فصلنامه علمی شناخت پژوهی مطالعات سیاسی
سال ۲، شماره ۴(۷)، ۵۴-۲۸
تاریخ دریافت: ۱۴۰۴/۰۶/۲۲
تاریخ پذیرش: ۱۴۰۴/۰۸/۲۵

Journal of cognitive research in political studies
Vol.2, No4 (7), 28-54
Reseived Date: 2025/09/13
Accept Date: 2025/11/16

DOI: 10.20241403/CRPS.2509.1075.4.7.2

مسئولیت دولت‌ها در مدیریت جنگ اطلاعاتی در دوران گذار به نظم چندقطبی: چالش‌ها و الزامات

محمد حسن شیخ الاسلامی[۱] | محمد علی صدیقی[۲]

شماره ٤(٧)
سال ۲
فصل زمستان ١٤٠٤

مقاله پژوهشی

تاریخ دریافت:
١٤٠٤/٠٦/٢٢
تاریخ پذیرش:
١٤٠٤/٠٨/٢٥
صص: ٥٤-٢٨

چکیده

در دوران گذار از نظم تک‌قطبی به نظم چندقطبی، جنگ اطلاعاتی به‌عنوان یکی از تهدیدات نوظهور، امنیت ملی و انسجام اجتماعی دولت‌ها را با چالش‌های جدی مواجه کرده است. مسئله اصلی این پژوهش، بررسی مسئولیت دولت‌ها در مدیریت جنگ اطلاعاتی در بستر تحولات ساختاری نظام بین‌الملل است. هدف آن، تبیین الزامات و راهبردهای دولت‌ها برای مقابله مؤثر با جنگ اطلاعاتی در سه سطح ملی، منطقه‌ای و بین‌المللی می‌باشد. سؤال اصلی تحقیق این است که «مسئولیت دولت‌ها در مواجهه با جنگ اطلاعاتی در دوران گذار از نظم تک‌قطبی به چندقطبی چیست و چگونه قابل تحقق است؟» فرضیه پژوهش بر این مبنا استوار است که ضعف نهادهای بین‌المللی، رقابت قدرت‌های بزرگ و تکثر بازیگران غیردولتی اطلاعاتی، موجب کاهش اثربخشی دولت‌ها در مدیریت جنگ اطلاعاتی می‌شود، مگر آن‌که اقدامات مشخصی در حوزه حکمرانی سایبری، همکاری منطقه‌ای و ارتقاء سواد اطلاعاتی شهروندان صورت گیرد. رویکرد توصیفی- تحلیلی است و با بهره‌گیری از چارچوب نظری امنیت سایبری و رئالیسم ساختاری، به تحلیل تطبیقی تجارب اوکراین، ایران و ایالات متحده پرداخته شده است. یافته‌ها نشان می‌دهد که دولت‌هایی که در سه حوزه مذکور سرمایه‌گذاری راهبردی داشته‌اند، توانسته‌اند تا حدی در برابر موج‌های اطلاعاتی خصمانه مقاومت کنند. این پژوهش بر ضرورت تدوین راهبردهای ملی فراگیر و مشارکت‌جویانه برای بازتعریف نقش دولت‌ها در عصر جنگ شناختی تأکید دارد.

کلمات کلیدی: جنگ اطلاعاتی، نظم بین‌المللی، مسئولیت، حکمرانی، اوکراین، ایران، ایالات متحده آمریکا

[۱] دانشیار گروه روابط بین‌الملل، دانشکده وزارت امور خارجه، تهران، ایران. mhsheikh@gmail.com
[۲] دانش آموخته کارشناسی ارشد روابط بین الملل، دانشکده روابط بین الملل وزارت امور خارجه، تهران، ایران. (نویسنده مسئول). mohammadaliseddighy@gmail.com

استناد: شیخ الاسلامی، محمد حسن و صدیقی، محمد علی. (۱۴۰۴). مسئولیت دولت‌ها در مدیریت جنگ اطلاعاتی در دوران گذار به نظم چندقطبی: چالش‌ها و الزامات. شناخت پژوهی مطالعات سیاسی، ۲(۴)، ۵۴-۲۸. doi: 10.20241403/CRPS.2509.1075.4.7.2

Sheikholeslami, M.H. and Seddighi, M. (2025). The Responsibility of States in Managing Information Warfare during the Transition to a Multipolar Order: Challenges and Requirements. Cognitive Research in Political Studies, 2(4), 28-54 doi: 10.20241403/CRPS.2509.1075.4.7.2

مقدمه

نظام بین‌الملل در حال گذار از نظم تک‌قطبی به سوی نظمی چندقطبی است که در آن قدرت نه‌تنها در قالب نظامی و اقتصادی، بلکه در ابعاد فناورانه، شناختی و اطلاعاتی بازتعریف می‌شود. قدرت‌های نوظهور مانند چین و روسیه با بهره‌گیری از فناوری‌های نوین و ظرفیت‌های اطلاعاتی، جایگاه خود را در ساختار جهانی تثبیت می‌کنند. در این چارچوب، جنگ اطلاعاتی به‌عنوان ابزار منازعه پیچیده قرن بیست‌ویکم، مرزهای سنتی امنیت ملی را درنوردیده و به ابزاری در دست دولت‌ها، بازیگران غیردولتی و حتی کاربران شبکه‌های اجتماعی برای رقابت ژئوپلیتیکی و مهندسی افکار عمومی تبدیل شده است (Craig & Valeriano, 2018: 42–46).

در چنین شرایطی، مفهوم امنیت ملی نیز دچار تحول شده است. دیگر نمی‌توان امنیت را صرفاً در قالب حفاظت از مرزهای جغرافیایی یا مقابله با تهدیدات نظامی تعریف کرد؛ بلکه حفاظت از «مرزهای شناختی» و «مرزهای اطلاعاتی» جامعه، به بخشی جدایی‌ناپذیر از امنیت ملی تبدیل شده است (Moleka, 2025: 31-32). حمله به افکار عمومی، تضعیف اعتماد اجتماعی، القای روایت‌های ساختگی و ایجاد چنددستگی در جوامع، بخشی از پیامدهای مستقیم جنگ اطلاعاتی هستند که حتی قدرتمندترین دولت‌ها را آسیب‌پذیر کرده‌اند. این تهدیدات، به‌ویژه در نظم چندقطبی نوظهور، به دلیل ضعف نهادهای بین‌المللی، رقابت فزاینده میان قدرت‌های بزرگ و تکثر منابع اطلاعاتی در دست بازیگران غیردولتی، پیچیده‌تر و فراگیرتر شده‌اند. در نظم چندقطبی نوظهور، برخلاف دوران تک‌قطبی پس از جنگ سرد، چارچوب‌های حقوقی و نهادی مشترک در عرصه‌های امنیتی و فناورانه از میان رفته و فضای سایبری به میدان نبردی بی‌قاعده تبدیل شده است. در این شرایط، دولت‌ها ناچاراند خود به‌تنهایی با تهدیدات اطلاعاتی مقابله کنند و از امنیت شناختی جامعه دفاع نمایند.

این مقاله در پی آن است که با تمرکز بر رابطه میان تغییرات ساختاری در نظم بین‌الملل و ظهور جنگ اطلاعاتی، به بررسی مسئولیت دولت‌ها در مدیریت این پدیده بپردازد. هدف اصلی، شناسایی چالش‌ها و الزامات دولت‌ها برای ایستادگی در برابر جنگ‌های اطلاعاتی و ارائه راهکارهایی در سه سطح ملی، منطقه‌ای و بین‌المللی است. سؤال اصلی پژوهش آن است که دولت‌ها در دوران گذار از نظم تک‌قطبی به چندقطبی چگونه می‌توانند مسئولیت خود را در مواجهه با جنگ اطلاعاتی ایفا کنند؟ فرضیه پژوهش بر این مبنا استوار است که در دوران گذار از نظم تک‌قطبی به چندقطبی، خلأ نهادی در سطح بین‌الملل، رقابت میان قدرت‌های بزرگ و تکثر منابع اطلاعاتی غیردولتی، موجب تضعیف توان دولت‌ها در مدیریت مسئولانه جنگ اطلاعاتی می‌شود، مگر آن‌که دولت‌ها به توسعه

DOR: 20.1001.1.30926459.1404.2.4.2.0

حکمرانی سایبری ملی، تقویت همکاری‌های منطقه‌ای و ارتقاء سواد شناختی شهروندان بپردازند. نوآوری این مقاله در آن است که جنگ اطلاعاتی را نه‌تنها به‌عنوان تهدیدی فناورانه، بلکه به‌عنوان پدیده‌ای ساختاری و برآمده از تحولات ژئوپلیتیکی تحلیل می‌کند. همچنین، این مقاله با بهره‌گیری از چارچوب نظری تلفیقی رئالیسم ساختاری و امنیت سایبری و مطالعه موردی کشورهایی چون ایران، اوکراین و ایالات متحده، به بررسی مسئولیت دولت‌ها در مدیریت جنگ اطلاعاتی می‌پردازد.

۱ـ روش تحقیق

روش‌شناسی این پژوهش بر پایه تلفیق دو رویکرد توصیفی- تحلیلی و تطبیقی استوار است؛ رویکردی که امکان بررسی عمیق و چندلایه مسئولیت دولت‌ها در مواجهه با جنگ اطلاعاتی را در بستر گذار از نظم تک‌قطبی به نظم چندقطبی فراهم می‌سازد. در این چارچوب، هدف اصلی پژوهش نه‌تنها توصیف وضعیت موجود، بلکه تحلیل نحوه کنش‌گری دولت‌ها در برابر تهدیدات شناختی و اطلاعاتی در شرایطی است که نهادهای بین‌المللی از کارآمدی لازم برخوردار نیستند و رقابت قدرت‌ها به فضای دیجیتال نیز تسری یافته است. این رویکرد به‌ویژه در تحلیل پدیده‌هایی که دارای ابعاد چندگانه سیاسی، فناورانه و اجتماعی هستند، کارآمدی بالایی دارد. در کنار آن، روش تطبیقی به‌عنوان مکمل تحلیلی، امکان بررسی تفاوت‌ها و شباهت‌های سیاستی میان کشورها را فراهم می‌سازد؛ به‌ویژه در زمینه حکمرانی اطلاعاتی، نحوه مواجهه با تهدیدات شناختی و ظرفیت‌های دفاعی سایبری.

برای تحقق این هدف، سه کشور ایران، اوکراین و ایالات متحده به‌عنوان موارد مطالعاتی انتخاب شده‌اند. انتخاب این کشورها بر اساس سه معیار اصلی صورت گرفته است: نخست، شدت و گستردگی تجربه جنگ اطلاعاتی در سال‌های اخیر؛ دوم، تفاوت در سطح توسعه زیرساخت‌های سایبری و شناختی؛ و سوم، تنوع در موقعیت ژئوپلیتیکی و نوع حکمرانی. ایران به‌عنوان قدرت منطقه‌ای با تجربه مواجهه با عملیات شناختی پیچیده، اوکراین به‌عنوان یکی از قربانی جنگ اطلاعاتی سازمان‌یافته و ایالات متحده به‌عنوان قدرت جهانی با زیرساخت‌های پیشرفته اما چالش‌های داخلی در حوزه اطلاعات، سه نمونه مناسب برای تحلیل تطبیقی محسوب می‌شوند.

فرآیند تحلیل داده‌ها در این پژوهش به‌صورت مرحله‌ای و نظام‌مند طراحی شده است. در مرحله نخست، ابعاد مختلف جنگ اطلاعاتی در هر کشور شناسایی شده‌اند؛ از جمله مؤلفه‌های سایبری، شناختی، روانی و رسانه‌ای. در مرحله دوم، پاسخ‌های دولت‌ها در سه سطح ملی (حکمرانی داخلی)،

منطقه‌ای (همکاری‌های فراملی) و بین‌المللی (مشارکت در قواعد جهانی) مورد بررسی قرار گرفته‌اند. مرحله سوم به تطبیق یافته‌های تجربی با چارچوب نظری تلفیقی (رئالیسم ساختاری و امنیت سایبری) اختصاص یافته است تا پیوند میان نظریه و واقعیت برقرار شود. در مرحله چهارم، بر اساس تحلیل تطبیقی، الگویی پیشنهادی برای مسئولیت دولت‌ها در عصر جنگ شناختی استخراج شده است.

۲ـ پیشینه پژوهش

مطالعات مختلفی به بررسی ابعاد مختلف جنگ اطلاعاتی پرداخته‌اند. به‌عنوان مثال، در مقاله‌ای به نام جنگ سایبری: استراتژی‌ها، تأثیرات و جهت‌گیری‌های آینده در میدان نبرد دیجیتال[1]، در این حوزه نگارش شده است. در این مقاله نویسندگان به تحلیل استراتژی‌ها، تأثیرات و جهت‌گیری‌های آینده جنگ سایبری پرداخته‌اند. آن‌ها بر لزوم تدوین راهبردهای جامع و همکاری‌های بین‌المللی برای مقابله با تهدیدات سایبری تأکید کرده‌اند (Rahimi & Jones, 2025). در مطالعه‌ای دیگر با عنوان «سیاست‌گذاری امنیت سایبری در دولت‌های نوظهور: چالش‌ها و فرصت‌ها»، نویسندگان به بررسی نحوه مواجهه کشورهای در حال توسعه با تهدیدات اطلاعاتی پرداخته‌اند. آن‌ها با تحلیل موردی کشورهای جنوب شرق آسیا، نشان داده‌اند که ضعف زیرساخت‌های فناورانه، نبود چارچوب‌های حقوقی و فقدان دیپلماسی اطلاعاتی، موجب افزایش آسیب‌پذیری این کشورها در برابر جنگ سایبری شده است. این مقاله بر ضرورت طراحی سیاست‌های چندسطحی و مشارکت منطقه‌ای برای مقابله با تهدیدات شناختی تأکید دارد (Lee & Ahmad, 2024).

در مقاله‌ای با عنوان انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل به این نکته اشاره شد که تحت تأثیر انقلاب ارتباطات و اطلاعات و انقلاب سایبری، جنگ اطلاعاتی از سطح عملیاتی و تاکتیکی به سطح راهبردی گسترش‌یافته و ابعاد سیاسی، اقتصادی، فرهنگی و اجتماعی را دربرگرفته است (Torabi & Taherzadeh, 2020). در مطالعه‌ای دیگر، با عنوان مروری نظام‌مند بر جنگ سایبری و هک‌های حمایت‌شده توسط دولت‌ها[2]، نویسنده با بررسی سیستماتیک مقالات علمی موجود، به تحلیل جنگ سایبری و هک‌های حمایت‌شده دولتی پرداخته‌اند. آن‌ها بر اهمیت درک تهدیدات سایبری و توسعه سیاست‌های مؤثر برای مقابله با آن‌ها تأکید کرده‌اند (Gbormittah, 2022).

[1] Cyber Warfare: Strategies, Impacts, and Future Directions in the Digital Battlefield
[2] A Systematic Literature Review on Cyberwarfare and State-Sponsored Hacking

DOR: 20.1001.1.30926459.1404.2.4.2.0

در مقاله‌ای با عنوان «جنگ شناختی و تحول در مفهوم قدرت در روابط بین‌الملل»، نویسنده بر این نکته تأکید می‌کند که در عصر دیجیتال، قدرت دیگر صرفاً به توان نظامی یا اقتصادی محدود نمی‌شود، بلکه توانایی شکل‌دهی به ادراک عمومی و کنترل روایت‌ها، به یکی از مؤلفه‌های اصلی قدرت ملی تبدیل شده است. این مقاله با بهره‌گیری از نظریه‌های قدرت نرم و امنیت شناختی، نشان می‌دهد که جنگ اطلاعاتی می‌تواند مشروعیت سیاسی و انسجام اجتماعی دولت‌ها را به‌طور مستقیم تحت تأثیر قرار دهد (Delgado, 2023). همچنین، در مقاله‌ای با عنوان تروریسم سایبری به‌عنوان یک تهدید جهانی: بررسی پیامدها و اقدامات مقابله‌ای[1]، نویسندگان به بررسی تهدیدات سایبری تروریستی و پیامدهای آن‌ها بر امنیت ملی پرداخته‌اند. آن‌ها بر لزوم تقویت زیرساخت‌های امنیتی و افزایش آگاهی عمومی برای مقابله با این نوع تهدیدات تأکید کرده‌اند (Iftikhar, 2024).

نتیجه آن‌که با وجود غنای نسبی ادبیات موجود در حوزه جنگ اطلاعاتی، امنیت سایبری و تهدیدات شناختی، اغلب مطالعات پیشین به بررسی ابعاد فناورانه، راهبردی یا پیامدهای امنیتی این پدیده پرداخته‌اند، بدون آن‌که پیوند آن را با تحولات ساختاری در نظم بین‌الملل به‌طور منسجم تحلیل کنند. مقاله حاضر با تلفیق نظریه‌های امنیت سایبری و رئالیسم ساختاری، جنگ اطلاعاتی را نه صرفاً یک تهدید فناورانه، بلکه پدیده‌ای ساختاری و برآمده از رقابت قدرت‌ها در نظم چندقطبی در حال ظهور می‌داند. نوآوری این پژوهش در آن است که مسئولیت دولت‌ها را در سه سطح ملی، منطقه‌ای و بین‌المللی تبیین کرده و از طریق مطالعه تطبیقی تجارب ایران، اوکراین و ایالات متحده، الگویی تحلیلی برای مواجهه با جنگ اطلاعاتی ارائه می‌دهد؛ الگویی که همزمان به الزامات فناورانه، نهادی و ژئوپلیتیکی توجه دارد و خلأ موجود در مطالعات پیشین را پر می‌کند.

۳ـ ادبیات مفهومی

۳ـ۱ـ جنگ اطلاعاتی

جنگ اطلاعاتی اگرچه سابقه‌ای طولانی دارد، اما در عصر حاضر با بهره‌گیری از فناوری‌های نوین، ابعاد و ویژگی‌های تازه‌ای یافته است که موجب تسریع و گسترش چشمگیر انتقال داده‌ها شده‌اند. این نوع جنگ به عنوان مجموعه‌ای از اقدامات هدفمند برای دستیابی به برتری اطلاعاتی نسبت به رقیب تعریف می‌شود. در این چارچوب، کنترل بر فضای اطلاعاتی، حفاظت از داده‌های شخصی، تلاش برای دستیابی و بهره‌برداری از اطلاعات حساس، تخریب زیرساخت‌های اطلاعاتی

[1] Cyberterrorism as a global threat: A review on repercussions and countermeasures

دشمن و ایجاد اختلال در روند تبادل اطلاعات از جمله راهبردهای اصلی به شمار می‌روند. بر همین اساس، جنگ اطلاعاتی می‌تواند به صورت ترکیبی و انتصابی رخ دهد؛ یعنی تلفیقی از ظرفیت‌های فضای سایبری، جنگ الکترونیکی، عملیات اطلاعاتی، روانی و فریب نظامی. هدف نهایی این اقدامات، اثرگذاری بر محیط اطلاعاتی و تغییر نگرش یا رفتار طرف مقابل است (Torabi & Taherzadeh, 2020: 51–53).

جنگ اطلاعاتی یکی از پیچیده‌ترین اشکال منازعه در عصر دیجیتال به شمار می‌رود و شامل مجموعه‌ای از اقدامات هدفمند در فضای اطلاعاتی است. این اقدامات با استفاده از فناوری‌های ارتباطی، رسانه‌های اجتماعی، الگوریتم‌های هوشمند و عملیات روانی، بر ادراک، رفتار و انسجام اجتماعی گروه‌های هدف تأثیر می‌گذارند. برخلاف جنگ‌های سنتی که بر تسلط فیزیکی تمرکز داشتند، جنگ اطلاعاتی بر کنترل شناختی، دستکاری ادراک و تغییر رفتار جمعی متمرکز است. نقش شبکه‌های اجتماعی نیز در تضعیف انسجام ملی، تحریک افکار عمومی و ایجاد شکاف‌های اجتماعی برجسته شده است.

۳ـ۲ـ گذار به نظم چندقطبی

دوران گذار در روابط بین‌الملل به مرحله‌ای اطلاق می‌شود که در آن نظم تثبیت‌شده‌ای بر نظام بین‌المللی حاکم نیست و بازیگران مختلف در تلاش‌اند تا جایگاه، نفوذ و قدرت خود را در ساختار جدید تعریف کنند. این وضعیت پس از فروپاشی اتحاد جماهیر شوروی و پایان جنگ سرد پدید آمد، زمانی که نظم دوقطبی جای خود را به وضعیتی نامتعین داد؛ برخی آن را نظم تک‌قطبی با محوریت ایالات متحده دانستند، برخی دیگر از ظهور نظم چندقطبی سخن گفتند و گروهی آن را دوره‌ای انتقالی تلقی کردند که در آن رقابت برای بازتعریف قدرت و ساخت نظم جدید جریان دارد (Dehshiar, 2021: 154). در این دوره، شاهد افول قدرت‌های سنتی، ظهور بازیگران نوظهور، تغییر در مرزها و افزایش اهمیت قدرت‌های نرم و سخت هستیم. بازیگران بین‌المللی برای ارتقای موقعیت خود، به ایجاد شبکه‌های منطقه‌ای و فراملی، تولید گفتمان‌های جدید و دستیابی به اجماع‌های سیاسی و امنیتی روی آورده‌اند. این تلاش‌ها نشان دهنده نبود یک نظم فراگیر و تثبیت شده و تداوم رقابت برای شکل‌دهی به آینده نظام بین‌الملل است (Tabatabaee & Bahrami, 2018: 80-85).

گذار به نظم چندقطبی به معنای انتقال قدرت جهانی از تمرکز در یک قدرت غالب به توزیع آن میان چند بازیگر بزرگ است. این تغییر با افزایش رقابت ژئوپلیتیکی، تضعیف نهادهای لیبرال

DOR: 20.1001.1.30926459.1404.2.4.2.0

بین‌المللی و ظهور قدرت‌های منطقه‌ای همراه شده و پیامدهای گسترده‌ای برای امنیت، دیپلماسی و حکمرانی جهانی دارد (Buzan & Lawson, 2015). از دیدگاه رئالیسم ساختاری، نظم بین‌الملل تحت تأثیر توزیع قدرت میان دولت‌ها شکل می‌گیرد و هرگونه تغییر، قواعد رفتاری را بازتعریف کرده و بی‌ثباتی را افزایش می‌دهد (Waltz, 1979). در چنین شرایطی، دولت‌ها با تهدیداتی فراتر از منازعات سنتی مواجه هستند؛ تهدیداتی که توسط شرکت‌های فناوری، شبکه‌های اطلاعاتی و حتی شهروندان فعال در فضای مجازی ایجاد می‌شوند. منابع داخلی نیز بر تضعیف هژمونی آمریکا، افزایش نقش قدرت‌های منطقه‌ای در غرب آسیا و ظهور الگوهای نوین کنشگری تأکید دارند (Sharifi & Fallahi, 2022). این گذار نه تنها ساختار تعاملات بین‌المللی را تغییر داده، بلکه زمینه‌ساز افزایش تهدیدات فراملی، از جمله جنگ اطلاعاتی، شده است.

۳ـ۳ـ مسئولیت دولت‌ها

در شرایط گذار به نظم چندقطبی و افزایش جنگ اطلاعاتی، مسئولیت دولت‌ها در حفظ امنیت ملی، انسجام اجتماعی و سلامت روانی جامعه پیچیده‌تر شده است. دولت‌ها دیگر نمی‌توانند تنها به روش‌های سنتی امنیتی متکی باشند و باید در سه سطح راهبردی عمل کنند. نخست، توسعه حکمرانی سایبری ملی از طریق تدوین قوانین جامع، ایجاد نهادهای پاسخ‌گو و تقویت زیرساخت‌های دفاعی اطلاعاتی ضروری است. دوم، تقویت همکاری‌های منطقه‌ای و بین‌المللی برای تبادل اطلاعات، مقابله با تهدیدات مشترک و ایجاد سازوکارهای اعتمادسازی اهمیت دارد. سوم، ارتقاء سواد اطلاعاتی شهروندان برای کاهش آسیب‌پذیری شناختی، افزایش تاب‌آوری اجتماعی و تقویت توان تحلیل انتقادی در برابر اطلاعات جعلی، از الزامات اساسی مقابله با جنگ اطلاعاتی به شمار می‌رود (Nye, 2010). همچنین، بازتعریف نقش دولت‌ها در حکمرانی فضای مجازی و تنظیم‌گری اطلاعاتی و توجه به «امنیت شناختی» به عنوان ابزاری غیرنظامی برای مقابله با تهدیدات اطلاعاتی، اهمیت آموزش عمومی و تقویت سواد رسانه‌ای را برجسته می‌سازد (Sharifi & Fallahi, 2022: 41–45).

۴ـ چارچوب نظری

۴ـ۱ـ رئالیسم ساختاری و امنیت سایبری- شناختی

رئالیسم ساختاری یا نئورئالیسم، یکی از نظریه‌های بنیادین در حوزه روابط بین‌الملل است که توسط کنت والتز در دهه ۱۹۷۰ بنیان نهاده شد. این نظریه بر آن است که نظام بین‌الملل ذاتاً آنارشیک

است؛ به این معنا که فاقد مرجع اقتدار مرکزی برای تنظیم رفتار دولت‌هاست. در چنین نظمی، دولت‌ها به‌عنوان بازیگران اصلی و مستقل، ناگزیر از خودیاری برای حفظ امنیت و بقاء هستند. این وضعیت آنارشیک، بی‌اعتمادی متقابل میان دولت‌ها را افزایش می‌دهد و آن‌ها را به سوی رقابت برای انباشت قدرت سوق می‌دهد (Waltz, 1979).

در چارچوب رئالیسم ساختاری، ساختار نظام بین‌الملل بر اساس توزیع قدرت میان واحدهای تشکیل دهنده آن تعریف می‌شود. هرگونه تغییر در این توزیع، موجب بازتعریف قواعد رفتاری، افزایش بی‌ثباتی و تشدید رقابت میان دولت‌ها می‌شود. از منظر این نظریه، دولت‌ها عقلانی عمل می‌کنند و بر اساس تحلیل هزینه- فایده، گزینه‌هایی را انتخاب می‌کنند که بیشترین منافع امنیتی و راهبردی را برای آن‌ها به همراه داشته باشد (Dehghani Firouzabadi, 2016: 232–234).

در زمینه جنگ اطلاعاتی، رئالیسم ساختاری توضیح می‌دهد که چرا دولت‌ها در فضای سایبری نیز همانند حوزه‌های نظامی و اقتصادی، به دنبال توسعه ابزارهای بازدارنده، افزایش ظرفیت‌های کنترلی و انباشت قدرت اطلاعاتی هستند. فضای سایبری، به‌ویژه در نظم چندقطبی نوظهور، به میدان نبردی بی‌قاعده تبدیل شده است که در آن، دولت‌ها برای حفظ موقعیت خود، ناگزیر از رقابت در حوزه اطلاعاتی هستند. جنگ اطلاعاتی، از این منظر، نه یک پدیده حاشیه‌ای، بلکه بخشی از رقابت قدرت‌ها برای بقاء و تثبیت جایگاه در ساختار جهانی است (Mearsheimer, 2001).

رئالیسم ساختاری همچنین بر این نکته تأکید دارد که در غیاب نهادهای بین‌المللی مؤثر، دولت‌ها نمی‌توانند به قواعد الزام‌آور جهانی تکیه کنند و باید خود به طراحی راهبردهای دفاعی و تهاجمی در فضای اطلاعاتی بپردازند. این منطق، به‌ویژه در شرایط گذار به نظم چندقطبی، اهمیت بیشتری می‌یابد؛ زیرا در چنین نظمی، قواعد رفتاری تثبیت شده وجود ندارد و رقابت میان قدرت‌ها به حوزه‌های نوین مانند اطلاعات، روایت‌سازی و عملیات شناختی نیز کشیده شده است.

در کنار رئالیسم ساختاری، نظریه‌های امنیت سایبری و شناختی نیز نقش مهمی در تحلیل مسئولیت دولت‌ها در مواجهه با جنگ اطلاعاتی ایفا می‌کنند. این نظریه‌ها، که عمدتاً در دو دهه اخیر توسعه یافته‌اند، بر تحول ماهیت تهدیدات امنیتی در عصر دیجیتال تأکید دارند. در این چارچوب، تهدیدات امنیتی دیگر صرفاً در قالب حملات نظامی یا تروریستی ظاهر نمی‌شوند، بلکه در قالب حملات سایبری، عملیات روانی، انتشار اطلاعات جعلی و دستکاری ادراک عمومی نیز بروز می‌یابند (Nye, 2010). امنیت سایبری به حفاظت از زیرساخت‌های دیجیتال، داده‌های حساس، و جریان اطلاعات در فضای مجازی می‌پردازد. اما امنیت شناختی، که به‌عنوان زیرمجموعه‌ای از

DOR: 20.1001.1.30926459.1404.2.4.2.0

امنیت سایبری شناخته می‌شود، تمرکز خود را بر حفاظت از فرآیندهای ادراکی، باورها و رفتارهای جمعی شهروندان قرار می‌دهد. در این رویکرد، جنگ اطلاعاتی نوعی نبرد شناختی است که هدف آن، تضعیف انسجام اجتماعی، ایجاد شکاف‌های سیاسی- فرهنگی و تغییر نگرش یا رفتار جمعی از طریق روایت‌سازی، القای شبه‌اطلاعات و تحریک روانی است (Craig & Valeriano, 2018: 42–46).

نظریه‌پردازان امنیت شناختی بر این باورند که دولت‌ها باید علاوه بر حفاظت فنی از زیرساخت‌ها، به ارتقاء سواد رسانه‌ای، آموزش تفکر انتقادی و ایجاد سازوکارهای اعتبارسنجی اطلاعات نیز توجه کنند. رویکردهای سیستمی در امنیت سایبری نیز تأکید دارند که تعامل میان حمله و دفاع و همچنین میان بازیگران دولتی و غیردولتی، باید در قالب یک سیستم پیچیده تحلیل شود؛ سیستمی که تغییرات آن می‌تواند پیامدهای گسترده‌ای بر ثبات یا بی‌ثباتی امنیت ملی داشته باشد (Xu, 2020: 119–123). در این چارچوب، دولت‌ها باید راهبردهای چندلایه‌ای برای مقابله با تهدیدات شناختی طراحی کنند؛ راهبردهایی که شامل حکمرانی سایبری، تنظیم‌گری اطلاعاتی، ارتقاء تاب‌آوری شناختی و همکاری با نهادهای مدنی و علمی باشد. این نظریه‌ها، به‌ویژه در شرایطی که جنگ اطلاعاتی به ابزار اصلی رقابت قدرت‌ها تبدیل شده است، اهمیت بیشتری یافته‌اند و می‌توانند مبنای طراحی سیاست‌های ملی و منطقه‌ای قرار گیرند.

۴ـ۲ـ تلفیق نظری: مسئولیت دولت‌ها در دو سطح داخلی و ساختاری

تلفیق رئالیسم ساختاری و امنیت سایبری، امکان تحلیل جامع‌تر و چندسطحی‌تری از مسئولیت دولت‌ها در مواجهه با جنگ اطلاعاتی فراهم می‌سازد. این تلفیق نظری، بر آن است که دولت‌ها باید هم به الزامات داخلی توجه کنند و هم به الزامات ساختاری در سطح بین‌الملل پاسخ دهند. در سطح داخلی، دولت‌ها باید ظرفیت‌های فناورانه، نهادی و اجتماعی خود را برای مقابله با تهدیدات شناختی تقویت کنند. این شامل ایجاد نهادهای تخصصی در حوزه اطلاعات، تدوین قوانین جامع برای تنظیم‌گری فضای مجازی، ارتقاء سواد شناختی شهروندان و توسعه زیرساخت‌های دفاعی سایبری است. این اقدامات، به دولت‌ها امکان می‌دهد تا در برابر عملیات روانی، اطلاعات جعلی و روایت‌های ساختگی، مقاومت مؤثرتری نشان دهند. در سطح ساختاری، دولت‌ها باید در غیاب نهادهای بین‌المللی مؤثر، از طریق خودیاری اطلاعاتی، دیپلماسی سایبری و مشارکت در تدوین قواعد جهانی، جایگاه خود را در نظم نوظهور تثبیت کنند. این شامل همکاری با نهادهای منطقه‌ای، مشارکت در مجامع بین‌المللی و تلاش برای ایجاد اجماع جهانی در برابر تهدیدات فراملی مانند تروریسم سایبری و هک‌های دولتی است.

این تلفیق نظری روشن می‌سازد که جنگ اطلاعاتی نه‌تنها تهدیدی فناورانه، بلکه پدیده‌ای ساختاری و ژئوپلیتیکی است که در بستر رقابت قدرت‌ها معنا می‌یابد. هرگونه ضعف یا عقب‌ماندگی در حوزه سایبری، می‌تواند به تضعیف جایگاه یک دولت در نظم جهانی و افزایش آسیب‌پذیری آن در برابر رقبای بین‌المللی منجر شود. بنابراین، مسئولیت دولت‌ها در عصر جنگ شناختی، ترکیبی از الزامات داخلی و ساختاری است که باید در قالب راهبردی چندسطحی بازتعریف شود. بر این اساس، چارچوب نظری پژوهش حاضر تأکید دارد که دولت‌ها برای ایفای مسئولیت خود در مدیریت جنگ اطلاعاتی، باید از یک‌سو به الزامات فناورانه و اطلاعاتی توجه کنند و از سوی دیگر، آن را به‌عنوان بخشی از راهبرد بقاء و رقابت قدرت‌ها در نظم چندقطبی در حال ظهور در نظر بگیرند. این تلفیق میان نظریه امنیت سایبری و رئالیسم ساختاری، امکان تحلیل واقع‌بینانه‌تری از مسئولیت‌های دولت‌ها در عصر جنگ شناختی و اطلاعاتی فراهم می‌سازد و می‌تواند مبنای طراحی سیاست‌های ملی، منطقه‌ای و بین‌المللی قرار گیرد.

۵ـ یافته‌های پژوهش

در دهه‌های اخیر، نظام بین‌الملل شاهد تحولات ساختاری مهمی بوده است؛ تحولی که از نظم تک‌قطبی به سوی نظم چندقطبی نوظهور میل کرده است. پس از فروپاشی اتحاد جماهیر شوروی، ایالات متحده با برخورداری از توانایی‌های نظامی، اقتصادی و فناورانه برتر، در جایگاهی بی‌سابقه قرار گرفت و نظم تک‌قطبی شکل گرفت (Ikenberry et al., 2009: 20– 27). با این حال، رشد اقتصادی و سیاسی بازیگران نوظهوری مانند چین، روسیه، هند و اتحادیه اروپا، دلالت‌گر افول مطلق هژمونی آمریکاست و زمینه‌ساز تولد نظم چندقطبی در قرن بیست‌ویکم شده است (Muzaffar et al., 2017: 49– 61).

نظم چندقطبی، با ویژگی‌هایی همچون پیچیدگی بیشتر در نظام‌های اتحاد و ائتلاف، ابهام در نیت دول بزرگ و دشواری در حفظ ثبات ساختاری همراه است. نظریه‌پردازان نئورئالیست در این باره هشدار داده‌اند که ظرفیت رخدادهای خطرناک و واگذار کردن مسئولیت در نظم چندقطبی بیشتر است؛ به این معنا که ممکن است یک کشور یا ائتلاف وارد درگیری خطرناکی شود که ساختار ائتلاف اجازه موازنه مؤثر را نمی‌دهد (Polarity, 2025).

در این بستر سیاسی متلاطم، ماهیت جنگ اطلاعاتی دچار تغییر بنیادی شده است. در نظم تک‌قطبی، چارچوب‌های نهادی بین‌المللی از قبیل ناتو، سازمان ملل یا نظام مالی جهانی، می‌توانستند

DOR: 20.1001.1.30926459.1404.2.4.2.0

برای ایجاد ضوابط فراملی و تنظیم فضای اطلاعاتی تا حدی مؤثر باشند. اما با ظهور ساختار چندقطبی، این چارچوب‌ها کارآمدی خود را از دست داده‌اند و خلأ نهادی ایجاد شده، فضای مناسبی برای تهدیدات جنگ اطلاعاتی فراهم کرده است (World Economic Forum, 2024). یکی از نمونه‌های بارز این تحول، پژوهش بازاولوک و کووالف است که ابعاد فنی و معرفتی جنگ اطلاعاتی در سیستم چندقطبی را تحلیل می‌کند. تحلیل این دو پژوهشگر نشان می‌دهد که بازیگران قدرتمند مانند ایالات متحده بدون استفاده مستقیم از نیروی نظامی، با اتکا به ابزارهای نرم همچون نفوذ شناختی، جنگ روانی و رسانه‌ای، در حال شکل‌دهی نظم ارزشی به نفع خود هستند (Bazavluk & Kovalev, 2025: 236–250).

چنین فضای سیاسی و فناورانه‌ای، دولت‌ها را به مواجهه با چالشی جدید سوق داده است: نبود ساختار نهادی جهانی مقتدر و رقابت پیچیده نیروهای متعدد، مدیریت جنگ اطلاعاتی را به مأموریتی دشوار و چندبخشی تبدیل کرده است. این وضعیت، دولت‌ها را وادار می‌سازد تا در سطح ملی به‌سرعت ظرفیت‌های سایبری، حکمرانی اطلاعاتی و سواد رسانه‌ای جامعه را تقویت کنند؛ در سطح منطقه‌ای به همکاری برای ایجاد امنیت اطلاعاتی و تبادل داده‌های راهبردی بپردازند؛ و در سطح بین‌المللی به ساخت نهادهای جدید یا بازتعریف چارچوب‌های نهادی موجود برای مقابله با جنگ اطلاعاتی اقدام کنند. در نتیجه، آشفتگی ساختاری ناشی از گذار از نظم تک‌قطبی به چندقطبی، نه‌تنها بر شدت رقابت میان قدرت‌ها افزوده، بلکه میدان جنگ اطلاعاتی را گسترده‌تر و مرزهای آن را مبهم‌تر کرده است.

۵ـ۱ـ جنگ اطلاعاتی و مسئولیت دولت‌ها (ایران، اوکراین و ایالات متحده)

۱ـ ایران

تجربه جنگ اطلاعاتی ترکیبی و مهندسی ادراک جمهوری اسلامی ایران طی دو دهه اخیر، به‌ویژه پس از تحولات منطقه‌ای و تشدید رقابت‌های ژئوپلیتیکی، نشانگر هدف اصلی جنگ ترکیبی بوده است؛ جنگی که بخش اطلاعاتی آن نقشی محوری و تعیین‌کننده دارد. این جنگ شامل مجموعه‌ای از عملیات روانی، رسانه‌ای، سایبری و فریب نظامی است که با هدف تضعیف مشروعیت سیاسی، ایجاد شکاف میان دولت- ملت و کاهش انسجام اجتماعی طراحی شده‌اند (Rezapur & Majidi, 2021: 74). در چارچوب نظم جهانی در حال گذار به چندقطبی، ایران با جنگ اطلاعاتی چندلایه‌ای مواجه شده که علاوه بر عملیات رسانه‌ای، شامل تحریم‌های اقتصادی، تهدیدات نظامی، و فشارهای دیپلماتیک نیز می‌شود. در حوزه رسانه و روانی، شبکه‌های ماهواره‌ای، کمپین‌های فضای

مجازی و اتاق‌های فکر غربی برای تولید روایت‌های ضعیف‌کننده علیه ایران به‌کار گرفته شده‌اند. این روایت‌ها تلاش کرده‌اند تا ناکارآمدی ساختاری، بحران‌های داخلی و شکاف‌های فرهنگی را برجسته کرده و اعتماد عمومی به نهادهای رسمی را تضعیف کنند. در پاسخ، ایران راهبرد دفاعی- اطلاعاتی خود را با ایجاد زیرساخت‌های سایبری بومی، تقویت جنگ الکترونیک، توسعه روایت‌های ملی و مذهبی و سامانه‌های رصد اطلاعاتی پیش برده است (Kangavari, 2022: 95–97). جنگ اطلاعاتی در ایران عمدتاً به شکل جنگ روایت‌ها مشاهده می‌شود؛ جایی که روایت‌های متضاد درباره هویت ملی، سیاست خارجی و مشروعیت سیاسی در فضای رسانه‌ای و مجازی رقابت می‌کنند. شبکه‌هایی مانند پرس‌تی‌وی و الکوثر، پیام‌های ضدغرب و ضدآمریکایی را جهانی‌سازی کرده‌اند و تلاش کرده‌اند تا تصویر جایگزینی از ایران در برابر روایت‌های غالب غربی ارائه دهند (Therme, 2023). با این حال، محدودیت دسترسی رسانه‌ای، پایین بودن سواد رسانه‌ای و قطبی‌سازی سیاسی، آسیب‌پذیری فضای داخلی ایران را افزایش داده‌اند؛ به‌ویژه در دوره‌هایی مانند جنگ اوکراین که روایت‌های متناقض در فضای مجازی گسترش یافته‌اند.

مدل مقاومت ادراکی ایران، ترکیبی از تاب‌آوری روانی، ظرفیت‌های رسانه‌ای و نمادهای فرهنگی- دینی است که توانسته آثار عملیات دشمن را کاهش دهد. دیپلماسی عمومی هوشمندانه نیز با طراحی پیام‌های متناسب فرهنگی و اجتماعی، استفاده از ابزارهای دیجیتال و شبکه‌های اجتماعی و ایجاد گفت‌وگوی چندجانبه، به چالش کشیدن روایت‌های تحریف‌شده و ارائه تصویر واقع‌گرایانه ایران کمک کرده است (Rahbar, 2025). در مجموع، جنگ اطلاعاتی علیه ایران با پیوند به جنگ شناختی، از عملیات رسانه‌ای سنتی فراتر رفته و به مهندسی ادراک ارتقاء یافته است. ایران برای مقابله، نیازمند راهبرد چندلایه شامل تقویت تاب‌آوری ادراکی، سواد رسانه‌ای و فعال‌سازی دیپلماسی عمومی و گفتمان‌سازی بین‌المللی است؛ زیرا بقاء و امنیت ملی بیش از ابزارهای سخت‌افزاری، به مدیریت فضای معنایی و ادراکی گره خورده است (Kangavari, 2022).

الف. حکمرانی سایبری و تنظیم‌گری داخلی

در سطح ملی، جمهوری اسلامی ایران تلاش کرده است تا با توسعه زیرساخت‌های حکمرانی سایبری، ظرفیت‌های دفاعی خود را در برابر تهدیدات اطلاعاتی ارتقاء دهد. ایجاد مرکز ملی فضای مجازی، شورای عالی فضای مجازی و تدوین سند راهبردی امنیت فضای تولید و تبادل اطلاعات از جمله اقدامات کلیدی در این حوزه بوده‌اند. این نهادها وظیفه تنظیم‌گری، پایش تهدیدات و پاسخ

DOR: 20.1001.1.30926459.1404.2.4.2.0

به حملات سایبری را بر عهده دارند و تلاش کرده‌اند تا با ایجاد سامانه‌های بومی، وابستگی به زیرساخت‌های خارجی را کاهش دهند (Rezaei & Kazemi, 2019: 44– 47).

با این حال، حکمرانی سایبری در ایران با چالش‌هایی مواجه است. نخست، فقدان شفافیت در سیاست‌گذاری موجب شده است که اعتماد عمومی به نهادهای تنظیم‌گر کاهش یابد. دوم، تمرکز بیش از حد بر کنترل محتوا به‌جای ارتقاء امنیت زیرساختی، موجب شده است که حکمرانی سایبری بیشتر جنبه انفعالی و واکنشی داشته باشد تا راهبردی و پیش‌دستانه. سوم، ضعف در هماهنگی میان نهادهای مسئول، از جمله وزارت ارتباطات، مرکز افتا[1] و نهادهای امنیتی، موجب شده است که پاسخ به تهدیدات اطلاعاتی با تأخیر و پراکندگی همراه باشد. همچنین، نبود چارچوب حقوقی جامع برای حفاظت از داده‌های شخصی و مقابله با عملیات شناختی، خلأی جدی در حکمرانی سایبری ایران ایجاد کرده است.

ب. چالش‌های دیپلماسی اطلاعاتی منطقه‌ای

در سطح منطقه‌ای، ایران فاقد سازوکارهای مؤثر برای دیپلماسی اطلاعاتی است. برخلاف کشورهایی مانند اوکراین که با ناتو و اتحادیه اروپا در زمینه تبادل اطلاعات، طراحی کمپین‌های مشترک و اعتبارسنجی روایت‌ها همکاری می‌کنند، ایران به دلیل محدودیت‌های ژئوپلیتیکی، تحریم‌های بین‌المللی و بی‌اعتمادی ساختاری، از چنین ظرفیت‌هایی محروم است. تلاش‌هایی مانند همکاری با کشورهای عضو سازمان همکاری شانگهای یا پیمان امنیتی منطقه‌ای، هنوز به سطح عملیاتی در حوزه اطلاعات نرسیده‌اند و بیشتر در سطح بیانیه‌های سیاسی باقی مانده‌اند. این خلأ موجب شده است که ایران در برابر تهدیدات فراملی، از جمله عملیات شناختی سازمان‌یافته از سوی قدرت‌های رقیب، به‌صورت منفرد عمل کند. نبود سازوکارهای اعتمادسازی، تبادل داده و هماهنگی منطقه‌ای، آسیب‌پذیری ایران را در برابر جنگ اطلاعاتی افزایش داده است و موجب شده است که روایت‌های خصمانه در فضای منطقه‌ای و جهانی، بدون پاسخ مؤثر باقی بمانند (Sharifi & Fallahi, 2022: 41–45).

ج. ارتقاء سواد شناختی و محدودیت‌های اعتماد عمومی

در سطح اجتماعی، ایران تلاش‌هایی برای ارتقاء سواد رسانه‌ای و شناختی شهروندان انجام داده است. برنامه‌هایی مانند آموزش سواد رسانه‌ای در مدارس، تولید محتوای آموزشی در رسانه ملی، راه‌اندازی پلتفرم‌های بومی و طراحی کمپین‌های عمومی برای مقابله با اطلاعات جعلی، بخشی از

[1] امنیت فضای تولید و تبادل اطلاعات

این اقدامات هستند (Yousefi, 2023: 61– 64). هدف این برنامه‌ها، افزایش تاب‌آوری شناختی جامعه در برابر روایت‌های ساختگی، عملیات روانی و شبه‌اطلاعات است.

با این حال، این تلاش‌ها با محدودیت‌هایی مواجه‌اند. نخست، فقدان اعتماد عمومی به منابع رسمی موجب شده است که روایت‌های دولتی کمتر مورد پذیرش قرار گیرند و شهروندان به منابع غیررسمی یا خارجی روی آورند. دوم، قطبی‌سازی سیاسی- اجتماعی، زمینه‌ساز گسترش روایت‌های متضاد و تضعیف انسجام شناختی شده است. سوم، نبود نهادهای مستقل برای اعتبارسنجی اطلاعات، موجب شده است که شهروندان در مواجهه با اطلاعات متناقض، دچار سردرگمی و بی‌اعتمادی شوند. در مجموع، ایران در سطح ملی گام‌هایی برای حکمرانی سایبری و ارتقاء سواد شناختی برداشته است، اما در سطح منطقه‌ای و اجتماعی، با چالش‌های جدی مواجه است که اثربخشی اقدامات دولت را در برابر جنگ اطلاعاتی محدود می‌سازد. تجربه ایران نشان می‌دهد که مقابله با جنگ شناختی، نیازمند راهبردی چندلایه، چندبازیگری و چندسطحی است که در آن، دولت، جامعه مدنی، رسانه‌ها و نهادهای علمی به‌صورت هماهنگ عمل کنند. تنها در چنین چارچوبی است که می‌توان تاب‌آوری شناختی را افزایش داد و امنیت ملی را در برابر تهدیدات اطلاعاتی حفظ کرد.

۲ـ اوکراین

تجربه اوکراین نشان می‌دهد که مقابله با جنگ اطلاعاتی نیازمند راهبردی چندسطحی، چندبازیگری و چندرسانه‌ای است؛ راهبردی که در آن، دولت، جامعه مدنی، رسانه‌ها و فناوری، به‌صورت هماهنگ و هدفمند عمل کنند. این تجربه همچنین تأکید می‌کند که جنگ اطلاعاتی، نه‌تنها تهدیدی امنیتی، بلکه چالشی برای مشروعیت، انسجام و بقاء دولت‌ها در نظم نوظهور جهانی است.

الف. تجربه جنگ شناختی با روسیه

اوکراین از سال ۲۰۱۴، به‌ویژه پس از بحران شبه‌جزیره کریمه، به یکی از برجسته‌ترین نمونه‌های جنگ اطلاعاتی سازمان‌یافته در جهان تبدیل شده است. در این دوره، فدراسیون روسیه با بهره‌گیری از مجموعه‌ای پیچیده از ابزارهای اطلاعاتی، رسانه‌ای، سایبری و روانی، تلاش کرد تا مشروعیت دولت اوکراین را تضعیف، انسجام اجتماعی آن را مختل و افکار عمومی را در جهت منافع خود شکل دهد. این عملیات نه‌تنها در فضای مجازی، بلکه از طریق رسانه‌های روس‌زبان، شبکه‌های اجتماعی، پلتفرم‌های پیام‌رسان و حتی نهادهای مذهبی و فرهنگی انجام شد (Gbormittah, 2022).

DOR: 20.1001.1.30926459.1404.2.4.2.0

الحاق کریمه نمونه‌ای بارز از بهره‌گیری روسیه از قدرت نرم در قالب جنگ هیبریدی بود؛ جایی که بدون درگیری نظامی گسترده، با استفاده از روایت‌سازی، تحریک قومیت‌ها و بهره‌برداری از شکاف‌های اجتماعی، کنترل منطقه‌ای را به‌دست گرفت. بحران یورومیدان ۲۰۱۴ نیز تحت تأثیر شدید روایت‌های رسانه‌ای روسیه قرار داشت و نشان داد که جنگ اطلاعاتی می‌تواند به‌طور مستقیم بر تحولات سیاسی داخلی اثرگذار باشد (Rezapur & Majidi, 2021: 97–99). در جریان جنگ ۲۰۲۲ نیز، حملات اطلاعاتی روسیه به اوج خود رسید. این حملات شامل انتشار اطلاعات جعلی درباره اهداف نظامی، تحریک قومیت‌ها، ایجاد بی‌اعتمادی نسبت به دولت مرکزی و تلاش برای تضعیف انسجام ملی بود. شبکه‌های هماهنگ حساب‌های کاربری، بات‌ها و کمپین‌های رسانه‌ای، با هدف برجسته‌سازی ناکارآمدی دولت و القای شکست سیاسی- نظامی، به‌کار گرفته شدند (Prysiazhniuk et al., 2025). این تجربه، اوکراین را به یکی از پیشگامان مقابله با جنگ شناختی در سطح ملی و بین‌المللی تبدیل کرده است.

ب. پاسخ چندلایه و همکاری‌های منطقه‌ای

پاسخ اوکراین به جنگ اطلاعاتی روسیه، چندلایه و ترکیبی بوده است. در سطح نهادی، دولت اوکراین نهادهای تخصصی برای مقابله با اطلاعات نادرست، پایش تهدیدات سایبری و هماهنگی میان دستگاه‌های امنیتی و رسانه‌ای ایجاد کرده است. همچنین، کارزارهای ملی برای ارتقاء سواد رسانه‌ای، آموزش عمومی و تقویت رسانه‌های بومی راه‌اندازی شده‌اند (Gouliev, 2025). در سطح منطقه‌ای، اوکراین برخلاف ایران، توانسته است با نهادهای فرامنطقه‌ای مانند ناتو و اتحادیه اروپا همکاری مؤثری در حوزه اطلاعاتی برقرار کند. همکاری با مرکز ارتباطات راهبردی ناتو[1]، مشارکت در برنامه‌های امنیت سایبری اتحادیه اروپا و تبادل داده‌های تهدید، موجب ارتقاء ظرفیت‌های دفاعی اوکراین در برابر تهدیدات شناختی شده است (Muzaffar et al., 2025).

این همکاری‌ها شامل آموزش نیروهای سایبری، طراحی کمپین‌های مقابله با اطلاعات جعلی و ایجاد سازوکارهای اعتبارسنجی اطلاعات بوده‌اند. همچنین، اوکراین توانسته است با استفاده از دیپلماسی اطلاعاتی، حمایت سیاسی و رسانه‌ای گسترده‌ای از سوی کشورهای غربی جلب کند؛ حمایتی که در مقابله با روایت‌های روسی نقش کلیدی داشته است. این دیپلماسی، نه‌تنها در سطح دولتی، بلکه از طریق شبکه‌های مدنی، رسانه‌های مستقل و پلتفرم‌های بین‌المللی دنبال شده است.

[1] NATO StratCom

ج. تاب‌آوری شناختی و جنگ روایت‌ها

در سطح اجتماعی، دولت اوکراین با همکاری نهادهای مدنی، رسانه‌های مستقل و شرکت‌های فناوری و علمی، کمپین‌های گسترده‌ای برای ارتقاء سواد شناختی شهروندان خود راه‌اندازی کرده است. این کمپین‌ها شامل آموزش عمومی درباره شناسایی اطلاعات جعلی، تقویت رسانه‌های بومی، ایجاد پلتفرم‌های اعتبارسنجی محتوا و توسعه الگوریتم‌های تشخیص روایت‌های جعلی و ساختگی بوده‌اند (Torabi & Taherzadeh, 2020). همچنین، استفاده از فناوری‌های نوین مانند هوش مصنوعی، یادگیری ماشین و تحلیل شبکه‌های اجتماعی، بخشی از راهبرد اوکراین در مقابله با جنگ اطلاعاتی بوده است. همکاری با شرکت‌های فناوری غربی برای حذف محتوای مخرب، محدودسازی دسترسی بات‌ها و حساب‌های جعلی و تقویت روایت‌های ملی، موجب افزایش تاب‌آوری شناختی جامعه و کاهش آسیب‌پذیری در برابر عملیات روانی شده‌اند.

در بُعد فرهنگی و نمادین، اوکراین از ابزارهایی مانند میم‌ها، تصاویر و ویدئوهای کوتاه برای پیشبرد روایت مقاومت استفاده کرده است. این روایت‌ها، که در برابر روایت‌های روسی طراحی شده‌اند، موجب جلب حمایت جهانی، تقویت همبستگی داخلی و افزایش مشروعیت دولت مرکزی شده‌اند (Mejova et al., 2023). این تجربه نشان می‌دهد که جنگ اطلاعاتی، نه‌تنها در سطح فنی، بلکه در سطح فرهنگی و روانی نیز باید مدیریت شود. در مجموع، بحران اوکراین نشان دهنده بهره‌گیری روسیه از ترکیبی پیچیده از قدرت سخت، نیمه‌سخت و نرم در قالب جنگ هیبریدی است؛ جنگی که با استفاده از ابزارهای اطلاعاتی، رسانه‌ای، دیپلماتیک و سایبری، به‌دنبال بی‌ثبات‌سازی دولت هدف و تغییر رفتار جمعی جامعه بوده است. پاسخ اوکراین، با بهره‌گیری از حکمرانی سایبری فعال، دیپلماسی اطلاعاتی منطقه‌ای و ارتقاء سواد شناختی، توانسته است الگویی نسبی از مقاومت در برابر جنگ اطلاعاتی ارائه دهد؛ الگویی که می‌تواند برای سایر کشورها، به‌ویژه قدرت‌های منطقه‌ای، قابل اقتباس باشد.

۳ـ ایالات متحده

الف. نهادسازی امنیت سایبری و راهبردهای ملی

ایالات متحده به‌عنوان یکی از پیشرفته‌ترین کشورها در حوزه فناوری اطلاعات و ارتباطات، از دهه ۲۰۰۰ به‌طور جدی به توسعه زیرساخت‌های امنیت سایبری و اطلاعاتی پرداخته است. این کشور با درک ماهیت نوظهور تهدیدات شناختی و اطلاعاتی، مجموعه‌ای از نهادهای تخصصی را برای مقابله با این تهدیدات ایجاد کرده است. از جمله مهم‌ترین این نهادها می‌توان به آژانس امنیت

DOR: 20.1001.1.30926459.1404.2.4.2.0

سایبری و زیرساخت‌ها (CISA)، فرماندهی سایبری ایالات متحده[1] و دفتر دیپلماسی سایبری در وزارت امور خارجه اشاره کرد. این نهادها وظیفه پایش تهدیدات، طراحی راهبردهای ملی و هماهنگی میان دستگاه‌های امنیتی و فناورانه را بر عهده دارند (Craig & Valeriano, 2018).

راهبرد ملی امنیت سایبری ایالات متحده، بر اساس اسناد منتشرشده در سال‌های اخیر، شامل چهار محور اصلی است: ۱ـ دفاع از زیرساخت‌های حیاتی؛ ۲ـ مقابله با عملیات اطلاعاتی خارجی؛ ۳ـ ارتقاء تاب‌آوری شناختی جامعه؛ و ۴ـ توسعه همکاری‌های بین‌المللی. این راهبردها با بودجه‌های کلان، همکاری با شرکت‌های فناوری بزرگ مانند گوگل، مایکروسافت و متا و استفاده از ظرفیت‌های اطلاعاتی نهادهای امنیتی همراه بوده‌اند. همچنین، ایالات متحده تلاش کرده است تا با استفاده از فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین، سامانه‌های پیش‌بینی تهدیدات اطلاعاتی را توسعه دهد و توان پاسخ‌دهی سریع خود را در برابر حملات شناختی افزایش دهد.

ب. دیپلماسی اطلاعاتی جهانی

در سطح بین‌المللی، ایالات متحده یکی از پیشگامان دیپلماسی اطلاعاتی محسوب می‌شود. راه‌اندازی دفتر سی دی بی[2] در وزارت امور خارجه، مشارکت در تدوین قواعد جهانی حکمرانی سایبری، و همکاری با نهادهایی مانند گروه پنج چشم[3]، بخشی از اقدامات آمریکا در این حوزه است (Nye, 2010, 8–12). هدف از این دیپلماسی، ایجاد اجماع جهانی برای مقابله با تهدیدات شناختی، تنظیم‌گری فضای اطلاعاتی و مقابله با عملیات روانی سازمان‌یافته از سوی دولت‌های رقیب، به‌ویژه روسیه و چین است.

ایالات متحده همچنین از دیپلماسی عمومی به‌عنوان ابزاری برای تثبیت روایت‌های خود در سطح جهانی بهره گرفته است. استفاده از رسانه‌های بین‌المللی مانند سی‌ان‌ان، صدای آمریکا و شبکه‌های اجتماعی، به‌منظور تأثیرگذاری بر افکار عمومی در کشورهای هدف، بخشی از راهبرد اطلاعاتی آمریکا در عرصه جهانی است. این کشور تلاش کرده است تا با بهره‌گیری از قدرت نرم، روایت‌های خود را در برابر روایت‌های خصمانه تقویت کرده و مشروعیت سیاست‌های خارجی خود را افزایش دهد.

---

[1] USCYBERCOM

[2] Cyber Diplomacy Bureau

[3] گروه پنج چشم (Five Eyes) یک اتحاد اطلاعاتی متشکل از پنج کشور انگلیسی‌زبان ایالات متحده، بریتانیا، کانادا، استرالیا و نیوزیلند است که به‌طور گسترده در زمینه اشتراک‌گذاری اطلاعات امنیتی و نظارت جهانی همکاری می‌کنند.

ج. چالش قطبی‌سازی و اطلاعات جعلی

با وجود زیرساخت‌های پیشرفته و راهبردهای ملی، ایالات متحده در سطح اجتماعی با چالش‌های جدی مواجه است. قطبی‌سازی سیاسی، گسترش اطلاعات جعلی و کاهش اعتماد عمومی به رسانه‌ها و نهادهای رسمی، موجب شده است که تاب‌آوری شناختی جامعه آمریکا در برابر جنگ اطلاعاتی کاهش یابد (Iftikhar, 2024: 58– 62). انتخابات ریاست‌جمهوری ۲۰۱۶ و ۲۰۲۰، نمونه‌های بارز این چالش هستند؛ جایی که انتشار اطلاعات جعلی، عملیات روانی خارجی و روایت‌های متضاد، موجب تضعیف مشروعیت انتخاباتی و افزایش شکاف‌های اجتماعی شدند.

نقش پلتفرم‌هایی مانند فیس‌بوک، توییتر و یوتیوب در انتشار محتوای مخرب، موجب شد که دولت آمریکا به تدوین مقررات جدید برای تنظیم‌گری اطلاعاتی روی آورد. با این حال، تداوم قطب‌بندی سیاسی و قطبی‌شدن جامعه، همچنان یک آسیب‌پذیری ساختاری است که امکان سوءاستفاده بازیگران بیرونی از شکاف‌های اجتماعی و فرهنگی را فراهم می‌سازد. این وضعیت نشان می‌دهد که ابزارهای فناورانه و نهادی، اگر با سیاست‌های اجتماعی و فرهنگی همراه نشوند، نمی‌توانند به‌تنهایی تاب‌آوری شناختی جامعه را تضمین کنند.

د. بازدارندگی اطلاعاتی و ابتکارهای شفاف‌سازی

فراتر از ساختار نهادی، ایالات متحده در حوزه «بازدارندگی اطلاعاتی» نیز فعالانه عمل کرده است. برخلاف الگوی سنتی «پنهان‌کاری امنیتی»، این کشور از شفاف‌سازی هدفمند به‌عنوان ابزاری برای ایجاد بازدارندگی و تقویت انسجام داخلی بهره گرفته است. نمونه‌ای از این رویکرد، انتشار به‌موقع اطلاعات معتبر و قابل اتکا درباره تهدیدات خارجی، از جمله تحرکات نظامی در مناطق حساس مانند اوکراین و تایوان، بود که پیش از وقوع بحران‌های بزرگ منتشر شد تا روایت‌های خصمانه را بی‌اثر کرده و اعتبار روایت رسمی دولت را تقویت کند (Time, 2024). همچنین، ایالات متحده نهادهایی مانند (GEC)[1] را برای مقابله با روایت‌های رسانه‌ای خصمانه در مناطق مختلف جهان، به‌ویژه آفریقا و آمریکای لاتین، ایجاد کرده است. این نهاد با همکاری سازمان‌های مدنی و رسانه‌ای، تلاش کرده است تا روایت‌های ساختگی را شناسایی، افشا و خنثی کند (Rubin, 2025: 112– 115). با این حال، بحران بودجه و تعطیلی اخیر این نهاد، به‌عنوان یک نقطه ضعف راهبردی در برابر جنگ اطلاعاتی تعبیر شده است (Washington Post, 2025).

[1] Global Engagement Center

DOR: 20.1001.1.30926459.1404.2.4.2.0

در حوزه داخلی نیز، تجربه‌های انتخاباتی آمریکا نشان داده‌اند که عملیات اطلاعاتی خارجی می‌تواند به‌طور مستقیم بر روندهای دموکراتیک اثرگذار باشد. به همین دلیل، سرمایه‌گذاری در سامانه‌های پایش فضای مجازی، آموزش عمومی برای تشخیص اطلاعات نادرست و همکاری با شرکت‌های فناوری بزرگ برای کاهش دسترسی بازیگران مخرب به مخاطبان داخلی، به بخشی مهم از راهبرد ملی آمریکا تبدیل شده است. این اقدامات نشان می‌دهد که بازدارندگی اطلاعاتی، نه‌تنها به معنای دفاع سایبری، بلکه به معنای پیش‌دستی در روایت‌سازی، شفاف‌سازی و تقویت اعتماد عمومی است. در مجموع، تجربه ایالات متحده نشان می‌دهد که مدیریت جنگ اطلاعاتی تنها به ابزارهای فناورانه و نهادی محدود نیست، بلکه نیازمند ترکیب هوشمندانه‌ای از سیاست‌های شفاف‌سازی، آموزش عمومی، تقویت اعتماد به رسانه‌های داخلی و مشارکت فعال در تنظیم قواعد بین‌المللی است. این کشور با وجود برخورداری از ظرفیت‌های گسترده، همچنان با چالش‌های درونی و نهادی مواجه است که اگر برطرف نشوند، می‌توانند توانایی‌اش را در برابر جنگ اطلاعاتی آینده تضعیف کنند. تجربه آمریکا نشان می‌دهد که تاب‌آوری شناختی، محصول تعامل میان فناوری، سیاست، جامعه و دیپلماسی است و تنها در چارچوبی چندسطحی و یکپارچه قابل تحقق خواهد بود.

۵ـ۲ـ تحلیل تطبیقی و کاربست نظریه‌ها

۱ـ تطبیق با رئالیسم ساختاری: خودیاری اطلاعاتی در غیاب نهادهای جهانی

مطالعه موردی سه کشور ایران، اوکراین و ایالات متحده نشان می‌دهد که در غیاب نهادهای بین‌المللی مؤثر برای تنظیم‌گری فضای اطلاعاتی، دولت‌ها ناگزیر به اتخاذ راهبردهای خودیاری در حوزه جنگ اطلاعاتی شده‌اند. این وضعیت کاملاً با منطق رئالیسم ساختاری هم‌خوانی دارد؛ جایی که دولت‌ها در نظامی آنارشیک، برای حفظ بقاء و امنیت، به توسعه ظرفیت‌های داخلی و ابزارهای بازدارنده روی می‌آورند (Waltz, 1979: 98- 101). در ایران، این خودیاری به شکل تمرکز بر حکمرانی سایبری داخلی و تلاش برای کنترل روایت‌های داخلی نمود یافته است. در اوکراین، خودیاری اطلاعاتی با تکیه بر همکاری‌های منطقه‌ای و دیپلماسی اطلاعاتی فعال دنبال شده است. در ایالات متحده، خودیاری در قالب نهادسازی پیشرفته، دیپلماسی جهانی و توسعه ابزارهای مقابله با عملیات شناختی خارجی تحقق یافته است. در هر سه مورد، دولت‌ها به‌جای اتکا به نهادهای جهانی، به ظرفیت‌های خود برای مقابله با تهدیدات اطلاعاتی تکیه کرده‌اند.

۲ـ تطبیق با امنیت سایبری: تفاوت ظرفیت‌های دفاعی و تاب‌آوری شناختی

از منظر نظریه‌های امنیت سایبری، تفاوت میان سه کشور در سطح حکمرانی داخلی، زیرساخت‌های فناورانه و تاب‌آوری شناختی جامعه، تعیین‌کننده میزان اثربخشی آن‌ها در مقابله با جنگ اطلاعاتی بوده است (Craig & Valeriano, 2018). ایالات متحده با برخورداری از نهادهای تخصصی، بودجه‌های کلان و همکاری با شرکت‌های فناوری، توانسته است زیرساخت‌های دفاعی قدرتمندی ایجاد کند. اوکراین با وجود محدودیت‌های اقتصادی، از طریق همکاری‌های منطقه‌ای و کمپین‌های اجتماعی، تاب‌آوری شناختی جامعه را ارتقاء داده است. ایران نیز با وجود تلاش‌های داخلی، به دلیل ضعف در اعتماد عمومی و فقدان همکاری‌های منطقه‌ای، با محدودیت‌هایی در اثربخشی مواجه است.

۳ـ جنگ اطلاعاتی به‌مثابه ابزار بازتعریف مشروعیت سیاسی

در هر سه کشور، جنگ اطلاعاتی نه‌تنها تهدیدی امنیتی، بلکه ابزاری برای بازتعریف مشروعیت سیاسی و انسجام اجتماعی بوده است. در ایران، عملیات شناختی خارجی و داخلی موجب تضعیف اعتماد عمومی و افزایش شکاف‌های اجتماعی شده است. در اوکراین، جنگ اطلاعاتی روسیه تلاش کرده است تا مشروعیت دولت مرکزی را زیر سؤال ببرد. در ایالات متحده، انتشار اطلاعات جعلی و قطبی‌سازی سیاسی، مشروعیت انتخاباتی و انسجام اجتماعی را تهدید کرده‌اند (Iftikhar, 2024: 58–62). این یافته‌ها نشان می‌دهد که جنگ اطلاعاتی در نظم چندقطبی، به ابزاری برای بازآرایی قدرت، تضعیف دولت‌ها و تغییر رفتار جمعی تبدیل شده است؛ ابزاری که دولت‌ها باید آن را نه‌تنها در سطح امنیتی، بلکه در سطح حکمرانی و مشروعیت سیاسی مدیریت کنند.

۵ـ۳ـ مدل پیشنهادی مسئولیت دولت‌ها در عصر جنگ شناختی

۱ـ سطح ملی: حکمرانی سایبری و تنظیم‌گری اطلاعاتی

در سطح ملی، دولت‌ها موظف‌اند ظرفیت‌های داخلی خود را برای مقابله با تهدیدات شناختی و اطلاعاتی به‌طور بنیادین تقویت کنند. این مسئولیت مستلزم طراحی و اجرای مجموعه‌ای از سیاست‌های جامع در حوزه حکمرانی سایبری و تنظیم‌گری اطلاعاتی است. نخست، تدوین قوانین فراگیر برای حفاظت از داده‌های شخصی، مقابله با اطلاعات جعلی و تنظیم‌گری پلتفرم‌های دیجیتال، به‌عنوان پایه حقوقی حکمرانی اطلاعاتی، ضروری است. دوم، ایجاد نهادهای تخصصی برای پایش تهدیدات سایبری، پاسخ به حملات اطلاعاتی و هماهنگی میان دستگاه‌های امنیتی، ارتباطی و رسانه‌ای، نقش کلیدی در ارتقاء تاب‌آوری ملی ایفا می‌کند. سوم، سرمایه‌گذاری در فناوری‌های

DOR: 20.1001.1.30926459.1404.2.4.2.0

نوین، آموزش نیروی انسانی متخصص و توسعه سامانه‌های اعتبارسنجی محتوا، زیرساخت‌های دفاعی اطلاعاتی را تقویت کرده و توان پاسخ‌دهی دولت‌ها را در برابر عملیات شناختی افزایش می‌دهد. نمونه‌هایی از این اقدامات را می‌توان در سیاست‌های ایالات متحده با محوریت آژانس CISA[1]، در ایران با تمرکز بر مرکز ملی فضای مجازی و در اوکراین با همکاری با مرکز امنیت سایبری ناتو مشاهده کرد؛ کشورهایی که هر یک با سطحی متفاوت از ظرفیت نهادی، به تقویت حکمرانی سایبری داخلی پرداخته‌اند.

۲ـ سطح منطقه‌ای: دیپلماسی اطلاعاتی و سازوکارهای اعتمادسازی

در سطح منطقه‌ای، مسئولیت دولت‌ها از حوزه داخلی فراتر رفته و به دیپلماسی اطلاعاتی و توسعه سازوکارهای اعتمادسازی میان کشورها گسترش می‌یابد. در این سطح، دولت‌ها باید از طریق توافق‌نامه‌های منطقه‌ای، زمینه تبادل داده‌های تهدید، هماهنگی در پاسخ به حملات سایبری و طراحی کمپین‌های مشترک مقابله با اطلاعات جعلی را فراهم سازند. مشارکت در نهادهای منطقه‌ای مانند اتحادیه اروپا، سازمان همکاری شانگهای، یا پیمان‌های امنیتی منطقه‌ای، می‌تواند ظرفیت‌های دفاعی شناختی کشورها را ارتقاء داده و از طریق هم‌افزایی اطلاعاتی، اثربخشی مقابله با عملیات روانی سازمان‌یافته را افزایش دهد. توسعه سازوکارهای اعتمادسازی میان دولت‌ها، شرکت‌های فناوری و نهادهای مدنی نیز نقش مهمی در کاهش سوءتفاهم‌های اطلاعاتی و افزایش شفافیت در فضای منطقه‌ای ایفا می‌کند. تجربه اوکراین در همکاری با ناتو و اتحادیه اروپا، نمونه موفقی از دیپلماسی اطلاعاتی منطقه‌ای است که توانسته است حمایت سیاسی، رسانه‌ای و فناورانه گسترده‌ای را برای مقابله با جنگ شناختی جلب کند. در مقابل، ایران به دلیل محدودیت‌های ژئوپلیتیکی، تحریم‌های بین‌المللی و فقدان سازوکارهای عملیاتی، هنوز در این حوزه با خلأهای ساختاری مواجه است و به‌صورت منفرد با تهدیدات فراملی مقابله می‌کند.

۳ـ سطح بین‌المللی: مشارکت در تدوین قواعد جهانی

در سطح بین‌المللی، دولت‌ها باید نقش فعالی در تدوین قواعد حکمرانی اطلاعاتی ایفا کنند؛ نقشی که نه‌تنها برای حفاظت از منافع ملی، بلکه برای شکل‌دهی به نظم جهانی اطلاعاتی ضروری است. مشارکت در تدوین استانداردهای جهانی برای امنیت سایبری، حفاظت از داده‌ها و مقابله با عملیات شناختی، می‌تواند به ایجاد چارچوب‌های حقوقی الزام‌آور در سطح بین‌الملل منجر شود.

---

[1] آژانس امنیت سایبری و زیرساخت‌های ایالات متحده (Cybersecurity and Infrastructure Security Agency) مسئول حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات سایبری و اطلاعاتی می‌باشد.

همکاری با سازمان‌های بین‌المللی مانند سازمان ملل، اتحادیه بین‌المللی ارتباطات (ITU)[1] و مجامع تخصصی، بستری برای اجماع‌سازی و تنظیم‌گری چندجانبه فراهم می‌سازد. دولت‌ها همچنین باید در برابر تهدیدات فراملی مانند تروریسم سایبری، هک‌های دولتی و انتشار اطلاعات جعلی، تلاش کنند تا سازوکارهای پاسخ سریع، هماهنگ و مشروع بین‌المللی ایجاد شود. ایالات متحده با راه‌اندازی دفتر دیپلماسی سایبری در وزارت امور خارجه و مشارکت در گروه‌های چندجانبه مانند پنج چشم[2]، نمونه‌ای از ایفای مسئولیت در این سطح را ارائه داده است؛ مدلی که تلفیق قدرت فناورانه، ظرفیت دیپلماتیک، و مشروعیت بین‌المللی را در مواجهه با تهدیدات اطلاعاتی نشان می‌دهد.

جدول-۱. این مدل سه‌سطحی، چارچوبی مفهومی برای طراحی راهبردهای ملی و منطقه‌ای در مواجهه با جنگ اطلاعاتی

نمونه‌های تطبیقی	حوزه‌های اقدام	سطح مسئولیت
ایران، ایالات متحده	حکمرانی سایبری، تنظیم‌گری اطلاعاتی، ارتقاء زیرساخت‌ها	ملی
اوکراین، اتحادیه اروپا	دیپلماسی اطلاعاتی، تبادل داده، سازوکارهای اعتمادسازی	منطقه‌ای
ایالات متحده، نهادهای بین‌المللی	تدوین قواعد جهانی، همکاری چندجانبه، اجماع‌سازی	بین‌المللی

نتیجه‌گیری

پژوهش حاضر با تمرکز بر پیوند میان تحولات ساختاری در نظم بین‌الملل و ظهور جنگ اطلاعاتی، نشان داد که در دوران گذار از نظم تک‌قطبی به نظم چندقطبی، دولت‌ها با نوعی تهدید نوظهور و پیچیده مواجه‌اند که ماهیت آن فراتر از تهدیدات سنتی نظامی و اقتصادی است. جنگ اطلاعاتی، به‌عنوان یکی از ابزارهای راهبردی در رقابت قدرت‌ها، نه‌تنها زیرساخت‌های فناورانه و

[1] اتحادیه بین‌المللی ارتباطات (ITU) یک نهاد تخصصی وابسته به سازمان ملل متحد است که وظیفه تدوین استانداردهای جهانی در حوزه فناوری اطلاعات، ارتباطات و مدیریت طیف فرکانسی را بر عهده دارد.

[2] Five Eyes

DOR: 20.1001.1.30926459.1404.2.4.2.0

سایبری را هدف قرار می‌دهد، بلکه به‌طور مستقیم بر افکار عمومی، انسجام اجتماعی، مشروعیت سیاسی و حاکمیت ملی اثر می‌گذارد. این تهدیدات، به‌ویژه در نظم چندقطبی که فاقد چارچوب‌های نهادی تثبیت‌شده و قواعد الزام‌آور جهانی است، به‌صورت فزاینده‌ای از سوی بازیگران دولتی و غیردولتی هدایت می‌شوند و مرزهای سنتی امنیت را درنوردیده‌اند.

یافته‌های نظری پژوهش، با اتکا به رئالیسم ساختاری و نظریه‌های امنیت سایبری، نشان داد که دولت‌ها در چنین نظمی ناگزیر از خودیاری اطلاعاتی هستند؛ زیرا در فقدان اقتدار مرکزی و ضعف نهادهای بین‌المللی، حفظ بقاء و امنیت شناختی تنها از طریق تقویت ظرفیت‌های داخلی، توسعه همکاری‌های منطقه‌ای و مشارکت فعال در تدوین قواعد جهانی ممکن است. از سوی دیگر، تحلیل تجربی سه کشور ایران، اوکراین و ایالات متحده نشان داد که موفقیت دولت‌ها در مقابله با جنگ اطلاعاتی، به میزان سرمایه‌گذاری آن‌ها در سه حوزه کلیدی بستگی دارد: ۱ـ حکمرانی سایبری؛ ۲ـ دیپلماسی اطلاعاتی؛ و ۳ـ ارتقاء تاب‌آوری شناختی جامعه.

در سطح ملی، دولت‌ها باید با ایجاد چارچوب‌های قانونی و نهادی برای حکمرانی سایبری، امنیت زیرساخت‌های حیاتی و سامانه‌های اطلاعاتی را تضمین کنند. این شامل تدوین قوانین جامع برای حفاظت از داده‌ها، مقابله با اطلاعات جعلی و تنظیم‌گری پلتفرم‌های دیجیتال است. همچنین، ارتقاء سواد رسانه‌ای و شناختی شهروندان از طریق آموزش عمومی، تولید محتوای آموزشی و ایجاد مراکز اعتبارسنجی اطلاعات، نقش مهمی در کاهش آسیب‌پذیری شناختی و افزایش مقاومت اجتماعی در برابر عملیات روانی دارد. تجارب اوکراین در مقابله با عملیات اطلاعاتی روسیه نشان داد که ایجاد نهادهای تخصصی، کمپین‌های عمومی و همکاری با رسانه‌های مستقل، می‌تواند اثربخشی دولت‌ها را در مواجهه با تهدیدات شناختی به‌طور چشمگیری افزایش دهد.

در سطح منطقه‌ای، یافته‌ها تأکید می‌کنند که دولت‌ها نمی‌توانند به‌تنهایی با تهدیدات فراملی مقابله کنند. همکاری‌های امنیت سایبری میان کشورهای همجوار، تبادل داده‌های تهدید، طراحی کمپین‌های مشترک و ایجاد توافق‌نامه‌های امنیتی اطلاعاتی، ظرفیت جمعی برای مقابله با عملیات شناختی را افزایش می‌دهد. این همکاری‌ها نه‌تنها موجب هماهنگی در اقدامات پاسخ‌دهی می‌شوند، بلکه به ایجاد ثبات و اعتماد منطقه‌ای کمک کرده و از سوءاستفاده بازیگران غیردولتی و دشمنان خارجی از شکاف‌های ملی جلوگیری می‌کنند. در این زمینه، اوکراین با بهره‌گیری از همکاری‌های اطلاعاتی با ناتو و اتحادیه اروپا، توانسته است الگویی موفق از دیپلماسی اطلاعاتی منطقه‌ای ارائه دهد.

در سطح بین‌المللی، خلأهای حقوقی و نهادی در حوزه حکمرانی اطلاعاتی، نیازمند مشارکت فعال دولت‌ها در تدوین قواعد الزام‌آور، استانداردهای جهانی و سازوکارهای پاسخ سریع است. همکاری با سازمان‌های بین‌المللی مانند سازمان ملل، اتحادیه بین‌المللی ارتباطات و مجامع تخصصی، مشارکت در کنوانسیون‌های چندجانبه و تلاش برای اجماع‌سازی جهانی، نقش دولت‌ها را در مقابله با جنگ اطلاعاتی مشروع و اثربخش می‌سازد و امنیت جمعی را تقویت می‌کند. ایالات متحده با راه‌اندازی دفتر دیپلماسی سایبری و مشارکت در گروه‌های چندجانبه، نمونه‌ای از این سطح مسئولیت را ارائه داده است.

بر اساس این تحلیل چندسطحی، می‌توان نتیجه گرفت که موفقیت دولت‌ها در مدیریت جنگ اطلاعاتی در دوران گذار به نظم چندقطبی، مستلزم رویکردی جامع، یکپارچه و چندلایه است. این رویکرد باید شامل اقدامات پیشگیرانه، واکنشی و مشارکتی باشد که در سه سطح ملی، منطقه‌ای و بین‌المللی به‌صورت هم‌زمان اجرا شوند. دولت‌ها باید ظرفیت‌های فناورانه، نهادی و اجتماعی خود را تقویت کنند، شبکه‌های همکاری منطقه‌ای را توسعه دهند و در تدوین قواعد جهانی مشارکت فعال داشته باشند. تنها در چنین چارچوبی است که می‌توان تهدیدات پیچیده و چندوجهی جنگ اطلاعاتی را مهار کرده و امنیت ملی، انسجام اجتماعی و حاکمیت سیاسی را حفظ نمود.

در نهایت، توصیه‌های سیاستی پژوهش بر آن است که دولت‌ها باید استراتژی‌هایی پیشگیرانه، انعطاف‌پذیر و چندسطحی طراحی کنند که با تحولات سریع فناوری، تغییرات ساختاری در نظم بین‌الملل و ظهور بازیگران غیردولتی اطلاعاتی همسو باشند. این استراتژی‌ها باید شامل طراحی زیرساخت‌های سایبری مقاوم، ایجاد سامانه‌های نظارتی هوشمند، توسعه ظرفیت‌های تحلیل تهدیدات، آموزش عمومی و مشارکت در نهادهای بین‌المللی باشد. همچنین، سرمایه‌گذاری در توانمندسازی ملی از جمله نهادینه‌سازی قوانین و مقررات سایبری، آموزش و ارتقای سواد رسانه‌ای شهروندان و تقویت ظرفیت‌های پاسخ سریع، ضروری است تا تاب‌آوری جامعه و دولت در برابر عملیات روانی و حملات اطلاعاتی افزایش یابد.

در جمع‌بندی، پژوهش حاضر نشان داد که جنگ اطلاعاتی در نظم چندقطبی، نه یک تهدید گذرا، بلکه یک واقعیت ساختاری و پایدار است که دولت‌ها باید آن را در قلب راهبردهای امنیتی، حکمرانی و سیاست‌گذاری خود قرار دهند. تنها از طریق رویکردی جامع، چندسطحی و مشارکتی است که دولت‌ها می‌توانند نقش خود را به‌عنوان بازیگران مسئول، مشروع و تاب‌آور در نظم جهانی

DOR: 20.1001.1.30926459.1404.2.4.2.0

نوین ایفا کنند و امنیت، انسجام اجتماعی، و حاکمیت ملی را در برابر موج‌های پیچیده و چندوجهی تهدیدات اطلاعاتی حفظ نمایند.

تعارض منافع

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

Translated References to English

Bazavluk, S.V., & Kovalev, A.A. (2025). Information warfare in a multipolar world. International Relations, 25(2), 236–250. https://doi.org/10.22363/2313-0660-2025-25-2-236-250

Christou, G. (2016). Cybersecurity in the European Union: Resilience and adaptability in governance policy. Palgrave Macmillan.

Craig, A.J.S., & Valeriano, B. (2018). Realism and cyber conflict: Security in the digital age. CyberIR@MIT. https://cyberir.mit.edu/site/realism-and-cyber-conflict-security-digital-age/

Dehghani Firouzabadi, S.J. (2016). *General principles of international relations*. Tehran: Mokhatab Publications. [**In Persian**]

Dehshyar, H. (2021). *U.S. foreign policy in theory and practice*. Tehran: Mizan Publications. [**In Persian**]

ENISA. (2023). National Cybersecurity Strategies: Mapping and Analysis. European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/publications/national-cybersecurity-strategies

European Commission. (2022). Digital Services Act (DSA) and Digital Markets Act (DMA). Retrieved from https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Fried, D., & Polyakova, A. (2018). Democratic defense against disinformation. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/

Gbormittah, E. (2022). A systematic literature review on cyberwarfare and state-sponsored hacking. TechRxiv. https://www.techrxiv.org/users/813920/articles/1215154/master/file/data/Ebenezer_Gbormittah_UoG/Ebenezer_Gbormittah_UoG.pdf

Ghaderi Kangavari, R. (2022). America's hybrid war against the Islamic Republic of Iran through diplomacy and negotiation: From coercive diplomacy to informational deterrence. *Strategic American Studies, 2*(4), 11–47. [**In Persian**]

Gouliev, Z. (2025). Propaganda and information dissemination in the Russo-Ukrainian war: Natural language processing of Russian and Western Twitter narratives. arXiv. https://arxiv.org/abs/2506.01807

Ikenberry, G.J., Mastanduno, M., & Wohlforth, W.C. (2009). Unipolarity, state behavior, and systemic consequences. World Politics, 61(1), 1–27. https://doi.org/10.1017/S004388710900001X

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Libicki, M.C. (2007). Conquest in cyberspace: National security and information warfare. Cambridge University Press.

Mearsheimer, J.J. (2001). The tragedy of great power politics. W.W. Norton & Company. https://samuelbhfaure.com/wp-content/uploads/2015/10/s2-mearsheimer-2001.pdf

Mejova, H., Capozzi, A., Monti, C., & de Francisci Morales, G. (2023). Narratives of war: Ukrainian memetic warfare on Twitter. arXiv. https://arxiv.org/abs/2309.08363

Mousavi, S., & Ahmadi, R. (2021). Social media and national cohesion: Impacts on collective behavior and public opinion. Journal of Communication Studies, 11(3), 78–101. [**In Persian**]

Muzaffar, M., Yaseen, Z., & Rahim, N. (2017). Changing dynamics of global politics: Transition from unipolar to multipolar world. Liberal Arts and Social Sciences International Journal (LASSIJ), 1(1), 49–61. https://doi.org/10.47264/idea.lassij/1.1.6

Nordic Council of Ministers. (2021). Digital Literacy for Resilience: Strengthening Societal Resistance to Disinformation. Retrieved from https://www.norden.org/en/publication/digital-literacy-resilience

Nye, J.S. (2011). The future of power. PublicAffairs.

Nye, J.S. (2022). Soft power and information warfare in the digital age. Oxford University Press.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In Proceedings of the 7th European Conference on Information Warfare and Security (pp. 163–168). Academic Conferences Limited.

Ottis, R. (2018). From Estonia with love: Developing cyber resilience in small states. Journal of Cyber Policy, 3(1), 100–114. https://doi.org/10.1080/23738871.2018.1436944

Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model: Why it might work and options to counter it (RAND Perspective). RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html

Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html

Prysiazhniuk, M., et al. (2025). Strategic narratives and information warfare: Russian FIMI campaigns against Ukraine's armed forces. Culture. Society. Economy. Politics, 5(1), 88–108. https://sciendo.com/article/10.2478/csep-2025-0007

Rahbar, A. (2025). Public diplomacy of the Islamic Republic of Iran in facing cognitive warfare: Opportunities and challenges. COGRPS: Journal on Information and Security Studies. https://www.cogrps.ir/article_217214.html [**In Persian**]

Rahimi, N., & Jones, H. (2025). Cyber warfare: Strategies, impacts, and future directions in the digital battlefield. Journal of Information Security, 16, 252–269. https://www.scirp.org/journal/paperinformation?paperid=141708

Rezaii, H., & Kazemi, F. (2020). Redefining state roles in cyberspace governance and information regulation. Journal of Political Science, 12(2), 45–67. [**In Persian**]

Rezapur, D., & Majidi, A. (2021). Russia's hybrid warfare against Ukraine with an emphasis on information strategy. *Defense Management and Research Journal, 20*(91), 69–101. [**In Persian**]

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Rubin, J. P. (2025). America just surrendered to foreign lies. Washington Post.

Saedi, A. (2015). Site title. Tehran: Arena Publications. [**In Persian**]

Sharifi, M., & Falahy, A. (2022). The decline of U.S. hegemony and the rise of regional powers in West Asia: New patterns of international agency. Journal of Middle Eastern Studies, 8(1), 23–48. [**In Persian**]

Singer, P.W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

Tabatabaei, S.M., & Bahrami, Z. (2018). Continuity of transition in the international system. *Foreign Policy Quarterly, 32*(2), 39–70. [**In Persian**]

Thomas, T. (2021). Information warfare in the twenty-first century: New threats and responses. Journal of Information Warfare, 20(3), 1–15.

Time. (2024). Inside the White House program to share America's secrets. Time Magazine. https://time.com/2024/03/15/us-efforts-counter-russian-information-warfare/

DOR: 20.1001.1.30926459.1404.2.4.2.0

Torabi, G., & Taherizadeh, M.N. (2021). Cyber revolution and transformation of information warfare in international relations. Quarterly Journal of Information and Security Studies, 14(2), 45–68. https://doi.org/10.22034/isj.2021.279939.1432 [**In Persian**]

Valeriano, B., & Maness, R.C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.

Waltz, K.N. (1979). Theory of international politics. Addison-Wesley. https://dl1.cuni.cz/pluginfile.php/486328/mod_resource/content/0/Kenneth%20N.%20Waltz%20Theory%20of%20International%20Politics%20AddisonWesley%20series%20in%20political%20science%20%20%201979.pdf

Woolley, S.C., & Howard, P.N. (Eds.). (2018). Computational propaganda: Political parties, politicians, and political manipulation on social media. Oxford University Press.

World Economic Forum. (2024). The role of geopolitics in a multipolar world. https://www.weforum.org/stories/2024/05/why-geopolitics-matters-more-than-ever-in-a-multipolar-world

Xu, S. (2020). Cybersecurity dynamics: A foundation for the science of cybersecurity. arXiv. https://arxiv.org/abs/2010.05683

Yousefi, A. (2023). Cognitive security and public education: Tools for countering information threats. Iranian Journal of Security Studies, 16(1), 12–35. [**In Persian**]