Supreme National Defense University Quarterly Journal of Strategic Futures Studies
https://jsfs.sndu.ac.ir E-ISSN: 2980-7816
Vol. 5, No. 1, Issue. 17, Spring 2026 **Received:** 2025/05/28 **Accepted:** 2025/12/31
Research paper

Future Scenarios of Soft and Cognitive Threats and Their Implications and Challenges for the Security of the Islamic Republic of Iran

Majid Mokhtari
Ph.D. Candidate in Middle Eastern Studies, Department of Regional Studies, Allameh Tabataba'i University, Tehran, Iran
Email: majidmokhtari90@yahoo.com

Abstract

Security developments over recent decades indicate that the nature of threats facing states has shifted from predominantly conventional and military patterns toward soft, cognitive, and perceptual forms of threat. In this context, the Islamic Republic of Iran, owing to its geopolitical position, regional and extraregional rivalries, and confrontation with hostile actors, has become increasingly exposed to narrative warfare, cognitive operations, and perceptual pressure. Drawing on a futures studies approach and scenario planning methodology, this study analyzes plausible futures of soft and cognitive threats and their implications and risks for national security, particularly for the functioning of the country's defense institutions. To this end, the study first examines the theoretical foundations of soft threats, cognitive threats, and hybrid warfare, and subsequently identifies and analyzes relevant actors and political–geopolitical, technological, social, and economic drivers. The findings indicate that soft and cognitive threats may generate profound strategic, operational, and social consequences, including the erosion of the accuracy of strategic assessments, disruption of decision-making, decline in defense-related social capital, and an increased likelihood of adversarial miscalculation. Based on these analyses, four overarching scenarios are developed for the next five to ten years, ranging from the escalation of full-scale cognitive warfare to the desirable scenario of "Cognitive Resilience and Active Management." The findings underscore the need to formulate a cognitive defense doctrine and strengthen institutional capacities for the proactive management of such threats.

Keywords: Cognitive Threats; Cognitive Defense; Hybrid Warfare; Narrative Warfare; National Security of the Islamic Republic of Iran

فصلنامه آینده پژوهی راهبردی

سال پنجم، شماره اول (پیاپی ۱۷)، بهار ۱۴۰۵، صص. ۱۳۲-۹۷

تاریخ دریافت: ۱۴۰۴/۰۳/۰۷ ـ تاریخ پذیرش: ۱۴۰۴/۱۰/۱۰

مقاله پژوهشی

سناریوهای آینده تهدیدات نرم و شناختی و پیامدها و چالش‌های آن بر امنیت جمهوری اسلامی ایران

مجید مختاری

دانشجوی دکتری مطالعات خاورمیانه، گروه مطالعات منطقه‌ای، دانشگاه علامه طباطبائی، تهران، ایران

Email: majidmokhtari90@yahoo.com

چکیده

تحولات امنیتی دهه‌های اخیر نشان می‌دهد که ماهیت تهدیدات علیه دولت‌ها از الگوهای سخت و نظامی به‌سوی تهدیدات نرم، شناختی و ادراکی تغییر یافته است. در این میان، جمهوری اسلامی ایران به‌واسطه موقعیت ژئوپلیتیکی، رقابت‌های منطقه‌ای و فرامنطقه‌ای و تقابل با بازیگران متخاصم، به‌طور فزاینده‌ای در معرض جنگ روایت‌ها، عملیات شناختی و فشارهای ادراکی قرار دارد. پژوهش حاضر با بهره‌گیری از رویکرد آینده‌پژوهی و روش سناریونویسی، به تحلیل آینده‌های محتمل تهدیدات نرم و شناختی و پیامدها و مخاطرات آن بر امنیت ملی و به‌ویژه کارکرد نهادهای دفاعی کشور می‌پردازد. در این راستا، ابتدا مبانی نظری تهدید نرم، تهدید شناختی و جنگ ترکیبی تبیین شده و سپس بازیگران مؤثر، پیشران‌های سیاسی-ژئوپلیتیکی، فناورانه، اجتماعی و اقتصادی شناسایی و تحلیل می‌شوند. یافته‌های پژوهش نشان می‌دهد که تهدیدات نرم و شناختی می‌توانند پیامدهای راهبردی، عملیاتی و اجتماعی عمیقی ازجمله تضعیف دقت تحلیل راهبردی، اختلال در تصمیم‌سازی، کاهش سرمایهٔ اجتماعی دفاعی و افزایش احتمال محاسبه غلط دشمن به‌همراه داشته باشند. براساس این تحلیل‌ها، چهار سناریوی کلان برای افق ۵ تا ۱۰ سال آینده ترسیم شده که از تشدید جنگ شناختی تمام‌عیار تا تحقق سناریوی مطلوب «تاب‌آوری شناختی و مدیریت فعال» را در برمی‌گیرد. نتایج پژوهش بر ضرورت تدوین دکترین دفاع شناختی و تقویت ظرفیت‌های نهادی برای مدیریت فعال این نوع تهدیدات تأکید دارد.

کلیدواژه‌ها: تهدیدات شناختی، دفاع شناختی، جنگ ترکیبی، جنگ روایت‌ها، امنیت ملی جمهوری اسلامی ایران.

مقدمه

در عصر حاضر، ماهیت تهدیدات علیه امنیت ملی دولت‌ها دستخوش تحولی بنیادین شده است. مرزهای سنتی جنگ و صلح درهم‌شکسته و میدان نبرد از عرصه‌های فیزیکی و نظامی صرف، به فضاهای پیچیده‌تر ذهن، ادراک و باورهای جوامع گسترش یافته است. این دگرگونی که با انقلاب اطلاعاتی و شبکه‌ای شدن جهان تشدید شده، الگوی نوینی از رویارویی به‌نام «جنگ ترکیبی» را پدید آورده که در آن، عملیات روانی، جنگ روایت‌ها و حملات شناختی، در هماهنگی کامل با فشارهای اقتصادی، سایبری و سیاسی قرار می‌گیرند. در این پارادایم جدید، امنیت ملی دیگر صرفاً تابعی از قدرت سخت و بازدارندگی نظامی نیست، بلکه در گرو تاب‌آوری در برابر هجمه‌هایی است که هدفشان تضعیف اراده، ایجاد تردید، فروپاشی اعتماد عمومی و مختل کردن فرایند تصمیم‌سازی راهبردی است. جمهوری اسلامی ایران به‌دلیل موقعیت ژئوپلیتیک منحصربه‌فرد، نقش راهبردی در منطقه و تقابل ذاتی با پروژه هژمونی غرب و رژیم صهیونیستی، در خط مقدم این نبرد نوین قرار دارد. شناسایی، تحلیل و تدبیر برای مواجهه با این دسته از تهدیدات، نه یک گزینه که یک ضرورت حیاتی برای حفظ تمامیت ارضی، استقلال و نظام سیاسی کشور است.

امنیت جمهوری اسلامی ایران در دهه‌های اخیر با طیف وسیعی از تهدیدات سخت و نرم مواجه بوده است. بااین‌حال، شواهد و تحولات منطقه‌ای و بین‌المللی نشان می‌دهد که تمرکز دشمنان این نظام به‌طور فزاینده‌ای از الگوهای متعارف نظامی به‌سوی تهدیدات نامتعارفی معطوف شده که ماهیتی نرم، شناختی و ادراکی دارند. این تهدیدات که در قالب جنگ روایت‌ها، عملیات روانی پیچیده، دستکاری اطلاعات، تولید و انتشار گسترده محتوای جعلی و هدف قرار دادن ذهنیت نخبگان و توده‌های مردم ظاهر می‌شوند، قادرند بدون درگیری فیزیکی مستقیم، مشروعیت نظام، انسجام ملی، اعتماد عمومی به نهادهای حاکمیتی به‌ویژه نهادهای دفاعی–امنیتی و در نهایت، کارآمدی حکمرانی را مورد هدف قرار دهند. مسئله اصلی این است که با توجه به شتاب تحولات فناورانه (به‌ویژه در حوزه هوش مصنوعی و فضای سایبر)، تشدید رقابت‌های ژئوپلیتیک و افزایش آسیب‌پذیری جوامع شبکه‌ای، آینده تهدیدات نرم و شناختی علیه امنیت جمهوری اسلامی ایران در افق ۵ تا ۱۰ سال آینده چگونه ترسیم می‌شود و این تهدیدات چه

پیامدها و چالش‌های راهبردی، عملیاتی و اجتماعی را برای نهادهای دفاعی و امنیتی کشور ایجاد خواهند کرد؟ عدم تبیین دقیق این آینده‌های محتمل و آماده نبودن برای مواجهه با آن‌ها، می‌تواند منجر به غافل‌گیری راهبردی، کاهش شدید توان بازدارندگی غیرنظامی و افزایش احتمال محاسبات غلط از سوی دشمنان شود.

ضرورت انجام این پژوهش از چند منظر آشکار است: اول، ضرورت راهبردی: درک عمیق از سناریوهای آینده تهدیدات شناختی، پیش‌نیاز تدوین هرگونه دکترین و سند راهبردی دفاعی در دنیای پرآشوب کنونی است. دوم، ضرورت عملیاتی: نهادهای دفاعی و امنیتی کشور برای طراحی سازوکارهای شناسایی، هشدار، مقابله و انعطاف‌پذیری در برابر این تهدیدات، نیازمند نقشه‌ای از آینده‌های پیش‌رو هستند. سوم، ضرورت نظری: ادبیات پژوهشی داخلی در حوزه آینده‌پژوهی تهدیدات نرم و شناختی علیه ایران، علی‌رغم اهمیت موضوع، هنوز جایگاه بایسته خود را نیافته و این تحقیق می‌کوشد به غنای آن بیفزاید. چهارم، ضرورت اجتماعی: با توجه به هدف‌گیری افکار عمومی و سرمایهٔ اجتماعی توسط این تهدیدات، روشن شدن ابعاد خطر برای جامعه و نخبگان، خود بخشی از تاب‌آوری ملی محسوب می‌شود؛ بنابراین هدف کلی این پژوهش، ترسیم آینده‌های محتمل تهدیدات نرم و شناختی علیه امنیت جمهوری اسلامی ایران و تحلیل پیامدهای آن با تأکید بر کارکرد نهادهای دفاعی–امنیتی است.

۱. مبانی نظری پژوهش

تحولات امنیتی چند دهه اخیر باعث شده است که تهدیدات علیه دولت‌ها از قالب سنتی و سخت‌افزاری خارج شود و ابعاد جدیدی به خود بگیرد که عمدتاً غیرفیزیکی، ادراکی، ذهنی و سازمانی هستند. اگرچه مفهوم تهدید نرم در ادبیات سیاسی از دهه ۱۹۹۰ به بعد با آثار جوزف نای درباره قدرت نرم (Nye, 2004) وارد جریان اصلی مطالعات امنیت ملی شد؛ اما در دهه ۲۰۱۰ به بعد، ظهور جنگ‌های ترکیبی، عملیات شناختی، هوش مصنوعی و انقلاب در فضای سایبر سبب شد که تهدیدات نرم و شناختی به جایگاه تهدیدات اصلی و نه فرعی ارتقا یابند. در چنین فضایی، سازمان‌های دفاعی مانند ودجا دیگر تنها با تهدیدهایی مواجه نیستند که ماهیت سخت دارند؛ بلکه هرگونه تغییر در ادراک مدیران، اختلال در روایت‌های دفاعی، تخریب روانی جامعه،

بی‌ثبات‌سازی سازوکارهای مدیریتی و دستکاری اطلاعات نیز می‌تواند نظام دفاعی را به‌طور مستقیم دچار اختلال کند.

تهدیدات نرم، شناختی و سایبری به‌طور پیوسته در تعامل با یکدیگر عمل می‌کنند و دشمنان ایران، به‌ویژه رژیم صهیونیستی، در یک دهه گذشته الگوی رفتاری خود را از جنگ نظامی مستقیم به سمت «درگیری چنددامنه‌ای» تغییر داده‌اند؛ درگیری‌ای که بخش عمده آن بر ادراک، اطلاعات، روایت و تصمیم‌گیری متمرکز است، نه صرفاً عملیات نظامی مستقیم؛ بنابراین، تحلیل ادبیات موضوع برای درک این نوع تهدیدات به‌ویژه برای نهادهایی مانند ودجا اهمیت بنیادین دارد.

۱-۱. تهدید نرم: جنگ روایت‌ها، مشروعیت‌زدایی و فرسایش ذهنی

در تعریف تهدید نرم، اغلب بر عناصر غیرمادی قدرت و تأثیرگذاری بر رفتار و نگرش‌ها بدون استفاده از زور تأکید می‌شود(Nye, 2004)؛ اما در ادبیات امنیتی جدید، تهدید نرم صرفاً به معنای استفاده از ابزارهای فرهنگی یا رسانه‌ای نیست؛ بلکه تهدید نرم به‌عنوان بخشی از جنگ روانی، عملیات اطلاعاتی، جنگ روایت و جنگ ادراکی تعریف می‌شود. این نوع تهدید با هدف تضعیف پایه‌های مشروعیت، اعتماد ملی، انسجام اجتماعی و باور عمومی به توان دفاعی کشور طراحی می‌شود.

مطالعات سیمپسون (Simpson, 2018) درباره جنگ روایت نشان می‌دهد که در دوران جدید، رقابت میان دولت‌ها عمدتاً رقابت بر سر «داستانی» است که درباره جنگ، امنیت، سیاست خارجی و تهدیدات تعریف می‌کنند. اگر دشمن بتواند روایت خود را بر افکار عمومی تحمیل کند، مثلاً این‌که برنامه دفاعی ایران ناکارآمد است، یا توان بازدارندگی ایران مبالغه‌آمیز است. آنگاه حتی بدون شلیک یک گلوله، قدرت دفاعی ایران در ذهن جامعه و حتی در ذهن تصمیم‌گیران تضعیف خواهد شد.

۱-۲. تهدید شناختی: هدف قرار دادن ذهن، ادراک و تصمیم‌سازی

یکی از پیشرفته‌ترین انواع تهدیدهای نوین، تهدید شناختی است؛ تهدیدی که در آن، بازیگر دشمن به‌جای حمله به ساختارهای فیزیکی، ذهن، حافظه، قضاوت و توان تحلیل نخبگان را هدف می‌گیرد(NATO, 2021) . تهدید شناختی دارای سه عنصر اصلی است:

- «دستکاری داده‌ها»[1]
- «اختلال در پردازش ذهنی»[2]
- «ایجاد خطای محاسباتی یا تأخیر در تصمیم‌گیری»[3]

۱-۳. پیوند تهدیدات نرم-شناختی با جنگ ترکیبی

مفهوم جنگ ترکیب بر تعامل میان تهدیدات سخت، نرم، سایبری، اقتصادی و اطلاعاتی تأکید دارد(Qiao & Wang, 1999) . به‌طورکلی جنگ ترکیبی زمانی بیشترین تأثیر را دارد که عملیات سایبری، عملیات روانی، عملیات فریب، تهدیدهای مدیریتی، اقدامات امنیتی و جنگ روایت‌ها به‌صورت هماهنگ عمل کنند.

مطالعات ناتو (NATO, 2021) نشان می‌دهد که جنگ شناختی، نقطه اوج جنگ ترکیبی است؛ زیرا هنگامی که ذهن و روایت طرف مقابل تصرف و به گروگان گرفته شود، دیگر نیازی به عملیات سخت یا نظامی گسترده نیست؛ چراکه طرف مقابل دچار «فلج تصمیم‌گیری» می‌شود.

تمام مبانی نظری ذکرشده به این نتیجه اشاره دارند که جمهوری اسلامی باید تهدیدهای نرم و شناختی را نه یک موضوع جانبی، بلکه بخشی از دکترین اصلی امنیت ملی بداند. چراکه چنین تهدیدهایی قادر است بدون جنگ مستقیم، ظرفیت دفاع ملی را کاهش دهد. ضمن آنکه محیط ژئوپلیتیکی ایران، با توجه به رقابت با بازیگران منطقه‌ای و فرامنطقه‌ای، موجب می‌شود که این کشور به‌صورت دائمی در معرض عملیات روانی، شناختی و مدیریتی باشد. همچنین ادبیات موجود نیز نشان می‌دهد که هر کشوری که تهدیدات نرم و شناختی را نادیده گرفته است، در نهایت در لحظه بحران دچار غافل‌گیری راهبردی شده است(Singer & Brooking, 2018) .

1. Information manipulation
2. Cognitive distortion
3. Decision paralysis

۲. روش‌شناسی پژوهش

این پژوهش مبتنی بر روش سناریونویسی پیش خواهد رفت. سناریونویسی یکی از کلیدی‌ترین روش‌های آینده‌پژوهی و شیوه‌ای برای بهبود تصمیم‌گیری در برابر آینده‌های ممکن و محتمل است. «وندل بل» تعریف کوتاه و مفید آن را چنین بیان می‌کند که سناریوها محصول روش‌های آینده‌پژوهی هستند (پدرام و احمدیان، ۱۳۹٤: ۱۷۵) وی بر این باور است که تمامی روش‌های آینده‌پژوهی مقدمه سناریونویسی هستند و می‌توانند به خلق سناریو منجر شوند. روش سناریو را می‌توان روشی برای خلاصه‌سازی نتایج تلاش‌های آینده‌پژوهی دانست (بل، ۱۳۹۲: ٤٧٤).

اگرچه نگارش سناریو، اصولاً یک شیوه معین ندارد اما به‌صورت عمومی برای تدوین سناریوها، گام‌ها و اصول اولیه نسبتاً مشترکی وجود دارد. این گام‌های اولیه و بنیادین به شرح زیر هستند که با بازخوانی و کمی تغییر در الگوی پدرام و احمدیان (۱۳۹٤) به‌دست‌آمده است؛

۱. انجام تمهیدات اولیه؛ در این ارتباط، باید مسئله اصلی از سوی سازمان تعریف و برای محقق تشریح شود. تمهیداتی اجرایی مانند تهیه فهرست محققان همکار (احتمالی)، تدارک فهرستی از خبرگان احتمالی برای حضور در پنل‌های خبرگی، تهیه تقویم زمانی برای گردآوری داده و تشکیل جلسات خبرگی و دیگر موارد در این مرحله قرار دارند که همگی در فاز صفر این پژوهش نیز به انجام می‌رسد.

۲. شناسایی و تحلیل کنشگران؛ در این گام، محققین باید تمامی بازیگران احتمالی که بر آینده تأثیر خواهند داشت را شناسایی و براساس یک مدل معین تحلیل کنند. باید توجه داشت که در این مرحله، این بازیگران به‌صورت اولیه از سوی محققین شناسایی شده و در جلسه خبرگی نخست معرفی و مرور شدند. سپس تکمیل این مجموعه و تحلیل نهایی با همکاری خبرگان به انجام رسید. در این بخش باید به سؤالات متعددی پاسخ داده شود که برخی از آن‌ها عبارت‌اند از «منابع هر بازیگر»، «نقاط قوت و ضعف بازیگران»، «الگوی رقابت و دوستی با دیگر بازیگران»، «آینده مطلوب هر بازیگر»، «گزینه‌های اقدام در شرایط مختلف».

۳. شناسایی و تحلیل پیشران‌ها؛ در این گام باید نیروهای ایجادکننده تغییرات را شناسایی و دسته‌بندی کرد. این دسته‌بندی می‌تواند براساس موضوع، زمان و یا جهت تأثیرات نسبت به

سازمان انجام شود. بااین‌حال، جامع و متنوع بودن این مجموعه کمک خواهد کرد تا تصویر از آینده به شکلی منسجم‌تر ترسیم شود.

٤. شناسایی و ارزیابی نااطمینانی‌ها؛ در این مرحله باید پرسش‌هایی با این مضمون پرسیده شود که «چه چیزی در ارتباط با پیشران‌ها و وقوع آن‌ها در آینده زمانی مورد نظر، مشخص نیست؟» با این کار، به تعدادی از مواردی دست خواهیم یافت که نسبت به آن‌ها در آینده قطعیت نداریم. درنتیجه، با وقوع هر حالت از آن موضوع، عملاً به سمت یک آینده متفاوت حرکت خواهیم کرد.

۵. تعیین عدم قطعیت‌های کلیدی و طراحی چهارچوب سناریوها؛ در این بخش باید موارد دارای بیشترین میانگین اثرگذاری و عدم قطعیت را از میان فهرست بلند و بالای نااطمینانی‌ها تفکیک کرد. سپس نوبت به مطالعه نوع حالات تداخل و برخورد این نااطمینانی‌ها است.

٦. تدوین سناریوها؛ در این مرحله که شاید مهم‌ترین، طولانی‌ترین و پیچیده‌ترین مرحله در کل سناریوپردازی است، باید روایت داستانی هر سناریو با دقت نوشته شوند. در این راستا، نباید فراموش کرد که گزینه اقدام بازیگران باید براساس تعامل میان پیشران‌ها و نااطمینانی‌ها انتخاب شده و واکنش منطقی هر بازیگر به اقدام کنشگر دیگر نیز مشخص شود.

۷. ارزیابی سناریوها؛ در این گام باید سناریوی مطلوب، مرجح، محتمل و فاجعه تعیین شوند؛ یعنی طیف مقبولیت سناریوها برای مخاطب مشخص شود. طبیعی است که این موضوع برای تکمیل پیشنهادها بوده و مسیر انتقال از وضع موجود در هر یک از سناریوها به سمت شرایط بهتر را مشخص خواهد کرد. برای این مرحله، از حضور خبرگان و یا یک پرسش‌نامه بسیار ساده و محدود استفاده خواهد شد. نباید فراموش کرد که سازمان، مخاطب یا سفارش‌دهنده یک پروژه سناریوپردازی، نقش کلیدی در ارزیابی داشته و امتیاز این فرد در محاسبات نهایی دارای ضریب بالاتری خواهد بود.

۳. یافته‌های پژوهش

۳-۱. بازیگران تهدیدآفرین در حوزه تهدیدات نرم، شناختی و مدیریتی

درک تهدیدات نرم و شناختی بدون شناخت دقیق بازیگرانی که در شکل‌دِهی، هدایت و تقویت این نوع تهدیدها فعال هستند، امکان‌پذیر نیست. برخلاف تهدیدات سخت که از سوی دولت‌ها، ارتش‌ها یا گروه‌های مسلح اعمال می‌شوند، تهدیدات نرم و شناختی از سوی مجموعه‌ای متنوع از کنشگران دولتی، غیردولتی، فناورانه، رسانه‌ای، شبکه‌ای و اجتماعی به‌طور هم‌زمان اعمال می‌شود. همان‌طور که بیان شد بخش مهمی از قدرت این نوع تهدیدها، نه در توان تخریبی فیزیکی، بلکه در توان اثرگذاری بر ادراک، ذهنیت، روایت، تصمیم‌گیری و انسجام مدیریتی نهفته است (Nye, 2004).

در چنین محیطی، نیروهای تهدیدکننده علیه ایران را نمی‌توان به چند دولت یا سازمان محدود کرد؛ بلکه باید آن‌ها را به‌عنوان بخشی از یک «اکوسیستم تهدید» در نظر گرفت؛ اکوسیستمی که بازیگران آن در حوزه‌های رسانه، فناوری، اطلاعات، سیاست، جامعه و دیپلماسی به‌صورت هم‌افزا عمل می‌کنند.

۳-۱-۱. بازیگران فرامنطقه‌ای

ساختار صنعت دفاعی رژِیم صهیونیستی بر پایه ارتباط سازمان‌یافته میان چند رکن بنا شده که دولت، شرکت‌های بزرگ، شرکت‌های متوسط و کوچک، مراکز پژوهشی و زیست‌بوم نوآوری (های‌تک) را به‌صورت شبکه منسجم گرد هم می‌آورد.

❖ ایالات‌متحده آمریکا

ایالات‌متحده مهم‌ترین بازیگر دولتی در حوزه تهدیدات نرم و شناختی علیه ایران محسوب می‌شود. در دهه‌های اخیر، سیاست امنیت ملی آمریکا بر پایه «قدرت هوشمند» شکل گرفته است؛ مفهومی که بر ادغام قدرت سخت (نظامی-اقتصادی) و قدرت نرم (رسانه، فرهنگ، فناوری، روایت) تأکید دارد (Nye, 2009). این رویکرد به آمریکا این امکان را می‌دهد بدون ورود به جنگ مستقیم، از طریق فشار ادراکی، عملیات روانی، جنگ روایت، نفوذ اطلاعاتی و هدایت افکار عمومی بر محیط امنیتی کشورها اثر بگذارد.

شبکه گسترده رسانه‌ای آمریکا، شامل سی‌ان‌ان، صدای آمریکا و ده‌ها رسانه فرعی دیگر، در هماهنگی با شرکت‌های فناوری آمریکایی نظیر گوگل، متا و مایکروسافت، جریان عمده‌ای از اطلاعات جهانی را مدیریت می‌کنند. الگوریتم‌های این شرکت‌ها که در مرکز جریان اطلاعات جهانی قرار دارند، به‌طور مستقیم بر ادراک عمومی و تصمیم‌های نخبگان تأثیر می‌گذارند (Singer & Brooking, 2018).

در حوزه اطلاعاتی، سازمان‌هایی مانند CIA و NSA نقش محوری در جمع‌آوری داده‌ها، تجزیه‌وتحلیل تهدیدها و انجام عملیات روانی و سایبری دارند(Rid & Buchanan, 2015) . هدف اصلی آمریکا از این اقدامات، ایجاد ابهام شناختی، فشار روانی و اختلال تصمیم‌سازی در ایران است.

❖ اتحادیه اروپا

اتحادیه اروپا به‌طور مستقیم وارد مواجهه سخت با ایران نمی‌شود، اما از طریق ابزارهای نرم و روایت‌ساز، می‌تواند بر محیط ادراکی ایران اثرگذار باشد. اروپا دارای شبکه رسانه‌ای منسجم، اندیشکده‌های تأثیرگذار و نهادهای حقوق بشری قدرتمندی است که به‌صورت مداوم در حال تولید روایت‌های معنادار درباره ایران هستند (Simpson, 2018). دیپلماسی روایتی اتحادیه اروپا از طریق گزارش‌ها، بیانیه‌ها، رسانه‌های فراملی و قدرت نمادین فرهنگی، می‌تواند ادراک بین‌المللی و منطقه‌ای نسبت به توان دفاعی و رفتار امنیتی ایران را تحت تأثیر قرار دهد. این تأثیرات، هرچند غیرمستقیم، اما در نهایت بر فضای روانی و مدیریتی نهادهای امنیتی تأثیرگذار است.

۳-۱-۲. بازیگران منطقه‌ای

❖ عربستان سعودی

عربستان سعودی یکی از بازیگران اصلی محیط منطقه‌ای است که از ابزارهای رسانه‌ای و سیاسی برای ساخت روایت‌های امنیتی علیه ایران بهره می‌برد. شبکه‌های رسانه‌ای نزدیک به این کشور، در دهه‌های اخیر به‌صورت هدفمند تصویری از ایران ارائه کرده‌اند که آن را عامل بی‌ثباتی منطقه معرفی می‌کند. چنین سازه‌های روایتی در فضای عربی تأثیر قابل توجهی داشته است و توانسته

است در بلندمدت ذهنیت بخش قابل توجهی از افکار عمومی منطقه را شکل دهد (Al-Rasheed, ۲۰۲۰). این عملیات روانی منطقه‌ای در سطح داخلی ایران نیز فضای ادراکی را پیچیده‌تر می‌کند. هرچه تصویر ایران در محیط پیرامونی آن تضعیف شود، فشار روانی و سیاسی بر نخبگان امنیتی و دفاعی افزایش می‌یابد.

❖ ترکیه

ترکیه بازیگری چندوجهی است؛ ترکیه ترکیبی از قدرت نرم فرهنگی، شبکه رسانه‌ای گسترده، دیپلماسی فعال و سیاست ژئوپلیتیکی تهاجمی را در اختیار دارد. لازم به ذکر است تولیدات رسانه‌ای ترکیه در ایران مخاطب زیاد دارد و همین امر نفوذ فرهنگی و روانی خاصی ایجاد کرده است. این نفوذ در شرایط سیاسی یا امنیتی حساس می‌تواند به‌طور غیرمستقیم بر ادراک عمومی و فضای ذهنی جامعه اثرگذار باشد (Çevik, 2019). افزون بر آن، ترکیه در حوزه قومیتی و جغرافیایی نیز ظرفیت‌های بالقوه‌ای برای اعمال فشار ادراکی دارد که در زمان بحران می‌تواند تقویت شود.

❖ امارات متحده عربی

امارات با در اختیار داشتن ظرفیت‌های قابل‌توجه رسانه‌ای، لابی‌گری جهانی و زیرساخت‌های فناورانه پیشرفته، یکی از فعال‌ترین بازیگران در حوزه جنگ نرم است. این کشور سیاست «برندسازی ژئوپلیتیکی» را دنبال می‌کند و تلاش دارد با تصویرسازی مثبت از خود و منفی از رقبای منطقه‌ای، وزن سیاسی‌اش را در معادلات جهانی افزایش دهد(Ulrichsen, 2017) . در این راستا، امارات از شبکه رسانه‌ای گسترده، شرکت‌های تحلیل داده و ارتباط با پلتفرم‌های فناوری استفاده می‌کند. نقش این کشور در شکل‌دِهی به افکار عمومی منطقه‌ای، اثرات مستقیم بر امنیت روانی و ادراکی جمهوری اسلامی ایران دارد.

❖ رژیم صهیونیستی

رژیم صهیونیستی در سال‌های اخیر به‌عنوان یکی از بازیگران فعال منطقه‌ای، تمرکز ویژه‌ای بر نبرد شناختی و جنگ روانی در تقابل با جمهوری اسلامی ایران داشته است. در این چهارچوب، این رژیم تلاش می‌کند فراتر از تقابل‌های سخت‌افزاری و نظامی، بر لایه‌های ادراکی، ذهنی و

روانی جامعه هدف اثر بگذارد و معادلات قدرت را در سطح افکار عمومی، نخبگان و تصمیم‌سازان دگرگون سازد. استفاده گسترده از رسانه‌های بین‌المللی، عملیات اطلاعاتی، روایت‌سازی هدفمند، بزرگ‌نمایی تهدیدها و القای بی‌ثباتی، ازجمله ابزارهایی است که در این نبرد شناختی به‌کار گرفته می‌شود. از این منظر، جنگ روانی و شناختی به یکی از مؤلفه‌های ثابت راهبرد منطقه‌ای رژیم صهیونیستی تبدیل شده که مکمل سایر ابزارهای سیاسی، امنیتی و دیپلماتیک آن تلقی می‌شود.

۳-۱-۳. بازیگران غیردولتی

❖ شرکت‌های فناوری

شرکت‌های فناوری بزرگ، شاید مهم‌ترین بازیگران تهدیدهای شناختی باشند. این شرکت‌ها مالک پلتفرم‌هایی هستند که میلیاردها کاربر از آن‌ها استفاده می‌کنند و تصمیم‌گیری درباره آنکه چه محتوا دیده شود یا نشود، در اختیار آن‌ها است. الگوریتم‌های هوش مصنوعی در پلتفرم‌هایی مانند گوگل، متا و ایکس حتی ابزارهای هوش مصنوعی مولد، به‌عنوان «دست نامرئی ادراک» عمل می‌کنند (Tufekci, 2015).

❖ رسانه‌های فراملی

رسانه‌های فراملی در شکل‌دهی به تهدیدهای نرم نقشی بی‌بدیل بازی می‌کنند. شبکه‌هایی همچون بی.بی.سی فارس، ایران اینترنشنال و سایر رسانه‌های منطقه‌ای و جهانی، بخشی از جریان خبری ایران را در اختیار دارند. این رسانه‌ها با استفاده از تکنیک‌های حرفه‌ای، روایتی از توان دفاعی یا مدیریت داخلی جمهوری اسلامی ایران ارائه می‌دهند که می‌تواند فضای روانی جامعه و نخبگان را تحت تأثیر قرار دهد(Price, 2002) .

❖ اپوزیسیون برون‌مرزی

گروه‌های مخالف خارج از کشور نیز از بازیگران فعال در جنگ نرم هستند. این گروه‌ها معمولاً از منابع مالی، رسانه‌ای و اطلاعاتی قدرت‌های خارجی بهره‌مند می‌شوند و تلاش دارند با عملیات

روانی، انتشار اطلاعات نامعتبر و ایجاد روایت‌های منفی، اعتماد عمومی به نهادهای دفاعی را تضعیف کنند.(Milani, 2013) .

❖ افکار عمومی شبکه‌ای

جامعه شبکه‌ای یکی از بازیگران مهم تهدیدهای شناختی است. افکار عمومی امروز نه‌تنها مصرف‌کننده پیام، بلکه تولیدکننده پیام نیز هست و این امر محیط ادراکی را بی‌ثبات می‌کند. ویژگی محیط شبکه‌ای سرعت، احساسی بودن، ضعف در تفکیک واقعیت از اطلاعات جعلی و قابلیت موج‌سازی باعث می‌شود هر رویداد کوچک به‌سرعت تبدیل به بحران روانی شود (Pariser, 2011). این امر برای سازمان‌های دفاعی زیان‌بار است، زیرا فشار روانی جامعه به‌سرعت به سطح تصمیم‌گیری منتقل می‌شود و توان تمرکز راهبردی مدیران را کاهش می‌دهد.

۳-۲. پیشران‌های اثرگذار بر تهدیدات نرم، شناختی

تهدیدات نرم محصول رخدادهای لحظه‌ای نیستند، بلکه نتیجه انباشت نیروهای ساختاری، روندهای کلان، تغییرات اجتماعی، تحول فناوری، دگرگونی‌های قدرت و پویایی‌های منطقه‌ای‌اند که به‌تدریج زمینه شکل‌گیری تهدید را فراهم می‌کنند. در نگاه آینده‌پژوهانه، پیشران‌ها نقش «موتورهای تغییر» را ایفا می‌کنند؛ نیروهایی که نه‌تنها ماهیت تهدیدات را شکل می‌دهند، بلکه سرعت، شدت، عمق و دامنه اثرگذاری آن‌ها را نیز تعیین می‌کنند(Bishop & Hines, 2012) .

۳-۲-۱. پیشران‌های سیاسی-ژئوپلیتیکی

یکی از اصلی‌ترین پیشران‌های تهدیدات نرم و شناختی علیه جمهوری اسلامی ایران تغییرات ساختاری در محیط سیاسی-ژئوپلیتیکی جهان است. از سال ۲۰۱۰ به بعد، جهان وارد مرحله‌ای از بی‌ثباتی راهبردی شده است که ویژگی‌های آن عبارت‌اند از رقابت قدرت‌های بزرگ، چندقطبی شدن نظام بین‌الملل، کاهش نقش نهادهای بین‌المللی و رشد بازیگران غیردولتی. این بی‌ثباتی، میدان جنگ روایت‌ها و ذهن‌ها را گسترده‌تر کرده و تهدیدات شناختی را در اولویت قدرت‌های جهانی قرار داده است (Walt, 2018).

رقابت آمریکا و چین، رقابت‌های امنیتی میان جمهوری اسلامی ایران و بازیگران عربی و به‌ویژه عربستان سعودی و امارات و تقابل ایران و رژیم صهیونیستی مهم‌ترین پیشران‌های سیاسی-ژئوپلیتیکی هستند که به‌طور مستقیم بر محیط ادراکی ایران اثر می‌گذارد.

آمریکا برای مهار چین، تلاش می‌کند شبکه‌ای از ائتلاف‌های سیاسی، اقتصادی و رسانه‌ای ایجاد کند و در این چهارچوب، کشورهایی مانند ایران که در مدار چین قرار گرفته‌اند، به‌طور خودکار در معرض عملیات ادراکی و شناختی آمریکا قرار می‌گیرند (Nye, 2009). در سطح منطقه‌ای، رقابت‌های امنیتی میان جمهوری اسلامی ایران و بازیگران عربی و به‌ویژه عربستان سعودی و امارات باعث شده است محیط رسانه‌ای و ادراکی منطقه همواره تحت تأثیر روایت‌های امنیتی قرار گیرد (Al-Rasheed, 2020). رژیم صهیونیستی نیز دارای پیشرفته‌ترین شبکه عملیات روانی، سایبری و اطلاعاتی در منطقه است و سال‌ها تجربه در دست‌کاری ادراکات امنیتی دارد (Singer & Brooking, 2018). این رژیم تلاش می‌کند از طریق تکنیک‌های فریب شناختی، انتشار اطلاعات ساختگی، تحریک افکار عمومی و عملیات پنهان، ذهنیت تصمیم‌گیران در جمهوری اسلامی ایران را تحت فشار بگذارد.

۳-۲-۲. پیشران‌های فناوری-سیاسی

فناوری‌های نوظهور نه‌تنها ابزارهای جدیدی برای عملیات نرم و شناختی در اختیار بازیگران قرار می‌دهند، بلکه ماهیت مواجهه دفاعی را نیز تغییر می‌دهند. فناوری امروز صرفاً یک ابزار جانبی برای تهدید نیست؛ بلکه «محیط اصلی تهدید» است (Tufekci, 2015) . ظهور هوش مصنوعی، ظرفیت عظیم ربات‌های تولید محتوا، قدرت الگوریتم‌ها در شکل‌دِهی به توجه و ادراک، وابستگی شدید دولت‌ها و افکار عمومی به زیرساخت‌های دیجیتال و گسترش فضای سایبری به تمام ابعاد زندگی، سبب شده است که تهدیدات نرم و شناختی نه به‌عنوان تهدید جانبی، بلکه به‌عنوان تهدیدی بنیادی شناخته شوند. این تحول اهمیت فناوری را از سطح تاکتیکی به سطح راهبردی ارتقا داده است.

۳-۲-۳. پیشران‌های فرهنگی-اجتماعی

در دهه اخیر، تحولات اجتماعی در ایران و جهان الگویی ایجاد کرده است که در آن جامعه، رسانه، هویت و شبکه‌های دیجیتال به هم گره خورده‌اند و شکل‌گیری ادراک جمعی تابعی از این هم‌پوشانی پیچیده است. یکی از مهم‌ترین پیشران‌ها، شبکه‌ای شدن جامعه است. با گسترش اینترنت و تلفن همراه هوشمند، افراد نه‌تنها مصرف‌کننده پیام بلکه تولیدکننده فعال آن شده‌اند. این وضعیت باعث شده است که روایت‌ها، اخبار و تحلیل‌ها از مسیرهای بسیار متنوع منتشر شوند و امکان کنترل و مدیریت روایت‌ها بسیار دشوار گردد (Tufekci, 2015) در چنین شرایطی، عملیات روانی یا رسانه‌ای می‌تواند بدون نیاز به یک مرکز فرماندهی، به‌صورت «گله‌ای» یا «خودتکاملی» در جامعه گسترش یابد.

۳-۲-٤. پیشران‌های فرهنگی-اجتماعی

پیشران‌های اقتصادی—مدیریتی یکی از ریشه‌ای‌ترین عوامل شکل‌دهنده تهدیدات نرم و شناختی هستند؛ زیرا اقتصاد نه‌تنها بر زندگی روزمره مردم اثر می‌گذارد، بلکه به‌طور مستقیم بر ادراک امنیت، اعتماد عمومی، پایداری سیاسی و ظرفیت سازمانی تأثیر دارد. اقتصاد، بستر روانی جامعه است و جامعه‌ای که در آن نااطمینانی اقتصادی بالا باشد، نسبت به عملیات روانی و روایت‌های بی‌ثبات کننده آسیب‌پذیرتر است (Akerlof & Shiller, 2009).

ایران طی سال‌های اخیر تحت تأثیر فشارهای ناشی از تحریم، نوسانات ارزی، محدودیت‌های مالی، کاهش درآمدهای نفتی و تغییرات ساختاری اقتصاد جهانی قرار داشته است. این وضعیت، فضای روانی جامعه و مدیران را در حالت نااطمینانی اقتصادی مزمن قرار داده است. در چنین شرایطی، هر موج رسانه‌ای درباره بحران اقتصادی، احتمالاً چند برابر اثر واقعی خود، بر ذهنیت جامعه اثر می‌گذارد. این امر یک پیشران مهم تهدید نرم است، چراکه تهدید نرم نیازمند بستری آماده در سطح افکار عمومی است و بحران اقتصادی دقیقاً چنین بستری را ایجاد می‌کند.

۳-۳. پیامدها و مخاطرات تهدیدات نرم و شناختی

تهدیدات نرم و شناختی صرفاً پدیده‌هایی بیرونی نیستند؛ بلکه اثر نهایی آن‌ها در «کارکرد دفاعی»، «نظام سازمانی»، «تصمیم‌سازی»، «انسجام داخلی» و «تاب‌آوری دفاعی» کشور آشکار می‌شود؛ بنابراین باید نشان داد که تهدیدات نرم و شناختی چگونه به «پیامد» تبدیل می‌شوند. به‌طورکلی پیامدها و مخاطرات تهدیدهای نرم و شناختی چندلایه و پیچیده‌اند؛ چراکه محل اثرگذاری تهدید نرم ذهن، ادراک، سازمان و روایت است نه زیرساخت فیزیکی؛ تهدیدات نرم «پیش‌رونده» هستند؛ یعنی اگر پاسخ داده نشوند، خودبه‌خود تشدید می‌گردند.

۳-۳-۱. پیامدهای راهبردی تهدیدات نرم و شناختی

پیامدهای راهبردی معمولاً دیر بروز می‌کنند؛ اما اثر آن‌ها عمیق، گسترده و بلندمدت است.

❖ تضعیف دقت در تحلیل راهبردی

جنگ شناختی دقیقاً نقطه‌ای را هدف می‌گیرد که زیربنای امنیت ملی است: «تحلیل تهدید». اگر ادراک راهبردی نسبت به تهدیدات خارجی یا ظرفیت‌های داخلی دچار خطا شود، تصمیم‌گیری دفاعی دچار اشتباه می‌شود. به‌عنوان مثال اگر دشمن موفق شود از طریق رسانه‌ها یا عملیات اطلاعاتی توان دشمن واقعی را کم‌تر از حد واقعی جلوه دهد یا برعکس، تهدیدی کوچک را بزرگ جلوه دهد در هر دو حالت، تحلیل‌های راهبردی دچار «انحراف تحلیلی» می‌شوند. این انحراف، خطرناک‌ترین پیامد تهدید نرم است چراکه تصمیم‌سازی دفاعی بر پایه برداشت غلط شکل می‌گیرد.

❖ کاهش انسجام راهبردی و چندپارگی دستگاه دفاعی

تهدیدات نرم اغلب در تلاش‌اند «شکاف» ایجاد کنند: این شکاف می‌تواند بین بخش‌های مختلف سازمان، یا شکاف بین نهادهای دفاعی و نخبگان، یا شکاف میان مردم و تصمیم‌گیران باشد.

❖ انحراف در اولویت‌بندی راهبردی

یکی از ترفندهای تهدیدات نرم این است که تمرکز رهبران دفاعی را از مسائل حیاتی دور کرده و بر موضوعات کم‌اهمیت متمرکز کنند؛ به‌عنوان مثال:

- بزرگ‌نمایی یک بحران کوچک؛
- تحریک افکار عمومی برای اولویت‌های احساسی؛
- برجسته‌سازی موضوعات جانبی و غیرضروری؛
- ایجاد موج‌های رسانه‌ای که مدیران را مجبور به واکنش عجولانه کند.

❖ مختل شدن سازوکار بازدارندگی

بازدارندگی مؤثر نیازمند سه عنصر توان واقعی، نمایش صحیح این توان و ادراک دشمن از قدرت بازدارندگی است. اگر عملیات شناختی بتواند در هر یک از این سه حوزه اختلال ایجاد کند، بازدارندگی لطمه می‌بیند. برای مثال، اگر دشمن تصور کند توان دفاعی ایران ضعیف شده، احتمال ماجراجویی افزایش می‌یابد. همچنین اگر افکار عمومی تصور کند نظام دفاعی ناتوان است، فشار داخلی افزایش می‌یابد؛ و نهایتاً اگر نخبگان به توان خود بی‌اعتماد شوند، بازدارندگی تحلیل می‌رود. این پیامد، یکی از خطرناک‌ترین پیامدهای راهبردی تهدید نرم است.

۳-۳-۲. پیامدهای عملیاتی

تهدیدات نرم و شناختی زمانی خطرناک‌تر می‌شوند که از سطح ادراکی به سطح «عملیاتی» و «سازمانی» منتقل شوند؛ یعنی پدیده‌ای که در ابتدا یک جنگ رسانه‌ای یا شایعه بوده، به تغییر رفتار سازمانی تبدیل شود.

❖ کاهش سرعت واکنش سازمانی

جنگ شناختی در بیشتر مواقع «سرعت» دارد، ولی سازمان‌ها «کند» هستند. وقتی هجمه‌های رسانه‌ای، اطلاعات نادرست و موج‌های ادراکی در جامعه شکل می‌گیرند، سازمان ناگزیر می‌شود نشست‌های متعدد تنظیم پیام برگزار کند؛ لایه‌های مختلف مدیریتی را هماهنگ کند؛ واکنش رسانه‌ای طراحی کند؛ گزارش‌های تحلیلی تهیه کند. درنتیجه این فرایند زمان‌بر است و در همین زمان، تهدید ادراکی اثر خود را گذاشته است؛ بنابراین کاهش سرعت واکنش برابر با افزایش آسیب‌پذیری عملیاتی است.

❖ افزایش بار اطلاعاتی و خستگی تحلیلی

«بار شناختی» یکی از ابزارهای جنگ ادراکی است. دشمن سعی می‌کند حجم عظیمی از داده، تحلیل، خبر، گزارش و روایت متناقض تولید کند تا تحلیل‌گران خسته شوند، دقت تحلیل کاهش یابد، تصمیم‌ها با تأخیر گرفته شود و در نهایت، سازمان دچار حالت «فلج تحلیلی» گردد.

❖ اختلال در نظام گردش اطلاعات

عملیات شناختی معمولاً تلاش می‌کند «سامانه اطلاعاتی» سازمان را دچار آشفتگی کند. این آشفتگی می‌تواند از طریق تزریق اطلاعات نادرست، ایجاد تردید در صحت داده‌ها، انتشار گسترده روایت‌های متضاد و یا ایجاد همهمه اطلاعاتی رخ دهد.

❖ افزایش خطای تصمیم‌گیری

خطاهای تصمیم‌گیری زمانی بیشتر رخ می‌دهند که اطلاعات آلوده باشد، فضای روانی پرتنش باشد، زمان تصمیم محدود باشد، اختلاف داخلی وجود داشته باشد و یا فشار رسانه‌ای و اجتماعی زیاد باشد. تهدید شناختی دقیقاً همین شرایط را ایجاد می‌کند.

۳-۳-۳. پیامدهای اجتماعی و روانی

تهدیدات نرم تنها مدیران را هدف نمی‌گیرند؛ بلکه جامعه هدف مستقیم این تهدیدهاست؛ زیرا ادراک مردم، روایت مسلط در جامعه و احساس امنیت یا ناامنی عمومی، بر کارکرد دفاعی امنیتی اثر مستقیم دارد.

❖ کاهش سرمایهٔ اجتماعی دفاعی

به‌طورکلی سرمایهٔ اجتماعی دفاعی یعنی اعتماد عمومی به سازمان دفاعی، احترام جامعه به حوزه نظامی، باور مردم به توان دفاعی کشور، همراهی اجتماعی با سیاست‌های دفاعی و آمادگی جامعه برای همکاری در زمان بحران. تهدیدات نرم معمولاً تلاش می‌کنند این سرمایه را تحلیل برند. در این حالت روایت دشمن تقویت می‌شود، مقاومت روانی جامعه در برابر جنگ روایت کاهش می‌یابد، دفاع ملی «تنها» می‌شود و فشار روانی دفاعی افزایش می‌یابد.

❖ تحریک نارضایتی اجتماعی و ایجاد موج‌های روانی

عملیات نرم می‌تواند کوچک‌ترین مشکل اجتماعی یا اقتصادی را به «بحران ملی» تبدیل کند. نمونه‌هایی از پیامد روانی عبارت‌اند از: ایجاد ترس گسترده از ناامنی، حتی بدون وجود تهدید واقعی، ایجاد اضطراب جمعی درباره آینده، تبدیل نارضایتی اقتصادی به بدبینی امنیتی، گسترش حس ناکارآمدی سامانه و نهایتاً شکل‌گیری موج‌های هیجانی کوتاه‌مدت که تصمیم سیاسی را تحت تأثیر قرار می‌دهد. این موج‌های روانی می‌توانند در مدت کوتاهی ظرفیت مدیریت بحران را مختل کنند.

❖ ایجاد شکاف میان مردم و نهادهای دفاعی

جنگ نرم معمولاً روایت‌هایی ساختگی ایجاد می‌کند مانند این‌که نهادهای دفاعی هزینه‌زا هستند، تصمیمات دفاعی اشتباه بوده، نظام دفاعی مردم‌محور نیست و تهدید خارجی واقعی نیست و تهدید از داخلی است. این روایت‌ها در جامعه «شکاف ادراکی» ایجاد می‌کنند؛ که نتایج این شکاف ۱. کاهش حمایت اجتماعی از برنامه‌های دفاعی؛ ۲. افزایش فشار روانی بر مدیران؛ ۳. کاهش اعتماد عمومی به سیاست‌های کلان و ٤. دشوار شدن بسیج اجتماعی در زمان بحران هستند.

❖ شکل‌گیری بحران‌های هویتی و رسانه‌ای

روندهای رسانه‌ای جهانی و عملیات نرم می‌توانند بحران‌های هویتی ایجاد کنند که تضاد میان هویت ملی و هویت جهانی، دوگانه‌سازی میان نسل‌ها، القای سرخوردگی نسبت به آینده کشور، ایجاد حس بی‌معنایی جمعی و تضعیف هویت دفاعی جامعه از این قبیل هستند. این بحران‌های هویتی، سازمان دفاعی را با «بی‌هنجاری فرهنگی» مواجه می‌کنند، چراکه جامعه به روایت‌های دفاعی پاسخ مناسب نمی‌دهد.

❖ افزایش حساسیت و واکنش‌پذیری جامعه

در روان‌شناسی امنیت ملی، جامعه‌ای که در معرض فشارهای ادراکی باشد، «واکنش‌پذیر» می‌شود؛ یعنی ۱. سریع‌تر دچار هیجان می‌شود؛ ۲. سریع‌تر دچار ناامیدی می‌شود؛ ۳. به‌سرعت از یک روایت به روایت دیگر می‌پرد و ٤. مقاومت روانی پایینی دارد. درنتیجه این واکنش‌پذیری، کارکرد

دفاعی دشوار می‌شود زیرا سیاست‌گذار ممکن است ناگزیر شود تصمیم‌های خود را تحت فشار احساسی اتخاذ کند.

۳-۳-٤. مخاطرات امنیت ملی ناشی از تهدیدات نرم و شناختی

در سطح کلان، تهدیدات نرم می‌توانند به بحران امنیت ملی تبدیل شوند. در این بخش، مهم‌ترین مخاطراتی را که مستقیماً کارکرد سازمانی چون ودجا را تهدید می‌کنند، بررسی می‌شود.

❖ افزایش احتمال محاسبه غلط دشمن

وقتی دشمن تصور کند ایران دچار اختلاف داخلی شده، ناتوان از مدیریت بحران است، یا دچار بی‌ثباتی اجتماعی شده، احتمال اقدام نظامی یا فشار شدیدتر افزایش می‌یابد. این خطر در متون امنیتی به‌عنوان «محاسبه غلط ناشی از جنگ روایت» شناخته می‌شود(Walt, 2018) . محاسبه غلط، زمینه‌ساز درگیری‌های ناخواسته می‌شود.

❖ تضعیف انسجام ملی در زمان بحران

در زمان بحران امنیتی، کشور نیازمند وحدت، آرامش روانی، اعتماد عمومی و انسجام اطلاعاتی است. تهدیدات نرم هر چهار عنصر را تضعیف می‌کنند و بنابراین اگر در زمان بحران، جامعه دچار ترس، شکاف، اطلاعات جعلی و بی‌اعتمادی باشد، کارکرد دفاعی کاهش می‌یابد و اثرگذاری تصمیم‌سازی دفاعی محدود می‌شود.

❖ از کار افتادن مکانیسم‌های بازدارندگی روانی

امنیت ملی فقط به بازدارندگی نظامی وابسته نیست؛ بخش مهمی از آن «بازدارندگی روانی» است؛ یعنی جامعه نسبت به تهدید خارجی احساس قدرت و ثبات داشته باشد. به بیان دیگر اگر عملیات شناختی بتواند تصویر ضعف در نظام دفاعی بسازد، موفقیت‌های دفاعی را بی‌اعتبار کند، یا اعتمادبه‌نفس ملی را کاهش دهد، بازدارندگی روانی فرو می‌ریزد.

❖ افزایش آسیب‌پذیری در برابر جنگ ترکیبی

تهدیدات نرم در صورتی خطرناک‌تر می‌شوند که با تهدیدات اقتصادی، سایبری یا منطقه‌ای ترکیب شوند. این وضعیت، «جنگ ترکیبی» را فعال می‌کند و توان دفاعی را فرسوده می‌کند.

❖ فرصت‌سازی برای نفوذ اطلاعاتی

اگر فضای شناختی کشور آشفته باشد نفوذ عوامل خارجی آسان‌تر می‌شود، اعتماد مردم کاهش می‌یابد، اطلاعات نادرست راحت‌تر پنهان می‌شود و فضا برای عملیات سایبری گسترده‌تر می‌شود که این مخاطره، ممکن است تهدید مستقیم برای ودجا محسوب شود.

۳-٤. سناریوهای آینده تهدیدات نرم، شناختی و مدیریتی علیه ودجا

در این بخش، با استفاده از بازیگران و پیشران‌های شناسایی‌شده، چهار سناریوی کلان برای ۵ تا ۱۰ سال آینده ارائه می‌شود. هر سناریو براساس منطق ماهیت تهدید، بازیگران اصلی، سازوکار عملیات، اثر بر نظام تصمیم‌سازی، اثر بر جامعه، نقاط قوت و ضعف جمهوری اسلامی ایران، پیامدها و نشانه‌های هشدار اولیه تحلیل می‌شوند.

۳-٤-۱. سناریوی اول: تشدید جنگ شناختی تمام‌عیار

این سناریو محتمل‌ترین سناریو برای ۵ سال آینده است، زیرا روندهای جهانی – به‌ویژه پیشرفت هوش مصنوعی، پیچیده‌تر شدن جنگ رسانه‌ای، تشدید رقابت ژئوپلیتیکی و افزایش وابستگی به پلتفرم‌های خارجی – به سمت گسترش جنگ شناختی حرکت می‌کنند (Singer & Brooking, 2018).

❖ ماهیت سناریو

در این سناریو، ایران وارد مرحله‌ای می‌شود که «جنگ شناختی» نه صرفاً عملیات رسانه‌ای، بلکه نبردی چندلایه تمام‌عیار است. بدین معنا که:

- هر رویداد کوچک تبدیل به بحران ادراکی می‌شود؛
- حجم اطلاعات جعلی چند برابر امروز می‌شود؛
- حملات سایبری با حملات شناختی ادغام می‌شود؛
- رسانه‌های خارجی فعالیت خود را چند برابر می‌کنند؛
- شرکت‌های فناوری غربی سیاست‌های محدودکننده‌تری اعمال می‌کنند؛
- فضای اجتماعی ایران در معرض موج‌های هیجانی مستمر قرار می‌گیرد.

این وضعیت مشابه چیزی است که مؤسسه رند از آن با عنوان جنگ شناختی تمام‌عیار یاد می‌کند(Rid & Buchanan, 2015) .

❖ بازیگران سناریو

- ایالات‌متحده و شبکه هوش مصنوعی دفاعی آن؛
- رژیم صهیونیستی؛
- عربستان و امارات (در لایه رسانه‌ای و تبلیغاتی)؛
- شرکت‌های بزرگ فناوری غربی؛
- شبکه اپوزیسیون برون‌مرزی؛
- گروه‌های سایبری وابسته.
- این ترکیب بازیگران، «زیست‌بوم جنگ شناختی» را تشکیل می‌دهد.

❖ سازوکار عملیات

در این سناریو عملیات از سه مسیر دنبال می‌شود:

الف. حملات شناختی هوشمند

به‌طوری‌که هوش مصنوعی الگوهای رفتاری جامعه را شناسایی می‌کند، پیام‌ها را شخصی‌سازی می‌کند، روایت‌های ضد جمهوری اسلامی ایران تولید می‌کند و محتوای جعلی طبیعی‌نما می‌سازد. این حملات می‌توانند بسیار مؤثر باشند زیرا انسان قادر به تشخیص اصالت آن‌ها نیست (Tufekci, 2015).

ب. حملات سایبری و شناختی ترکیبی

ابتدا زیرساخت یا وبگاه‌ها هدف حمله سایبری قرار می‌گیرند، سپس بلافاصله موج رسانه‌ای آغاز می‌شود.

ج. حملات ادراکی از مسیر بحران‌های اجتماعی–اقتصادی

دشمن از هر بحران داخلی ولو کوچک برای ساخت بحران ادراکی بزرگ استفاده می‌کند (Akerlof & Shiller, 2009).

❖ پیامدهای احتمالی برای ودجا

- کاهش دقت تحلیل راهبردی؛
- افزایش خطای تصمیم‌گیری؛
- از دست رفتن کنترل روایت در جامعه؛
- تضعیف بازدارندگی روانی؛
- افزایش احتمال محاسبه غلط دشمن.
- این سناریو، می‌تواند کشور را وارد وضعیت «دفاع شناختی فرسایشی» کند.

❖ نشانه‌های هشدار

- افزایش حجم اخبار جعلی سیاسی؛
- گسترش روایت‌های هم‌زمان در چند رسانه خارجی؛
- جهش ناگهانی فعالیت ربات‌های شبکه اجتماعی؛
- هم‌زمانی حملات سایبری و رسانه‌ای؛
- افزایش ترندسازی ساختگی در شبکه‌های اجتماعی.

۳-٤-۲. سناریوی دوم: فرسایش ادراکی و بحران اعتماد عمومی

در این سناریو، تهدیدات نرم نه به‌صورت حملات شدید، بلکه به‌صورت فرسایش تدریجی اعتماد عمومی عمل می‌کنند. این سناریو خطرناک است زیرا «آرام، خاموش و انباشتی» است.

❖ ماهیت سناریو

این سناریو زمانی شکل می‌گیرد که:

- عملیات شناختی مستمر اما کم‌شدت باشد؛
- رسانه‌های خارجی روایت‌های بی‌وقفه ضد جمهوری اسلامی ایران تولید کنند؛
- نارضایتی اقتصادی و اجتماعی ادامه‌دار باشد؛
- افکار عمومی به‌مرور دچار بی‌اعتمادی شود.

شایان ذکر است این «فرسایش تدریجی»، طی سال‌ها قابلیت دفاع ادراکی را تضعیف می‌کند.

❖ بازیگران سناریو

- رسانه‌های فراملی؛
- اپوزیسیون خارج از کشور؛
- پلتفرم‌های اجتماعی؛
- محافل تبلیغاتی خارجی.

بازیگران دولتی نقش پررنگی ندارند؛ بلکه بازیگران رسانه‌ای و اجتماعی محور هستند

❖ سازوکار عملیات

- روایت‌سازی آرام و مداوم؛
- برجسته‌سازی ضعف‌های کوچک؛
- تولید ناامیدی و بی‌اعتمادی؛
- القای ناکارآمدی سیستمی؛
- دوگانه‌سازی میان مردم و نهادهای دفاعی؛
- ایجاد حس تضعیف تدریجی توان دفاعی.

ازآنجایی‌که این نوع حملات هیچ «لحظه حمله» مشخصی ندارد و تهدید به‌صورت خزنده پیش می‌رود، بسیار خطرناک هستند (Sunstein, 2017).

❖ پیامدهای احتمالی

- کاهش حمایت اجتماعی از برنامه‌های دفاعی؛
- بی‌تفاوتی جامعه نسبت به تهدید خارجی؛
- کاهش سرمایهٔ اجتماعی دفاعی؛
- افزایش فشار روانی بر مدیریت دفاعی؛
- تضعیف نشاط سازمانی؛
- افزایش بدبینی داخلی میان واحدها؛
- کاهش جذابیت استخدامی در حوزه دفاع.

در این سناریو، کشور نه با «حمله»، بلکه با «تحلیل رفتن تدریجی» مواجه است.

❖ نشانه‌های هشدار

- جذاب شدن روایت‌های منفی درباره نظام دفاعی؛
- ترندسازی آرام، اما پیوسته علیه نهادهای دفاعی؛
- کاهش مشارکت اجتماعی در پروژه‌های ملی؛
- افزایش شایعات درباره ناکارآمدی دفاعی؛
- دوگانه‌سازی رسانه‌ای «مردم–دفاع».

۳-٤-۳. سناریوی سوم: جنگ ترکیبی چندساحتی

این سناریو، خطرناک‌ترین و پیچیده‌ترین سناریوی ممکن است، زیرا ترکیبی از تهدید سخت + تهدید نرم + تهدید سایبری + فشار اقتصادی + جنگ ادراکی است. در این سناریو، دشمنان ایران به‌صورت هم‌زمان از چند جبهه حمله می‌کنند تا ساختار دفاعی، صنعتی، اطلاعاتی و روانی کشور را درگیر بحران چندلایه کنند.

این همان چیزی است که در ادبیات امنیتی «جنگ ترکیبی» نامیده می‌شود (Rid & Buchanan, 2015)؛ اما در این سناریو، تمرکز اصلی بر جنگ شناختی ترکیبی است، یعنی جایی که هر تهدید سخت با یک عملیات ادراکی همراه است تا اثر تخریبی آن بیشتر شود.

❖ ماهیت سناریو

در این سناریو، دشمن به‌صورت هم‌زمان حملاتی در حوزه‌های زیر انجام می‌دهد:

- حملات سایبری تخریب‌گر و نفوذی؛
- عملیات رسانه‌ای شدید و لحظه‌ای؛
- تحریک اجتماعی و اقتصادی داخلی؛
- افزایش تحرکات منطقه‌ای و نظامی؛
- اعمال فشارهای سیاسی و حقوقی در سطح بین‌الملل؛
- جنگ روایت‌ها علیه توان دفاعی ایران.

نکته کلیدی این سناریو آن است که همه این حملات به‌طور مستقل نیستند؛ بلکه با هم هماهنگ و مکمل‌اند.

برای مثال:

- یک حمله سایبری: هم‌زمان یک موج رسانه‌ای ایجاد می‌شود.
- یک تنش مرزی: هم‌زمان تحلیل‌های ساختگی درباره ضعف دفاعی منتشر می‌شود.
- یک بحران اقتصادی: هم‌زمان ادراک ضعف مدیریتی تقویت می‌شود.

این سناریو ایران را وارد وضعیت «چندبحرانی» می‌کند.

❖ بازیگران سناریو

- ایالات‌متحده (میدان سایبری و رسانه‌ای)؛
- رژیم صهیونیستی (میدان سایبری و جنگ روانی)؛
- عربستان و امارات (جنگ تبلیغاتی منطقه‌ای)؛
- شبکه‌های امنیتی غرب؛
- شرکت‌های فناوری غربی؛
- سازمان‌های بین‌المللی با رویکرد سیاسی؛
- رسانه‌های جهانی؛
- اپوزیسیون برون‌مرزی هم‌سو با سرویس‌های خارجی.

در این سناریو، ایران عملاً با یک شبکه تهدید مواجه است؛ نه یک بازیگر منفرد.

❖ سازوکار عملیات در جنگ ترکیبی

الف. سوءاستفاده از بحران‌های داخلی

دشمن تلاش می‌کند هر بحران داخلی را به یک «دال مرکزی» در جنگ روایت تبدیل کند. مثلاً:

- بحران ارزی: «بی‌ثباتی دفاعی»؛
- حادثه اجتماعی: «بی‌اعتمادی گسترده»؛
- تغییر مدیریتی: «اختلاف در نهادهای دفاعی»؛
- حادثه صنعتی: «ناتوانی دفاعی»

این تکنیک براساس نظریه «سواری بر موج بحران» است (Akerlof & Shiller, 2009).

ب. عملیات سایبری و اطلاعاتی متوالی

حملات سایبری در این سناریو نقش اصلی دارند:

- هدف‌گیری زیرساخت‌های صنعتی دفاعی؛
- نفوذ به سامانه‌های اطلاعاتی؛
- دست‌کاری داده‌ها؛
- افشای کنترل‌شده اطلاعات؛
- ایجاد اختلال در ارتباطات حساس.

ج. ترکیب جنگ روایتی با عملیات روانی

در جنگ ترکیبی، روایت‌ها هم‌زمان در چند حوزه القا می‌شوند:

- ایران منزوی است؛
- توان دفاعی ایران فرسوده شده است؛
- مدیریت دفاعی ناتوان است؛
- جامعه علیه سیاست‌های امنیتی است؛
- وحدت دفاعی از بین رفته است.

لازم به ذکر است این روایت‌ها با شواهد ساختگی تقویت می‌شوند (Price, 2002).

د. فعال‌سازی شبکه‌های اجتماعی برای ایجاد موج‌های هیجانی

- در این سناریو، شبکه‌های اجتماعی اصلی‌ترین ابزار دشمن هستند.
- در این شبکه‌ها ربات‌ها، صفحات هدایت‌شده، ترندهای ساختگی، هشتگ‌های هماهنگ و محتوای احساسی سریع برای ایجاد «موج‌های ادراکی» استفاده می‌شوند.

❖ پیامدهای احتمالی

پیامدهای این سناریو بسیار عمیق و خطرناک هستند:

- کاهش توان تحلیل ستادی؛
- سقوط سرعت تصمیم‌گیری دفاعی؛
- آشفتگی گسترده اطلاعاتی؛

- بی‌ثباتی مدیریتی؛
- کاهش اعتماد عمومی به نهاد دفاع؛
- انشقاق میان واحدهای مختلف؛
- افزایش احتمال خطای راهبردی؛
- آسیب‌دیدن زیرساخت‌های صنعتی دفاعی؛
- تضعیف بازدارندگی ملی؛
- افزایش احتمال رویارویی ناخواسته در منطقه.

این سناریو از میان تمام سناریوها بیشترین «ضرر بالقوه» را دارد.

❖ نشانه‌های هشدار

- جهش ناگهانی حملات سایبری پیشرفته؛
- افزایش حملات روایت‌محور در رسانه‌های جهانی؛
- تغییرات هماهنگ در الگوریتم پلتفرم‌های غربی؛
- شایعات بزرگ و بدون منبع؛
- تمرکز شدید رسانه‌های خارجی بر توان دفاعی ایران؛
- حملات سایبری هم‌زمان با حملات رسانه‌ای؛
- افزایش فعالیت شبکه‌های اپوزیسیون.

۳-٤-٤. سناریوی چهارم: تاب‌آوری شناختی و مدیریت فعال

این سناریو تصویر آینده‌ای است که در آن نهادهای دفاعی ایران موفق می‌شوند و به‌عنوان سناریوی مطلوب و بهترین مسیر آینده برای ودجا در نظر گرفته می‌شود.

- تهدیدات نرم را بشناسند؛
- آن‌ها را مدیریت کنند؛
- سامانه دفاع شناختی بسازند؛
- ثبات ادراکی ایجاد کنند؛
- و آسیب‌پذیری سازمانی را کاهش دهند.

این سناریو بهترین گزینه برای آینده و همان «سناریوی هدف» است.

❖ ماهیت سناریو

در این سناریو، ایران به مرحله‌ای می‌رسد که:

- تهدیدات نرم را نه‌تنها دفع می‌کند، بلکه از آن‌ها فرصت می‌سازد؛
- درک دقیقی از عملیات شناختی دارد؛
- از فناوری برای حفاظت ذهنی استفاده می‌کند؛
- روایت‌های دفاعی را با قدرت و جذابیت تولید می‌کند؛
- جامعه نسبت به جنگ نرم واکسینه می‌شود (Sunstein, 2017).

درواقع، این سناریو مرحله‌ای است که در آن «دفاع شناختی» به یک دکترین رسمی تبدیل می‌شود.

❖ مؤلفه‌های کلیدی این سناریو

۱. ایجاد دکترین دفاع شناختی: این دکترین دربرگیرنده اصول جنگ شناختی، روش‌های مقابله، نظام هشدار زودهنگام، پروتکل‌های تحلیلی، سامانه‌های شناسایی محتوای جعلی و آموزش مدیران به تفکر نقادانه است(Kahneman, 2011) .

۲. ساخت سامانه هشدار زودهنگام ادراکی: این سامانه قادر است ۱. تحلیل کند چه موجی در شبکه‌ها شکل گرفته است؛ ۲. منشأ آن را شناسایی کند؛ ۳. مدل تکرارش را بررسی کند و ٤. قبل از بحران هشدار دهد.

۳. تقویت سواد رسانه‌ای مدیران: مدیران دفاعی امنیتی بهتر است آموزش‌هایی در حوزه‌های خطاهای شناختی، تحلیل روایت، تشخیص اطلاعات جعلی، تکنیک‌های عملیات روانی، جنگ رسانه‌ای و تفکر سیستمی دریافت کنند.

۴. چابک‌سازی ساختار تصمیم‌گیری: در این سناریو تصمیم‌گیری سریع‌تر، اطلاعات سازمانی یکپارچه‌تر، بوروکراسی کوچک‌تر و هماهنگی میان بخش‌ها بیشتر است.

۵. تقویت ارتباط دفاعی با جامعه: در این سناریو روایت دفاعی شفاف‌تر است، اعتماد عمومی تقویت می‌شود، جامعه در برابر عملیات شناختی مقاومت بیشتری دارد، رسانه‌های داخلی توان پاسخ‌گویی بالا دارند(Price, 2002) .

❖ پیامدهای احتمالی

- ارتقای امنیت ادراکی؛
- کاهش آسیب‌پذیری شناختی؛
- افزایش اعتماد عمومی؛
- تقویت انسجام سازمانی؛
- افزایش سرعت تصمیم‌گیری؛
- واکنش‌پذیری بالا در مقابل حملات نرم؛
- افزایش بازدارندگی روانی؛
- تقویت ارتباطات ملی؛
- افزایش کارآمدی مدیریتی؛
- توسعه زیرساخت‌های دفاع هوشمند.

این سناریو نشان می‌دهد که با معماری درست، تهدیدات نرم می‌توانند مدیریت شوند.

❖ نشانه‌های تحقق این سناریو

- ایجاد مرکز ملی دفاع شناختی؛
- شروع آموزش‌های تخصصی برای مدیران؛
- رشد رسانه‌های دفاعی داخلی؛
- مشارکت جامعه در روایت امنیتی دفاعی؛
- کاهش اثرگذاری رسانه‌های خارجی؛
- تولید محتوای ملی مبتنی بر هویت؛
- تقویت سامانه‌های سایبری و اطلاعاتی.

به‌طور خلاصه، آینده تهدیدات نرم و شناختی علیه کشورمان یک «خط سیر واحد» ندارد؛ بلکه چند مسیر ممکن وجود دارد. مسیر آینده به رفتار بازیگران، وضعیت جامعه، تحولات فناوری، روندهای جهانی و قدرت مدیریت سازمان بستگی دارد.

٤. نتیجه‌گیری

یافته‌های این پژوهش نشان می‌دهد که تهدیدات نرم و شناختی نه پدیده‌هایی مقطعی یا حاشیه‌ای، بلکه بخشی ساختاری از محیط امنیتی آینده جمهوری اسلامی ایران هستند. تحول در ماهیت منازعات، گسترش جنگ‌های ترکیبی، پیشرفت فناوری‌های اطلاعاتی و هوش مصنوعی و شبکه‌ای شدن جامعه موجب شده است که میدان اصلی تقابل امنیتی از حوزه‌های فیزیکی و نظامی به لایه‌های ادراکی، ذهنی و تصمیم‌سازی منتقل شود. در چنین شرایطی، امنیت ملی دیگر صرفاً به توان سخت و بازدارندگی نظامی وابسته نیست، بلکه به میزان کنترل، مدیریت و تاب‌آوری در برابر جنگ روایت‌ها و عملیات شناختی نیز گره خورده است.

تحلیل بازیگران و پیشران‌ها نشان می‌دهد که تهدیدات نرم و شناختی علیه ایران محصول کنش یک بازیگر منفرد نیست، بلکه نتیجه عملکرد یک «شبکه تهدید» متشکل از بازیگران دولتی، منطقه‌ای، فرامنطقه‌ای، رسانه‌ای، فناورانه و اجتماعی است. این شبکه با بهره‌گیری از ابزارهای متنوع، از رسانه‌های فراملی و پلتفرم‌های دیجیتال تا عملیات سایبری و اطلاعاتی، تلاش می‌کند ادراک عمومی، انسجام اجتماعی، اعتماد به نهادهای دفاعی و فرایند تصمیم‌سازی راهبردی را هدف قرار دهد. در چنین فضایی، نادیده گرفتن تهدید شناختی یا تقلیل آن به یک مسئله رسانه‌ای، خود می‌تواند به یکی از عوامل اصلی آسیب‌پذیری امنیتی تبدیل شود.

سناریوهای ترسیم‌شده در این پژوهش نشان می‌دهد که محتمل‌ترین مسیر آینده، تشدید تدریجی یا ناگهانی جنگ شناختی و ادراکی است؛ جنگی که می‌تواند از فرسایش آرام اعتماد عمومی تا بروز یک جنگ ترکیبی چندساحتی امتداد یابد. پیامدهای این سناریوها به‌روشنی بیانگر آن است که تهدیدات نرم قادرند بدون درگیری نظامی مستقیم، دقت تحلیل راهبردی را کاهش دهند، سرعت و کیفیت تصمیم‌گیری دفاعی امنیتی را مختل کنند، سرمایهٔ اجتماعی دفاعی را

تضعیف نمایند و حتی احتمال محاسبه غلط دشمن را افزایش دهند. از این منظر، تهدید شناختی نه‌تنها یک تهدید مکمل، بلکه می‌تواند به محرک اصلی بحران‌های امنیتی آینده تبدیل شود.

در مقابل، سناریوی «تاب‌آوری شناختی و مدیریت فعال» نشان می‌دهد که این مسیر آینده الزاماً اجتناب‌ناپذیر نیست. شرط اصلی تحقق این سناریوی مطلوب، عبور از رویکرد واکنشی و مقطعی به سمت یک رویکرد ساختاری، پیش‌دستانه و دکترین‌محور در مواجهه با تهدیدات نرم و شناختی است. تدوین دکترین دفاع شناختی، ایجاد سامانه‌های هشدار زودهنگام ادراکی، چابک‌سازی ساختارهای تصمیم‌گیری، ارتقای سواد شناختی و رسانه‌ای مدیران و تقویت ارتباط معنادار و اعتمادمحور میان نهادهای دفاعی و جامعه، ازجمله الزامات راهبردی این مسیر محسوب می‌شوند.

در نهایت، این پژوهش تأکید می‌کند که آینده امنیت ملی جمهوری اسلامی ایران، بیش از هر زمان دیگر، به توان مدیریت ذهن، روایت و ادراک وابسته است. کشوری که بتواند ثبات شناختی جامعه و انسجام تصمیم‌سازی خود را حفظ کند، حتی در شرایط فشار چندلایه و جنگ ترکیبی نیز قادر خواهد بود بازدارندگی مؤثر و پایداری راهبردی خود را تداوم بخشد. ازاین‌رو، سرمایه‌گذاری در حوزه دفاع شناختی نه یک انتخاب، بلکه یک ضرورت اجتناب‌ناپذیر راهبردی برای آینده امنیت کشور است.

فهرست منابع

پدرام، عبدالرحیم؛ احمدیان، مهدی (۱۳۹٤). ***آموزه‌ها و آزموده‌های آینده‌پژوهی***. تهران: مؤسسه افق آینده‌پژوهی راهبردی.

بِل، وندل (۱۳۹۲). ***مبانی آینده‌پژوهی: تاریخچه، اهداف و دانش***، ترجمه مصطفی تقوی و محسن محقق، تهران: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

References

Akerlof, G., & Shiller, R. (2009). *Animal Spirits: How Human Psychology Drives the Economy, and Why It Matters for Global Capitalism*. Princeton University Press.

Al-Rasheed, M. (2020). *The Politics of Saudi Arabia*. Cambridge University Press.

Bishop, P., & Hines, A. (2012). *Thinking about the Future: Guidelines for Strategic Foresight*. Wiley.

Kahneman, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux.

NATO Innovation Hub. (2021). *Cognitive Warfare Study*. NATO Allied Command Transformation.

Nye, J. S. (2004). *Soft Power: The Means to Success in World Politics*. Public Affairs.

Price, M. (2002). *Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power*. MIT Press.

Rid, T., & Buchanan, B. (2015). *Attributing Cyber Attacks*. Journal of Strategic Studies, 38(1–2), 4–37.

Singer, P. W., & Brooking, E. (2018). *LikeWar: The Weaponization of Social Media*. Houghton Mifflin Harcourt.

Sunstein, C. R. (2017). *Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.

Tufekci, Z. (2015). *Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency*. Colorado Technology Law Journal, 13(203), 203–218.

Walt, S. M. (2018). *The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S*. Primacy. Farrar, Straus and Giroux.