



Imam Sadiq Research Institute

for Islamic Sciences

Research Institute for Political
and Defence Studies

P. ISSN: 2345-5705 & E. ISSN: 2717-3720

Website: <http://ipr.isri.ac.ir>

Autumn 2025 & Winter 2026



The Islamic Revolution in the Cognitive Battlefield: Assessing the Relationship between the “Jihād-e Tabyīn” Doctrine and the Emerging Challenge of Deepfakes

Ali Zareei*, Reza Mohammadi**

Doi: 10.22034/ipr.2026.557823.2331

Receipt: 2025/11/05 - Revised: 2025/11/22- Accepted: 2026/02/10

(72-100)

Abstract

In the contemporary era, the pattern of confrontation with the Islamic Revolution has shifted from hard warfare to cognitive warfare—a battle aimed at dominating minds and managing societal perceptions. In this context, “deepfake” technology, as a novel cognitive weapon with the capability to produce fabricated yet realistic content, has become a primary tool for the enemy to spread falsehoods and disinformation, targeting official authorities and the credibility of narratives. This situation poses a serious challenge to the “Jihād-e Tabyīn” doctrine as the Islamic Republic’s cognitive defense strategy. Therefore, the main question of this research is how deepfake technology challenges the effectiveness of the “Jihād-e Tabyīn” doctrine in the cognitive battlefield, and what strategies exist to enhance this doctrine against this emerging threat. This article, using a descriptive-analytical method and a qualitative approach, examines the interaction between this doctrine and the deepfake threat. Findings indicate that deepfakes disrupt the effectiveness of the “Jihād-e Tabyīn” through five mechanisms: “authority erosion,” “information flooding,” “activation of societal fault lines,” “memory distortion,” and “systematic delegitimization.” The results suggest that countering this threat necessitates a transition from reactive defense to integrated defense. Accordingly, solutions are proposed across three complementary levels: technical-legal, educational-media, and strategic-institutional.

Keywords: Islamic Revolution, Cognitive Warfare, Jihad of Clarification, Deepfakes, Cognitive Security, Domination of Minds.

*. Assistant Professor, Department of Islamic Studies, Central Tehran Branch, Islamic Azad University, Tehran, Iran. (Corresponding Author). ali.zareei@iaiu.ac.ir

** Associate Professor, Department of Islamic Studies, Faculty of Humanities, Bu-Ali Sina University, Hamedan, Iran. r.muhammadi@basu.ac.ir





پژوهشگاه علوم اسلامی امام صادق (علیه السلام)
پژوهشکده مطالعات سیاسی و دفاعی
P. ISSN: 2345-5705 & E. ISSN: 2717-3720
نشانی پانگه نشریه: <http://ipr.isri.ac.ir>
پاییز و زمستان ۱۴۰۴

انقلاب اسلامی در میدان جنگ شناختی: نسبت‌سنجی دکترین «جهاد تبیین» با چالش نوظهور جعل عمیق

علی زارعی*، رضا محمدی**

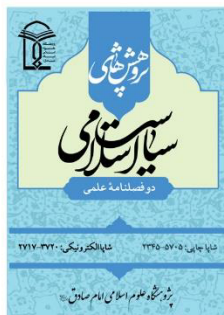
Doi: 10.22034/ipr.2026.557823.2331

تاریخ دریافت: ۱۴۰۴/۰۸/۱۴ - تاریخ بازنگری: ۱۴۰۴/۹/۱ - تاریخ پذیرش: ۱۴۰۴/۱۱/۲۱
(۷۲-۱۰۰)

چکیده

در دوران معاصر، الگوی تقابل با انقلاب اسلامی از جنگ‌های سخت به جنگ شناختی تغییر یافته است؛ نبردی که هدف آن تسلط بر ذهن‌ها و مدیریت ادراکات جامعه است. در این میان، فناوری «جعل عمیق» به عنوان سلاحی شناختی نوین، با توان تولید محتوای جعلی اما واقع‌نما، به ابزار اصلی دشمن برای جعل و دروغ‌پردازی تبدیل شده و مرجعیت‌های رسمی و اعتبار روایت‌ها را هدف قرار می‌دهد. این وضعیت، چالشی جدی برای دکترین «جهاد تبیین» به مثابه راهبرد دفاع شناختی جمهوری اسلامی ایجاد کرده است. از این رو مسئله اصلی پژوهش آن است که فناوری جعل عمیق چگونه کارآمدی دکترین جهاد تبیین را در میدان جنگ شناختی با چالش مواجه می‌کند و راهکارهای ارتقای این دکترین در برابر این تهدید نوظهور چیست. مقاله حاضر با روش توصیفی-تحلیلی و رویکردی کیفی، به نسبت‌سنجی میان این دکترین و تهدید جعل عمیق می‌پردازد. یافته‌ها نشان می‌دهد جعل عمیق از طریق پنج مکانیزم «فرسایش مرجعیت»، «خلق سیلاب اطلاعاتی»، «فعال‌سازی گسل‌ها»، «تحریف حافظه» و «مشروعیت‌زدایی»، کارآمدی جهاد تبیین را مختل می‌سازد. نتایج حاکی از آن است که مقابله با این تهدید مستلزم گذار از پدافند واکنشی به دفاعی یکپارچه است؛ از این رو راهکارهایی در سه سطح مکمل فنی-حقوقی، آموزشی-رسانه‌ای و راهبردی-نهادی پیشنهاد می‌شود.

واژگان کلیدی: انقلاب اسلامی، جنگ شناختی، جهاد تبیین، جعل عمیق، امنیت شناختی، تسلط بر مغزها.



*. استادیار گروه معارف اسلامی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول).
ali.zareei@iauo.ac.ir

** استادیار گروه معارف اسلامی، دانشکده علوم انسانی، دانشگاه بوعلی سینا، همدان، ایران.
r.muhammadi@basu.ac.ir

۱. مقدمه

در سپهر نوین امنیت بین‌الملل، شاهد یک تغییر الگوی راهبردی هستیم: میدان نبرد به طور فزاینده‌ای از عرصه‌های فیزیکی و نظامی محور به حوزه‌های ناملموس و پیچیده شناختی منتقل شده است؛ تا جایی که مغز را میدان نبرد قرن ۲۱ می‌دانند (Du Cluzel, 2022: 4; Nye, 2004b: 681). در این پارادایم جدید که از آن با عناوینی چون «جنگ شناختی»، «نبرد روایت‌ها» یا «عصر پساحقیقت» یاد می‌شود، هدف اصلی نه تصرف سرزمین، بلکه فتح ذهن و «تسلط بر مغزهاست» (Poisant, 2021: 4; Nye, 2004a: 11). بازیگران متخاصم در این عرصه، دیگر نه صرفاً با اتکا به توان سخت، بلکه با بهره‌گیری از ابزارهای پیشرفته اطلاعاتی و روانشناختی، به دنبال مدیریت ادراکات، مهندسی افکار عمومی و درنهایت، کنترل رفتار جوامع هدف هستند (Du Cluzel, 2022: 6). ظهور فناوری‌های مبتنی بر هوش مصنوعی مولد، این عرصه را با سلاح‌هایی بی‌سابقه تجهیز کرده است که مرز میان حقیقت و جعل را به شکل خطرناکی کمرنگ می‌کنند (Devilliers, 2021: 26-33).

در کانون این تحولات، فناوری «جعل عمیق»^۱ به عنوان یک سلاح شناختی نوین و قدرتمند ظهور کرده است. این فناوری با قابلیت تولید محتوای صوتی و تصویری جعلی اما به شدت واقع‌نما، تهدیدی استراتژیک محسوب می‌شود که می‌تواند با هزینه اندک و مقیاس بالا، بحران‌های امنیتی، سیاسی و اجتماعی خلق کند (Chesney & Citron, 2019: 1753-60). اهمیت این تهدید به حدی است که دیگر در حوزه نظری باقی‌نمانده و وارد دکترین‌های عملیاتی قدرت‌های جهانی شده است؛ هشدار دیرکل سازمان ملل متحد درباره پتانسیل جعل عمیق برای «تضعیف نهادها، گسترش بی‌اعتمادی و ایجاد هرج و مرج جهانی» و لزوم ایجاد «سیستم‌های تأیید محتوا»، (United Nations, 2023: 8) و از سوی دیگر، سرمایه‌گذاری رسمی فرماندهی عملیات ویژه ارتش آمریکا (SOCOM) بر روی «نسل آینده فناوری جعل عمیق» برای استفاده در «عملیات‌های نفوذ غیرسنتی»، به وضوح نشان می‌دهد که این پدیده از یک کنجکاوی فناورانه به یک سلاح عملیاتی-نظامی تبدیل شده است

(Biddle, 2023, March 6). نمونه‌های داخلی متعددی، از جمله عملیات تقطیع و جعل صدای رهبر معظم انقلاب در مرداد ۱۳۹۷ (خبر آنلاین، ۲۴ / ۵ / ۱۳۹۷)، انتشار فایل‌های صوتی و تصویری منتسب به برخی مقامات عالی رتبه و فرماندهان نظامی و نیز تولید محتوای جعلی در بستر شبکه‌های اجتماعی طی سال‌های اخیر (جهان نیوز، ۱۴۰۴/۸/۲۷)، این واقعیت را تأیید می‌کند که به‌کارگیری سلاح جعل عمیق به‌صورت گسترده در دستور کار دشمن قرار گرفته است.

در چنین فضای پرآشوبی، انقلاب اسلامی ایران که موجودیت و تداوم خود را بیش از هر چیز در گروی اقتناع فکری، انسجام ملی و پیوند با افکار عمومی تعریف کرده، با چالشی وجودی روبروست. در پاسخ به همین ضرورت، دکترین «جهاد تبیین» توسط رهبر معظم انقلاب به‌عنوان یک راهبرد کلان دفاعی-شناختی برای مصون‌سازی ادراکی جامعه و مقابله با حجم عظیم دروغ‌پراکنی دشمن، تبیین و ترویج شده است (ذوعلم، ۱۴۰۱). این دکترین بر اصالت روایت، شفاف‌سازی حقایق، روایتگری پیش‌دستانه و کنشگری فعال آحاد جامعه در عرصه تبیین دستاوردها و مبانی انقلاب استوار است (رک: صلح میرزایی، ۱۴۰۰). با این حال، جهاد تبیین در مواجهه با سلاحی که می‌تواند «واقعیت» را به‌صورت صنعتی تولید و تکثیر کند، با پرسش‌های جدیدی روبرو می‌شود. پرسش بنیادین این پژوهش آن است که سلاح نوظهور جعل عمیق، چگونه و از طریق چه مکانیزم‌هایی می‌تواند کارآمدی دکترین «جهاد تبیین» را به‌مثابه یک سپر دفاع شناختی به چالش بکشد و راهکارهای راهبردی برای کارآمدسازی و ارتقاء این سپر در برابر تهدیدات نوین چیست؟

این پژوهش کاربردی-توسعه‌ای، با روش توصیفی-تحلیلی و گردآوری اسنادی انجام شده است. چارچوب تحلیل داده‌ها مبتنی بر مدل کیفی «تحلیل تهدید-آسیب‌پذیری» است که ابتدا با کالبدشکافی تهدید جعل عمیق در مطالعات موردی (نظیر جنگ روایت ایران-اسرائیل)، نقاط آسیب‌پذیر دکترین جهاد تبیین را شناسایی کرده و نهایتاً راهکارهای مقابله‌ای را در سه سطح فنی-حقوقی، آموزشی-رسانه‌ای و راهبردی-نهادی ارائه می‌دهد.

۲. پیشینه پژوهش

بررسی ادبیات پژوهشی مرتبط با موضوع حاضر نشان می‌دهد که مطالعات موجود را می‌توان در سه حوزه اصلی اما مجزا از یکدیگر دسته‌بندی کرد. حوزه اول، بر خود فناوری جعل عمیق متمرکز است و ابعاد فنی، حقوقی و امنیتی آن را می‌کاود. پژوهش‌های فنی مانند آثار خان^۱ و همکاران (2025)، الگوریتم‌های تولید و کشف این پدیده را تشریح می‌کنند. در بعد حقوقی، تحقیقاتی نظیر مقاله السان و دهستانی (۱۴۰۱) به چالش‌های قانونی آن برای حریم خصوصی و مسئولیت کیفری پرداخته و بر لزوم تدوین مقررات بازدارنده تأکید دارند. همچنین، در بعد امنیتی-سیاسی، آثار تأثیرگذاری چون مقاله چسنی^۲ و سیترون^۳ (2019)، خطرات استراتژیک جعل عمیق برای بی‌ثبات‌سازی سیاسی و فرسایش اعتماد عمومی را به خوبی کالبدشکافی کرده‌اند. با این حال، این دسته از پژوهش‌ها عمدتاً تهدید را به صورت انتزاعی تحلیل کرده و کمتر به کاربرد عملیاتی آن در بستر یک تقابل راهبردی مشخص علیه جمهوری اسلامی ایران پرداخته‌اند. حوزه دوم پژوهش‌ها، به میدان نبرد کلان‌تر یعنی جنگ شناختی می‌پردازد. آثاری چون کتاب «جنگ شناختی: مواد خاکستری در منازعات سیاسی معاصر» اثر هنشکه^۴ (2025) مبانی مفهومی و اخلاقی این نبرد را تبیین کرده و در داخل کشور نیز محققان متعددی ابعاد جنگ ترکیبی علیه ایران را بررسی نموده‌اند. ضعف اصلی این دسته از آثار، کلی‌نگری نسبت به ابزارهاست؛ آن‌ها ضمن توصیف صحیح تاکتیک‌های دشمن، کمتر به طور مشخص به مکانیزم‌های عمل یک سلاح نوظهور مانند جعل عمیق در این کارزار ورود کرده‌اند. در نهایت، حوزه سوم تحقیقات، به دکترین دفاعی یعنی جهاد تبیین اختصاص دارد. این آثار که عمدتاً پس از تأکیدات رهبر معظم انقلاب تدوین شده‌اند، مانند مجموعه بیانات ایشان با عنوان «جهاد تبیین» (۱۴۰۰)، مبانی نظری و الزامات این راهبرد دفاعی مبتنی بر حقیقت را به خوبی روشن می‌سازند، اما طبیعتاً به صورت مستقیم به

-
1. Khan
 2. Robert Chesney
 3. Danielle K. Citron
 4. Adam Henschke

نسبت‌سنجی آن با چالش‌های فناورانه پیچیده‌ای مانند جعل عمیق نپرداخته و فاقد تحلیل آسیب‌شناسانه در این زمینه هستند؛ بنابراین، با بررسی این سه جریان پژوهشی، شکاف تحقیقاتی به وضوح نمایان می‌شود: تاکنون پژوهشی منسجم که سه ضلع «سلاح جعل عمیق»، «میدان نبرد جنگ شناختی» و «سپر دفاعی جهاد تبیین» را در یک چارچوب تحلیلی واحد قرار دهد و به نسبت‌سنجی عملیاتی میان آن‌ها بپردازد، انجام نشده است. نوآوری این مقاله دقیقاً در پر کردن همین شکاف نهفته است؛ یعنی ایجاد یک پل مفهومی میان این سه حوزه مجزا و تحلیل چالش‌های یک سلاح شناختی نوین برای یک دکترین دفاع شناختی بومی و نهایتاً ارائه راهکارهای انطباقی برای کارآمدسازی این دکترین در مواجهه با تهدیدات عصر هوش مصنوعی.

۳. چارچوب مفهومی

برای درک عمیق نسبت میان دکترین جهاد تبیین و چالش جعل عمیق، ضروری است ابتدا سه مفهوم بنیادین این حوزه یعنی جنگ شناختی، جعل عمیق و جهاد تبیین به دقت تعریف و روابط نظری میان آن‌ها تبیین شود.

۳-۱. جنگ شناختی^۱

جنگ شناختی، مفهومی است که نخستین بار به صورت نظام‌یافته در درون ساختار ناتو توسط دفتر نوآوری فرماندهی تحول متحدین^۲ و در ادامه توسط پژوهشگران برنار کلاوریه^۳ فرانسوا دوکلوزل^۴ صورت‌بندی شد. در این چارچوب، ناتو «ذهن انسان» را هم‌زمان هدف و سلاح نبرد می‌داند و از جنگ شناختی به عنوان «نبردی که ذهن را میدان اصلی خود می‌سازد» یاد می‌کند (Claverie & du Cluzel, 2021: 5). مطابق تعریف رسمی این سازمان، جنگ شناختی نه ابزار جنگ بلکه خود جنگ است؛ عرصه‌ای که در آن مجموعه‌ای از

1. Cognitive Warfare

2. Allied Command Transformation - ACT

3. Bernard Claverie

4. François du Cluzel

اقدامات نظامی و غیرنظامی با هدف تحریف ادراک، تضعیف عقلانیت و تأثیرگذاری بر فرآیندهای عالی ذهنی انسان مانند تفکر، داوری و تصمیم‌گیری طراحی می‌شوند (NATO Allied Command Transformation, n.d). هدف نهایی در این پارادایم، نه تخریب فیزیکی، بلکه «فروپاشی از درون» از طریق دستکاری نظام محاسباتی و ادراکی نخبگان و توده‌های مردم است. دشمن در این نبرد می‌کوشد با ایجاد عدم قطعیت، ترویج بی‌اعتمادی و ارائه روایت‌های جایگزین، توانایی جامعه هدف برای تشخیص واقعیت و اتخاذ تصمیمات منطبق با منافع ملی را سلب نماید (Deppe & Schaal, 2024: 2-11). این نوع جنگ، به تعبیر کلوزویتس، «ادامه سیاست با ابزارهای دیگر» است (Clausewitz, 1976: 87). با این تفاوت که ابزارها اکنون شامل داده‌های کلان، هوش مصنوعی، علوم اعصاب شناختی و شبکه‌های اجتماعی می‌شوند (Deppe & Schaal, 2024). انقلاب اسلامی به دلیل ماهیت گفتمانی و تکیه بر قدرت نرم، همواره در معرض تهاجمات شناختی با هدف «وارونه‌نمایی واقعیت‌ها»، «مشروعیت‌زدایی از آرمان‌ها» و ایجاد گسست میان ملت و حاکمیت بوده است.

از منظر مدل‌سازی فرآیندی، مکانیسم اثرگذاری جنگ شناختی را می‌توان با مدل چرخه تصمیم‌گیری جان بوید یا همان «حلقه اودا» (OODA)^۱ تبیین کرد. این مدل شامل چهار مرحله تکرارشونده «مشاهده»، «جهت‌گیری»، «تصمیم» و «اقدام» است که بنیان هر رفتار هوشمندانه را شکل می‌دهد (Boyd, 1987). نکته راهبردی آنجاست که برخلاف نبردهای کلاسیک که بر شکست دشمن در مرحله نهایی (اقدام) تمرکز دارند، جنگ شناختی نوک پیکان حمله را به سمت دو مرحله نخستین این حلقه، یعنی «مشاهده» (دریافت ورودی‌های اطلاعاتی) و «جهت‌گیری» (تحلیل داده‌ها بر اساس باورها و پیش‌فرض‌ها) نشان می‌دهد. در این وضعیت، دشمن با آلوده کردن مشاهدات (از طریق داده‌های جعلی) و دستکاری جهت‌گیری‌ها (از طریق روایات انحرافی)، سیستم پردازش ذهنی حریف را مختل می‌کند؛ به گونه‌ای که قربانی حتی با وجود عقلانیت ظاهری، در یک جبر محاسباتی گرفتار شده و ناخودآگاه تصمیماتی مغایر با منافع حیاتی خود و همسو با خواست دشمن اتخاذ می‌کند.

1. OODA: Observe, Orient, Decide, Act

۳-۲. جعل عمیق

جعل عمیق، ترکیبی از «یادگیری عمیق» و «جعلی»، به فناوری‌ای اطلاق می‌شود که با استفاده از الگوریتم‌های پیشرفته هوش مصنوعی، به ویژه شبکه‌های مولد تخاصمی (GANs)^۱، قادر به تولید یا دستکاری محتوای صوتی و تصویری با سطح خیره‌کننده‌ای از واقع‌گرایی است. این فناوری می‌تواند چهره یک فرد را در یک ویدئو با چهره فردی دیگر جایگزین کند، کلماتی را که هرگز گفته نشده از زبان او بیان نماید، یا صدایی کاملاً مشابه صدای یک شخص خاص تولید کند (Goodfellow et al. 2014: 2672-9; Chesney & Citron, 2019: 1757-60). خطر اصلی جعل عمیق در توانایی آن برای نابود کردن «بنیان اعتماد» در سپهر اطلاعاتی جامعه نهفته است. در دنیایی که دیگر نمی‌توان به صحت یک ویدئو یا فایل صوتی اطمینان داشت، پدیده‌ای به نام «بن بست معرفتی»^۲ رخ می‌دهد که در آن، شهروندان از تشخیص حقیقت عاجز مانده و به دامان شکاکیت مطلق یا پذیرش کورکورانه اطلاعاتی که صرفاً با باورهای پیشین آن‌ها همسوست، پناه می‌برند (Chesney & Citron, 2019: 1777, 1786).

۳-۳. جهاد تبیین

در پاسخ به پیچیدگی‌های فزاینده جنگ شناختی و ظهور سلاح‌های نوین آن، رهبر معظم انقلاب اسلامی، دکترین «جهاد تبیین» را به عنوان یک «فریضه قطعی و فوری» مطرح نمودند (آیت‌الله خامنه‌ای، بیانات، ۱۴۰۰/۱۱/۱۹). در واقع جهاد تبیین یک راهبرد کنشگرانه و هوشمند در عرصه روشنگری و مقابله با جنگ روایت‌هاست و فراتر از یک توصیه اخلاقی، یک دکترین دفاعی-تهاجمی محسوب می‌شود.^۳ این دکترین بر چند رکن اساسی استوار

1. Generative Adversarial Networks

2. Epistemic Gridlock

۳. «دشمن در رأس نقشه‌های تبلیغات است؛ به قول خودشان پروپاگاندا است. علاج پروپاگاندا «تبیین» است...» (آیت‌الله خامنه‌ای، بیانات، ۱۴۰۱/۱۰/۱۹).

«امروز مهم‌ترین شیوه‌ی دشمن، جعل و دروغ‌پردازی است... خب وقتی که دانستید، طبعاً وظیفه می‌آید روی دوشتان. تبیین کنید. «جهاد تبیین» که گفتیم، یکی از جاهایش اینجا است.» (همان، ۱۴۰۱/۰۹/۰۵).

«آن چیزی که می‌تواند به بهترین وجهی به صورت یک سلاح مؤثری عمل کند، تبیین مفاهیم عالی اسلامی است... اینها چیزهایی است که سلاحهای جدید ما است، باید از اینها استفاده کرد.» (همان، ۱۴۰۰/۱۲/۱۹).

است: کنشگری فعال و پیش‌دستانه برای روایتگری دست اول به‌جای پاسخ‌گویی منفعلانه؛^۱ تکیه بر منطق محکم و بیان عقلانی برای اقناع قلوب و اذهان، به‌ویژه نسل جوان؛^۲ تمرکز بر امیدآفرینی از طریق بیان دستاوردها برای خنثی‌سازی راهبرد یأس‌پراکنی دشمن؛^۳ و تأکید بر همگانی بودن این جهاد به‌عنوان یک مسئولیت ملی که بر عهده تمام صاحبان تربیون و اندیشه است.^۴ درواقع، جهاد تبیین را می‌توان راهبرد کلان جمهوری اسلامی برای ایمن‌سازی شناختی جامعه در برابر ویروس‌های ذهنی و اطلاعاتی دشمن تعریف کرد که به دنبال تقویت قوه تحلیل و تشخیص مخاطب در برابر امواج تحریف و دروغ است.

بنابراین، نسبت میان این سه مفهوم در قالب یک زنجیره علی قابل فهم است: جنگ شناختی به‌عنوان میدان اصلی منازعه، جعل عمیق به‌عنوان ابزار اخلال‌گر در حلقه ادراک و تصمیم‌گیری و جهاد تبیین به‌عنوان دکترین ایمن‌ساز و ترمیم‌کننده که مأموریت آن بازسازی اعتماد، تثبیت مرجعیت و خنثی‌سازی عملیات فریب در سپهر شناختی جامعه است.

۴. تحلیل چالش‌ها: مکانیزم‌های تضعیف جهاد تبیین با سلاح جعل عمیق

همان‌طور که اشاره شد، هدف اصلی جنگ شناختی اختلال در مراحل «مشاهده» و

۱. «وظیفه‌ی خواص این است: در مواقع لازم، باید تردیدافکنی و شک‌آفرینی دشمن را خنثی کنند و (مسائل را) تبیین کنند.» (همان، ۱۴۰۲/۱۱/۱۶).

۲. «وسوسه‌ای را که روی آن جوان یا نوجوان اثر میگذارد، چه میتواند برطرف کند؟ باتوم که نمیتواند برطرف کند، آن وسوسه را تبیین میتواند برطرف کند.» (همان، ۱۴۰۱/۱۰/۱۹).

۳. «شما جوانان عزیز و دانشجویان عزیز... به مسئله‌ی «تبیین» اهمیت بدهید... جوانهای ما امروز بحمدالله مجهزند؛ مجهز به فکر، مجهز به عقلانیت، مجهز به آگاهی‌های فراوان و میتوانند در این زمینه‌ها خیلی تلاش کنند.» (همان، ۱۴۰۰/۰۷/۰۵).

۴. «وظیفه این است که ایمانها را تقویت کنند، امیدها را تقویت کنند، شبهه‌ها را برطرف کنند، شیوه‌های دشمن در شبهه‌آفرینی و یأس‌آفرینی را خنثی کنند.» (همان، ۱۴۰۲/۰۳/۱۴).

«تلاش میکنند مردم را مأیوس کنند، مردم را بی‌اعتماد کنند... در مقابل اینها «جهاد تبیین» باید سینه سپر کند.» (همان، ۱۴۰۲/۱۰/۱۳).

۴. «جهاد تبیین را جدی باید گرفت. همه، در حوزه، در دانشگاه، در صداوسیما بالخصوص، در مطبوعات، در هر جایی که شما ایستاده‌اید و یک شعاع پیرامونی‌ای دارید و میتوانید روی آن اثر بگذارید، باید تبیین انجام بگیرد.» (همان، ۱۴۰۱/۱۰/۱۹).

«هر کدام از شما به‌عنوان یک وظیفه، مثل یک چراغی، مثل یک نوری پیرامون خودتان را روشن کنید.» (همان، ۱۴۰۰/۰۷/۰۵).

«جهت‌گیری» در حلقه اودا است. فناوری جعل عمیق دقیقاً به‌عنوان پیشرفته‌ترین سلاح برای تحقق این اختلال وارد عمل می‌شود و از طریق مکانیزم‌های زیر، دکترین جهاد تبیین را هدف قرار می‌دهد.

۴-۱. فرسایش مرجعیت از طریق حملات اعتباری دقیق

دکترین جهاد تبیین، پیش از آنکه به صدق و کذب محتوای یک پیام بپردازد، معطوف به شکل‌گیری، حفظ و بازتولید مرجعیت‌های معتبر معرفتی در ذهن مخاطب است؛ مرجعیت‌هایی که بدون آن‌ها فرآیند اقتناع اصولاً امکان‌پذیر نیست. این مرجعیت که می‌تواند در قالب یک شخصیت حقیقی (مانند رهبران نظام، مسئولان ارشد، نخبگان فکری) یا یک نهاد حقوقی (مانند دولت، نیروهای مسلح، رسانه ملی) تجلی یابد، سرمایه اجتماعی و شناختی حیاتی نظام است که امکان اقتناع‌سازی را فراهم می‌آورد. مکانیزم «فرسایش مرجعیت» با بهره‌گیری از فناوری جعل عمیق، این سرمایه را به‌طور مستقیم و با دقت زیاد هدف قرار می‌دهد. این فناوری با تولید محتوای صوتی و تصویری جعلی اما به‌شدت واقع‌نما، قادر است تصویری مخدوش، متناقض و غیرقابل اعتماد از این مراجع ارائه دهد (Chesney & Citron, 2019: 1759-61)؛ تصویری که در آن یک مقام مسئول سخنانی علیه امنیت ملی بیان می‌کند، یک شخصیت مورد احترام به فساد اعتراف می‌کند، یا یک فرمانده نظامی روحیه‌ای متزلزل از خود نشان می‌دهد.

این مواجهه مکرر، به شکل‌گیری حالت پایدار بدبینی شناختی در مخاطب می‌انجامد. این پدیده به‌طور دقیق توسط مؤسسه RAND تحت عنوان «زوال حقیقت»^۱ تئوریزه شده است که یکی از چهار روند اصلی آن، «کاهش اعتماد به منابعی است که قبلاً به‌عنوان منابع معتبر واقعیت شناخته می‌شدند» (Kavanagh & Rich, 2018). در این وضعیت، پرسش ویرانگر «از کجا معلوم این واقعی باشد؟» نه تنها در مواجهه با محتوای مشکوک، بلکه در برابر هر پیام رسمی شکل می‌گیرد. این تردید، یک سپر روانی قدرتمند در برابر هرگونه تبیین ایجاد کرده و باعث می‌شود حتی بیانی‌های صادقانه و مستدل نیز با دیده شک نگریده

1. Truth Decay

شوند. دوم، این وضعیت منجر به پدیده‌ای موسوم به «سود سهام دروغ‌گو»^۱ می‌شود؛ در محیطی که همه چیز می‌تواند جعلی باشد، دیکتاتورها و مجرمان می‌توانند با برجسب «جعل عمیق» به راحتی شواهد و مدارک واقعی علیه خود را بی اعتبار کنند و از پاسخگویی بگریزند. در این حالت، جعل عمیق نه تنها با تولید دروغ، بلکه با نابود کردن توانایی اثبات حقیقت، به دشمن خدمت می‌کند (Chesney & Citron, 2019: 1785).

این استراتژی بر یک عدم تقارن ویرانگر بنا شده است به طوری تولید و انتشار یک جعل عمیق، سریع و کم هزینه است، اما فرآیند راستی‌آزمایی و اقتناع افکار عمومی بسیار دشوارتر است. پژوهش‌ها نشان می‌دهند که اخبار نادرست به شکل معناداری سریع‌تر و گسترده‌تر از اخبار حقیقی منتشر می‌شوند (Vosoughi et al. 2018). این چالش با این واقعیت تشدید می‌شود که تکذیبیه‌ها اغلب در خنثی کردن کامل تأثیر اولیه اطلاعات غلط ناتوان هستند و لکه تردید حتی پس از افشاگری نیز باقی می‌ماند (Lewandowsky et al, 2012).

شواهد بین‌المللی، قدرت این مکانیزم را به وضوح نشان می‌دهد. ویدئوی دستکاری شده از «نانسی پلوسی» در سال ۲۰۱۹ که او را نامتعادل نشان می‌داد، یک هشدار اولیه بود، این ویدئوی دستکاری شده به سرعت در شبکه‌های اجتماعی منتشر شد و توسط چهره‌های سیاسی برجسته نیز تقویت گردید (Mervosh, 2019)؛ اما نقطه عطف، انتشار ویدئوی جعل عمیق از رئیس‌جمهور اوکراین، «ولودیمیر زلنسکی»، در روزهای ابتدایی تهاجم روسیه بود که در آن از سربازانش می‌خواست تسلیم شوند (Allyn, 2022). اگرچه این ویدئو به سرعت افشا شد، اما هدف راهبردی آن کاملاً روشن بود: اعتبارزدایی از بالاترین مرجع فرماندهی در حساس‌ترین لحظه ممکن برای ایجاد آشوب و فروپاشی روانی. در عرصه داخلی، انتشار فایل‌های صوتی منتسب به فرماندهان ارشد نظامی و مقامات عالی‌رتبه طی سال‌های اخیر، نمونه‌ای بارز از کاربست همین استراتژی جنگ شناختی است. این کنش‌ها، فارغ از درستی یا نادرستی محتوایشان، با هدف ترویج روایت اختلاف و فساد در رأس حاکمیت و نهایتاً فرسایش انسجام ظاهری و تضعیف مرجعیت نهادهای امنیتی طراحی شده بودند.

سناریوهای بالقوه آینده، این تهدید را ملموس‌تر می‌سازند. تصور کنید ویدئویی حاصل از جعل عمیق از وزیر اقتصاد منتشر شود که در آن به مردم توصیه می‌کند فوراً سپرده‌های خود را از بانک‌ها خارج کنند. حتی تکذیب چند ساعته نیز نمی‌تواند جلوی شکل‌گیری موج اولیه هجوم بانکی و آغاز یک بحران اقتصادی را بگیرد. یا سناریوی تولید یک فایل صوتی جعلی از یکی از مراجع عظام تقلید که فتوایی خلاف وحدت ملی صادر می‌کند. در تمامی این موارد، هدف نهایی یکسان است: با از بین بردن اعتماد به منابع رسمی، جهاد تبیین از کارآمدترین ابزار خود، یعنی «اعتبار»، محروم شده و به صدایی بی‌اثر در هیاهوی اطلاعاتی تبدیل می‌شود. این مکانیزم، جنگ روایت‌ها را به جنگ بر سر خود «واقعیت» ارتقا می‌دهد و با تهی کردن مفهوم مرجعیت، جامعه را در برابر هرگونه روایت‌پردازی دشمن، خلع سلاح و آسیب‌پذیر می‌سازد.

۲-۴. سیلاب اطلاعاتی به مثابه ابزار اخلال در تشخیص شناختی

یکی از کارکردهای محوری جهاد تبیین، استقرار و حاکمیت «روایت صحیح» در برابر روایت‌های تحریف‌شده است. این فرآیند مستلزم آن است که روایت صحیح بتواند در شرایط اشباع اطلاعاتی، قابلیت دریافت و پردازش مؤثر توسط مخاطب را حفظ کند. مکانیزم «سیلاب اطلاعاتی» که توسط اندیشکده RAND به عنوان دکتترین روسی «شیلنگ آتش دروغ‌پراکنی»^۱ مدل‌سازی شده، این پیش‌فرض را به طور کامل نابود می‌کند. در این استراتژی، هدف اصلی دشمن، متقاعد کردن مخاطب به یک دروغ مشخص و واحد نیست؛ بلکه هدف، «فلج ساختن قوه تشخیص»^۲ از طریق بمباران مخاطب با حجم عظیمی از محتوای جعلی، متناقض، شایعات و شبه‌روایت‌ها پیرامون یک رویداد واحد است (Paul & Matthews, 2016). این رویکرد، روایت صحیح و رسمی را از جایگاه مرجع به یکی از گزینه‌های بی‌شمار در میان انبوهی از جعلیات تنزل می‌دهد و مخاطب سردرگم و خسته را به یک «نسبی‌گرایی شناختی» سوق می‌دهد: این باور فلج‌کننده که «هیچ حقیقتی قابل دسترسی نیست و همه در حال دروغ‌گویی هستند» (Kavanagh & Rich, 2018).

1. Firehose of Falsehood

2. Analysis Paralysis

فناوری جعل عمیق، این استراتژی را از یک تهدید نظری به یک واقعیت عملیاتی ویرانگر تبدیل کرده است. در گذشته، تولید محتوای بصری جعلی زمان‌بر و پرهزینه بود، اما اکنون جعل عمیق این امکان را فراهم می‌آورد که برای یک حادثه واحد، در عرض چند ساعت، ده‌ها روایت تصویری و صوتی جعلی اما باورپذیر تولید و به صورت ویروسی منتشر شود. این فناوری به دشمن اجازه می‌دهد که به جای ارائه یک ضدروایت، یک «اکوسیستم کامل از ضدروایت‌ها» خلق کند (Chesney & Citron, 2019: 1762-1786). این پدیده که در آن جعل عمیق نقش «تولیدکننده مهمات برای ماشین جنگ روایت» را ایفا می‌کند، در جنگ اوکراین به وضوح دیده شد؛ جایی که هر دو طرف به طور مداوم متهم به استفاده از محتوای دستکاری شده برای شکل‌دهی به افکار عمومی جهانی شدند و تشخیص واقعیت از روایت‌های جهت‌مند رسانه‌ای برای ناظر بیرونی تقریباً غیرممکن شد.

ابعاد عملیاتی این تهدید در عرصه داخلی را می‌توان در قالب یک مدل تحلیلی سه‌مرحله‌ای تبیین کرد:

مرحله اول (تصویر): بلافاصله پس از یک حادثه امنیتی (مانند یک اعتراض یا درگیری)، کارزار سیلاب اطلاعاتی آغاز می‌شود. ده‌ها ویدئوی جعل عمیق به سرعت تولید و منتشر می‌شود. یکی، یک مقام محلی را نشان می‌دهد که با بغض، آمار تلفات را ده‌ها برابر آمار رسمی اعلام می‌کند. دیگری، یک «شاهد عینی» ساختگی است که نیروهای امنیتی را به شلیک مستقیم متهم می‌کند. ویدئوی سوم، یک «کارشناس» جعلی را به تصویر می‌کشد که حادثه را یک فاجعه داخلی معرفی می‌کند. این محتواهای احساسی و تکان‌دهنده، مرحله اول عملیات (تصویرسازی) را شکل می‌دهند.

مرحله دوم (انگاره): هم‌زمان، فایل‌های صوتی جعلی از مکالمات مسئولان منتشر می‌شود که در آن بر سر نحوه مدیریت بحران با یکدیگر نزاع می‌کنند. تحلیلگران جعلی در شبکه‌های اجتماعی این ویدئوها را به عنوان «اسناد انکارناپذیر» بازنشر کرده و انگاره «سرکوب سیستماتیک» یا «فروپاشی درونی» را تئوریزه می‌کنند.

مرحله سوم (رفتار): این حجم از محتوای بصری متناقض و به‌ظاهر مستند، مخاطب را

از توانایی تشخیص واقعیت خلع کرده و او را مستعد پذیرش روایت‌های هیجانی می‌کند و زمینه را برای کنش‌های میدانی فراهم می‌آورد.

در چنین آشوب اطلاعاتی، تلاش سخنگوی دولت یا رسانه ملی برای «تبیین» واقعیت، مانند فریاد زدن در طوفان است. روایت رسمی، دیگر مرجع اصلی نیست، بلکه به یکی از چندین گزینه موجود تبدیل شده که هرکدام «سند ویدئویی» خود را دارند. مخاطب که با تصاویر و صداهای متناقض بمباران شده، طبق «اثر حقیقت خیالی»،^۱ صرفاً به دلیل تکرار بالای یک روایت جعلی، ممکن است آن را به‌عنوان حقیقت بپذیرد (Hasher et al, 1977; 107-110; Pennycook et al, 2018). در نتیجه، تلاش نهادهای مسئول برای مدیریت بحران و حفظ آرامش عمومی، در نويز اطلاعاتی کارایی خود را از دست می‌دهد و عملاً جهاد تبیین در میدان، پیش از آنکه آغاز شود، شکست می‌خورد. این مکانیزم با جایگزین کردن «وضوح» با «اغتشاش»، محیطی را فراهم می‌کند که در آن حقیقت نه تنها شکست می‌خورد، بلکه اساساً بی‌معنا می‌شود.

۳-۴. بازنویسی حافظه جمعی از طریق جعل اسناد

جهاد تبیین در یکی از حیاتی‌ترین ابعاد خود، به‌مثابه یک «صیانت‌گر حافظه» عمل می‌کند و وظیفه آن پاسداری از روایت اصیل رویدادهای تاریخی سرنوشت‌ساز، به‌ویژه تاریخ انقلاب اسلامی و دوران دفاع مقدس، به‌عنوان سنگ‌بنای هویت ملی است. دشمنان انقلاب اسلامی همواره از طریق تحریف و وارونه‌نمایی تاریخ، به دنبال گسستن پیوند هویتی نسل‌های جدید با گذشته خود بوده‌اند، همان‌طور که در تلاش برای تزئین چهره ساواک و مخدوش کردن چهره امام علیه السلام و انقلاب در امپراتوری رسانه‌ای غرب مشهود است؛ اما فناوری جعل عمیق، این نبرد را وارد مرحله‌ای به مراتب خطرناک‌تر می‌کند؛ این فناوری، ماهیت تهدید را از «تحریف تفسیر» به «تولید سند جعلی» تغییر می‌دهد و به دشمن قابلیت «مهندسی حافظه جمعی» را می‌بخشد. دیگر سخن بر سر نقل قول گزینشی یا تحلیل مغرضانه نیست؛ جعل عمیق قادر است «شواهد» و «اسناد» صوتی و تصویری کاملاً

ساختگی از گذشته خلق کند، سخنانی که هرگز گفته نشده را در دهان شخصیت‌های تاریخی بگذارد و رویدادهایی که رخ نداده را با جزئیات بصری بازسازی نماید. قدرت هولناک این فناوری در «بازنویسی تاریخ» به بهترین شکل در پروژه هنری-تحقیقاتی هشداردهنده دانشگاه MIT با عنوان «در صورت وقوع فاجعه ماه»^۱ به اثبات رسید. این پروژه که با هدف صریح «ایجاد آگاهی انتقادی در میان عموم» طراحی شده بود، سخنرانی منتشرنشده‌ای از رئیس جمهور نیکسون را بازسازی کرد که برای اعلام شکست مأموریت آپولو ۱۱ تهیه شده بود. نتیجه، یک ویدئوی بی نقص بود که به شکلی تکان‌دهنده نشان داد چگونه مرز میان واقعیت تاریخی و جعل هنرمندانه در حال فروریختن است و مخاطبان را وادار کرد تا «آنچه را می‌بینند و می‌شنوند، زیر سؤال ببرند» (Arts at MIT, n.d).

در بستر تاریخ انقلاب اسلامی، این تهدید ابعادی جدی‌تر پیدا می‌کند. برای دهه‌ها، جریان‌های معاند با تحریف سخنان معروف امام خمینی^{علیه‌السلام} در بهشت زهرا، تلاش کرده‌اند روایتی مادی‌گرایانه از اهداف انقلاب ارائه دهند. حال تصور کنید ویدئویی جعل عمیق با کیفیت بالا از همان سخنرانی ساخته شود که در آن، امام^{علیه‌السلام} مبانی انقلاب را به گونه‌ای متناقض با اصول واقعی بیان می‌کنند. چنین «سند» جعلی، به سرعت می‌تواند تمام تلاش‌های چندین ساله برای تبیین حقیقت را بی‌اثر کرده و یک دروغ تاریخی را در حافظه جمعی رسوب دهد.

جعل عمیق با توانایی خود در خلق یک «تاریخ موازی» و مخدوش کردن اسناد گذشته، ارتباط عاطفی و فکری نسل جدید را با ریشه‌های هویتی خود قطع کرده و جهاد تبیین در حوزه تاریخ را که متکی بر سند و مدرک است، با چالش بنیادین «اصالت» مواجه می‌سازد و به این ترتیب، زمینه را برای فروپاشی هویتی از درون فراهم می‌کند.

۴-۴. فعال‌سازی گسل‌های اجتماعی و مهندسی قطبی‌سازی هویتی

جهاد تبیین در یکی از کارکردهای راهبردی خود، به دنبال تقویت «انسجام ملی» و ترمیم شکاف‌های اجتماعی از طریق ایجاد فهم مشترک و گفتگو است. این دکتترین بر این اصل استوار است که با تبیین دقیق می‌توان جامعه را حول منافع و ارزش‌های مشترک متحد ساخت

1. In Event of Moon Disaster

(آیت‌الله خامنه‌ای، بیانات، ۱۴۰۰/۱۲/۱۹). مکانیزم «مهندسی قطبی‌سازی» با استفاده از جعل عمیق، این فرآیند وحدت‌بخش را به‌طور مستقیم خنثی می‌کند. در این استراتژی، هدف، تولید مصنوعی نفرت و بی‌اعتمادی میان گروه‌های مختلف اجتماعی (اعم از قومی، مذهبی، سیاسی یا طبقاتی) است تا «گسل‌های اجتماعی» نهفته، فعال شده و به مرز انفجار برسند. فناوری جعل عمیق این امکان را فراهم می‌کند که از طریق انتساب گفتارهای تحریک‌آمیز و تقابلی به چهره‌های منتسب به یک گروه علیه گروه دیگر، چارچوب‌های ادراکی مبتنی بر تقابل و تعارض بازتولید شود. این مکانیزم با هدف قرار دادن عمیق‌ترین احساسات هویتی و تعصبات گروهی عمل کرده و با طراحی محتوایی که واکنش‌های احساسی آنی را برانگیزد، فرصت تفکر انتقادی را از مخاطب سلب می‌کند (Du Cluzel, 2022: 2-6; Poisant, 2021: 2-). برای مثال، در جریان درگیری‌های هند و پاکستان در سال ۲۰۲۵، از تصاویر و ویدئوهای تولیدشده با هوش مصنوعی برای دامن زدن به «احساسات فرقه‌ای» استفاده شد (Kava, 2025). ابعاد این تهدید برای کشوری با تنوع قومی و مذهبی ایران، بسیار جدی است. سناریوهای زیر تنها بخشی از پتانسیل ویرانگر آن را آشکار می‌سازد:

تشنه قومی: تصور کنید ویدئویی جعل عمیق از یک مقام مسئول فارسی‌زبان منتشر شود که با لحنی تحقیرآمیز، به یکی از اقوام شریف ایرانی توهین می‌کند. انتشار وسیع چنین ویدئویی می‌تواند در عرض چند ساعت، احساسات قومی را جریحه‌دار کرده و تلاش‌های چندین ساله برای وحدت ملی را نابود سازد.

تشنه مذهبی: سناریوی خطرناک‌تر، تولید ویدئویی جعلی از یک چهره مذهبی منتسب به یک مذهب است که در آن به مقدسات مذهب دیگر اهانت می‌کند. چنین محتوایی پتانسیل ایجاد یک بحران امنیتی تمام‌عیار را دارد.

در چنین فضای مسمومی که مملو از خشم و بی‌اعتمادی متقابل است، «جهاد تبیین» عملاً مخاطب خود را از دست می‌دهد. وقتی گروه‌های اجتماعی یکدیگر را به چشم تهدیدی برای بقای خود ببینند، دیگر گوش شنوایی برای پیام‌های وحدت‌بخش و تبیین‌های عقلانی باقی نمی‌ماند.

۴-۵. مشروعیت‌زدایی سیستمی از طریق انهدام دوگانه کارآمدی و اعتماد

در نقطه اوج تهاجم شناختی، پیچیده‌ترین مکانیزم، نه صرفاً تغییر روایت، بلکه انهدام هم‌زمان دو ستون اصلی مشروعیت نظام یعنی «کارآمدی» و «اعتماد» را به شیوه‌ای بنیان‌کن هدف قرار می‌دهد. این تهاجم یک راهبرد دومرحله‌ای است که در گام نخست، با تضعیف باور عمومی به دستاوردهای ملموس نظام، زمینه را برای گام دوم، یعنی آلوده ساختن کل فضای اطلاعاتی و نابود ساختن خود «امکان تشخیص حقیقت»، فراهم می‌آورد. جهاد تبیین که بر پایه ارائه «واقعیات» و «دستاوردها» برای تقویت امید بنا شده، در برابر این مکانیزم با یک چالش وجودی روبرو می‌شود. در مرحله اول، نوک پیکان حمله متوجه «کارآمدی» نظام است. برای این منظور، از دو تاکتیک مکمل بهره می‌برد: تحریف کامل و کوچک‌نمایی موزیانه (Poisant, 2021: 2-5).

در تاکتیک تحریف، یک موفقیت واقعی، از طریق یک سند جعلی، به یک شکست فاجعه‌بار تبدیل می‌شود. تصور کنید در آستانه بهره‌برداری از یک پروژه بزرگ ملی (مانند یک ماهواره بر)، ویدئویی جعل عمیق از مدیر پروژه منتشر می‌شود که در یک جلسه خصوصی «لورفته»، به وجود یک نقص فنی بزرگ یا فساد گسترده در پروژه «اعتراف» می‌کند. چنین محتوایی که در زمان بندی دقیق منتشر می‌شود، می‌تواند روایت قدرت و پیشرفت را به شکست تبدیل کرده و تمام تلاش‌ها برای تبیین اهمیت آن را در نطفه خفه سازد.

تاکتیک دوم، کوچک‌نمایی است، در این روش، اصل دستاورد انکار نمی‌شود، بلکه با قرار دادن آن در یک چارچوب مقایسه‌ای تحقیرآمیز، از ارزش تهی می‌گردد. برای مثال، پس از رونمایی از یک داروی پیشرفته بیوتکنولوژی، ویدئویی جعلی از یک «دانشمند ایرانی مقیم خارج» منتشر می‌شود که ضمن تأیید خبر، با لحنی دلسوزانه بیان می‌کند که «این تکنولوژی مربوط به ۲۰ سال پیش غرب است و به دلیل عوارض جانبی منسوخ شده». این پیام، با ایجاد تردید در کیفیت، حس افتخار ملی را به حس عقب ماندگی تبدیل کرده و کارکرد جهاد تبیین در حوزه روایت پیشرفت را فلج می‌سازد.

این حملات به کارآمدی، زمین بازی را برای مرحله دوم و ویرانگرتر آماده می‌کنند. در این فاز، دشمن از پدیده «سود سهام دروغ‌گو»^۱ بهره‌برداری می‌کند تا جهاد تبیین را با یک بن‌بست معرفت‌شناختی^۲ مواجه سازد (Chesney & Citron, 2019: 1785). با فراگیر شدن آگاهی عمومی از وجود جعل عمیق، هر فرد گناهکاری می‌تواند هرگونه شواهد واقعی علیه خود را به سادگی یک «جعل عمیق» بنامد. این مکانیزم یک حرکت گازانبری مرگبار را علیه حقیقت شکل می‌دهد: از یک سو، محتوای جعلی، اعتماد عمومی را سست می‌کند و از سوی دیگر، «سود سهام دروغ‌گو» به عاملان فساد اجازه می‌دهد تا اسناد واقعی افشاگرانه را با برچسب «دیپ‌فیک» بی‌اثر کنند. در چنین فضایی، اگر یک فایل صوتی واقعی از اذعان یک مقام به تخلف افشا شود، آن مقام می‌تواند با اطمینان در برابر دوربین‌ها قرار گرفته و اصالت آن سند را زیر سؤال ببرد. این وضعیت، جامعه را به سمت یک «سینسیزم یا کلبی مسلکی شناختی»^۳ سوق می‌دهد؛ حالتی از خستگی و بی‌اعتمادی مطلق که در آن شهروندان به این نتیجه می‌رسند که «هیچ چیز قابل باور نیست» و از تلاش برای تشخیص حقیقت دست می‌کشند (Kavanagh & Rich, 2018). این نقطه، یعنی مرگ اعتماد عمومی و فلج شدن قوه تشخیص، پیروزی نهایی در جنگ شناختی است؛ زیرا سیستمی که دیگر قادر به اثبات کارآمدی خود از طریق اسناد معتبر نباشد و نتواند دروغ را از راست برای مردمش متمایز کند، پایه‌های مشروعیت خود را از دست داده و از درون به شدت آسیب‌پذیر خواهد شد.

۴-۶. واکاوی مصادیق عینی: ردپای هوش مصنوعی در میدان جنگ شناختی ایران

برای پرهیز از انتزاعی شدن بحث جنگ شناختی مبتنی بر جعل عمیق، بررسی مصادیق واقعی و مستند از کاربست هوش مصنوعی در عملیات روانی علیه افکار عمومی ایران ضروری است. شواهد رسانه‌ای سال ۱۴۰۴ نشان می‌دهد که جعل عمیق از مرحله

1. Liar's Dividend

2. Epistemic Deadlock

۳. واژه «کلبی» از یک مکتب فلسفی در یونان باستان به نام «مکتب کلبیون» (Cynics) می‌آید. آن‌ها معتقد بودند که اکثر افراد تنها به دنبال منافع شخصی خود هستند و ادعاهایشان درباره فضیلت، شرافت و خدمت به دیگران، ریاکارانه و دروغین است.

«آزمایش رسانه‌ای» عبور کرده و به یک ابزار عملیاتی سازمان‌یافته برای تخریب اعتماد، قطبی‌سازی اجتماعی و مهندسی ادراک جمعی تبدیل شده است. یکی از بارزترین نمونه‌ها در آبان ماه همین سال رخ داد؛ جایی که انتشار ویدئویی ساختگی از بازرسی بدنی نامتعارف یک زن جوان توسط مأموران پلیس، به سرعت فضای مجازی را ملتهب کرد. اگرچه بررسی‌های فنی بعدی اثبات کرد که این ویدئو با استفاده از هوش مصنوعی تولید شده و ناهماهنگی‌های دیجیتال در حرکات بدن مشهود بود (مشرق نیوز، ۱۴۰۴/۰۸/۲۲)، اما دشمن با بهره‌گیری از اصل روان‌شناختی «اثر نخستین تصویر»،^۱ کوشید پیش از آنکه فرصتی برای تبیین عقلانی یا تکذیب رسمی فراهم شود، تصویری تکان‌دهنده از نقض حریم خصوصی و اخلاقی را در ذهن مخاطب حک کند؛ تصویری که حتی پس از افشای جعلی بودن آن، ردپای هیجانی‌اش در ناخودآگاه جمعی باقی ماند.

این الگوی «واقعیت‌سازی مصنوعی» در سناریوهای مدیریت وحشت و بحران‌سازی نیز با پیچیدگی بیشتری تکرار شده است. نمونه عینی آن، شایعه‌سازی پیرامون کشف «۷۴ جسد» در سد کرج هم‌زمان با کاهش سطح آب این سد بود. در این عملیات شناختی، ویدئویی ساختگی که اجساد را در کف سد به تصویر می‌کشید، به‌عنوان «سند» ارائه شد و با پیوند دادن آن به وقایع سال ۱۴۰۱، تلاش گردید تا ضمن بازنمایی زخم‌های اجتماعی و القای گزاره «جنایت پنهان حاکمیت»، اعتماد عمومی به نهادهای رسمی منهدم شود. هم‌زمان با این ماجرا، انتشار ویدئوهای جعلی دیگری نظیر برخورد تانکر سوخت با برج آزادی، تیراندازی در زاهدان و ادعای هک شدن دوربین‌های ترافیکی تهران توسط رژیم صهیونیستی، نشان داد که دشمن به دنبال ایجاد نوعی «فلج تحلیلی» در مخاطب است؛ وضعیتی که در آن مبارزان مداوم ذهن با تصاویر جعلی اما هراس‌ناک، قدرت تشخیص واقعیت را از جامعه سلب می‌کند (جهان نیوز، ۱۴۰۴/۸/۲۷).

در سطحی دیگر، جنگ شناختی با استفاده از هوش مصنوعی به دنبال «تصویرسازی کاذب از فروپاشی درونی» و «قدرت‌نمایی مجازی برای اپوزیسیون» بوده است. انتشار

ویدئوهایی از افرادی با لباس ارتش جمهوری اسلامی که پرچم شیر و خورشید در دست داشته و یا در مقابل جمعیت‌های ساختگی سخنرانی می‌کردند، تلاشی برای القای این توهم بود که بدنه نیروهای مسلح به جریان سلطنت طلب پیوسته‌اند. با این حال، افشاگری‌های بعدی، از جمله اعترافات عوامل شبکه «من‌وتو» و گزارش‌های سیتیزن‌لب و هآرتص، پرده از واقعیتی تلخ برداشت: بسیاری از این تصاویر نه در میدان واقعی، بلکه به صورت صحنه‌سازی و یا با کمک هوش مصنوعی تولید شده بودند تا برای جریانی که فاقد پایگاه میدانی است، اعتبار و محبوبیت مجازی خلق کنند (باشگاه خبرنگاران جوان، ۱۴۰۴/۸/۲۵). مجموع این شواهد اثبات می‌کند که در عصر جعل عمیق، جهاد تبیین با دشمنی روبروست که دیگر فقط «روایت» نمی‌سازد، بلکه «سند» تولید می‌کند؛ اسنادی که اگرچه جعلی‌اند، اما قدرت تخریبی آن‌ها بر ادراک عمومی، نیازمند راهکارهای دفاعی نوین و فراتر از تکذیبیه‌های سنتی است.

۵. راهبردهای مقابله: کارآمدسازی جهاد تبیین در عصر جعل عمیق

با توجه به ماهیت پیچیده، چندلایه و غیرخطی تهدید جعل عمیق در جنگ شناختی، مقابله مؤثر با آن مستلزم چارچوبی فراتر از اقدامات واکنشی و تک‌ساحتی است. از این رو، راهبردهای این پژوهش برای کارآمدسازی دکترین «جهاد تبیین» بر مبنای تلفیق تحلیل مضمون کیفی بیانات مقام معظم رهبری پیرامون الزامات جهاد تبیین و الگوی جهانی «دفاع در عمق»^۱ صورت‌بندی شده است.

تحلیل بیانات رهبر انقلاب نشان می‌دهد که جهاد تبیین ناظر به سه ساحت مکمل است: مهار ابزار تحریف،^۲ ایمن‌سازی ادراک عمومی و کنشگری فعال در میدان روایت (آیت‌الله خامنه‌ای، بیانات، ۱۴۰۰/۷/۵، ۱۴۰۰/۹/۲۱). این سه ساحت با لایه‌های

۱. الگوی جهانی «دفاع در عمق» ریشه در اسناد امنیت سایبری ایالات متحده دارد (NIST, SP-800-53-53, 2020) و در مطالعات امنیت شناختی برای مقابله چندلایه با اطلاعات نادرست اقتباس شده است (Klein & Hoffman, 2021).

۲. «اگر جریان تحریف شکست بخورد، جریان تحریم قطعاً شکست خواهد خورد؛ زیرا که عرصه، عرصه‌ی جنگ اراده‌ها است» (آیت‌الله خامنه‌ای، بیانات، ۱۰/۰۵/۱۳۹۹).

«فناوران-حقوقی»، «انسانی-آموزشی» و «راهبردی-نهادی» در الگوی دفاع در عمق انطباق کامل دارد. بر این اساس، راهبردهای پیشنهادی پژوهش در سه سطح زیر سامان یافته‌اند:

۵-۱. سطح فنی-حقوقی:

نخستین لایه در الگوی «دفاع در عمق» شناختی، ایجاد محیطی است که در آن هزینه تولید جعل افزایش یافته و امکان تشخیص آن برای مخاطبان و نهادهای رسمی تسهیل شود. در برابر راهبرد «تخریب اعتماد»، پاسخ دفاعی باید بر ایجاد یک «زیرساخت فنی و حقوقی اعتماد» متمرکز گردد. این زیرساخت با توسعه فناوری‌های بومی تشخیص جعل عمیق آغاز می‌شود. اتکای صرف به ابزارهای خارجی - علاوه بر تعارض با دکترین «قوی شدن و اعمال حاکمیت بر فضای مجازی» مورد تأکید رهبری (همان، ۱۴۰۰/۱/۱؛ ۱۴۰۴/۷/۲۷) - از نظر فنی نیز ناکارآمد است؛ زیرا پژوهش‌ها نشان می‌دهد بسیاری از مدل‌های جهانی بر داده‌های غربی آموزش دیده‌اند و در تحلیل زبان‌ها و بافت‌های فرهنگی خاص با خطا مواجه می‌شوند (Naous & Xu, 2025). از این رو، توسعه الگوریتم‌های بومی حساس به ظرایف زبانی و فرهنگی ایران ضرورتی راهبردی است.

در گام بعدی، این زیرساخت از طریق پیاده‌سازی راهبرد پیش‌دستانه «احراز اصالت» محتوا تکمیل می‌گردد. ایجاد «سامانه ملی احراز اصالت محتوای رسمی» مبتنی بر امضای دیجیتال (نظیر پروتکل C2PA)، امکان راستی‌آزمایی سریع را برای شهروندان فراهم می‌سازد و پدیده «سود سهام دروغ‌گو» را خنثی می‌کند. نهایتاً، این بنیان فنی باید با یک «قانون بازدارنده و هوشمند» تقویت شود؛ قانونی که ضمن تفکیک میان طنز و تخریب، با تعیین مجازات‌های مؤثر و شفاف‌سازی مسئولیت پلتفرم‌ها، هزینه اقدامات مخرب را به شکل معناداری افزایش دهد (ر.ک: السان و دهستانی، ۱۴۰۱).

۵-۲. سطح آموزشی-رسانه‌ای:

پس از ایجاد استحکامات فنی، لایه دوم دفاعی بر ساخت یک «سپر انسانی» استوار است تا جامعه از یک قربانی منفعل به مشارکت‌کننده فعال در فرآیند اعتبارسنجی تبدیل شود. در سطح عمومی، هدف اصلی گذار از سواد رسانه‌ای سنتی به «تاب‌آوری شناختی» است؛ چراکه فناوری

جعل عمیق با هدف قرار دادن اعتماد شناختی انسان به ادراکات دیداری و شنیداری به عنوان «واقعیت غیرقابل مناقشه»، عملاً توان ابزارهای سنتی تشخیص را از کار می‌اندازد. برای خنثی‌سازی این تهدید و تحقق منویات مقام معظم رهبری مبنی بر «بصیرت‌افزایی عمومی» (آیت‌الله خامنه‌ای، بیانات، ۱۳۹۶/۱۰/۶، ۱۴۰۱/۵/۵، ۱۴۰۲/۹/۸)، لازم است فرهنگ «تأمل پیش از واکنش» در جامعه نهادینه شود. این رویکرد که در روانشناسی شناختی با عنوان فعال‌سازی «تفکر سیستم ۲» (Kahneman, 2011) شناخته می‌شود، به معنای آموزش جامعه برای ایجاد یک وقفه ارادی و عبور از هیجانات لحظه‌ای به تحلیل منطقی است. هم‌زمان، برای ایمن‌سازی ذهنیت عمومی پیش از وقوع حمله، باید از راهبرد «پیش‌افشاگری» بهره برد. این راهبرد که ریشه در نظریه علمی «واکسیناسیون ذهنی» دارد (Lewandowsky et al. 2020)، بیانگر آن است که اگر شهروندان پیشاپیش با نمونه‌های شبیه‌سازی شده و تکنیک‌های فریب دشمن آشنا شوند، در لحظه مواجهه با بحران واقعی، به جای پذیرش منفعلانه، نوعی «شک مقدس» و ایمنی ذهنی از خود نشان خواهند داد.

در تکمیل این دفاع عمومی، عرصه نخبگانی و رسانه‌ای کشور نیازمند تحولی بنیادین در شیوه نقش‌آفرینی است. کنشگران این میدان باید، بر پایه تعبیر رهبر انقلاب، از قالب مبلغ سنتی فراتر روند و در جایگاه «افسران جنگ نرم» (آیت‌الله خامنه‌ای، بیانات، ۱۳۹۹/۱۲/۲۱)، مهارت‌های نوین نبرد شناختی را فراگیرند.

در این الگو، افسر جنگ نرم تنها یک فعال رسانه‌ای نیست؛ او شخصیتی است با صلابت و تاب‌آوری روانی بالا که حتی اگر در مسیر مبارزه «فحش ناموسی بشنود، از میدان خارج نمی‌شود» (همان، ۱۴۰۲/۰۳/۱۴). چنین پایداری زمانی ضروری‌تر می‌شود که دشمن با شتابی فزاینده به تولید و تزریق واقعیت‌های ساختگی می‌پردازد. در چنین شرایطی، انجام «فریضه قطعی و فوری جهاد تبیین» (همان، ۱۴۰۰/۱۱/۱۹) به معنای صرف تکذیب خبر نیست؛ بلکه مأموریت اصلی شبکه نخبگانی آن است که ایمان و امید جامعه را تقویت کرده و با خنثی‌سازی راهبردهای دشمن در شبهه‌افکنی و یأس‌آفرینی، میدان ادراکات عمومی را بازپس گیرند (همان، ۱۴۰۲/۳/۱۴).

تحقق این مأموریت، مستلزم تسلط کنشگران بر مهارت «مدیریت بحران روایت» است؛ مهارتی که آنان را قادر می‌سازد تا در برابر روایت‌های تحریف‌شده دشمن، «پاداروایت» تولید کنند. پاداروایت، روایتی تهاجم‌کننده و امیدبخش است که تنها به رد محتوای جعلی بسنده نمی‌کند، بلکه با افشای نیت پشت پرده و بافت سیاسی-امنیتی حمله، ماهیت دشمن را برای مخاطب آشکار می‌سازد.

۵-۳. سطح راهبردی-نهادی:

پایدارترین لایه دفاعی در برابر جعل عمیق، فراتر از ابزار و آموزش، تغییر در تفکر و ساختار حکمرانی است. هدف غایی در این سطح، دستیابی به «برتری شناختی» است؛ وضعیتی که در آن نظام حاکمیت به جای آنکه دائماً در حال پاسخگویی به حملات دشمن باشد، خود تعیین‌کننده زمین بازی و روایت غالب است. این تحول راهبردی با تغییر دکترین از حالت تدافعی به تهاجمی آغاز می‌شود. بزرگ‌ترین آسیب‌پذیری فعلی، تقلیل «جهاد تبیین» به «پاسخگویی به شبهات» است که عملاً نظام را در موضع انفعال و در زمین طراحی شده توسط دشمن قرار می‌دهد. مطابق با منطق تهاجمی جهاد تبیین در اندیشه رهبر انقلاب، راهکار اصلی باید «روایت‌سازی پیش‌دستانه» باشد (همان، ۱۴۰۰/۹/۲۱). این مهم از طریق راهبرد «اشباع روایت» و «شفافیت ساختاری» محقق می‌شود؛ چراکه جعل عمیق تنها در ابهام و بی‌اعتمادی رشد می‌کند. انتشار پیش‌دستانه داده‌ها و گزارش‌های عملکرد، اکوسیستم شایعه را خشک کرده و اعتماد عمومی را بازسازی می‌کند.

این رویکرد تهاجمی، نیازمند «چابک‌سازی ساختاری» نیز هست، چراکه سرعت بالای انتشار اطلاعات جعلی، ساختارهای کند دیوان‌سالاری را ناکارآمد کرده است. از این رو، ایجاد یک «قرارگاه فرماندهی یکپارچه»، چابک و فرانهادی برای بسیج هماهنگ تمام ظرفیت‌های رسانه‌ای در لحظات بحرانی، امری ضروری است.

در نهایت باید پذیرفت که بنیان این دفاع راهبردی، شناسایی، اعتباربخشی و بهره‌گیری از چهره‌های مورد اعتماد مردم به‌عنوان سرمایه‌های انسانی اعتمادساز است. در عصری که فناوری قادر به جعل واقع‌گرایانه چهره و صداست، تنها تکیه‌گاه مطمئن، «صداقت آزموده

شده» است؛ بنابراین، راهبرد پایدار باید بر شناسایی و تقویت شخصیت‌های مورد وثوق جامعه متمرکز شود تا در طوفان‌های شناختی، نقش قطب‌نمای حقیقت را برای افکار عمومی ایفا کند.

نتیجه‌گیری

نتایج حاصل از این پژوهش نشان می‌دهد که فناوری «جعل عمیق» در میدان جنگ شناختی، کارکردی فراتر از یک ابزار پیشرفته برای تولید دروغ پیدا کرده و به سلاحی راهبردی جهت انهدام مرجعیت حقیقت تبدیل شده است. یافته‌ها گویای آن است که دشمن با بهره‌گیری از پنج مکانیزم «فرسایش مرجعیت»، «سیلاب اطلاعاتی»، «تحریف حافظه»، «فعال‌سازی گسل‌ها» و «مشروعیت‌زدایی»، در پی خلق یک بن‌بست معرفتی است؛ وضعیتی که در آن جامعه توانایی تمیز سره از ناسره را از دست داده و به ورطه کلبی مسلکی شناختی سقوط می‌کند. در چنین فضای مسمومی، اگر زمینه پذیرش حقیقت نابود شود، دکترین جهاد تبیین نیز کارآمدی خود را از دست خواهد داد.

برای خنثی‌سازی این سناریو و عبور از رویکرد انفعالی، استقرار الگوی «دفاع در عمق» در لایه‌های به‌هم پیوسته ضروری است. این راهبرد ابتدا با توسعه زیرساخت‌های فنی و حقوقی آغاز می‌شود که از طریق ایجاد سامانه‌های بومی احراز اصالت و وضع قوانین بازدارنده، هزینه تولید جعل را افزایش داده و امکان راستی‌آزمایی فوری را برای شهروندان فراهم می‌آورد. در امتداد این لایه فنی، ضروری است نظام آموزشی و رسانه‌ای با گذار از سواد رسانه‌ای سنتی به سمت واکسیناسیون ذهنی جامعه و تربیت افسران جنگ نرم مسلط بر تولید پاداروایت، یک سپر شناختی مستحکم ایجاد کند. نهایتاً این چرخه دفاعی با تغییر رویکرد راهبردی حاکمیت به سمت شفافیت و روایتگری پیش‌دستانه تکمیل می‌شود تا با پر کردن خلأهای اطلاعاتی، فرصت رشد شایعات و جعلیات از بین برود.

درنهایت، جوهره اصلی یافته‌های این مقاله آن است که در عصر هوش مصنوعی، مؤثرترین راه برای مقابله با فناوری‌های فریب، تکذیب کلامی نیست، بلکه پایدارترین شکل جهاد تبیین، کاهش شکاف میان ادعا و واقعیت از طریق کارآمدی و صداقت‌ساختاری

است. نظام اسلامی تنها زمانی در برابر امواج جعل عمیق به تاب‌آوری شناختی مؤثری دست می‌یابد که حقیقت موجود در متن جامعه، گویاتر از هر تصویر برساخته مجازی باشد.

تشکر و سپاسگذاری

بدین وسیله از تمام پژوهشگرانی که مطالعاتشان در این پژوهش به کار رفت، صمیمانه سپاسگزاری می‌شود.

تعارض منافع

این مطالعه برای نویسنده هیچ گونه تضاد منافی به همراه نداشته است.

منابع مالی

این پژوهش هیچ کمکی از سازمان‌های تأمین مالی عمومی، تجاری یا غیرانتفاعی دریافت نکرده است.

کتابنامه:

- السان، مصطفی و سوور دهستانی (۱۴۰۱). جنبه‌های حقوقی جعل عمیق. تحقیقات حقوقی، ۲۵ (۹۹)، ۱۹۳-۲۱۸.
- باشگاه خبرنگاران جوان (۲۵ آبان ۱۴۰۴). ارتش فیک پهلوی داد منوورا هم درآورد. دسترسی در: yjc.ir/00bs76
- بیانات آیت‌الله خامنه‌ای، دسترسی در: <https://farsi.khamenei.ir>
- جهان نیوز (۲۷ آبان ۱۴۰۴). مأموریت شایعه‌سازی با هوش مصنوعی / از دختر برهنه تا کشف اجساد در سد کرج. دسترسی در: jahannews.com
- خبرآنلاین (۱۳۹۷). «پشت پرده پیام منتشرشده با صدای رهبر انقلاب درباره سرکوب مردم چه بود؟». دسترسی در: khabaronline.ir/x8MZp
- ذوعلم، علی (۱۴۰۱). «جهاد تبیین: مقدمه‌ای برای اصلاح، تحول و مطالبه». یادداشت منتشر شده در پایگاه اطلاع‌رسانی دفتر مقام معظم رهبری، دسترسی در: <https://khl.ink/f/49982>
- صلح میرزایی، سعید (۱۴۰۰). جهاد تبیین. تهران، انتشارات انقلاب اسلامی.
- مشرق نیوز (۲۳ آبان ۱۴۰۴). هوش مصنوعی چگونه ابزار جنگ رسانه‌ای شده است؟. دسترسی در: mshrg.ir/1764091
- Allyn, B. (2022, March 16). Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn. NPR. <https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia>
- Biddle, S. (2023, March 6). U.S. Special Forces want to use deepfakes for psy-ops. The Intercept. <https://theintercept.com/2023/03/06/pentagon-socom-deepfake-propaganda/>
- Boyd, J. R. (1987). A Discourse on Winning and Losing. Maxwell Air Force Base, AL: Air University Library.
- Chesney, B. & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753-1820. <https://doi.org/10.15779/Z38RV0D15J>
- Clausewitz, C. von. (1976). On war (M. Howard & P. Paret, Eds. & Trans). Princeton University Press.
- Deppe, C. & Schaal, G. S. (2024). Cognitive warfare: A conceptual analysis of the NATO ACT cognitive warfare exploratory concept. Frontiers in Big Data, 7, 1452129. <https://doi.org/10.3389/fdata.2024.1452129>

- Devilliers, L. (2021). Désinformation: Les armes de l'intelligence artificielle. *Pour la Science, Intelligence Artificielle et Artifices Intelligents*, 523, 26–33.
- Du Cluzel, F. (2022). Cognitive warfare: The future of cognitive dominance (Report No. NATO-CSO-CW 2022-03-01). North Atlantic Treaty Organization, Science and Technology Organization.
- Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. In *Advances in Neural Information Processing Systems 27* (pp. 2672–2680). MIT Press.
- Hasher, L., Goldstein, D. & Toppino, T. (1977). Frequency and the conference of referential validity. *Journal of Verbal Learning and Verbal Behavior*, 16(1), 107–112. [https://doi.org/10.1016/S0022-5371\(77\)80012-1](https://doi.org/10.1016/S0022-5371(77)80012-1)
- Henschke, A. (2025). Cognitive warfare: Grey matters in contemporary political conflict. Routledge. <https://doi.org/10.4324/9781003126959>
- Kahneman, D. (2011). *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.
- Kava, S. (2025, June 4). Deepfakes, voice clones and AI images amplified disinformation on India-Pak conflict. *The News Minute*. <https://www.thenewsminute.com/news/deepfakes-voice-clones-and-ai-images-amplified-disinformation-on-india-pak-conflict>
- Kavanagh, J. & Rich, M. D. (2018). Truth decay: An initial exploration of the diminishing role of facts and analysis in American public life. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2314.html
- Khan, I, Khan, K. & Ahmad, A. (2025). A comprehensive survey of deepfake generation and detection techniques in audio-visual media. *ICCK Journal of Image Analysis and Processing*, 1(2), 73–95. <https://doi.org/10.62762/JIAP.2025.431672>
- Klein, G. & Hoffman, R. R. (2021). Defending cognitive security: Applying defense-in-depth principles to information environments. In *Proceedings of the NATO Strategic Communications Conference*. NATO Strategic Communications Centre of Excellence.
- L Lewandowsky, S, Ecker, U. K. H, & Cook, J. (2017). Beyond misinformation: Understanding and coping with the “post-truth” era. *Journal of Applied Research in Memory and Cognition*, 6(4), 353–369. <https://doi.org/10.1016/j.jarmac.2017.07.008>
- Lewandowsky, S, Ecker, U. K. H, Seifert, C. M, Schwarz, N, & Cook, J. (2012). Misinformation and its correction: Continued influence and successful debiasing.

- Psychological Science in the Public Interest, 13(3), 106–131.
<https://doi.org/10.1177/1529100612451018>
- Mervosh, S. (2019, May 24). Distorted videos of Nancy Pelosi spread on Facebook and Twitter, helped by Trump. The New York Times.
<https://www.nytimes.com/2019/05/24/us/politics/pelosi-doctored-video.html>
- Naous, T, & Xu, W. (2025). On the origin of cultural biases in language models: From pre-training data to linguistic phenomena. arXiv preprint arXiv:2501.04662. Available at: <https://arxiv.org/abs/2501.04662>
- National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (Special Publication No. 800-53 Rev. 5). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-53r5>
- NATO Allied Command Transformation. (n.d). Cognitive warfare. Retrieved October 30, 2025, from <https://www.act.nato.int/activities/cognitive-warfare/>
- Nye, J. S, Jr. (2004a). Soft power: The means to success in world politics. PublicAffairs.
- Nye, J. S, Jr. (2004b). The decline of America’s soft power. Foreign Affairs, 83(3), 1-13.
- Paul, C. & Matthews, M. (2016). The Russian “firehose of falsehood” propaganda model: Why it might work and options to counter it. RAND Corporation. <https://www.rand.org/pubs/perspectives/PE198.html>
- Pennycook, G, Cannon, T. D, & Rand, D. G. (2018). Prior exposure increases perceived accuracy of fake news. Journal of Experimental Psychology: General, 147(12), 1865–1880. <https://doi.org/10.1037/xge0000465>
- Poisant, D. (Ed). (2021). Cognitive warfare: A battle for the brain (Report No. STO-MP-HFM-334). NATO Science and Technology Organization.
- United Nations, Executive Office of the Secretary-General. (2023). Information integrity on digital platforms (Our Common Agenda Policy Brief 8). United Nations. <https://doi.org/10.18356/27082245-31>
- Vosoughi, S, Roy, D, & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Elsan, M., & Dehestani, S. (2022). Legal aspects of deepfake. Legal Research Quarterly, 25(99), 193–218. doi: 10.52547/jlr.2022.229466.2369
- Khabar Online. (2018, August 15). Pasht-e parde-ye payām-e montasher shode bā sedā-ye rahbar-e enghelāb darbāre-ye sarkoub-e mardom chi bood? [What was

- behind the published message with the voice of the Supreme Leader about the suppression of people?]. Retrieved from <https://khabaronline.ir/x8MZp>
- Khamenei.ir. (n.d.). Bayanāt [Statements]. Retrieved from <https://farsi.khamenei.ir>
- Mashregh News. (2025, November 14). How artificial intelligence has become a tool of media war. Retrieved from <https://mshrgn.ir/1764091>
- Solehmirzaei, S. (2021). Jahād-e tabyin [The jihad of clarification]. Tehran: Enteshārāt-e Enghelāb-e Eslāmī.
- Young Journalists Club (YJC). (2025, November 16). Artēsh-e fik-e Pahlavi dād-e Manoto rā ham dar āvard [The fake Pahlavi army also shut down Manoto]. Retrieved from <https://yjc.ir/00bs76>
- Zoualim, A. (2022). ‘Jahād-e tabyin’; moghadameh-ī barā-ye eslāh, tahavvol va matālebeh [‘The jihad of clarification’; an introduction to reform, change, and demand]. Khamenei.ir. Retrieved from <https://khl.ink/f/49982>