس استاکس‌نت نخستین بدافزار طراحی‌شده برای خرابکاری در تأسیسات هسته‌ای بود که در سال ۲۰۰۷ وارد سامانه‌های نطنز شد. گمانه‌زنی‌ها حاکی است که واحد ۸۲۰۰ ارتش رژیم صهیونیستی با همکاری آژانس امنیت ملی آمریکا آن را برای حمله به نطنز به کار گرفت (Golmohammadi & Jamshidi, 2022: 17). حمله از طریق یک حافظه آلوده آغاز شد و نخستین نشانه‌ها در ۲۰۱۰ آشکار گردید؛ زمانی که آژانس بین‌المللی انرژی اتمی از کار افتادن سانتریفیوژها را مشاهده کرد. استاکس‌نت به دلیل پیچیدگی احتمالاً از میانه دهه ۲۰۰۰ در حال توسعه بود و نشان داد رژیم صهیونیستی در کدنویسی و ابزارهای جنگ سایبری برتری دارد. این ویروس به‌عنوان نخستین سلاح سایبری واقعی شناخته شد، چراکه بدون سابقه‌ای برای اجرا یا مدیریت پیامدها به کار گرفته شد. کشف آن نه در ایران بلکه پس از خروج از محیط نطنز صورت گرفت. هرچند امروز تهدید آن کاهش یافته، در آن زمان ایران از آسیب‌پذیری‌های خود آگاه نبود و استاکس‌نت انگیزه‌ای جدی برای تقویت برنامه‌های دفاع سایبری ایران شد (Bishop, 2022: 9).

در آوریل ۲۰۱۱، ایران از شناسایی ویروس «ستاره‌ها» خبر داد که با تقلید از فایل‌های دولتی قصد نفوذ به تأسیسات هسته‌ای داشت. غلامرضا جلالی، رئیس سازمان پدافند غیرعامل، ایالات متحده و رژیم صهیونیستی را مسئول معرفی کرد. در نوامبر همان سال، ویروس «دوکو» شناسایی شد که از کدهای مشابه استاکس‌نت بهره می‌برد. سپس در آوریل ۲۰۱۲، بدافزار «وایپر» کشف شد که دیسک‌های سخت وزارت نفت و شرکت ملی نفت ایران را پاک کرده بود و شباهت‌های زیادی با استاکس‌نت و دوکو داشت. در مه ۲۰۱۲ نیز ویروس «شعله» معرفی شد که رایانه‌های دولتی را آلوده و اطلاعات حساس را سرقت می‌کرد. گزارش‌ها حاکی است رژیم صهیونیستی و آمریکا از آن برای جمع‌آوری اطلاعات و آماده‌سازی کمپین‌های گسترده‌تر بهره بردند. موشه یعلون، معاون نخست‌وزیر وقت رژیم صهیونیستی، ضمن رد دخالت مستقیم تأکید کرد که این رژیم از همه ابزارهای ممکن برای آسیب به برنامه هسته‌ای ایران استفاده خواهد کرد. این رخدادها پیش از توافق هسته‌ای ایران با گروه ۵+۱ اتفاق افتاد و پس از آن متوقف شد. اما پس از خروج آمریکا از برجام، حملات بار دیگر از سر گرفته شد. در دوم ژوئیه ۲۰۲۰ انفجاری در سایت اصلی غنی‌سازی نطنز رخ داد که خسارات سنگینی وارد کرد و برنامه‌های ایران را چند ماه به تأخیر انداخت. این انفجار به کارخانه سانتریفیوژهای نسل IR-4 و IR-6 آسیب زد و رژیم صهیونیستی متهم به کارگذاری بمب شد. در آوریل ۲۰۲۱ نیز حمله سایبری شدیدی علیه نطنز رخ داد که منجر به خاموشی گسترده شد. این حمله سیستم برق سانتریفیوژها را مختل کرد و برنامه غنی‌سازی را تا نه ماه عقب انداخت. زمان‌بندی این حمله مهم بود؛ درست پس از اعلام ایران مبنی بر نصب سانتریفیوژهای پیشرفته و آغاز غنی‌سازی ۶۰ درصدی و همزمان با مذاکرات احیای برجام. بسیاری آن را نشانه تمایل رژیم صهیونیستی به اقدام مستقل دانستند، حتی در صورت تداوم مسیر دیپلماتیک (Mirzaei & Ghorashi, 2024: 325-327). به‌طور کلی، حملات سایبری علیه تأسیسات هسته‌ای ایران از ۲۰۰۹ تا ۲۰۲۱ نشان‌دهنده گذار به مرحله‌ای جدید از جنگ سایبری است. استاکس‌نت آغازگر این روند بود و پس از آن، ویروس‌هایی چون ستاره‌ها، دوکو، وایپر و شعله به‌کار گرفته شدند. در ادامه، حملات فیزیکی و سایبری به نطنز بارها برنامه هسته‌ای ایران را مختل کرد. این تجربه‌ها اهمیت فضای سایبری به‌عنوان میدان نوین تقابل ژئوپلیتیکی را برجسته کرده و نشان داده است که ایران و رژیم صهیونیستی با حمایت آمریکا درگیر یکی از پیچیده‌ترین نمونه‌های جنگ سایبری در جهان هستند.

DOR: 20.1001.1.30926459.1404.2.4.3.1

۴ـ۲ـ عملیات نیوزکستر

پس از حمله استاکس‌نت، ایران با تأسیس فرماندهی دفاع سایبری و یک بخش امنیت سایبری جدید تحت عنوان «سازمان پدافند غیرعامل»، اقدام به ایجاد ساختاری برای محافظت از سیستم‌های اطلاعاتی داخلی در برابر نفوذ دشمنان خارجی به شبکه‌های کلیدی کرد. لازم به ذکر است که توانایی‌های آفندی سایبری ایران صرفاً معطوف به رژیم صهیونیستی نبوده و سایر کشورهای متخاصم را نیز در بر می‌گرفت. با این حال، با بررسی آمار حملات صورت‌گرفته، آشکار است که گروه‌های هکری ایرانی، رژیم صهیونیستی را به‌عنوان هدف اصلی اولویت‌بندی کرده‌اند. به‌عنوان مثال، کمپین سایبری سال ۲۰۱۴ موسوم به عملیات «نیوزکستر» یکی از برجسته‌ترین نمونه‌های جنگ سایبری مبتنی بر مهندسی اجتماعی و نفوذ اطلاعاتی است که نخستین بار توسط پژوهشگران امنیتی۲۰۱۴ شناسایی و گزارش شد. این عملیات که آغاز آن به اوایل دهه ۲۰۱۰ بازمی‌گردد، با ایجاد پروفایل‌ها و هویت‌های جعلی در شبکه‌های اجتماعی همچون فیس‌بوک، لینکدین و توییتر، افراد و نهادهای کلیدی در ایالات متحده، رژیم صهیونیستی، عربستان سعودی و چند کشور دیگر را هدف قرار داد. در چارچوب این کمپین، هکرهای ایرانی هویت‌های ساختگی شامل روزنامه‌نگاران، کارشناسان دفاعی و کارکنان سازمان‌های بین‌المللی ایجاد کردند. یکی از ابزارهای اصلی آنان یک پایگاه خبری جعلی با نام «نیوزآنایر» بود که در تهران ثبت شده و به‌عنوان پشتوانه اطلاعاتی برای شخصیت‌های ساختگی به‌کار گرفته می‌شد. مهاجمان از طریق این هویت‌های جعلی اعتماد قربانیان را جلب کرده و سپس آنان را به صفحات فیشینگ یا بدافزارهای طراحی‌شده هدایت می‌کردند. بر اساس گزارش‌های منتشرشده بیش از دو هزار نفر از مقام‌های سیاسی، نظامی، روزنامه‌نگاران و تحلیلگران امنیتی در سراسر جهان هدف این عملیات قرار گرفتند و با بهره‌گیری از توانمندی‌های فناورانه، برخی از منابع مدعی هستند که ایران بیش از ۲۰۰۰ رایانه را آلوده کرده و حتی به اطلاعات محرمانه برخی نهادهای دولتی رژیم دست یابد. اگرچه ماهیت دقیق اطلاعات به‌دست‌آمده مشخص نشد، اما گستردگی اهداف و استمرار چندساله عملیات نشان می‌دهد که ایران در پی توسعه یک شبکه اطلاعاتی غیرمستقیم و پایدار در چارچوب رقابت سایبری بوده است (Amaliya, 2025: 4).

تلاش‌های آفندی ایران پس از حمله استاکس‌نت علیه رژیم صهیونیستی، بر همکاری با گروه‌های هکری همچون حماس و حزب‌الله متمرکز بود تا عملیات‌هایی را علیه نهادهای مختلف رژیم صهیونیستی از جمله آژانس امنیتی این کشور، فرماندهی جبهه داخلی، دفتر نخست‌وزیری، وزارت دفاع، بانک اورشلیم، خطوط هواپیمایی ملی، احزاب سیاسی لیکود و کادیما و همچنین

اجزای عملیاتی ارتش رژیم صهیونیستی انجام دهند. بر اساس گزارش‌های منتشرشده، در بازه زمانی ۲۰۱۲ تا ۲۰۱۵، یکی از هکرهای برجسته حماس به نام «جواد اودح» با موفقیت به شبکه‌های ارتباطی داده‌های ارتش رژیم صهیونیستی نفوذ کرد و پیوندهای داده‌ای هواپیماهای بدون سرنشین ارتش رژیم صهیونیستی را که بر فراز غزه پرواز می‌کردند، دریافت نمود. این نفوذ برای فرماندهان نظامی در غزه این امکان را فراهم آورد که تصویری پایدار از فعالیت پهپادهای نظارتی رژیم صهیونیستی به‌دست آورده و خود را از دایره نظارت آن‌ها خارج کنند (Mirzaei & Ghorashi, 2024: 330). از منظر ژئوپلیتیک سایبری، عملیات نیوزکستر را می‌توان بخشی از رقابت راهبردی جمهوری اسلامی ایران و رژیم صهیونیستی در فضای مجازی دانست. رژیم صهیونیستی بارها ایران را متهم به انجام این عملیات کرده و آن را تهدیدی علیه امنیت ملی خود معرفی نموده است. در مقابل، ایران با بهره‌گیری از چنین اقدامات اطلاعاتی و سایبری، کوشیده است تا بخشی از برتری فناورانه و اطلاعاتی دشمنان خود را خنثی کند و در قالب بازدارندگی نامتقارن موقعیت خود را تثبیت نماید. از این‌رو، عملیات نیوزکستر نمونه‌ای شاخص از جنگ سایبری غیرمتقارن و کم‌هزینه محسوب می‌شود که بر مواجهه نرم اطلاعاتی میان ایران و رژیم صهیونیستی متمرکز بوده است.

۴ـ۳ـ حمله سایبری به زیرساخت‌های آب و فاضلاب رژیم صهیونیستی

یک دهه پس از استاکس‌نت، جنگ سایبری ایران و رژیم صهیونیستی آشکارتر و پرشتاب‌تر شده و بیش‌ازپیش در معرض دید عموم قرار گرفته است. عمومی‌سازی حملات سایبری مزایا و معایبی دارد که رژیم صهیونیستی و ایران هنگام بازی در صفحه‌ی شطرنج جنگ سایبری باید در نظر گیرند. در آوریل ۲۰۲۰ یکی از نمونه‌های برجسته استفاده از افکار عمومی به‌عنوان ابزار، برای نخستین‌بار به نمایش گذاشته شد. رژیم صهیونیستی به رسانه‌ها اطلاع داد که حمله‌ای سایبری شبکه‌ی آب و فاضلاب این کشور را هدف قرار داده است، اما هیچ اطلاعاتی درباره گروه یا دولت عامل ارائه نکرد. هدف حمله، افزایش سطح کلر در آب آشامیدنی رژیم صهیونیستی تا میزان خطرناک بود. کلر هرچند به‌طور رایج برای ضدعفونی آب به‌کار می‌رود، اما افزایش بیش از حد آن می‌تواند تهدیدی جدی برای سلامت جمعیت محسوب شود. هکرهای ایرانی توانستند به سامانه‌های «اس سادا[1]» که وظیفه نظارت و کنترل سطح کلر را بر عهده داشت، نفوذ کنند و در برخی از مراکز آبی، سیستم‌ها به‌صورت ناگهانی از حالت خودکار خارج و در وضعیت دائمی کار قرار گرفتند؛ در موردی دیگر، سامانه‌های عملیاتی کاملاً تحت کنترل مهاجمان درآمدند و در نتیجه پمپ‌ها متوقف

[1] SCADA

DOR: 20.1001.1.30926459.1404.2.4.3.1

شدند یا به‌طرز ناهمگونی عمل کردند. بر اساس گزارش‌ها، مهاجمان با دسترسی به این سیستم‌ها تلاش کردند میزان کلر ورودی به آب را افزایش دهند؛ سناریویی که در صورت موفقیت‌آمیز بودن، می‌توانست منجر به مسمومیت گسترده شود. این حمله با برنامه‌ریزی، منابع و جمع‌آوری اطلاعات پیشرفته صورت گرفت. «ییگال اونا»، رئیس وقت اداره ملی سایبری رژیم صهیونیستی، هرچند مستقیماً ایران را نام نبرد یا درباره حمله تلافی‌جویانه رژیم صهیونیستی دو هفته بعد اظهار نظر نکرد، اما هشدار داد که تحولات اخیر «عصر جدیدی از جنگ پنهان» را آغاز کرده و به‌طور نمادین گفت: «زمستان سایبری در راه است» (Haroon, 2024). زیرساخت‌های آب عموماً کمتر در معرض حملات سایبری تصور می‌شوند، اما این حمله نشان داد که حتی چنین تأسیساتی نیز هدف‌پذیر هستند. مقامات اطلاعاتی رژیم صهیونیستی و غربی این حمله را به ایران نسبت دادند، در حالی که دولت ایران مسئولیت حملات به سیستم آبی رژیم را رد کرد و مدعی شد که موضع سایبری ایران کاملاً دفاعی است و این کشور نمی‌تواند اقداماتی را که ممکن است به غیرنظامیان رژیم صهیونیستی آسیب برساند، تحمل کند. با این وجود در ژوئن ۲۰۲۰، هکرها تأسیسات مدیریت آب رژیم صهیونیستی را هدف قرار دادند و به پمپ‌های آب کشاورزی در منطقه جلیل علیا و مرکز این کشور حمله کردند. این رویدادها حاکی از آن است که مفهوم بازدارندگی در فضای سایبری به دلیل ماهیت غیرملموس و انکارپذیری حملات، با بازدارندگی در عرصه متعارف بسیار متفاوت است و اجرای آن با دشواری‌های فراوانی همراه است؛ چرا که شناسایی متجاوز و تعیین پاسخ متناسب در محیط سایبری از پیچیدگی خاصی برخوردار است (Mirzaei & Ghorashi, 2024: 325-327). از منظر واقع‌گرایی، این حمله نشان‌دهنده تلاش ایران برای نمایش توانمندی‌ها و آمادگی‌های خود در حوزه سایبری بود تا از این طریق دشمنانش را مهار کند. در مقابل، رژیم صهیونیستی بر اساس اصل «چشم در برابر چشم» به فرودگاه ایران حمله کرد. به گزارش منابع اطلاعاتی و امنیتی، این حمله سایبری توسط نیروهای رژیم صهیونیستی انجام شد که «احتمالاً در تلافی تلاش ایران برای نفوذ به سامانه‌های آبرسانی روستایی رژیم صهیونیستی» صورت گرفت. از منظر تبیینی و ژئوپلیتیکی، این حمله نمادی از تحول در نوع تقابل ایران و رژیم صهیونیستی است؛ راهبردی که به جای رویارویی نظامی مستقیم، از ابزار سایبری برای اعمال فشار و ایجاد بازدارندگی استفاده می‌کند. با توجه به اهمیت حیاتی زیرساخت‌های آب برای امنیت داخلی، جنگ سایبری در این حوزه به‌عنوان بخشی از تقابل ژئوپلیتیک و بازتعریف موازنه قدرت میان دو کشور قابل تحلیل است.

۴ـ۴ـ حوادث بندر شهید رجایی

در نهم مه ۲۰۲۰، رایانه‌های تنظیم‌کننده ترافیک دریایی در بندر شهید رجایی واقع در سواحل جنوبی ایران در خلیج‌فارس، مورد حمله سایبری قرار گرفتند و شاهد توقف ناگهانی و کامل سیستم‌های کامپیوتری کنترل حرکت شناورها، کامیون‌ها و کالاها بود؛ پدیده‌ای که موجب ایجاد ترافیک طولانی بر جاده‌ها و محبوس شدن کشتی‌ها در اسکله‌ها شد. این اختلال به‌سرعت شناسایی و اعلام شد که ناشی از حمله سایبری بوده است. گزارش‌ها حاکی است که رژیم صهیونیستی در ۹ مه ۲۰۲۰ حمله سایبری به بندر شهید رجایی در بندرعباس را انجام داد. این بندر به‌عنوان یکی از مراکز اصلی لجستیکی کشور، بیش از ۸۵ درصد بار واردات و صادرات ایران را جابه‌جا می‌کند. تصاویر ماهواره‌ای نشان دهنده تداوم اختلالات و تأخیرهای گسترده در مسیرهای ورود و خروج وسایل نقلیه به ترمینال‌های کانتینری بود. بر اساس گزارش واشنگتن‌پست، رژیم صهیونیستی عامل پشت پرده این حمله بود، هرچند این رژیم هرگونه مسئولیتی در قبال آن را نپذیرفت. با این وجود رسانه‌های غربی و رژیم صهیونیستی این حادثه را به عملیات تهاجمی دولت رژیم صهیونیستی نسبت داده‌اند که گفته می‌شود در واکنش مستقیم به تلاش ایران برای نفوذ به شبکه‌های آب رژیم صهیونیستی در آوریل ۲۰۲۰ انجام شده است (Abbasi, 2024: 9). ایران این حمله را تأیید کرد ولی یک مقام مسئول در بندر «شهید رجایی» ضمن رد ادعای حمله موفق به تأسیسات این بندر گفت: «در هفته گذشته برخی اختلال‌ها در سامانه‌های رایانه‌ای بندر به وقوع پیوست که می‌تواند ناشی از حمله سایبری باشد، ولی با توجه به آمادگی کامل واحدهای پدافند غیرعامل در تأسیسات بندر شهید رجایی و مقابله به موقع و مؤثر با اشکالات به وجود آمده، هیچ‌گونه اخلالی در روند فعالیت‌های جاری ایجاد نشد». آموس یدلین، مقام سابق امنیتی رژیم صهیونیستی نیز در گفتگو با روزنامه تایمز رژیم صهیونیستی با تأیید این خبر، یادآور شد که این حمله در واکنش به عملیات سایبری ماه آوریل ایران به «تأسیسات آب» انجام شده است. مقام سابق امنیتی رژیم صهیونیستی تأکید کرده که رژیم صهیونیستی حمله به تأسیسات غیرنظامی خود را برنمی‌تابد و بر پایه همین رویکرد از طریق حمله سایبری اخیر به ایران هشدار داده که می‌تواند با استفاده از ابزارهای مدرن اقتصاد این کشور را دچار اخلال جدی کند. روزنامه تایمز رژیم صهیونیستی تأیید کرده که انجام حمله متقابل سایبری به تأسیسات ایران، پیش از انجام در نشست محرمانه کابینه امنیتی رژیم صهیونیستی بررسی شده بود. همچنین برخی رسانه‌ها نیز با انتشار فرضیه‌ای غیررسمی احتمال داده‌اند که حمله سایبری رژیم صهیونیستی با هدف اخلال در روند بارگیری و حرکت ۵ نفت‌کش ایرانی بوده که با محموله بنزین

DOR: 20.1001.1.30926459.1404.2.4.3.1

و با نادیده گرفتن تحریم‌ها و هشدارهای آمریکا، عازم ونزوئلا شده‌اند (Tabnak, 2020). در تحلیل ژئوپلیتیکی، حمله رژیم صهیونیستی به بندر شهید رجایی پیامی آشکار برای ایران قلمداد می‌شد تا خطوط قرمز در فضای سایبری برای رژیم صهیونیستی تعیین نشده است و هدف‌گیری زیرساخت‌های حیاتی غیرنظامی نیز امکان پذیر است. در مجموع، این حادثه نمادی از تحولات جدی در رقابت سایبری میان ایران و رژیم صهیونیستی به‌شمار می‌رود؛ جنگی دیجیتال که برخلاف تقابل نظامی کلاسیک، از ابزارهای پنهان و دقیق برای اعمال فشار و بازدارندگی بهره می‌برد و به‌طور فزاینده در ساختار امنیت منطقه جلب توجه کرده است.

۴ـ۵ـ طوفان الاقصی

درپی آغاز عملیات طوفان الاقصی[1] در ۷ اکتبر ۲۰۲۳، جنگ سایبری میان ایران و رژیم صهیونیستی وارد مرحله‌ای عمیق و گسترده شد و تنش‌های سیاسی و تشدید درگیری، جنگ میان این دو ابرقدرت غرب آسیا را اجتناب‌ناپذیر ساخته است. نظام آنارشیک بین‌المللی باعث شده رژیم صهیونیستی برای تقویت قدرت خود در منطقه غرب آسیا تلاش کند. بر اساس گزارش اکونومیست شدت حملات سایبری ایران و رژیم صهیونیستی سه برابر نسبت به قبل افزایش یافته است و هدف‌گیری سایبری رژیم صهیونیستی توسط ایران پس از آغاز درگیری گسترده‌تر منطقه‌ای، به‌شدت افزایش یافته است. پس از جنگ حماس و رژیم صهیونیستی در سال ۲۰۲۳، ایران سامانه‌های راداری رژیم صهیونیستی را در عرض چند هفته مورد حمله قرار داد. همچنین، ایران عملیات‌های متعدد رسانه‌ای با هدف بی‌ثبات‌سازی امنیت سایبری رژیم صهیونیستی انجام داده است. برای مثال، حسابی به نام «اشک‌های جنگ» که ظاهراً متعلق به فعالان رژیم صهیونیستی منتقد نتانیاهو بود، ایجاد شد. همچنین حسابی با نام «کارما» توسط واحد اطلاعاتی ایران ایجاد شد که خود را نماینده رژیم صهیونیستی‌های خواهان استعفای نتانیاهو معرفی می‌کرد (Umar, 2025: 7). از این‌رو گروه‌های سایبری وابسته به ایران به‌شکلی منسجم و هدفمند، تسلط خود را بر زیرساخت‌های دیجیتال رژیم صهیونیستی گسترش دادند؛ اقدامی که نمادی بارز از تغییر ماهیت منازعات ژئوپلیتیکی در فضای سایبری مدرن بود. بر اساس گزارش هوش تهدیدات سایبری کوروم[2] پس از آغاز این عملیات، ایران به شرایطی فعالانه‌تر در نبرد سایبری روی آورد؛ برخلاف رویکرد دفعی پیشین، حملات سایبری به شکلی هماهنگ و رو به افزایش انجام می‌گرفت. رژیم صهیونیستی در این دوره عمده

[1] Operation Al-Aqsa Storm
[2] Quorum Cyber Threat Intelligence

هدف حملات سایبری، عملیات نفوذ و حملات خرابکارانه علیه زیرساخت‌های حیاتی خود را تجربه کرد. حتی گزارش‌های رسانه‌ای فارسی‌زبان حاکی از آن است که از زمان آغاز عملیات «طوفان الاقصی» تاکنون، بیش از ۱۳۱ حمله سایبری علیه اهداف رژیم صهیونیستی اعلام شده است. بررسی داده‌های موجود نشان می‌دهد که بیشترین تعداد این حملات در ماه مهر به ثبت رسیده است؛ دوره‌ای که هم‌زمان با آغاز عملیات طوفان الاقصی در سال ۲۰۲۳، سالگرد آن در ۲۰۲۴ و همچنین عملیات موسوم به «وعده صادق ۲» ایران بوده است. بر اساس این داده‌ها، ۲۹ حمله سایبری در این بازه گزارش شده که این ماه را در صدر نمودار حملات سایبری قرار می‌دهد. همچنین تداوم تعداد بالای حملات در ماه‌های بعد نشان دهنده استمرار فاز تهاجمی سایبری در پی رویدادهای میدانی و حملات هوایی رژیم صهیونیستی به نوار غزه ارزیابی شده است. افزون بر آن، عملیات خرابکارانه رژیم علیه ایران در نوامبر ۲۰۲۴ نیز زمینه‌ساز واکنش سایبری گروه‌های مقاومت و تشدید حملات الکترونیکی در این ماه شده است. در مارس ۲۰۲۴ نیز جهش محسوسی در تعداد حملات مشاهده می‌شود که هم‌زمان با اولین پاسخ موشکی رسمی ایران در قالب عملیات وعده صادق ۱ به رژیم صهیونیستی است. این هم‌راستایی زمانی، حاکی از هم‌افزایی بین قدرت موشکی و ظرفیت سایبری جمهوری اسلامی در پاسخ به اقدامات صهیونیست‌ها است. این حملات از اخلال در خدمات حیاتی تا نفوذ به سامانه‌های امنیتی را دربر می‌گرفت به طوری‌که فرمانده مرکز رایانه ارتش این رژیم اعلام کرده که حدود سه میلیارد حمله سایبری علیه سیستم‌های رایانه‌ای ارتش رژیم صهیونیستی از زمان آغاز جنگ انجام شده، اگرچه به ادعای او همه این حملات مهار شده‌اند (ISNA, 2025; mashregh, 2025). در تبیین ژئوپلیتیکی این روند می‌توان گفت حملات سایبری پس از عملیات طوفان الاقصی نشان دهنده تحولی در ماهیت جنگ مدرن است و از ابعاد متعارف و آشکار به سوی جنگ ترکیبی[1] سایبری تبدیل شده است؛ روشی که نفوذ، روان‌سازی و اخلال اطلاعاتی را در اهداف امنیتی و سیاسی هم‌زمان دنبال می‌کند و این تحولات، چشم‌انداز رقابت سایبری میان ایران و رژیم صهیونیستی را به‌طور قابل توجهی تقویت کرده است.

[1] ترکیب هم‌زمان ابزارهای متعارف، نامتقارن، سایبری، اطلاعاتی و روانی برای دستیابی به اهداف راهبردی در یک منازعه است.

DOR: 20.1001.1.30926459.1404.2.4.3.1

۴ـ۶ـ جنگ تحمیلی ۱۲ روزه

پیش از آغاز حملات متعارف، رژیم صهیونیستی با بهره‌گیری از عملیات سایبری موفق شد رادارها و سامانه‌های ارتباطی نظامی ایران را از کار بیندازد و زمینه را برای حملات نیروی هوایی رژیم صهیونیستی[1] بدون مقاومت فراهم کند. اندکی پس از علنی شدن عملیات نظامی رژیم صهیونیستی، فعالیت در کانال‌های تلگرام به‌طور چشمگیری افزایش یافت؛ فعالیت‌هایی که شامل کارزارهای هماهنگ تبلیغاتی و بسیج نیروهای سایبری همسو با ایران بود. شماری از این گروه‌ها به کشورهای همسایه رژیم صهیونیستی هشدار دادند که در صورت حمایت از تل‌آویو، با پیامدهای جدی مواجه خواهند شد، در حالی‌که برخی دیگر مدعی انجام موفق حملات سایبری علیه زیرساخت‌های رژیم صهیونیستی شدند؛ هرچند اغلب این ادعاها تأیید نشد. در روزهای نخست درگیری، بازیگران سایبری همسو با دو طرف به‌طور قابل‌توجهی فعالیت خود را افزایش دادند. مشهورترین گروه وابسته به رژیم صهیونیستی با عنوان گنجشک درنده[2] که سابقه حملات گسترده علیه ایران را دارد، به‌طور علنی مسئولیت یک حمله سایبری علیه نهادهای مالی ایران را برعهده گرفت. گروه‌های طرفدار رژیم صهیونیستی حملات پرشدتی علیه زیرساخت‌های مالی ایران انجام دادند که از جمله شامل یک سرقت بزرگ رمزارزی به ارزش ۹۰ میلیون دلار بود. به نظر می‌رسد این حمله به سامانه‌های بانکی ایران تلاشی حساب شده برای تضعیف ثبات مالی کشوری بود که پیش‌تر نیز تحت فشار تحریم‌های بین‌المللی قرار داشت. در مقابل، ارزیابی‌های متعدد طی سال‌های گذشته نشان داده‌اند که ایران از یک شبکه پیچیده از تهدیدهای مداوم پیشرفته[3] آ پ تی‌ها برخوردار است و از آن‌ها برای جاسوسی و اقدامات اخلال‌گرانه استفاده می‌کند. در جریان جنگ ۱۲ روزه نیز گروه‌های حامی ایران فعالیت سایبری خود را افزایش دادند و از نظر حجم، بر گروه‌های همسو با رژیم صهیونیستی پیشی گرفتند. در یک نمونه، گروه باج‌افزاری Pay2Key.I2P که به ایران وابسته دانسته می‌شود، تا ۸۰ درصد از سود پرداخت‌های را به همکارانی وعده داد که حاضر باشند حملات سایبری علیه رژیم صهیونیستی و ایالات متحده انجام دهند. منابع اطلاعات متن‌باز اوسینت[4] نیز ظهور بازیگران جدیدی مانند، شکارچیان شب، نیروی سایبری نقابداران تونسی، شمشیر سیاه[5] و دیگران را گزارش کردند؛ گروه‌هایی که به‌طور فعال در خدمت اهداف طرف‌های درگیر عمل کرده و مرز

[1] IAF
[2] Predatory Sparrow
[3] APT
[4] OSINT
[5] Night Hunters ،Tunisian Maskers Cyber, ForceBlacksword

میان عملیات‌های دولتی و جنگ دیجیتال غیرمتمرکز را بیش از پیش مبهم ساختند. همچنین هکرهای ایرانی تلاش کردند با نفوذ به دوربین‌های امنیتی متصل به اینترنت در رژیم صهیونیستی، اطلاعات زنده گردآوری کنند تا دقت حملات موشکی را افزایش دهند (Sharma, 2025: 4-7). ویژگی خاص فضای سایبری این است که عوامل تهدید، اغلب حتی پس از توقف خصومت‌های متعارف، به درگیری خود ادامه می‌دهند. اگرچه کاهش محسوسی در فعالیت‌های سایبری پس از آتش‌بس مشاهده شد، اما عملیات تهاجمی در قلمرو سایبر به‌طور کامل متوقف نگردید. اگرچه رویارویی نظامی مستقیم بین رژیم صهیونیستی و ایران بی‌سابقه بود، اما عملیات سایبری تهاجمی، نشان‌دهنده تغییر محسوسی در روش سنتی انجام جنگ سایبری بین این دو دولت نبود. این عملیات‌ها بیشتر یک «مزیت تدریجی» در درگیری فراهم کردند تا این‌که نتیجه‌ای با سودمندی راهبردی عمیق به ارمغان آورند. اگرچه برنده واضحی در درگیری سایبری ایران و رژیم صهیونیستی وجود نداشت، اما جمهوری اسلامی در محافظت از زیرساخت‌های حیاتی خود با تمام چالش‌ها و ضربه‌ها موفق عمل کرد، در حالی که رژیم صهیونیستی آسیب جدی دیده است. به احتمال زیاد، هر دو کشور تا تشدید درگیری بعدی به استفاده از عملیات سایبری به عنوان بخشی از تاکتیک‌های «منطقه خاکستری» ادامه خواهند داد.

نتیجه‌گیری

بررسی ژئوپلیتیک جنگ سایبری در مناقشه ایران و رژیم صهیونیستی در پرتو واقع‌گرایی نشان می‌دهد که ذات قدرت‌طلبی دولت‌ها موجب شده است این دو بازیگر، در پی تحکیم موقعیت خود از رهگذر ابزارهای نوین فناورانه باشند. در این چارچوب، جنگ سایبری به صحنه‌ای برای رقابت هژمونیک بدل شده است؛ رژیم صهیونیستی با اتکا به فناوری پیشرفته و حمایت غرب می‌کوشد موقعیت مسلط خود را حفظ کند، در حالی که ایران با توسعه توان بومی و شبکه نیابتی، مانع تثبیت کامل این هژمونی می‌شود که حمله به تأسیسات هسته‌ای ایران با ویروس استاکس‌نت، نقطه آغاز این تقابل بود. رژیم صهیونیستی نشان داد که قادر است از فاصله دور به زیرساخت‌های حیاتی ایران ضربه بزند و از این طریق پیام بازدارندگی بفرستد. در واکنش، ایران نیز کوشید با عملیات نیوزکستر و اقدامات مشابه، توان سایبری خود را برای مقابله به نمایش بگذارد. این اقدامات گرچه خسارت محدودی داشت، اما نشان داد تهران می‌تواند وارد میدان متقابل شود و مانع یک‌سویه بودن قدرت رژیم صهیونیستی گردد در ادامه، تقابل به زیرساخت‌های حیاتی کشیده شد و حمله سایبری به شبکه

DOR: 20.1001.1.30926459.1404.2.4.3.1

آب و فاضلاب رژیم صهیونیستی که به ایران نسبت داده شد، بیانگر توان ایران در هدف‌گیری امنیت داخلی رژیم صهیونیستی بود. در برابر، رژیم صهیونیستی نیز با عملیات‌هایی مانند حادثه بندر شهید رجایی، مسیرهای حیاتی اقتصادی ایران را مختل کرد تا نشان دهد همچنان برتری تکنولوژیک دارد. این رقابت سایبری با تحولات میدانی پیوند یافت و در طوفان الاقصی ۲۰۲۳، گروه‌های مقاومت از فضای مجازی و ابزارهای دیجیتال برای هماهنگی حملات و جنگ روانی علیه رژیم صهیونیستی بهره گرفتند. به همین شکل، در جنگ تحمیلی ۱۲ روزه نیز ترکیب سامانه‌های هوش مصنوعی رژیم صهیونیستی (مانند گنبد آهنین) با عملیات سایبری ایران و متحدانش، شکل تازه‌ای از نبرد چندلایه را به نمایش گذاشت. از منظر واقع‌گرایی کلاسیک، همه این رخدادها نشان می‌دهد که دو طرف از منطق قدرت پیروی می‌کنند: رژیم صهیونیستی با استفاده از فناوری سایبری و هوش مصنوعی، در پی تثبیت موقعیت هژمونیک خویش است؛ ایران نیز با توسعه ظرفیت‌های بومی و بهره‌گیری از بازیگران منطقه‌ای، این هژمونی را به چالش می‌کشد. نتیجه اما چیزی جز تشدید چرخه بی‌ثباتی نیست. به بیان دیگر، جنگ سایبری در غرب آسیا صرفاً یک ابزار امنیتی نیست، بلکه میدان اصلی رقابت هژمونیک میان ایران و رژیم صهیونیستی شده است. رژیم صهیونیستی آن را به ابزاری برای مهار ایران بدل ساخته، اما ایران نیز با بهره‌گیری از توان بازدارندگی متقابل، خود را به بازیگری فعال و تأثیرگذار در بازتعریف موازنه قدرت سایبری منطقه‌ای تبدیل کرده است. در نهایت، همان‌گونه که واقع‌گرایی پیش‌بینی می‌کند، این رقابت قدرت‌طلبانه نه به ثبات پایدار، بلکه به بازتولید ناامنی و بی‌ثباتی در غرب آسیا منجر شده است.

تعارض منافع

بنا بر اظهار نویسندگان، مقاله پیش‌رو فاقد هر گونه تعارض منافع بوده است.

Translated References to English

Abbasi, U. (2024). Cyber Threats to Iran from USA and Israel: Counter Strategies by Iran. Global Strategic & Security Studies Review, IX(I), 44-56.

Amaliya, L.R. (2025). A Cyber War of Iran-Israel: A Geopolitical Rivalry. https://www.atlantis-press.com/proceedings/icsgs-24/126008135

Bahgat, G., Anoushiravan E. (2021). Defending Iran: From Revolutionary Guards to Ballistic Missiles. Cambridge: Cambridge University Press.

Bishop, H. (2022). What are the motivations behind Israel's cyber war with Iran, and the implications it has today?. https://sites.wp.odu.edu/ids493hbish001/wp-content/uploads/sites/33133/2023/04/IDS-300W.pdf.

Cano, D.P. (2025). The Strategic Thinking of the Islamic Republic of Iran: continuity, evolution or change after the War in Gaza?.

https://www.defensa.gob.es/documents/2073105/2320887/el_pensamiento_estrategico_de_la_republica_islamica_de_iran_eng.pdf/c640f4c3-6695-fd49-d968-f63ab355ac08?t=1736337940701.

Ebrahimi, F., et al. (2017). Donald Trump and the legacy of Obama's realist policy in West Asia. *Global Politics Quarterly*, 6(2), 123–153. [**In Persian**]

Elhami, A.H., et al. (2024). Military activities of the Zionist regime in Southwest Asia after the Syrian crisis. *Islamic Awakening Studies Quarterly*, 13(2), 77–110. [**In Persian**]

Farhadian, M., Modarres, M., & monavari, S. A. (2024). Israel and the official narrative of national security of the Islamic Republic of Iran. Security Horizons, 17(63), 183-213. [**In Persian**]

Gaietta, M. (2025). Iran's Nuclear Programme after the 12-Day War: Options and Challenges. https://www.iai.it/en/pubblicazioni/c03/irans-nuclear-programme-after-12-day-war-options-and-challenges.

Golmohammadi, V., & Jamshidi, T. (2022). Cyber deterrence and the transformation of the Zionist regime's security-defense doctrine. *Journal of Political Geography Research*, 7(4), 1–23. [**In Persian**]

Habibi, A., & Abbasi Karafashani, A (2024). Cyberspace in the offensive and defensive strategy of the Zionist regime from the perspective of upstream documents. *Fundamental and Applied Studies of the Islamic World*, 6(4), 139–164. [**In Persian**]

Haroon, A. (2024). AI and Cyber Drove Warfare in the Israeli-Iran Conflict and its Impact on Gulf States' Security. Journal of Politics and International Studies Vol. 10, No. 2, July–December 2024, pp.145–163.

ISNA. (2025). 3 billion cyberattacks registered against the Zionist regime since the beginning of Operation Al-Aqsa Storm. Retrieved from https://www.isna.ir/news/1403042315775. [**In Persian**]

Joshua, D. (2022). IRAN, ISRAEL, AND THE STRUGGLE FOR THE SKIES OVER THE MIDDLE EAST. JOURNAL OF STRATEGIC AIRPOWER & SPACEPOWER, https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-2_Number-1/Dryden-Iran-Israel-and-the-Struggle.pdf.

Mashregh News. (2025). A look at overt cyberattacks against the Zionist regime since October 7: From disruption of vital services to the disclosure of classified data. Retrieved from https://www.mashreghnews.ir/news/1732523. [**In Persian**]

Mirzaei, M, & Ghorashi, Y. (2024). Cyber Trojan horses in Asia: An analysis of the confrontation between the Zionist regime and Iran after the Stuxnet attack . *Iranian Journal of Asian Studies*, 1(1), 309–331. [**In Persian**]

Ostovar, A. (2019). The Grand Strategy of Militant Clients: Iran's Way of War. Security Studies 28, no. 1.

Qeitasi, S., Ahmadinejad, H., Mousavi-Tabar, S.A (2024), The grey zone: The Zionist regime's strategy against Iran (2010–2023). *Fundamental and Applied Studies of the Islamic World*, 6(1), 235–258. [**In Persian**]

Rodman, D. (2022). Sword and Shield of Zion: The Israel Air Force in the Arab-Israeli Conflict, 1948–2012, Brighten, UK: Sussex Academic Press.

Sharma, R.K. (2025). The 12-Day War: Cyber Frontlines between Israel and Iran. https://www.idsa.in/wp-content/uploads/2025/08/Commentary-Mr-Rohit-Kumar-Sharma-11-August-2025.pdf.

Slater, J. (2021). Mythologies Without End: The US, Israel, and the Arab-Israeli Conflict, 1917–2020. Oxford University Press.

Tabnak. (2020). Escalation of cyber war between Iran and the Zionist regime with the attack on Shahid Rajaee Port. Retrieved from https://www.tabnak.ir/fa/news/979587. [**In Persian**]

Umar, M. (2025). Iran and Israel Cyber Warfare and Interference of US. https://policyjournalofms.com/index.php/6/article/view/824.

DOR: 20.1001.1.30926459.1404.2.4.3.1