Security Horazions

Validation of the strategic deception model with Offensive Approach to Intelligence

Ehsan Kiani[1]| Hadi Tajik[2] | Mehdi Firouzkouhi[3]

1. Corresponding Author: Phd of Middle East Studies. University of Imam Hussein, Tehran, Iran. Email: e1386k@gmail.com
2. Associate Professor, University of Imam Hussein, Tehran, Iran
3. Associate Professor, University of Imam Hussein, Tehran, Iran

Volume info

Vol. 18
Series: 68
Autumn 2025
P.P: 11-38

Article Type

Research Paper

Article History

Received:
2024-01-31
Revised:
2025-03-29
Accepted:
2025-08-20
Published:
2025-11-29

ISSN – E-ISSN

ISSN: 2538-1857
E-ISSN: 2645-5250

Abstract

Adopting an offensive approach to intelligence is one of the issues that has not received much attention in the foreign policy of the Islamic Republic of Iran. This should be taken seriously, especially regarding the Hybrid war against Iran at hard and soft power, as well as in various security, economic, military and diplomatic fields. Due to the necessity of this issue, in this research, an offensive approach to intelligence has been tried from the perspective of strategic deception. In this regard, a definition of offensive approach has been tried first. Then, according to the literature on deception, a strategic deception model with an offensive Intelligence approach has be formulated. In the next step, to increase the validity of the final Pattern, this model is submitted to the opinion of elites to measure its validity and reliability. These elites included people who had scientific or practical experience of working in the country's foreign policy in various agencies. In the end, the components that had a stronger evaluation formed the final model.

Keywords: Strategic deception, information invasion, foreign policy

Cite this Article: Kiani, E., Tajik, H., & Firouzkouhi, M. (2025). Validation of the strategic deception model with Offensive Approach to Intelligence. Security Horizons, 18(68), 11-38.
DOR: 20.1001.1.25381857.1404.18.68.1.5

OPEN ACCESS

Publisher: Imam Hossein University.

«آفاق امنیت»

اعتبارسنجی الگوی فریب راهبردی با رویکرد تهاجم اطلاعاتی

احسان کیانی[1] | هادی تاجیک[2] | مهدی فیروزکوهی[3]

۱. نویسنده مسئول: دکترای مطالعات خاورمیانه، دانشگاه امام حسین(ع)، تهران، ایران، Email: e1386k@gmail.com

۲. استادیار دانشگاه امام حسین(ع)، تهران، ایران

۳. استادیار دانشگاه امام حسین(ع)، تهران، ایران.

سال و شماره

سال ۱۸ ، پیاپی: ۶۸

پاییز ۱۴۰۴

صص: ۳۸-۱۱

نوع مقاله

مقاله پژوهشی

سابقه مقاله

تاریخ دریافت: ۱۴۰۲/۱۱/۱۱

تاریخ بازنگری: ۱۴۰۴/۰۱/۰۹

تاریخ پذیرش: ۱۴۰۴/۰۵/۲۹

تاریخ انتشار: ۱۴۰۴/۰۹/۰۸

شاپا چاپی و الکترونیکی

شاپا چاپی: ۱۸۵۷-۲۵۳۸

الکترونیکی: ۵۲۵۰-۲۶۴۵

چکیده

اتخاذ رویکرد تهاجمی به اطلاعات از مسائلی است که در سیاست خارجی جمهوری اسلامی ایران، چندان مورد توجه قرار نگرفته است. این امر به خصوص ناظر به جنگ ترکیبی علیه ایران در سطوح سخت، نیمه‌سخت و نرم و هم‌چنین در حوزه‌های گوناگون امنیتی، اقتصادی، نظامی و دیپلماتیک، باید جدی گرفته شود. ناظر به ضرورت این موضوع، در این پژوهش سعی شده تا رویکرد تهاجمی به اطلاعات از منظر فریب راهبردی، مورد بررسی قرار بگیرد. در این راستا ابتدا سعی شده تعریفی از رویکرد تهاجمی ارائه شود. سپس ناظر به ادبیات موضوع فریب، مدل فریب راهبردی با رویکرد تهاجم اطلاعاتی تدوین شود. در مرحله بعد، برای افزایش اعتبار الگوی نهایی، این مدل به نظرخواهی نخبگان گذاشته شده تا روایی و پایایی آن سنجیده شود. این نخبگان، شامل افرادی بوده‌اند که تجربه علمی یا عملی از فعالیت در زمینه سیاست خارجی کشور در نهادهای مختلف داشته‌اند. در پایان، مؤلفه‌هایی که دارای ارزیابی قوی‌تری بوده‌اند، الگوی نهایی را شکل داده‌اند.

کلیدواژه‌ها: فریب راهبردی، تهاجم اطلاعاتی، سیاست خارجی، رویکرد آفندی

استناد: کیانی، احسان، تاجیک، هادی، و فیروزکوهی، مهدی. (۱۴۰۴). اعتبارسنجی الگوی فریب راهبردی با رویکرد تهاجم اطلاعاتی. فصلنامه آفاق امنیت، ۱۸(۶۸)، ۱۱-۳۸.

DOR: 20.1001.1.25381857.1404.18.68.1.5

ناشر: دانشگاه جام امام حسین(ع).

مقدمه

بروز غافل‌گیری را می‌توان یکی از مهم‌ترین تهدیدات جامعه اطلاعاتی و ساختارهای سیاسی قلمداد کرد. یکی از مسیرهای سلبی برای کاهش این تهدید، سیاست‌های پدافندی از طریق گسترش اِشراف و احاطه اطلاعاتی بر محیط امنیتی کشور است. ولی مسیر ایجابی و پایدارتر، می‌تواند پیگیری یک سیاست آفندی برای تهاجم به دستگاه محاسباتی حریف یا دشمن باشد. یکی از روش‌های این سیاست تهاجمی، طراحی فریب راهبردی به هدف ایجاد تصورات نادرست و انحراف توجه حریف از اهداف واقعی باشد. به این ترتیب، با ارائه داستانی مجعول از مسیرهایی که برای رقیب، باورپذیر محسوب شود، به اختلال در سیستم‌های اطلاعاتی و تصمیم‌گیری وی مبادرت ورزد. توجه به این نکته، از این منظر مهم‌تر تلقی می‌شود که فریب در شرایطی که دیگر مؤلفه‌های قدرت در وضعیتی نسبتاً برابر باشند، نقش تعیین‌کننده‌ای در تغییر موازنه نیروها ایفا می‌کند و می‌تواند پیروزی را سریع‌تر و با هزینه‌ای کمتر به ارمغان بیاورد. به همین دلیل، طرفی که در موقعیت سخت‌افزاری ضعیف‌تری است، انگیزه بیشتری برای کاربرد فریب دارد. به همین دلیل قدرت‌های منطقه‌ای مانند ایران که در قیاس با ابرقدرت‌های جهانی مانند آمریکا، از توان نظامی کمتری برخوردار هستند، اهتمام بیشتری به تهاجم اطلاعاتی دارند و لازم است که استفاده از روش‌های نرم‌افزاری برای برتری اطلاعاتی را جدی‌تر بگیرند. در این خصوص می‌توان به گزاره کهن ولی هنوز مهم ماکیاولی اشاره نمود که درباره استفاده از فریب در شرایطی که امکان زور عریان وجود نداشته باشد، تصریح می‌کند:«شهریارانی موفق به انجام کارهای بزرگ شده‌اند که اعتنای چندانی به وفای عهد و قول نداشته، با زیرکی و حیله‌گری موفق شده‌اند مستولی گردند»(Machiavelli, 2013).

کوچک‌نمایی ضعف خودی و قوت رقیب و در مقابل بزرگ‌نمایی ضعف دشمن و قوت خودی از جمله مؤلفه‌های فریب در جهت ایجاد رعب در پایگاه نیروهای دشمن در قرون هفده و هجدهم میلادی بود که آن را دوران فریب سنتی می‌نامند. ولی جنگ‌های جهانی اول و دوم با توجه به توسعه فناوری ارتباطات به خصوص رادیو و امکان شنود، تکنیک‌های فریب را ارتقا داد. برای مثال شناسایی ماشین رمز آلمان نازی توسط انگلیسی‌ها و ارائه رمز غلط به آن‌ها از جمله

دلایل شکست آلمان در اروپای غربی بود. در این راستا، بسیاری از فرماندهان با ارائه اطلاعات غلط به طرف شنودکننده، وی را فریب می‌دادند (Ebrahimi, 2007). عملیات فریب تا جنگ‌های جهانی اول و دوم عمدتاً در حوزه نظامی، قابل ردگیری بود. فریب راهبردی شوروی توسط آلمان با معاهده عدم تجاوز در اوت ۱۹۳۹ از مشهورترین این موارد می‌باشد. شوروی با وجود استقرار نیروهای نظامی آلمان در نزدیکی مرز بالکان، به واسطه تبلیغات نازی‌ها مبنی بر حمله قریب‌الوقوع آلمان به بریتانیا، درصدد مقابله برنیامد که به غافلگیری شوروی از تهاجم آلمان در نبرد مشهور به باربروسا انجامید(Ebrahimi, 2007).

با آغاز جنگ سرد، فریب راهبردی از حوزه نظامی به حوزه امنیتی‌اطلاعاتی نیز تسری یافت. تهاجم اطلاعاتی با بهره‌مندی از اِشراف اطلاعاتی به هدف تخریب یا تغییر دستگاه محاسباتی طرف مقابل موجب سازمان‌دهی فریب به مثابه زنجیره‌ای از عملیات‌های به هم پیوسته امنیتی شده و کارکرد آن را پایدارتر می‌نماید.

ادبیات نظری

برای بررسی مفهوم تهاجم اطلاعاتی ابتدا سعی می‌شود سابقه تعابیر و تعاریف نزدیک به این مفهوم در دیگر متون بررسی شود. مطالعه مرور ادبیات مرتبط با مفهوم تهاجم اطلاعاتی، تعاریف متعدد ولی نزدیک به یکدیگر را نشان می‌دهد.

۱- مقاله «تهاجم اطلاعاتی: نبرد اطلاعاتی در ۲۰۲۵» به پیش‌بینی امنیت سایبری دولت آمریکا در قرن بیست‌ویکم پرداخته و رویکرد تهاجمی در اطلاعات را نوعی برتری اطلاعاتی قلمداد کرده که در بستر فناوری اطلاعات، به **اختلال در فرآیند شناختی هدف** منجر می‌شود (Stein, 1996, 7).

۲- پژوهش‌گران مؤسسه رَند در فصل پایانی کتاب «ارزیابی راهبردی: تغییر نقش اطلاعات در جنگ» که به تبیین تأثیر فناوری‌های اطلاعاتی بر نبردهای نظامی پرداخته، تهاجم اطلاعاتی را **ضربه مخفیانه به نخبگان** دانستند (Libicki, 1999, 450).

۳- مقاله «دست‌یابی به تاب‌آوری اطلاعاتی» به تبیین چگونگی مقابله با تهاجم سایبری می‌پردازد و برای مقابله، تاکتیک «دفاع از عمق» را پیشنهاد می‌دهد. بدین معنا که به جای رویکرد واکنشی تشخیص و مقابله با تهاجم، در پی ارزیابی و سپس اقدام پیش‌دستانه در عمق راهبردی فراتر از مرزهای سیستم باشیم. بنابراین مشخص می‌شود تهاجم اطلاعاتی **حمله‌ای به درون سیستم** قلمداد می‌شود (Zavidniak, 1999, 8).

۴- نویسنده کتاب «جنگ اطلاعات و امنیت» معتقد است جنگ اطلاعاتی عملیاتی با «حاصل جمع صفر» است که مخازن، حاملان، حس‌گرها، ضبط‌کننده‌ها و یا پردازش‌گرهای اطلاعاتی را هدف قرار می‌دهد تا **محرمانگی، جامعیت و یا دسترس‌پذیری اطلاعات** مهاجم را افزایش و آن را برای طرف مقابل کاهش دهد (Denning, 2004).

رویکرد تهاجم اطلاعاتی در عرصه امنیتی، بدواً معطوف به اثرگذاری بر قوه تحلیل جامعه هدف به ویژه نخبگان اجتماعی تعریف شده بود. به گونه‌ای که می‌توان آن را مترادف جنگ نرم یا در ابعاد فنی‌تر، عملیات روانی قلمداد کرد. به همین دلیل می‌توان تعریف اولیه از تهاجم اطلاعاتی را چنین بیان کرد:«ضربه‌ای مخفی به نخبگان سیستم حریف که با کاهش محرمانگی، جامعیت و دسترس‌پذیری اطلاعات، به اخلال در فرآیند شناختی آنها منجر شود.»

ویژگی اصلی این تعریف از منظر کارکردی، هدف‌مندی تهاجم به تأثیر بر روال آگاهی حریف از محیط است. این مسأله می‌تواند با هدف‌گیری بخش‌هایی از روند جمع‌آوری اطلاعاتی و یا ارزیابی آن در چرخه اطلاعاتی محقق شود. ولی به مرحله تغییر رفتار ورود نمی‌کند. با این حال، به تدریج ورود سرویس‌های اطلاعاتی به این حوزه، هم مخاطب را از منظر سطح اقتدار و هم روش را از نظر دقت هدف‌گذاری ارتقا داد به نحوی که تهاجم اطلاعاتی با کنترل محیط تصمیم‌گیری حریف و تسلط بر ادراک مقام‌های مؤثر و تصمیم‌ساز، اولاً منجر به سلب ابتکار عمل مقام‌های تصمیم‌ساز در ساختار دولت یا گروه‌های فراملی/فروملی حریف شده؛ که در واقع به مرحله تغییر رفتار می‌رسد و ثانیاً با اخلال در فرآیند شناختی و ادراکی می‌خواهد وی را تحت تسلط اراده خودی گرفتار نموده و او را به سوی تصمیمی سوق دهد که به‌واقع مطلوبیت مهاجم است ولی وی آن را به مثابه مطلوبیت خود تصور خواهد کرد. پس این تغییر رفتار نیز در اتخاذ تصمیم مطلوب مهاجم نمود می‌یابد. تعاریفی که این بخش از مفهوم تهاجم اطلاعاتی را توسعه دادند به شرح زیر است:

اساتید دانشگاه‌های امنیتی و نظامی غرب در تعاریفی، تهاجم اطلاعاتی را **سلب ابتکار عمل دشمن** (Welch, 1999, 50) و را **نفوذ بر تصمیم‌گیران انسانی** (Woodcock, 1999, 172) تبیین کردند که وجه پُررنگی از تأثیرگذاری بر تصمیم طرف مقابل را معنا می‌کنند.

یکی از پژوهش‌گران ارشد پنتاگون، در توسعه این تعریف، اثرگذاری بر تصمیم قربانی را با تعبیر **پذیرش مطلوبیت‌های مهاجم به مثابه منافع خودی** تعریف می‌کند(Waltz, 2000, 5). این تعریف را می‌توان عالی‌ترین سطح اثرگذاری بر حریف عنوان کرد که کاملاً در راستای منافع مهاجم عمل می‌کند.

با توجه به موارد مذکور می‌توان تهاجم اطلاعاتی را چنین تعریف کرد:

نوعی حمله پیش‌دستانه به چرخه اطلاعاتی منتج به تصمیم‌سازی دولت/سازمان‌های متحد، مؤتلف، رقیب یا متخاصم که به هدف مدیریت ادراک و تغییر محاسبات آن، زمین بازی را مطابق منافع خودی طراحی می‌کند و به تغییر رفتار طرف مقابل به شکل اتخاذ تصمیم مطلوب مهاجم بیانجامد(Kiani, 2021)

مهم‌ترین مؤلفه‌های رویکرد تهاجم اطلاعاتی را به عنوان سنجه‌های این تعریف می‌توان چنین برشمرد:

۱. **روش‌مندی اطلاعاتی:** این تهاجم فارغ از آن‌که در حوزه‌های موضوعی نظامی، دیپلماتیک، اقتصادی، سیاسی یا فرهنگی رخ دهد، با ماهیت اطلاعاتی رخ می‌دهد و سعی می‌کند با تخریب و ضربه به فرآیند چرخه اطلاعاتی رقیب، به تغییر در اولویت‌بندی طراحی‌های اطلاعاتی، دست‌کاری در کانال‌های جمع‌آوری داده، جهت‌دهی به نوع ارزیابی و دسته‌بندی داده‌ها و نهایتاً چگونگی تحلیل آن‌ها بپردازد و این مسیر را برخلاف روال صحیح آن در جبهه حریف، تغییر دهد.

۲. **زمان‌بندی پیش‌دستانه:** رویکرد تهاجمی از اقدامی کنش‌مند برمی‌خیزد. در این رویکرد می‌بایست با پیش‌دستی و با هدف بازدارندگی و جلوگیری از افزایش تنش به سمت‌وسوی نبرد فیزیکال، به نوعی جهت‌دهی در تصمیم‌گیری حریف منجر شد که پیش از آن‌که اقدامی تهاجمی علیه منافع ملی انجام دهد، محاسباتش بر مبنای مطلوبیت‌های خودی تغییر یابد و اصولاً به پیشگیری از اقدام تهاجمی بینجامد و یا حداقل اینکه بر مؤلفه‌های اقدام خصمانه اعم از زمان، روش و هدف‌مندی مسلط شود.

۳. **آماج ادراکی:** در این رویکرد بر مبنای ماهیت اطلاعاتی می‌توان در سه سطح تاکتیکی، عملیاتی و یا راهبردی به انجام مأموریت پرداخت. با این حال فارغ از سطح مأموریت، می‌بایست در ادراک حریف نسبت به میدان نبرد مطابق مطلوبیت خودی تغییر ایجاد شود. بنابراین اینکه مبدأ عملیات، زیرساختی فیزیکی یا شبکه‌های ارتباطی باشد و یا مستقیماً به مقصد شبکه ادراکی حریف حمله شود، نهایتاً مقصد نهایی تهاجم تغییر در محاسبات و ادراک حریف از میدان منازعه است. وگرنه صرف حمله به زیرساخت فیزیکی شبکه‌ها و یا شبکه‌های فناوری اطلاعاتی، بدون تغییر ادراکی، فاقد ماهیت اطلاعاتی در رویکرد تهاجمی است.

۴. **معیار رفتاری:** سنجه مهم‌تر اینکه تغییر ادراکی و محاسباتی باید خود را در تغییر رفتاری نشان دهد. تهاجم صرفاً یک اقدام برای اثرگذاری بر نحوه فهم و تحلیل حریف نیست. بلکه می‌بایست متناسب با میدان نبرد تعیین‌شده در حوزه‌های نظامی، دیپلماتیک، سیاسی یا فرهنگی، به تغییر رفتار بر مبنای مطلوبیت خودی منجر شود تا بتوان موفقیت یا ناکامی مأموریت را در تطبیق چگونگی تغییر را اهداف اولیه مورد ارزیابی قرار داد.

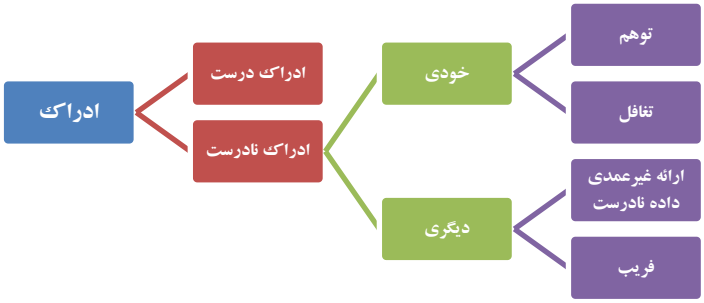
ازآنجا که تولید ادبیات تهاجم اطلاعاتی در ابتدای راه قرار دارد، نمی‌توان مدعی شد این تعریف کاملی است ولی به نظر می‌رسد تعریف مناسبی باشد. به همین دلیل می‌توان عناصر تهاجم اطلاعاتی شامل هدف، ضرورت، قابلیت، سطوح، روش و مؤلفه‌ها را بر مبنای تعریف مذکور، چنین استنتاج کرد.

جدول ۱. عناصر رویکرد تهاجم اطلاعاتی

	ابعاد	نظامی	اقتصادی	دیپلماتیک	امنیتی
عناصر					
هدف	تسلط بر اطلاعات		توزیع آگاهی مطلوب		ترسیم میدان نبرد
	کسب اطلاعات		تحلیل میدان نبرد		آماده‌سازی میدان
ضرورت	فقدان توجیه تهاجم سخت				
قابلیت	تعیین هدف و حمله به آن				
سطح	ادراکی			شبکه‌ای	زیرساختی
روش	فریب		غافلگیری	بازنمایی	عملیات روانی
مؤلفه‌ها	پیش‌دستانه		شناختی	تغییر رفتار	اطلاعاتی

با این توضیح می‌توان پس از تبیین مؤلفه‌های فریب استراتژیک، ویژگی‌های الگوی فریب استراتژیک با رویکرد تهاجم اطلاعاتی را مورد بررسی قرار داد.

فریب، ادراک نادرستی است که به طور عامدانه و به هدف تغییر باور قربانی انجام می‌گیرد. این تعریف را بارتون ویلی از کارشناسان اطلاعاتی ارتش آمریکا، چنین ترسیم می‌کند (Whaley, 1982, 180).



شکل ۱. دسته‌بندی انواع ادراک نادرست

ادراک نادرست می‌تواند از فهم خودی یا عمل دیگری نشأت بگیرد. تفاوت توهم با تغافل در آن است که در اولی، فرد توان مشاهده واقعیت را نداشته و به وهم و خیال دچار می‌شود ولی در دومی، دچار غفلت شده و با آن‌که امکان مشاهده واقعیت وجود دارد، نسبت به آن ناآگاه است. ولی اگر این امر در فعل دیگری ریشه یابد، در صورتی که عمدی باشد، فریب قلمداد می‌گردد. به همین دلیل، فریب را دستکاری عمدی ادراک و باورهای حریف به منظور تحریف آگاهی وی از وضعیت جاری و تأثیر بر تصمیم وی در راستای منافع خودی دانسته‌اند (Zand, 2017). پژوهشگران مؤسسه رَند فریب را چنین تعریف کرده‌اند:«ساختار **الف** می‌تواند ساختار **ب** را فریب دهد، اگر و فقط اگر تأثیر **الف** بر **ب**؛ عامل اساسی در اعتقاد ساختار **ب** به این باور باشد که وی در موقعیت غیرواقعی قرار دارد. به شرطی که این باور **ب** سود بیشتری برای **الف** داشته باشد تا اینکه باور کند که در وضعیت واقعی قرار دارد»(Hutchinson, 2006, 219). تعریف مؤسسه رَند علاوه بر عمد و آگاهی، مؤلفه دیگری را نیز تبیین می‌کند و آن کسب منفعت فریب‌گر است. اثر دیگری نیز فریب را اقدامی عمدی به هدف کسب مزیتی از حریف قلمداد می‌کند(Zolfaghari, 2013). چنانچه در تعریف رَند دیده می‌شود؛ از منظر هدف‌مندی، این القای باور نادرست، می‌تواند هدف مأموریت فریب قلمداد شود. گاهی صرف تغییر باور می‌تواند به

مزیت نسبی فریب‌کار نسبت به حریف فریب‌خورده بدل شود. ولی تعاریف دیگری معتقدند ممکن است فریب کار عمدتاً مقصودی عملیاتی و کارکردی از این تغییر باور در سر داشته باشد، در نتیجه هدف مأموریت زمانی محقق می‌شود که کنش مطلوب فریب‌کار از سوی فریب‌خورده انجام شود. چنانچه ارتش آمریکا، علاوه بر القای عامدانه باور مطلوب از طریق انتقال اطلاعات واقعی، تحریف‌شده یا جعلی؛ هدف فریب را «دست‌کاری در روند تصمیم‌گیری دشمن» خوانده است (Monoro, 2012, 40). در تعاریف دیگری نیز هدف فریب «اثرگذاری بر باور **یا** رفتار» ذکر شده (Reid, 2020, 1865) که نشان می‌دهد این مسأله معطوف به اصل عملیات، می‌تواند متغیر باشد.

ویژگی دیگر فریب اینکه با توجه به ماهیت ادراکی نسبت به دشمن، می‌تواند یکی از روش‌های تهاجم اطلاعاتی محسوب شود. به بیان دیگر، تغییر محاسبات حریف از طریق فریب راهبردی، اگر پیش‌دستانه و آفندی باشد، می‌تواند رویکرد تهاجمی داشته باشد. برای مثال، متفقین در جریان نبرد نرماندی، چند مانور و تجمع نیرو در نقاطی در جبهه‌های شمالی و جنوبی اروپا داشتند تا نیروهای آلمانی گمان کنند نبرد در نقطه دیگری رخ خواهد داد. این تغییر محاسبه از طریق ارائه داستانی غیرواقعی که پیامدی پایدار و بلندمدت بر جبهه رزم داشت، فریب راهبردی تلقی می‌شود که با رویکردی تهاجمی، برتری اطلاعاتی مد نظر را از منظر توزیع آگاهی میدان نبرد در راستای مطلوبیت‌های نیروهای متفقین در جبهه جنگ محقق کرد و از منظر کسب اطلاعات نیز ناظر به تحرکات نیروهای آلمانی پس از عملیات فریب، روشن ساخت که اولویت‌های نیروهای آلمانی به‌چه‌نحوی قابل درک بوده و محاسبات طرف مقابل را تغییر داد. در همین راستا ارتش آمریکا در جزوه آموزشی‌اش، بیان داشته که «یک مانور و حرکت فریبنده نسبت به تحرکات دشمن، می‌تواند اقدامی با رویکرد تهاجمی به منظور فریب حریف در مورد مکان یا زمان واقعی عملیات باشد» (Monoro, 2012, 9). در تداوم همین دیدگاه، سازمان نیروی دفاعی استرالیا در اثر آموزشی «عملیات اطلاعاتی»، روش‌های تهاجم اطلاعاتی را جنگ الکترونیک، جنگ روانی، جنگ سایبری، فریب و یا ترکیبی از همه آن‌ها تعریف کرد(Australian defense force, 2001, 4). نکته‌ای که بعدها در پژوهش سرهنگ وندوم، افسر سابق اطلاعاتی و استاد مطالعات دفاعی کالج نظامی فرانسه نیز مورد تأیید قرار گرفت(Vandome, 16, 2010). در همین راستا میلان پودوره، استاد دانشگاه دفاع ملی جمهوری

چِک نیز استفاده از فریب و انکـار در راسـتای اخـلال در تصـمیم‌گیـری‌هـای فرمانـدهی سـرویس اطلاعاتی دشمن را مورد اشـاره قـرار داده اسـت(Podhorec, 2011, 57). هِنـری پروخـون، کارشناس دانشکده پلیس و امنیـت اسـترالیا نیـز در تبیـین ضـدتهاجم اطلاعـاتی، روش مهـم آن را فریب دانسته و معتقد است به گمراه‌سازی تصمیم‌سازان سـرویس رقیـب دربـاره نگـرش آن‌هـا بـه ظرفیت‌ها یا مقاصد طرف خودی در یک عملیات اطلاعاتی می‌انجامـد(Prunckun, 43, 2014). اسکات گرور، پژوهشگر سیا نیز بیان می‌دارد که فریب با اخلال در فرماندهی و کنتـرل دشـمن بـر محیط در راستای تهاجم اطلاعاتی عمل می‌کند(Gerwehr, 2000, 20). ادوارد والتز نیـز معتقـد است بهترین روش برای بالاترین سطح تهاجم اطلاعـاتی، یعنـی تغییـر ادراک رهبـران عـالی‌رتبـه، فریب است(Waltz, 2008). نکته‌ای که با تعریـف رویکـرد تهـاجم اطلاعـاتی هـم‌پوشـانی دارد. برخی کارشناسان معتقدند در قیاس دو رویکرد تهاجمی و تدافعی به اطلاعات، فریب در دسته اول و ضـدفریب در دسـته دوم قـرار مـی‌گیرنـد (Zolfaghari, 2013). همچنـین برخـی عملیـات روانی(Soltanian, 2024) و برخی دیگر نیـز نفـوذ(Motaghi, 2017) را نـوعی فریـب قلمـداد کرده‌اند. ولی به نظر می‌رسد فریب به مثابه یک روش، می‌تواند در رویکردهـای دفـاعی نیـز علیـه دشمن و در اجتناب از تحمیل فشارها و هزینه‌های تهاجم اطلاعاتی حریـف نیـز بـه کـار بـرود. در واقع، هنگامی که فریب به مثابـه یـک روش، مـد نظـر قـرار بگیـرد، چـه در حیطـه مأموریـت‌هـای اطلاعاتی و چه در حیطه عملیات ضداطلاعاتی، بسته به اهداف تعیین‌شده در این دو نوع آفنـدی و پدافندی، می‌تواند مورد استفاده قرار بگیرد.

علاوه بر ویژگی‌های اصلی فریب، در تمایز سـطوح تـاکتیکی و راهبـردی، دو مؤلفـه مهـم بـه چشم می‌خورد. اولی اهمیت هدف که به‌تبع به اهمیت سوژه و هم‌چنین ارتقای سطح تصمیم‌گیری در عملیات می‌انجامد. به طور سنتی سنتی، فریب صـرفاً در کتمـان واقعیـت از دیـد دشـمن دانسـته می‌شد، حال آن‌که به تعبیر مایکل هندل، نویسنده «ادراک، فریب و غافل‌گیری: مورد یوم‌کیپـور»، فریـب هـم کتمـان نیـات و تـوان‌منـدی‌هـای اساسـی و مهـم و هـم گمراهـی یـا بـزرگ‌نمـایی و کوچک‌نمایی آن‌ها به اقتضای منافع فریب‌گر است(بنت، ۱۳۹۳، ۸۲). هم‌چنین فریب نـه لزومـاً بـه هدف جلوگیری از تصمیم‌های راهبردی حریف، بلکه ممکن است به هدف سوق‌دهی مخاطب را به سوی تصمیمی استراتژیک که مطلوبیت فریب‌گر را تأمین نماید، انجام گیرد. در همین خصوص

در پـژوهش دیگـری، معیـار تمـایز فریـب در سـطوح عملیـاتی، تـاکتیکی و اسـتراتژیک را میـزان دستاورد حاصله برای دولت خودی یا آسیب وارده به حریف دانسته‌اند(Ebrahimi, 2007). جان لاتمیر افسر اطلاعاتی ارتش بریتانیا و استاد کالج فرماندهی لندن، طی کتابی تحت عنوان «فریب در جنگ» علاوه بر تجارب عملیات‌های فریب نظامی در جنگ جهانی دوم، مواردی از جملـه فریـب رژیـم صهیونیسـتی توسـط مصـر در ۱۹۷۳ را مـورد ارزیـابی قـرار داد. از نظـر او فریـب تـاکتیکی محصول یک ضرورت و تفکر سریع است. مانند فریب تـک‌تیرانـدازان آلمـانی در جنـگ جهـانی دوم با شکلک‌هایی از سربازان که به گمراهی در تشخیص هدف مـی‌انجامیـد(Latimer, 2001, 85). فریب عملیاتی نتیجه افزایش کمّیت و کیفیت فریب‌های تاکتیکی است کـه توسـط نیروهـای ستادی اجرا می‌شود. مانند ایجاد تسلیحات شبیه‌سازی‌های‌شده به هدف نجات نیروهای بریتانیایی از جزیره‌ای در یونـان(Latimer, 2001, 99). سـطح اسـتراتژیک بـه فریبـی اطـلاق مـی‌شـودکه در سـطوح عـالی طراحـی مـی‌شـود، ماننـد عملیـات بادیگـارد بـرای آزادسـازی فرانسـه از اشـغال آلمان(Latimer, 2001, 166). بنـابراین سـطح تصـمیم‌گیـری بـرای طراحـی و اجـرای عملیـات فریب، از جمله سنجه‌های تمایز میان فریب‌هـای تـاکتیکی و عملیـاتی بـا راهبـردی اسـت. چنانچـه ارزیابی عملیات گسترده نرماندی نشان می‌دهد نقش‌آفرینـی مسـتقیم رهبـران در طراحـی عملیـاتی پیچیده با ابعاد متنوع سیاسی، نظامی و اقتصادی ویژگی مهم این فریب بوده است(Erdie, 2004, 5). بنابراین هدف فریب راهبردی در قیاس با سطوح دیگر می‌بایست مقام‌هـای عـالی‌رتبـه سیسـتم حریف باشند(Godson, 2000, 6). مقام‌هایی که سـطح اثرگـذاری آن‌هـا در دولـت یـا سـازمان حریف بسـیار زیـاد باشـد(Shulusky, 2000, 19). نکتـه‌ای کـه در دیگـر پـژوهش‌هـای مراکـز آموزشی و دانشکده‌های وابسته به ارگان‌های نظامی آمریکا، پس از ۱۱ سـپتامبر مـورد توجـه قـرار گرفت(Sharp, 2006, 19). پژوهش‌هایی نیز در همین راستا اهمیت اهداف پنهان‌شده(Caddell, 2004, 17) یـا هـدف‌گـذاری بـر زیرسـاخت‌هـای مـدیریتی(Reid, 2017, 2) را تمـایز فریـب راهبردی با سطوح پایین‌تر ذکر کرده‌اند. دومین ویژگی متمایز سطح راهبردی فریب را بازه زمـانی آن قلمداد کرده‌اند. مقالاتی به تمایز زمـانی اشـاره داشـته و کتمـان واقعیـت یـا تحقـق اهـداف در بلندمدت را مصداق فریب راهبردی دانسته‌اند(Cohen, 2004, 17).

بر مبنای آن‌چه در ادبیات ویژگی‌ها و روش‌های فریب مرور شد، می‌توان فریب راهبردی را چنین تعریف کرد:

جعل اطلاعات نادرست، انکار اطلاعات صحیح و یا ترکیبی از این دو به نحوی که به تحمیل باوری نادرست به مدیران ارشد دولت/سازمان حریف منجر گردد که تأثیرات مثبت آن به نفع جبهه خودی یا تأثیر منفی آن به ضرر رقیب/دشمن بر مبنای اهداف تعیین‌شده، در بازه‌های زمانی کوتاه‌مدت و میان‌مدت قابل بازگشت نباشد.

به بیانی دیگر می‌توان مؤلفه‌های فریب راهبردی را چنین بیان داشت:

۱. **تحمیل باوری نادرست**: ماهیت فریب راهبردی تحمیل باوری نادرست به حریف نسبت به درک او از صحنه نبرد است. این باور نادرست می‌تواند با انکار حقیقت، جعل داده غیرواقعی یا ترکیبی از این دو به گمراهی سوژه بینجامد. حتی بیان بخشی از واقعیت با ترفندهایی که به سوگیری مناسب منجر گردد نیز می‌تواند بخشی از یک عملیات فریب باشد.

۲. **اهمیت هدف**: یکی از مهم‌ترین معیارهای این تعریف، اهمیت هدف عملیاتی است. هر چه هدف مهم‌تر و مؤثرتر باشد، جایگاه تصمیم‌گیری سوژه عملیات افزایش می‌یابد. فرد یا افرادی که طی این مأموریت مورد هدف قرار می‌گیرند باید از سطح اختیارات و مسئولیت عالی‌رتبه‌ای در حوزه موضوعی اعم از مسائل نظامی، دیپلماتیک، اقتصادی یا فرهنگی برخوردار باشند و تصمیم آنان نسبت به رده‌های میانی، بسیار مؤثرتر و نافذتر قلمداد شود. هر چه سطح تصمیم‌گیری عالی‌تر باشد، مأموریت بُعد استراتژیک‌تری به خود می‌گیرد.

۳. **بازه بلندمدت**: مؤلفه دیگری که قابلیت بررسی دارد اینکه مطلوبیت رخ‌داده در بازه زمانی بلندمدت پایدار بماند و حریف نتواند به‌زودی اقدامی بازگشت‌پذیر در راستای تغییر موازنه نیروها به شرایط پیشین به انجام برساند.

پیشینه پژوهش

در جدول زیر، پژوهش‌های انجام‌شده درباره ارتباط فریب و تهاجم اطلاعاتی به تفکیک سوال، روش و نتیجه ذکر شده است.

جدول ۲. پیشینه پژوهش

عنوان	نویسنده	سوال	روش	نتیجه
«عملیات فریب در عملیات روانی»(۱۳۸۳)	کریمی‌نیا	نقش فریب در عملیات روانی	توصیفی و مطالعات کتابخانه‌ای	فریب به مثابه تحریف، دستکاری و کتمان شواهد
«فریب در عملیات روانی»(۱۳۸۶)	حجت‌زاده	نقش فریب در عملیات روانی	توصیفی و مطالعات کتابخانه‌ای	کتمان توان‌مندی‌ها و انگیزه‌های جبهه فریب‌گر
«مبانی تئوریک و مصداقی تهدید نرم»(۱۳۸۶)	کرمی	چگونگی طرح فریب راهبردی	توصیفی و مطالعات کتابخانه‌ای	اقناع رقیب به پذیرش فریب به مثابه مطلوبیتش
«طرح‌ریزی الگوی کلان امنیت نرم»(۱۳۸۸)	عبدالله‌خانی	نسبت فریب با جنگ نرم	توصیفی و مطالعات کتابخانه‌ای	فریب یکی از روش‌های جنگ نرم
«بازخوانی قدرت نرم، مطالعه موردی: عملیات روانی»(۱۳۹۰	قربی	نسبت فریب با عملیات روانی	توصیفی و مطالعات کتابخانه‌ای	فریب جزیی از عملیات روانی برای تغییر محاسبات حریف
«عصر اطلاعات و جنگ اطلاعاتی»(۱۳۸۵)	رشیدزاده	نقش فناوری در نبردهای اطلاعاتی	توصیفی و مطالعات کتابخانه‌ای	نبرد غیرمستقیم از طریق حملات سایبری و سرقت اطلاعاتی
«جنگ در عصر اطلاعات»(۱۳۸۷)	افضلی	چگونگ برتری اطلاعاتی از طریق تهاجم اطلاعاتی	توصیفی و مطالعات کتابخانه‌ای	ضربه به محیط اجتماعی حریف
«تحلیل سناریویی، رویکردی نوین در فرآیند تحلیل و آینده‌نگاری اطلاعاتی»(۱۳۹۱)	صابرفرد	نقش آینده‌پژوهی در تهاجم اطلاعاتی	توصیفی و مطالعات کتابخانه‌ای	آینده‌پژوهی به مثابه روش کاهش عدم قطعیت‌ها برای طراحی سیاست آفندی

در مقالات فوق اشاره‌ای به مبحث تهاجم اطلاعاتی نشده و بعضاً نیز به فریب با رویکرد پدافندی نگریسته شده است. در مواردی نیز تنها بر کارکرد فریب در عملیات روانی متمرکز شده‌اند. پس ارتباطی میان فریب با رویکرد تهاجمی به اطلاعات مشاهده نمی‌شود. حال آن‌که مقاله حاضر از بُعد محتوایی، ناظر به تطبیق مؤلفه‌های رویکرد تهاجمی به فریب راهبردی تدوین شده و تمایز جدی با موارد پیشین دارد. از منظر روشی نیز علاوه بر روش کیفی تحلیل مضمون، از روش کمّی تحلیل پرسش‌نامه برای اخذ نظرات خبرگان امر بهره برده و روایی و اعتبار بیشتری نسبت به مقالات مشابه، کسب کرده است.

روش‌شناسی پژوهش

در این تحقیق هم از روش کیفی در بخش اول برای کسب تعریفی از دو مفهوم اصلی یعنی تهاجم اطلاعاتی و فریب راهبردی و هم از روش کمّی در بخش دوم برای احصای نظرات نخبگان در خصوص اعتبارسنجی، استفاده شده است. دلیل استفاده از روش کیفی در بخش اول پژوهش آن است که این پژوهش فاقد فرضیه پیشینی است و به همین دلیل در انواع پدیدارشناسانه از پژوهش‌های کیفی قرار می‌گیرد که محقق با مشاهده و مطالعات خود درصدد کشف ماهیت سوژه تحقیق برمی‌آید(Namazi, 2003). بنابراین راهبرد تحقیق، تلفیقی قلمداد می‌شود. روش کیفی برای کشف مضمون و روش کمّی برای اعتباربخشی به آن از طریق پرسش‌نامه است. تلفیق این دو باعث می‌شود از نقاط قوت هر دو روش بهره‌مند شویم و به درک بهتری از موضوع پژوهش دست یابیم. در این پژوهش، بخش اصلی کار بهره‌مندی از داده‌های کیفی است که به مدل اولیه می‌انجامد و سپس در مرحله پرسش‌نامه مورد ارزیابی بخشی از خبرگان موضوع قرار گرفته و با تأیید و کسب روایی، به یک الگو تبدیل می‌شود. این کار سبب می‌شود داده‌های گردآوری‌شده در روش کیفی، با روش دقیق‌تری مورد ارزیابی قرار گرفته و نتایج آن برای مخاطبان متخصص در موضوع پژوهش، قابل‌قبول‌تر باشد. این نکته‌ای است که به طور خاص درباره موضوع این پژوهش، صدق می‌کند.

چهار نوع روش برای این استراتژی وجود دارد (Almalki, 2016: 292):

- **روش موازی**: این روش به طور هم‌زمان از روش‌های کیفی و کمّی به صورتی موازی بهره‌مند می‌شود. استفاده متوازن از هر دو راهبرد، مزیت این روش است. در عین حال که تلاش برای حفظ این توازن در مراحل یک پژوهش، بسته به موضوع می‌تواند با دشواری‌هایی همراه باشد.
- **روش ترکیبی**: این روش زمانی مورد استفاده قرار می‌گیرد که پژوهش به منابع کمتری احتیاج دارد و برخی داده‌های کیفی صرفاً در نقش کمکی و ثانویه ظاهر می‌شوند. این روش عمدتاً در جایی طرح‌های آزمایشی و پیمایشی کمّی به تعداد معدودی داده کیفی نیازمند است، مورد رجوع قرار گرفته است. گرچه ممکن است در موضوعات کیفی‌تر، ادغام دو راهبرد در این روش، مشکل به نظر برسد.
- **روش توضیحی**: این یک روش دو مرحله‌ای است که در آن داده‌های کمّی را به عنوان پایه‌ای برای ساخت و توضیح داده‌های کیفی مورد استفاده قرار می‌دهد. داده‌های کمی فرآیند انتخاب داده‌های کیفی را مشخص می‌کند که مزیت نسبی در این زمینه است که محققان را قادر سازد داده‌هایی را که مربوط به پروژه تحقیقاتی خاص هستند، مشخص کنند. وجود حد نصابی از خبرگان موضوع برای ساخت ابتدایی این روش در مرحله اول، از چالش‌های آن است.
- **روش اکتشافی**: طرح اکتشافی معکوس روش توضیحی است. در این روش، داده‌های کیفی زمینه جمع‌آوری اطلاعات کمّی از نخبگان را فراهم می‌سازد. مزیت این روش در این است که مراحل به راحتی قابل اجرا هستند و داده‌های کیفی برای محققان قابل قبول است. ولی چالش آن اینکه زمان‌بر است.

در این پژوهش، به دلیل اینکه مرحله اول، گردآوری داده‌های کیفی و کشف مؤلفه‌های مؤثر بر موضوع است، از روش اکتشافی در بین انواع روش تلفیقی بهره برده می‌شود. زیرا موضوع پژوهش مبتنی بر طرح تهاجم اطلاعاتی، موضوعی است که ادبیات لازم درباره آن به زبان فارسی تولید نشده است. به همین دلیل، اهمیت کشف عناصر آن به روش کیفی، در اولویت قرار دارد. در مرحله بعدی، از روش کمّی برای تبیین دقیق‌تر موضوع، اعتباربخشی به آن و تشخیص نقاط ضعف

و قوت در فرآیند کیفی پژوهش، بهره برده خواهد شد. انعطاف‌پذیری روش تلفیقی در کنار افزایش دقت پژوهش‌گر به دلیل برخورداری از مزیت‌های هر دو استراتژی، در موضوع این پژوهش که پیش‌تر کمتر مورد توجه بوده، اهمیت می‌یابد.

یافته‌های پژوهش

بر مبنای تعاریف مذکور درباره تهاجم اطلاعاتی و فریب راهبردی، می‌توان درباره ارتباط فریب راهبردی با رویکرد تهاجم اطلاعاتی بیان داشت که فریب راهبردی، روشی از روش‌هایی است که می‌تواند با کارکرد تهاجمی به اطلاعات، برای تغییر محاسبات و ادراکات و تحمیل زمین بازی به حریف به کار برود. از منظر تطابق مؤلفه‌های عملیات فریب به عنوان یک روش با مؤلفه‌های رویکرد تهاجم اطلاعاتی می‌بایست به این نکات متذکر شد که

۱. فریب ذاتاً ماهیت ادراکی دارد و بر مبنای تغییر ادراک قربانی نسبت به موضوع بر اساس مشاهدات دریافتی، مطابق مطلوبیت‌های مهاجم طراحی می‌شود. پس این مؤلفه رویکرد تهاجمی به اطلاعات به طور خاص در روش فریب نهفته است. زیرا در تهاجم اطلاعاتی نیز به هدف تغییر محاسبات قربانی، می‌بایست در ادراک حریف نسبت به میدان نبرد تغییر ایجاد کرد.

۲. هر مأموریت فریب، ماهیت اطلاعاتی نیز خواهد داشت و بر اساس دستکاری در اطلاعات دریافتی قربانی درصدد تغییر درک او از وضعیت برخواهد آمد. به بیان دیگر در بُعد روش می‌توان گفت که با توجه به ضرورت تغییر ادراک بر مبنای ورودی سیستم تصمیم‌گیری، هر مأموریت فریب یک ماهیت اطلاعاتی دارد.

اما سه مسأله باقی است که در فریب راهبردی با رویکرد تهاجم اطلاعاتی، مد نظر است:

۱. آیا هر فریب ماهیتی پیش‌دستانه و پیشاواکنشی نسبت به دشمن دارد؟ عموماً تصور بر آن است که ضدفریب بر مبنای واکنش به کنش دشمن عمل می‌کند و در فریب به طور طبیعی برنامه‌ریزی پیشینی بر مبنای حمله تهاجمی صورت می‌پذیرد. با این حال باید گفت که فریب هم از عملیات تهاجمی و هم تدافعی پشتیبانی می‌کند. به‌واقع ممکن

است در عملیاتی که دشمن تهاجم کرده و نیروهای خودی در موقعیتی گرفتار آمده‌اند، با عملیات فریب سعی شود آن نیروها به موقعیتی بهتر منتقل گردند. به تعبیری در یک پازل کلان‌تر ممکن است این فریب در یک فاز گسترده‌تر دفاعی، مثلاً در برابر تجاوز دشمن به تمامیت ارضی، باشد. پس در عملیات فریب با رویکرد تهاجمی تلاش می‌شود پیش از آن‌که دشمن با اقدامی منافع ملی را به خطر بیندازد، با طرح فریب از کنش او جلوگیری شده یا وی را در مسیر مطلوب فریب‌گر قرار دهند. در این حالت برنامه‌ریزی و هدف‌گذاری پیشینی عملیات فریب در راستای تهاجم، به آن موقعیتی پیش‌دستانه در برابر دشمن می‌دهد.

۲. مسأله دیگر در فریب با رویکرد تهاجمی این‌که در رویکرد تهاجمی، ارزیابی فریب بر اساس تغییر رفتار یا اقدام ناشی از تغییر ادراک صورت می‌پذیرد. بنابراین در این حوزه، عملیات فریب در تغییر ادراک متوقف باقی نمی‌ماند، بلکه باید واکنش مطلوب برای فریب‌گر از سوی قربانی اتخاذ شود. در صورت عدم واکنش یا واکنشی دیگر، عملاً مأموریت فریب تهاجمی شکست خورده است. این ضرورت تغییر رفتاری در مؤلفه‌های تهاجم اطلاعاتی نیز ذکر شده که با روش فریب مطابقت دارد.

۳. دیگر اینکه فریب با رویکرد تهاجمی از جنس فریب فعال است. بدین معنا که صرف گمراهی قربانی و رهاساختن وی در میان گزینه‌های مبهم و پراکنده کفایت نمی‌کند. گرچه این مقدمه‌ای برای دور ساختن وی از امر نامطلوب تلقی شود، ولی در ادامه بایستی مطابق تعریف فریب فعال، شاخص‌های فریب‌گر به قربانی منتقل شده و وی به سوی گزینه‌ای مشخص هدایت شود. این گزینه می‌تواند اقدام یا عدم اقدام در راستای منافع خودی باشد. حال آن‌که در فریب منفعل چنین مقصودی در پی نیست.

در مدل فریب راهبردی با رویکرد تهاجم اطلاعاتی، با توجه به اینکه فریب به مثابه روشی برای تحقق این رویکرد تلقی می‌شود و ناظر به تعریف کسب‌شده از این رویکرد مبتنی بر حمله‌ای پیش‌دستانه به چرخه اطلاعاتی حریف، می‌توان ابعاد، سطوح، مؤلفه‌ها و شاخص‌های این مدل را چنین تبیین نمود.

➢ ابعاد

از آن‌جا که رویکرد مأموریت فریب راهبردی، مبتنی بر تهاجم اطلاعاتی است، دارای دو بُعد برتری اطلاعاتی و کسب اطلاعات است.

- ❖ در بُعد **برتری اطلاعاتی**، فریب‌گر با کنترل کانال‌های اطلاعاتی سوژه، فضای تبادل اطلاعات و نوع و جهت‌گیری داده‌های انتقالی را تحت تسلط قرار داده و مطلوبیت‌های خود را به عنوان مطلوبیت‌های حریف به محیط اطلاعاتی او تزریق می‌کند.
- ❖ در بُعد **کسب اطلاعات** از منظر محتوا، سعی خواهد داشت تا اهداف و اولویت‌های حریف را مورد شناسایی قرار دهد. بدین ترتیب که واکنش حریف به عملیات فریب، معطوف به متغیرهای قابل‌سنجش در عملکرد وی، نشان‌گر آن خواهد بود که بر مبنای باور به داستان، چه میزان در توجه و تمرکز منابع او به سمت اولویت‌هایش، تغییر ایجاد شده است. هم‌چنین از منظر روشی، تلاش خواهد نمود تا نحوه تجزیه‌وتحلیل و چگونگی پردازش داده‌ها و تولید خروجی اطلاعاتی را درک کند.

➢ سطوح

- ❖ در سطح **ادراک حریف**، عملیات فریب راهبردی با رویکرد تهاجم اطلاعاتی منجر به تغییر محاسبات سوژه فریب می‌شود و در این درک وی از عناصر محیطی، بازیگران و یا راهبردهای آنان مطابق اهداف فریب‌گر تغییر می‌یابد و سبب می‌شود نسبت به موضوع فریب، چنان بیندیشد که فریب‌گر خواسته است.
- ❖ در سطح **شبکه‌های اطلاعاتی**، با توجه به اِشراف مهاجم به کانال‌های اطلاعاتی فریب‌خورده، می‌توان زمینه‌های نفوذ در این شبکه فراهم می‌شود. بدین ترتیب که بسته به نوع ساختار سیاسی، روابط فردی و تشکیلاتی سوژه

فریب و تنوع و تکثر کانال‌های اطلاعاتی؛ می‌توان این شبکه‌ها را مورد ارزیابی قرار داده و امکان نفوذ در آن‌ها و اثرگذاری بر محیط تبادل اطلاعات را میسر نمود.

- **مؤلفه‌ها**

- عملیات فریب راهبردی با رویکرد تهاجم اطلاعاتی اقدامی **پیش‌دستانه** و کُنش‌مند است و پیش از آن‌که طرح و عملیاتی از سوی رقیب یا دشمن علیه کشور صورت بگیرد، برای طراحی و برنامه‌ریزی ذهن و ادراک او و در جهت منافع ملی انجام می‌پذیرد تا مانع از توطئه‌ها و رفتارهای خصمانه گردد و ابتکار عمل را در اختیار نیروهای خودی قرار دهد.
- این عملیات بر مبنای **مداخله در چرخه اطلاعاتی** حریف صورت می‌پذیرد. بدین ترتیب که محاسبات قربانی در یکی از مراحل طرح‌ریزی، گردآوری، تجزیه‌وتحلیل یا نتیجه‌گیری و بازخورد مورد هدف قرار داده و متناسب با اهداف فریب‌گر تغییراتی ایجاد کند. تزریق داستان فریب از طریق کانال‌های اطلاعاتی، مجرای گردآوری داده‌ها را دستخوش تغییر کرده و در نتیجه در تجزیه‌وتحلیل نهایی ساختار درک محیطی طرف، مطلوبیت فریب‌گر را به سوژه منتقل خواهد کرد که در تغییر رفتار وی در مرحله نتیجه‌گیری نماایان خواهد شد. این مسأله در صورت توالی عملیات در مرحله بازخورد، بر طرح‌ریزی قربانی در آتی نیز مؤثر خواهد بود.
- عملیات فریب راهبردی با رویکرد تهاجم اطلاعاتی، مبتنی بر نگرشی **ایجابی** محقق می‌شود. بدین معنا که با پیگیری عملیات فریب فعال، سعی خواهد کرد مطلوبیت فریب‌گر را به قربانی القا نماید. حتی اگر این مطلوبیت، بازدارندگی و انفعال فریب‌خورده باشد، ولی در هر صورت، بر اساس مطلوبیت‌ها و منافع ملی دولت مهاجم رقم می‌خورد.
- مؤلفه دیگر این مدل این است که موجب **تغییر رفتار** سوژه فریب شود و صرفاً در گام تغییر ادراک وی، متوقف نشود.

- ❖ قربانی عملیات فریب راهبردی با رویکرد تهاجم اطلاعاتی، **نخبگان** عالی‌رتبه و تصمیم‌سازانی هستند که در تغییر راهبردی رفتار دولت/سازمان یا به تعبیری بازیگر حریف، نقشی جدی و مؤثر ایفا می‌کنند.
- ❖ عملیات فریب راهبردی با رویکرد تهاجم اطلاعاتی، تأثیراتی به نفع جبهه خودی دارد که در بازه‌های زمانی کوتاه‌مدت و میان‌مدت قابل برگشت نیستند و در **بلندمدت**، منافع ملی را تأمین خواهد کرد.

➢ **شاخص‌ها**

- ❖ اولین شاخص ارزیابی عملیات فریب این است که تغییر رفتار سوژه، **زمینه نفوذ فردی و شبکه‌ای** در چارچوب تحلیلی قربانی را فراهم نماید.
- ❖ شاخص دیگر این است که این عملیات به **انباشت تجربه** فریب‌گر انجامیده و او را در طراحی دقیق‌تر عملیات‌های آتی یاری کند.
- ❖ دیگر شاخص اینکه **شناخت خوبی از ساختار ادراکی** قربانی نسبت به محیط ارائه کند.
- ❖ یک شاخص اینکه عملیات فریب راهبردی در بازه‌ای **فراتر از بازه‌های کوتاه‌مدت** به طول می‌انجامد.

برای اعتبارسنجی پرسش‌های مرتبط با مدل کسب‌شده در بخش کیفی، از ۱۵ تن از کارشناسان که دارای تجربه علمی یا عملی و یا تؤأم هر دو بوده‌اند، بهره برده شد. طبیعی است با توجه به فقدان دسترسی پژوهش‌گر و محدودیت‌های موجود، تعداد افراد پاسخ‌گو به نسبت اندک می‌باشد.تحصیلات این افراد در رشته‌های مرتبط با علوم سیاسی، مطالعات منطقه‌ای و روابط بین‌الملل و هم‌چنین رشته‌های تحصیلی مرتبط با اطلاعات نظامی بوده است. رده خدمت آن‌ها نیز پژوهش‌گری، کارشناسی یا عضویت در هیئت علمی دانشگاه‌های نظامی کشور بوده است. سابقه فعالیت علمی یا عملی آنان در حوزه مرتبط با موضوع اعم از حوزه نظامی یا حوزه سیاست خارجی بوده است. مشخصات این نمونه در جدول شماره ۲ شده است.

جدول ۲. مشخصات نمونه آماری

ردیف	شاخص		تعداد	درصد
۱	ماهیت ارتباط نخبگان با موضوع تحقیق	علمی	۴	۲۸
۲		عملی	۳	۲۰
۳		علمی و عملیاتی	۸	۵۲
۱	سطح تحصیلات	دکتری	۱۳	۸۷
۲		کارشناسی ارشد	۲	۱۳
۱	میزان فعالیت نخبگان در موضوعات مرتبط با تحقیق	بیش از ۲۰ سال	۵	۳۳
۲		بیش از ۱۰ سال	۸	۵۲
۳		زیر ۵ سال	۲	۱۵
۱	رده سازمانی	کارشناس	۶	۴۰
۲		مدیر	۶	۴۰
۳		عضو هیئت علمی	۳	۲۰

ابتدا، روایی و پایایی پرسش‌نامه‌ها مورد ارزیابی قرار گرفته است. روایی بدین معناست که روش یا ابزار به کار رفته تا چه حد می تواند خصوصیت مورد نظر را درست اندازه‌گیری کند. به عبارت دیگر مفهوم روایی، به این سوال پاسخ می‌دهد که ابزار اندازه‌گیری تا چه حد خصیصه مورد نظر را می‌سنجد. برای بررسی روایی محتوایی به شکل کمی، از ضریب نسبی روایی محتوا (CVR) استفاده می‌شود.

$$CVR = \frac{n_E - \frac{N}{۲}}{\frac{N}{۲}}$$

در این رابطه n_E تعداد متخصصانی است که به گزینه ضروری پاسخ داده‌اند و N تعداد کل متخصصان است. اگر مقدار محاسبه‌شده از مقدار جدول بزرگتر باشد اعتبار محتوای آن آیتم پذیرفته می‌شود. مقدار CVR در نسبت با تعداد متخصصان مورد رجوع، متفاوت است. برای این پژوهش با تعداد ۱۵ نفر، حداقل مقدار باید ۰/۴۹ باشد تا روایی آن گزاره مورد تأیید باشد. وضعیت روایی محورهای مورد پرسش در جدول شماره ۳ نمایش داده شده است.

جدول ۳. روایی

سازه‌ها	گویه‌ها	CVR	نتیجه
ابعاد	برتری اطلاعاتی	۱	تأیید
	کسب اطلاعات	/۴۹	تأیید
سطوح	مدیریت ادراک	۱	تأیید
	نفوذ زیرساختی	/۸۷	تأیید
مؤلفه‌ها	پیش‌دستانه	/۸۷	تأیید
	مبتنی بر نفوذ در چرخه اطلاعاتی	/۸۷	تأیید
	مبتنی بر تغییر رفتار	/۳۳	رد
	ایجابی	۱	تأیید
	نخبگانی	/۷۳	تأیید
	بلندمدت	/۳۳	رد
شاخص‌ها	انجام عملیات در بلندمدت	۰/۲	رد
	انباشت تجربه	/۷۳	تأیید
	شناخت نحوه درک قربانی از محیط	/۴۹	تأیید
	زمینه‌سازی نفوذ انسانی و شبکه‌ای	/۶	تأیید

سازه‌های ابعاد و سطوح، روایی مناسبی داشته‌اند. در خصوص مؤلفه‌ها کاهش روایی «تغییر رفتار» نشان‌گر آن است که از منظر اکثریت نخبگان، صرف تغییر محاسبات و مدیریت ادراک، حتی اگر به انفعال و بی‌عملی سوژه منجر گردد، ارزشمند تلقی شده است. هم‌چنین ماهیت راهبردی فریب را در تأثیرگذاری و عمق آن و نه در بازه زمانی آن در نظر گرفته‌اند. از نظر آنان، اگر هدفی مهم و حیاتی، در میان‌مدت و کوتاه‌مدت نیز بتواند محقق شود و ادراک طرف مقابل را به نفع طرف مهاجم تغییر دهد، مقصود حاصل شده است. هم‌چنین معتقدند نیازی نیست به قربانی مهلت چندانی برای تعمیق باور داده شود و بهتر است عملیات فروتر از بازه زمانی بلندمدت به انجام برسد.

در خصوص پایایی پرسش‌ها نیز بدین معناست که اگر در چند زمان مختلف در یک جمعیت از آن استفاده کنیم در نتیجه به دست‌آمده اختلاف چندانی مشاهده نمی‌کنیم. یعنی ابزار اندازه‌گیری در شرایط یکسان تا چه اندازه نتایج یکسانی به ما می‌دهد. برای اندازه‌گیری پایایی از

شاخصی به نام ضریب پایایی استفاده می‌شود. دامنه ضریب پایایی از صفر تا +۱ است به این معنا که اگر ضریب صفر باشد عدم پایایی و اگر این ضریب یک باشد پایایی کامل را نشان می‌دهد. هرچند پایایی کامل به ندرت دیده می‌شود. جهت ارزیابی پایایی از شاخص آلفای کرونباخ استفاده می‌گردد. حداقل مقدار قابل قبول برای ضریب آلفای کرونباخ مقدار ۰/۷ می‌باشد. میزان پایایی گویه‌های ابعاد، سطوح، مؤلفه‌ها و شاخص‌های مدل فریب راهبردی با رویکرد تهاجم اطلاعاتی در جدول زیر ذکر شده است.

جدول ۴. پایایی

سازه‌ها	آلفای کرونباخ	سازه‌ها	آلفای کرونباخ
ابعاد	۰,۷۰۴۴	سطوح	۰,۶۹۹۴
مولفه‌ها	۰,۷۰۲۰	شاخص‌ها	۰,۷۵۸۷

طبق جدول ۴، همه گویه‌ها در ابعاد، مؤلفه‌ها و شاخص‌ها از پایایی مناسبی برخوردار هستند و در سطوح نیز پایایی در مرز حد نصاب قرار دارد. این مسأله نشان می‌دهد که ارزیابی این سازه‌ها در شرایط مشابه نیز نتایج نسبتاً مشابهی را ارائه خواهند داد.

ارزیابی دیگر، بررسی انسجام درونی سازه‌های پرسش‌نامه است. بدین معنا که آیا گویه‌هایی که در یک سازه گرد هم آمده‌اند؛ سازه اصلی را تبیین می‌کنند و آیا در کنار یکدیگر به صورتی افرازشده توانسته‌اند سازه اصلی را ساختارمند نمایند. یکی از سنجه‌هایی که برای ارزیابی این امر به کار می‌رود، روایی همگرا نام دارد که میزان همبستگی درونی هم‌سویی گویه‌های یک مقوله را نشان می‌دهد. این سنجه را از طریق ارتباط دو ضریب می‌سنجند: میانگین واریانس استخراج‌شده (Average Variance Extracted) و پایایی ترکیبی(Composite Reliability). شرط همبستگی درونی گویه‌های یک سازه آن است که پایایی ترکیبی هم از ۰,۷ و هم از میانگین واریانس استخراج‌شده بیشتر باشد.

جدول ۵. سازگاری درونی

سازه‌ها	CR	AVE	سازه‌ها	CR	AVE
ابعاد	۰,۷۴۵۵	۰,۶۱۹۴	مولفه‌ها	۰,۷۴۰۷	۰,۳۸۹۳
سطوح	۰,۶۹۹۵	۰,۵۴۴۸	شاخص‌ها	۰,۷۴۹۴	۰,۴۲۹۰

نتایج جدول ۵ نشان دهنده این است کـه تمـامی سـازه‌هـا از اعتبـار و معنـاداری قابـل توجـه و حداقلی برخوردار هستند و گویه‌های درونی هر سازه به نحوی طراحی و تدوین شده‌اند کـه یـک سازه، یک ساختار منسجم و معین را شکل داده است. دربـاره سـازه سـطوح مـدل، ضـریب پایـایی ترکیبی گرچه کمتر از مقدار حد نصاب، ولی بسیار نزدیک به ۰,۷ است.

نتیجه‌گیری و پیشنهادها

با توجه به اعتبارسنجی مدل توسط نخبگان مـورد رجـوع، عناصـر الگـوی فریـب راهبـردی بـا رویکرد تهاجم اطلاعاتی چنین هستند.

جدول ۶. نتایج اعتبارسنجی

سازه‌ها	**گویه‌ها**
ابعاد	برتری اطلاعاتی
	کسب اطلاعات
سطوح	مدیریت ادراک
	نفوذ زیرساختی
مؤلفه‌ها	پیش‌دستانه
	مبتنی بر نفوذ در چرخه اطلاعاتی
	ایجابی
	نخبگانی
شاخص‌ها	انباشت تجربه
	شناخت نحوه درک قربانی از محیط
	زمینه‌سازی نفوذ انسانی و شبکه‌ای

بررسی نتایج این نظرخواهی از نخبگان که در جدول شماره ۶ نمایان شده، نشان می‌دهد که گویه‌های مدل استخراج‌شده، مورد تأیید قرار گرفته است و به این ترتیب می‌توان گفت که مدل، به دلیل تأیید نخبگانی، ظرفیت تبدیل به یک الگو را دارد. در این راستا باید بتوان این گویه‌ها را و به تعبیر دقیق‌تر، سازه‌های ابعاد، سطوح، مؤلفه‌ها و شاخص‌ها را که طبق عنوانش، ساختمان این مدل را تشکیل می‌دهند، در چارچوب مراحل یک الگو، تنظیم نمود. مراحل یک الگو شامل هدف‌گذاری، سوژه‌یابی، مأموریت و نهایتاً نظارت و کنترل بر چگونگی اجراست.

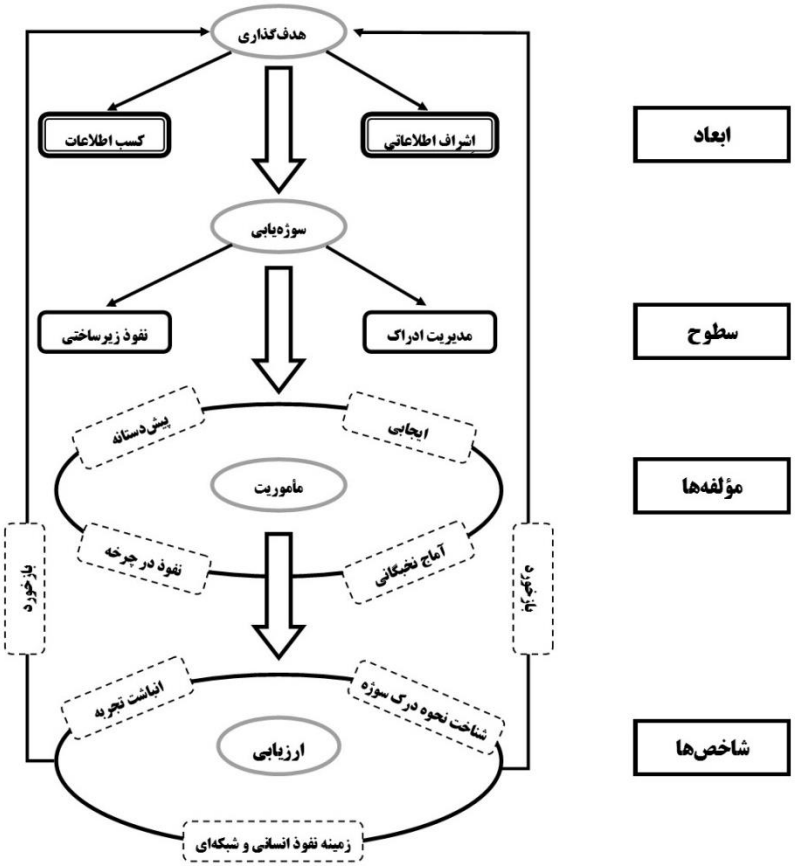
هدف‌گذاری: تعیین اهداف راهبردی و نهایتاً طراحی سناریوی فریب با ملاحظه روش‌های معقول و ابزارهای موجود.

سوژه‌یابی: شناسایی مقصود و مقصد عملیات فریب از طریق تحلیل رفتار دشمن، مسیرهای موجود برای انتقال و طراحی گزاره‌های مجعول و اطلاعات گزینش‌شده برای تدوین داستان فریب.

مأموریت: انتشار اطلاعات نادرست و اجرای نمایش‌های ساختگی از طریق هماهنگی بین‌بخشی.

ارزیابی: نظارت بر واکنش دشمن و ارزیابی اثربخشی فریب و اصلاح فرآیندها برای عملیات بعدی.

در همین راستا، ابعاد شامل اِشراف و سپس کسب اطلاعات به مثابه اهداف راهبردی این الگو در مرحله اول جای می‌گیرند. مدیریت ادراک و نفوذ زیرساختی، به مثابه سطوح این الگو، در مرحله سوژه‌یابی و طراحی عملیات، مورد کاربرد قرار می‌گیرند. در واقع، اینکه در سطح نفوذ یا در سطح مدیریت ادراک، اقدام به تغییر دستگاه محاسباتی حریف شود، بستگی به سوژه‌یابی در این مرحله دارد. مؤلفه‌ها شامل ایجابی، پیش‌دستانه، نفوذ در چرخه و آماج نخبگانی عملیات، در اجرای مأموریت، نمود می‌یابد. و در نهایت اینکه ثمرات عملیات در شناخت نحوه درک و محاسبات سوژه نمود یابد و به انباشت تجربه ما و زمینه نفوذ انسانی و شبکه‌ای منجر شده باشد یا خیر، در مرحله نهایی یعنی کنترل و ارزیابی، مشخص می‌شود.



شکل ۲. الگوی فریب راهبردی با رویکرد تهاجمی

این فرآیند را می‌توان چنین تبیین نمود.

- **هدف‌گذاری**: در این گام، متناسب با مسأله‌ای که ذهنیت سیاست‌گذار را درگیر کرده، اعم از اینکه منطقه‌ای یا بین‌المللی باشد؛ نظامی، امنیتی، دیپلماتیک یا اقتصادی باشد؛ تصمیم گرفته می‌شود که کدام‌یک یا هر دو بُعد الگوی فریب راهبردی با رویکرد تهاجم اطلاعاتی مد نظر قرار بگیرد. اینکه هدف کسب اطلاعات و ارزش‌افزوده دانشی باشد و یا اینکه مهم‌تر از آن، بتوان میدان تبادل داده و اطلاعات را کنترل نمود و یا اینکه ضمن اِشراف اطلاعاتی، بتوان داده جدیدی از میدان مورد نظر کسب کرد.

- **سوژه‌یابی**: در این گام سوژه یا قربانی مأموریت فریب انتخاب شده و سپس تصمیم گرفته می‌شود که در سطح نفوذ به زیرساخت‌های ارتباطی و اطلاعاتی سوژه و یا سطح مدیریت ادراک وی، مأموریت تعریف و طراحی گردد. توانمندی‌ها و منابع انسانی و مادی طراحان و سیاست‌مداران در این موضوع مؤثر است و اینکه چه کانال‌های ارتباطی در جریان مدیریت مأموریت فریب در اختیار دارند.
- **مأموریت**: در گام اجرای عملیات، مؤلفه‌های الگو نشان‌گر ویژگی‌های یک مأموریت فریب با رویکرد تهاجم اطلاعاتی است. اینکه پیش‌دستانه و کنشی باشد. هم‌چنین اینکه ایجابی و مبتنی بر پیشبرد یک طرح تهاجمی باشد. با نفوذ در مراحل چرخه اطلاعاتی اعم از گردآوری، تجزیه‌وتحلیل، ارزیابی یا بازخورد حریف به اجرا دربیاید و اینکه نخبگان دولت یا سازمان حریف، آماج اصلی این مأموریت باشند.
- **ارزیابی**: در گام نهایی، مأموریت بر مبنای شاخص‌های این الگو مورد ارزیابی قرار گرفته و بر این اساس که به انباشت تجربه، زمینه‌سازی برای نفوذ و شناخت نحوه درک قربانی منجر شده باشد، بازخورد مأموریت به دست طراحان و سیاست‌گذاران خواهد رسید.

این الگو تلاش دارد ضمن تقویت ادبیات بومی در حوزه مفهوم تهاجم اطلاعاتی، مسیرها و راهکارهای روشن‌تری برای تقویت و ارتقای امنیت ملی از طریق تدوین مدل فریب راهبردی با رویکرد تهاجم اطلاعاتی ارائه دهد. در عین حال که تلاش برای تقویت ادبیات تهاجم اطلاعاتی در دیگر موضوعات می‌تواند ضمن تولید دانش کاربردی در این موضوع، در حوزه عملیاتی نیز رویکردهای ایجابی و کنش‌ورزانه را برتری دهد. البته که اذعان می‌شود دسترس‌ناپذیری به منابع پنهان و هم‌چنین فقدان دسترسی به بخشی از کارشناسان و خبرگان موضوع، از کاستی‌های این پژوهش بوده که طبعاً می‌تواند در پژوهش‌های دیگر دانشجویان و پژوهشگران علاقه‌مند به این موضوع، مرتفع شده و نتایج دقیق‌تری را نمایان شود.

فهرست منابع

Almalki. Sami (2016), Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits, Journal of Education and Learning; Volume 5, Number 3.

Australian defense force, (2001), **Information Operations Planning Manual**

Caddell. Joseph (2004), deception 101: primer on deception, Army War College, Strategic Studies Institute

Cohen. Fred (2006), The Use of Deception Techniques: Honeypots and Decoys, **Handbook of Information Security**, Volume 3

Denning, Doherty (2004), Information Warfare and Security, Translators' Group, Tehran: Intelligent Signal Processing Research Institute. (In Persian).

Ebrahimi, Mansour (2007), **Psychological Operations and Strategic Deception**, Tehran: Abrar Moaser. (In Persian).

Erdie. Philip (2004), Network-Centric Strategic-Level Deception, Monterey, California. Naval Postgraduate School

Gerwehr. Scott, (2000), The Art of Darkness: Deception and Urban Operations

Godson. Roy (2000), Strategic Denial and Deception**, International Journal of Intelligence and Counter Intelligence**, Volume 13, Number 4, 2000

Hutchinson. William (2006), Information Warfare and Deception, **Informing Science**, Volume 9

Kiani, Ehsan (2021), Conceptualization of the Aggressive Approach to Information, Journal of Security Horizons, No. 51.

Latimer. Jon, (2001), Deception in war, John Murray, London

Libicki. Martin, (1999), **The Changing Role of Information in Warfare**, "Strategic Appraisal: The Changing Role of Information in Warfare", Publisher: Rand Corporation.

Machiavelli, Niccolo (2013), **The Prince**, translated by Ahmad Zarkesh, Tehran: Pajhwok Publishing. (In Persian).

Mottaqi, Ebrahim (2017), Semiotics of Influence in Iran's Foreign Policy, Journal of Security Horizons, No. 35.

Monoro. James (2012), **Deception**: **Theory and Practice,** Naval Postgraduate School.

Namazi, Mohammad (2003), "The Role of Qualitative Research in the Humanities", Journal of Geography and Development, No. 1. (In Persian).

Podhorec. Milan (2011), **Information Operations in the Command and Control Process at the Time of Their Planning**, Economics and Management of Faculty of Military Leadership in University of Defence.

Prunckun. Henry (2014), Extending the Theoretical Structure of Intelligence to Counterintelligence**, Salus Journal**, Issue 2, Number 2.

Reid. Iain, 2020, Toward a holistic model of deception: Subject matter expert validation, Proceedings of the 53rd Hawaii International Conference on System Sciences

Stein. Georg (1996), Information Attack, Information Warfare in 2025, Air War College

Shulusky. Abram (2000), Elements of strategic denial and deception, **Trends in Organized Crime**, Volume 6, Number 1

Sharp, Walter (2006), Military Deception, Joint Chiefs of Staff.

Soltanian, Hamid (2024), The United States' Psychological Operations Strategy Against the Islamic Republic of Iran's Nuclear Program, Journal of Security Horizons, No. 62.
Vandome. Roger (2010), From Intelligence to Influence: The Role of Information Operations, Centre for National Security Studies
Waltz. Edward, June (2000), Data Fusion in Offensive and Defensive Information Operations, National symposium of sensor and data fusion
Welch. Donald (1999), Strike Back: Offensive Actions in Information Warfare, United States Military Academy
Whaley. Barton (2008), Toward a general theory of deception, **Journal of Strategic Studies**, Volume 5, Issue 1
Woodcock. Alexander (1999), Information Operations in Support of Civil-Military Interactions, Conference Analysis of Civil-Military Interactions
Zand, Ebrahim (2017), **Generalities of Information Investigation**, Tehran: National Intelligence and Security Faculty Publications. (In Persian).
Zavidniak. Paul (1999), Achieving Information Resiliency, Information Technology Security Report, Volume 4, Number 3
Zolfaghari, Mehdi (2013), **Psychological Operations, Information Warfare and Strategic Deception**, Tehran: Imam Sadeq University Publications. (In Persian).