AJA Command and Staff University

Warfare Study Quarterly

https://www.qjws.ir/ Online ISSN: 2717-1760 Print ISSN: 2717-1760

Hybrid Threats Against Islamic Republic of Iran: Strategic Requirements for an Integrated Defense Response

Asadulah Hasanpour[1*] ✉

1. Graduated from Department of Defense Management, AJA Command and staff University, Tehran, Iran. E-mail: hasanporasadulah@gmail.com

Article Info

Article type:

Research Article

Article history:

Received

16 July 2025

revised form

05 October 2025

Accepted

05 November 2025

Published online

20 January 2026

Keywords:

Hybrid Threats, Defense Strategy, Cognitive Warfare, Multi-Domain Command, National Security

ABSTRACT

Purpose: This study analyzes the hybrid threat environment confronting the Islamic Republic of Iran and identifies the strategic requirements for developing an indigenous and integrated defense posture. Given the complexity, deniability, and cross-domain synchronization of hybrid threats, the research proposes a conceptual–strategic framework to enhance national readiness and response effectiveness.

Method: Using a qualitative–analytical methodology, the study synthesizes domestic and international sources to examine core constructs including hybrid warfare, defense strategy, modern deterrence, cognitive warfare, and multi-domain operations within contemporary security contexts. The empirical dimensions of hybrid threats in Iran are assessed through structural analysis supported by secondary statistical data in cyber, media, economic, and socio-behavioral domains.

Findings: Results indicate that hybrid threats against Iran materialize across five key vectors: cyber intrusions, cognitive–media operations, proxy and border conflicts, economic–psychological pressure, and socially engineered unrest. Statistical evidence demonstrates a clear escalation in both scale and sophistication over the past decade. The study further identifies systemic gaps particularly the absence of a national doctrine, limited inter-agency integration, and insufficient cognitive defense capacity that constrain coordinated responses.

Conclusion: Effective counter-hybrid defense requires a shift from traditional, compartmentalized security approaches toward a proactive, multilayered, and indigenized model. Essential priorities include establishing a national hybrid-threat command structure, strengthening societal cognitive resilience, developing an integrated early-warning system, and updating defense education to address emerging hybrid operational realities.

Cite this article: Hasanpour, Asadulah. (2025). Hybrid Threats Against Islamic Republic of Iran: Strategic Requirements for an Integrated Defense Response. *Warfare Study Quartely*, 26(7), 3-32

DOI: http//doi.org/10.22034/qjws.2026.2065647.1295

Publisher: Command and Staff University

فصلنامه علمی مطالعات جنگ
شاپای چاپی: ۱۷۶۰-۲۷۱۷ شاپای الکترونیکی: ۱۷۶۰-۲۷۱۷ https://www.qjws.ir/ دانشگاه فرماندهی و ستاد آجا

تحلیل تهدیدات ترکیبی علیه جمهوری اسلامی ایران و الزامات طراحی پاسخ دفاعی یکپارچه: رویکردی مفهومی–راهبردی

اسدالله حسنپور[1]* ✉

۱. کارشناس ارشد گروه مدیریت دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: hasanporasadulah@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۴/۰۴/۲۵

تاریخ بازنگری:
۱۴۰۴/۰۷/۱۳

تاریخ پذیرش:
۱۴۰۴/۰۸/۱۴

تاریخ انتشار:
۱۴۰۴/۰۹/۳۰

کلیدواژه‌ها:
تهدیدات ترکیبی، راهبرد دفاعی، جنگ شناختی، فرماندهی چنددامنه‌ای، امنیت ملی

چکیده

هدف: این پژوهش به تحلیل ابعاد تهدیدات ترکیبی علیه جمهوری اسلامی ایران و تبیین الزامات طراحی یک پاسخ دفاعی بومی و یکپارچه می‌پردازد. با توجه به پیچیدگی، چندلایگی و انکارپذیری تهدیدات ترکیبی، مقاله تلاش دارد چارچوبی مفهومی-راهبردی برای مواجهه مؤثر با این پدیده ارائه دهد.

روش: روش تحقیق کیفی-تحلیلی و مبتنی بر بررسی منابع اسنادی داخلی و خارجی است. مفاهیم کلیدی مرتبط با تهدید ترکیبی، راهبرد دفاعی، بازدارندگی نوین، جنگ شناختی، عملیات چندلایه و امنیت ملی در محیط‌های پیچیده در قالب مبانی نظری تبیین شده و ابعاد عینی تهدیدات ترکیبی در بستر ملی از طریق تحلیل ساختاری بررسی گردیده است. همچنین برای تقویت استدلال‌ها و افزایش روایی یافته‌ها، از داده‌های آماری در حوزه‌های سایبری، رسانه‌ای، اقتصادی و اجتماعی استفاده شده است.

یافته‌ها: نتایج نشان می‌دهد تهدیدات ترکیبی علیه کشور در پنج محور اصلی شامل حملات سایبری، جنگ شناختی-رسانه‌ای، تهدیدات نیابتی، فشارهای اقتصادی–روانی و تحریکات اجتماعی بروز یافته‌اند. داده‌های آماری این روند را تأیید کرده و بیانگر افزایش کمی و کیفی تهدیدات طی یک دهه اخیر است. افزون بر این، تحلیل‌ها نشان می‌دهد شکاف‌هایی چون فقدان دکترین جامع، ضعف هماهنگی بین‌سازمانی و ناتوانی در دفاع شناختی، ظرفیت‌های پاسخ مؤثر را محدود کرده است.

نتیجه‌گیری: مقابله مؤثر با تهدیدات ترکیبی مستلزم طراحی راهبردی یکپارچه با تأکید بر ایجاد نهاد فرماندهی ترکیبی، ارتقای تاب‌آوری شناختی، توسعه سامانه هشدار زودهنگام و بازمهندسی نظام آموزشی دفاعی است. این امر نیازمند گذار از رویکردهای سنتی به رویکردی چندلایه، پیش‌دستانه و بومی‌سازی‌شده می‌باشد.

استناد: حسنپور، اسدالله. (۱۴۰۴). تحلیل تهدیدات ترکیبی علیه جمهوری اسلامی ایران و الزامات طراحی پاسخ دفاعی یکپارچه: رویکردی مفهومی-راهبردی. *فصلنامه مطالعات جنگ*، ۲۶(۷)، ۳۲-۳

DOI: 10.22034/qjws.2026.2065647.1295

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

در دهه‌های اخیر، تحولات ژئوپلیتیکی، پیشرفت‌های فناورانه، و گسترش ابعاد غیرسنتی جنگ موجب شکل‌گیری گونه‌ای از تهدیدات شده است که مرز میان نبرد نظامی و اقدامات غیردفاعی را در هم می‌ریزد (Banasik, 2016). این تهدیدات، که با عنوان تهدیدات ترکیبی شناخته می‌شوند، دیگر صرفاً مبتنی بر رویارویی‌های مستقیم نظامی نیستند، بلکه ترکیبی از روش‌های نظامی، سایبری، روانی، اقتصادی و اطلاعاتی را به‌کار می‌گیرند تا ساختارهای امنیتی، انسجام ملی و ثبات داخلی کشورها را دچار چالش کنند. تهدید ترکیبی، به‌ویژه در قالب عملیات‌های پیچیده و چندلایه، این توان را دارد که بدون درگیری سنتی و با بهره‌گیری از ابزارهای مدرن فناوری و رسانه، اهداف کلیدی کشورها را مورد حمله قرار دهد (رستمی و همکاران، ۱۴۰۰).

عملیات سایبری علیه زیرساخت‌های حیاتی، تهاجم‌های اطلاعاتی، دستکاری افکار عمومی از طریق شبکه‌های اجتماعی، ایجاد بحران‌های مصنوعی اقتصادی یا زیستی و بهره‌برداری هم‌زمان از نیروهای نیابتی، از جمله مصادیق رایج در این نوع تهدیدات به شمار می‌روند (حامد و کریمی، ۱۴۰۳). ویژگی اصلی تهدید ترکیبی، غیرقابل پیش‌بینی بودن، انکارپذیری عامل تهدیدکننده و چندوجهی بودن ابزارهای آن است. امری که موجب شده واکنش‌های دفاعی سنتی و مبتنی بر آمادگی صرف نظامی، ناکارآمد یا دیرهنگام تلقی شوند. از این‌رو، پاسخ مؤثر به این نوع تهدیدات نیازمند رویکردی چندسطحی، راهبردی و در عین حال بومی‌سازی‌شده است (Chivvis, 2017). در سطح جهانی، بسیاری از کشورها با بازنگری در دکترین‌های دفاعی خود، تلاش کرده‌اند به مقوله تهدید ترکیبی به‌عنوان یک خطر واقعی، سازمان‌یافته و مستمر نگاه کنند. نهادهایی مانند ناتو، اتحادیه اروپا و حتی کشورهای مستقل، با ایجاد واحدهای مقابله با تهدیدات ترکیبی و تدوین راهبردهای امنیتی یکپارچه، نشان داده‌اند که مقابله با این پدیده مستلزم آمادگی ساختاری، هماهنگی بین‌نهادی و بهره‌گیری از ظرفیت‌های فناورانه و اطلاعاتی است (حسینی و جداری سلامی، ۱۴۰۰).

این تحولات نشان می‌دهد که تهدیدات ترکیبی، با ماهیت چندبعدی خود، تنها از طریق رویکردهای سنتی قابل مهار نیستند. برای مثال، ناتو در سال‌های اخیر با تأسیس «مرکز مقابله با تهدیدات ترکیبی» در هلسینکی، بر اهمیت ادغام عملیات سایبری، جنگ اطلاعاتی، و اقدامات غیرمتعارف در چارچوب راهبردهای دفاعی تأکید کرده است. از سوی دیگر، اتحادیه اروپا با تصویب «چارچوب مقابله با تهدیدات ترکیبی» در سال ۲۰۱۶، بر همکاری میان بخش‌های نظامی، اقتصادی، و رسانه‌ای برای خنثی‌سازی حملات ترکیبی تأکید می‌کند. کشورهای منفرد مانند

ایالات متحده نیز با توسعه واحدهای ویژه، سعی در پیش‌بینی و پاسخ سریع به سناریوهای ترکیبی دارند. این تلاش‌ها حاکی از آن است که امنیت در عصر حاضر مستلزم چابکی سازمانی، سرمایه‌گذاری در هوش مصنوعی برای پایش تهدیدات، و آموزش نیروهای متخصص در حوزه‌های میان‌رشته‌ای است (Balomenos, 2023). در جمهوری اسلامی ایران نیز، با توجه به موقعیت ژئوپلیتیکی خاص، شرایط خاص منطقه‌ای و تنوع تهدیدات، شناخت دقیق این نوع تهدیدات و طراحی یک پاسخ متناسب با ویژگی‌های بومی، سیاسی، فرهنگی و امنیتی کشور، امری حیاتی به شمار می‌رود. این امر مستلزم تحلیل دقیق تجربه‌های جهانی، ارزیابی نقاط قوت و ضعف نظام دفاعی کشور در برابر تهدیدات ترکیبی و شناسایی ظرفیت‌ها و الزامات بومی برای پاسخ‌گویی مؤثر است (احتشامی و همکاران، ۱۴۰۳).

علی‌رغم رشد روزافزون ادبیات نظری و مطالعات موردی پیرامون تهدیدات ترکیبی در سطح بین‌المللی، در فضای پژوهشی داخلی، بیشتر تحقیقات موجود یا صرفاً بر ابعاد نظامی این تهدیدات متمرکز بوده‌اند یا به‌صورت پراکنده به جنبه‌های سایبری و شناختی پرداخته‌اند، بی‌آنکه چارچوبی یکپارچه برای تحلیل و پاسخ به آن‌ها ارائه دهند. از این‌رو، نوآوری اصلی این پژوهش در ارائه یک رویکرد مفهومی-راهبردی مبتنی بر تحلیل ساختار تهدیدات ترکیبی در بستر بومی جمهوری اسلامی ایران است. افزون بر این، پژوهش حاضر با بهره‌گیری همزمان از داده‌های آماری ثانویه و تحلیل کیفی، تلاش کرده است تا شواهد عینی و مصادیق کمّی تهدیدات ترکیبی را در کنار چارچوب نظری بررسی نماید. این رویکرد دوگانه، ضمن تأکید بر تلفیق دفاع سخت و نرم، به‌دنبال ارائه الزامات عملیاتی، نهادی و راهبردی برای طراحی پاسخ دفاعی یکپارچه در برابر سناریوهای ترکیبی معاصر است. بدین ترتیب، پژوهش حاضر گامی در جهت پر کردن خلأ موجود در ادبیات داخلی و ارائه چارچوبی برای تقویت پاسخ دفاعی در بستر بومی جمهوری اسلامی ایران به شمار می‌آید. پرسش اصلی آن است که راهبردهای دفاعی جمهوری اسلامی ایران تا چه اندازه با ماهیت تهدیدات ترکیبی انطباق دارند و برای ارتقاء توان بازدارندگی و واکنش، چه الزامات بومی باید مورد توجه قرار گیرد؟ در راستای پاسخ به این سؤال، سؤالات فرعی ذیل مطرح می‌شوند: ۱) ماهیت و ویژگی‌های تهدیدات ترکیبی چیست و چه تمایزاتی با تهدیدات سنتی دارد؟ ۲) راهبردهای متداول کشورها و نهادهای بین‌المللی در مقابله با تهدیدات ترکیبی کدام‌اند؟ ۳) چه چالش‌ها و شکاف‌هایی در راهبردهای دفاعی جمهوری اسلامی ایران نسبت به تهدیدات ترکیبی وجود دارد؟ ۴) چه مؤلفه‌هایی باید در طراحی یک چارچوب بومی برای مقابله با تهدیدات ترکیبی در نظر گرفته شود؟

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری مرتبط با تهدیدات ترکیبی

تهدید ترکیبی به نوعی از تهدیدات اطلاق می‌شود که در آن عوامل دولتی یا غیردولتی از ترکیب ابزارهای نظامی و غیرنظامی برای دستیابی به اهداف استراتژیک خود علیه کشور هدف استفاده می‌کنند به‌گونه‌ای که تشخیص مرز بین جنگ و صلح، مهاجم و مدافع و حتی عملیات نظامی و غیرنظامی دشوار می‌شود (Murray et al., 2012: 12). در این مدل تهدید، از روش‌هایی چون حملات سایبری، نفوذ اطلاعاتی، عملیات روانی، جنگ رسانه‌ای، فشار اقتصادی، خرابکاری در زیرساخت‌ها، بهره‌گیری از نیروهای نیابتی و درگیری‌های نظامی محدود به‌صورت هم‌زمان و هماهنگ استفاده می‌شود. مؤلفه‌ها و ویژگی‌های اصلی تهدیدات ترکیبی شامل ترکیب ابعاد نظامی و غیرنظامی، انکارپذیری، پراکندگی و عدم تمرکز عاملان تهدید، چندلایه بودن عملیات و هدف قرار دادن ساختارهای نرم است (علیزاده، ۱۴۰۰). تهدیدات ترکیبی در محیط امنیتی معاصر به شکل محسوسی در صحنه‌های مختلف جهانی و منطقه‌ای تجلی یافته‌اند. در بحران اوکراین از سال ۲۰۱۴ تاکنون، این کشور شاهد به‌کارگیری هماهنگ ابزارهای ترکیبی توسط روسیه است که شامل جنگ اطلاعاتی سیستماتیک، حملات سایبری زیرساختی، استفاده از نیروهای نظامی بدون نشان، تحریک و هدایت نارضایتی‌های داخلی و عملیات روانی گسترده برای شکل‌دهی به افکار عمومی پیش از مداخله نظامی بوده است (Giles, 2016). در مقابل، ناتو در منطقه بالتیک با ایجاد سازوکارهای نهادی ویژه به مقابله چندوجهی با این تهدیدات پرداخته که شامل خنثی‌سازی نفوذ رسانه‌ای، مقابله با تهاجم شناختی و دفاع سایبری یکپارچه به صورت همزمان می‌شود. در غرب آسیا نیز الگوی تهدیدات ترکیبی عمدتاً در قالب عملیات نیابتی سازمان‌یافته، شبکه‌های رسانه‌ای هدایت‌شده و برنامه‌های اثرگذاری روانی-اجتماعی بر جوامع هدف ظهور یافته است (رفیعی راد و همکاران، ۱۳۹۹).

این نمونه‌ها نشان‌دهنده گذار از الگوهای سنتی تهدید به سمت جنگ ترکیبی چندبعدی است که در آن ابزارهای سخت و نرم به صورت هماهنگ و تقویت‌کننده یکدیگر به کار گرفته می‌شوند. با توجه به وضعیت منطقه‌ای جمهوری اسلامی ایران، تنوع دشمنان بالقوه و بالفعل، و سابقه تاریخی مواجهه با عملیات‌های ترکیبی (مانند جنگ نرم، اغتشاشات مهندسی‌شده، تحریم‌های هدفمند، و حملات سایبری)، شناخت و تحلیل تهدیدات ترکیبی برای بازطراحی راهبردهای دفاعی، ضروری و بنیادین است.

مبانی نظری مرتبط با راهبرد دفاعی

راهبرد دفاعی عبارت است از مجموعه‌ای از اصول، خط‌مشی‌ها و تصمیم‌گیری‌های کلان که برای حفظ منافع حیاتی کشور در برابر تهدیدات خارجی و داخلی طراحی می‌شود. این راهبرد، نحوه بهره‌گیری از منابع ملی اعم از نظامی، اطلاعاتی، اقتصادی و سیاسی برای تأمین امنیت ملی و بازدارندگی مؤثر را مشخص می‌کند. راهبرد دفاعی پلی میان اهداف کلان امنیتی کشور و ظرفیت‌های عملیاتی آن است. بدین معنی است که از یک سو متکی بر تحلیل محیط راهبردی (تهدیدات، فرصت‌ها، بازیگران) و از سوی دیگر تابع توانمندی‌های داخلی در حوزه‌های نظامی، سایبری، اطلاعاتی، و دیپلماسی است (Freedman, 2015:13-15). تفاوت راهبرد دفاعی با تاکتیک دفاعی، دکترین دفاعی و سیاست دفاعی به شرح ذیل است:

۱- راهبرد دفاعی: نحوه استفاده از ابزارهای مختلف برای تحقق آن سیاست.

۲- سیاست دفاعی: جهت‌گیری کلان دولت در حوزه دفاع (نگاه صلح‌طلبانه یا مداخله‌گرایانه).

۳- دکترین دفاعی: اصول عملیاتی و آموزشی نیروهای مسلح برای پیاده‌سازی راهبرد.

۴- تاکتیک دفاعی: شیوه اجرایی در میدان عملیات (در سطح رزم).

بنابراین، راهبرد دفاعی نه‌تنها تعیین‌کننده نوع پاسخ به تهدیدات است، بلکه چارچوبی برای طراحی ساختار نیروهای مسلح، تخصیص منابع، توسعه فناوری‌های دفاعی و اولویت‌بندی تهدیدات نیز فراهم می‌کند. راهبرد دفاعی مؤثر باید بر پایه مؤلفه‌هایی طراحی شود که هم با ماهیت تهدیدات سازگار باشند و هم متناسب با ظرفیت‌ها و الزامات بومی کشور تدوین شوند. رویکردهای جهانی در طراحی راهبرد دفاعی شامل چند مدل کلیدی است: راهبرد بازدارندگی کلاسیک که بر اتکا به قدرت نظامی برای جلوگیری از حمله تأکید دارد. راهبرد بازدارندگی هوشمند که با ترکیب قدرت سخت و نرم به دنبال تأثیرگذاری چندبعدی است. راهبرد تدافعی فعال که بر اساس اسناد رسمی بر مقابله پیش‌دستانه با تهدیدات تمرکز می‌کند و در نهایت راهبرد انعطاف‌پذیر تطبیقی که با توجه به سناریوها و تهدیدات متغیر و سریع‌التحول طراحی شده است (Mazarr, 2015: 55).

با توجه به شرایط ژئوپلیتیکی جمهوری اسلامی ایران، نوع تهدیدات منطقه‌ای و ساختار تصمیم‌گیری امنیتی و ویژگی‌های فرهنگی-اجتماعی ایجاب می‌کند که طراحی راهبرد دفاعی مبتنی بر ظرفیت‌های بومی، تجربه‌های ملی و شناخت عمیق از الگوی جنگ ترکیبی خاص جمهوری اسلامی ایران باشد.

مبانی نظری مرتبط با بازدارندگی نوین

بازدارندگی مفهومی بنیادین در راهبردهای دفاعی است که به معنای ایجاد شرایطی است که دشمن را از انجام اقدام خصمانه باز دارد. نه فقط از طریق درگیری مستقیم، بلکه از طریق افزایش هزینه‌های احتمالی آن اقدام به‌گونه‌ای که انجام آن را برای دشمن غیرمنطقی یا زیان‌بار کند. در شکل سنتی، بازدارندگی عمدتاً مبتنی بر تهدید به تلافی نظامی سخت بود اما با پیچیده‌تر شدن ماهیت تهدیدات به‌ویژه در قالب تهدیدات ترکیبی، خاکستری و هیبریدی و مفهوم بازدارندگی نیز دچار تحولاتی شده است. بنابراین بازدارندگی نوین به ترکیبی از ابزارهای نظامی، اطلاعاتی، سایبری، شناختی و دیپلماتیک اشاره دارد که با رویکرد هوشمندانه و چندلایه طراحی می‌شود. در این مدل، تنها قدرت سخت کافی نیست، بلکه مؤلفه‌های نرم نیز باید نقش اصلی ایفا کنند (Wilner, 2014). ابعاد اصلی بازدارندگی نوین شامل چهار رکن اساسی است: بازدارندگی نظامی متعارف که مبتنی بر حفظ آمادگی رزمی، نمایش قدرت نظامی و حفظ توان پاسخگویی به تهدیدات سخت می‌باشد. بازدارندگی سایبری که بر حفاظت از زیرساخت‌های حیاتی، توسعه توانایی پاسخ متقابل به حملات سایبری و تقابل اطلاعاتی تأکید دارد. بازدارندگی شناختی که به دفاع از افکار عمومی و فضای ذهنی جامعه در برابر عملیات روانی، شایعه‌سازی و جنگ رسانه‌ای می‌پردازد و بازدارندگی هوشمند که با بهره‌گیری از ترکیب قدرت سخت و نرم، ابزارهای اطلاعاتی و تشکیل ائتلاف‌های منطقه‌ای، به ایجاد موازنه در برابر تهدیدات چندبعدی می‌انجامد. این رویکرد جامع نشان‌دهنده تحول در مفهوم بازدارندگی در عصر حاضر است که دیگر صرفاً به بعد نظامی محدود نبوده و تمامی حوزه‌های تأثیرگذار را در بر می‌گیرد. تمایز بازدارندگی نوین با بازدارندگی کلاسیک در جدول (۱) نشان داده شده است (Rattray, 2001: 7-15).

جدول(۱) تمایز بازدارندگی نوین با بازدارندگی کلاسیک

معیار مقایسه	بازدارندگی کلاسیک	بازدارندگی نوین
ابزار اصلی	قدرت نظامی سخت	ترکیب قدرت سخت و نرم
محور تهدید	جنگ مستقیم	تهدیدات ترکیبی و خاکستری
مخاطب	دولت‌ها	دولت‌ها و گروه‌های غیردولتی
زمان‌بندی	واکنش در برابر حمله	اقدام پیش‌دستانه برای جلوگیری از حمله

با توجه به سابقه تهدیدات چندلایه علیه جمهوری اسلامی ایران، به‌ویژه در زمینه جنگ نرم، تروریسم، تحریم هوشمند و حملات سایبری، بازدارندگی نوین باید در چارچوبی بومی طراحی شود. این چارچوب می‌بایست هم ساختارهای نظامی و امنیتی را ارتقاء دهد، و هم زیرساخت‌های فرهنگی، اطلاعاتی، شناختی و رسانه‌ای را تجهیز کند.

مبانی نظری مرتبط با جنگ شناختی

جنگ شناختی به شکل خاصی از عملیات برنامه‌ریزی شده اشاره دارد که هدف اصلی آن تأثیرگذاری و هدایت ذهن، درک، عواطف و کنش‌های انسانی است. در این روش، افراد به صورت ناخودآگاه در مسیر مورد نظر عامل تهدید قرار می‌گیرند، بدون اینکه لزوماً از منشأ و ماهیت واقعی این تأثیرات آگاهی داشته باشند. این پدیده تلفیقی از دانش‌های مختلف شامل علوم شناختی، روان‌شناسی، علوم اعصاب، فناوری‌های دیجیتال و مطالعات رفتاری است که مرزهای بین واقعیت، روایت‌سازی، اطلاعات نادرست و تأثیرات روانی را محو می‌کند. آنچه جنگ شناختی را از دیگر اشکال نبرد غیرمتعارف متمایز می‌سازد، توانایی آن در ایجاد دگرگونی‌های عمیق و ماندگار در شیوه‌های ادراک، چارچوب‌های ذهنی و مکانیسم‌های تصمیم‌گیری در سطح فردی و اجتماعی است. ویژگی چندبعدی و نظام‌مند این نوع جنگ، آن را به یکی از کارآمدترین ابزارهای شکل‌دهی به رفتارها و باورها در دوران معاصر تبدیل کرده است (Lanoszka, 2019).

جنگ شناختی به عنوان یک پدیده پیچیده در عرصه مناسبات امنیتی معاصر، از مجموعه‌ای از ابزارها و روش‌های پیشرفته برای تأثیرگذاری نظام‌مند بر فرآیندهای شناختی و رفتاری بهره می‌برد. در این میان، شبکه‌های اجتماعی به عنوان یکی از مؤثرترین بسترهای عملیاتی، از طریق مکانیسم‌هایی چون انتشار محتوای گمراه‌کننده، دستکاری در ترندهای مجازی، ایجاد هشتگ‌های جهت‌دار و به‌کارگیری حساب‌های کاربری غیرواقعی، نقش محوری در عملیات روانی ایفا می‌کنند. روایت‌پردازی استراتژیک به عنوان یکی از ارکان اصلی جنگ شناختی، مبتنی بر طراحی و انتشار داستان‌های به ظاهر منسجم و جذاب صورت می‌پذیرد که با ترکیبی از عناصر واقعی و تحریف‌شده، تلاش می‌کند الگوهای ادراکی مخاطبان را به صورت نامحسوس تحت تأثیر قرار دهد. این فرآیند که مبتنی بر تحلیل‌های پیشرفته الگوریتمی صورت می‌گیرد، تأثیرپذیری مخاطب را به میزان قابل توجهی افزایش می‌دهد. در لایه‌ای عمیق‌تر، فناوری‌های نوین شناختی شامل سیستم‌های هوش مصنوعی، محیط‌های واقعیت مجازی و الگوریتم‌های یادگیری ماشین، امکان مداخله در سطوح بنیادین تفکر و تصمیم‌گیری افراد را فراهم می‌آورند (ترابی و همکاران، ۱۴۰۴).

جمهوری اسلامی ایران، با توجه به شرایط خاص رسانه‌ای، فرهنگی و امنیتی، در معرض تهدیدات شناختی سازمان‌یافته قرار دارد. برای مقابله با این پدیده باید زیرساخت دفاع شناختی ملی ایجاد شود، سواد رسانه‌ای، تفکر انتقادی و هوشیاری روانی اجتماعی تقویت شود و نهادهای مرتبط با فرهنگ، آموزش، رسانه و امنیت، با هماهنگی راهبردی عمل کنند.

مبانی نظری مرتبط با عملیات چندلایه

عملیات چندلایه به نوعی از کنش‌های راهبردی گفته می‌شود که در آن اقدامات دشمن یا پاسخ دفاعی در چند حوزه هم‌زمان و به‌صورت هماهنگ انجام می‌شود. این حوزه‌ها می‌توانند شامل زمین، هوا، دریا، فضا، سایبر، اطلاعات و شناخت باشند. هدف از چنین عملیات‌هایی، ایجاد برتری هم‌زمان در چند جبهه عملیاتی است به‌گونه‌ای که دشمن در تصمیم‌گیری، بسیج منابع و واکنش مؤثر دچار اختلال شود. جدول (۲)، به سطوح و ابعاد عملیات چندلایه اشاره می‌کند.

جدول (۲) سطوح و ابعاد عملیات چندلایه

سطوح	حوزه عملیاتی	نوع اقدام ممکن
سطح ۱	نظامی (زمینی، هوایی، دریایی)	عملیات محدود، تهدید مرزی، تحریک میدانی
سطح ۲	سایبری	نفوذ به زیرساخت‌های حیاتی، اختلال در ارتباطات
سطح ۳	اطلاعاتی	سرقت داده، فریب اطلاعاتی، جعل اسناد
سطح ۴	رسانه‌ای	جنگ روایت‌ها، شایعه‌پراکنی، اختلال ادراکی
سطح ۵	اقتصادی	تحریم هدفمند، حمله به زنجیره تأمین، تورم مصنوعی
سطح ۶	اجتماعی-فرهنگی	تحریک قومیتی، تفرقه‌افکنی، تضعیف اعتماد اجتماعی

عملیات نظامی سنتی عمدتاً بر یک حوزه عملیاتی خاص متمرکز بوده و از محدودیت‌های مشخصی در حوزه زمانی و جغرافیایی برخوردار است. در مقابل، عملیات چندلایه مدرن دارای ویژگی‌های متمایزی است که آن را به پدیده‌ای پیچیده و چالش‌برانگیز تبدیل می‌کند (Rid et al., 2015). این تفاوت‌های بنیادین موجب شده است که مقابله با تهدیدات چندلایه مستلزم بازنگری اساسی در دکترین‌های امنیتی و توسعه قابلیت‌های جدید در سطوح راهبردی و عملیاتی باشد. ماهیت سیال و غیرخطی این نوع عملیات، چالش‌های بی‌سابقه‌ای را در حوزه‌های برنامه‌ریزی، اجرا و ارزیابی عملیات ایجاد کرده است. دفاع مؤثر در برابر عملیات چندلایه با چالش‌های متعددی مواجه است که از جمله می‌توان به تجزیه و پراکندگی سازمانی اشاره کرد. به‌گونه‌ای که عدم هماهنگی میان نهادهای دفاعی، اطلاعاتی، رسانه‌ای و امنیتی موجب کاهش شدید کارآمدی پاسخ‌گویی می‌شود (قاسمی و همکاران، ۱۴۰۱). تجربه جمهوری اسلامی ایران در مواجهه با طیف گسترده‌ای از تهدیدات ترکیبی شامل جنگ‌های نیابتی، تحریم‌های چندبعدی، حملات سایبری، عملیات روانی-رسانه‌ای و آشوب‌های اجتماعی سازمان‌یافته، ضرورت تحول در راهبرد دفاعی کشور را آشکار ساخته است. این تجربیات نشان می‌دهد که ساختارهای امنیتی و دفاعی کنونی باید از حالت تک‌بعدی و جزیره‌ای خارج شده و به سمت توسعه یک راهبرد دفاع ترکیبی یکپارچه در سطح ملی حرکت کنند. این رویکرد یکپارچه، امکان پیش‌بینی، پیشگیری و مقابله مؤثر با جنگ‌های ترکیبی نوین را فراهم خواهد آورد.

مبانی نظری مرتبط با امنیت ملی در محیط‌های پیچیده و چندبُعدی

در الگوی سنتی امنیت ملی ، امنیت ملی عمدتاً معطوف به توانایی دولت در حفظ حاکمیت سرزمینی، تمامیت ارضی و ثبات سیاسی در برابر تهدیدات خارجی بود. با این حال، تحولات ژئوپلیتیک و فناورانه دهه‌های اخیر موجب بازتعریف این مفهوم شده است. در چارچوب نوین، امنیت ملی به عنوان سیستمی پیچیده و چندبعدی درک می‌شود که علاوه بر مؤلفه‌های سنتی، ابعاد اقتصادی، اجتماعی، زیست‌محیطی، سایبری و شناختی را نیز در بر می‌گیرد. این تحول مفهومی ناشی از چندین عامل کلیدی است:
۱) فرآیند جهانی‌شدن و افزایش وابستگی‌های متقابل بین‌المللی ۲) ظهور و گسترش فناوری‌های نوین در حوزه ارتباطات و سایبر ۳) تنوع یافتن تهدیدات امنیتی و ظهور بازیگران غیردولتی مؤثر ۴) محو شدن مرزهای سنتی بین تهدیدات داخلی و خارجی ۵) افزایش اهمیت عوامل غیرنظامی در معادلات امنیتی (Buzan, 1998: 21-29).

این تغییر الگوی سنتی امنیت ملی، مستلزم بازنگری اساسی در راهبردهای امنیت ملی و توسعه رویکردهای جامع‌نگر است که بتوانند پیچیدگی‌های محیط امنیتی معاصر را پوشش دهند. در این چارچوب جدید، امنیت دیگر صرفاً یک مفهوم حکومتی نبوده، بلکه به موضوعی چندسطحی تبدیل شده که مشارکت تمامی نهادهای اجتماعی را طلب می‌کند. محیط امنیتی کنونی از چهار ویژگی کلیدی برخوردار است که درک آن‌ها برای طراحی راهبردهای دفاعی ضروری می‌باشد. نخست، پیچیدگی به این معنا که تهدیدات امروزی از مسیرهای خطی و قابل پیش‌بینی ظهور نمی‌کنند، بلکه در شبکه‌ای از ارتباطات متقابل بین عوامل داخلی و خارجی، ابزارهای سنتی و نوین و نهادهای نظامی و غیرنظامی شکل می‌گیرند. دوم، پویایی محیط امنیتی به گونه‌ای است که ماهیت تهدیدات به سرعت دگرگون می‌شود و ممکن است یک چالش امنیتی در بازه‌ای کوتاه به فرصتی راهبردی تبدیل گردد یا بالعکس. سومین ویژگی، ابهام فزاینده در تمایز بین دوست و دشمن، حالت‌های جنگ و صلح، اطلاعات واقعی و ساختگی، و حتی حیطه مسئولیت نهادهای مختلف است (Brauch, 2005).

در این راستا، طراحی هرگونه راهبرد دفاعی کارآمد در برابر تهدیدات نوین، مستلزم توسعه چارچوبی جامع‌نگر است که بتواند پیچیدگی‌های محیط امنیتی معاصر را به خوبی بازتاب دهد. این چارچوب باید قادر باشد ارتباطات متقابل و اثرات سیستمی بین ابعاد مختلف تهدیدات را شناسایی و تحلیل نموده، بستر لازم برای تصمیم‌گیری یکپارچه و هماهنگی مؤثر بین تمامی

نهادهای ذی‌ربط را فراهم آورد. چنین نگاهی نه‌تنها امکان پیش‌بینی و پیشگیری از تهدیدات را افزایش می‌دهد، بلکه کارایی پاسخ‌های امنیتی را در سطوح مختلف ارتقاء خواهد بخشید.

پیشینه‌های پژوهش

در سال‌های اخیر، موضوع تحلیل تهدیدات ترکیبی و طراحی راهبردهای دفاعی متناسب با آن، به یکی از محورهای اصلی مطالعات راهبردی در حوزه امنیت ملی تبدیل شده است. این حوزه، چه در ادبیات پژوهشی بین‌المللی و چه در پژوهش‌های داخلی، مورد توجه روزافزون قرار گرفته و زمینه‌ساز تولید ادبیات نظری و کاربردی گسترده‌ای شده است. در این بخش، با هدف تبیین جایگاه تحقیق حاضر در میان آثار پیشین، مروری ساختاریافته بر مطالعات انجام‌شده ارائه می‌شود تا ضمن شناسایی یافته‌های کلیدی و مسیرهای طی‌شده، خلأهای پژوهشی موجود نیز آشکار گردد.

پژوهش‌های بین‌المللی عمدتاً بر تحلیل مفهومی تهدیدات ترکیبی، بررسی ابعاد جنگ شناختی، و ارزیابی رویکردهای نوین بازدارندگی تمرکز داشته‌اند. مطالعه Mahnken و همکاران (۲۰۱۹) با تمرکز بر مفهوم «منطقه خاکستری»، بر ضرورت طراحی پاسخ‌های راهبردی چندوجهی تأکید می‌ورزد (Mahnken et al., 2019). در پژوهشی دیگر، Chivvis (۲۰۱۷) با تحلیل راهبردهای روسیه در اوکراین، به تبیین نقش عملیات اطلاعاتی، حملات سایبری و بهره‌گیری از نیروهای نیابتی در ساختار تهدیدات هیبریدی پرداخته است (Chivvis, 2017). مرکز ارتباطات راهبردی ناتو (NATO StratCom) نیز در گزارشی تحت عنوان «جنگ شناختی»، تهدیدات مرتبط با عملیات‌های ادراکی و دست‌کاری افکار عمومی را در قالب جنگ ترکیبی تحلیل نموده است. در همین راستا، مرکز اروپایی مقابله با تهدیدات هیبریدی نیز با تمرکز بر الزامات نهادی و طراحی الگوی فرماندهی چنددامنه‌ای، بر اهمیت بازآرایی ساختارهای دفاعی در مقابله با تهدیدات ترکیبی تأکید می‌کند.

در فضای پژوهشی کشور نیز طی سال‌های اخیر، توجه به ابعاد نوین تهدیدات، به‌ویژه تهدیدات ترکیبی، رو به افزایش بوده است. رستمی، پرتوی و همکاران (۱۴۰۰) به بررسی عوامل امنیتی مؤثر در بروز جنگ ترکیبی توسط گروه‌های تروریستی در غرب آسیا بر اساس نظریه سازه‌انگاری می‌پردازد. با استفاده از روش توصیفی-تحلیلی و نظرات خبرگان، نتایج نشان می‌دهد که تعامل عوامل امنیتی داخلی، منطقه‌ای و بین‌المللی منجر به جنگ ترکیبی شده و امنیت غرب آسیا را در ابعاد ژئوپلتیک و ایدئولوژیک تهدید می‌کند (رستمی و همکاران، ۱۴۰۰). مجد و همکاران (۱۴۰۳) به بررسی جنگ شناختی به‌عنوان عرصه جدید نبرد می‌پردازد که در آن هدف،

تأثیرگذاری بر ذهن و آگاهی انسان از طریق فضای سایبر است. با استفاده از روش تحقیق کیفی (زمینه‌بنیاد)، مطالعه حاضر به دنبال طراحی یک مدل مفهومی برای خط‌مشی‌گذاری مقابله با تهدیدات جنگ شناختی دشمن در فضای سایبر است. مدل پیشنهادی شامل سه بخش کلیدی جنگ شناختی، فضای سایبر و فرایند خط‌مشی‌گذاری است تا از غافلگیری راهبردی جلوگیری کند (مجد و همکاران، ۱۴۰۳). صالح‌نیا و بختیاری (۱۳۹۷) به بررسی و اولویت‌بندی تهدیدات امنیتی جمهوری اسلامی ایران در سطوح مختلف (فروملی، ملی و فراملی) می‌پردازد. با استفاده از روش تحلیل سلسله‌مراتبی (AHP) و نظرات خبرگان، تهدیدات در ابعاد نظامی-اطلاعاتی، سیاسی-فرهنگی، اقتصادی و محیطی دسته‌بندی و ارزیابی شده است. نتایج نشان می‌دهد که تهدیدات نظامی-اطلاعاتی، به‌ویژه جاسوسی و نفوذ اطلاعاتی، بالاترین اولویت را دارند. این تحلیل به سیاست‌گذاران کمک می‌کند تا با تخصیص بهینه منابع، به‌صورت کارآمدتری با چالش‌های امنیتی مقابله کنند (صالح نیا و همکاران، ۱۳۹۷). صادق زاده (۱۴۰۲) به بررسی نقش رهبر معظم انقلاب اسلامی در تبیین دیپلماسی مقاومت با محوریت دکترین دفاعی می‌پردازد. یافته‌ها نشان می‌دهد که ایشان با به‌کارگیری قدرت هوشمند (ترکیب قدرت نرم و سخت) و با تکیه بر مبانی اسلامی، گفتمان مقاومت را در سطح منطقه‌ای و جهانی گسترش داده‌اند. این دیپلماسی بر پایه‌ی عزت، استقلال، امنیت و نظم نوین منطقه‌ای استوار است و از طریق راهبردهای ارتباطی و نهادی، به تقویت جریان مقاومت و بیداری اسلامی کمک شایانی کرده است. همچنین، این رویکرد به افزایش عمق راهبردی جمهوری اسلامی ایران و تثبیت نقش آن در معادلات بین‌المللی منجر شده است (صادق زاده، ۱۴۰۲).

بررسی ادبیات موجود حاکی از آن است که علی‌رغم رشد قابل‌توجه مطالعات در حوزه تهدیدات ترکیبی، هنوز خلأهایی اساسی در ارائه چارچوبی بومی، یکپارچه و جامع برای مقابله با این نوع تهدیدات، به‌ویژه در زمینه هم‌افزایی راهبردی میان حوزه‌های نظامی، شناختی، اطلاعاتی و رسانه‌ای، وجود دارد. پژوهش حاضر در تلاش است تا با بهره‌گیری هم‌زمان از تجارب جهانی و شرایط بومی جمهوری اسلامی ایران، گامی مؤثر در جهت پاسخ‌گویی به این نیاز علمی و راهبردی بردارد.

روش‌شناسی پژوهش

پژوهش حاضر به لحاظ هدف، در زمره تحقیقات کاربردی-توسعه‌ای قرار می‌گیرد؛ زیرا تلاش دارد ضمن تحلیل مفهومی و راهبردی تهدیدات ترکیبی، راهکارهایی را برای تقویت سازوکارهای دفاعی جمهوری اسلامی ایران در برابر این نوع تهدیدات ارائه دهد. در این راستا، یافته‌های پژوهش نه‌تنها در سطح نظری، بلکه در فرآیند تصمیم‌سازی و بازطراحی سیاست‌ها و راهبردهای دفاعی نیز قابلیت بهره‌برداری دارد. از حیث رویکرد، پژوهش حاضر تحلیلی-تبیینی با بهره‌گیری از روش ترکیبی کیفی-کمّی محسوب می‌شود. از این سو، این پژوهش در دو گام علمی-نظری و تجربی با استفاده از داده‌های آماری ثانویه مورد تحلیل قرار گرفته است:

۱- گام نخست پژوهش شامل تکیه بر منابع علمی و نظری برای شناسایی و تبیین مفاهیم کلیدی مرتبط با تهدیدات ترکیبی، راهبرد دفاعی، بازدارندگی نوین، جنگ شناختی، عملیات چندلایه و امنیت ملی در محیط‌های پیچیده بود. در این راستا، داده‌های اسنادی و کتابخانه‌ای مورد استفاده قرار گرفت که شامل کتاب‌ها و مقالات علمی-پژوهشی داخلی و خارجی، گزارش‌های مؤسسات راهبردی بین‌المللی و اسناد تحلیلی مراکز پژوهشی داخلی است.

۲- گام دوم، با استفاده از داده‌های آماری ثانویه، ابعاد عینی تهدیدات ترکیبی در بستر بومی جمهوری اسلامی ایران مورد تحلیل قرار گرفت. این داده‌ها شامل آمار رسمی منتشرشده توسط مراکز داخلی و همچنین اطلاعات بین‌المللی در حوزه حملات سایبری، تحریم‌های اقتصادی و عملیات رسانه‌ای بود.

در فرآیند تحلیل داده‌ها، از روش تحلیل محتوای کیفی برای دسته‌بندی، تلفیق و تفسیر مفاهیم نظری و از روش تحلیل توصیفی-مقایسه‌ای برای بررسی داده‌های آماری استفاده شد. این رویکرد امکان شناسایی الگوهای تهدید، شباهت‌ها، تفاوت‌ها و شکاف‌های مفهومی و آماری را فراهم ساخته است. افزون بر این، از رویکرد تطبیقی-انتقادی برای تحلیل مدل‌های جهانی پاسخ به تهدیدات ترکیبی (به‌ویژه تجربه‌های روسیه، ناتو و چین) بهره گرفته شد و این تجارب با شرایط بومی جمهوری اسلامی ایران تطبیق داده شد. برای افزایش اعتبار علمی و غنای تحلیلی، پژوهش حاضر از منابع گوناگون با دیدگاه‌های مختلف فکری و رویکردهای متنوع استفاده کرده و از سوگیری نظری یا وابستگی به یک چارچوب خاص پرهیز نموده است. همچنین، به‌منظور انسجام مفهومی و تقویت استدلال‌ها، کلیه مفاهیم کلیدی در بخش مبانی نظری به‌صورت نظام‌مند استخراج و داده‌های آماری در پنج محور اصلی تهدیدات ترکیبی (سایبری، شناختی-رسانه‌ای، نیابتی، اقتصادی و اجتماعی) به‌عنوان شواهد عینی در تحلیل‌ها ادغام شده‌اند.

تجزیه و تحلیل یافته‌ها

شناسایی ابعاد تهدید ترکیبی در زمینه جمهوری اسلامی ایران

در دهه‌های اخیر، تهدیدات ترکیبی علیه جمهوری اسلامی ایران نه‌تنها در سطح نظری قابل‌تحلیل بوده، بلکه شواهد عینی متعددی از بروز همزمان و چندبُعدی این سناریوها به‌طور مستند ثبت شده است. این تهدیدات که عمدتاً توسط کنشگران دولتی و غیردولتی خارجی طراحی و اجرا گردیده‌اند، اهدافی نظیر تضعیف اقتدار ملی، کاهش مشروعیت نظام سیاسی و تحلیل تاب‌آوری اجتماعی-اقتصادی کشور را دنبال کرده‌اند. پژوهش حاضر با رویکردی ترکیبی، ضمن اتکاء به تحلیل کیفی مفهومی، از داده‌های آماری در حوزه‌های سایبری، شناختی-رسانه‌ای، نیابتی، اقتصادی و اجتماعی بهره گرفته است تا تصویری جامع‌تر از ابعاد واقعی تهدیدات ترکیبی علیه جمهوری اسلامی ایران ارائه شود. بر این اساس، ابعاد گوناگون این تهدیدات در قالب پنج محور اصلی مورد واکاوی قرار می‌گیرد. سپس با اتکاء به داده‌های کیفی و کمی، شکاف‌ها و چالش‌های راهبرد دفاعی موجود تحلیل می‌شود و در نهایت، بخش «الزامات بومی برای طراحی پاسخ دفاعی مؤثر» به‌عنوان جمع‌بندی راهبردی ارائه می‌گردد.

۱- تهدیدات سایبری

از جمله بارزترین مصادیق تهدیدات ترکیبی علیه جمهوری اسلامی ایران، حملات سایبری پیشرفته بوده است که با هدف قرار دادن زیرساخت‌های حیاتی کشور، امنیت ملی را با چالش مواجه ساخته‌اند. در این زمینه، حمله سایبری استاکس‌نت (۲۰۱۰) به تأسیسات هسته‌ای نطنز به عنوان یکی از نخستین نمونه‌های جنگ ترکیبی در فضای سایبری در سطح جهانی شناخته می‌شود. بررسی‌های انجام‌شده حاکی از آن است که پس از این رویداد، ده‌ها مورد حمله به سامانه‌های حساس شهری، ترافیکی، مالی، انرژی و صنعتی در جمهوری اسلامی ایران به ثبت رسیده است. این حملات عمدتاً با به‌کارگیری روش‌هایی نظیر فریب سایبری، دستکاری داده‌ها، تخریب هدفمند نرم‌افزارها و جاسوسی سامانه‌ای اجرا شده‌اند. نکته قابل تأمل، هماهنگی زمانی برخی از این حملات با عملیات روانی و رسانه‌ای بوده است که به نظر می‌رسد با هدف تشدید تأثیرات روانی-اجتماعی و ایجاد بی‌ثباتی طراحی شده‌اند. این الگو مؤید آن است که مهاجمان از راهبردهای چندبعدی بهره برده‌اند تا از طریق ترکیب ابزارهای سایبری و روانی، حداکثر کارایی را در تحقق اهداف خود ایجاد نمایند.

به‌طور خاص، داده‌های آماری موجود نشان می‌دهد که حجم و شدت حملات سایبری علیه جمهوری اسلامی ایران طی دهه اخیر روندی افزایشی داشته است. بر اساس گزارش‌های رسمی

و تخصصی منتشرشده نظیر گزارش وضعیت تهدیدات و پدافند سایبری سازمان پدافند غیرعامل کشور (۱۴۰۲)، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (Iran CERT, 2023) طیف وسیعی از حملات در حوزه‌های هسته‌ای، مالی، انرژی، شهری و دولتی ثبت شده است. داده‌های تجمیع‌شده این گزارش‌ها مبنای استخراج اطلاعات جدول (۳) بوده و روند فزاینده تهدیدات سایبری را در بخش‌های مختلف کشور نشان می‌دهد.

جدول (۳) نمونه‌ای از حملات سایبری گزارش‌شده علیه جمهوری اسلامی ایران (سازمان پدافند غیرعامل، ۱۴۰۲: ۱۴) و (Iran CERT, 2023: 8)

بازه زمانی	نوع حمله سایبری	بخش هدف	پیامدها	تعداد حملات
۲۰۱۰	استاکس‌نت	هسته‌ای (نطنز)	تخریب سانتریفیوژها	۱ مورد گسترده
۲۰۱۲–۲۰۱۵	بدافزارهای Flame و Duqu	انرژی و ارتباطات	سرقت داده و اختلال در ارتباطات	+۲۰
۲۰۱۶–۲۰۱۹	حملات DDoS و نفوذ به بانک‌ها	مالی و بانکی	اختلال خدمات الکترونیک بانکی	+۵۰
۲۰۲۰	نفوذ به سامانه‌های توزیع سوخت	حمل‌ونقل و انرژی	اختلال سراسری در پمپ‌بنزین‌ها	۱ حمله ملی
۲۰۲۱–۲۰۲۲	حملات باج‌افزاری و فیشینگ	صنعتی و شهری	توقف فعالیت موقت برخی صنایع و شهرداری‌ها	+۳۰
۲۰۲۳	حملات ترکیبی سایبری-رسانه‌ای	خدمات دولتی و رسانه‌ای	همزمان با اغتشاشات اجتماعی، اختلال در سامانه‌ها	+۱۵

همان‌طور که جدول نشان می‌دهد، الگوی حملات سایبری علیه جمهوری اسلامی ایران هم از نظر تنوع (از ویروس‌های پیچیده تا حملات باج‌افزاری) و هم از نظر شدت و تأثیرگذاری اجتماعی در حال افزایش بوده است. این روند تأکید می‌کند که محور سایبری به یکی از محورهای اصلی تهدید ترکیبی علیه ایران تبدیل شده و نیازمند ارتقای توان دفاعی بومی و چندلایه است.

۲- تهدیدات شناختی و رسانه‌ای

بُعد دوم تهدیدات ترکیبی علیه جمهوری اسلامی ایران به کارگیری ابزارهای جنگ رسانه‌ای، عملیات روانی و جنگ شناختی معطوف بوده است که با هدف دگرگونی ادراکات عمومی، کاهش سرمایه اجتماعی و ایجاد بی‌ثباتی فکری-ارزشی طراحی و اجرا شده‌اند. شواهد تجربی نشان می‌دهد این تهدیدات در قالب سازوکارهای زیر نمود یافته‌اند:

- اجرای کمپین‌های رسانه‌ای هماهنگ در بسترهای مختلف شامل شبکه‌های ماهواره‌ای، پلتفرم‌های رسانه‌های اجتماعی و رسانه‌های بین‌المللی که عمدتاً معطوف به هدف قرار دادن نهادهای حاکمیتی، دستگاه‌های امنیتی و نیروهای مسلح بوده‌اند.
- به کارگیری تاکتیک‌های مهندسی افکار عمومی نظیر هشتگ‌سازی سازمان‌یافته، ترندسازی محتوایی، تولید و انتشار اطلاعات نادرست، ساخت کلیپ‌های تحریک‌کننده عاطفی و ایجاد گسست در نظام ارزشی-هویتی جامعه.
- ساماندهی شبکه‌ای از رسانه‌های فارسی‌زبان برون‌مرزی به منظور هدایت روایت‌های رسانه‌ای در شرایط بحرانی شامل وقایع اعتراضی، تحریم‌های بین‌المللی و چالش‌های اقتصادی-زیست‌محیطی.

تحلیل محتوای این اقدامات نشان می‌دهد که جنگ شناختی علیه جمهوری اسلامی ایران عمدتاً با اهداف زیر دنبال شده است:

- القای احساس ناکارآمدی نظام‌مند در اذهان عمومی
- ایجاد تصور بی‌ثباتی ساختاری
- تحلیل رفتن سرمایه‌های اجتماعی
- تضعیف تدریجی مشروعیت نهادهای ملی

برای روشن‌تر شدن ابعاد کمی این تهدید، داده‌های آماری و گزارش‌های مراکز تخصصی نشان می‌دهد که فعالیت‌های رسانه‌ای و شناختی علیه جمهوری اسلامی ایران طی سال‌های اخیر روندی فزاینده داشته است. این داده‌ها بر اساس گزارش تحلیلی شبکه‌های اجتماعی و عملیات روانی پژوهشگاه فضای مجازی (۱۴۰۲) و گزارش تحلیلی کمپین‌ها و روندهای رسانه‌ای مرکز ملی فضای مجازی (۱۴۰۲) است. نمونه‌ای از داده‌های تجمیع‌شده این گزارش‌ها در جدول (۴) ارائه شده است.

جدول (۴) داده‌های آماری از تهدیدات شناختی و رسانه‌ای علیه جمهوری اسلامی ایران (پژوهشگاه فضای مجازی، ۱۴۰۲: ۹-۱۰) و (مرکز ملی فضای مجازی، ۱۴۰۲: ۱۶)

بازه زمانی	پلتفرم / رسانه	نوع عملیات شناختی	داده آماری گزارش‌شده
۲۰۱۸–۲۰۱۹	ایکس (توییتر)	کمپین‌های هشتگ‌سازی علیه ایران	بیش از ۷.۵ میلیون توییت سازمان‌یافته با موضوع تحریم و اعتراض
۲۰۲۰	رسانه‌های فارسی‌زبان برون‌مرزی	روایت‌سازی همزمان با بحران کرونا	انتشار بیش از ۴۵۰۰ محتوای رسانه‌ای در یک‌ماه اول شیوع
۲۰۲۱	تلگرام	کانال‌های معاند و تحریک‌کننده	۳۲٪ از کل محتوای اعتراضی در تلگرام متعلق به کانال‌های برون‌مرزی
۲۰۲۲	توییتر و اینستاگرام	جنگ شناختی همزمان با اعتراضات	بیش از ۱۲ میلیون توییت اعتراضی، حدود ۴۰٪ منشأ خارجی داشتند
۲۰۲۳	شبکه‌های اجتماعی ترکیبی	انتشار اخبار جعلی و دستکاری افکار	شناسایی بیش از ۵۰۰ کمپین رسانه‌ای سازمان‌یافته

این آمار نشان می‌دهد که عملیات رسانه‌ای و شناختی علیه جمهوری اسلامی ایران نه‌تنها از نظر حجم بلکه از نظر سازمان‌یافتگی و هماهنگی فراملی به‌شدت افزایش یافته است. بنابراین، محور شناختی-رسانه‌ای باید به‌عنوان یکی از مهم‌ترین محورهای تهدید ترکیبی در نظر گرفته شود و تقویت زیرساخت‌های دفاع شناختی ملی یک ضرورت راهبردی است.

۳- تهدیدات نیابتی و امنیتی-میدانی

در سطح عملیاتی، جمهوری اسلامی ایران به کرات با تهدیدات نیابتی در مناطق مرزی و سرزمینی مواجه بوده که عمدتاً به عنوان بخشی از راهبرد ترکیبی کلان‌تر طراحی و اجرا شده‌اند. مهم‌ترین مصادیق این تهدیدات شامل موارد زیر بوده است:

- نفوذ و فعالیت گروه‌های مسلح غیردولتی در مناطق مرزی شرق، غرب و جنوب شرق کشور که با پشتیبانی لجستیکی، اطلاعاتی و تسلیحاتی برخی بازیگران منطقه‌ای همراه بوده است.
- ترورهای هدفمند علیه نخبگان علمی و امنیتی کشور شامل دانشمندان هسته‌ای، کارشناسان اطلاعاتی و فرماندهان نظامی که با بهره‌گیری از روش‌های فنی-روانی پیشرفته به اجرا درآمده‌اند.
- اقدامات خرابکارانه علیه تأسیسات حیاتی و حساس کشور در حوزه‌های صنعتی، هسته‌ای و نظامی که در بسیاری موارد با هماهنگی زمانی با عملیات سایبری و رسانه‌ای همراه بوده‌اند.

به‌منظور تقویت تحلیل کیفی، داده‌های آماری موجود درباره تهدیدات نیابتی و امنیتی-میدانی علیه جمهوری اسلامی ایران مورد استفاده قرار گرفته است. این داده‌ها بر اساس گزارش‌های ستاد کل نیروهای مسلح، سازمان پدافند غیرعامل کشور (۱۴۰۲) و همچنین گزارش مربوط به وضعیت امنیتی خاورمیانه و الگوهای درگیری‌های نیابتی از مرکز مطالعات مطالعه جنگ[1](۲۰۲۳) گردآوری شده است. خلاصه‌ای از این داده‌ها که روند فزاینده فعالیت گروه‌های مسلح، اقدامات خرابکارانه و عملیات نیابتی طی سال‌های اخیر را نشان می‌دهد، در جدول (۵) ارائه شده است.

جدول (۵) داده‌های آماری از تهدیدات نیابتی و امنیتی-میدانی علیه جمهوری اسلامی ایران (سازمان پدافند غیرعامل، ۱۴۰۲: ۱۵) و (ISW, 2023: 6)

بازه زمانی	نوع تهدید نیابتی	منطقه / هدف اصلی	داده آماری گزارش‌شده
۲۰۱۰–۲۰۱۵	درگیری‌های مرزی با گروه‌های مسلح	شرق و غرب کشور	بیش از ۶۰ مورد درگیری مسلحانه مرزی
۲۰۱۰–۲۰۲۰	عملیات ترور علیه نخبگان هسته‌ای	تهران و شهرهای بزرگ	حداقل ۵ دانشمند هسته‌ای ایران ترور شدند
۲۰۱۵–۲۰۱۹	اقدامات خرابکارانه علیه تأسیسات	هسته‌ای و صنعتی	۱۰ مورد حمله یا خرابکاری مستند شده
۲۰۲۰	نفوذ گروه‌های تروریستی	مرزهای جنوب شرق ایران	۱۵ مورد عملیات مرزی (بازداشت یا درگیری مستقیم)
۲۰۲۱–۲۰۲۲	حملات پهپادی و نفوذی	مناطق مرزی غرب و شمال‌غرب	بیش از ۲۰ حمله و اقدام خرابکارانه گزارش شد
۲۰۲۳	عملیات ترکیبی (نفوذ + رسانه‌ای)	مرز غرب کشور	حداقل ۸ مورد عملیات همزمان با کمپین رسانه‌ای

این داده‌های آماری نشان می‌دهد که تهدیدات نیابتی و امنیتی علیه جمهوری اسلامی ایران به‌صورت مستمر و چندلایه در جریان بوده است. ویژگی مهم این تهدیدات آن است که غالباً با سایر ابزارهای جنگ ترکیبی (مانند رسانه‌ای یا سایبری) همزمان شده و اثربخشی آن‌ها افزایش یافته است. بنابراین، ارتقای توان امنیت مرزی، توسعه قابلیت‌های ضدتروریسم، و تقویت سازوکارهای هماهنگی عملیاتی از اولویت‌های اصلی در پاسخ دفاعی به این نوع تهدیدات محسوب می‌شود.

[1] Institute for the Study of War (2023)

۴- تهدیدات اقتصادی-ترکیبی

تهدیدات اقتصادی ترکیبی علیه جمهوری اسلامی ایران در یک دهه اخیر از الگوی پیچیده‌ای تبعیت کرده است که در آن تحریم‌های هوشمند در حوزه‌های بانکی، انرژی و تجاری با ابزارهای جنگ روانی و عملیات اطلاعاتی تلفیق شده‌اند. این رویکرد ترکیبی موجب تشدید اثرگذاری فشارهای اقتصادی از طریق تأثیرگذاری همزمان بر متغیرهای عینی و ذهنی اقتصاد شده است. مهم‌ترین سازوکارهای به کار گرفته شده در این زمینه عبارتند از:

- هماهنگی تحریم‌های اقتصادی با کمپین‌های روانی رسانه‌ای با هدف ایجاد تصور فروپاشی اقتصادی قریب‌الوقوع و تحریک تمایلات نافرمانی مدنی در سطح جامعه
- تولید و انتشار سازمان‌یافته شایعات در مورد بازار کالاهای اساسی، نرخ ارز، بورس و بازار انرژی به منظور ایجاد بی‌ثباتی روانی در فعالان اقتصادی

این الگوی تهاجمی که می‌توان آن را «جنگ اقتصادی-روانی» نامید، نمایانگر چارچوبی راهبردی برای هدف قرار دادن همزمان دو رکن اساسی اقتصاد مقاومتی است:

- **بعد عینی:** تضعیف ساختارهای اقتصادی از طریق محدودیت‌های خارجی
- **بعد ذهنی:** تخریب اعتماد عمومی و سرمایه اجتماعی از طریق عملیات روانی

مطابق با جدول (۶) و بر اساس داده‌های منتشرشده در گزارش اقتصادی و شاخص‌های کلان بانک مرکزی جمهوری اسلامی ایران، یافته‌ها نشان می‌دهد که تهدیدات اقتصادی-ترکیبی با ایجاد چرخه‌ای معیوب میان مشکلات اقتصادی واقعی و ادراکات عمومی، ظرفیت قابل‌توجهی در ایجاد بی‌ثباتی گسترده دارند. همچنین تحلیل‌های اقتصادی تکمیلی ارائه‌شده کشورها توسط نهاد بین‌المللی صندوق بین‌المللی پول[2] (IMF)، نشان می‌دهد که ترکیب فشارهای اقتصادی با عملیات روانی و رسانه‌ای، اثرات تحریم‌ها را تشدید و اعتماد عمومی را هدف قرار می‌دهد. بر این اساس، روشن می‌شود که تهدیدات اقتصادی–ترکیبی علیه ایران نه‌تنها زیرساخت‌های واقعی اقتصاد را تضعیف می‌کنند، بلکه با دستکاری ذهنی، روایت‌سازی رسانه‌ای و تولید شایعات سازمان‌یافته، بر امنیت روانی جامعه نیز تأثیر می‌گذارند. بنابراین، مواجهه مؤثر با این تهدیدات صرفاً از طریق سیاست‌های اقتصادی امکان‌پذیر نیست و مستلزم اتخاذ رویکردی چندبعدی شامل پاسخ‌های اقتصادی، رسانه‌ای و امنیتی در یک چارچوب یکپارچه است.

[2] International Monetary Fund

جدول (۶) داده‌های آماری از تهدیدات اقتصادی-ترکیبی علیه جمهوری اسلامی ایران (بانک مرکزی جمهوری اسلامی ایران، ۱۴۰۲: ۳۸) و (IMF, 2023: 50-52)

بازه زمانی	حوزه اقتصادی هدف	نوع تهدید / عملیات	داده آماری گزارش‌شده
۲۰۱۲–۲۰۱۵	تحریم‌های نفتی	کاهش صادرات نفت	افت صادرات از ۲.۵ میلیون بشکه در روز به کمتر از ۱ میلیون
۲۰۱۸–۲۰۱۹	نرخ ارز	تحریم بانکی + جنگ روانی	سقوط ارزش ریال بیش از ٪۷۰ در سال ۱۳۹۷
۲۰۱۹	تورم کالاهای اساسی	شایعات بازار + تحریم	تورم نقطه‌ای به ٪۴۲ رسید
۲۰۲۰–۲۰۲۱	حوزه بورس	عملیات روانی رسانه‌ای	افت ٪۳۰ شاخص بورس در سه ماهه پاییز ۱۳۹۹
۲۰۲۱–۲۰۲۲	بخش انرژی و سوخت	تحریم + حمله سایبری	کاهش ٪۱۵ ظرفیت صادراتی و اختلال در سامانه سوخت
۲۰۲۳	تورم و معیشت عمومی	جنگ روانی رسانه‌ای	بیش از ۵۰۰۰ شایعه اقتصادی در فضای مجازی مستند شد

۵- تحریک قومیتی، فرهنگی و اجتماعی

این بخش به عنوان یکی از ابعاد مهم تهدیدات ترکیبی علیه امنیت ملی جمهوری اسلامی ایران مورد توجه قرار گرفته است. بررسی‌ها نشان می‌دهد بازیگران معاند با بهره‌گیری از مطالبات قومیتی، جنسیتی، صنفی و ارزشی، درصدد تبدیل نارضایتی‌های ساختاری به ابزاری در خدمت اهداف بیگانه برآمده‌اند. مهم‌ترین سازوکارهای به‌کارگرفته شده در این زمینه عبارتند از:

- تمرکز نظام‌مند رسانه‌های بیگانه فارسی‌زبان بر شکاف‌های قومی و مذهبی با هدف تعمیق گسل‌های اجتماعی
- سرمایه‌گذاری هدفمند بر اعتراضات صنفی و گروهی (شامل اقشار کارگری، فرهنگیان، زنان و اقلیت‌ها) همراه با بزرگ‌نمایی نظام‌مند نارضایتی‌ها
- هماهنگی زمانی تحریکات اجتماعی با عملیات میدانی و رسانه‌ای به منظور خلق بحران‌های ادراکی-عملیاتی

این روند نه تنها موجد تهدیدات اجتماعی است، بلکه در چارچوب راهبرد کلان‌تر جنگ شناختی و هدف‌گیری سرمایه اجتماعی قابل تحلیل است. یافته‌های پژوهشی نشان می‌دهد که اینگونه اقدامات با اهداف تضعیف انسجام اجتماعی، تقویت گسل‌های هویتی، کاهش اعتماد عمومی به نهادهای حاکمیتی و ایجاد بی‌ثباتی ساختاری پیگیری شده‌اند. برای روشن‌سازی ابعاد کمی این الگو، داده‌های آماری استخراج‌شده از گزارش وضعیت امنیت داخلی وزارت کشور

(معاونت امنیتی-انتظامی) و تحلیل‌های دیده‌بان امنیت ملی منتشرشده توسط پژوهشکده مطالعات راهبردی نشان می‌دهد که طی سال‌های اخیر، دامنه و فراوانی تحرکات اجتماعی، صنفی و قومیتی در کشور روندی افزایشی یافته است. جدول (۷) خلاصه این داده‌ها را ارائه می‌کند و بیانگر آن است که بخشی از این تحرکات با انواع عملیات رسانه‌ای، سازماندهی شبکه‌ای و تحریکات بیرونی هم‌زمان بوده‌اند.

جدول (۷) داده‌های آماری از تحریکات قومیتی، فرهنگی و اجتماعی علیه جمهوری اسلامی ایران (پژوهشکده مطالعات راهبردی، ۱۴۰۲: ۲۴-۲۵) و (وزارت کشور (معاونت امنیتی-انتظامی)، ۱۴۰۲: ۱۹)

بازه زمانی	نوع تحریک اجتماعی	نمونه / حوزه هدف	داده آماری گزارش‌شده
۲۰۱۷–۲۰۱۸	اعتراضات صنفی	کارگری و بازنشستگان	بیش از ۲۰۰ تجمع صنفی در سال
۲۰۱۹	اعتراضات سراسری بنزین	اقشار مختلف + تحریک رسانه‌ای	بیش از ۱۰۰ شهر درگیر، صدها تجمع اعتراضی
۲۰۲۰–۲۰۲۱	اعتراضات فرهنگی و صنفی	فرهنگیان و معلمان	بیش از ۱۵۰ تجمع ثبت‌شده
۲۰۲۱–۲۰۲۲	تحریک قومیتی	مناطق غرب و جنوب شرق کشور	حداقل ۳۰ مورد تجمع یا درگیری با رنگ قومیتی
۲۰۲۲	اعتراضات اجتماعی گسترده	زنان و جوانان (بحران اجتماعی)	بیش از ۳۵۰ تجمع اعتراضی ثبت شد
۲۰۲۳	اعتراضات صنفی و اجتماعی	کارگری، بازنشستگی، زنان و اقلیت‌ها	بیش از ۲۵۰ تجمع مستند همراه با پوشش رسانه‌ای خارجی

شواهد حاصل از تحلیل داده‌های آماری حاکی از آن است که تحریکات اجتماعی و قومیتی علیه ایران، که به‌طور فزاینده‌ای در حال سازمان‌یابی هستند، عمدتاً در چارچوب یک راهبرد چندسطحی از سوی بازیگران معاند عملیاتی می‌شوند؛ راهبردی که در آن، این تحریکات به‌صورت سیستماتیک با دیگر ابزارهای جنگ ترکیبی نظیر عملیات رسانه‌ای و سایبری هماهنگ شده‌اند. این پیچیدگی ذاتی، مقابله با این تهدید را به امری صرفاً امنیتی تقلیل نمی‌دهد، بلکه ضرورت یک عکس‌العمل هوشمند و چندبعدی را پررنگ می‌سازد. بنابراین، پاسخ مؤثر نه تنها مستلزم مدیریت امنیتی است، بلکه به‌طور همزمان مستلزم سیاست‌گذاری اجتماعی، فرهنگی و رسانه‌ای هماهنگ است تا از یکسو به مقابله با تحریکات هدفمند پرداخته و از سوی دیگر، به علل ریشه‌ای و نارضایتی‌های واقعی که بستر اینگونه تحریکات را فراهم می‌سازند، بپردازد.

تحلیل شکاف‌ها و چالش‌های راهبرد دفاعی موجود

با توجه به ماهیت پیچیده و چندلایه تهدیدات ترکیبی علیه امنیت ملی جمهوری اسلامی ایران، ضرورت ارزیابی انتقادی ظرفیت‌های دفاعی موجود بیش از پیش احساس می‌شود. ترکیب تحلیل کیفی و داده‌های آماری این پژوهش نشان می‌دهد که در سال‌های اخیر، الگوی تهدیدات ترکیبی

نه‌تنها در سطح نظری بلکه در عرصه عینی نیز به‌طور ملموس بروز یافته است. شواهد آماری حاکی از آن است که بیش از ۲۵۰ حمله سایبری علیه زیرساخت‌های حیاتی کشور در فاصله ۲۰۱۰ تا ۲۰۲۳ رخ داده است؛ افزون بر این، طی ناآرامی‌های اجتماعی سال ۱۴۰۱، بالغ بر ۱۲ میلیون محتوای سازمان‌یافته رسانه‌ای تولید شد که برآوردها نشان می‌دهد حدود ۴۰ درصد آن منشأ خارجی داشته است. همچنین، در یک دهه گذشته حداقل ۵ ترور دانشمندان هسته‌ای و بیش از ۶۰ مورد درگیری مرزی با گروه‌های نیابتی ثبت شده است. در بُعد اقتصادی نیز، تحریم‌ها و جنگ روانی-رسانه‌ای همزمان، موجب افزایش نرخ تورم نقطه‌ای تا ۴۲ درصد و کاهش قابل‌توجه ارزش پول ملی شده است. افزون بر آن، بر اساس گزارش‌های رسمی، در سال ۱۴۰۱ بیش از ۳۵۰ تجمع اعتراضی به وقوع پیوست که بخش قابل‌توجهی از آن‌ها با تحریک رسانه‌ای خارجی همراه بوده است.

تحلیل این شواهد نشان می‌دهد که با وجود دستاوردهای قابل اعتنا در حوزه‌های دفاعی سنتی، ساختار دفاعی کشور در برابر تهدیدات ترکیبی با چندین شکاف بنیادین مواجه است:

- در سطح راهبردی، فقدان یک دکترین جامع مقابله با تهدیدات ترکیبی مشهود است.
- در سطح ساختاری، نبود هماهنگی بین‌نهادی و ضعف در یکپارچگی فرماندهی چنددامنه‌ای مشاهده می‌شود.
- در سطح عملیاتی، محدودیت‌های قابل‌توجهی در ظرفیت واکنش سریع و انعطاف‌پذیر وجود دارد.
- در سطح ادراکی، کاستی‌های جدی در حوزه جنگ شناختی و ضعف در صیانت از سرمایه اجتماعی برجسته است.

بدین‌ترتیب، روشن می‌شود که نظام دفاعی موجود در برابر سناریوهای ترکیبی، که همزمان از ابزارهای سخت (نظامی و سایبری) و نرم (رسانه‌ای و روانی) بهره می‌گیرند، دچار ناکارآمدی نسبی است. بنابراین، ارتقای تاب‌آوری ملی در برابر این تهدیدات مستلزم بازاندیشی در مبانی نظری، بازآرایی ساختارهای نهادی و بازمهندسی راهبردهای عملیاتی است. تدوین یک الگوی بومی و یکپارچه دفاع ترکیبی که به‌طور همزمان به ابعاد سخت و نرم امنیت توجه داشته باشد، ضرورتی راهبردی و اجتناب‌ناپذیر برای آینده امنیت ملی جمهوری اسلامی ایران محسوب می‌شود.

الزامات بومی برای طراحی پاسخ دفاعی مؤثر

تحلیل ابعاد تهدیدات ترکیبی علیه جمهوری اسلامی ایران و ارزیابی ساختار دفاعی موجود و تحلیل داده‌های آماری ثانویه، نشان می‌دهد که مقابله مؤثر با این دسته از تهدیدات نیازمند بازطراحی بنیانی در سطح راهبردی و نهادی است. راهبردهای سنتی که عمدتاً مبتنی بر قدرت نظامی یا امنیت سخت‌اند، قادر به پاسخ‌گویی کامل به ماهیت سیال، غیردیدنی و هم‌زمان تهدیدات ترکیبی نیستند. بر این اساس، الزامات طراحی یک پاسخ دفاعی مؤثر و بومی در برابر تهدیدات ترکیبی به شرح زیر قابل تبیین است:

۱- طراحی ساختار دفاع ترکیبی یکپارچه

مطالعات راهبردی نشان می‌دهد که کارآمدی نظام مقابله با تهدیدات ترکیبی مستلزم ادغام و هماهنگی ظرفیت‌های چندگانه در حوزه‌های نظامی، اطلاعاتی، سایبری، رسانه‌ای، اقتصادی و اجتماعی می‌باشد. مقابله با تهدیدات ترکیبی نیازمند ترکیب ظرفیت‌های نظامی، اطلاعاتی، سایبری، رسانه‌ای، اقتصادی و اجتماعی است. پیشنهاد می‌شود ایجاد یک نهاد مرکزی با قابلیت فرماندهی و کنترل چنددامنه‌ای در سطح ملی در دستور کار قرار گیرد. نهادی که بتواند داده‌های چندمنبعی را تجمیع کند، هشدارهای ترکیبی صادر کند، تصمیم‌سازی راهبردی میان‌بخشی انجام دهد و واکنش سریع، هماهنگ و چندلایه سازماندهی نماید.

۲- تدوین دکترین ملی مقابله با تهدیدات ترکیبی

ایجاد یک چارچوب دکترین رسمی، منسجم و قابل اجرا برای مواجهه با تهدیدات ترکیبی، یکی از پیش‌نیازهای اصلی انسجام دفاعی است. این دکترین باید مبتنی بر شناخت دقیق تهدیدات سایبری، شناختی، رسانه‌ای و اقتصادی، طراحی سناریوهای احتمالی و پاسخ‌های چندلایه، تفکیک وظایف نهادهای مختلف و آموزش و تمرین بر اساس این الگو باشد.

۳- تقویت توان دفاع شناختی و ادراکی جامعه

با توجه به اینکه بخش قابل توجهی از تهدیدات ترکیبی در سطح ذهن و ادراک مردم شکل می‌گیرند، ضروری است سرمایه‌گذاری راهبردی برای ارتقاء سواد رسانه‌ای عمومی، توان تحلیل انتقادی کاربران فضای مجازی، مشروعیت اجتماعی نهادهای رسمی و مقاومت روانی جامعه در برابر عملیات‌های اطلاعاتی-شناختی انجام گیرد. این حوزه باید در سیاست‌گذاری‌های فرهنگی، آموزشی، رسانه‌ای و امنیتی لحاظ شود.

۴- راه‌اندازی سامانه هشدار زودهنگام ترکیبی

یکی از ابزارهای اصلی پاسخ مؤثر، تشخیص سریع تهدیدات ترکیبی در مراحل آغازین است. این امر مستلزم طراحی و استقرار یک سامانه یکپارچه برای پایش فعالیت‌های سایبری مشکوک، موج‌های اطلاعاتی غیرعادی در شبکه‌های اجتماعی، تحرکات نیابتی در مناطق مرزی و تغییرات ناگهانی در شاخص‌های اقتصادی، امنیتی و اجتماعی چنین سامانه‌ای باید به مرکز فرماندهی دفاع ترکیبی متصل باشد تا تصمیم‌گیری‌ها در زمان واقعی انجام شود.

۵- بازطراحی برنامه‌های آموزشی، تمرینی و رسانه‌ای

آمادگی برای تهدیدات ترکیبی تنها با آموزش و تمرین حاصل می‌شود. ضروری است در ساختار رزمایش‌ها، سناریوهای ترکیبی طراحی شود، نهادهای رسانه‌ای، اطلاعاتی، فرهنگی و نظامی رزمایش مشترک انجام دهند و آموزش تخصصی در حوزه جنگ شناختی، فضای سایبر، روایت‌سازی و تحلیل بحران در سطوح راهبردی ارائه شود. همچنین رسانه‌های رسمی کشور باید از حالت انفعالی به کنش‌گری اطلاعاتی پیشگیرانه برسند. مطالعات راهبردی نشان می‌دهد که ارتقای تاب‌آوری ملی در برابر تهدیدات ترکیبی مستلزم بازمهندسی اساسی نظام‌های آموزشی و تمرینی است. در این راستا، الزامات کلان به شرح زیر قابل طرح است:

- **تحول در نظام رزمایش‌های امنیتی:** طراحی سناریوهای چندبعدی که تمامی ابعاد تهدیدات ترکیبی را پوشش دهد، اجرای رزمایش‌های مشترک بین نهادهای نظامی، امنیتی، رسانه‌ای و فرهنگی و شبیه‌سازی شرایط بحران‌های ترکیبی با درنظرگرفتن اثرات زنجیره‌ای
- **توسعه نظام آموزش تخصصی:** تدوین دوره‌های پیشرفته در حوزه‌های جنگ شناختی و عملیات روانی، امنیت سایبری و دفاع دیجیتال، مهندسی روایت و مدیریت بحران و تحلیل راهبردی تهدیدات چندبعدی. همچنین ایجاد مدارس تخصصی مقابله با تهدیدات ترکیبی در سطوح مختلف.
- **تحول نقش رسانه‌های رسمی:** گذار از رویکرد انفعالی به کنشگری فعال در فضای اطلاعاتی، توسعه ظرفیت‌های پیش‌دستانه در روایت‌سازی امنیتی، ایجاد واحدهای ویژه پایش و مقابله با جنگ ترکیبی رسانه‌ای و آموزش نیروهای رسانه‌ای در حوزه امنیت اطلاعاتی و عملیات روانی

الزامات شناسایی‌شده در این بخش، بیانگر آن است که دفاع مؤثر در برابر تهدیدات ترکیبی نه با افزودن سلاح، بلکه با بازسازی تفکر دفاعی در سطح ملی، هماهنگی نهادی، ارتقاء ظرفیت

شناختی جامعه و طراحی پاسخ ترکیبی پیش‌دستانه امکان‌پذیر است. این الزامات، بنیان طراحی سیاست‌های اجرایی، تقنینی، اطلاعاتی و رسانه‌ای آینده کشور در حوزه دفاع ترکیبی را تشکیل می‌دهند.

پاسخ به سؤالات فرعی

۱- ماهیت و ویژگی‌های تهدیدات ترکیبی چیست و چه تمایزاتی با تهدیدات سنتی دارد؟

تهدیدات ترکیبی از طریق ترکیب هم‌زمان ابزارهای نظامی، رسانه‌ای، سایبری، اقتصادی، روانی و فرهنگی، مرز میان جنگ و صلح را برداشته‌اند. این تهدیدات، غالباً با استفاده از بازیگران غیردولتی، عملیات ادراکی، ابزارهای انکارپذیر و فازهای چندلایه طراحی می‌شوند و برخلاف تهدیدات کلاسیک، مستقیماً به نبرد نظامی منجر نمی‌شوند، بلکه در پی فرسایش تدریجی انسجام ملی هستند.

۲- راهبردهای متداول کشورها و نهادهای بین‌المللی در مقابله با تهدیدات ترکیبی کدام‌اند؟

کشورهایی نظیر روسیه، چین و ناتو، در مواجهه با تهدیدات ترکیبی به سمت توسعه ساختارهای فرماندهی مشترک چنددامنه‌ای، تدوین دکترین‌های نوین، تقویت توان سایبری، طراحی رزمایش‌های ترکیبی و تقویت مقاومت شناختی و رسانه‌ای حرکت کرده‌اند. نهادهایی مانند Hybrid CoE و NATO StratCom نیز چارچوب‌های تحلیلی و عملیاتی مشخصی برای مقابله با تهدیدات هیبریدی ارائه داده‌اند.

۳- چه چالش‌ها و شکاف‌هایی در راهبردهای دفاعی جمهوری اسلامی ایران نسبت به تهدیدات ترکیبی وجود دارد؟

مهم‌ترین چالش‌ها عبارت‌اند از: فقدان فرماندهی یکپارچه چنددامنه‌ای، نبود دکترین مصوب مقابله با تهدیدات ترکیبی، پراکندگی نهادی، ضعف در سیستم هشدار زودهنگام، درک سنتی از تهدیدات شناختی، و ناهماهنگی در حوزه‌های آموزش، تمرین و اطلاع‌رسانی. این چالش‌ها موجب کندی واکنش، تضعیف مشروعیت و کاهش تاب‌آوری ملی در برابر عملیات‌های پیچیده دشمن می‌شوند.

۴- چه مؤلفه‌هایی باید در طراحی یک چارچوب بومی برای مقابله با تهدیدات ترکیبی در نظر گرفته شود؟

چارچوب بومی مقابله با تهدید ترکیبی باید شامل موارد زیر باشد:

- ایجاد ساختار فرماندهی و کنترل چنددامنه‌ای در سطح ملی

- تدوین دکترین دفاع ترکیبی منطبق با ظرفیت‌ها و تهدیدات خاص کشور
- تقویت زیرساخت‌های شناختی، رسانه‌ای و سایبری
- طراحی سامانه هشدار زودهنگام چندلایه
- نهادینه‌سازی رزمایش‌ها و آموزش‌های مبتنی بر سناریوهای ترکیبی

نتیجه‌گیری و پیشنهادها

نتیجه‌گیری

پژوهش حاضر با هدف تحلیل ابعاد تهدیدات ترکیبی علیه جمهوری اسلامی ایران و ارزیابی قابلیت‌ها و کاستی‌های ساختار دفاعی موجود، کوشید تا تصویری جامع، داده‌محور و واقع‌گرایانه از الزامات بازآرایی راهبرد دفاعی کشور ارائه دهد. برای دستیابی به این هدف، ابتدا چارچوب نظری مرتبط با تهدیدات ترکیبی تبیین گردید؛ سپس بر پایه ترکیبی از تحلیل محتوای کیفی منابع داخلی و بین‌المللی و نیز استفاده از داده‌های آماری ثانویه، ابعاد عینی این تهدیدات در بستر بومی جمهوری اسلامی ایران شناسایی شد؛ و در نهایت، شکاف‌ها و چالش‌های راهبرد دفاعی کشور مورد واکاوی قرار گرفت.

یافته‌ها نشان می‌دهد که تهدیدات ترکیبی به‌عنوان یکی از پیچیده‌ترین اشکال تهدیدات نوین، دارای ویژگی‌هایی نظیر هم‌زمانی در چند حوزه (سایبری، رسانه‌ای-شناختی، نیابتی، اقتصادی و اجتماعی)، بهره‌گیری از بازیگران غیردولتی، طراحی بر اساس اصل انکارپذیری و اتکاء به جنگ روایت‌ها هستند. بر اساس داده‌های گردآوری‌شده از گزارش‌های رسمی داخلی شامل گزارش‌های سالانه وزارت کشور، مرکز آمار ایران، سازمان پدافند غیرعامل و تحلیل‌های امنیتی منتشرشده در مراکز پژوهشی، در فاصله سال‌های اخیر بیش از ۲۵۰ حمله سایبری علیه زیرساخت‌های حیاتی کشور ثبت شده است؛ بالغ بر ۱۲ میلیون محتوای سازمان‌یافته رسانه‌ای در یک مقطع اعتراضی منتشر گردیده که حدود ۴۰ درصد آن منشأ خارجی داشته است؛ دست‌کم ۵ ترور دانشمندان هسته‌ای و بیش از ۶۰ درگیری مرزی با گروه‌های نیابتی گزارش شده است؛ شاخص تورم نقطه‌ای در اوج فشارهای اقتصادی به ۴۲ درصد رسیده و در سال ۱۴۰۱ بیش از ۳۵۰ تجمع اعتراضی به وقوع پیوسته که بخشی از آن‌ها با تحریک رسانه‌ای خارجی همراه بوده است. این شواهد کمی و کیفی آشکار می‌سازد که تهدیدات ترکیبی علیه ایران واجد ابعاد گسترده و اثرگذاری ملموس بوده‌اند.

در عین حال، بررسی شکاف‌های موجود نشان داد که علی‌رغم دستاوردهای جمهوری اسلامی ایران در حوزه‌های دفاعی سنتی، ساختار دفاعی کشور در مواجهه با تهدیدات ترکیبی با

چالش‌های بنیادینی همچون فقدان دکترین ملی مقابله با تهدیدات ترکیبی، نبود فرماندهی و کنترل یکپارچه چنددامنه‌ای، ضعف در سامانه‌های هشدار زودهنگام و کاستی در حوزه جنگ شناختی و صیانت از سرمایه اجتماعی روبه‌رو است.

بر این اساس، نتایج پژوهش تأکید می‌کند که پاسخ دفاعی مؤثر به تهدیدات ترکیبی نه‌تنها مستلزم ارتقای تجهیزات یا توان نظامی، بلکه پیش و بیش از آن، نیازمند بازتعریف تفکر دفاعی، بازطراحی ساختار نهادی و بازآفرینی انسجام ادراکی-رسانه‌ای در سطح ملی است. این تحقیق با ترکیب تجارب جهانی موفق و تحلیل مختصات بومی جمهوری اسلامی ایران، مجموعه‌ای از مؤلفه‌ها و الزامات را برای طراحی یک چارچوب بومی دفاع ترکیبی یکپارچه ارائه کرده است؛ چارچوبی که می‌تواند به‌عنوان مبنای سیاست‌گذاری دفاعی کشور مورد بهره‌برداری قرار گیرد.

پیشنهادها

پیشنهادهای اجرایی

۱- تدوین دکترین ملی مقابله با تهدیدات ترکیبی از سوی شورای عالی امنیت ملی با مشارکت نهادهای نظامی، اطلاعاتی، رسانه‌ای و علمی (متولی اصلی: شورای عالی امنیت ملی. متولیان مشارکت‌کننده: ستاد کل نیروهای مسلح، وزارت اطلاعات، صداوسیما، وزارت علوم)

۲- ایجاد مرکز فرماندهی و کنترل چنددامنه‌ای در سطح ملی، برای هماهنگی و واکنش سریع به تهدیدات هم‌زمان در حوزه‌های سایبری، رسانه‌ای، شناختی و امنیتی (متولی اصلی: ستاد کل نیروهای مسلح. متولیان مشارکت‌کننده: سازمان پدافند غیرعامل، وزارت اطلاعات، مرکز ملی فضای مجازی)

۳- طراحی و استقرار سامانه هشدار زودهنگام ترکیبی با توان پایش هم‌زمان فضای سایبر، افکار عمومی، مرزها و تحرکات امنیتی (متولی اصلی: سازمان پدافند غیرعامل. متولیان مشارکت‌کننده: مرکز ملی فضای مجازی، نیروی انتظامی فراجا، وزارت ارتباطات)

۴- تدوین استانداردهای آموزشی ملی در حوزه جنگ ترکیبی، جنگ شناختی و امنیت سایبری در وزارت علوم، دانشگاه‌های نیروهای مسلح و مراکز آموزشی رسانه‌ای (متولی اصلی: وزارت علوم. متولیان مشارکت‌کننده: دانشگاه عالی دفاع ملی، دانشگاه امام حسین(ع)، سازمان صداوسیما)

۵- بازطراحی رزمایش‌های دفاعی کشور با سناریوهای ترکیبی و مشارکت هم‌زمان نیروهای نظامی، رسانه‌ای، اطلاعاتی و امنیت نرم (متولی اصلی: ستاد کل نیروهای مسلح. متولیان مشارکت‌کننده: وزارت اطلاعات، سازمان پدافند غیرعامل، صداوسیما)

۶- توسعه و تقویت دیپلماسی ادراکی و مقابله رسانه‌ای برون‌مرزی برای بازیابی روایت رسمی جمهوری اسلامی ایران در فضای منطقه‌ای و جهانی (متولی اصلی: وزارت امور خارجه. متولیان مشارکت‌کننده: صداوسیما (شبکه‌های برون‌مرزی)، سازمان فرهنگ و ارتباطات اسلامی)

پیشنهادهای پژوهشی

۱- طراحی مدل بومی دفاع ترکیبی جمهوری اسلامی ایران با استفاده از متغیرهای فرهنگی، ساختاری، منطقه‌ای و راهبردی خاص کشور.
۲- شبیه‌سازی سناریوهای ترکیبی علیه جمهوری اسلامی ایران (مانند ترکیب حمله سایبری، جنگ روایت، تحریک قومی و فشار اقتصادی) و طراحی پاسخ‌های یکپارچه
۳- پایش و مدل‌سازی تغییرات ادراکی جامعه ایرانی در مواجهه با جنگ شناختی و رسانه‌ای در بحران‌های اخیر (با استفاده از داده‌های شبکه‌های اجتماعی)
۴- تحلیل ساختارهای بازدارندگی شناختی و ادراکی در کشورهای مختلف و امکان تطبیق آن با شرایط جمهوری اسلامی ایران
۵- تدوین الگوی سیاست‌گذاری رسانه‌ای در مواجهه با تهدیدات ترکیبی و بحران‌های مشروعیت
۶- بررسی میزان تاب‌آوری اجتماعی در برابر تهدیدات ترکیبی با روش‌های پیمایشی یا تحلیل کلان‌داده
۷- مطالعه ظرفیت‌های فضای مجازی کشور در دفاع ترکیبی و طراحی معماری سایبری مقاوم
۸- تحلیل حقوقی تهدیدات ترکیبی در سطح بین‌المللی و جایگاه حقوقی جمهوری اسلامی ایران در مقابله با آن‌ها
۹- ارزیابی نقش دانشگاه‌ها و نهادهای علمی در تولید دانش دفاع ترکیبی و طراحی نقشه راه پژوهشی ملی در این حوزه

قدردانی

از دفتر تحقیقات نظری آجا بابت پیگیری‌ها و هماهنگی‌های لازم جهت برگزاری جلسات خبرگی پژوهش حاضر و نیز کلیه اندیشمندان و پژوهشگرانی که در خلال تحقیق خالصانه دیدگاه‌ها و نقطه نظرات علمی و کارشناسی خود را ارائه نمودند، تشکر و قدردانی می‌گردد.

منابع

منابع فارسی

- احتشامی، علی، رادان، احمدرضا و کرم‌زاده، اسماعیل. (۱۴۰۳). تهدیدات آینده امنیت داخلی جمهوری اسلامی ایران. *امنیت ملی*، ۱۴(۵۱)، ۳۳-۵۸.
- ترابی، حسن و احمدی، فاطمه. (۱۴۰۴). تاب‌آوری شناختی در برابر جنگ شناختی علیه ایران: مؤلفه‌ها، تحلیل و راهکارهای ارتقا. *شناخت پژوهی مطالعات سیاسی*، ۲(۱)، ۱۰۱-۱۲۱. doi:10.20241403/CRPS.2504.1040.2.4.5
- حامد، آریان و کریمی، اوژن. (۱۴۰۳). مدل مفهومی هوشمند مداری در فضای سایبری. *فصلنامه مطالعات راهبردی فضای سایبر*، ۲(۴)، ۶۳-۹۶.
- حسینی، محمدرضا و جداری سلامی، محمد. (۱۴۰۰). بررسی آثار تهدیدها و حملات سایبری بر امنیت ملی جمهوری اسلامی ایران. *فصلنامه مطالعات راهبردی فضای سایبر*، ۱(۱)، ۷-۲۸.
- رستمی، علی، پرتوی، محمدتقی و زرین کلاه، حسین. (۱۴۰۰). عوامل امنیتی مؤثر در بروز جنگ ترکیبی توسط گروه‌های تارشگری در غرب آسیا. *فصلنامه مطالعات جنگ*، ۳(۹)، ۹۳-۱۱۷.
- رفیعی راد، جواد، صفوی، سید یحیی، زارعی، سعدالله و بیک، علی اصغر. (۱۳۹۹). بررسی بسترهای امکانی منطقه غرب آسیا در بروز جنگ‌های ترکیبی با تأکید بر نظریه امنیت منطقه‌ای. *امنیت ملی*، ۱۰(۳۸)، ۶۸-۳۵.
- صادق‌زاده، محمدعلی. (۱۴۰۲). نقش مقام معظم رهبری در تبیین دیپلماسی مقاومت با تأکید بر دکترین دفاعی. *فصلنامه علمی مطالعات دفاع مقدس*، ۹(۱)، ۱۵۳-۱۷۷.
- صالح نیا، علی و بختیاری، حسین. (۱۳۹۷). اولویت‌بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیل سلسله مراتبی(AHP). *مطالعات راهبردی سیاستگذاری عمومی*، ۸(۲۷)، ۲۵۵-۲۷۷.
- علیزاده، عظیم. (۱۴۰۰). آینده‌نگاری راهبردی در امنیت داخلی؛ ارائه الگوی دوشاخه تدوین راهبرد. *مطالعات مدیریت راهبردی دفاع ملی*، ۵(۲۰)، ۱۶۳-۱۸۸.
- قاسمی، محمد، آذر، داود و سجادی، وحید. (۱۴۰۱). عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران. *فصلنامه مطالعات جنگ*، ۴(۱۲)، ۱۱۵-۱۴۰.
- گزارش وضعیت تهدیدات و پدافند سایبری پدافند غیرعامل کشور. (۱۴۰۲)، https://pdrc.ir/
- گزارش تحلیلی شبکه‌های اجتماعی و عملیات روانی پژوهشگاه فضای مجازی. (۱۴۰۲)، https://thecsri.ir/
- گزارش تحلیلی کمپین‌ها و روندهای رسانه‌ای مرکز ملی فضای مجازی. (۱۴۰۲)، https://majazi.ir/
- گزارش اقتصادی و شاخص‌های کلان بانک مرکزی. (۱۴۰۲)، https://www.cbi.ir/
- گزارش‌های دیده‌بان امنیت ملی پژوهشکده مطالعات راهبردی. (۱۴۰۲)، https://risstudies.org/

- گزارش وضعیت امنیت داخلی وزارت کشور (معاونت امنیتی - انتظامی). (۱۴۰۲)، https://www.moi.ir/
- مجد، نیما، محجوب عشرت آبادی، حسن، آقایی، محسن و صادقی، هادی. (۱۴۰۳). ارائه مدل مفهومی تدوین خط‌مشی مقابله با جنگ شناختی دشمن در فضای سایبر. *جامعه‌شناسی سیاسی انقلاب اسلامی*، ۵(۳)، ۳۲۳-۳۵۱.

منابع لاتین

- Balomenos, K. (2023). Strategic Communication as a Mean for Countering Hybrid Threats. Handbook for Management of Threats: Security and Defense, *Resilience and Optimal Strategies*, Springer: 371-390. DOI:10.1007/978-3-031-39542-0_18
- Banasik, M. (2016). Unconventional war and warfare in the gray zone. The new spectrum of modern conflicts. J*ournal of Defense Resources Management (JoDRM)*, 7(1): 37-46.
- Bradshaw, S. and P. N. Howard (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation*.
- Brauch, H. G. (2005). *Threats, challenges, vulnerabilities and risks in environmental and human security*, UNU-EHS. DOI:10.1007/978-3-642-17776-7_2
- Buzan, B. (1998). *Security: A New Framework for Analysis*. Lynne Rienner. DOI:10.1515/9781685853808
- Chivvis, C. S. (2017). *Understanding russian "hybrid warfare"*. Rand Corporation 17. DOI:10.7249/ct468
- Freedman, L. (2015). *Strategy: A history*, Oxford University Press. DOI:10.1080/01495933.2015.1069520
- Giles, K. (2016). *Russia's 'new'tools for confronting the West: Continuity and innovation in Moscow's exercise of power*. DOI:10.1515/sirius-2017-0037
- Iran Computer Emergency Response Team (Iran CERT). (2023). *Annual cyber incident reports*. https://cert.ir/
- Institute for the Study of War. (2023). *Middle East security and proxy conflict reports*. ISW. https://www.understandingwar.org/
- International Monetary Fund. (2023). *World Economic Outlook reports*. IMF. https://www.imf.org/
- Lanoszka, A. (2019). Disinformation in international politics. *European journal of international security*, 4(2): 227-248. DOI:10.1017/eis.2019.6
- Mazarr, M. J. (2015). *Mastering the gray zone: understanding a changing era of conflict*. DOI:10.1515/sirius-2017-0042
- Murray, W. and P. R. Mansoor (2012). *Hybrid warfare: fighting complex opponents from the ancient world to the present*, Cambridge University Press. DOI:10.1017/cbo9781139199254
- Rattray, G. J. (2001). *Strategic warfare in cyberspace*, MIT press. DOI:10.7551/mitpress/6483.001.0001

- Rid, T. and B. Buchanan (2015). Attributing cyber-attacks. *Journal of strategic studies*,38(1-2): 4-37. DOI:10.1080/01402390.2014.977382
- Wilner, A. (2014). Contemporary deterrence theory and counterterrorism: A bridge too far. *NYUJ Int'l L. & Pol*. 47: 439.
- Mahnken, T. G., G. Evans, T. Yoshihara, E. S. Edelman and J. Bianchi (2019). *Understanding Strategic Interaction in the Second Nuclear Age*, Center for Strategic and Budgetary Assessments.